ΕΘΝΙΚΟ ΚΑΙ ΚΑΠΟΔΙΣΤΡΙΑΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Ασφάλεια Πληροφοριών σε Τραπεζικούς και Χρηματοπιστωτικούς Οργανισμούς

Σόλων Ε. Μαρμάρου

Παναγιώτης Α. Αυρηλιώνης

Επιβλέποντες: **Παναγιώτης Γεωργιάδης**, Καθηγητής ΕΚΠΑ

Κωνσταντίνος Παπαπαναγιώτου, Διδάκτωρ ΕΚΠΑ

ΑΘΗΝΑ

Οκτώβριος 2012

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Ασφάλεια Πληροφοριών σε Τραπεζικούς και Χρηματοπιστωτικούς Οργανισμούς

Σόλων Ε. Μαρμάρου

Α.Μ.: Μ1168

Παναγιώτης Α. Αυρηλιώνης

Α.Μ.: Μ1201

ΕΠΙΒΛΕΠΟΝΤΕΣ: **Παναγιώτης Γεωργιάδης**, Καθηγητής ΕΚΠΑ

Κωνσταντίνος Παπαπαναγιώτου, Διδάκτωρ ΕΚΠΑ

Οκτώβριος 2012

ΠΕΡΙΛΗΨΗ

Στην παρούσα διπλωματική γίνεται ανάλυση των ζητημάτων ασφάλειας πληροφοριών όσον αφορά τραπεζικούς και χρηματοπιστωτικούς οργανισμούς. Η ανάλυση γίνεται τόσο σε θεωρητικό επίπεδο με παρουσίαση των διεθνών προτύπων ασφάλειας όπως τα ISO 27001 / ISO 17799 και των ρυθμιστών αρχών στην Ελλάδα, όσο και σε πιο πρακτικό επίπεδο με υλοποίηση παραδειγμάτων πολιτικών ασφάλειας αλλά και τεχνική ανάλυση των κινδύνων και των αντίστοιχων μέτρων προστασίας. Επιπλέον γίνεται αναφορά στις τεχνικές εσωτερικού ελέγχου των πληροφοριακών συστημάτων και στο τέλος παρουσιάζονται μερικά γνωστά περιστατικά ασφάλειας σε τραπεζικούς - και όχι μόνο – οργανισμούς, καθώς και θέματα επιχειρησιακής συνέχειας.

ΘΕΜΑΤΙΚΗ ΠΕΡΙΟΧΗ: Ασφάλεια Πληροφοριακών Συστημάτων

ΛΕΞΕΙΣ ΚΛΕΙΔΙΑ: Ασφάλεια τραπεζικών οργανισμών, πολιτικές ασφάλειας πληροφοριών, διεθνή πρότυπα ασφάλειας, κανονιστική συμμόρφωση, εσωτερικός έλεγχος

ABSTRACT

In this thesis, is presented an analysis of the information security issues on banking and financial institutions. The analysis is performed both at a theoretical level by presentation of the international security standards such as ISO 27001 / ISO 17799 and regulative authorities in Greece, as well as with more practical examples by implementing of security policies and by a technical risk analysis and the corresponding measures of protection. Further reference is made to techniques of informational systems audit and finally, there is a presentation of some known security incidents in banking - and not only – organizations, and also are presented business continuity issues.

SUBJECT AREA: Information Systems Security

KEYWORDS: banking organizations security, information security policies, international security standards, PCI DSS, internal audit

ΠΕΡΙΕΧΟΜΕΝΑ

ΠΡΟΛΟΓΟΣ

Η παρούσα διπλωματική εργασία συντάχθηκε στα πλαίσια του μεταπτυχιακού κύκλου σπουδών του τμήματος Πληροφορικής και Τηλεπικοινωνιών του Εθνικού και Καποδιστριακού Πανεπιστημίου Αθηνών. Για την εκπόνησή της θα θέλαμε να ευχαριστήσουμε θερμά τον Διδάκτωρ ΕΚΠΑ Κωνσταντίνο Παπαπαναγιώτου, για το χρόνο που μας διέθεσε, τις πολύτιμες συμβουλές, παρατηρήσεις και διορθώσεις του, συμβάλλοντας σημαντικά στην ολοκλήρωση του συγκεκριμένου πονήματος.

ΚΕΦΑΛΑΙΟ 1

Εισαγωγή στην ασφάλεια τραπεζικών συστημάτων

1.1 Εισαγωγή στην ασφάλεια πληροφοριών

Ένας γενικός ορισμός της ασφάλειας πληροφοριών είναι: η προστασία των πληροφοριών και των συστημάτων πληροφοριών από μη εξουσιοδοτημένη πρόσβαση, χρήση, αποκάλυψη, διατάραξη, τροποποίηση, διάβασμα, επιθεώρηση, εγγραφή ή καταστροφή.

Οι όροι της ασφάλειας πληροφοριών, της ασφάλειας υπολογιστών και της διασφάλισης της πληροφορίας συχνά χρησιμοποιούνται εναλλακτικά. Τα πεδία αυτά είναι αλληλένδετα και συχνά μοιράζονται κοινούς στόχους για την προστασία της εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας της πληροφορίας. Ωστόσο, υπάρχουν κάποιες λεπτές διαφορές μεταξύ τους.

Οι διαφορές αυτές έγκεινται κυρίως στην προσέγγιση του θέματος, στις μεθοδολογίες που χρησιμοποιούνται, και στους τομείς που αφορούν. Η ασφάλεια πληροφοριών ασχολείται με την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα των δεδομένων, ανεξάρτητα από τη μορφή που μπορούν να λάβουν τα δεδομένα: ηλεκτρονική, εκτύπωση, ή άλλες μορφές. Η ασφάλεια υπολογιστών μπορεί να επικεντρωθεί στην εξασφάλιση της διαθεσιμότητας και της σωστής λειτουργίας του υπολογιστικού συστήματος, χωρίς να ενδιαφέρεται για τις πληροφορίες που αποθηκεύονται ή υποβάλλονται σε επεξεργασία από τον υπολογιστή. Η διασφάλιση της πληροφορίας επικεντρώνεται στους λόγους για διαβεβαίωση της προστασίας πληροφοριών, και είναι ως εκ τούτου αιτιολόγηση για την ασφάλεια πληροφοριών.

Κυβερνήσεις, στρατός, εταιρείες, χρηματοπιστωτικά ιδρύματα, νοσοκομεία, και ιδιωτικές επιχειρήσεις συγκεντρώνουν πολλές εμπιστευτικές πληροφορίες σχετικά με τους υπαλλήλους, τους πελάτες, τα προϊόντα, την έρευνα, και την οικονομική κατάστασή τους. Οι περισσότερες από αυτές τις πληροφορίες συλλέγονται, υποβάλλονται σε

επεξεργασία και αποθηκεύονται σε ηλεκτρονικούς υπολογιστές και μεταδίδονται μέσω δικτύων σε άλλους υπολογιστές.

Αν εμπιστευτικές πληροφορίες σχετικά με τους πελάτες ή τα οικονομικά στοιχεία μιας επιχείρησης ή μια νέα σειρά προϊόντων πέσουν στα χέρια ενός ανταγωνιστή, μια τέτοια παραβίαση της ασφάλειας μπορεί να οδηγήσει σε πολύ αρνητικές συνέπειες. Η προστασία των εμπιστευτικών πληροφοριών είναι μια απαίτηση των επιχειρήσεων, και σε πολλές περιπτώσεις, επίσης, μια ηθική και νομική υποχρέωση.

Ο τομέας της ασφάλειας πληροφοριών έχει εξελιχθεί σημαντικά τα τελευταία χρόνια. Υπάρχουν και πολλοί τρόποι για να εργασθεί κανείς στο χώρο. Διαθέτει πολλούς τομείς εξειδίκευσης όπως οι εξής: η διασφάλιση του δικτύου και συναφών υποδομών, η διασφάλιση εφαρμογών και βάσεων δεδομένων, οι δοκιμές ασφάλειας, ο έλεγχος των πληροφοριακών συστημάτων, ο σχεδιασμός της επιχειρησιακής, κλπ.

1.2 Η ασφάλεια πληροφοριών σε χρηματοπιστωτικούς οργανισμούς

Ο κλάδος των χρηματοπιστωτικών υπηρεσιών σε παγκόσμιο επίπεδο έχει γίνει το αντικείμενο της συζήτησης τα τελευταία χρόνια, και πιο πρόσφατα, λόγω της συνεχιζόμενης κρίσης.

Από την πλευρά των πληροφοριακών συστημάτων, οι τράπεζες είναι από τους πρώτους που εφάρμοσαν την τεχνολογία. Τάσεις όπως η εφαρμογή των προϊόντων πληροφορικής από τους καταναλωτές στους οργανισμούς (consumerization), η έλευση της κινητής (mobile) και της διαδικτυακής (internet) τραπεζικής (banking) και ο αυξανόμενος όγκος δεδομένων που οι τράπεζες είναι υποχρεωμένες να διαχειρίζονται σε καθημερινή βάση, απαιτούν από τα ιδρύματα σε αυτόν τον τομέα να βρίσκονται σε σημείο αιχμής σε τεχνολογία.

Αυτή η προχωρημένη τεχνολογικά προσέγγιση, ωστόσο, σημαίνει ότι καθώς η τεχνολογία εξελίσσεται με ταχείς ρυθμούς, οι επιχειρήσεις δεν μπορούν πάντα να είναι έτοιμες να αντιμετωπίσουν τις προκλήσεις που φέρνουν. Για παράδειγμα, πώς μπορεί ένας οργανισμός να διασφαλίσει ότι οι ταυτότητες χρηστών του mobile banking είναι αυθεντικές και νόμιμές; Πώς να διαχειριστεί αποτελεσματικά τις μεγάλες ποσότητες πληροφοριών και να αποκτήσει καλύτερες γνώσεις από αυτές; Και το πιο σημαντικό,

πώς μπορούν οι τράπεζες να τηρούν έναν αυξανόμενο αριθμό κανόνων και πλαισίων που διέπουν τον τρόπο με τον οποίο χειρίζονται τις πληροφορίες και προλαμβάνουν την απάτη;

Από τη συνθήκη Βασιλεία III έως τις πιο πρόσφατες κατευθυντήριες οδηγίες για την ασφάλεια πληροφοριών, οι τράπεζες σήμερα είναι υποχρεωμένες να εξασφαλίσουν την ασφάλεια. Αυτή είναι επίσης μια βασική κινητήρια δύναμη για την εμπιστοσύνη μεταξύ των πελατών τους, ιδίως μετά από επανειλημμένες επιθέσεις στον κυβερνοχώρο που έχουν προκαλέσει παραβιάσεις της ασφάλειας και που έγιναν πρωτοσέλιδα.

Για να το θέσουμε απλά, οι παραβιάσεις δεδομένων είναι μια πραγματικότητα που έχει απασχολήσει ολόκληρο τον τραπεζικό κλάδο - όχι μόνο μεμονωμένα ιδρύματα, αλλά και τους κορυφαίους φορείς και τις ρυθμιστικές αρχές. Το τοπίο της ασφάλειας όπως το βλέπουν τα σημερινά χρηματοπιστωτικά ιδρύματα αποτελείται από τρία πεδία:

- *Το μεταβαλλόμενο τοπίο των απειλών*, όπου αυξάνονται οι στοχευμένες επιθέσεις που αποσκοπούν στο να θέσουν σε κίνδυνο εμπιστευτικές πληροφορίες, συμπεριλαμβανομένων των δεδομένων των πελατών, των οικονομικών στοιχείων και δεδομένων επιχειρηματικής ευφυΐας, καθώς επίσης αυξάνονται και οι απώλειες που οφείλονται σε ψηφιακές επιθέσεις.
- *Το μεταβαλλόμενο τοπίο Τεχνολογίας Πληροφορικής (Information Technology - IT)*, όπου η αύξηση των συναλλαγών με τους πελάτες μέσω κινητής τηλεφωνίας και διαδικτύου, καθώς και η αυξανόμενη χρήση εμπορικών υπηρεσιών IT εντός της επιχείρησης ανοίγουν περισσότερους δρόμους για εμπιστευτικές πληροφορίες που μπορούν να τεθούν σε κίνδυνο.
- *Οι αλλαγές στο ρυθμιστικό τοπίο*, όπου η επιχειρηματικοί και κρατικοί φορείς «σφίγγουν» το περιβάλλον και θεσπίζουν ειδικούς κανόνες για την ελαχιστοποίηση των κινδύνων και τη διασφάλιση της ασφάλειας.

Σε ένα τέτοιο σενάριο, τα τραπεζικά ιδρύματα επικεντρώνονται όλο και περισσότερο στο να πάρουν τα μέγιστα από τα τμήματα IT τους, χωρίς να δίνουν αντάλλαγμα (trade-off) για την ασφάλεια. Σε ένα αντιδιαμετρικό σενάριο που καθοδηγείται από την εμπιστοσύνη, οι οργανισμοί δεν μπορούν να ανεχθούν καμία παραβίαση. Αυτός είναι ο λόγος που πρέπει να ακολουθήσουν μια προσέγγιση ασφάλειας που βασίζεται στον κίνδυνο και καθοδηγείται από μια πολιτική ασφάλειας, με επίκεντρο την πληροφορία και να συγκεκριμενοποιηθεί σε μια καλά διαχειριζόμενη υποδομή. Θα πρέπει να

αναπτύξουν και να εφαρμόσουν πολιτικές IT, να προστατεύσουν πληροφορίες και ταυτότητες, να προστατεύσουν την υποδομής και να διαχειριστούν αποτελεσματικά τα συστήματα.

Καθώς η ασφάλεια για ένα τραπεζικό ίδρυμα μπορεί να είναι ένα πολύπλοκο έργο, μια ολιστική στρατηγική μπορεί να διαρκέσει πολύ. Εδώ είναι μερικές προτάσεις για τους γενικούς διευθυντές IT και τους υπεύθυνους ασφαλείας των τραπεζικών ιδρυμάτων:

- Οι χρηματοπιστωτικοί οργανισμοί πρέπει να προστατεύσουν την υποδομή τους διασφαλίζοντας τα τελικά σημεία τους (endpoints), τα μηνύματα και τα Web περιβάλλοντα. Επιπλέον προτεραιότητες θα πρέπει να είναι η προστασία των κρίσιμων εσωτερικών servers και η δυνατότητα δημιουργίας αντιγράφων ασφαλείας και ανάκτησης δεδομένων. Οι οργανισμοί χρειάζονται επίσης την προβολή και την νοημοσύνη ως προς την ασφάλεια για τη γρήγορη αντιμετώπιση των απειλών.
- Οι διαχειριστές IT πρέπει να προστατεύσουν τις πληροφορίες προληπτικά λαμβάνοντας μια πληροφοριοκεντρική προσέγγιση για την προστασία τόσο των πληροφοριών όσο και των αλληλεπιδράσεων. Η λήψη μιας προσέγγισης επίγνωσης περιεχομένου για την προστασία των πληροφοριών είναι το κλειδί για να γνωρίζει πού βρίσκονται ευαίσθητες πληροφορίες, ποιος έχει πρόσβαση, και πώς εισέρχονται ή εξέρχονται από τον οργανισμό.
- Οι οργανισμοί πρέπει να αναπτύξουν και να εφαρμόσουν πολιτικές IT και να αυτοματοποιήσουν τις διαδικασίες συμμόρφωσης τους. Με την ιεράρχηση των κινδύνων και τον καθορισμό των πολιτικών που εκτείνονται σε όλες τις τοποθεσίες, οι πελάτες μπορούν να επιβάλλουν πολιτικές μέσω ενσωματωμένου αυτοματισμού και ροής εργασίας και όχι μόνο να εντοπίζουν τις απειλές αλλά και να αποκαταστήσουν περιστατικά που συμβαίνουν ή να τα προβλέψουν πριν συμβούν.
- Οι οργανισμοί πρέπει να διαχειρίζονται τα συστήματα μέσω της εφαρμογής ασφαλών περιβαλλόντων λειτουργίας, διανέμοντας και επιβάλλοντας το επίπεδο των patch, αυτοματοποιώντας διαδικασίες για τον εξορθολογισμό της αποδοτικότητας, καθώς και παρακολουθώντας την υποβολή εκθέσεων σχετικά με την κατάσταση του συστήματος.

1.3 Οι πιο σημαντικές απειλές για τους Οργανισμούς

Η καταγραφή των απειλών που απειλούν τα χρηματοπιστωτικά ιδρύματα και προκαλούν τους επαγγελματίες της ασφάλειας αποτελεί μια ατέρμονη μάχη. Από το οργανωμένο έγκλημα έως τις τεχνικές SQL injection, παρουσιάζουμε τις επιλογές των εμπειρογνωμόνων των οκτώ μεγάλων απειλών για την ασφάλεια που χρήζουν προσοχής:

1. Το οργανωμένο έγκλημα που στοχεύει Τραπεζικά συστήματα

   Κατά τα τελευταία χρόνια, οι έρευνες των αστυνομικών αρχών στον κυβερνοχώρο έχουν αποκαλύψει παγκόσμια δίκτυα ομάδων οργανωμένου εγκλήματος (πολλά βασίζονται στην Ανατολική Ευρώπη) που προσλαμβάνουν και κατευθύνουν hackers. Ο συνδυασμός των μη ασφαλών συστημάτων, του κίνητρου λόγω των πολλών χρημάτων στις τράπεζες και της έλλειψης τιμωρίας στους ενόχους ισοδυναμούν με μεγάλες πιθανότητες ώστε να δραστηριοποιηθούν αυτές οι ομάδες.

2. Επίθεση στην αυθεντικοποίηση

   Οι τραπεζικές ρυθμιστικές αρχές έχουν ζητήσει εδώ και καιρό την υποχρεωτική πιστοποίηση δύο παραγόντων για όλα τα online banking sites. Τώρα, ειδικοί σε θέματα ασφάλειας της βιομηχανίας προειδοποιούν ότι οι επιθέσεις κατά των παραδοσιακών μεθόδων ελέγχου ταυτότητας πελάτη είναι υπό αμφισβήτηση και μπορούν να «νικηθούν».

   Λέγεται ότι οι απειλές περιλαμβάνουν επιθέσεις στο πρόγραμμα περιήγησης (man-in-the-browser attack) που «νικούν» την πιστοποίηση κωδικού μιας χρήσης από ειδικό κουπόνι (όπως το δημοφιλές SecureID), καθώς και προωθήσεις κλήσεων που υποκλέπτουν την αυθεντικοποίηση μέσω τηλεφώνου και την επαλήθευση συναλλαγών μέσω SMS. Αυτά αποτελούν άσχημα νέα για τις τράπεζες που χρησιμοποιούν αυτές τις τεχνικές για την προστασία λογαριασμών και συναλλαγών υψηλής αξίας.

3. Περισσότερο κακόβουλο λογισμικό

   Οι αριθμοί λένε ότι ποσοστό της μόλυνσης προσωπικών υπολογιστών από κακόβουλου λογισμικού ήταν 10 φορές υψηλότερα κατά τη διάρκεια του 2009 σε σύγκριση με το 2008.

Ολοένα και περισσότερο, εκλεπτυσμένο και κατανεμημένο κακόβουλο λογισμικό φαίνεται στην διερεύνηση των εγκλημάτων στον κυβερνοχώρο, Οι εγκληματίες προσθέτουν επίσης μια γεύση κοινωνικής μηχανικής για να προωθήσουν το κακόβουλο λογισμικό σε μηχάνημα του χρήστη. Τα μεγάλης κλίμακας botnets αυξάνονται και σε αριθμό, και η ποιότητα του κώδικα βελτιώνεται, καθώς αυτά τα είδη malware χρηματοδοτούνται όλο και περισσότερο από εγκληματικές οργανώσεις.

4. Επιστροφή στην απάτη μέσω τηλεφώνου

Καθώς οι οργανισμοί ενισχύουν την online ασφάλειά τους, πολλοί απατεώνες στράφηκαν προς την παραδοσιακή απάτη μέσω τηλεφωνίας.

Οπλισμένοι με τα δεδομένα που έχουν κλαπεί μέσω trojans και επιθέσεων phishing - συμπεριλαμβανομένων των «vishing» (voice phishing), «smishing» (SMS phishing) και παραλλαγών του spear phishing, απατεώνες καλούν την εξυπηρέτηση πελατών στις τράπεζες, πιστωτικές ενώσεις και εταιρείες πιστωτικών καρτών, προκειμένου να εκτελέσουν την απάτη που ονομάζεται απόκτηση ελέγχου του λογαριασμού (account takeover).

5. Αυξανόμενη εσωτερική απειλή

Ο αξιόπιστος εσωτερικός παράγοντας (insider) είναι ο πιο επικίνδυνος εχθρός για κάθε οργανισμό - και αυτός που πρέπει να φοβούνται, όπως φαίνεται από τα ποσά και τα δεδομένα που λαμβάνονται από insiders.

Επικίνδυνοι για να απειλήσουν τον οργανισμό είναι άτομα με οικονομικά προβλήματα που μπορεί να οδηγηθούν στο έγκλημα αλλά και άτομα που δεν είναι μόνιμοι εργαζόμενοι και έχουν αρκετές γνώσεις των IT συστημάτων. Ακόμη μπορεί κάποιοι να μην γνωρίζουν ότι έχουν εμπλακεί σε μια τέτοια απειλή σε περίπτωση που μολυνθούν οι υπολογιστές τους με οικονομικά trojans με στόχο αυτούς και τα εταιρικά PC τους και laptops.

6. Επιθέσεις κινητής τραπεζικής (mobile banking)

Η υπηρεσία του mobile banking από τα χρηματοπιστωτικά ιδρύματα είναι πολύ δημοφιλής, με εκατοντάδες ιδρύματα τώρα να προσφέρουν στους πελάτες τη δυνατότητα να αναζητήσουν τα στοιχεία του λογαριασμού τους και το υπόλοιπο τους μέσω των κινητών τους τηλεφώνων. Ωστόσο, οι ειδικοί σε θέματα ασφάλειας

βλέπουν προβλήματα όταν τα ιδρύματα αρχίζουν να επιτρέπουν στους πελάτες κάτι περισσότερο από ελέγχους στο υπόλοιπο του λογαριασμού τους.

Η ευκαιρία για απάτη μέσω του κινητού τηλεφώνου υπάρχει ήδη και εκμεταλλεύεται τη συνεχώς αυξανόμενη βάση των έξυπνων τηλεφώνων, με αποτέλεσμα την πιθανή δημιουργία ενός δικτύου μολυσμένων μηχανών (botnet) που βασίζεται σε iPhone ή Android τηλέφωνα. Μέρος του προβλήματος είναι ότι οι πελάτες δεν δίνουν πάντα προσοχή σε ό,τι λαμβάνουν στο κινητό τους

7. Επιθέσεις μέσω WEB 2.0 και ιστοσελίδων κοινωνικής δικτύωσης

Την ίδια ώρα που οι οργανισμοί συρρέουν στο Facebook και στο Twitter, οι εγκληματίες του κυβερνοχώρου οργανώνουν τα οπλοστάσιά τους για την επίθεση μέσω Web 2.0 εφαρμογών και μέσω των κοινωνικών δικτύων. Οι επιθέσεις μέσω ιστοσελίδων κοινωνικής δικτύωσης είναι ο νέος τρόπος για τους εγκληματίες να μπουν σε τραπεζικούς λογαριασμούς. Αυτές οι περιοχές χρησιμοποιούνται από τους «κακούς» για την αναγνώριση για να μάθουν περισσότερα σχετικά με τους στόχους τους ενώ την ίδια στιγμή, παραδίδουν κακόβουλο περιεχόμενο σε ανυποψίαστους χρήστες.

8. Περισσότερες επιθέσεις SQL έρχονται στο μέλλον

Η μεγαλύτερη καταγεγραμμένη παραβίαση δεδομένων - στη Heartland Payment Systems - έγινε με τη χρήση επίθεσης SQL injection. Οι SQL επιθέσεις είναι ένας δημοφιλής τρόπος για να μολύνουν οι hackers τις ιστοσελίδες και στη συνέχεια να πάρουν τον έλεγχο τους

1.4 Η σημασία της ασφάλειας στο Internet Banking

Τα τελευταία χρόνια, οι συντριπτικές δυνατότητες του Διαδικτύου έχουν γίνει όλο και περισσότερο ενδιαφέρουσες για τις τράπεζες, δεδομένου ότι ανοίγουν μια νέα διεπαφή με τον πελάτη. Την ίδια στιγμή, οι δυνατότητες του Διαδικτύου δεν φαίνεται να έχουν αξιοποιηθεί πλήρως ακόμη. Η χρήση του Διαδικτύου είναι σε πολλές περιπτώσεις η δυνατότητα να προσφέρουν σύγχρονες τραπεζικές υπηρεσίες με επίκεντρο τον πελάτη καθώς και για εξοικονόμηση κόστους.

Νέες απειλές έχουν ανακύψει με αυτή τη νέα τεχνολογία και την ευρεία χρήση της. Αν τα τραπεζικά ιδρύματα θέλουν να επωφεληθούν από τις μεγάλες δυνατότητες της, θα

πρέπει να αντιμετωπίσουν τις προκλήσεις των νέων αυτών απειλών κατά της ασφάλειας. Βλέπουμε μια νέα κατηγορία απατεώνων με ένα ευρύ φάσμα δόλιων μεθόδων και ιδεών. Ο τραπεζικός τομέας έχει, επομένως, ανάγκη από νέες στρατηγικές και μέτρα ασφαλείας.

Δεν είναι μόνο η τράπεζα, αλλά και οι πελάτες της οι οποίοι θέλουν να επωφεληθούν από online τραπεζικές υπηρεσίες κι έτσι αναγκάζονται να αντιμετωπίσουν αυτές τις απειλές ασφαλείας. Ειδικά για τους προσωπικούς υπολογιστές πελατών, η τράπεζα έχει λίγες έως καθόλου δυνατότητες για τη λήψη μέτρων προς εφαρμογή των προτύπων της. Το ερώτημα είναι αν ο πελάτης αποδέχεται την ευθύνη για τον υπολογιστή του/της και πώς αυτή η ευθύνη σχετίζεται με την προθυμία του/της να πληρώσει για ένα υψηλότερο επίπεδο ασφαλείας. Πρόσφατα, η νομοθεσία έχει αρχίσει να αγκαλιάζει το ζήτημα της ευθύνης και να επιβάλει την ευθύνη στον πελάτη. Εάν η ευθύνη είναι αποδεκτή από τους πελάτες, είναι σημαντικό να διερευνηθεί τι κινδύνους αντιλαμβάνονται οι πελάτες στις online τραπεζικές συναλλαγές και να γίνουν επενδύσεις σε κατάλληλες υπηρεσίες και προϊόντα.

Μερικά ενδεικτικά γεγονότα για το internet banking είναι τα παρακάτω:

- Τα ζητήματα ασφαλείας είναι ένας σημαντικός παράγοντας στη διαδικασία λήψης αποφάσεων για την επιλογή της τράπεζας από τους πελάτες.
- Ένας σημαντικός αριθμός των ευρωπαίων πελατών τραπεζών θεωρεί ότι υπάρχει αρκετά μεγάλος κίνδυνος ότι ένα μη εξουσιοδοτημένο πρόσωπο μπορεί να αποκτήσει πρόσβαση στον τραπεζικό λογαριασμό τους.
- Σε περίπτωση σοβαρών περιστατικών ασφάλειας 76% των πελατών δηλώνουν ότι θα μεταφέρουν τον τραπεζικό λογαριασμό τους σε άλλο τραπεζικό ίδρυμα.
- Οι πελάτες θέλουν να είναι (καλύτερα) ενημερωμένοι για τα μέτρα ασφαλείας που λαμβάνονται από την τράπεζα και η ευαισθητοποίηση τους θα αυξηθεί περαιτέρω, σύμφωνα με επαγγελματίες της τραπεζικής ασφάλειας.
- Οι ανησυχίες για την ασφάλεια είναι ένα κεντρικό επιχείρημα για να μην χρησιμοποιούν online τραπεζικές υπηρεσίες.
- Οι πελάτες έχουν την εντύπωση ότι η ασφάλεια του internet banking θα βελτιωθεί αισθητά τα επόμενα χρόνια, κάτι που δεν προκύπτει σύμφωνα με έρευνες.

Από τα παραπάνω γίνεται φανερό ότι οι τραπεζικοί οργανισμοί πρέπει να μελετήσουν τα θέματα ασφάλειας του internet banking εξειδικευμένα καθώς αποτελούν τον πιο σημαντικό παράγοντα για τη χρήση της υπηρεσίας αυτής.

1.5 Ιδιαιτερότητες της ασφάλειας πληροφοριών τραπεζικών οργανισμών σε σχέση με άλλους τύπους οργανισμών

Η ασφάλεια πληροφοριών αφορά όλους τους τύπους οργανισμών όπως είναι οι κυβερνητικοί οργανισμοί, οι τηλεπικοινωνιακοί, ο στρατός, οι εμπορικές επιχειρήσεις και άλλες. Στην παρούσα εργασία παρουσιάζουμε πρότυπα, πολιτικές και τεχνικές ασφάλειας που εφαρμόζονται σε κάθε είδος οργανισμού περιλαμβανομένων και των χρηματοπιστωτικών ιδρυμάτων για τα οποία κάνουμε ειδική αναφορά σε συγκεκριμένα ζητήματα. Τα χρηματοπιστωτικά ιδρύματα έχουν κάποιες ιδιαιτερότητες που τα διαφοροποιούν από οργανισμούς άλλου είδους. Παρακάτω παρουσιάζουμε κάποιες από αυτές:

- Τα οικονομικά μεγέθη: Το χρήμα αποτελεί τον πιο σημαντικό παράγοντα στην καθημερινότητα των ανθρώπων καθώς είναι το μέσο με το οποίο αμείβονται για την εργασία τους και το μέσο για την απόκτηση των αγαθών. Οι τράπεζες σε αυτό παίζουν τον κύριο ρόλο καθώς μέσω αυτών διακινείται όλο το χρήμα που διατίθεται στην αγορά. Αυτό τις κάνει ελκυστικούς στόχους για τους κακοποιούς καθώς τα οφέλη από παράνομες πράξεις μπορεί να είναι τεράστια. Είναι λοιπόν κατανοητό πως για την ασφάλεια πληροφοριών σχετικά με το χρήμα πρέπει να δοθεί η μεγαλύτερη σημασία στους χρηματοπιστωτικούς οργανισμούς. Οικονομικά μεγέθη αποτελούν και οι άλλοι τύποι οργανισμών όπως είναι οι επιχειρήσεις και οι τηλεπικοινωνιακοί πάροχοι αλλά σε πολύ μικρότερη κλίμακα.
- Η εξάρτηση από την τεχνολογία: Όπως είπαμε οι τράπεζες είναι από τους πιο ένθερμους υποστηρικτές τις τεχνολογίας καθώς έχουν εμφανιστεί πολλές τραπεζικές υπηρεσίες που σχετίζονται με την πληροφορική όπως είναι το internet banking και το mobile banking. Όσο πιο εκτεθειμένος είναι ένας οργανισμός στην τεχνολογία τόσο μεγαλύτερο πεδίο υπάρχει διαθέσιμο για πιθανές παραβιάσεις. Επίσης υπάρχουν πεδία που δεν βρίσκονται στην άμεση δικαιοδοσία των οργανισμών αλλά αφορούν τους τελικούς χρήστες οι οποίοι πρέπει να

προστατευτούν κι αυτοί. Εντός του οργανισμού υπάρχουν κι άλλες διαδικασίες οι οποίες δεν αφορούν υπηρεσίες των χρηστών αλλά είναι εξαιρετικά ευαίσθητες και πρέπει να προστατεύονται (π.χ. πληροφορίες διατραπεζικών συναλλαγών, χρηματιστηριακές πληροφορίες κλπ). Σε άλλου τύπου εμπορικές επιχειρήσεις πιθανόν να υπάρχει εξάρτηση από την τεχνολογία αλλά μπορεί και να μην υπάρχει και σίγουρα δεν θα διακυβεύονται τόσο πολλά. Επίσης τα πιο παλιά χρόνια, πριν την ηλεκτρονική εποχή, δεν υπήρχε τόσο μεγάλη ανάγκη για ασφάλεια καθώς τα λεφτά και οι πληροφορίες λογαριασμών ήταν σε έντυπη μορφή και το μόνο που χρειαζόταν ο οργανισμός ήταν φυσική ασφάλεια κτιρίου.

- Η αλληλεπίδραση μεταξύ τραπεζικών ιδρυμάτων: Στον τραπεζικό κλάδο υπάρχει μεγάλη αλληλεπίδραση μεταξύ των ιδρυμάτων κάτι που δημιουργεί επιπλέον πεδία για πιθανές ευπάθειες. Η αλληλεπίδραση δεν περιορίζεται μόνο εντός της κάθε χώρας αλλά μπορεί να επεκταθεί σε παγκόσμια κλίμακα. Για παράδειγμα μπορεί να πραγματοποιούνται συναλλαγές μεταξύ χρηματοπιστωτικών ιδρυμάτων που βρίσκονται σε διαφορετικές ηπείρους και για να πραγματοποιηθούν να πρέπει να παρεμβάλλονται πολλοί ενδιάμεσοι φορείς. Τόσο μεγάλη αλληλεπίδραση δεν υπάρχει σε κανέναν άλλο τομέα. Συνήθως σε άλλους τομείς, όπως είναι ο στρατός ή ένας κυβερνητικός οργανισμός, η μετάδοση της πληροφορίας δεν εξέρχεται από τον οργανισμό πόσο μάλλον από τη χώρα. Μόνο στον τομέα των τηλεπικοινωνιών μπορεί να υπάρξει παρόμοια αλληλεπίδραση μεταξύ απομακρυσμένων παρόχων αλλά η πληροφορία που μεταδίδεται σε όλη την αλυσίδα συνήθως δεν είναι τόσο κρίσιμη όσο είναι για τραπεζικές συναλλαγές.
- Η αλληλεπίδραση μεταξύ τραπεζικών οργανισμών και οργανισμών άλλου τύπου: Λόγω της ιδιαιτερότητας του χρήματος που λειτουργεί σαν εργαλείο αγοραπωλησιών οι τραπεζικοί οργανισμοί πολλές φορές λειτουργούν σαν ενδιάμεσοι φορείς για αλληλεπιδράσεις μεταξύ όλων των τύπων των οργανισμών. Για παράδειγμα για πληρωμές μεταξύ εμπορικών επιχειρήσεων μέσω τραπέζης, για μισθοδοσία δημόσιων και ιδιωτικών υπαλλήλων, για πληρωμές στρατιωτικών εξοπλισμών και για πολλά άλλα σχήματα που μπορούν να προκύψουν. Αυτό δίνει ακόμα μεγαλύτερο βάρος στην ασφάλεια πληροφοριών σε τραπεζικά ιδρύματα.

ΚΕΦΑΛΑΙΟ 2

Διεθνή Πρότυπα Ασφάλειας Οργανισμών

2.1 Διεθνή πρότυπα ασφάλειας Πληροφοριακών Συστημάτων

Τα τελευταία χρόνια βλέπουμε στο χώρο της ασφάλειας πληροφοριών ολοένα και περισσότερο καθορισμένες και συγκεκριμένες απαιτήσεις, οι οποίες πηγάζουν κατ' ευθείαν από τα συμβούλια εταιρικής διακυβέρνησης των μεγάλων οργανισμών. Καθώς η τεχνολογία των πληροφοριών έχει καταστεί κυρίαρχη, υποστηρίζοντας σχεδόν κάθε πτυχή του οργανισμού, διαχειρίζοντας και αποθηκεύοντας τις πληροφορίες από τις οποίες ο οργανισμός εξαρτάται για την επιβίωσή του, έτσι και ο ρόλος της πληροφορικής στην εταιρική διακυβέρνηση έχει γίνει πιο ξεκάθαρα καθορισμένος και η διακυβέρνηση της τεχνολογίας πληροφορικής αναγνωρίζεται όλο και περισσότερο ως μια ειδική περιοχή που τραβάει την προσοχή των διοικητικών συμβουλίων και των οργανισμών συνολικά. Μια βασική πτυχή της διακυβέρνησης της Τεχνολογίας Πληροφορικής είναι η προστασία της πληροφορίας – η διαθεσιμότητα, η εμπιστευτικότητα και η ακεραιότητα – από την οποία εξαρτώνται όλες οι εταιρικές διαδικασίες.

Παράλληλα, έχουν προκύψει τα διεθνή πρότυπα που σχετίζονται με την ασφάλεια των πληροφοριών τα οποία έχουν καταστεί ακρογωνιαίος λίθος ενός αποτελεσματικού πλαισίου διακυβέρνησης Τεχνολογίας Πληροφορικής. Τα βασικά πρότυπα τα οποία και θα αναλύσουμε είναι το ISO/IEC 17799 ή αλλιώς ISO/IEC 27002 και το ISO/IEC 27001.

2.1.1 Τα πρότυπα ασφάλειας των πληροφοριών

Το πρότυπο ISO27001 αποτέλεσε συνέχεια του προτύπου BS7799, το οποίο δημιουργήθηκε το 1995, από το Βρετανικό Ινστιτούτο Προτύπων. Ήταν ένα πρότυπο για να καθοδηγήσει την ανάπτυξη και υλοποίηση ενός Συστήματος Διαχείρισης Ασφαλείας Πληροφοριών, κοινώς γνωστό ως ISMS (International Security Management System).

Το BS7799 επινοήθηκε, από την αρχή, ως ένα τεχνολογικά ουδέτερο σύστημα διαχείρισης το οποίο, με κατάλληλη υλοποίηση, θα επέτρεπε στη διοίκηση ενός

οργανισμού να βεβαιώνεται ότι τα μέτρα ασφάλειας πληροφόρησης ήταν αποτελεσματικά.

Το BS7799 εστιάζεται στην προστασία της διαθεσιμότητας, εμπιστευτικότητας και ακεραιότητας των πληροφοριών του οργανισμού, και αυτοί παραμένουν και σήμερα οι κινητήριοι στόχοι του προτύπου. Κυρίως όμως, δεν μιλάει για προστασία από κάθε πιθανή απειλή, αλλά μόνο από εκείνες που ο οργανισμός θεωρεί σχετικές και μόνο στο βαθμό που δικαιολογείται οικονομικά και εμπορικά μέσω εκτίμησης του κινδύνου.

Το BS7799 αρχικά ήταν ένα απλό πρότυπο, και χαρακτηριζόταν σαν Κώδικας Πρακτικής (Code of Practice). Με άλλα λόγια, παρείχε καθοδήγηση για οργανισμούς, αλλά δεν ήταν γραμμένο σαν προδιαγραφές που θα μπορούσαν να αποτελέσουν τη βάση για μια επαλήθευση από εξωτερικούς τρίτους παράγοντες και για ένα σχήμα πιστοποίησης.

Καθώς όλο και περισσότεροι οργανισμοί άρχισαν να αναγνωρίζουν την έκταση, τη σοβαρότητα και τη διασύνδεσιμότητα των απειλών κατά της ασφάλειας πληροφοριών, και με την εμφάνιση ενός όλο και μεγαλύτερου φάσματος προστασίας δεδομένων και αντίστοιχης νομοθεσίας σχετικής με την ιδιωτικότητα, έτσι και η απαίτηση για μια επιλογή πιστοποίησης που συνδέεται με το πρότυπο άρχισε να αναπτύσσεται. Αυτό οδήγησε, τελικά, στην εμφάνιση ενός δεύτερου μέρους του προτύπου με τη μορφή προδιαγραφών (μία προδιαγραφή χρησιμοποιεί λέξεις όπως «πρέπει»), και απαριθμείται ως BS7799-2 (ή, μέρος 2).

Ο Κώδικας Πρακτικής (ο οποίος χρησιμοποιεί λέξεις όπως «μπορεί» και ο οποίος ασχολείται με τους ελέγχους, όχι με Συστήματα Διαχείρισης Ασφάλειας Πληροφοριών), αναγνωρίζονταν για πολλά χρόνια σαν ISO17799 ή/και BS7799-1 (ή, μέρος 1). Τώρα πλέον έχει επανεκδοθεί με το νέο αριθμό ISO27002. Η σχέση μεταξύ του κώδικα πρακτικής και της προδιαγραφής καθιερώνεται επίσης: μια προδιαγραφή είναι η βάση για τα συστήματα πιστοποίησης και το ISO27001 επιβάλει τη χρήση του ISO27002 ως πηγή καθοδήγησης για την επιλογή και την εφαρμογή των ελέγχων που επιβάλλονται από το πρότυπο ISO27001. Στην πράξη, το πρότυπο ISO27002 είναι το δεύτερο μέρος του προτύπου ISO 27001.

Η πιο πρόσφατη έκδοση του κώδικα πρακτικής, και αυτή που πρέπει να χρησιμοποιείται, είναι το ISO / IEC 27002:2005. Το BS7799-2: 2002 έχει επίσης υποστεί την αναθεώρηση και τη διεθνοποίηση, και αντικαταστάθηκε, το Νοέμβριο του 2005 από το ISO / IEC 27001:2005. Έτσι το BS7799-2: 2002 έχει πλέον αποσυρθεί.

2.1.2 Η Ασφάλεια Πληροφοριών και τα ρυθμιστικά περιβάλλοντα

Οι δυο κύριοι λόγοι για το αυξανόμενο ενδιαφέρον για πιστοποίηση στο ISO27001 είναι ο πολλαπλασιασμός των απειλών και το αυξανόμενο εύρος ρυθμιστικών και κανονιστικών απαιτήσεων που σχετίζονται με την προστασία των πληροφοριών.

Οι απειλές για την ασφάλεια πληροφοριών έχουν παγκόσμιο χαρακτήρα, και στοχεύουν αδιακρίτως σε κάθε οργανισμό ή μεμονωμένο άτομο που κατέχει ή χρησιμοποιεί (κυρίως) ηλεκτρονικές πληροφορίες. Οι απειλές αυτές είναι αυτοματοποιημένες και ελεύθερες στο διαδίκτυο. Επιπλέον, τα δεδομένα είναι εκτεθειμένα σε πολλούς άλλους κινδύνους, από φυσικές καταστροφές ή εξωτερικές επιθέσεις έως και διαφθορά ή κλοπή εκ των έσω.

Τα τελευταία δέκα χρόνια έχει εμφανιστεί επίσης μια αυξανόμενη ποσότητα νομοθετικών ρυθμίσεων γύρω από την ασφάλεια πληροφοριών και δεδομένων, Η νομοθεσία αποσκοπεί είτε στη διασφάλιση ότι τα ατομικά στοιχεία προστατεύονται είτε αποσκοπεί στην εξασφάλιση ότι τα οικονομικά της εταιρίας, η λειτουργική διαχείριση και τα συστήματα διαχείρισης κινδύνων υποστηρίζονται κατάλληλα.

Ένα τυπικό Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών, το οποίο παρέχει καθοδήγηση για την ανάπτυξη των βέλτιστων πρακτικών, θεωρείται όλο και περισσότερο ως μια αναγκαιότητα όσον αφορά τη συμμόρφωση και η πιστοποίηση απαιτείται όλο και περισσότερο από του οργανισμούς (και τις κυβερνήσεις) πριν θα συμμετάσχουν σε σημαντικές εμπορικές συναλλαγές με πιθανούς νέους προμηθευτές. Οι συνέπειες του γεγονότος αυτού για τη βιομηχανία αναθέσεων (outsourcing) είναι αυτονόητες.

2.1.3 Πιστοποίηση έναντι συμμόρφωσης

Είναι δυνατόν για έναν οργανισμό να αναπτύξει Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών (ΣΔΑΠ) σύμφωνα με το πρότυπο ISO27002 μόνο, επειδή η καλή πρακτική που προσδιορίζεται στον παρόντα Κώδικα Πρακτικής είναι γενικής εφαρμογής. Ωστόσο, επειδή δεν είχε σχεδιαστεί για να αποτελέσει τη βάση ενός συστήματος πιστοποίησης, δεν διευκρινίζει τις απαιτήσεις του συστήματος με τις οποίες ένα ΣΔΑΠ πρέπει να συμφωνεί, αν ώστε να είναι και πιστοποιημένο.

Το πρότυπο ISO27001 περιέχει αυτές τις προδιαγραφές. Σε τεχνικούς όρους, αυτό σημαίνει ότι ένας οργανισμός που χρησιμοποιεί μόνο το ISO27002 μπορεί να είναι

σύμφωνος με την καθοδήγηση του κώδικα πρακτικής, αλλά δεν μπορεί να βεβαιωθεί από έναν εξωτερικό οργανισμό ότι συμμορφώνεται με το πρότυπο. Ένας οργανισμός που χρησιμοποιεί ISO27001 και ISO27002 σε συνδυασμό μεταξύ τους μπορεί να σχεδιάσει ένα ΣΔΑΠ που είναι σύμφωνο με τις προδιαγραφές και το οποίο ακολουθεί τις οδηγίες του κώδικα πρακτικής και το οποίο είναι επομένως ικανό να επιτύχει εξωτερική πιστοποίηση.

2.1.4 Πιστοποίηση και άλλα πρότυπα διαχείρισης

Το ISO27001 έχει σχεδιαστεί ώστε να είναι συμβατό με άλλα πρότυπα διαχείρισης, όπως ISO9001 και ISO14001. Είναι επίσης συμβατό με το πρότυπο ISO/IEC 20000:2005. Οι απαιτήσεις διαχείρισης εγγράφων έχουν σχεδιαστεί ώστε να είναι συμβατά και να επιτρέπουν στους οργανισμούς να αναπτύξουν συστήματα διαχείρισης που ενσωματώνουν στο μεγαλύτερο δυνατό βαθμό τις απαιτήσεις του καθενός από τα πρότυπα διαχείρισης που η οργάνωση χρησιμοποιεί.

Σε γενικές γραμμές, οι οργανώσεις θα πρέπει να επιδιώξουν πιστοποίηση ISO27001 από τον οργανισμό πιστοποίησης που χρησιμοποιούν τώρα για την πιστοποίηση ISO9000 ή άλλο σύστημα διαχείρισης. Η εμπειρία του διευθυντή ποιοτικού ελέγχου του οργανισμού στη διαδικασία αυτή θα είναι πολύτιμη για την υλοποίηση του έργου του ΣΔΑΠ. Δεν υπάρχει κάποιος περιορισμός ώστε οι οργανισμοί να μην ασχοληθούν με το ISO27001 χωρίς να έχουν εφαρμόσει πρώτα κάποια άλλη μορφή συστήματος διαχείρισης. Στην περίπτωση αυτή, τότε θα επιλέξουν ένα φορέα πιστοποίησης σε εμπορική βάση μεταξύ εκείνων που είναι διαθέσιμοι και λειτουργούν στη χώρα τους.

Ένας φορέας πιστοποίησης θα πρέπει να έχει πρώτα πιστοποιηθεί από έναν εθνικό οργανισμό διαπίστευσης ώστε να έχει τη δυνατότητα να μεταφέρει διαπιστευμένες πιστοποιήσεις και να απονέμει το σχετικό σήμα που δηλώνει επίσημα την πιστοποίηση. Οι περισσότερες χώρες έχουν τις δικές τους υπηρεσίες διαπίστευσης και οι οποίες διατηρούν όλες τις λίστες των οργανισμών οι οποίοι είναι διαπιστευμένοι για ΣΔΑΠ πιστοποιήσεις.

2.1.5 Εθνικό Σύστημα Διαπίστευσης

Στην Ελλάδα με το άρθρο 11 του Νόμου 3066/2002 ιδρύθηκε η ανώνυμη εταιρεία με την επωνυμία **Εθνικό Σύστημα Διαπίστευσης Α.Ε.** και το διακριτικό τίτλο **ΕΣΥΔ**. Εταιρεία λειτουργεί χάριν του δημόσιου συμφέροντος και υπόκειται στην εποπτεία και τον έλεγχο του Κράτους από το Υπουργείο Ανάπτυξης. Η πρωταρχική δραστηριότητα του ΕΣΥΔ είναι να χορηγεί πιστοποιητικά διαπίστευσης σε φορείς πιστοποίησης, φορείς επιθεώρησης και ελέγχου, σε περιβαλλοντικούς επαληθευτές, σε εργαστήρια δοκιμών και εργαστήρια μετρολογίας, που έχουν την έδρα τους ή υποκαταστήματά τους στην Ελλάδα ή στην αλλοδαπή.

Παρακάτω παρουσιάζουμε ένα πραγματικό παράδειγμα αυτής της δομής:

- Ο ΕΣΥΔ παρέχει διαπίστευση στο φορέα πιστοποίησης TÜV ΕΛΛΑΣ (TÜV NORD) Α.Ε., μεταξύ άλλων, ως Φορέα Πιστοποίησης Συστημάτων Διαχείρισης της Ασφάλειας Πληροφοριών κατά ISO/IEC 27001:2005.
- Η τράπεζα Πειραιώς πιστοποιείται από την TUV Hellas κατά ISO/IEC 27001 παρέχοντας επιπλέον επίπεδα διασφάλισης και εμπιστοσύνης προς τους πελάτες και τους μετόχους της.

2.1.6 Ασφάλεια πληροφορίας και τεχνολογία

Ο περισσότερος κόσμος πιστεύει ότι η ασφάλεια πληροφοριών αποτελεί ένα θέμα που αφορά μόνο την τεχνολογία, και πως οτιδήποτε έχει να κάνει με προστασία δεδομένων ή προστασία υπολογιστών από επιθέσεις μπορεί να αντιμετωπιστεί μόνο από προσωπικό πληροφορικής και ειδικότερα από υπεύθυνους ασφάλειας υπολογιστών. Αυτό όμως απέχει πολύ από την πραγματικότητα. Ο χρήστης του υπολογιστή είναι το άτομο που πρέπει να πάρει αποφάσεις σχετικά με το από ποιές απειλές να προστατευτεί και ποιά αντιστάθμιση (trade-off) μεταξύ ασφάλειας και ευελιξίας είναι έτοιμος να δεχτεί.

Πράγματι, μόλις αυτές οι αποφάσεις παρθούν, ο ειδικός στην ασφάλεια υπολογιστών θα πρέπει να σχεδιάσει και να υλοποιήσει μια τεχνολογική λύση που θα προσφέρει να αναμενόμενα αποτελέσματα. Σε έναν οργανισμό αυτές οι αποφάσεις θα πρέπει να παίρνονται από τη διοίκηση και όχι από το τμήμα πληροφορικής. Ένα ΣΔΑΠ αναγνωρίζει εμφανώς και συγκεκριμένα ότι η ευθύνη λήψης αποφάσεων πρέπει να τίθεται στο διοικητικό συμβούλιο και τη διοίκηση του οργανισμού. Το ΣΔΑΠ θα πρέπει να αντικατοπτρίζει τις επιλογές τους και να παρέχει αποδείξεις για την αποτελεσματικότητα με την οποία έχουν πραγματοποιηθεί αυτές.

Ως εκ τούτου, δεν είναι απαραίτητο για ένα έργο σχεδίασης ΣΔΑΠ να καθοδηγείται από έναν ειδικό της τεχνολογίας. Στην πραγματικότητα, υπάρχουν πολλές περιπτώσεις στις οποίες θα μπορούσε αυτό να είναι αντιπαραγωγικό. Τα έργα αυτά είναι, συχνά, καθοδηγούνται από τους διαχειριστές της ποιότητας, γενικούς διευθυντές ή άλλα στελέχη που είναι σε θέση να αναπτύξουν κάτι που έχει επιρροή και σημασία σε όλο τον οργανισμό.

2.1.7 Προετοιμάζοντας ένα έργο ΣΔΑΠ και ο κύκλος PDCA

Ένα σχέδιο ΣΔΑΠ μπορεί να είναι πολύπλοκο. Είναι πιθανό να περιλαμβάνει ολόκληρο τον οργανισμό, μπορεί να πρέπει να μετέχουν όλοι από τη διοίκηση μέχρι τους απλούς εργαζόμενους, και μπορεί κάλλιστα να πάρει πολλούς μήνες - και, σε ορισμένες περιπτώσεις, χρόνια.

Η πιστοποίηση ISO27001 εξακολουθεί να είναι σχετικά νέα και, ως εκ τούτου, δεν υπάρχει διαθέσιμη αρκετή εμπειρία από επιτυχημένες υλοποιήσεις. Αυτό σημαίνει ότι οι λίγες δημοσιεύσεις που περιγράφουν από μια πρακτική και ρεαλιστική άποψη πώς να επιτευχθεί η πιστοποίηση, θα πρέπει να μελετηθούν σε πρώιμο στάδιο της διαδικασίας σχεδιασμού του έργου. Το ISO27001 καθορίζει το πως ένας οργανισμός πρέπει να προσεγγίζει το έργο του ΣΔΑΠ και προσδιορίζει τα στοιχεία που είναι απαραίτητα. Καθορίζονται τα στάδια του έργου και αυτό που ονομάζεται ο κύκλος PDCA.

Ο κύκλος PDCA είναι ο κύκλος Plan-Do-Check-Act (δηλαδή Σχεδίασε-Κάνε-Έλεγξε-Πράξε) που ξεκίνησε το 1950 από τον W. Edwards Deming και η οποία λέει ότι οι επιχειρηματικές διαδικασίες θα πρέπει να αντιμετωπίζονται σαν να βρίσκονται σε συνεχή βρόχο ανάδρασης, έτσι ώστε οι διαχειριστές να μπορούν να προσδιορίσουν και να αλλάξουν αυτά τα μέρη της διαδικασίας που χρειάζονται βελτίωση.

Η διαδικασία, ή μια βελτίωση στη διαδικασία, πρέπει πρώτα να σχεδιαστεί, μετά να εφαρμοστεί και να μετρηθεί η απόδοσή της, ύστερα οι μετρήσεις θα πρέπει να ελέγχονται ως προς τις προγραμματισμένες προδιαγραφές και να εντοπιστούν τυχόν παρεκκλίσεις ή πιθανές βελτιώσεις, και τέλος αναφορά στη διοίκηση για να αποφασίσει σχετικά με το τι μέτρα να λάβει.

2.1.8 Εκτίμηση κινδύνων και σχέδια αντιμετώπισής τους

Ένα ΣΔΑΠ πρέπει να αναπτυχθεί και σχεδιαστεί για να ανταποκριθεί στις ιδιαίτερες απαιτήσεις του κάθε οργανισμού.

Ο κάθε οργανισμός έχει τα δικό του συγκεκριμένο επιχειρηματικό μοντέλο, τους στόχους του, τα μοναδικά χαρακτηριστικά πώλησης και του κουλτούρας, αλλά έχει επίσης και διαφορετικές «ορέξεις» για κίνδυνο. Με άλλα λόγια, κάτι που ένας οργανισμός βλέπει ως απειλή κατά της οποίας πρέπει να προφυλαχθεί, κάποιος άλλος μπορεί να δει ως μια ευκαιρία που πρέπει να κυνηγήσουν.

Ομοίως, ένας οργανισμός μπορεί να είναι λιγότερο διατεθειμένος να επενδύσει στην προστασία κατά ενός κινδύνου που έχει εντοπίσει από ότι ένας άλλος. Γι 'αυτόν, και για άλλους λόγους, κάθε οργανισμός που υλοποιεί ένα ΣΔΑΠ πρέπει να το πράξει σύμφωνα με τα πορίσματα της αξιολόγησης κινδύνου της οποίας η μεθοδολογία, τα πορίσματα και οι συστάσεις έχουν εγκριθεί από το διοικητικό συμβούλιο.

Το ISO27001, στην πραγματικότητα, απαιτεί να υπάρχει μια εκτίμηση του κινδύνου και, ενώ δεν προσδιορίζει τη μεθοδολογία, είναι πολύ σαφές ότι αυτή η αξιολόγηση του κινδύνου πρέπει να βασίζεται στον προσδιορισμό των απειλών και των τρωτών σημείων σε επίπεδο μεμονωμένων περιουσιακών στοιχείων (assets) και, στη συνέχεια, στην ανάλυση και στην αξιολόγηση των κινδύνων.

2.1.9 Καταγραφή εγγράφων συστήματος

Το πιο χρονοβόρο, αλλά και το πιο σημαντικό κομμάτι ολόκληρου του έργου είναι η ανάπτυξη των εγγράφων (documentation) που περιγράφουν πως δουλεύει συνολικά το ΣΔΑΠ.

Υπάρχουν μια σειρά από διαφορετικές πιθανές προσεγγίσεις σε αυτό, από τη χρήση εξωτερικών συμβούλων έως το να το αντιμετωπίσει ο ίδιος ο οργανισμός από μόνος του. Το σημαντικό επιχείρημα υπέρ του το κάνει ο οργανισμός (εκτός από την αποφυγή ή τη μείωση του κόστος παροχής συμβουλών) είναι ότι θα αναπτυχθεί στον οργανισμό ένα πολύ μεγαλύτερο βάθος και ευαισθητοποίηση του «πώς να κάνετε την ασφάλεια».

Όλοι οι οργανισμοί αντιμετωπίζουν την πρόκληση του να αναπτυχθεί αποτελεσματικά το documentation του ΣΔΑΠ, εξασφαλίζοντας ότι ελέγχεται σωστά, ότι είναι προσιτό σε όλους όσους χρειάζεται να το δουν, και ότι υπάρχουν στοιχεία που αποδεικνύουν ότι οι

χρήστες έχουν διαβάσει και κατανοήσει όλες αυτές τις πολιτικές που εφαρμόζονται σε αυτά. Αυτό το είδος της διαδρομής ελέγχου καθίσταται ολοένα και σημαντικότερο καθώς οι κανονιστικές ρυθμίσεις σχετικά με πληροφορίες γίνονται όλο και πιο διαδεδομένες. Ο πιο πρακτικός τρόπος για την αντιμετώπιση όλων των προκλήσεων διαχείρισης της πολιτικής είναι να αναπτύξει ένα εργαλείο διαχείρισης της πολιτικής.

2.2 Πρότυπο ISO/IEC 17799 (ISO/IEC 27002)

Το ISO/IEC 27002:2005 αναπτύχθηκε από το BS7799, το οποίο δημοσιεύτηκε στα μέσα της δεκαετίας του ’90 από το Βρετανικό Ινστιτούτο Προτύπων. Στη συνέχεια υιοθετήθηκε από το Διεθνή Οργανισμό Πιστοποίησης σαν ISO/IEC 17799:2000, αναθεωρήθηκε το 2005 και τελικά απλώς μετονομάστηκε το 2007, χωρίς να αλλάξει κάτι στο κείμενο, σε ISO/IEC 27002 για να ταιριάξει με της οικογένεια των προτύπων ISO/IEC 27000-series.

Όπως αναφέραμε και παραπάνω το ISO/IEC 27002 είναι ένα συμβουλευτικό πρότυπο που έχει ως στόχο να ερμηνεύεται και να εφαρμόζεται σε όλους τους τύπους και τα μεγέθη οργανισμών, σύμφωνα με τους ιδιαίτερους κινδύνους ασφάλειας των πληροφοριών που αντιμετωπίζουν. Στην πράξη, η ευελιξία αυτή δίνει στους χρήστες μια μεγάλη ελευθερία να υιοθετήσουν τους ελέγχους ασφάλειας των πληροφοριών που έχουν νόημα για αυτούς, αλλά το καθιστά ακατάλληλο για τον σχετικά απλό έλεγχο συμμόρφωσης στα περισσότερα επίσημα συστήματα πιστοποίησης.

Στις παρακάτω παραγράφους θα παρουσιάσουμε με λίγα λόγια όλες τις ενότητες του προτύπου.

2.2.1 Εισαγωγή στο ISO/IEC 17799

Αρχικά το πρότυπο απαντάει δύο βασικά ερωτήματα για την ασφάλεια πληροφοριών. Τι είναι η ασφάλεια πληροφοριών και γιατί χρειάζεται;

Η πληροφορίες μπορούν να θεωρηθούν ως ένα περιουσιακό στοιχείο που, όπως όλα τα περιουσιακά στοιχεία της επιχείρησης, είναι ουσιαστικής σημασίας για έναν οργανισμό

και συνεπώς πρέπει να προστατεύεται κατάλληλα. Στο όλο και πιο διασυνδεδεμένο επιχειρηματικό περιβάλλον αυτό έχει σαν αποτέλεσμα οι πληροφορίες να εκτίθενται σε ένα μεγαλύτερο εύρος απειλών και ευπαθειών. Οι πληροφορίες μπορούν να υπάρχουν σε πολλές μορφές όπως καταγεγραμμένες ή εκτυπωμένες σε χαρτί, αποθηκευμένες σε ηλεκτρονική μορφή, να διαβιβάζονται ταχυδρομικώς ή με τη χρήση ηλεκτρονικών μέσων, να εμφανίζονται με οπτικά μέσα, ή προφορικά σε συζητήσεις. Ό,τι μορφή παίρνει η πληροφορία θα πρέπει πάντα να είναι κατάλληλα προστατευμένη.

Η ασφάλεια των πληροφοριών είναι η προστασία των πληροφοριών από ένα ευρύ φάσμα απειλών, προκειμένου να διασφαλίζεται η επιχειρησιακή συνέχεια, να ελαχιστοποιείται ο επιχειρησιακός κίνδυνος, και να μεγιστοποιείται η απόδοση των επενδύσεων και των επιχειρηματικές ευκαιριών. Η ασφάλεια των πληροφοριών επιτυγχάνεται με την εφαρμογή ενός κατάλληλου συνόλου ελέγχων, περιλαμβάνοντας πολιτικές, διαδικασίες, επιχειρησιακές δομές και λειτουργίες λογισμικού και υλικού. Οι έλεγχοι αυτοί πρέπει να θεσπιστούν, να εφαρμοστούν, να παρακολουθούνται, να αξιολογούνται και να βελτιώνονται, όπου είναι αναγκαίο, για να διασφαλιστεί ότι η συγκεκριμένη ασφάλεια και οι επιχειρησιακοί στόχοι του οργανισμού πληρούνται. Αυτό πρέπει να γίνει σε συνδυασμό με άλλες μεθόδους διαχείρισης των επιχειρήσεων

Οι πληροφορίες, οι διαδικασίες υποστήριξης, τα συστήματα και τα δίκτυα είναι σημαντικά στοιχεία του ενεργητικού των επιχειρήσεων. Ο καθορισμός, η επίτευξη, η διατήρηση και η βελτίωση της ασφάλειας των πληροφοριών είναι απαραίτητη για τη διατήρηση του ανταγωνιστικού πλεονεκτήματος, των ταμειακών ροών, της κερδοφορίας, της νομικής συμμόρφωσης, και της εμπορικής εικόνας του οργανισμού. Οι Οργανισμοί και τα πληροφοριακά τους συστήματα και τα δίκτυα τους, έρχονται αντιμέτωποι με απειλές κατά της ασφάλειας από ένα ευρύ φάσμα πηγών, μεταξύ αυτών, απάτη μέσω ηλεκτρονικών υπολογιστών, κατασκοπεία, δολιοφθορά, βανδαλισμοί, πυρκαγιά ή πλημμύρα. Οι αιτίες των ζημιών, όπως κακόβουλος κώδικας, ηλεκτρονική πειρατεία και επιθέσεις άρνησης παροχής υπηρεσίας έχουν γίνει πιο συχνές, πιο φιλόδοξες και ολοένα πιο σύνθετες.

Η ασφάλεια των πληροφοριών είναι σημαντική τόσο στις δημόσιες όσο και ιδιωτικές επιχειρήσεις, και για την προστασία των υποδομών ζωτικής σημασίας. Η ασφάλεια των πληροφοριών λειτουργεί ως καταλύτης για πολλές φιλόδοξες λειτουργίες όπως για την επίτευξη της ηλεκτρονικής διακυβέρνησης ή το ηλεκτρονικό επιχειρείν με το να αποφεύγονται ή να μειώνονται οι σχετικοί κίνδυνοι.

Πολλά συστήματα πληροφοριών δεν έχουν σχεδιαστεί για να είναι ασφαλής. Η ασφάλεια που μπορεί να επιτευχθεί με τεχνικά μέσα είναι περιορισμένη, και θα πρέπει να

υποστηρίζεται από την κατάλληλη διαχείριση και τις διαδικασίες. Το να εντοπίσουμε ποίοι έλεγχοι πρέπει να δημιουργηθούν απαιτεί προσεκτικό σχεδιασμό και προσοχή στη λεπτομέρεια. Η διαχείριση της ασφάλειας πληροφορίας απαιτεί, ως ελάχιστο, τη συμμετοχή όλων των εργαζομένων στον οργανισμό. Μπορεί επίσης να απαιτεί τη συμμετοχή των μετόχων, τους προμηθευτών, των πελατών και των εξωτερικών συνεργατών. Συμβουλές ειδικών από εξωτερικούς οργανισμούς μπορεί επίσης να χρειάζονται.

Αφού απαντώνται τα δύο βασικά ερωτήματα λοιπόν «τι είναι η ασφάλεια πληροφοριών και γιατί χρειάζεται;», ύστερα διαχωρίζονται οι πηγές των απαιτήσεων ασφαλείας:

- Μια πηγή προέρχεται από την αξιολόγηση των κινδύνων για τον οργανισμό, λαμβάνοντας υπόψη τη συνολική επιχειρηματική στρατηγική και τους στόχους του οργανισμού. Μέσα από μια αξιολόγηση των κινδύνων, προσδιορίζονται οι απειλές των περιουσιακών στοιχείων, και εκτιμάται η τρωτότητα και η πιθανότητα εμφάνισης από τις πιθανές επιπτώσεις.
- Μια άλλη πηγή είναι οι νομικές, κανονιστικές, ρυθμιστικές και συμβατικές απαιτήσεις που ο οργανισμός, οι εμπορικοί του εταίροι, οι ανάδοχοι και οι πάροχοι υπηρεσιών πρέπει να πληρούν.
- Μια άλλη πηγή είναι το σύνολο των αρχών, στόχων και απαιτήσεων των επιχειρήσεων για την επεξεργασία πληροφοριών όπου ο οργανισμός έχει αναπτύξει για να υποστηρίξει τις δραστηριότητές του.

Άλλο σημαντικό θέμα που θίγεται και σε επόμενο κεφάλαιο είναι η αξιολόγηση των κινδύνων καθώς οι απαιτήσεις ασφαλείας καθορίζονται από αυτή τη διαδικασία. Οι δαπάνες σχετικά με τους ελέγχους πρέπει να σταθμιστούν σε σχέση με τη ζημία των επιχειρήσεων που ενδέχεται να προκύψουν από τις αποτυχίες της ασφάλειας. Τα αποτελέσματα της αξιολόγησης του κινδύνου θα βοηθήσουν στο να καθοδηγήσουν και να καθορίσουν την κατάλληλη διαχείριση δράσης και τις προτεραιότητες για τη διαχείριση των κινδύνων ασφάλειας των πληροφοριών, και για την εφαρμογή των ελέγχων που επιλέγονται για την προστασία από τους κινδύνους αυτούς. Η εκτίμηση κινδύνου θα πρέπει να επαναλαμβάνεται περιοδικά για την αντιμετώπιση τυχόν αλλαγών που ενδέχεται να επηρεάσουν τα αποτελέσματα της αξιολόγησης του κινδύνου.

Αφού λοιπόν έχουν εντοπιστεί οι απαιτήσεις ασφάλειας και οι κίνδυνοι, και αφού έχουν παρθεί οι αποφάσεις για την αντιμετώπιση των κινδύνων, ύστερα πρέπει να επιλεγούν οι κατάλληλοι έλεγχοι και να εφαρμοστούν ώστε να εξασφαλίσουν ότι οι κίνδυνοι έχουν

μειωθεί σε αποδεκτό επίπεδο. Οι έλεγχοι μπορούν να επιλεγούν από αυτό το πρότυπο ή από άλλα σύνολα ελέγχου, ή ακόμα μπορεί να σχεδιαστούν νέοι έλεγχοι για να ανταποκρίνονται στις ιδιαίτερες ανάγκες ανάλογα με την περίπτωση. Η επιλογή των ελέγχων ασφαλείας εξαρτάται από τις αποφάσεις του οργανισμού με βάση τα κριτήρια αποδοχής των κινδύνων, τις επιλογές αντιμετώπισης κινδύνου, και τη γενική προσέγγιση της διαχείρισης κινδύνων που εφαρμόζεται στον οργανισμό, και θα πρέπει επίσης οι έλεγχοι να υπόκεινται σε όλες τις σχετικές εθνικές και διεθνείς νομοθεσίες και κανονισμούς.

Μερικοί από τους ελέγχους σε αυτό το πρότυπο μπορούν να θεωρηθούν ως κατευθυντήριες αρχές για τη διαχείριση της ασφάλειας των πληροφοριών και να ισχύουν για τους περισσότερους οργανισμούς. Εξηγούνται με περισσότερες λεπτομέρειες στη συνέχεια.

Ένας αριθμός ελέγχων μπορεί να θεωρηθεί ως ένα καλό σημείο εκκίνησης για την υλοποίηση της ασφάλειας των πληροφοριών. Είτε βασίζονται στις βασικές νομοθετικές απαιτήσεις είτε θεωρούνται ότι είναι κοινή πρακτική για την ασφάλεια των πληροφοριών. Περισσότερα για τους ελέγχους παρουσιάζονται στη συνέχεια στο πρότυπο.

Στη συνέχεια αναφέρονται οι κυριότεροι παράγοντες για την ασφάλεια πληροφοριών σε έναν οργανισμό. Μερικοί από αυτούς είναι οι εξής:

1. Η ύπαρξη πολιτικής ασφάλειας πληροφοριών, στόχων και δραστηριοτήτων που αντικατοπτρίζουν τους επιχειρησιακούς στόχους.
2. Η προσέγγιση και το πλαίσιο για την υλοποίηση, τη διατήρηση, την παρακολούθηση και τη βελτίωση της ασφάλειας των πληροφοριών να είναι συνεπής με την οργανωτική κουλτούρα.
3. Ορατή υποστήριξη και δέσμευση από όλα τα επίπεδα της διοίκησης.
4. Μια καλή κατανόηση των απαιτήσεων ασφάλειας των πληροφοριών, εκτίμηση του κινδύνου και διαχείρισης κινδύνου
5. Αποτελεσματική προώθηση της ασφάλειας των πληροφοριών σε όλους τους διευθυντές, υπαλλήλους, και άλλα μέρη για να επιτύχουν την ευαισθητοποίηση.
6. Διανομή των οδηγιών σχετικά με την πολιτική ασφάλειας των πληροφοριών και των προτύπων σε όλους τους διευθυντές, τους υπαλλήλους και άλλα μέρη.
7. Πρόβλεψη για χρηματοδότηση των δραστηριοτήτων διαχείρισης ασφάλειας πληροφοριών.

8. Η παροχή κατάλληλης ενημέρωσης, κατάρτισης και εκπαίδευσης.
9. Καθιέρωση μιας αποτελεσματικής διαδικασίας διαχείρισης μετά από περιστατικά ασφάλειας των πληροφοριών.
10. Εφαρμογή ενός συστήματος μέτρησης που χρησιμοποιείται για την αξιολόγηση των επιδόσεων στον τομέα της διαχείρισης της ασφάλειας των πληροφοριών και ύπαρξη προτάσεων ανατροφοδότησης για βελτίωση.

Στο τέλος αυτής της εισαγωγής αναφέρεται πως συνολικά αυτός ο κώδικας πρακτικής μπορεί να θεωρηθεί ως σημείο εκκίνησης για να αναπτύξει κανείς συγκεκριμένες κατευθυντήριες γραμμές σε έναν οργανισμό. Μπορεί να μην εφαρμόζονται όλοι οι έλεγχοι και η καθοδήγηση αυτού του κώδικα πρακτικής και επιπλέον, μπορεί να απαιτηθούν πρόσθετοι έλεγχοι και τις κατευθυντήριες γραμμές που δεν περιλαμβάνονται σε αυτό το πρότυπο.

2.2.2 Δομή του προτύπου

Αυτό το πρότυπο περιέχει 11 παραγράφους ελέγχου της ασφάλειας που περιέχουν συνολικά 39 κύριες κατηγορίες ασφάλειας και μια εισαγωγική παράγραφο για την εκτίμηση του κινδύνου και την αντιμετώπισή του.

Κάθε παράγραφος περιέχει μια σειρά από βασικές κατηγορίες ασφάλειας. Οι έντεκα παράγραφοι (σε παρένθεση ο αριθμός των κύριων κατηγοριών ασφαλείας που περιλαμβάνονται σε κάθε μια) είναι οι εξής:

1. Πολιτική Ασφάλειας (1)
2. Οργάνωση της Ασφάλειας Πληροφορίας (2)
3. Διαχείριση αγαθών/περιουσιακών στοιχείων (2)
4. Ασφάλεια Ανθρωπίνου Δυναμικού (3)
5. Φυσική και περιβαλλοντική ασφάλεια (2)
6. Διαχείριση Επικοινωνιών και Λειτουργιών (10)
7. Έλεγχος πρόσβασης (7)
8. Απόκτηση, ανάπτυξη και συντήρηση Πληροφοριακών συστημάτων (6)

9. Διαχείριση Περιστατικών Ασφάλειας Πληροφοριών (2)
10. Διαχείριση Επιχειρησιακής συνέχειας (1)
11. Συμμόρφωση (3)

Η σειρά των παραγράφων σε αυτό το πρότυπο δεν καθορίζει και τη σημασία τους. Ανάλογα με τις συνθήκες, όλες θα μπορούσαν να είναι σημαντικές, συνεπώς, κάθε οργανισμός που εφαρμόζει το εν λόγω πρότυπο θα πρέπει να προσδιορίζει τις παραγράφους που ισχύουν, πόσο σημαντικές είναι αυτές και πως εφαρμόζονται σε μεμονωμένες επιχειρηματικές διαδικασίες.

Κάθε κύρια κατηγορία ασφάλειας περιέχει:

- Ένα στόχο του ελέγχου που δηλώνει τι πρέπει να επιτευχθεί.
- Έναν ή περισσότερους ελέγχους που μπορούν να εφαρμοσθούν για να επιτευχθεί ο κάθε στόχος.

Η δομή των περιγραφών των ελέγχων είναι η εξής:

Έλεγχος

Καθορίζει τη δήλωση του συγκεκριμένου ελέγχου που θα ικανοποιήσει το στόχο του ελέγχου.

Καθοδήγηση Υλοποίησης

Παρέχει περισσότερο λεπτομερείς πληροφορίες για την υποστήριξη της υλοποίησης του ελέγχου και την επίτευξη του στόχου του ελέγχου. Ορισμένες από αυτές τις κατευθυντήριες γραμμές μπορεί να μην είναι κατάλληλες σε όλες τις περιπτώσεις, έτσι άλλοι τρόποι εφαρμογής του ελέγχου μπορεί να είναι πιο κατάλληλοι.

Άλλες Πληροφορίες

Παρέχει επιπλέον πληροφορίες που πιθανώς να πρέπει να εξεταστούν, για παράδειγμα, νομικά ζητήματα και αναφορές σε άλλα πρότυπα.

2.2.3 Εκτίμηση Κινδύνου και Αντιμετώπιση

Στην εισαγωγική αυτή παράγραφο παρουσιάζεται αρχικά η εκτίμηση/αξιολόγηση κινδύνου και εν συνεχεία η αντιμετώπιση (treatment) του κινδύνου.

2.2.3.1 Αξιολόγηση των Κινδύνων Ασφάλειας

Οι αξιολογήσεις των κινδύνων θα πρέπει να εντοπίζουν, να ποσοτικοποιούν και να ιεραρχούν τους κινδύνους σύμφωνα με τα κριτήρια για την αποδοχή των κινδύνων και των στόχων που σχετίζονται με τον οργανισμό. Τα αποτελέσματα θα πρέπει να καθοδηγούν και να καθορίζουν τα κατάλληλα μέτρα διαχείρισης και τις προτεραιότητες για τη διαχείριση των κινδύνων ασφάλειας των πληροφοριών. Η διαδικασία αξιολόγησης των κινδύνων και επιλογής των ελέγχων μπορεί να χρειαστεί να πραγματοποιηθεί αρκετές φορές για να καλυφθούν διαφορετικά μέρη του οργανισμού ή ξεχωριστά συστήματα πληροφοριών.

Η εκτίμηση κινδύνου πρέπει να περιλαμβάνει τη συστηματική προσέγγιση της εκτίμησης του μεγέθους των κινδύνων (ανάλυση κινδύνου) και τη διαδικασία της σύγκρισης των εκτιμώμενων κινδύνων με βάση τα κριτήρια κινδύνου έτσι ώστε να προσδιοριστεί η σημασία των κινδύνων (εκτίμηση του κινδύνου).

Οι αξιολογήσεις κινδύνων θα πρέπει επίσης να διεξάγονται περιοδικά, για την αντιμετώπιση των αλλαγών στις απαιτήσεις της ασφάλειας και της κατάστασης κινδύνου, π.χ. όταν συμβαίνουν σημαντικές αλλαγές στα αγαθά, στις απειλές, στα τρωτά σημεία, στις επιπτώσεις, στην αξιολόγηση των κινδύνων. Αυτές οι αξιολογήσεις του κινδύνου θα πρέπει να υλοποιηθούν με ένα μεθοδικό τρόπο ικανό να παράγει συγκρίσιμα και αναπαραγόμενα αποτελέσματα. Η αξιολόγηση των κινδύνων ασφάλειας πληροφοριών θα πρέπει να έχει ένα σαφώς προσδιορισμένο πεδίο εφαρμογής, προκειμένου να είναι αποτελεσματική και θα πρέπει να περιλαμβάνει σχέσεις με την εκτίμηση κινδύνων σε άλλους τομείς, ανάλογα με την περίπτωση.

Το πεδίο μιας αξιολόγησης κινδύνου μπορεί να είναι είτε το σύνολο του οργανισμού, ή τμήματα του οργανισμού, ή ένα μεμονωμένο πληροφοριακό σύστημα, ή συγκεκριμένα στοιχεία του συστήματος, ή υπηρεσίες όπου αυτό είναι εφικτό, ρεαλιστικό και χρήσιμο. Παραδείγματα των μεθοδολογιών αξιολόγησης του κινδύνου συζητούνται στο πρότυπο ISO / IEC TR13335-3 (Κατευθυντήριες γραμμές για τη διαχείριση του IT Security: Τεχνικές για τη Διαχείριση του IT Security - Guidelines for the Management of IT Security: Techniques for the Management of IT Security).

2.2.3.2 Αντιμετώπιση των Κινδύνων Ασφάλειας

Πριν εξεταστεί η αντιμετώπιση ενός κινδύνου, ο οργανισμός θα πρέπει να αποφασίσει κριτήρια για τον προσδιορισμό κατά πόσον ένας κίνδυνος μπορεί να είναι αποδεκτός. Ένας κίνδυνος μπορεί να γίνει αποδεκτός εάν, για παράδειγμα, εκτιμάται ότι ο κίνδυνος είναι χαμηλός ή ότι το κόστος της αντιμετώπισης δεν είναι αξίζει για τον οργανισμό. Οι αποφάσεις αυτές πρέπει να καταγράφονται.

Για καθένα από τους κινδύνους που διαπιστώθηκαν μετά από την αξιολόγηση κινδύνου πρέπει να παρθεί απόφαση για την αντιμετώπισης του. Πιθανές επιλογές για την αντιμετώπιση του κινδύνου περιλαμβάνουν:

1. Εφαρμογή των κατάλληλων ελέγχων για τη μείωση των κινδύνων.
2. Εν γνώσει και βάσει στόχου αποδοχή των κινδύνων, εφόσον ικανοποιούν σαφώς την πολιτική του οργανισμού και τα κριτήρια για την αποδοχή του κινδύνου.
3. Αποφυγή των κινδύνων, μη επιτρέποντας ενέργειες που θα προκαλέσουν πιθανούς κινδύνους.
4. Μεταφορά των συναφών κινδύνων σε άλλα μέρη, π.χ. ασφαλιστές ή τους προμηθευτές

Για τους κινδύνους αυτούς όπου η απόφαση της αντιμετώπισης τους ήταν να εφαρμοστούν κατάλληλοι έλεγχοι, οι έλεγχοι αυτοί θα πρέπει να επιλεγούν και να εφαρμοστούν για να πληρούν τις απαιτήσεις που προσδιορίζονται από την εκτίμηση του κινδύνου. Οι έλεγχοι πρέπει να εξασφαλίζουν ότι οι κίνδυνοι μειώνονται σε αποδεκτό επίπεδο, λαμβάνοντας υπόψη:

1. Τις απαιτήσεις και τους περιορισμούς της εθνικής και διεθνούς νομοθεσίας και των κανονισμών.
2. Στόχους του οργανισμού.
3. λειτουργικές απαιτήσεις και περιορισμούς.
4. Το κόστος υλοποίησης και λειτουργίας σε σχέση με τη μείωση των κινδύνων.
5. Την ανάγκη εξισορρόπησης των επενδύσεων στην εφαρμογή και τη λειτουργία των ελέγχων έναντι της ζημιάς που μπορεί να προκύψει από αποτυχίες της ασφάλειας.

Έλεγχοι ασφαλείας πληροφοριών θα πρέπει να εξεταστούν στα συστήματα και στα έργα στη φάση καθορισμού προδιαγραφών και στο στάδιο του σχεδιασμού. Σε αντίθετη περίπτωση, μπορεί να οδηγήσει σε πρόσθετο κόστος και λιγότερο αποτελεσματικές λύσεις, και στη χειρότερη περίπτωση, η αδυναμία να επιτευχθεί επαρκής ασφάλεια.

Θα πρέπει να έχουμε κατά νου ότι κανένα σύνολο ελέγχων δεν μπορεί να επιτύχει απόλυτη ασφάλεια, και ότι πρέπει να εφαρμόζονται πρόσθετα μέτρα διαχείρισης για την παρακολούθηση, την αξιολόγηση και τη βελτίωση της αποδοτικότητας και της αποτελεσματικότητας των ελέγχων ασφαλείας για την υποστήριξη των σκοπών του οργανισμού.

2.2.4 Πολιτική ασφάλειας

Στόχος της πολιτικής ασφάλειας είναι να παρέχει μια κατεύθυνση διαχείρισης και υποστήριξη για ασφάλεια πληροφοριών σε συμφωνία με τις επιχειρησιακές απαιτήσεις και τους σχετικούς νόμους και κανονισμούς.

Η διοίκηση πρέπει να θέσει μια σαφή κατεύθυνση πολιτικής σε συμφωνία με τους επιχειρηματικούς στόχους και να επιδείξει υποστήριξή και δέσμευσή στην ασφάλεια των πληροφοριών με την έκδοση και τη διατήρηση μιας πολιτικής για την ασφάλεια πληροφοριών σε όλη τον οργανισμό.

2.2.4.1 Έγγραφο πολιτικής ασφάλειας πληροφοριών

Το έγγραφο πολιτικής ασφάλειας των πληροφοριών θα πρέπει να εγκριθεί από τη διοίκηση, και δημοσιεύεται και επικοινωνείται σε όλους τους υπαλλήλους και ενδιαφερόμενα μέρη.

Το έγγραφο αυτό πρέπει να αναφέρει την πολιτική δέσμευση της διοίκησης και καθορίζει την προσέγγιση του οργανισμού για τη διαχείριση της ασφάλειας των πληροφοριών. Το έγγραφο πολιτικής θα πρέπει να περιέχει δηλώσεις που αφορούν:

1. Έναν ορισμό της ασφάλειας πληροφοριών, του στόχους της και τη σημαντικότητά της για τον οργανισμό.
2. Μια δήλωση στήριξης της διοίκησης στις αρχές της ασφάλειας.
3. Ένα να πλαίσιο για τον καθορισμό των στόχων του ελέγχου και των ελέγχων, συμπεριλαμβανομένης της δομής της εκτίμησης και διαχείρισης κινδύνων.

4. Μια σύντομη επεξήγηση για πολιτικές ασφάλειας, αρχές, πρότυπα και τις απαιτήσεις συμμόρφωσης ιδιαίτερης σημασία για τον οργανισμό, συμπεριλαμβανομένων την κανονιστική συμμόρφωση, την εκπαίδευση ασφάλειας, την επιχειρησιακή συνέχεια και τις επιπτώσεις των παραβιάσεων της πολιτικής.
5. Έναν ορισμό των γενικών και των συγκεκριμένων αρμοδιοτήτων για τη διαχείριση της ασφάλειας των πληροφοριών.
6. Αναφορές σε έγγραφα που μπορεί να υποστηρίζουν την πολιτική, π.χ. πιο αναλυτικές πολιτικές και τις διαδικασίες ασφάλειας για συγκεκριμένα συστήματα πληροφοριών ή κανόνες ασφάλειας με τους οποίου οι χρήστες θα πρέπει να συμμορφώνονται.

Η πολιτική ασφάλειας των πληροφοριών θα μπορούσε να είναι ένα μέρος ενός εγγράφου γενικής πολιτικής. Εάν η πολιτική ασφάλειας των πληροφοριών διανέμεται εκτός του οργανισμού, πρέπει να ληφθεί μέριμνα να μην αποκαλύψει ευαίσθητες πληροφορίες. Περισσότερες πληροφορίες μπορούν να βρεθούν στο πρότυπο ISO / IEC 13335-1:2004.

2.2.4.2 Επανεξέταση της πολιτικής ασφάλειας πληροφοριών

Η πολιτική ασφάλειας των πληροφοριών θα πρέπει να επανεξετάζονται σε τακτά χρονικά διαστήματα ή εάν σημειωθούν σημαντικές αλλαγές.

Η πολιτική της ασφάλειας των πληροφοριών θα πρέπει να έχει έναν ιδιοκτήτη που έχει εγκρίνει τη διαχειριστική ευθύνη για την ανάπτυξη, επανεξέταση και αξιολόγηση της πολιτικής ασφάλειας. Η αναθεώρηση θα πρέπει να περιλαμβάνει εκτίμηση των δυνατοτήτων βελτίωσης της πολιτικής ασφάλειας των πληροφοριών του οργανισμού και προσέγγιση στη διαχείριση της ασφάλειας των πληροφοριών σε συνάρτηση με τις αλλαγές στο οργανωτικό περιβάλλον, τις επιχειρησιακές συνθήκες, τους νομικούς όρους, ή το τεχνικό περιβάλλον.

Η αναθεώρηση της πολιτικής για την ασφάλεια των πληροφοριών θα πρέπει να λαμβάνει υπόψη τα σχόλια της επανεξέτασης της διοίκησης. Πρέπει να ορίζονται οι διαδικασίες επανεξέτασης της διοίκησης, που θα συμπεριλαμβάνει χρονοδιάγραμμα ή περίοδο της επανεξέτασης.

Η είσοδος στην αναθεώρηση της διοίκησης πρέπει να περιλαμβάνει πληροφορίες σχετικά με:

1. Ανατροφοδότηση από τα ενδιαφερόμενα μέρη.

2. Αποτελέσματα ανεξάρτητων σχολιασμών.
3. Κατάσταση των προληπτικών και διορθωτικών ενεργειών.
4. Αποτελέσματα των προηγούμενων ανασκοπήσεων από τη διοίκηση.
5. Απόδοση της διαδικασίας και συμμόρφωση με την πολιτική ασφαλείας.
6. Αλλαγές που θα μπορούσαν να επηρεάσουν την προσέγγιση του οργανισμού για τη διαχείριση της ασφάλειας των πληροφοριών, συμπεριλαμβανομένων των αλλαγών στο οργανωτικό περιβάλλον, τις συνθήκες των επιχειρήσεων, τη διαθεσιμότητα πόρων, τις συμβατικές, ρυθμιστικές και νομικές προϋποθέσεις, ή το τεχνικό περιβάλλον.
7. Τάσεις σχετικά με απειλές και ευπάθειες.
8. Αναφορές περιστατικών ασφάλειας πληροφοριών
9. Συστάσεις που παρέχονται από τις αρμόδιες αρχές

Το αποτέλεσμα της αναθεώρησης της διοίκησης πρέπει να περιλαμβάνει όλες τις αποφάσεις και δράσεις που σχετίζονται με:

1. Βελτίωση της προσέγγισης του οργανισμού για τη διαχείριση της ασφάλειας των πληροφοριών και των διαδικασιών της.
2. Βελτίωση των στόχων και των ελέγχων.
3. Βελτίωση στην κατανομή των πόρων και / ή ευθυνών. Μια καταγραφή της επανεξέτασης της διοίκησης θα πρέπει να διατηρηθεί.

Θα πρέπει να λαμβάνεται η έγκριση της διοίκησης για την αναθεωρημένη πολιτική.

2.2.5 Οργάνωση της ασφάλειας πληροφοριών

Η οργάνωση της ασφάλεια πληροφοριών χωρίζεται σε δύο κατηγορίες: ασφάλεια εντός του οργανισμού και ασφάλεια εξωτερικών μερών.

2.2.5.1 Οργάνωση εντός του οργανισμού

Ο στόχος της οργάνωσης εντός του οργανισμού είναι η διαχείριση της ασφάλειας εντός του οργανισμού.

Ένα πλαίσιο διαχείρισης θα πρέπει να συσταθεί για να ξεκινήσει και να ελέγχει την εφαρμογή της ασφάλειας των πληροφοριών εντός του οργανισμού. Η διοίκηση πρέπει να εγκρίνει την πολιτική της ασφάλειας των πληροφοριών, να ορίσει τους ρόλους ασφαλείας και να συντονίζει και να επανεξετάσει την εφαρμογή των μέτρων ασφαλείας σε ολόκληρο τον οργανισμό.

Εάν είναι απαραίτητο, μια πηγή ειδικών συμβούλων στην ασφάλεια πληροφοριών θα πρέπει να καθορίζεται και να διατίθεται εντός του οργανισμού. Επαφές με τους εξωτερικούς ειδικούς ασφάλειας ή ομάδες, συμπεριλαμβανομένων των αρμόδιων αρχών, θα πρέπει να αναπτυχθούν για να συμβαδίσει ο οργανισμός με τις βιομηχανικές τάσεις, να παρακολουθούν τα πρότυπα και τις μεθόδους αξιολόγησης και να παρέχουν κατάλληλη σημεία επαφής κατά το χειρισμό περιστατικών ασφάλεια. Μια διεπιστημονική προσέγγιση για την ασφάλεια των πληροφοριών θα πρέπει να ενθαρρύνεται.

2.2.5.1.1 Δέσμευση της διοίκησης για ασφάλεια πληροφοριών

Η διοίκηση πρέπει να υποστηρίξει ενεργά την ασφάλεια εντός του οργανισμού μέσω σαφούς κατεύθυνσης, επίδειξη δέσμευσης, ρητή ανάθεση, και την αναγνώριση των ευθυνών της ασφάλειας των πληροφοριών.

Η διοίκηση θα πρέπει:

1. Να διασφαλίσει ότι προσδιορίζονται οι στόχοι της ασφάλειας των πληροφοριών, ότι πληρούν τις οργανωτικές απαιτήσεις, και ενσωματώνονται στις σχετικές διεργασίες.
2. Να διατυπώσει, να επανεξετάσει και να εγκρίνει την πολιτική ασφάλειας πληροφοριών.
3. Να επανεξετάζει την αποτελεσματικότητα της εφαρμογής της πολιτικής για την ασφάλεια των πληροφοριών.
4. Να παρέχει τους απαραίτητους πόρους για ασφάλεια πληροφοριών.
5. Να εγκρίνει ανάθεση συγκεκριμένων ρόλων και αρμοδιοτήτων για την ασφάλεια των πληροφοριών σε όλο τον οργανισμό.
6. Να ξεκινήσει σχέδια και προγράμματα για τη διατήρηση πληροφοριών ευαισθητοποίησης σε θέματα ασφάλειας.
7. Να διασφαλίσει ότι η εφαρμογή των ελέγχων της ασφάλειας των πληροφοριών είναι συντονισμένη σε όλη την οργάνωση.

Περισσότερες πληροφορίες περιέχονται στο πρότυπο ISO/IEC 13335-1:2004.

2.2.5.1.2 Συντονισμός ασφάλειας πληροφοριών

Οι δραστηριότητες ασφάλειας πληροφοριών θα πρέπει να είναι συντονισμένες με τους εκπροσώπους από διάφορα τμήματα του οργανισμού με τους σχετικούς ρόλους.

Συνήθως, ο συντονισμός της ασφάλειας πληροφοριών πρέπει να περιλαμβάνει τη συνεργασία προϊσταμένων, χρηστών, διαχειριστών, σχεδιαστών των εφαρμογών, ελεγκτών και του προσωπικού ασφαλείας, και ειδικών σε τομείς όπως η ασφάλεια, νομικά θέματα, ανθρώπινο δυναμικό, τεχνολογία πληροφορικής ή τη διαχείριση του κινδύνου.

Σε γενικές γραμμές αυτή η δραστηριότητα θα πρέπει να διασφαλίσει ότι οι δραστηριότητες ασφάλειας εκτελούνται σύμφωνα με την πολιτική ασφάλειας πληροφοριών, να αξιολογεί την επάρκεια και να συντονίσει την εφαρμογή των ελέγχων, και επίσης να προωθεί αποτελεσματικά την πληροφόρηση για την εκπαίδευση ασφαλείας και ευαισθητοποίηση σε ολόκληρη την οργάνωση.

Εάν ο οργανισμός δεν χρησιμοποιεί μια ξεχωριστή διατμηματική ομάδα, οι ενέργειες θα πρέπει να αναληφθούν από άλλο κατάλληλο διοικητικό φορέα ή διευθυντικό στέλεχος.

2.2.5.1.3 Κατανομή των αρμοδιοτήτων ασφάλειας πληροφοριών

Όλες οι ευθύνες για την ασφάλεια πληροφοριών πρέπει να ορίζονται με σαφήνεια.

Η κατανομή των αρμοδιοτήτων πρέπει να γίνεται σύμφωνα με την πολιτική ασφάλειας. Οι ευθύνες για την προστασία των ατομικών αγαθών και για την εκτέλεση συγκεκριμένων διαδικασιών ασφαλείας θα πρέπει να προσδιορίζονται σαφώς. Η ευθύνη αυτή θα πρέπει να συμπληρωθεί, όπου απαιτείται, με πιο λεπτομερείς οδηγίες για συγκεκριμένες τοποθεσίες και εγκαταστάσεις επεξεργασίας πληροφοριών. Οι τοπικές αρμοδιότητες για την προστασία των περιουσιακών στοιχείων και για την εκτέλεση συγκεκριμένων διαδικασιών ασφαλείας, όπως σχεδιασμό της επιχειρησιακής συνέχειας, θα πρέπει να ορίζονται με σαφήνεια.

Τα άτομα που τους έχουν κατανεμηθεί αρμοδιότητες ασφαλείας μπορούν να αναθέτουν καθήκοντα ασφάλειας σε άλλους. Παρ 'όλα αυτά παραμένουν υπεύθυνοι και θα πρέπει να ελέγχουν ότι οι τα καθήκοντα που έχουν αναθέσει εκτελούνται σωστά.

Περιοχές για τις οποίες τα μεμονωμένα άτομα είναι υπεύθυνα θα πρέπει να αναφέρονται σαφώς και θα πρέπει να πραγματοποιούνται τα ακόλουθα:

1. Τα αγαθά και οι διαδικασίες ασφαλείας που σχετίζονται με κάθε συγκεκριμένο σύστημα θα πρέπει να προσδιορίζονται και να καθορίζονται σαφώς.
2. Θα πρέπει να ανατίθεται η οντότητα που έχει την ευθύνη για κάθε αγαθό ή τη διαδικασία ασφάλειας και οι λεπτομέρειες αυτής της ευθύνης θα πρέπει να τεκμηριώνονται.
3. Τα επίπεδα εξουσιοδότησης θα πρέπει να είναι σαφώς καθορισμένα και τεκμηριωμένα.

Σε πολλούς οργανισμούς ένας διαχειριστής ασφάλειας πληροφοριών θα πρέπει να οριστεί για να αναλάβει τη γενική ευθύνη για την ανάπτυξη και εφαρμογή της ασφάλειας και να στηρίξει τον καθορισμό των ελέγχων.

Ωστόσο, η ευθύνη για τη στελέχωση και την εφαρμογή των ελέγχων συχνά παραμένει στους επιμέρους διευθυντές. Μια κοινή πρακτική είναι να ορίσει έναν ιδιοκτήτη για κάθε αγαθό που στη συνέχεια γίνεται υπεύθυνος για την καθημερινή προστασία της.

2.2.5.1.4 Διαδικασία αδειοδότησης για τις εγκαταστάσεις επεξεργασίας πληροφοριών

Πρέπει να καθοριστεί και να εφαρμοστεί μια διαδικασία διαχείρισης εξουσιοδότησης για νέες εγκαταστάσεις επεξεργασίας των πληροφοριών.

Οι ακόλουθες κατευθυντήριες γραμμές θα πρέπει να εξεταστούν για τη διαδικασία αδειοδότησης:

1. Οι νέες εγκαταστάσεις πρέπει να διαθέτουν κατάλληλη εξουσιοδότηση διαχείρισης χρηστών, που εξουσιοδοτεί το σκοπό και τη χρήση τους. Η εξουσιοδότηση πρέπει επίσης να λαμβάνεται από τον υπεύθυνο για τη διατήρηση του περιβάλλοντος ασφαλείας του τοπικού πληροφοριακού συστήματος για να εξασφαλίσει ότι πληρούνται όλες οι σχετικές πολιτικές ασφάλειας και απαιτήσεις.

2. Όπου είναι αναγκαίο, το υλικό και το λογισμικό θα πρέπει να ελέγχονται για να διασφαλιστεί ότι αυτά είναι συμβατά με άλλα στοιχεία του συστήματος.
3. Η χρήση των προσωπικών ή ιδιόκτητων συστημάτων, π.χ. φορητοί υπολογιστές, υπολογιστές οικίας ή φορητές συσκευές, για την επεξεργασία των επιχειρηματικών πληροφοριών, μπορεί να εισάγει νέα τρωτά σημεία και οι απαραίτητοι έλεγχοι θα πρέπει να προσδιοριστούν και να υλοποιηθούν.

2.2.5.1.5 Συμφωνίες εμπιστευτικότητας

Θα πρέπει να εντοπίζονται και να επανεξετάζονται τακτικά οι απαιτήσεις για εμπιστευτικότητα ή συμφωνίες μη αποκάλυψης οι οποίες απαιτήσεις αντικατοπτρίζουν τις ανάγκες του οργανισμού για την προστασία των πληροφοριών.

Η εμπιστευτικότητα ή τα συμφωνητικά μη αποκάλυψης θα πρέπει να αντιμετωπίσουν την απαίτηση για την προστασία των εμπιστευτικών πληροφοριών χρησιμοποιώντας νομικά δεσμευτικούς όρους. Για τον προσδιορισμό των απαιτήσεων για λόγους εμπιστευτικότητας ή μη αποκάλυψης συμφωνιών, τα ακόλουθα στοιχεία θα πρέπει να θεωρούνται:

1. Ο ορισμός των πληροφοριών που πρέπει να προστατεύονται (π.χ. εμπιστευτικές πληροφορίες).
2. Η αναμενόμενη διάρκεια της συμφωνίας, συμπεριλαμβανομένων των περιπτώσεων όπου η εμπιστευτικότητα θα πρέπει να διατηρηθεί επ 'αόριστον.
3. Απαιτούμενες δράσεις, όταν μια συμφωνία τερματίζεται.
4. Οι ευθύνες και οι ενέργειες των υπογραφόντων ώστε να αποφεύγεται μη εξουσιοδοτημένη κοινοποίηση πληροφοριών.
5. Η κυριότητα των πληροφοριών, των εμπορικών μυστικών και της πνευματικής ιδιοκτησίας, και πώς αυτό σχετίζεται με την προστασία των εμπιστευτικών πληροφοριών.
6. Η επιτρεπόμενη χρήση των εμπιστευτικών πληροφοριών, και τα δικαιώματα του υπογράφοντος να χρησιμοποιήσουν τις πληροφορίες.
7. Το δικαίωμα να ελέγχονται και να παρακολουθούνται δραστηριότητες που αφορούν εμπιστευτικές πληροφορίες.

8. Διαδικασία για κοινοποίηση και αναφορά μη εξουσιοδοτημένης αποκάλυψης ή παραβίασης εμπιστευτικών πληροφοριών.
9. Όρους για πληροφορίες που πρέπει να επιστραφούν ή να καταστραφούν κατά τη διακοπή της συμφωνίας.
10. Αναμενόμενες ενέργειες που πρέπει να ληφθούν σε περίπτωση παραβίασης αυτής της συμφωνίας.

Με βάση τις απαιτήσεις ασφαλείας του οργανισμού, άλλα στοιχεία μπορεί να χρειαστούν σε μια συμφωνία εμπιστευτικότητας ή μη αποκάλυψης.

Συμφωνίες εμπιστευτικότητας και μη αποκάλυψης πρέπει να συμμορφώνονται με όλους τους ισχύοντες νόμους και κανονισμούς για την αρμοδιότητα για την οποία ισχύει.

Οι απαιτήσεις για την εμπιστευτικότητα και τη μη γνωστοποίηση συμφωνιών θα πρέπει να επανεξετάζονται περιοδικά αλλά και όταν συμβαίνουν αλλαγές που επηρεάζουν αυτές τις απαιτήσεις.

2.2.5.1.6 Επικοινωνία με τις αρχές

Θα πρέπει να διατηρούνται οι κατάλληλες επαφές με τις αρμόδιες αρχές.

Οι οργανισμοί πρέπει να διαθέτουν διαδικασίες που καθορίζουν πότε και προς ποιές αρχές (π.χ. αστυνομία, πυροσβεστική, εποπτικές αρχές) θα πρέπει να επικοινωνήσουν, και πώς τα προσδιορισμένα περιστατικά ασφάλειας πληροφοριών θα πρέπει να αναφέρονται εγκαίρως.

Οι οργανισμοί που δέχονται επίθεση από το Διαδίκτυο μπορεί να χρειαστούν εξωτερικούς φορείς (π.χ. μια υπηρεσία παροχής Internet ή το φορέα τηλεπικοινωνιών) να αναλάβουν δράση ενάντια στην πηγή της επίθεσης.

Απαραίτητη προϋπόθεση για την υποστήριξη της διαχείρισης των περιστατικών ασφάλειας πληροφοριών ή την επιχειρησιακή συνέχεια και διαδικασία σχεδιασμού έκτακτης ανάγκης είναι το να διατηρούνται αυτές οι επαφές. Επαφές με τους ρυθμιστικούς φορείς είναι επίσης χρήσιμο να προβλεφθούν και να προετοιμαστούν για επικείμενες αλλαγές στη νομοθεσία ή κανονισμούς, οι οποίοι πρέπει να ακολουθούνται από τον οργανισμό. Επαφές με άλλες αρχές περιλαμβάνουν τις επαφές με επιχειρήσεις κοινής ωφέλειας, με υπηρεσίες έκτακτης ανάγκης και ασφάλειας, με τις υγειονομικές υπηρεσίες. Για παράδειγμα, πυροσβεστικές υπηρεσίες για την επιχειρησιακή συνέχεια,

πάροχοι τηλεπικοινωνιακών συστημάτων για τη δρομολόγηση γραμμής και διαθεσιμότητα και προμηθευτές νερού για την ψύξη για τις εγκαταστάσεις εξοπλισμού.

2.2.5.1.7 Επικοινωνία με ομάδες ειδικού ενδιαφέροντος

Θα πρέπει να διατηρούνται οι κατάλληλες επαφές με ομάδες ειδικού ενδιαφέροντος ή άλλα φόρουμ με ειδίκευση στην ασφάλεια.

Η συμμετοχή σε ομάδες ειδικών συμφερόντων ή φόρουμ θα πρέπει να θεωρείται ως μέσο για:

1. Τη βελτίωση των γνώσεων σχετικά με τις βέλτιστες πρακτικές και την ενημέρωση σχετικά με ασφάλεια πληροφοριών.
2. Τη διασφάλιση ότι το περιβάλλον ασφάλειας πληροφοριών είναι σύγχρονο και πλήρες.
3. Τη λήψη έγκαιρων προειδοποιήσεων για επιθέσεις και ευπάθειες.
4. Την απόκτηση πρόσβασης σε συμβουλές ασφάλειας πληροφοριών από ειδικούς.

2.2.5.1.8 Ανεξάρτητη αναθεώρηση της ασφάλειας των πληροφοριών

Η προσέγγιση του οργανισμού στη διαχείριση της ασφάλειας των πληροφοριών και η εφαρμογή της θα πρέπει να αναθεωρηθούν ανεξάρτητα σε προγραμματισμένα διαστήματα, ή όταν σημειώνονται σημαντικές αλλαγές στην υλοποίηση της ασφάλειας.

Την ανεξάρτητη αναθεώρηση πρέπει να την ξεκινάει η διοίκηση. Μια τέτοια ανεξάρτητη εξέταση είναι απαραίτητη για τη διασφάλιση της συνεχούς καταλληλότητας, επάρκειας και αποτελεσματικότητας της προσέγγισης του οργανισμού για ασφάλεια. Πρέπει να περιλαμβάνεται αξιολόγηση ευκαιριών για βελτίωση.

Η εξέταση αυτή θα πρέπει να πραγματοποιείται από άτομα ανεξάρτητα της υπό εξέταση περιοχής, π.χ. τη λειτουργία του εσωτερικού ελέγχου, ένα ανεξάρτητο στέλεχος ή έναν τρίτο εξωτερικό οργανισμό που ειδικεύεται σε τέτοιες αξιολογήσεις. Άτομα που εκτελούν αυτές τις αναθεωρήσεις θα πρέπει να έχουν τις κατάλληλες δεξιότητες και εμπειρία. Τα αποτελέσματα πρέπει να καταγράφονται και να αναφέρονται στη διοίκηση που ξεκίνησε αυτή τη διαδικασία. Αυτές οι αναφορές πρέπει να διατηρούνται.

Αν το αποτέλεσμα αναδείξει κάποιο έλλειμμα ασφάλειας ή μη συμμόρφωση με τις κατευθύνσεις του κειμένου πολιτικής ασφάλειας τότε η διοίκηση πρέπει να σκεφτεί για διορθωτικές ενέργειες.

2.2.5.2 Οργάνωση ασφάλειας εκτός του οργανισμού

Ο στόχος αυτής της κατηγορίας ασφάλειας είναι να διατηρηθεί η ασφάλεια των πληροφοριών του οργανισμού και των εγκαταστάσεων επεξεργασίας πληροφοριών που είναι προσβάσιμες, επεξεργάζονται, ή διαχειρίζονται από τρίτους εξωτερικούς φορείς ή επικοινωνούνται σε αυτούς. Η ασφάλεια αυτών των εγκαταστάσεων δεν πρέπει να μειώνεται με την εισαγωγή προϊόντων ή υπηρεσιών που παρέχονται από τους εξωτερικούς φορείς-συνεργάτες. Θα πρέπει να ελέγχεται η πρόσβαση που δίνεται σε εξωτερικούς φορείς στις εγκαταστάσεις αυτές.

Όταν υπάρχει επιχειρησιακή ανάγκη για συνεργασία με εξωτερικούς φορείς που ενδέχεται να απαιτούν πρόσβαση σε πληροφορίες του οργανισμού και εγκαταστάσεις επεξεργασίας πληροφοριών θα πρέπει να διεξάγεται εκτίμηση κινδύνων για τον προσδιορισμό τις επιπτώσεις ασφάλειας και τις απαιτήσεις ελέγχου. Οι έλεγχοι πρέπει να συμφωνούνται και να καθορίζονται από κοινού με τον εξωτερικό φορέα. Παρακάτω παρουσιάζονται οι τρεις τύποι ελέγχων για

2.2.5.2.1 Προσδιορισμός των κινδύνων που συνδέονται με εξωτερικούς φορείς

Οι κίνδυνοι για τις πληροφορίες του οργανισμού και τις εγκαταστάσεις επεξεργασίας πληροφοριών από τις επιχειρησιακές διαδικασίες που αφορούν τα εξωτερικά συμβαλλόμενα μέρη θα πρέπει να προσδιορίζονται και να εφαρμόζονται κατάλληλοι έλεγχοι πριν από τη χορήγηση της πρόσβασης.

Για τον προσδιορισμό κινδύνων που σχετίζονται με εξωτερική πρόσβαση τρίτων θα πρέπει να λαμβάνουν υπόψη τα ακόλουθα ζητήματα:

1. Οι εγκαταστάσεις που απαιτείται πρόσβαση από εξωτερικό φορέα.
2. Ο τύπος πρόσβασης που θα έχει στις εγκαταστάσεις και στις ίδιες τις πληροφορίες. Πχ. Φυσική πρόσβαση όπως σε γραφεία και αίθουσες υπολογιστών, ή λογική πρόσβαση όπως σε πληροφοριακά συστήματα και βάσεις

δεδομένων. Επίσης συνδεσιμότητα μεταξύ των δικτύων του οργανισμού και του εξωτερικού φορέα όπως απομακρυσμένη πρόσβαση.

3. Η αξία και η ευαισθησία των συγκεκριμένων πληροφοριών, και η κρισιμότητα της για τις επιχειρηματικές δραστηριότητες.
4. Τους απαραίτητους ελέγχους για την προστασία των πληροφοριών που δεν προορίζονται να είναι προσβάσιμες από τρίτους.
5. Το προσωπικό του εξωτερικού φορέα που έχει πρόσβαση και ζητήματα όπως η εξακρίβωση της εξουσιοδότησης σε αυτό, και πόσο συχνά πρέπει να επιβεβαιώνεται η εξουσιοδότηση αυτή.
6. Ο αντίκτυπος όταν η πρόσβαση δεν είναι διαθέσιμη στο εξωτερικό μέρος, και η λήψη ανακριβής ή παραπλανητικής πληροφορίας.
7. Νομικές υποχρεώσεις που σχετίζονται με εξωτερικούς φορείς.

Η πρόσβαση στις πληροφορίες του οργανισμού σε τρίτους δεν πρέπει να παρέχεται έως ότου οι κατάλληλοι έλεγχοι τεθούν σε εφαρμογή και, όπου αυτό είναι εφικτό, να έχει υπογραφεί ένα συμβόλαιο για τον καθορισμό των όρων και των προϋποθέσεων για τη σύνδεση ή την πρόσβαση και τη ρύθμιση εργασίας. Σε γενικές γραμμές, όλες οι απαιτήσεις ασφάλειας που προκύπτουν από την συνεργασία με εξωτερικούς φορείς ή από τους εσωτερικούς ελέγχους θα πρέπει να αντικατοπτρίζονται από τη συμφωνία με το εξωτερικό μέρος.

Πληροφορίες μπορεί να τεθούν σε κίνδυνο από εξωτερικούς φορείς με ανεπαρκή διαχείριση της ασφάλειας. Πρέπει να προσδιορίζονται και να εφαρμόζονται έλεγχοι για τη διαχείριση πρόσβαση των εξωτερικών φορέων σε εγκαταστάσεις επεξεργασίας των πληροφοριών. Για παράδειγμα, εάν υπάρχει μια ειδική ανάγκη εμπιστευτικότητας των πληροφοριών, θα μπορούσε να χρησιμοποιηθεί συμφωνία μη αποκάλυψης.

Οι οργανισμοί μπορεί να αντιμετωπίσουν κινδύνους που συνδέονται με τις διαδικασίες, τη διαχείριση και την επικοινωνία μεταξύ οργανισμών εάν εφαρμόζεται ένα υψηλό επίπεδο εξωτερικής ανάθεσης (outsourcing), ή όπου εμπλέκονται πολλοί εξωτερικό φορείς.

2.2.5.2.2 Αντιμετώπιση της ασφάλειας σε σχέση με πελάτες

Όλες οι καθορισμένες απαιτήσεις ασφαλείας θα πρέπει να αντιμετωπιστούν πριν δοθεί στους πελάτες πρόσβαση σε πληροφορίες ή αγαθά του οργανισμού.

Οι ακόλουθοι όροι πρέπει να θεωρηθούν πριν δοθεί στους πελάτες πρόσβαση στα αγαθά του οργανισμού:

1. Προστασία των αγαθών μέσω διαδικασιών προστασίας πληροφοριών και λογισμικού και διαχείρισης γνωστών ευπαθειών και μέσω προφύλαξης της ακεραιότητας και εμπιστευτικότητας των δεδομένων.
2. Πολιτικές ελέγχου πρόσβασης που καλύπτουν:

- Τις επιτρεπόμενες μεθόδους πρόσβασης, καθώς και τον έλεγχο και τη χρήση μοναδικών αναγνωριστικών όπως τα ονόματα χρήστη και οι κωδικοί πρόσβασης.
- Διαδικασία αδειοδότησης για την πρόσβαση και τα προνόμια των χρηστών.
- Διαδικασία για την ανάκληση των δικαιωμάτων πρόσβασης ή τη διακοπή της σύνδεσης μεταξύ των συστημάτων.

3. Διαδικασίες για αναφορά, ειδοποίηση και διερεύνηση ανακριβών πληροφοριών, περιστατικών και παραβιάσεων ασφάλειας.
4. Τα δικαιώματα πνευματικής ιδιοκτησίας και την εκχώρηση δικαιωμάτων πνευματικής ιδιοκτησίας.
5. Νομικό πλαίσιο που θα ικανοποιείται από τον έλεγχο αυτό.

Οι απαιτήσεις ασφάλειας μπορούν να αντιμετωπιστούν με συμφωνίες μεταξύ του οργανισμού και του πελάτη, οι οποίες περιέχουν τους συγκεκριμένους κινδύνους.

2.2.5.2.3 Αντιμετώπιση της ασφάλειας για συμφωνίες με εξωτερικούς φορείς

Οι συμφωνίες με τρίτους που αφορούν πρόσβαση, την επεξεργασία, την επικοινωνία ή τη διαχείριση των πληροφοριών του οργανισμού ή τις εγκαταστάσεις επεξεργασίας πληροφοριών, ή την προσθήκη των προϊόντων ή των υπηρεσιών στις εγκαταστάσεις επεξεργασίας των πληροφοριών πρέπει να καλύπτουν όλες τις σχετικές απαιτήσεις ασφάλειας.

Οι ακόλουθοι όροι θα πρέπει να εξεταστούν για συμπερίληψή τους στη συμφωνία, προκειμένου να ικανοποιήσει τις καθορισμένες απαιτήσεις ασφάλειας:

1. Η πολιτική ασφάλειας πληροφοριών.
2. Οι έλεγχοι διασφάλισης της προστασίας των αγαθών, που περιλαμβάνουν διαδικασίες προστασίας υλικού και λογισμικού, ελέγχους φυσικής προστασίας, ελέγχους ενάντια σε κακόβουλο λογισμικό, ελέγχους επιστροφής ή καταστροφής

πληροφοριών με το πέρας μιας συμφωνίας, και τέλος περιορισμούς στην αντιγραφή και αποκάλυψη των ιδιοτήτων κάθε αγαθού.

3. Εκπαίδευση χρηστών και διαχειριστών σε μεθόδους και διαδικασίες.
4. Επίγνωση των ευθυνών, ειδικότερα για εγκατάσταση και συντήρηση υλικού και λογισμικού.
5. Πολιτική ελέγχου πρόσβασης που περιλαμβάνει:
    - Τους διάφορους λόγους και απαιτήσεις για τους οποίους είναι απαραίτητη η πρόσβαση από τον εξωτερικό φορέα.
    - Τις επιτρεπόμενες μεθόδους πρόσβασης, καθώς και τον έλεγχο και τη χρήση μοναδικών αναγνωριστικών όπως τα ονόματα χρήστη και οι κωδικοί πρόσβασης.
    - Διατήρηση καταλόγου εξουσιοδοτημένων ατόμων για πρόσβαση και με τα αντίστοιχα δικαιώματα που τους έχουν δοθεί.
    - Διαδικασία ανάκλησης δικαιωμάτων ή διακοπής διασύνδεσης μεταξύ συστημάτων.
6. Το δικαίωμα να ελέγχει τις αρμοδιότητες που ορίζονται στη συμφωνία, οι έλεγχοι να διενεργούνται από τρίτους, και να απαριθμήσει τα νόμιμα δικαιώματα των ελεγκτών.
7. Άλλοι όροι κοινοί με την ασφάλεια σε σχέση με πελάτες όπως διαδικασίες για αναφορά περιστατικών, πνευματικά δικαιώματα και νομικό πλαίσιο.

Στο πρότυπο αναλύονται θέματα που αφορούν εξωτερική ανάθεση της ασφάλεια πληροφοριών σε άλλο εξωτερικό φορέα και πως και σε ποιό τομέα πρέπει να διαφοροποιηθούν οι διαδικασίες και οι συμφωνίες.

2.2.6 Διαχείριση αγαθών/περιουσιακών στοιχείων

Σε αυτή την παράγραφο περιέχονται δύο κύριες κατηγορίες ασφάλειας η ευθύνη των αγαθών και η ταξινόμηση των πληροφοριών.

2.2.6.1 Ευθύνη των αγαθών

Ο στόχος είναι να επιτευχθεί και να διατηρηθεί η κατάλληλη προστασία των αγαθών του οργανισμού με το να αντιπροσωπεύονται τα αγαθά από έναν ιδιοκτήτη ο οποίος θα έχει και ευθύνη για τον συγκεκριμένο πόρο. Η υλοποίηση των ελέγχων μπορεί να προωθηθεί σε άλλον αλλά την ευθύνη τη διατηρεί ο ιδιοκτήτης του αγαθού.

Η ευθύνη των αγαθών χωρίζεται σε τρείς κατηγορίες ελέγχων: στην καταγραφή των αγαθών, την κυριότητα των αγαθών και την αποδεκτή χρήση των αγαθών.

Καταγραφή των αγαθών

Όλα τα αγαθά πρέπει να προσδιορίζονται σαφώς και να καταρτίζεται και να διατηρείται μια καταγραφή όλων των σημαντικών αγαθών.

Η απογραφή/καταγραφή των αγαθών θα πρέπει να περιλαμβάνει όλες τις απαραίτητες πληροφορίες προκειμένου να γίνει ανάκτηση από μια καταστροφή, και να περιλαμβάνει τον τύπο του αγαθού, τη μορφή, τη θέση, την πληροφορία αντιγράφων ασφαλείας και την επιχειρησιακή αξία του. Η απογραφή δεν πρέπει να επικαλύπτει άλλες καταγραφές, αλλά θα πρέπει να διασφαλιστεί ότι το περιεχόμενο είναι σε συμφωνία με αυτές.

Υπάρχουν πολλοί τύποι αγαθών, μεταξύ αυτών:

1. Πληροφορίες: βάσεις δεδομένων και αρχεία δεδομένων, συμβόλαια και συμφωνίες, έγγραφα περιγραφής συστημάτων, πληροφορίες από έρευνες, εγχειρίδια χρήσης, εκπαιδευτικό υλικό, λειτουργικές διαδικασίες ή διαδικασίες υποστήριξης, πλάνα επιχειρησιακής συνέχειας, λογιστικοί έλεγχοι, και αρχειοθετημένες πληροφορίες.
2. Λογισμικό εφαρμογής, λογισμικό συστήματος, εργαλεία ανάπτυξης.
3. Υλικά αγαθά όπως υπολογιστές, τηλεπικοινωνιακό υλικό, αφαιρούμενα μέσα.
4. Υπηρεσίες όπως υπολογιστικές και τηλεπικοινωνιακές εργασίες, γενικές λειτουργίες όπως θέρμανση, φωτισμός, τροφοδοσία ρεύματος και κλιματισμός.
5. Προσωπικό και οι δυνατότητές του όπως οι γνώσεις και η εμπειρία.
6. Άϋλα στοιχεία, όπως η φήμη και η εικόνα του οργανισμού.

Η διαδικασία σύνταξης μιας καταγραφής των αγαθών/περιουσιακών στοιχείων είναι απαραίτητη προϋπόθεση της διαχείρισης κινδύνων

Κυριότητα των αγαθών

Όλες οι πληροφορίες και τα αγαθά που σχετίζονται με πληροφοριακά συστήματα θα πρέπει να ανήκουν σε προκαθορισμένο τμήμα της οργάνωσης.

Ο ιδιοκτήτης του αγαθού θα είναι υπεύθυνος για την εξασφάλιση της κατάλληλης ταξινόμησης των αγαθών και επίσης για τον καθορισμό και την περιοδική επανεξέταση των περιορισμών πρόσβασης και τις ταξινομήσεων, λαμβάνοντας υπόψη τις ισχύουσες πολιτικές ελέγχου πρόσβασης.

Η ιδιοκτησία μπορεί να αφορά μια επιχειρησιακή διαδικασία ή ένα σύνολο δραστηριοτήτων ή μια εφαρμογή ή ένα σύνολο δεδομένων.

Σε πολύπλοκα συστήματα πληροφοριών, μπορεί να είναι χρήσιμο να οριστούν ομάδες αγαθών, που δρουν μαζί για να προσφέρουν μια συγκεκριμένη λειτουργία σαν «υπηρεσίες». Σε αυτή την περίπτωση ο ιδιοκτήτης της υπηρεσίας είναι υπεύθυνος για την παροχή της υπηρεσίας, συμπεριλαμβανομένης και της λειτουργίας των αγαθών, τα οποία την παρέχουν.

Αποδεκτή χρήση των αγαθών

Πρέπει να προσδιορίζονται, να τεκμηριώνονται και να εφαρμόζονται κανόνες για την αποδεκτή χρήση των πληροφοριών και των αγαθών που σχετίζονται με εγκαταστάσεις επεξεργασίας των πληροφοριών.

Οι κανόνες αυτοί περιλαμβάνουν:

- Κανόνες περί ηλεκτρονικού ταχυδρομείου και χρήσης Διαδικτύου.
- Οδηγίες για χρήση κινητού τηλεφώνου, κυρίως για χρήση εκτός των κτιρίων του οργανισμού.

2.2.6.2 Ταξινόμηση των πληροφοριών

Στόχος της ταξινόμησης είναι να εξασφαλιστεί ότι κάθε πληροφορία λαμβάνει ένα κατάλληλο επίπεδο προστασίας.

Οι πληροφορίες πρέπει να ταξινομηθούν για να αναδειχθεί η ανάγκη, οι προτεραιότητες, και ο αναμενόμενος βαθμός προστασίας κατά το χειρισμό των πληροφοριών.

Η κάθε πληροφορία έχει διαφορετικό βαθμό ευαισθησίας και κρισιμότητας. Ορισμένα στοιχεία μπορεί να απαιτήσουν ένα επιπλέον επίπεδο προστασίας ή ειδικό χειρισμό. Ένα σύστημα ταξινόμησης πληροφοριών θα πρέπει να χρησιμοποιείται για να καθορίσει μια σειρά κατάλληλων επιπέδων προστασίας και να επικοινωνεί την ανάγκη για ειδικά μέτρα διαχείρισης.

Κατευθυντήριες γραμμές για την ταξινόμηση

Οι πληροφορίες πρέπει να κατατάσσονται με βάσει την αξία τους, τις νομικές απαιτήσεις, την ευαισθησία, και την κρισιμότητα για τον οργανισμό.

Θα πρέπει να είναι ευθύνη του ιδιοκτήτη κάθε αγαθού να καθορίσει την τάξη που ανήκει αυτό και να εξασφαλίσει ότι παραμένει ενήμερο ως προς το ποιά κλάση ανήκει το αγαθό.

Ένα θέμα είναι ο αριθμός των κλάσεων που θα οριστούν και τα οφέλη που προκύπτουν από τη χρήση τους. Τα μεγάλα και περίπλοκα σχήματα ταξινόμησης έχουν αποδειχθεί δυσκίνητα και αντιοικονομικά οπότε δεν προτιμώνται.

Σε γενικές γραμμές, ο χαρακτηρισμός που δίνεται στις πληροφορίες είναι ένας σύντομος δρόμος για τον καθορισμό του πώς αυτές οι πληροφορίες πρέπει να αντιμετωπίζονται και να προστατεύεται.

Επισήμανση και το χειρισμός πληροφοριών

Θα πρέπει να αναπτυχθεί και να εφαρμοστεί, σύμφωνα με το σύστημα ταξινόμησης που εγκρίθηκε από τον οργανισμό, μια σειρά κατάλληλων διαδικασιών για την επισήμανση και το χειρισμό των πληροφοριών.

Η έξοδος από συστήματα που περιέχουν πληροφορίες που χαρακτηρίζονται ευαίσθητες ή κρίσιμης σημασίας πρέπει να φέρουν κατάλληλη ετικέτα κατάταξης (στην έξοδο). Η επισήμανση θα πρέπει να αντικατοπτρίζει την ταξινόμηση σύμφωνα με τους κανόνες που θεσπίζονται στις κατευθυντήριες γραμμές. Στα στοιχεία προς εξέταση περιλαμβάνονται αναφορές σε έντυπη μορφή, εμφανίσεις οθονών, μέσα καταγραφής (π.χ. κασέτες, δίσκους, CD), ηλεκτρονικά μηνύματα και μεταφορές αρχείων.

Για κάθε επίπεδο ταξινόμησης πρέπει να καθοριστούν διαδικασίες διαχείρισης συμπεριλαμβανομένης της ασφαλούς επεξεργασίας, αποθήκευσης, μεταφοράς, αποχαρακτηρισμού την καταστροφής. Αυτό πρέπει να περιλαμβάνει επίσης τις διαδικασίες για την αλυσίδα επιτήρησης και καταγραφής των σχετικών περιστατικών ασφάλειας.

Η σήμανση και ο ασφαλής χειρισμό των διαβαθμισμένων πληροφοριών αποτελεί βασική προϋπόθεση για τη σύναψη συμφωνιών ανταλλαγής πληροφοριών. Οι φυσικές ετικέτες είναι μια κοινή μορφή της επισήμανσης. Ωστόσο, ορισμένα πληροφοριακά αγαθά, όπως έγγραφα σε ηλεκτρονική μορφή, δεν μπορούν να φέρουν φυσικά μέσα της σήμανσης και πρέπει να χρησιμοποιούνται ηλεκτρονικά.

2.2.7 Ασφάλεια ανθρώπινων πόρων

Η ασφάλεια ανθρωπίνων πόρων χωρίζεται σε τρεις φάσεις: πριν τη συνεργασία με κάποιον υπάλληλο ή εξωτερικό συνεργάτη, κατά τη διάρκεια της συνεργασίας και μετά το πέρας της συνεργασίας.

2.2.7.1 Πριν από τη συνεργασία/πρόσληψη

Στόχος είναι να εξασφαλιστεί ότι οι εργαζόμενοι, οι εργολάβοι και οι χρήστες των εξωτερικών φορέων κατανοούν τις ευθύνες τους, και είναι κατάλληλοι για τους ρόλους τους, και έτσι να μειωθεί ο κίνδυνος της κλοπής, απάτης ή κατάχρησης των εγκαταστάσεων.

Οι αρμοδιότητες ασφαλείας θα πρέπει να απευθυνθούν πριν από την πρόσληψη στις περιγραφές των θέσεων εργασίας και στους όρους και συνθήκες απασχόλησης. Όλοι οι υποψήφιοι για την απασχόληση, εργολάβοι και χρήστες εξωτερικών φορέων θα πρέπει να ελέγχονται επαρκώς, ιδιαίτερα για τις ευαίσθητες θέσεις εργασίας, και στη συνέχεια θα πρέπει να υποχρεωθούν να υπογράψουν συμφωνία πάνω στους ρόλους ασφάλειας και ευθυνών που θα αναλάβουν.

<u>Ρόλοι και ευθύνες</u>

Οι ρόλοι και οι ευθύνες των εργαζομένων, εργολάβων και τρίτων θα πρέπει να καθορίζονται και τεκμηριώνονται σύμφωνα με την πολιτική ασφάλειας πληροφοριών του οργανισμού.

Οι απαιτήσεις είναι:

- Η δράση σύμφωνα με την πολιτική ασφάλειας.
- Η προστασία των αγαθών από μη εξουσιοδοτημένη πρόσβαση, αποκάλυψη, τροποποίηση, καταστροφή ή παρεμβολή.
- Η εκτέλεση ειδικών διαδικασιών ή ενεργειών ασφάλειας.
- Η αναφορά περιστατικών ασφάλειας, ή εν δυνάμει απειλών, ή άλλων κινδύνων ασφαλείας για τον οργανισμό.

<u>Έλεγχος</u>

Πρέπει να πραγματοποιούνται έλεγχοι επαλήθευσης στο υποψήφιο υπάλληλο ή εξωτερικό συνεργάτη σχετικά με τους νόμους, κανονισμούς και τη δεοντολογία και ανάλογα με τις επιχειρησιακές απαιτήσεις.

Κάποιοι έλεγχοι που πρέπει να περιλαμβάνονται είναι οι εξής:

- Έλεγχος αν διαθέτει ικανοποιητικές συστατικές επιστολές.
- Έλεγχος (για την πληρότητα και την ακρίβεια) στο βιογραφικό σημείωμα του αιτούντος.
- Επιβεβαίωση των ακαδημαϊκών και επαγγελματικών προσόντων.
- Έλεγχος των στοιχείων του και εύρεση πιο λεπτομερών πληροφοριών όπως πιστωτικός έλεγχος ή έλεγχος των ποινικών μητρώων.

Για δουλειές που περιλαμβάνουν πρόσβαση σε συστήματα πληροφορικής και ειδικά αν έχουν ευαίσθητα δεδομένα ο οργανισμός θα πρέπει να πραγματοποιήσει πιο λεπτομερείς ελέγχους.

Όροι και προϋποθέσεις της απασχόλησης

Στο πλαίσιο της συμβατικής υποχρέωσης τους, υπάλληλοι, εργολάβοι και χρήστες εξωτερικών φορέων θα πρέπει να συμφωνήσουν και να υπογράψουν τους όρους και τις προϋποθέσεις της σύμβασης εργασίας τους, η οποία πρέπει να αναφέρει τις ευθύνες τους και αυτές του οργανισμού για την ασφάλεια των πληροφοριών.

Οι όροι που υπογράφουν αφορούν την πολιτική του οργανισμού και επιπλέον:

- Για ευαίσθητα δεδομένα υπογράφουν συμφωνητικό εμπιστευτικότητας.
- Νομικές υποχρεώσει και δικαιώματα π.χ. σχετικά με νόμους περί πνευματικής ιδιοκτησίας και περί προστασίας δεδομένων.
- Ευθύνες για τη διαβάθμιση των πληροφοριών και για το χειρισμό πληροφορίας από άλλες εταιρίες ή εξωτερικούς φορείς.
- Ευθύνες που εκτείνονται εκτός των εγκαταστάσεων και εκτός των κανονικών ωρών εργασίας του οργανισμού, π.χ. στην περίπτωση εργασίας από το σπίτι.

2.2.7.2 Κατά τη διάρκεια της συνεργασίας

Ο στόχος είναι να εξασφαλιστεί ότι οι εργαζόμενοι, εργολάβοι και εξωτερικοί χρήστες έχουν επίγνωση των απειλών κατά της ασφάλειας των πληροφοριών, επίγνωση των ευθυνών και υποχρεώσεών τους, και είναι εξοπλισμένοι για την υποστήριξη της πολιτικής ασφάλειας κατά τη διάρκεια της κανονικής εργασίας τους, και έτσι να μειωθεί ο κίνδυνος του ανθρώπινου λάθους.

Αρμοδιότητες διοίκησης

Η διοίκηση πρέπει να απαιτεί από τους υπαλλήλους, εργολάβους και τρίτους χρήστες να εφαρμόσουν την ασφάλεια σύμφωνα με τις καθορισμένες πολιτικές και διαδικασίες της οργάνωσης.

Αυτό πρέπει να το επιτύχει απαιτώντας από αυτούς συγκεκριμένα:

- Να είναι κατάλληλα ενημερωμένοι για τους ρόλους και ευθύνες τους.
- Να έχουν κίνητρα για να εκπληρώσουν τις πολιτικές ασφάλειας.
- Να διατηρούν τις κατάλληλες δεξιότητες και προσόντα.

Αν οι υπάλληλοι δεν έχουν επίγνωση των ευθυνών τους μπορεί να προκαλέσουν σημαντική ζημιά στον οργανισμό. Το προσωπικό με κίνητρο τείνει να είναι πιο αξιόπιστο και προκαλεί λιγότερα περιστατικά ασφάλειας.

Επίγνωση θεμάτων ασφαλείας, την εκπαίδευση και την κατάρτιση

Όλοι οι εργαζόμενοι και οι συνεργάτες ενός οργανισμού πρέπει να λαμβάνουν εκπαίδευση επίγνωσης τακτικές ενημερώσεις στις διαδικασίες ασφάλειας.

Η αρχική εκπαίδευση πρέπει να αφορά τις πολιτικές ασφάλειας. Σε μετέπειτα στάδιο πρέπει να περιλαμβάνονται απαιτήσεις ασφάλειας, νομικές υποχρεώσεις και επιχειρησιακοί έλεγχοι καθώς επίσης και εκπαίδευση στη σωστή χρήση πληροφοριακών συστημάτων, π.χ. διαδικασίας εισόδου στο σύστημα, χρήση πακέτων λογισμικού και πληροφορίες σχετικά με την πειθαρχική διαδικασία.

Πειθαρχική διαδικασία

Πρέπει να υπάρχει επίσημη πειθαρχική διαδικασία για τους υπαλλήλους που έχουν διαπράξει μια παραβίαση ασφάλειας.

Αρχικά πρέπει να επιβεβαιωθεί η παραβίαση ασφάλειας και από ποιόν προήλθε. Κατή την πειθαρχική διαδικασία περιέχονται στοιχεία για τον υπάλληλο όπως η σοβαρότητα του περιστατικού, ο αντίκτυπος στην επιχείρηση, αν είναι πρώτη φορά ή έχει επαναληφθεί, αν έχει περάσει από την αντίστοιχη εκπαίδευση και άλλα στοιχεία. Σε

σοβαρές περιπτώσεις παραπτώματος η διαδικασία πρέπει να επιτρέπει την άμεση αφαίρεση των καθηκόντων, των δικαιωμάτων πρόσβασης και τα προνόμια, καθώς και για την άμεση συνοδεία έξω από την περιοχή, εάν είναι απαραίτητο.

Η πειθαρχική διαδικασία πρέπει να έχει αποτρεπτικό χαρακτήρα.

2.2.7.3 Τερματισμός ή αλλαγή της συνεργασίας

Στόχος είναι να εξασφαλιστεί η έξοδος από τον οργανισμό ή αλλαγή της απασχόλησης με μεθοδευμένο τρόπο για τους εργαζομένους, εργολάβους και χρήστες εξωτερικών φορέων.

Ευθύνες Τερματισμού

Η ανακοίνωση του τερματισμού ευθυνών θα πρέπει να καλύπτει τις τρέχουσες απαιτήσεις ασφάλειας και νομικές ευθύνες και, ενδεχομένως, τις ευθύνες που περιέχονται σε οποιαδήποτε συμφωνία εμπιστευτικότητας, καθώς και τους όρους και τις συνθήκες της απασχόλησης (όπως αναφέραμε παραπάνω) συνεχίζοντας για μια ορισμένη χρονική περίοδο μετά το τέλος απασχόλησης του εργαζομένου, εργολάβου ή εξωτερικού φορέα.

Επιστροφή αγαθών

Όλοι οι εργαζόμενοι, εργολάβοι και εξωτερικοί φορείς θα πρέπει να επιστρέψουν όλα τα αγαθά του οργανισμού που έχουν στην κατοχή τους κατά τη λήξη της απασχόλησης, τη σύμβαση ή τη συμφωνία τους.

Η διαδικασία διακοπής θα πρέπει να επισημοποιηθεί να περιλαμβάνει την επιστροφή όλων των λογισμικών που έχουν εκδοθεί προηγουμένως, εταιρικά έγγραφα και εξοπλισμό. Άλλα αγαθά όπως φορητές συσκευές υπολογιστών, πιστωτικές κάρτες, κάρτες πρόσβασης, λογισμικό, εγχειρίδια, και πληροφορίες που αποθηκεύονται σε ηλεκτρονικά μέσα πρέπει επίσης να επιστρέφονται.

Διαγραφή δικαιωμάτων πρόσβασης

Τα δικαιώματα πρόσβασης όλων των εργαζομένων, των εργολάβων και εξωτερικών φορέων σε πληροφορίες και εγκαταστάσεις επεξεργασίας πληροφοριών θα πρέπει να αφαιρεθούν αμέσως μετά την λήξη της απασχόλησης, σύμβασης ή συμφωνίας τους, ή να προσαρμόζονται με την αλλαγή.

Τα δικαιώματα πρόσβασης σε αγαθά πληροφοριών πιθανών να πρέπει να μειωθούν ή αφαιρεθούν πριν τη λήξη ή αλλαγή της συνεργασίας, ανάλογα με την αξιολόγηση των παραγόντων κινδύνου, όπως:

- Αν ο τερματισμός έγινε από τη πλευρά του υπαλλήλου ή από τη διοίκηση και το λόγο του τερματισμού.
- Τις ευθύνες του υπαλλήλου, εργολάβου, ή εξωτερικού φορέα.
- Την αξία των αγαθών που έχει πρόσβαση.

Σε συγκεκριμένες περιστάσεις τα δικαιώματα πρόσβασης δίνονται έτσι ώστε να είναι διαθέσιμα σε περισσότερα από ένα άτομο π.χ. σε γκρουπ ατόμων. Σε αυτή την περίπτωση οι αποχωρούντες πρέπει να διαγραφούν από κάθε λίστα πρόσβασης ομάδας.

2.2.8 Φυσική ασφάλεια και ασφάλεια περιβάλλοντος

Η φυσική ασφάλεια χωρίζεται σε δύο κατηγορίες: ασφάλεια περιοχής και ασφάλεια εξοπλισμού.

2.2.8.1 Ασφάλεια περιοχής

Στόχος είναι να αποφευχθεί μη εξουσιοδοτημένη φυσική πρόσβαση, βλάβη, και παρέμβαση στους χώρους και τις πληροφορίες του οργανισμού.

Οι κρίσιμες ή ευαίσθητες εγκαταστάσεις επεξεργασίας πληροφοριών πρέπει να στεγάζονται σε ασφαλείς χώρους, να προστατεύονται από καθορισμένες περιμέτρους ασφαλείας, με κατάλληλα εμπόδια και με ελέγχους εισόδου. Θα πρέπει να προστατεύεται φυσικά από μη εξουσιοδοτημένη πρόσβαση, βλάβη, και παρεμβολές.

Η παρεχόμενη προστασία πρέπει να είναι ανάλογη με τους κινδύνους που εντοπίζονται

<u>Περίμετρος φυσικής ασφάλειας</u>

Η περίμετρος ασφαλείας (εμπόδια, τοίχους, πύλες εισόδου με ελεγχόμενη κάρτα ή επανδρωμένα γραφεία υποδοχής) πρέπει να χρησιμοποιηθεί για να προστατευθούν οι περιοχές που περιέχουν πληροφορίες και εγκαταστάσεις επεξεργασίας πληροφοριών.

Οι ακόλουθες οδηγίες πρέπει να θεωρηθούν και να υλοποιηθούν για φυσική περίμετρο:

- Ξεκάθαρα ορισμένη περίμετρος, φυσικά απροσπέλαστη χωρίς κενά, και με χρήση μπάρων ή πορτών είτε θα φυλάσσονται είτε θα μένουν κλειστές.
- Η πρόσβαση θα επιτρέπεται μόνο σε εξουσιοδοτημένο προσωπικό.
- Πρέπει να εγκατασταθούν συστήματα πυρασφάλειας και συναγερμός.

Ιδιαίτερη σημασία για φυσική ασφάλεια πρόσβασης θα πρέπει να δοθεί σε κτίρια όπου στεγάζονται πολλοί οργανισμοί.

Φυσική ασφάλεια και έλεγχος εισόδου

Για την υλοποίηση ελέγχων εισόδου πρέπει να ακολουθηθούν οι παρακάτω οδηγίες:

1. Καταγραφή ημερομηνίας εισόδου επισκεπτών και επίβλεψή τους κατά τη διάρκεια επίσκεψης.
2. Έλεγχος πρόσβασης σε περιορισμένες περιοχές με χρήση μηχανισμών όπως κάρτα ελέγχου πρόσβασης και κωδικός PIN και καταγραφή εισόδου.
3. Τα δικαιώματα πρόσβασης πρέπει να αναθεωρούνται και να καταργούνται όταν κρίνεται απαραίτητο.

Ασφάλεια γραφείων και εγκαταστάσεων

Οι ακόλουθες οδηγίες προτείνονται από το πρότυπο για την ασφάλεια γραφείων, δωματίων και εγκαταστάσεων:

- Να λαμβάνονται υπ’ όψιν οι σχετικοί κανονισμοί και πρότυπα υγείας και ασφάλειας.
- Οι σημαντικές εγκαταστάσεις πρέπει να τοποθετούνται σε σημεία μη προσβάσιμα από το κοινό.
- Ανάλογα με την περίπτωση, τα κτίρια πρέπει να είναι διακριτικά και να δίνουν ελάχιστη ένδειξη του σκοπού τους.

Προστασία από εξωτερικές και περιβαλλοντολογικές απειλές

Πρέπει να εφαρμοστεί έλεγχος προστασίας από πυρκαγιά, πλημμύρα, σεισμό, έκρηξη, πολιτική αναταραχή και άλλες μορφές φυσικών ή ανθρώπινων καταστροφών.

Μερικές οδηγίες είναι: να απομακρύνονται τα εύφλεκτα υλικά από τις εγκαταστάσεις, να υπάρχει εξοπλισμός σε ετοιμότητα (stand-by) σε απομακρυσμένο μέρος ώστε να μην επηρεάζεται από την ίδια καταστροφή, ύπαρξη πυροσβεστικού μηχανισμού.

Εργασία σε χώρους ασφαλείας

Για εργασία σε χώρους ασφάλεια πρέπει θεωρούνται τα εξής:

- Το προσωπικό πρέπει να γνωρίζει ότι χρειάζεται για τη δραστηριότητα που εμπλέκεται και όχι περισσότερα μέσα στην περιοχή ασφαλείας. Προτείνεται η επίβλεψη για εργασίες στο χώρο ασφαλείας.
- Όταν είναι άδειοι οι χώροι ασφαλείας να παραμένουν κλειδωμένοι.
- Να απαγορεύεται η λήψη φωτογραφίας και βίντεο στο χώρο ασφαλείας

Πρόσβαση του κοινού, παράδοση, και τους χώροι φόρτωσης

Σημεία πρόσβασης, όπως οι χώροι παράδοσης και φόρτωσης και άλλα σημεία, όπου μη εξουσιοδοτημένα πρόσωπα μπορούν να εισέρχονται οι εγκαταστάσεις πρέπει να ελέγχονται και, αν είναι δυνατό, να απομονώνονται από τις εγκαταστάσεις επεξεργασίας των πληροφοριών για την αποφυγή μη εξουσιοδοτημένης πρόσβασης.

2.2.8.2 Ασφάλεια εξοπλισμού

Στόχος είναι να αποτραπεί η απώλεια, βλάβη, ή κλοπή των αγαθών και η διακοπή των δραστηριοτήτων του οργανισμού. Η προστασία του εξοπλισμού είναι απαραίτητη για να μειωθεί ο κίνδυνος της μη εξουσιοδοτημένης πρόσβασης σε πληροφορίες και να προστατευτεί από απώλεια ή ζημιά.

Τοποθέτηση εξοπλισμού και προστασία

Οι ακόλουθες κατευθυντήριες γραμμές θα πρέπει να θεωρηθούν για προστασία του εξοπλισμού:

- Ο εξοπλισμός θα πρέπει να τοποθετείται έτσι ώστε να ελαχιστοποιηθεί η μη αναγκαία πρόσβαση σε χώρους εργασίας και η οπτική γωνία προς αυτόν να περιορίζεται για ευαίσθητα δεδομένα.
- Στοιχεία που χρήζουν ειδικής προστασίας θα πρέπει να απομονώνονται και να μειώσει το γενικό επίπεδο προστασίας που απαιτείται.
- Πρέπει να θεσπιστούν κατευθυντήριες γραμμές για φαγητό, ποτό και κάπνισμα κοντά σε εγκαταστάσεις επεξεργασίας των πληροφοριών.

- Να ελέγχονται οι συνθήκες περιβάλλοντος όπως θερμοκρασία και υγρασία ώστε να μην επηρεάζεται ο εξοπλισμός.

Υποστηρικτικά στοιχεία

Ο εξοπλισμός πρέπει να προστατεύεται από διακοπές ρεύματος και άλλες διαταραχές που προκαλούνται από αδυναμίες των στοιχείων υποστήριξης.

Όλα τα υποστηρικτικά στοιχεία, όπως ηλεκτρικό ρεύμα, ύδρευση, αποχέτευση, θέρμανση / εξαερισμός, και κλιματισμός πρέπει να επαρκούν για τα συστήματα που υποστηρίζουν και να επιθεωρούνται συχνά ώστε να μειωθεί ο κίνδυνος κακής λειτουργίας. Μια κατάλληλη παροχή ηλεκτρικού ρεύματος πρέπει να προβλεφθεί που να είναι σύμφωνη με τις προδιαγραφές του κατασκευαστή εξοπλισμού. Μια αδιάλειπτη παροχής ρεύματος (UPS) για την ομαλή υποστήριξη συνεχής λειτουργία συνιστάται για εξοπλισμό που υποστηρίζει βασικές λειτουργίες της επιχείρησης. Σε περίπτωση μεγάλης διακοπής ρεύματος χρειάζεται μια γεννήτρια ηλεκτρικού ρεύματος για να συνεχιστεί η λειτουργία των συστημάτων.

Επίσης προτείνονται λύσεις για την παροχή νερού και για τηλεπικοινωνιακό εξοπλισμό.

Ασφάλεια καλωδίωσης

Η καλωδιώσεις ενέργειας και τηλεπικοινωνιών που μεταφέρουν δεδομένα ή υποστηρίζουν υπηρεσίες πληροφοριών θα πρέπει να προστατεύονται από υποκλοπές ή βλάβες.

Η καλωδίωση πρέπει να βρίσκεται υπογείως ώστε να μην φαίνεται και να μην διέρχεται από δημόσιους χώρους. Επίσης τα καλώδια δικτύου πρέπει να είναι ξεκάθαρα σε έναν τεχνικό ώστε να αποφεύγονται τα λάθη.

Για ευαίσθητα συστήματα επιπλέον έλεγχοι χρειάζονται:

1. Εγκατάσταση οπλισμένων καλωδίων.
2. Χρήση εναλλακτικών διαδρομών και μετάδοσης.
3. Χρήση καλωδίωσης οπτικών ινών.
4. Έναρξη τεχνικών σάρωσης και φυσικών ελέγχων για χρήση μη εξουσιοδοτημένων συσκευών που συνδέονται με τα καλώδια

Συντήρηση εξοπλισμού

Η συντήρηση του εξοπλισμού πρέπει να είναι σε συμφωνία με τις προτεινόμενες επισκευές συντήρησης από τον κατασκευαστή. Επίσης πρέπει να καταγράφονται τα πιθανά και υπαρκτά σφάλματα που έχουν εμφανιστεί καθώς και οι εργασίες συντήρηση που έχουν γίνει.

Ασφάλεια εξοπλισμού εκτός εγκαταστάσεων

Ο εξοπλισμός και τα μέσα ενημέρωσης που λαμβάνονται εκτός του κτιρίου δεν πρέπει να εγκαταλείπονται αφύλακτα σε δημόσιους χώρους. Θα πρέπει να υπάρχει επαρκής ασφαλιστική κάλυψη για να προστατεύσει τον εξοπλισμό εκτός του χώρου.

Επαναχρησιμοποίηση εξοπλισμού

Όλα τα στοιχεία του εξοπλισμού που περιέχουν μέσα αποθήκευσης πρέπει να ελέγχονται για να εξασφαλιστεί ότι όλα τα ευαίσθητα δεδομένα και το λογισμικό έχει αφαιρεθεί ή αντικατασταθεί με ασφάλεια πριν από τη διάθεσή τους. Οι συσκευές που περιέχουν ευαίσθητες πληροφορίες θα πρέπει να καταστραφούν ως συσκευές ή οι πληροφορίες που περιέχουν να καταστραφούν, να διαγραφούν ή να αντικατασταθούν χρησιμοποιώντας τεχνικές που να κάνουν τις αρχικές πληροφορίες μη ανακτήσιμες.

Απομάκρυνση εξοπλισμού

Ο εξοπλισμός, λογισμικό ή πληροφορίες δεν θα πρέπει να απομακρύνεται χωρίς προηγούμενη άδεια.

.

2.2.9 Διαχείριση επικοινωνιών και λειτουργιών

Στην παράγραφο αυτή υπάρχουν 10 επιμέρους κατηγορίες ασφάλειας.

2.2.9.1 Επιχειρησιακές διαδικασίες και ευθύνες

Στόχος είναι να εξασφαλιστεί η ορθή και ασφαλής λειτουργία των εγκαταστάσεων επεξεργασίας πληροφοριών και πρέπει να δημιουργηθούν αρμοδιότητες και διαδικασίες για τη διαχείριση και λειτουργία των εγκαταστάσεων αυτών. Αυτό περιλαμβάνει την ανάπτυξη των κατάλληλων διαδικασιών λειτουργίας. Ενδεχομένως να πρέπει να εφαρμοστεί διαχωρισμός των καθηκόντων, ώστε να μειωθεί ο κίνδυνος της αμελείας ή της εκ προθέσεως κατάχρησης του συστήματος.

Καταγεγραμμένες λειτουργικές διαδικασίες

Θα πρέπει να υπάρχουν καταγεγραμμένες διαδικασίες για τις δραστηριότητες που σχετίζονται με τα πληροφοριακά συστήματα και τα μέσα επικοινωνίας, όπως διαδικασίες εκκίνησης και τερματισμού ηλεκτρονικών υπολογιστών, δημιουργίας αντιγράφων ασφαλείας, συντήρησης εξοπλισμού, χειρισμού μέσων, διαχείρισης αίθουσας ηλεκτρονικών υπολογιστών και ταχυδρομείου. Ακόμα πρέπει να υπάρχουν καταγεγραμμένες οδηγίες για χειρισμό λαθών και επαναφοράς του συστήματος, επαφές για υποστήριξη των συστημάτων, οδηγίες χειρισμού ειδικών εμπιστευτικών αποτελεσμάτων.

Διαχείριση αλλαγών

Πρέπει να ελέγχονται οι αλλαγές σε πληροφοριακά συστήματα. Ιδιαίτερη προσοχή πρέπει να δοθεί στην καταγραφή των αλλαγών, στο σχεδιασμό δοκιμών των αλλαγών, στην εκτίμηση των επιπτώσεων, στην ενημέρωση σε όσους σχετίζονται με το σύστημα που υπόκειται τις αλλαγές και τέλος ιδιαίτερη σημασία έχει να υπάρχει διαδικασία επαναφοράς του συστήματος σε ασφαλή κατάσταση σε περίπτωση αποτυχίας των αλλαγών ή απρόβλεπτων συμβάντων.

Ο ανεπαρκής έλεγχος των αλλαγών είναι μια συνήθης πηγή κινδύνων ασφάλειας. Για αυτό το λόγο πρέπει να υπάρχει επίσημη διαδικασία αλλαγών σε συστήματα και καταγραφή όλων των σχετικών πληροφοριών.

Διαχωρισμός των καθηκόντων

Τα καθήκοντα και οι τομείς ευθύνης θα πρέπει να απομονώνονται, προκειμένου να μειωθούν οι ευκαιρίες για μη εξουσιοδοτημένη ή ακούσια τροποποίηση ή κακή χρήση των αγαθών του οργανισμού. Πρέπει να λαμβάνεται μέριμνα ώστε κανένα πρόσωπο να μην μπορεί να έχει πρόσβαση, να τροποποιεί ή να χρησιμοποιεί αγαθά χωρίς άδεια ή ανίχνευση.

Διαχωρισμός των εγκαταστάσεων ανάπτυξης, δοκιμής, και λειτουργίας

Οι εγκαταστάσεις αυτές πρέπει να είναι ξεχωριστές ώστε να μειωθεί ο κίνδυνος μη εξουσιοδοτημένης πρόσβασης στα συστήματα λειτουργίας ή συστήματα παραγωγής του οργανισμού. Πρέπει να ορίζονται και να καταγράφονται κανόνες για τη μεταφορά του λογισμικού από το περιβάλλον ανάπτυξης στο περιβάλλον λειτουργίας. Το λογισμικό ανάπτυξης και το λογισμικό λειτουργίας πρέπει να τρέχουν σε διαφορετικά σύστημα ή περιοχές. Επίσης τα συστήματα δοκιμών (test systems) πρέπει να προσομοιώνουν τα συστήματα παραγωγής σε όσο μεγαλύτερο βαθμό γίνεται αλλά οι χρήστες να χρησιμοποιούν διαφορετικά προφίλ για τεστ συστήματα και συστήματα παραγωγής.

Όταν το προσωπικό ανάπτυξης και δοκιμών έχει πρόσβαση στο σύστημα παραγωγής και τις πληροφορίες του, μπορεί να είναι σε θέση να εισάγουν μη εξουσιοδοτημένο κώδικα που δεν έχει δοκιμαστεί ή να τροποποιήσουν επιχειρησιακά δεδομένα.

2.2.9.2 Διαχείριση υπηρεσίας παράδοσης από εξωτερικούς φορείς

Στόχος είναι να εφαρμοστεί και να διατηρηθεί το κατάλληλο επίπεδο ασφάλειας των πληροφοριών και παροχή υπηρεσιών σύμφωνα με τις συμφωνίες παροχής υπηρεσιών με τον εξωτερικό φορέα. Ο οργανισμός πρέπει να ελέγχει την εφαρμογή των συμφωνιών, την παρακολούθηση της συμμόρφωσης με τις συμφωνίες και να διαχειρίζεται τις αλλαγές για να διασφαλίσει ότι οι υπηρεσίες που παρέχονται πληρούν όλες τις απαιτήσεις που συμφωνήθηκαν με τον εξωτερικό φορέα.

Παράδοση υπηρεσίας

Ο οργανισμός πρέπει να διασφαλίσει ότι ο εξωτερικός διατηρεί επαρκή ικανότητα παροχής υπηρεσιών σε συνδυασμό με αποτελεσματικά σχέδια που αποσκοπούν στο να διασφαλίσουν ότι τηρούνται τα αποδεκτά επίπεδα συνέχειας των υπηρεσιών μετά από μεγάλες αποτυχίες της υπηρεσία ή

Παρακολούθηση και αξιολόγηση των υπηρεσιών εξωτερικών φορέων

Η παρακολούθηση και αξιολόγηση των υπηρεσιών τρίτων θα πρέπει να διασφαλίζει ότι οι συμφωνημένοι όροι ασφάλειας πληροφοριών τηρούνται, και ότι τα περιστατικά ασφάλειας πληροφοριών διαχειρίζονται κατάλληλα.

Οι υποχρεώσεις του οργανισμού είναι:

- Η παρακολούθηση των επιπέδων απόδοσης των υπηρεσιών.
- Η αναθεώρηση των εκθέσεων των υπηρεσιών που παράγονται τον εξωτερικό φορέα και να κανονίζει τακτικές συσκέψεις, όπως απαιτείται από τις συμφωνίες.
- Η παροχή πληροφοριών σχετικά με περιστατικά ασφάλειας.

Η ευθύνη για τη διαχείριση της σχέσης με τον εξωτερικό φορέα θα πρέπει να ανατεθεί σε ένα καθορισμένο άτομο ή σε ομάδα διαχείρισης υπηρεσιών.

Διαχείριση αλλαγών σε υπηρεσίες εξωτερικών φορέων

Η διαδικασία της διαχείρισης των αλλαγών σε μια υπηρεσία εξωτερικού φορέα πρέπει να λάβει υπόψη:

- Τις αλλαγές που πραγματοποιούνται από τον οργανισμό όπως βελτιώσεις των προσφερόμενων υπηρεσιών, ανάπτυξη νέων εφαρμογών, αλλαγές των πολιτικών του οργανισμού και νέους ελέγχους για επίλυση περιστατικών ασφάλειας.
- Τις αλλαγές στις υπηρεσίες εξωτερικού φορέα για να υλοποιηθούν βελτιώσεις στα δίκτυα, για χρήση νέων τεχνολογιών, υιοθέτηση νέων προϊόντων, αλλαγές στη φυσική τοποθεσία των συστημάτων και αλλαγές στους προμηθευτές.

2.2.9.3 Σχεδιασμός συστήματος και αποδοχή

Ο στόχος είναι να ελαχιστοποιηθεί ο κίνδυνος αστοχιών του συστήματος. Εκ των προτέρων σχεδιασμός και προετοιμασία απαιτούνται για την εξασφάλιση της διαθεσιμότητας επαρκούς χωρητικότητας και πόρων για να παραδοθεί η απαιτούμενη απόδοση του συστήματος. Θα πρέπει να γίνουν προβλέψεις των μελλοντικών απαιτήσεων για ικανότητα του συστήματος, για να μειώσει τον κίνδυνο υπερφόρτωσης του συστήματος στο μέλλον.

Διαχείριση Χωρητικότητας

Για κάθε νέα και τρέχουσα δραστηριότητα, θα πρέπει να προσδιοριστούν απαιτήσεις χωρητικότητας. Θα πρέπει να εφαρμοστεί αυτόματος συντονισμός και παρακολούθηση χωρητικότητας για την εξασφάλιση και τη βελτίωση της διαθεσιμότητας και της αποτελεσματικότητας των συστημάτων. Έλεγχοι εντοπισμού θα πρέπει να τεθούν σε ισχύ για να αναφέρουν προβλήματα που παρουσιάζονται.

Αποδοχή συστήματος

Η αποδοχή των κριτηρίων για εγκατάσταση ή αναβάθμιση συστημάτων θα πρέπει να εξετάσει τα εξής στοιχεία:

- Απαιτήσεις απόδοσης και χωρητικότητας υπολογιστών.
- Επαναφορά συστήματος και διαδικασίες επανεκκίνησης.
- Αποδείξεις ότι η εγκατάσταση νέου συστήματος δεν θα επηρεάσει τα ήδη υπάρχοντα.
- Ευκολία στη χρήση καθώς έτσι επηρεάζεται η απόδοση των χρηστών και αποφεύγονται τα ανθρώπινα λάθη.

2.2.9.4 Προστασία από κακόβουλο και κινητό κώδικα

Στόχος είναι η προστασία της ακεραιότητας λογισμικού και πληροφοριών.

Το λογισμικό και τα πληροφοριακά συστήματα είναι ευάλωτα στην εισαγωγή κακόβουλου κώδικα, όπως οι ιοί, δικτυακά σκουλήκια (worms), δούρειοι ίπποι, και λογικές βόμβες. Οι χρήστες πρέπει να γνωρίζουν τους κινδύνους αυτούς. Οι διευθυντές θα πρέπει, ενδεχομένως, θα καθιερώσουν ελέγχους για την πρόληψη, την ανίχνευση και αφαίρεση κακόβουλου κώδικα και τον έλεγχο των κινητού κώδικα.

Έλεγχος για κακόβουλο λογισμικό

Η προστασία από κακόβουλο κώδικα θα πρέπει να βασίζεται στην ανίχνευση του και σε λογισμικό επισκευής, και στην ευαισθητοποίηση σε θέματα ασφάλειας. Οι οδηγίες που ακολουθούν θα πρέπει να εξετάζονται:

- Η θέσπιση μιας επίσημης πολιτικής για την προστασία έναντι των κινδύνων που συνδέονται με τη λήψη αρχείων και λογισμικού, είτε μέσω εξωτερικών δικτύων, ή από οποιοδήποτε άλλο μέσο.
- Διεξαγωγή τακτικών ελέγχων λογισμικού και δεδομένων για κρίσιμα πληροφοριακά συστήματα.
- Εγκατάσταση λογισμικού ανίχνευσης και διόρθωσης κακόβουλου λογισμικού που θα ελέγχει αρχεία με αποσπώμενα μέσα, τα συνημμένα αρχεία ηλεκτρονικού ταχυδρομείου, και τις ιστοσελίδες.
- Ύπαρξη σχεδίου επιχειρησιακή συνέχειας μετά από επίθεση.
- Ενημέρωση για νέες μορφές κακόβουλου λογισμικού.

Έλεγχος για κινητό κώδικα

Ο κινητός κώδικας είναι κώδικας λογισμικού που μεταφέρεται από έναν υπολογιστή σε έναν άλλο και στη συνέχεια να εκτελείται αυτόματα και πραγματοποιεί μια συγκεκριμένη λειτουργία με ελάχιστη ή χωρίς αλληλεπίδραση του χρήστη. Ο κινητό κωδικός συνδέεται με μια σειρά από υπηρεσίες ενδιάμεσου λογισμικού.

Όταν η χρήση κινητού κώδικα επιτρέπεται η διαμόρφωση θα πρέπει να διασφαλίζει ότι ο επιτρεπόμενος κινητός κώδικας λειτουργεί σύμφωνα με μια σαφώς καθορισμένη πολιτική

ασφαλείας, και θα πρέπει να εμποδίζεται να εκτελεστεί μη εξουσιοδοτημένος κινητός κώδικας.

Οι ακόλουθες δράσεις θα πρέπει να εξετάζονται για προστασία από κινητό κώδικα που εκτελεί μη εξουσιοδοτημένες ενέργειες:

- Εκτέλεση του κώδικα σε απομονωμένο περιβάλλον.
- Μπλοκάρισμα κάθε χρήσης ή λήψης κινητού κώδικα.
- Κρυπτογραφικό έλεγχο για την αυθεντικοποίηση του κινητού κώδικα.

2.2.9.5 Δημιουργία αντιγράφων ασφαλείας (Back-up)

Στόχος είναι η διατήρηση της ακεραιότητας και διαθεσιμότητας της πληροφορίας. Πρέπει να προβλέπονται επαρκείς εγκαταστάσεις back-up για να εξασφαλιστεί ότι όλες οι βασικές πληροφορίες και το λογισμικό μπορούν να ανακτηθούν μετά από μια καταστροφή ή βλάβη των συστημάτων.

Θέματα που πρέπει να δοθεί βάρος είναι η ακρίβεια και η πληρότητα των αντιγράφων ασφαλείας, ο τρόπος αποθήκευσης τους, η συχνότητα που γίνεται το back-up, η προστασία των αντιγράφων και η κρυπτογράφηση τους αν πρόκειται για πολύ ευαίσθητα δεδομένα.

2.2.9.6 Διαχείριση ασφάλειας δικτύων

Στόχος είναι να εξασφαλιστεί η προστασία των πληροφοριών στα δίκτυα και η προστασία της υποδομής υποστήριξης.

Η ασφαλής διαχείριση των δικτύων, η οποία μπορεί να εκτείνεται πέρα από τα όρια του οργανισμού, απαιτεί προσεκτική εξέταση της ροής δεδομένων, των νομικών επιπτώσεων, της παρακολούθησης και προστασίας.

Έλεγχοι δικτύου

Για ελέγχους δικτύου πρέπει να καθοριστούν ειδικοί έλεγχοι για τη διαφύλαξη της εμπιστευτικότητας και της ακεραιότητας των δεδομένων που διέρχονται μέσω των δημοσίων δικτύων ή μέσω ασύρματων δικτύων, και για την προστασία των συνδεδεμένων συστημάτων και εφαρμογών.

Ασφάλεια υπηρεσιών δικτύου

Θα πρέπει να εντοπίζονται και να περιλαμβάνονται σε κάθε συμφωνία υπηρεσιών δικτύου τα χαρακτηριστικά ασφαλείας, τα επίπεδα υπηρεσιών, και οι απαιτήσεις της διαχείρισης όλων των υπηρεσιών του δικτύου, είτε αυτές οι υπηρεσίες παρέχονται εντός του οργανισμού είτε από εξωτερικούς φορείς.

Τα χαρακτηριστικά ασφαλείας των δικτυακών υπηρεσιών θα μπορούσε να είναι η τεχνολογία που εφαρμόζεται (πχ έλεγχοι αυθεντικοποίησης κρυπτογραφίας κλπ), οι απαιτούμενες τεχνικές παράμετροι, οι διαδικασίες για την περιορισμό πρόσβασης στις υπηρεσίες.

2.2.9.7 Χειρισμός μέσων

Αφαιρούμενα μέσα θεωρούνται οι ταινίες, οι δίσκοι, οι δίσκοι flash, οι αφαιρούμενοι σκληροί δίσκοι, τα CD, τα DVD και τα έντυπα μέσα.

Στόχος είναι η αποφυγή μη εξουσιοδοτημένης αποκάλυψης, τροποποίησης, αφαίρεσης ή καταστροφής των αγαθών. Τα μέσα θα πρέπει να ελέγχονται και να προστατεύονται σωματικά.

Διαχείριση αφαιρούμενων μέσων

Θα πρέπει να υπάρχουν διαδικασίες για τη διαχείριση των αφαιρούμενων μέσων. Οι παρακάτω οδηγίες πρέπει να εξεταστούν για αυτές τις διαδικασίες:

- Το περιεχόμενο των επαναχρησιμοποιήσιμων μέσων που πρόκειται να απομακρυνθούν από τον οργανισμό πρέπει να γίνει μη ανακτήσιμο.
- Τα μέσα πρέπει να αποθηκεύονται σε ασφαλές σημείο.
- Θα πρέπει να καταγράφεται η χρήση αφαιρούμενων μέσων.

Κατάργηση των μέσων

Οι επίσημες διαδικασίες για την ασφαλή κατάργηση των μέσων θα πρέπει να ελαχιστοποιούν τον κίνδυνο διαρροής ευαίσθητων πληροφοριών σε μη εξουσιοδοτημένα άτομα. Οι διαδικασίες για την ασφαλή κατάργηση των μέσων που περιέχουν ευαίσθητες πληροφορίες θα πρέπει να είναι ανάλογες με την ευαισθησία των εν λόγω πληροφοριών.

Διαδικασίες χειρισμού πληροφορίας

Οι διαδικασίες θα πρέπει να σχεδιαστούν για το χειρισμό, επεξεργασία, αποθήκευση και διαβίβαση πληροφοριών σύμφωνα με την ταξινόμηση του μέσου (βλέπε 2.2.6 Διαχείριση αγαθών). Τα ακόλουθα στοιχεία πρέπει να εξεταστούν:

- Χειρισμός και επισήμανση όλων των μέσων στο ενδεικνυόμενο επίπεδο ταξινόμησης.
- Περιορισμούς πρόσβασης και περιορισμό στο διαμοιρασμό της πληροφορίας στο ελάχιστο.
- Αποθήκευση των μέσων σύμφωνα με τις προδιαγραφές.

Ασφάλεια εγγράφων συστήματος

Για την προστασία αυτών των εγγράφων πρέπει να βρίσκονται αποθηκευμένα σε ασφαλές σημείο, να διατηρείται μικρός αριθμός ατόμων που έχουν εξουσιοδότηση πρόσβασης, και σε περίπτωση που κρατιούνται σε ένα δημόσιο δίκτυο θα πρέπει να προστατεύονται και δικτυακά.

2.2.9.8 Ανταλλαγή πληροφοριών

Στόχος είναι να διατηρηθεί η ασφάλεια των πληροφοριών και του λογισμικού που ανταλλάσσονται εντός του οργανισμού και με οποιαδήποτε εξωτερική οντότητα.

Οι ανταλλαγές πληροφοριών και λογισμικού μεταξύ των οργανισμών πρέπει να βασίζονται σε επίσημη πολιτική, η οποία πραγματοποιείται σύμφωνα με τις συμφωνίες ανταλλαγής πληροφοριών, και θα πρέπει να είναι συμβατή με τη σχετική νομοθεσία.

Πολιτικές και διαδικασίες ανταλλαγής πληροφοριών

Οι διαδικασίες και οι έλεγχοι που πρέπει να ακολουθούνται κατά τη χρήση ηλεκτρονικής επικοινωνίας για την ανταλλαγή πληροφοριών θα πρέπει να εξετάζουν τα ακόλουθα στοιχεία:

- Οι διαδικασίες να αποσκοπούν στην προστασία των πληροφοριών που ανταλλάσσονται από υποκλοπή, αντιγραφή, τροποποίηση, κακή δρομολόγηση, και καταστροφή.
- Διαδικασίες προστασίας από κακόβουλο λογισμικό και από αποκάλυψη ευαίσθητων πληροφοριών σε περιπτώσεις συνημμένων σε ηλεκτρονικό ταχυδρομείο.

- Τις ευθύνες οποιουδήποτε χρήστη να μην θέσει σε κίνδυνο την οργάνωση μέσω δυσφήμισης, παρενόχλησης, πλαστοπροσωπίας, διαβιβάζοντας αλυσιδωτές επιστολές κλπ.
- Χρήση τεχνικών κρυπτογράφησης.
- Υπενθύμιση στο προσωπικό για τους κινδύνους τηλεφωνικών συνομιλιών και χρήσης φαξ και αντίστοιχους τρόπους προστασίας.

Η ανταλλαγή πληροφοριών μπορεί να προκύψει μέσω της χρήσης ενός αριθμού διαφορετικών τύπων επικοινωνίας, όπως το ηλεκτρονικό ταχυδρομείο, φωνή, φαξ, και βίντεο ενώ η ανταλλαγή λογισμικού μπορεί να προκύψει μέσα από μια σειρά διαφορετικών μέσων, συμπεριλαμβανομένου και του κατεβάσματος από το διαδίκτυο.

Συμφωνίες ανταλλαγής

Θα πρέπει να δημιουργηθούν συμφωνίες για την ανταλλαγή των πληροφοριών και λογισμικού μεταξύ οργανισμού και εξωτερικών φορέων.

Αυτές οι συμφωνίες πρέπει να προβλέπουν τις ευθύνες διαχείρισης για έλεγχο μετάδοσης και λήψης πληροφοριών, ευθύνες μετά από απώλεια δεδομένων και ευθύνες για την προστασία των δεδομένων, των πνευματικών δικαιωμάτων και συμμόρφωσης άδειας λογισμικού .

Φυσικά μέσα σε διέλευση

Σε περίπτωση μεταφοράς των φυσικών μέσων πρέπει να προσεχθεί ο μεταφορέας που θα χρησιμοποιηθεί αν είναι αξιόπιστος και να συμφωνηθεί από τη διοίκηση η λίστα με τους αξιόπιστους. Άλλες εκκρεμότητες είναι η προστασία κατά τη μεταφορά η ιδιόχειρη αποστολή και παραλαβή και μηχανισμοί σφραγισμένων συσκευασιών για να μπορεί να αποκαλυφθεί αν έγινε παραβίαση κατά τη μεταφορά.

Ηλεκτρονικό ταχυδρομείο

Οι ακόλουθοι όροι πρέπει να εξετάζονται:

- Πρέπει να προστατεύεται από μη εξουσιοδοτημένη πρόσβαση, τροποποίηση και άρνηση υπηρεσία (denial-of-service)
- Να διασφαλίζεται ο χρήστης για τη σωστή προώθηση του μηνύματος.
- Νομικά ζητήματα, π.χ. απαιτήσεις για τις ηλεκτρονικές υπογραφές.
- Τη λήψη έγκρισης πριν από τη χρήση εξωτερικών δημόσιων υπηρεσιών όπως το instant messaging ή κοινή χρήση αρχείων.

Επιχειρησιακά πληροφοριακά συστήματα

Πολιτικές και διαδικασίες θα πρέπει να αναπτυχθούν και να εφαρμοστούν για την προστασία των πληροφοριών που σχετίζονται με τη διασύνδεση των επιχειρησιακών πληροφοριακών συστημάτων.

Θα πρέπει να περιλαμβάνονται γνωστές ευπάθειες πληροφοριών στα συστήματα επικοινωνιών, όπως καταγραφή κλήσεων, μη εμπιστευτικότητα κλήσεων αποθήκευση φαξ, διανομή αλληλογραφίας. Επίσης πολιτικές και έλεγχοι διαμοιρασμού πληροφοριών και απαιτήσεις επαναφοράς των συστημάτων.

2.2.9.9 Υπηρεσίες ηλεκτρονικού εμπορίου

Στόχος των ελέγχων αυτών είναι να εξασφαλιστεί η ασφάλεια των υπηρεσιών ηλεκτρονικού εμπορίου, και η ασφαλή χρήση τους.

Πρέπει να εξεταστούν οι συνέπειες για την ασφάλεια που συνδέονται με τη χρήση υπηρεσιών ηλεκτρονικού εμπορίου, συμπεριλαμβανομένων on-line συναλλαγών, και τις απαιτήσεις για τους ελέγχους. Πρέπει επίσης να εξεταστεί η ακεραιότητα και η διαθεσιμότητα των πληροφοριών που δημοσιεύονται ηλεκτρονικά μέσω διαθέσιμων στο κοινό συστημάτων.

Ηλεκτρονικό εμπόριο

Για υλοποίηση ελέγχων για το ηλεκτρονικό εμπόριο θα πρέπει να περιλαμβάνονται τα ακόλουθα ζητήματα ασφαλείας:

- Το επίπεδο της εμπιστοσύνης που απαιτεί κάθε συμβαλλόμενο μέρος από το άλλο για επαλήθευση ταυτότητας.
- Εξασφάλιση ότι οι εμπορικοί εταίροι ενημερώνονται πλήρως για τις άδειες τους.
- Η εμπιστευτικότητα και ακεραιότητα όλων των συναλλαγών σχετικά με στοιχεία πληρωμής, διεύθυνση παράδοσης, επιβεβαίωση είσπραξης.
- Η επιλογή της πλέον κατάλληλης μορφής τακτοποίησης της πληρωμής για την προστασία έναντι της απάτης.

Θα πρέπει να δοθεί σημασία στην ανθεκτικότητα από επίθεση στον υποδοχέα (host) που χρησιμοποιείται για το ηλεκτρονικό εμπόριο, καθώς και τις επιπτώσεις στην ασφάλεια τις

κάθε διασύνδεσης δικτύου που απαιτούνται για την εφαρμογή των υπηρεσιών ηλεκτρονικού εμπορίου.

Το ηλεκτρονικό εμπόριο είναι ευάλωτο σε μια σειρά από απειλές δικτύου που μπορεί να οδηγήσουν σε παράνομη δραστηριότητα, αμφισβήτηση συμβολαίων, και την αποκάλυψη ή τροποποίηση των πληροφοριών. Το ηλεκτρονικό εμπόριο μπορεί να κάνει χρήση ασφαλών μεθόδων ελέγχου ταυτότητας, π.χ. χρησιμοποιώντας δημόσιο κλειδί κρυπτογράφησης και ψηφιακών υπογραφών ώστε να μειωθούν οι κίνδυνοι. Επίσης, μπορεί να χρησιμοποιηθούν αξιόπιστοι εξωτερικοί φορείς, όπου απαιτούνται τέτοιες υπηρεσίες.

Ηλεκτρονικές συναλλαγές

Οι πληροφορίες που συμμετέχουν σε ηλεκτρονικές συναλλαγές θα πρέπει να προστατεύονται για να αποτρέπεται η μη πλήρης μετάδοση, η λανθασμένη δρομολόγηση, η αλλοίωση του μηνύματος, η μη εξουσιοδοτημένη αποκάλυψη, η μη εξουσιοδοτημένη αντιγραφή ή επανάληψη μηνύματος.

Μερικά πράγματα που πρέπει να εξεταστούν είναι η χρήση ψηφιακών υπογραφών, τα ζητήματα της συναλλαγής όπως η πιστοποίηση των συνθηματικών και η εμπιστευτικότητα, η κρυπτογράφηση της επικοινωνίας, τα πρωτόκολλα που θα χρησιμοποιηθούν, η χρήση αξιόπιστης εξωτερικής αρχής

Η έκταση των ελέγχων που εγκρίθηκαν θα πρέπει να είναι ανάλογη με το επίπεδο του κινδύνου που συνδέεται με κάθε μορφή on-line συναλλαγής. Οι συναλλαγές μπορεί να χρειαστεί να συμμορφωθούν με τους νόμους, κανόνες και κανονισμούς.

Δημοσίως διαθέσιμες πληροφορίες

Η ακεραιότητα των πληροφοριών που διατίθενται στο κοινό σύστημα πρέπει να προστατεύεται για να αποτρέψει μη εξουσιοδοτημένη τροποποίηση.

Λογισμικό, δεδομένα, καθώς και άλλες πληροφορίες που απαιτούν υψηλό επίπεδο ακεραιότητας, που διατίθενται σε ένα κοινό σύστημα, θα πρέπει να προστατεύονται από κατάλληλους μηχανισμούς, π.χ. ψηφιακές υπογραφές. Το δημοσίως προσβάσιμο σύστημα θα πρέπει να εξεταστεί για αδυναμίες και ανεπάρκειες πριν οι πληροφορίες γίνουν διαθέσιμες.

2.2.9.10 Παρακολούθηση

Τα συστήματα πρέπει να παρακολουθούνται και τα περιστατικά ασφάλειας θα πρέπει να καταγράφονται. Τα καταγραφικά αρχεία (logs) χειρισμού και η καταγραφή ελαττωμάτων θα πρέπει να χρησιμοποιηθούν για να εξασφαλιστεί ότι εντοπίζονται προβλήματα του συστήματος πληροφοριών.

Καταγραφή ελέγχου

Αρχεία καταγραφής ελέγχου που αναφέρουν τις δραστηριότητες των χρηστών, τις εξαιρέσεις, και τα περιστατικά ασφάλειας των πληροφοριών θα πρέπει να παράγονται και να διατηρούνται για μια συμφωνημένη περίοδο ώστε να βοηθήσουν σε μελλοντικές έρευνες και την παρακολούθηση του ελέγχου πρόσβασης.

Σε αυτά τα αρχεία πρέπει να αναφέρονται πληροφορίες όπως ταυτότητες χρηστών, χρονικές πληροφορίες των γεγονότων εισόδου/εξόδου στο σύστημα, το τερματικό που χρησιμοποιήθηκε, εγγραφές πετυχημένων και αποτυχημένων προσπαθειών πρόσβασης, αλλαγές στις ρυθμίσεις του συστήματος, χρήση προνομίων, αρχεία που προσπελάστηκαν, δικτυακές διευθύνσεις και πρωτόκολλα και τέλος ειδοποιήσεις συναγερμού που σήκωσε το σύστημα ελέγχου πρόσβασης.

Παρακολούθηση χρήσης συστήματος

Διαδικασίες παρακολούθησης της χρήσης πληροφοριακών συστημάτων πρέπει να καθιερωθούν και τα αποτελέσματα των δραστηριοτήτων παρακολούθησης να αναθεωρούνται τακτικά.

Το επίπεδο της παρακολούθησης που απαιτείται για μεμονωμένες εγκαταστάσεις θα πρέπει να καθορίζεται από την εκτίμηση του κινδύνου. Μερικά στοιχεία που εξετάζονται είναι οι λεπτομέρειες της εξουσιοδοτημένης πρόσβασης, όλες τις προνομιακές λειτουργίες, οι απόπειρες μη εξουσιοδοτημένης πρόσβασης, οι ειδοποιήσεις ή αποτυχίες του συστήματος, οι αλλαγές ή προσπάθειες αλλαγής των ρυθμίσεων ασφαλείας.

Το πόσο συχνά εξετάζονται τα αποτελέσματα των δραστηριοτήτων παρακολούθησης πρέπει να εξαρτάται από τους κινδύνους που εμπλέκονται. Οι παράγοντες κινδύνου που πρέπει να εξεταστούν περιλαμβάνουν:

- Κρισιμότητα των διαδικασιών εφαρμογής.
- Την αξία, ευαισθησία και κρισιμότητα των συγκεκριμένων πληροφοριών.
- Την εμπειρία από διείσδυση στο σύστημα και κατάχρηση στο παρελθόν, και τη συχνότητα των ευπαθειών που έχουν εκμεταλλευτεί.
- Το εύρος της διασύνδεσης του συστήματος.

- Την απενεργοποίηση της εγκατάστασης καταγραφής.

Προστασία της πληροφορίας καταγραφής

Οι εγκαταστάσεις και οι πληροφορίες καταγραφής πρέπει να προστατεύονται από αλλοίωση και μη εξουσιοδοτημένη πρόσβαση. Μερικά από τα προβλήματα που πρέπει να αντιμετωπίσουν οι έλεγχοι είναι αλλαγές στους τύπους μηνυμάτων που καταγράφονται, διαγραφές αρχείων καταγραφής και η υπερκάλυψη της χωρητικότητα αποθήκευσης που έχει σαν αποτέλεσμα αποτυχία εγγραφής ή επικάλυψη παρελθοντικών εγγραφών.

Τα αρχεία καταγραφής συνήθως γράφουν μεγάλο όγκο πληροφοριών και πρέπει με κάποιο τρόπο να αποσπαστούν οι εγγραφές εκείνες που αφορούν σημαντικά περιστατικά.

Αρχεία καταγραφής διαχείρισης και χειρισμού

Οι ενέργειες των διαχειριστών και χειριστών των συστημάτων πρέπει να καταγράφονται επίσης. Πρέπει κι αυτά τα αρχεία να περιλαμβάνουν τη χρονοσφραγίδα μιας πράξης, τους πόρους που προσπελάστηκαν, την ταυτότητα του χειριστή ή διαχειριστή.

Καταγραφή βλαβών

Οι βλάβες θα πρέπει να καταγράφονται, αναλύονται και να λαμβάνονται για αυτές τα κατάλληλα μέτρα.

Η καταγραφή των σφαλμάτων και τα σφαλμάτων μπορεί να επηρεάσουν την απόδοση του συστήματος. Η καταγραφή θα πρέπει να ενεργοποιηθεί από αρμόδιο προσωπικό, και το επίπεδο καταγραφής που απαιτείται για μεμονωμένα συστήματα πρέπει να καθορίζεται από εκτίμηση του κινδύνου, λαμβάνοντας υπόψη την υποβάθμιση των επιδόσεων.

Συγχρονισμός ρολογιού

Τα ρολόγια των συστημάτων επεξεργασίας πληροφοριών που σχετίζονται μεταξύ τους στο εσωτερικό ενός οργανισμού ή ενός τομέα της ασφάλειας θα πρέπει να συγχρονιστούν με συμφωνημένη ακριβή πηγή χρονισμού.

Η ορθή ερμηνεία της μορφής ημερομηνία/ώρα είναι σημαντικό να διασφαλίσει ότι η χρονική σήμανση αντανακλά την πραγματική ημερομηνία/ώρα. Οι τοπικές ιδιαιτερότητες (π.χ. θερινή ώρα) θα πρέπει να ληφθούν υπόψη.

2.2.10 Έλεγχος Πρόσβασης

Στην παράγραφο αυτή υπάρχουν 7 επιμέρους κατηγορίες ασφάλειας.

2.2.10.1 Επιχειρησιακή απαίτηση για έλεγχο πρόσβασης

Η πρόσβαση στις πληροφορίες, στις εγκαταστάσεις επεξεργασίας πληροφοριών, και στις επιχειρηματικές διαδικασίες θα πρέπει να ελέγχεται με βάση την επιχείρηση και τις απαιτήσεις ασφαλείας.

Πολιτική ελέγχου πρόσβασης

Μια πολιτική ελέγχου πρόσβασης θα πρέπει να συσταθεί, να καταγραφεί και να αξιολογηθεί με βάση τις επιχειρησιακές ανάγκες και τις απαιτήσεις ασφαλείας πρόσβασης.

Η πολιτική αυτή πρέπει να λαμβάνει υπόψη τις απαιτήσεις ασφάλειας, τον καθορισμό των πληροφοριών που σχετίζονται με τις επιχειρησιακές εφαρμογές, τη διαχείριση των δικαιωμάτων πρόσβασης, τη σχετική νομοθεσία και άλλα ζητήματα.

Κατά τον προσδιορισμό των κανόνων ελέγχου πρόσβασης πρέπει να εξετάζονται διάφορα θέματα ένα εκ των οποίων είναι οι κανόνες να βασίζονται στην αρχή «Οτιδήποτε είναι απαγορευμένο εκτός αν επιτραπεί ρητά».

2.2.10.2 Επιχειρησιακή απαίτηση για έλεγχο πρόσβασης

Στόχος είναι να εξασφαλιστεί άδεια πρόσβασης για εξουσιοδοτημένο χρήστη και αποτροπή μη εξουσιοδοτημένης πρόσβασης σε συστήματα πληροφοριών.

Οι διαδικασίες θα πρέπει να καλύπτουν όλα τα στάδια του κύκλου ζωής της πρόσβασης των χρηστών, από την πρώτη εγγραφή νέων χρηστών στην τελική διαγραφή χρηστών που δεν θα απαιτούν πλέον πρόσβαση σε συστήματα και υπηρεσίες πληροφοριών

Εγγραφή χρήστη

Πρέπει να υπάρξει μια επίσημη διαδικασία εγγραφής και διαγραφής διαδικασία στη θέση του για τη χορήγηση και την ανάκληση της πρόσβασης σε όλα τα συστήματα και υπηρεσίες πληροφοριών.

Η διαδικασία αυτή περιλαμβάνει μεταξύ άλλων απόδοση μοναδικής ταυτότητας χρήστη, ενημέρωση χρήστη για τα δικαιώματα, περιοδικό έλεγχο για μη έγκυρους χρήστες, έλεγχο ότι τα δικαιώματα χρηστών δεν παραβιάζουν την πολιτική ασφάλειας.

Διαχείριση προνομίων

Η κατανομή και χρήση των προνομίων θα πρέπει να περιορίζεται και να ελέγχεται. Ο χρήστης μπορεί να έχει διαφορετικά δικαιώματα για κάθε πόρο π.χ. για λειτουργικό σύστημα ή βάση δεδομένων.

Διαχείριση κωδικού χρήστη

Η διαδικασία απόδοσης κωδικών πρέπει να περιλαμβάνει μεταξύ άλλων τις απαιτήσεις: εμπιστευτικότητα των κωδικών από τους χρήστες, χρήση προσωρινών κωδικών αρχικά που πρέπει να αλλάξουν οι χρήστες, οι προσωρινοί κωδικοί να είναι δύσκολο να τους μαντέψει κανείς και να μην αποθηκεύονται οι κωδικοί σε υπολογιστές.

Άλλες τεχνολογίες για την αναγνώριση και επαλήθευση ταυτότητας χρήστη όπως είναι τα βιομετρικά στοιχεία π.χ. με έλεγχο δακτυλικών αποτυπωμάτων, η επαλήθευση της υπογραφής, και η χρήση έξυπνων καρτών, είναι διαθέσιμες, και θα πρέπει να εξετάζονται κατά περίπτωση.

Αναθεώρηση δικαιωμάτων πρόσβασης χρηστών

Η διοίκηση θα πρέπει να επανεξετάζει τα δικαιώματα πρόσβασης των χρηστών σε τακτά χρονικά διαστήματα χρησιμοποιώντας μια επίσημη διαδικασία.

Τα δικαιώματα χρηστών πρέπει να επανεξετάζονται μετά από καθορισμένες περιόδους π.χ. κάθε 6 μήνες, αλλά και όταν συμβαίνουν αλλαγές όπως μετά από προαγωγή ή απόλυση.

2.2.10.3 Ευθύνες χρηστών

Οι χρήστες θα πρέπει να συνειδητοποιήσουν τις ευθύνες τους για τη διατήρηση αποτελεσματικών ελέγχων πρόσβασης, ιδίως όσον αφορά τη χρήση των κωδικών πρόσβασης και την ασφάλεια του εξοπλισμού τους.

Χρήση Κωδικών

Οι χρήστες θα πρέπει να προτρέπονται να κρατούν τους κωδικούς τους μυστικούς, να μην τους έχουν γραμμένους σε χαρτί ή στον υπολογιστή ή κινητό, να αλλάζουν κωδικούς, να επιλέγουν ποιοτικούς κωδικούς και να μην χρησιμοποιούν ίδιους κωδικούς για επιχειρησιακού και μη-επιχειρησιακούς σκοπούς.

Μη επιβλεπόμενος εξοπλισμός χρήστη

Οι χρήστες θα πρέπει να διασφαλίζουν ότι ο αφύλακτος εξοπλισμός έχει κατάλληλη προστασία. Κάποιες σωστές πρακτικές είναι να κλείνουνε τα ανοιχτά sessions και να κλειδώνουν τους υπολογιστές τους όταν δεν δουλεύουν σε αυτούς.

Πολιτική καθαρού γραφείου και οθόνης

Αφορά την απομάκρυνση από το γραφείο και σε κοινή θέα εγγράφων που περιέχουν ευαίσθητες πληροφορίες και την προστασία από δυνατότητα παρατήρησης της οθόνης του υπολογιστή από τρίτους καθώς ενδέχεται να φανερώνονται πληροφορίες που πρέπει να παραμείνουν κρυφές. Επίσης το ίδιο ισχύει για αλληλογραφία, φαξ και φωτοτυπικό μηχάνημα όταν περιέχεται κρίσιμη πληροφορία για τον οργανισμό.

2.2.10.4 Έλεγχος πρόσβασης δικτύου

Στόχος είναι να αποτραπεί η μη εξουσιοδοτημένη πρόσβαση σε δικτυακές υπηρεσίες. Θα πρέπει να ελέγχεται η πρόσβαση τόσο στις εσωτερικές όσο και εξωτερικές υπηρεσίες δικτύου.

Πολιτική χρήσης δικτυακών υπηρεσιών

Μια πολιτική θα πρέπει να διατυπωθεί σχετικά με τη χρήση των δικτύων και των υπηρεσιών του δικτύου. Αυτή η πολιτική πρέπει να καλύπτει διαδικασίες αυθεντικοποίησης, προστασίας πρόσβασης στις δικτυακές υπηρεσίες και τα μέσα που χρησιμοποιούνται για πρόσβαση.

Αυθεντικοποίηση χρήστη για εξωτερικές συνδέσεις

Η αυθεντικοποίηση απομακρυσμένων χρηστών μπορεί να επιτευχθεί χρησιμοποιώντας, για παράδειγμα, μια τεχνική κρυπτογραφίας, εξωτερικές συσκευές, ή ένα πρωτόκολλο. Πιθανές εφαρμογές των τεχνικών αυτών μπορούν να βρεθούν σε διάφορες λύσεις

εικονικού ιδιωτικού δικτύου (VPN). Αποκλειστικές ιδιωτικές γραμμές μπορεί επίσης να χρησιμοποιηθούν για να παράσχει τη βεβαιότητα για την πηγή των συνδέσεων.

Αναγνώριση συσκευών σε δίκτυα

Η αναγνώριση συσκευών μπορεί να χρησιμοποιηθεί αν είναι σημαντικό η επικοινωνία να μπορεί να ξεκινήσει μόνο από μια συγκεκριμένη τοποθεσία ή εξοπλισμό. Με χρήση αναγνωριστικού ο εξοπλισμός μπορεί να χρησιμοποιηθεί για να δείξει αν ο εξοπλισμός αυτός επιτρέπεται να συνδεθεί με το δίκτυο.

Απομακρυσμένη διάγνωση και προστασία διαμόρφωσης πόρτας

Η φυσική και λογική πρόσβαση στα διαγνωστικά και στη διαμόρφωση θύρας θα πρέπει να ελέγχονται.

Πολλά συστήματα ηλεκτρονικών υπολογιστών, συστήματα δικτύων, και συστήματα επικοινωνίας είναι εγκατεστημένα με μια απομακρυσμένη διάγνωση ή εγκατάσταση διαμόρφωσης για χρήση από τους μηχανικούς συντήρησης. Αν μείνουν απροστάτευτα, αυτές οι διαγνωστικές θύρες παρέχουν ένα μέσο για μη εξουσιοδοτημένη πρόσβαση.

Διαχωρισμός σε δίκτυα

Μια μέθοδος ελέγχου της ασφάλειας των μεγάλων δικτύων είναι ο χωρισμός τους σε ξεχωριστούς λογικούς τομείς δικτύου, π.χ. τομέας εσωτερικού δικτύου ενός οργανισμού και εξωτερικοί τομείς, όπου κάθε ένας προστατεύεται από καθορισμένη περίμετρο ασφαλείας. Ένα βαθμιαίο σύνολο ελέγχων μπορεί να εφαρμοστεί σε διαφορετικούς λογικούς τομείς δικτύου ώστε να διαχωρίσουν περαιτέρω τα περιβάλλοντα ασφάλειας του δικτύου, π.χ. προσβάσιμα από το κοινό συστήματα, εσωτερικά δίκτυα και κρίσιμα αγαθά. Οι τομείς θα πρέπει να ορίζονται με βάση την αξιολόγηση κινδύνου και τις διαφορετικές απαιτήσεις ασφάλειας σε κάθε τομέα.

Έλεγχος συνδέσεων δικτύου

Η δυνατότητα σύνδεσης των χρηστών μπορεί να περιοριστεί μέσω δικτυακών πυλών που ελέγχουν την κίνηση μέσω προκαθορισμένων πινάκων ή κανόνων. Παραδείγματα εφαρμογών στις οποίες οι περιορισμοί πρέπει να εφαρμόζονται είναι το ηλεκτρονικό ταχυδρομείο, η μεταφορά αρχείων, η πρόσβαση σε εφαρμογή.

Έλεγχος δρομολόγησης δικτύου

Οι έλεγχοι δρομολόγησης πρέπει να βασίζονται σε θετικούς μηχανισμούς ελέγχου διεύθυνσης πηγής και προορισμού. Πύλες ασφαλείας μπορούν να χρησιμοποιηθούν για την επικύρωση διευθύνσεων πηγής και προορισμού στα εσωτερικά και εξωτερικά σημεία

ελέγχου του δικτύου, εφόσον εφαρμόζονται τεχνολογίες μεσολάβησης (proxy) ή/και δικτυακής μετάφρασης διευθύνσεων.

2.2.10.5 Έλεγχος πρόσβασης λειτουργικού συστήματος

Στόχος είναι η αποτροπή μη εξουσιοδοτημένης πρόσβασης στα λειτουργικά συστήματα. Οι διαδικασίες ασφάλειας πρέπει να είναι ικανές να αυθεντικοποιούν εξουσιοδοτημένους χρήστες, να καταγράφουν τη χρήση των προνομίων συστήματος, να προκαλούν συναγερμό όταν υπάρχει παραβίαση, και όταν πρέπει να περιορίζουν το χρόνο σύνδεσης των χρηστών.

Διαδικασίες ασφαλούς εισόδου στο λειτουργικό σύστημα

Μια καλή διαδικασία εισόδου μεταξύ άλλων θα πρέπει:

- Να μην εμφανίζει τα συνθηματικά συστήματος πριν την είσοδο.
- Να επικυρώνει τις πληροφορίες εισόδου μόνο μετά την ολοκλήρωση όλων των δεδομένων εισόδου. Εάν προκύψει κατάσταση σφάλματος, το σύστημα δεν θα πρέπει να αναφέρει ποιο μέρος των δεδομένων είναι σωστές ή λάθος.
- Να χειρίζεται θέματα αποτυχημένων προσπαθειών εισόδου όπως περιορισμό προσπαθειών, π.χ. έως 3 προσπάθειες.
- Να μην εμφανίζει τον κωδικό εισόδου στην οθόνη.

Αυθεντικοποίηση και αναγνώριση χρήστη

Όλοι οι χρήστες πρέπει να έχουν ένα μοναδικό αναγνωριστικό (αναγνωριστικό χρήστη) για προσωπική τους χρήση, και θα πρέπει να επιλεγεί μια κατάλληλη τεχνική πιστοποίησης για την τεκμηρίωση της δηλωθείσας ταυτότητας ενός χρήστη.

Σύστημα διαχείρισης κωδικών

Ένα σύστημα διαχείρισης κωδικών θα πρέπει να επιβάλει τη χρήση μοναδικής ταυτότητας χρήστη και κωδικού, να επιτρέπει και ενίοτε να επιβάλει στους χρήστες να αλλάζουν τον κωδικό τους και να διατηρεί λίστα με προηγούμενους κωδικούς ώστε να μην τους ξαναχρησιμοποιούν οι χρήστες. Επίσης πρέπει να αποθηκεύει τους κωδικούς χωριστά από τα δεδομένα της εφαρμογής και επίσης να τους αποθηκεύει και μεταδίδει σε κρυπτογραφημένη μορφή.

Λήξη συνόδου (session)

Μια εφαρμογή λήξης θα πρέπει να καθαρίζει την οθόνη συνόδου και επίσης, ενδεχομένως αργότερα, να κλείσει τόσο τη σύνοδο εφαρμογής όσο και τη σύνοδο στο δίκτυο μετά από μια ορισμένη περίοδο αδράνειας. Το χρονικό όριο καθυστέρησης θα πρέπει να αντανακλά τους κινδύνους ασφάλειας της περιοχής, τη διαβάθμιση των πληροφοριών που διακινούνται και τις εφαρμογές που χρησιμοποιούνται, καθώς και τους κινδύνους που σχετίζονται με τους χρήστες του εξοπλισμού.

Περιορισμός χρόνου σύνδεσης

Έλεγχοι χρόνου σύνδεσης θα πρέπει να εξετάζονται για ευαίσθητες εφαρμογές, ιδιαίτερα από θέσεις υψηλού κινδύνου, π.χ. δημόσιους ή εξωτερικούς χώρους που βρίσκονται εκτός της διαχείρισης της ασφάλειας του οργανισμού. Παραδείγματα τέτοιων περιορισμών αποτελούν η χρήση προκαθορισμένων χρονοθυρίδων, ο περιορισμός χρόνου σύνδεσης κατά τη διάρκεια ωρών γραφείου μόνο, επαναυθεντικοποίηση σε τακτά χρονικά διαστήματα.

2.2.10.6 Έλεγχος πρόσβασης εφαρμογών και πληροφοριών

Στόχος είναι η αποτροπή μη εξουσιοδοτημένης πρόσβαση σε πληροφορίες που βρίσκονται σε συστήματα εφαρμογής. Εγκαταστάσεις ασφαλείας θα πρέπει να χρησιμοποιηθούν για να περιορίσουν την πρόσβαση σε συστήματα και μέσα εφαρμογής.

Περιορισμός πρόσβασης σε πληροφορίες

Περιορισμοί στην πρόσβαση θα πρέπει να βασίζονται στις ατομικές απαιτήσεις της επιχειρησιακής εφαρμογής. Η πολιτική ελέγχου πρόσβασης θα πρέπει επίσης να είναι συνεπής με την πολιτική πρόσβασης στον οργανισμό.

Απομόνωση ευαίσθητων συστημάτων

Τα ευαίσθητα συστήματα πρέπει να βρίσκονται σε ένα ειδικό (απομονωμένο) υπολογιστικό περιβάλλον. Για υλοποίηση της απομόνωσης αυτής πρέπει αρχικά να καθοριστεί επ’ ακριβώς η ευαισθησία του συστήματος εφαρμογής και αν μια ευαίσθητη εφαρμογή πρόκειται να τρέξει σε διαμοιρασμένο περιβάλλον θα πρέπει να προσδιοριστούν οι κίνδυνοι που σχετίζονται με τα συστήματα που θα μοιραστεί τον ίδιο χώρο και να γίνει αυτό αποδεκτό από τον ιδιοκτήτη της ευαίσθητης εφαρμογής.

2.2.10.7 Χρήση φορητών υπολογιστικών συσκευών και τηλεργασία

Στόχος είναι να εξασφαλιστεί η ασφάλεια των πληροφοριών κατά τη χρήση φορητών υπολογιστών και εγκαταστάσεων τηλεργασία-εργασίας. Η προστασία που απαιτείται πρέπει να είναι ανάλογη με τους κινδύνους που αυτές οι ειδικές μέθοδοι εργασίας προκαλούν.

Φορητές συσκευές και επικοινωνίες

Κατά τη χρήση φορητών υπολογιστών και συσκευών επικοινωνίας, π.χ. φορητούς υπολογιστές, υπολογιστές παλάμης, έξυπνες κάρτες και κινητά τηλέφωνα, ιδιαίτερη προσοχή πρέπει να ληφθεί για να διασφαλιστεί ότι οι πληροφορίες των επιχειρήσεων δεν είναι σε κίνδυνο. Η πολιτική σχετικά με φορητές συσκευές πρέπει να λαμβάνει υπόψη τους κινδύνους της εργασίας με τον κινητό εξοπλισμό πληροφορικής σε απροστάτευτα περιβάλλοντα.

Τηλεργασία

Οι οργανισμοί πρέπει να επιτρέπουν δραστηριότητες τηλεργασίας μόνο εάν έχουν ληφθεί κατάλληλα μέτρα ασφαλείας και έλεγχοι, και ότι αυτές οι δραστηριότητες συμμορφώνονται με την πολιτική ασφάλειας του οργανισμού.

Παρακάτω παρουσιάζονται μερικά ζητήματα που πρέπει να εξεταστούν:

- Οι απαιτήσεις ασφάλειας των επικοινωνιών, λαμβάνοντας υπόψη την ανάγκη για την εξ αποστάσεως πρόσβαση σε εσωτερικά συστήματα του οργανισμού, η ευαισθησία των πληροφοριών που θα έχουν πρόσβαση θα περάσει πάνω από τον ζεύξη επικοινωνίας και η ευαισθησία του εσωτερικού συστήματος.
- Η απειλή της μη εξουσιοδοτημένης πρόσβασης σε πληροφορίες ή πόρους από άλλα άτομα που χρησιμοποιούν το ίδιο κατάλυμα, π.χ. οικογένεια και τους φίλους.
- Η χρήση των οικιακών δικτύων και οι απαιτήσεις ή περιορισμοί σχετικά με τη διαμόρφωση των ασυρμάτων υπηρεσιών δικτύου.
- Οι απαιτήσεις για προστασία από ιούς και τείχους προστασίας.

2.2.11 Απόκτηση, ανάπτυξη, συντήρηση Πληροφοριακών Συστημάτων

Στην παράγραφο αυτή υπάρχουν 6 επιμέρους κατηγορίες ασφάλειας.

2.2.11.1 Απαιτήσεις ασφάλειας πληροφοριακών συστημάτων

Τα συστήματα πληροφοριών περιλαμβάνουν τα λειτουργικά συστήματα, υποδομές, εφαρμογές, υπηρεσίες, και εφαρμογές που αναπτύχθηκαν από το χρήστη. Ο σχεδιασμός και η εφαρμογή του συστήματος πληροφοριών που υποστηρίζει την επιχειρησιακή διαδικασία μπορεί να είναι ζωτικής σημασίας για την ασφάλεια. Απαιτήσεις ασφαλείας θα πρέπει να αναζητούνται και να συμφωνούνται εκ των προτέρων για την ανάπτυξη και την εφαρμογή των συστημάτων πληροφοριών.

Προδιαγραφές και απαιτήσεις ασφάλειας

Ο καθορισμός των επιχειρησιακών απαιτήσεων για νέα πληροφοριακά συστήματα, ή η βελτίωση σε υφιστάμενα συστήματα πρέπει να προσδιορίζει τις απαιτήσεις για ελέγχους ασφαλείας.

Οι έλεγχοι που εισάγονται στο στάδιο του σχεδιασμού είναι σημαντικά φθηνότερο να εφαρμοστούν και να διατηρηθούν από τους ελέγχους που περιλαμβάνονται κατά τη διάρκεια της εφαρμογής ή μετά. Οπότε η φάση του σχεδιασμού είναι πολύ σημαντικό να περιέχει τους απαραίτητους ελέγχους.

2.2.11.2 Σωστός χειρισμός σε εφαρμογές

Στόχος είναι η αποφυγή λαθών, απωλειών, μη εξουσιοδοτημένης τροποποίησης και κακής χρήσης των πληροφοριών σε εφαρμογές. Κατάλληλοι έλεγχοι πρέπει να σχεδιάζονται σε εφαρμογές, περιλαμβάνοντας εφαρμογές που αναπτύχθηκαν από το χρήστη έτσι ώστε να εξασφαλιστεί η σωστή επεξεργασία. Οι έλεγχοι αυτοί θα πρέπει να περιλαμβάνουν την επικύρωση των δεδομένων εισόδου της εσωτερικής επεξεργασίας και των δεδομένων εξόδου.

Επικύρωση δεδομένων εισόδου

Η εισαγωγή των δεδομένων σε εφαρμογές θα πρέπει να επικυρώνεται για να εξασφαλίζεται ότι τα δεδομένα αυτά είναι ορθά και κατάλληλα. Θα πρέπει να εφαρμόζονται έλεγχοι εισόδου σε συναλλαγές, στατικά δεδομένα (π.χ. ονόματα, διευθύνσεις, όρια πιστώσεων), πίνακες παραμέτρων και άλλα.

Μερικά θέματα που πρέπει να εξετάζονται είναι:

- Έλεγχοι διπλής εισόδου και άλλοι, όπως έλεγχος ορίων ή περιορισμοί πεδίων σε συγκεκριμένες περιοχές των δεδομένων εισόδου, για να ανιχνευτούν σφάλματα όπως λάθος χαρακτήρες, υπέρβαση μέγιστου ορίου εισόδου, τιμές εκτός ορίων.
- Διαδικασίες για ανταπόκριση σε σφάλματα εγκυρότητας.
- Καθορισμός των αρμοδιοτήτων του προσωπικού που εμπλέκεται στη διαδικασία εισαγωγής δεδομένων.

Έλεγχος εσωτερικής επεξεργασίας

Έλεγχοι επαλήθευσης πρέπει να ενσωματωθούν σε εφαρμογές με σκοπό τον εντοπισμό αλλοίωσης των πληροφοριών μέσω των σφαλμάτων επεξεργασίας ή εσκεμμένων πράξεων. Σκοπός τους είναι να μειωθούν οι κίνδυνοι από αυτά τα σφάλματα επεξεργασίας.

Πρέπει να ελέγχεται η χρήση λειτουργιών προσθήκης, επεξεργασίας και διαγραφής για τα δεδομένα. Επίσης να προβλεφθούν διαδικασίες αποτροπής παράκαμψης της ορθής σειράς εκτέλεσης προγραμμάτων και να υλοποιηθούν μέθοδοι επαναφοράς των συστημάτων έπειτα από σφάλμα ώστε να προστατευτούν οι πληροφορίες. Τέλος πρέπει να εξεταστεί προστασία από επιθέσεις υπερχείλισης buffer (buffer overflow).

Ακεραιότητα μηνυμάτων

Θα πρέπει να προσδιοριστούν οι απαιτήσεις για την εξασφάλιση της αυθεντικότητας και την προστασία της ακεραιότητας μηνυμάτων σε εφαρμογές, και να υλοποιούνται κατάλληλοι έλεγχοι. Ένα μέσο υλοποίηση της αυθεντικοποίησης είναι οι τεχνικές κρυπτογραφίας.

Επικύρωση δεδομένων εξόδου

Τα δεδομένα εξόδου από την εφαρμογή πρέπει να επικυρώνονται για να εξασφαλίζεται ότι η επεξεργασία των αποθηκευμένων πληροφοριών είναι σωστή και κατάλληλη για τις περιστάσεις.

Η επικύρωση των δεδομένων εξόδου περιλαμβάνει λογικούς ελέγχους των δεδομένων αυτών και παροχή επαρκών πληροφοριών για το επόμενο σύστημα επεξεργασίας για να καθορίσει την ακρίβεια, πληρότητα και τη διαβάθμιση των πληροφοριών.

2.2.11.3 Έλεγχοι κρυπτογράφησης

Μια πολιτική πρέπει να αναπτυχθεί σχετικά με τη χρήση των κρυπτογραφικών ελέγχων. Πρέπει να υπάρχει μια μέθοδος διαχείρισης κλειδιών για να υποστηρίξει τη χρήση των κρυπτογραφικών τεχνικών.

Πολιτική χρήσης ελέγχων κρυπτογραφίας

Κατά την ανάπτυξη μιας πολιτικής κρυπτογραφίας πρέπει να εξεταστούν:

- Πρέπει να εντοπίζεται το απαιτούμενο επίπεδο προστασίας λαμβάνοντας υπόψη τον τύπο, τη δύναμη και την ποιότητα του απαιτούμενου αλγόριθμου κρυπτογράφησης.
- Τη χρήση κρυπτογράφησης για την προστασία των ευαίσθητων πληροφοριών που μεταφέρονται από κινητό τηλέφωνο ή από φορητές συσκευές πολυμέσων, ή πάνω από γραμμές επικοινωνίας.
- Ο χειρισμός καταστάσεων απώλειας, διακύβευσης ή καταστροφής κλειδιών.

Οι στόχοι της κρυπτογραφίας είναι η εμπιστευτικότητα των πληροφοριών, η ακεραιότητα και η μη-αποποίηση δράσεων ή συμβάντων.

Διαχείριση κλειδιών

Όλα τα κλειδιά κρυπτογραφίας πρέπει να προστατεύονται από τροποποίηση, απώλεια και καταστροφή. Επιπλέον, μυστικά και ιδιωτικά κλειδιά πρέπει να προφυλάσσονται από ανεπίτρεπτη αποκάλυψη. Ο εξοπλισμός που χρησιμοποιείται για την παραγωγή, αποθήκευση και αρχειοθέτηση κλειδιών πρέπει να προστατεύεται φυσικά.

Ένα σύστημα διαχείρισης κλειδιών δημιουργεί κλειδιά για διάφορα συστήματα και εφαρμογές, δημιουργεί και διατηρεί πιστοποιητικά δημοσίου κλειδιού, τροποποιεί κλειδιά, τα διανέμει στους κατάλληλους χρήστες και όταν πρέπει τα ανακαλεί σε περιπτώσεις απώλειας.

Η αυθεντικότητα των δημόσιων κλειδιών θα πρέπει επίσης να εξεταστεί. Η διαδικασία πιστοποίησης μπορεί να γίνει χρησιμοποιώντας πιστοποιητικά δημοσίου κλειδιού που εκδίδονται κανονικά από μια αρχή πιστοποίησης, η οποία θα πρέπει να είναι ένας αναγνωρισμένος οργανισμός με κατάλληλους ελέγχους και διαδικασίες ώστε να παρέχεται ο απαιτούμενος βαθμός εμπιστοσύνης.

Οι δύο τύποι τεχνικών κρυπτογραφίας είναι οι τεχνικές μυστικού κλειδιού όπου τα δύο μέρη μοιράζονται ένα κοινό κλειδί, και οι τεχνικές δημοσίου κλειδιού όπου κάθε χρήστης έχει ένα ζεύγος κλειδιών ένα δημόσιο (που μπορεί να αποκαλυφθεί σε όλους) και ένα ιδιωτικό (που πρέπει να παραμένει κρυφό).

2.2.11.4 Ασφάλεια αρχείων συστήματος

Η πρόσβαση στα αρχεία συστήματος και τον πηγαίο κώδικα του προγράμματος θα πρέπει να ελέγχονται, ώστε τα έργα Πληροφορικής και οι δραστηριότητες υποστήριξης να πραγματοποιούνται με ασφαλή τρόπο. Πρέπει να ληφθεί μέριμνα για την αποφυγή της έκθεσης των ευαίσθητων δεδομένων σε δοκιμαστικό περιβάλλον.

Έλεγχος λογισμικού λειτουργίας

Για να ελαχιστοποιηθεί ο κίνδυνος της αλλοίωσης στα επιχειρησιακά συστήματα, οι ακόλουθες κατευθυντήριες γραμμές θα πρέπει να εξετάζονται:

- Η αναβαθμίσεις των λειτουργικών συστημάτων, εφαρμογών και αποθηκών προγραμμάτων πρέπει να διενεργούνται από εκπαιδευμένους διαχειριστές κατόπιν εξουσιοδότησης.
- Στα λειτουργικά συστήματα πρέπει να βρίσκεται μόνο εκτελέσιμος κώδικας και όχι κώδικας ανάπτυξης ή μεταγλωττιστές.
- Οι εφαρμογές και το λογισμικό του λειτουργικού συστήματος θα πρέπει να εφαρμοστούν μόνο μετά από εκτεταμένες δοκιμές οι οποίες πρέπει να περιλαμβάνουν δοκιμές σε χρηστικότητα, ασφάλεια, επιπτώσεις σε άλλα συστήματα και φιλικότητα προς το χρήστη.
- Να προβλεφθεί στρατηγική επαναφοράς πριν την υλοποίηση αλλαγών, και να κρατιέται αποθηκευμένη η προηγούμενη έκδοση της εφαρμογής.

Υπάρχουν επίσης ζητήματα αναβάθμισης συστημάτων, και εφαρμογών ανάλογα με τις απαιτήσεις και συμβουλές των προμηθευτών τα οποία επηρεάζουν και την ασφάλεια. Σε γενικές γραμμές αναβαθμίσεις θα πρέπει να γίνονται μόνο όταν οι τρέχουσες εκδόσεις δεν καλύπτουν τις επιχειρησιακές απαιτήσεις.

Προστασία από δοκιμαστικά δεδομένα συστημάτων

Θα πρέπει να αποφεύγεται η χρήση των επιχειρησιακών βάσεων δεδομένων που περιέχουν προσωπικά δεδομένα ή οποιαδήποτε άλλη ευαίσθητη πληροφορία για δοκιμαστικούς σκοπούς. Εάν οι προσωπικές ή ευαίσθητες πληροφορίες χρησιμοποιούνται για τους δοκιμαστικούς σκοπούς, όλα τα ευαίσθητα στοιχεία και το περιεχόμενο θα πρέπει να αποσυρθούν ή να τροποποιηθούν πριν από τη χρήση ώστε να μην αναγνωρίζονται.

Έλεγχος πρόσβασης στον πηγαίο κώδικα

Η πρόσβαση στον πηγαίο κώδικα προγραμμάτων και των σχετικών ειδών (όπως προδιαγραφές, σχέδια, και σχέδια επαλήθευσης και επικύρωσης) θα πρέπει να ελέγχεται αυστηρά, προκειμένου να εμποδίζεται η εισαγωγή μη εγκεκριμένης λειτουργικότητας και για να αποφευχθεί η ακούσια αλλαγή. Για τον πηγαίο κώδικα του προγράμματος, αυτό μπορεί να επιτευχθεί με ελεγχόμενη κεντρική αποθήκευση του, κατά προτίμηση στις βιβλιοθήκες πηγής του προγράμματος.

Κάποιες οδηγίες είναι να μην δίνεται απεριόριστη πρόσβαση στο προσωπικό υποστήριξης, η ενημερώσει του κώδικα να γίνεται κατόπιν σχετικής εξουσιοδότησης, καταγραφή ελέγχου θα πρέπει να διατηρείται για κάθε πρόσβαση στον κώδικα.

2.2.11.5 Ασφάλεια στη διαδικασία ανάπτυξης και υποστήριξης

Στόχος είναι να διατηρηθεί η ασφάλεια του λογισμικού της εφαρμογής και των πληροφοριών. Τα έργα και τα περιβάλλοντα υποστήριξης θα πρέπει να ελέγχονται αυστηρά.

Τα στελέχη που είναι υπεύθυνα για τα συστήματα εφαρμογής θα πρέπει επίσης να είναι υπεύθυνα και για την ασφάλεια του έργου ή του περιβάλλοντος υποστήριξης. Θα πρέπει να διασφαλίζουν ότι όλες οι προτεινόμενες αλλαγές συστήματος επιθεωρούνται για να ελεγχθεί ότι δεν θέτουν σε κίνδυνο είτε το σύστημα ή το λειτουργικό περιβάλλον.

Διαδικασίες αλλαγής ελέγχου

Αυτή η διαδικασία πρέπει να περιλαμβάνει μια αξιολόγηση των κινδύνων, ανάλυση των επιπτώσεων των αλλαγών, και τις προδιαγραφές των ελέγχων ασφαλείας που απαιτούνται. Η διαδικασία αυτή θα πρέπει επίσης να εξασφαλίσει ότι η υπάρχουσα ασφάλεια και οι διαδικασίες ελέγχου δεν είναι σε κίνδυνο, ότι στους προγραμματιστές υποστήριξης παρέχεται πρόσβαση μόνο σε εκείνα τα τμήματα του συστήματος που είναι

αναγκαία για το έργο τους, και ότι επιτυγχάνεται η επίσημη συμφωνία και έγκριση για οποιαδήποτε μεταβολή.

Τεχνική αναθεώρηση εφαρμογών μετά από αλλαγές στα συστήματα

Όταν αλλάζουν συστήματα λειτουργίας, σημαντικές επιχειρησιακές εφαρμογές θα πρέπει να επανεξεταστούν και να ελεγχθούν για να εξασφαλιστεί ότι δεν υπάρχει καμία αρνητική επίπτωση στις οργανωτικές λειτουργίες ή την ασφάλεια.

Περιορισμοί σχετικά με τις αλλαγές στα πακέτα λογισμικού

Οι τροποποιήσεις σε πακέτα λογισμικού θα πρέπει να αποθαρρύνονται, να περιορίζονται στις αναγκαίες αλλαγές, και όλες οι αλλαγές πρέπει να ελέγχονται αυστηρά. Όλες οι αλλαγές θα πρέπει να ελεγχθούν πλήρως και να καταγράφονται σε έγγραφα, ώστε να μπορούν να επαναλαμβάνονται εάν είναι απαραίτητο για μελλοντική αναβάθμιση του λογισμικού

Διαρροή πληροφοριών

Πρέπει να αποτρέπονται ευκαιρίες διαρροής πληροφοριών και πρέπει να εξετάζονται τα παρακάτω για τη μείωση του κινδύνου:

- Σάρωση των εξερχόμενων μέσων για κρυφές πληροφορίες.
- Συγκάλυψης και διαμόρφωση του συστήματος επικοινωνιών για να μειωθεί η πιθανότητα ένας εξωτερικός φορέας να είναι σε θέση να συναγάγει πληροφορίες από μια τέτοια συμπεριφορά.
- Χρήση αξιόπιστων προϊόντων με υψηλή ακεραιότητα.
- Παρακολούθηση δραστηριοτήτων προσωπικού και συστημάτων και παρακολούθηση χρήση πόρων σε υπολογιστικά συστήματα.

Ανάθεση ανάπτυξης λογισμικού σε εξωτερικούς συνεργάτες

Όταν η ανάθεση ανάπτυξης λογισμικού γίνεται σε εξωτερικούς συνεργάτες πρέπει να εξετάζονται οι συμφωνίες παραχώρησης αδειών εκμετάλλευσης (licensing), η ιδιοκτησία κώδικα, τα δικαιώματα πνευματικής ιδιοκτησίας, η ύπαρξη πιστοποιητικού ποιότητας, οι δοκιμές πριν την εγκατάσταση για την ανίχνευση κακόβουλου κώδικα.

2.2.11.6 Τεχνική διαχείριση ευπαθειών

Θα πρέπει να εφαρμοστεί μια αποτελεσματική, συστηματική, επαναλαμβανόμενη τεχνική διαχείριση ευπαθειών. Οι εκτιμήσεις αυτές πρέπει να περιλαμβάνουν τα λειτουργικά συστήματα, και κάθε άλλη εφαρμογή που χρησιμοποιείται.

Έλεγχος τεχνικών ευπαθειών

Πρέπει να λαμβάνεται έγκαιρη ενημέρωση σχετικά με τις τεχνικές αδυναμίες των πληροφοριακών συστημάτων που χρησιμοποιούνται, να αξιολογείται η έκθεση του οργανισμού σε αυτές τις ευπάθειες, και να λαμβάνονται τα κατάλληλα μέτρα για την αντιμετώπιση των σχετικών κινδύνων.

Η σωστή λειτουργία της διαδικασίας τεχνικής διαχείρισης ευπαθειών ενός οργανισμού είναι ζωτικής σημασίας και επομένως πρέπει να παρακολουθείται τακτικά. Μια ακριβής απογραφή είναι σημαντικό να εξασφαλίσει ότι εντοπίζονται οι σχετικές τεχνικές αδυναμίες.

Η τεχνική διαχείρισης ευπάθειας μπορεί να θεωρηθεί ως μια υπο-λειτουργία της διαχείρισης της αλλαγής και ως εκ τούτου μπορούν να επωφεληθούν από τις διαδικασίες διαχείρισης της αλλαγής.

2.2.12 Διαχείριση περιστατικών ασφάλειας πληροφοριών

Στην παράγραφο αυτή υπάρχουν 2 επιμέρους κατηγορίες ασφάλειας.

2.2.12.1 Αναφορά περιστατικών ασφάλειας και αδυναμιών

Στόχος είναι να εξασφαλιστεί ότι τα περιστατικά ασφάλειας πληροφοριών και οι αδυναμίες που σχετίζονται με τα πληροφοριακά συστήματα επικοινωνούνται με τέτοιο τρόπον ώστε να λαμβάνονται έγκαιρα οι διορθωτικές ενέργειες.

Αναφορά περιστατικών ασφάλεια πληροφοριών

Μαζί με την ανταπόκριση περιστατικών και τη διαδικασία κλιμάκωσης σε ανώτερη ιεραρχία θα πρέπει να καθιερωθεί και μια διαδικασία αναφοράς περιστατικών, που καθορίζει τη δράση που πρέπει να ληφθεί για την παραλαβή της έκθεσης ενός περιστατικού ασφάλειας πληροφοριών.

Όλοι οι εργαζόμενοι, εργολάβοι και χρήστες εξωτερικών φορέων θα πρέπει να έχουν επίγνωση της ευθύνης τους να αναφέρουν τυχόν συμβάντα ασφάλειας πληροφοριών όσο το δυνατόν γρηγορότερα, και επίσης να γνωρίζουν τη διαδικασία για την αναφορά περιστατικών ασφάλειας και το σημείο επαφής.

Με τη δέουσα προσοχή τις πτυχές της εμπιστευτικότητας, τα περιστατικά ασφάλειας μπορούν να χρησιμοποιηθούν στην εκπαίδευση των χρηστών ως παραδείγματα του τι μπορεί να συμβεί, πώς να ανταποκρίνονται σε τέτοια περιστατικά, και πώς να αποφεύγονται στο μέλλον. Για να είναι σε θέση να αντιμετωπίσει τα περιστατικά ασφάλειας πληροφοριών κατάλληλα μπορεί να είναι αναγκαία η συλλογή αποδεικτικών στοιχείων, το συντομότερο δυνατό μετά το συμβάν.

Αναφορά αδυναμιών ασφάλειας

Όλοι οι εμπλεκόμενοι θα πρέπει να αναφέρουν αυτά τα θέματα, είτε για στη διοίκηση ή απ 'ευθείας στο φορέα παροχής υπηρεσιών τους όσο το δυνατόν γρηγορότερα, προκειμένου να αποφευχθούν συμβάντα στην ασφάλεια πληροφοριών. Ο μηχανισμός υποβολής εκθέσεων θα πρέπει να είναι όσο πιο εύκολος και προσιτός γίνεται. Θα πρέπει να ενημερώνονται ότι δεν πρέπει, σε καμία περίπτωση, προσπαθούν να αποδείξουν μια πιθανή αδυναμία.

2.2.12.2 Διαχείριση περιστατικών και βελτιώσεις

Αρμοδιότητες και διαδικασίες πρέπει να είναι σε θέση να χειριστούν τα περιστατικά ασφάλειας πληροφοριών και τις αδυναμίες αποτελεσματικά από τη στιγμή που έχουν αναφερθεί. Μια διαδικασία συνεχούς βελτίωσης πρέπει να εφαρμόζεται ως αντιμετώπιση της παρακολούθησης, αξιολόγησης και συνολικής διαχείρισης των περιστατικών ασφάλειας.

Αρμοδιότητες και διαδικασίες

Αρμοδιότητες διαχείρισης και διαδικασίες θα πρέπει να θεσπιστούν για να διασφαλιστεί μια γρήγορη, αποτελεσματική και ομαλή απόκριση σε περιστατικά ασφάλειας πληροφοριών.

Τα συμβάντα στην ασφάλεια πληροφοριών μπορούν να υπερβούν τα όρια του οργανισμού αλλά και τα εθνικά σύνορα. Για ανταπόκριση σε τέτοια περιστατικά υπάρχει

μια αυξανόμενη ανάγκη για συντονισμένη απάντηση και διαμοιρασμό πληροφοριών με εξωτερικούς οργανισμούς.

Μάθηση από περιστατικά ασφάλειας

Οι πληροφορίες που αποκτήθηκαν από την αξιολόγηση των περιστατικών ασφάλειας των πληροφοριών θα πρέπει να χρησιμοποιούνται για τον εντοπισμό επαναλαμβανόμενων περιστατικών υψηλής επίπτωσης. Η αξιολόγηση των συμβάντων μπορεί να καταδεικνύει την ανάγκη για ενίσχυση ή συμπληρωματικούς ελέγχους για να ελαχιστοποιήσουν τη συχνότητα, τη ζημιά και το κόστος μελλοντικών εμφανίσεων του κινδύνου.

Συλλογή αποδεικτικών στοιχείων

Όταν μια δράση παρακολούθησης εναντίον ενός ατόμου ή οργανισμού μετά από ένα περιστατικό ασφάλειας πληροφοριών περιλαμβάνει νομική δράση (είτε αστική ή ποινική) πρέπει να συλλέγονται, διατηρούνται και παρουσιάζονται αποδεικτικά στοιχεία ώστε οι οργανισμοί να συμμορφώνονται με τους σχετικούς κανόνες.

2.2.13 Διαχείριση επιχειρησιακής συνέχειας

Στόχος είναι η αντιστάθμιση της διακοπής επιχειρησιακών δραστηριοτήτων και η προστασία των κρίσιμων επιχειρησιακών διαδικασιών από τις επιπτώσεις σημαντικών σφαλμάτων ή καταστροφών των πληροφοριακών συστημάτων και η εξασφάλιση την έγκαιρη επαναφοράς τους.

Μια διαδικασία διαχείρισης επιχειρησιακής συνέχειας θα πρέπει να εφαρμοστεί για την ελαχιστοποίηση των επιπτώσεων στον οργανισμό και την ανάκτηση από την απώλεια πληροφοριακών αγαθών (η οποία μπορεί να είναι αποτέλεσμα φυσικών καταστροφών, ατυχημάτων, αστοχιών εξοπλισμού και σκόπιμων ενεργειών) σε ένα αποδεκτό επίπεδο μέσω ενός συνδυασμού αποτρεπτικών ελέγχων και ελέγχων επαναφοράς.

Εισαγωγή ασφάλειας στη διαδικασία διαχείρισης επιχειρησιακής συνέχειας.

Η διαδικασία πρέπει να καλύψει τα ακόλουθα κρίσιμα στοιχεία της διαχείρισης επιχειρησιακής συνέχειας:

- Κατανόηση των κινδύνων που αντιμετωπίζει ο οργανισμός ως προς την πιθανότητα και τις επιπτώσεις στο χρόνο.

- Ταυτοποίηση των αγαθών που εμπλέκονται σε κρίσιμες επιχειρησιακές διαδικασίες.
- Ενδεχόμενη αγορά κατάλληλης ασφάλισης.
- Προσδιορισμό επαρκών οικονομικών, οργανωτικών, τεχνικών και περιβαλλοντικών πόρων για την αντιμετώπιση των προσδιορισμένων απαιτήσεων ασφάλειας των πληροφοριών.
- Τακτικό έλεγχο και ενημέρωση των διαδικασιών που εφαρμόζονται.

Επιχειρησιακή συνέχεια και αξιολόγηση κινδύνου

Οι αξιολογήσεις κινδύνου επιχειρησιακής συνέχειας θα πρέπει να πραγματοποιούνται με πλήρη συμμετοχή από τους ιδιοκτήτες των πόρων και των διαδικασιών των επιχειρήσεων. Η αξιολόγηση αυτή θα πρέπει να εξετάσει όλες τις επιχειρησιακές διαδικασίες και δεν πρέπει να περιορίζεται στις πληροφοριακές εγκαταστάσεις, αλλά θα πρέπει να περιλαμβάνουν τα αποτελέσματα ειδικά για την ασφάλεια των πληροφοριών.

Κάθε εκτίμηση πρέπει να προσδιορίζει, ποσοτικοποιεί, και να ιεραρχεί τους κινδύνους ως προς τα κριτήρια και τους στόχους που σχετίζονται με τον οργανισμό, στον οποίο περιλαμβάνονται οι κρίσιμοι πόροι, οι επιπτώσεις των διακοπών λειτουργίας, οι επιτρεπόμενοι χρόνοι διακοπής, και οι προτεραιότητες ανάκτησης συστημάτων και υπηρεσιών.

Αναπτύσσοντας σχέδια συνέχειας περιλαμβάνοντας ασφάλεια πληροφοριών

Η διαδικασία σχεδιασμού επιχειρησιακής συνέχειας θα πρέπει να εξετάσει την αναγνώριση των ευθυνών, την αναγνώριση της αποδεκτής απώλειας πληροφορίας, την υλοποίηση μηχανισμών που επιτρέπουν επαναφορά των συστημάτων και υπηρεσιών, την καταγραφή της συμφωνημένης διαδικασίας, την κατάλληλη ενημέρωση του προσωπικού και τη δοκιμή και ενημέρωση των διαδικασιών αυτών.

Πλαίσιο σχεδιασμού επιχειρησιακής συνέχειας

Ένα ενιαίο πλαίσιο των σχεδίων επιχειρησιακής συνέχειας θα πρέπει να διατηρηθεί ώστε να διασφαλιστεί ότι όλα τα σχέδια είναι συνεπή, να αντιμετωπιστούν με συνέπεια οι απαιτήσεις ασφάλειας και να προσδιοριστούν οι προτεραιότητες για δοκιμές και συντήρηση.

Τα ακόλουθα θα πρέπει να εξετασθούν:

- Οι συνθήκες που ενεργοποιούν το σχέδιο επιχειρησιακής συνέχειας.
- Διαδικασίες έκτακτης ανάγκης.
- Διαδικασίες επαναφοράς ή υποστήριξης υπηρεσίας σε εναλλακτικές τοποθεσίες για να επιστρέψει η επιχειρησιακή διαδικασία σε λειτουργία.
- Ευαισθητοποίηση, εκπαίδευση και δραστηριότητες κατάρτισης που έχουν σχεδιαστεί για να δημιουργήσουν κατανόηση των διαδικασιών επιχειρησιακής συνέχειας και να διασφαλίσουν ότι οι διαδικασίες εξακολουθούν να είναι αποτελεσματική.
- Τα αγαθά ζωτικής σημασίας και οι πόροι που απαιτούνται για να είναι σε θέση να εκτελούνται οι διαδικασίες έκτακτης ανάγκης.

Δοκιμή, συντήρηση και επαναξιολόγηση σχεδίων επιχειρησιακής συνέχειας

Μια ποικιλία από τεχνικές θα πρέπει να χρησιμοποιούνται προκειμένου να παρέχουν τη βεβαιότητα ότι το σχέδιο θα λειτουργήσει σε πραγματικά συστήματα. Οι τεχνικές θα πρέπει να περιλαμβάνουν:

- Δοκιμές διάφορων σεναρίων και προσομοιώσεις.
- Τεχνικές δοκιμές επαναφοράς συστημάτων που να εξασφαλίζουν ότι οι πληροφορίες μπορούν να αποκατασταθούν αποτελεσματικά, και επαναφοράς σε απομακρυσμένο σημείο.
- Δοκιμές εγκαταστάσεων και εξοπλισμού και πλήρεις πρόβες.

Περιπτώσεις που χρειάζεται επαναξιολόγηση των σχεδίων επιχειρησιακής συνέχεια είναι η απόκτηση νέου εξοπλισμού, η αναβάθμιση συστημάτων και οι αλλαγές σε προσωπικό, σε διευθύνσεις ή τηλέφωνα, σε στρατηγικούς στόχους, στην τοποθεσία του οργανισμού , σε νομοθεσία, σε συνεργάτες ή πελάτες και τέλος σε αξιολογημένους κινδύνους.

2.2.14 Συμμόρφωση

Στην παράγραφο αυτή υπάρχουν 3 επιμέρους κατηγορίες ασφάλειας.

2.2.14.1 Συμμόρφωση με νομικές απαιτήσεις

Ο σχεδιασμός, η λειτουργία, η χρήση και η διαχείριση των πληροφοριακών συστημάτων μπορεί να υπόκειται σε νομικές, κανονιστικές και συμβατικές απαιτήσεις ασφαλείας.

Πληροφορίες για ειδικές νομικές απαιτήσεις θα πρέπει να αναζητηθούν από τους νομικούς συμβούλους του οργανισμού. Οι νομικές απαιτήσεις ποικίλλουν από χώρα σε χώρα και μπορεί να διαφέρουν για πληροφορίες που δημιουργούνται σε μια χώρα και μεταδίδεται σε άλλη.

Προσδιορισμός της εφαρμοστέας νομοθεσίας

Θα πρέπει να καθορίζονται και να τεκμηριώνονται οι ειδικοί έλεγχοι και οι επιμέρους αρμοδιότητες ώστε να ανταποκρίνονται στις νομικές απαιτήσεις.

Τα δικαιώματα πνευματικής ιδιοκτησίας

Μερικές από τις ακόλουθες οδηγίες θα πρέπει να ακολουθούνται για την προστασία κάθε υλικού που μπορεί να θεωρηθεί πνευματική ιδιοκτησία:

- Απόκτηση λογισμικού μόνο από αξιόπιστες πηγές.
- Διατήρηση αποδεικτικών στοιχείων ιδιοκτησίας αδειών.
- Υλοποίηση ελέγχων για χρήση αυθεντικού λογισμικού.

Τα ιδιόκτητα προϊόντα λογισμικού παρέχονται συνήθως βάσει συμφωνίας χρήσης αδειών που καθορίζει τους όρους και τις προϋποθέσεις άδειας, για παράδειγμα, περιορίζοντας τη χρήση των προϊόντων σε συγκεκριμένα μηχανήματα.

Προστασία των εγγράφων του οργανισμού

Η νομική συμμόρφωση περιλαμβάνει επίσης την υποχρέωση προστασίας των σημαντικών εγγράφων από απώλεια, καταστροφή και πλαστοποίηση.

Τα έγγραφα πρέπει να διαχωρίζονται σε διάφορους τύπους όπως λογιστικά έγγραφα, έγγραφα βάσεων δεδομένων, καταγραφές συναλλαγών και ελέγχων και λειτουργικές διαδικασίες. Σε περίπτωση κρυπτογράφησης των εγγράφων πρέπει να αποθηκεύεται και το σχετικό υλικό κρυπτογράφησης.

Προστασία δεδομένων και προσωπικών πληροφοριών

Η συμμόρφωση με την πολιτική προστασίας προσωπικών δεδομένων και όλη τη σχετική νομοθεσία απαιτεί κατάλληλη δομή διαχείρισης και ελέγχου. Συχνά αυτό επιτυγχάνεται καλύτερα με το διορισμό ενός υπευθύνου προστασίας δεδομένων ο οποίος θα πρέπει να παρέχει καθοδήγηση στους χρήστες και στους παρόχους υπηρεσιών σχετικά με τις ατομικές ευθύνες τους και τις συγκεκριμένες διαδικασίες που πρέπει να ακολουθούνται.

Πρόληψη εναντίον της κακής χρήσης των πληροφοριακών συστημάτων

Οποιαδήποτε χρήση των πληροφοριακών συστημάτων για μη επιχειρησιακούς σκοπούς χωρίς την έγκριση της διοίκησης πρέπει να θεωρηθεί ως καταχρηστική χρήση των εγκαταστάσεων

Κανονισμοί ελέγχων κρυπτογραφίας

Οι έλεγχοι κρυπτογραφίας θα πρέπει να χρησιμοποιούνται σύμφωνα με όλες τις σχετικές συμφωνίες, νόμους και κανονισμούς. Νομικές συμβουλές θα πρέπει να επιδιωχθούν για να εξασφαλιστεί η συμμόρφωση με τους εθνικούς νόμους και κανονισμούς.

2.2.14.2 Συμμόρφωση με νομικές απαιτήσεις και πρότυπα και τεχνική συμμόρφωση

Στόχος είναι να εξασφαλιστεί η συμμόρφωση των συστημάτων με τις πολιτικές του οργανισμού και τα πρότυπα ασφαλείας. Η ασφάλεια των συστημάτων πληροφοριών θα πρέπει να επανεξετάζεται τακτικά.

Συμμόρφωση με πολιτικές και πρότυπα

Οι διευθυντές θα πρέπει να διασφαλίζουν ότι όλες οι διαδικασίες ασφαλείας εντός της περιοχής ευθύνης τους πραγματοποιείται σωστά για να επιτευχθεί συμμόρφωση με τις πολιτικές και τα πρότυπα ασφαλείας.

Αν παρατηρηθεί μη συμμόρφωση, οι προϊστάμενοι οφείλουν να καθορίσουν τα αίτια της μη συμμόρφωσης, να καθορίσουν τις κατάλληλες διορθωτικές ενέργειες και στο τέλος να ελέγξουν αν έγιναν οι διορθώσεις.

Έλεγχος τεχνικής συμμόρφωσης

Ο έλεγχος της τεχνικής συμμόρφωσης θα πρέπει να γίνεται είτε χειροκίνητα από έναν έμπειρο μηχανικό συστήματος, ή/και με τη βοήθεια αυτοματοποιημένων εργαλείων, τα οποία δημιουργούν μια τεχνική έκθεση για την ερμηνεία που θα ακολουθήσει από έναν εξειδικευμένο τεχνικό.

Εάν χρησιμοποιούνται δοκιμές διείσδυσης ή αξιολογήσεις τρωτών σημείων, θα πρέπει να δοθεί προσοχή καθώς τέτοιες δραστηριότητες θα μπορούσαν να οδηγήσουν σε μια υποβάθμιση της ασφάλειας του συστήματος. Οι δοκιμές αυτές θα πρέπει να σχεδιάζονται, να καταγράφονται και να μπορούν να επαναλαμβάνονται.

2.2.14.3 Εξέταση εσωτερικού ελέγχου πληροφοριακών συστημάτων

Στόχος είναι να μεγιστοποιηθεί η αποτελεσματικότητα και να ελαχιστοποιηθεί η παρέμβαση προς/από την διαδικασία εσωτερικού ελέγχου των συστημάτων πληροφοριών.

Εσωτερικοί έλεγχοι πληροφοριακών συστημάτων

Απαιτήσεις ελέγχου και δραστηριότητες που περιλαμβάνουν ελέγχους πάνω σε συστήματα παραγωγής θα πρέπει να προγραμματιστούν προσεκτικά και να συμφωνηθούν ώστε να ελαχιστοποιηθεί ο κίνδυνος διατάραξης των επιχειρηματικών διαδικασιών.

Προστασία εργαλείων ελέγχου πληροφοριακών συστημάτων

Η πρόσβαση στα εργαλεία ελέγχου των συστημάτων πληροφοριών πρέπει να προστατεύεται για να αποτρέπεται οποιαδήποτε κατάχρηση ή διακινδύνευση.

Τα εργαλεία ελέγχου των πληροφοριακών συστημάτων, π.χ. λογισμικό ή αρχεία δεδομένων, θα πρέπει να διαχωριστούν από τα συστήματα ανάπτυξης και λειτουργίας και να μην βρίσκονται σε περιοχές χρήστη, εκτός και αν δοθεί κατάλληλο πρόσθετο επίπεδο προστασίας.

2.3 Πρότυπο ISO/IEC 27001

Το πρότυπο ISO/IEC 27001, μέρος της οικογένεια προτύπων ISO/IEC 27000, είναι ένα πρότυπο Συστημάτων Διαχείρισης Ασφάλειας Πληροφοριών (ΣΔΑΠ) που δημοσιεύθηκε τον Οκτώβριο του 2005 από τη Διεθνή Οργανισμό Τυποποίησης (International Organization for Standardization - ISO) και της Διεθνούς Ηλεκτροτεχνικής Επιτροπής (International Electrotechnical Commission - IEC).

Το ISO/IEC 27001 καθορίζει επίσημα ένα σύστημα διαχείρισης που έχει ως στόχο να φέρει την ασφάλεια πληροφοριών κάτω από διαχειριστικό έλεγχο. Όντας μια επίσημη προδιαγραφή σημαίνει ότι υποχρεώνει τους οργανισμούς με ειδικές απαιτήσεις. Οι οργανισμοί που ισχυρίζονται ότι έχουν υιοθετήσει το πρότυπο ISO/IEC 27001 μπορούν να ελέγχονται επίσημα και να πιστοποιούνται ως προς τη συμβατότητα τους με το πρότυπο.

Πως δουλεύει το πρότυπο

Οι περισσότεροι οργανισμοί έχουν ένα αριθμό ελέγχων ασφάλειας πληροφοριών. Ωστόσο, χωρίς ένα σύστημα διαχείρισης ασφάλειας πληροφοριών (ΣΔΑΠ), οι έλεγχοι τείνουν να είναι κάπως ανοργάνωτοι και ασυνάρτητοι, που εφαρμόζονται συχνά ως στοχευμένες λύσεις σε συγκεκριμένες καταστάσεις ή απλώς σαν συμβατικές λύσεις. Έτσι στην πράξη αφορούν κατά κανόνα μόνο ορισμένες πτυχές των πληροφοριακών στοιχείων ή της ασφάλισης πληροφοριών, αφήνοντας αγαθά εκτός πληροφορικής (όπως γραφειοκρατία και συγκεκριμένες γνώσεις) λιγότερο προστατευμένα.

Το πρότυπο ISO/IEC 27001 προβλέπει ότι η διοίκηση:

- Εξετάζει συστηματικά τους κινδύνους ασφάλειας πληροφοριών στον οργανισμό, λαμβάνοντας υπόψη τις απειλές, τα τρωτά σημεία, και τις επιπτώσεις.
- Σχεδιάζει και εφαρμόζει μια συνεκτική και ολοκληρωμένη ακολουθία ελέγχων ασφαλείας και άλλων μορφών αντιμετώπισης κινδύνου (όπως αποφυγή του κινδύνου ή μεταφορά του κινδύνου) για την αντιμετώπιση των κινδύνων αυτών που θεωρούνται μη αποδεκτοί.
- Υιοθετεί μια βασική διαδικασία διαχείρισης για τη διασφάλιση ότι οι έλεγχοι ασφάλειας πληροφοριών συνεχίζουν να ανταποκρίνονται στις ανάγκες ασφαλείας πληροφοριών του οργανισμού.

Ενώ ένα σύνολο ελέγχων ασφαλείας μπορεί δυνητικά να χρησιμοποιηθεί μέσα σε ένα ΣΔΑΠ με πρότυπο το ISO/IEC 27001, και άλλο σύνολο σε ΣΔΑΠ με πρότυπο το ISO/IEC 27002 (ο κώδικας ορθής πρακτικής για διαχείριση ασφαλείας πληροφοριών), αυτά τα δύο πρότυπα χρησιμοποιούνται συνήθως σε συνδυασμό στην πράξη. Στο παράρτημα Α του προτύπου ISO/IEC 27001 παρατίθενται συνοπτικά οι έλεγχοι της ασφάλειας πληροφοριών από το ISO/IEC 27002, ενώ το ISO/IEC 27002 παρέχει συμπληρωματικές πληροφορίες και συμβουλές σχετικά με την εφαρμογή των ελέγχων.

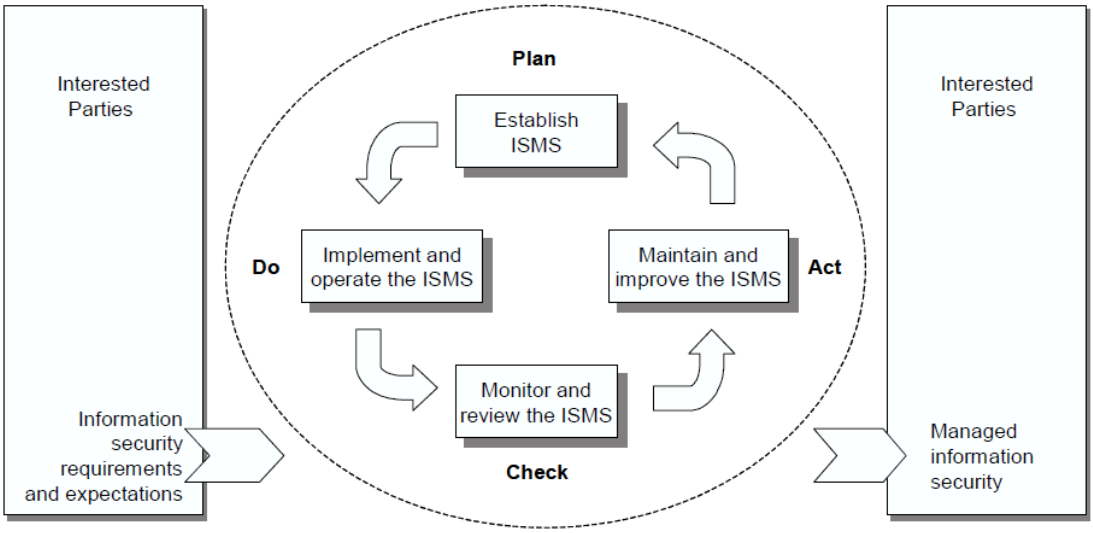
Οργανισμοί που εφαρμόζουν μια σειρά από ελέγχους ασφάλειας πληροφοριών βάσει του προτύπου ISO/IEC 27002 ταυτόχρονα ενδέχεται να ικανοποιούν πολλές από τις απαιτήσεις του ISO/IEC 27001, αλλά μπορεί να στερούνται ορισμένα από τα στοιχεία του συστήματος γενικής διαχείρισης. Το αντίστροφο είναι επίσης αλήθεια, με άλλα λόγια, ένα πιστοποιητικό συμμόρφωσης στο πρότυπο ISO/IEC 27001 παρέχει τη διαβεβαίωση ότι το σύστημα διαχείρισης της ασφάλειας πληροφοριών είναι στη θέση του, αλλά λέει λίγα για την απόλυτη κατάσταση ασφάλειας πληροφοριών εντός του οργανισμού. Τεχνικοί

έλεγχοι ασφαλείας όπως antivirus και firewall συνήθως δεν ελέγχονται στην πιστοποίηση του προτύπου ISO/IEC 27001. Ο οργανισμός ουσιαστικά υποτίθεται ότι έχει λάβει όλους τους απαραίτητους ελέγχους ασφάλειας, δεδομένου ότι το συνολικό ΣΔΑΠ έχει στηθεί και θεωρείται επαρκές, εφόσον πληροί τις απαιτήσεις του ISO/IEC 27001. Επιπλέον, η διοίκηση προσδιορίζει το πεδίο εφαρμογής του ΣΔΑΠ, για σκοπούς πιστοποίησης και μπορεί να το περιορίσει, για παράδειγμα, σε μια ενιαία επιχειρησιακή μονάδα ή διαδικασία. Το πιστοποιητικό για ISO/IEC 27001 για μια μονάδα του οργανισμού δεν σημαίνει ότι και στον υπόλοιπο οργανισμό, που δεν είναι στο πεδίο εφαρμογής του ΣΔΑΠ, υπάρχει κατάλληλη προσέγγιση στη διαχείριση ασφάλειας πληροφοριών.

Άλλα πρότυπα της οικογένειας ISO/IEC 27000 παρέχουν πρόσθετες οδηγίες σχετικά με ορισμένες πτυχές του σχεδιασμού, της υλοποίησης και λειτουργίας ενός ΣΔΑΠ, για παράδειγμα στη διαχείριση κινδύνων ασφάλειας πληροφοριών (ISO/IEC 27005).

2.3.1 Εισαγωγή στο ISO/IEC 27001

Αυτό το Διεθνές Πρότυπο υιοθετεί το «Plan-Do-Check-Act» μοντέλο διαδικασίας (PDCA), το οποίο εφαρμόζεται για τη δόμηση όλων των διαδικασιών του ΣΔΑΠ. Το σχήμα 1 επεξηγεί πως το ΣΔΑΠ παίρνει ως είσοδο τις απαιτήσεις ασφάλειας των πληροφοριών και τις προσδοκίες των ενδιαφερομένων μερών και μέσω των απαραίτητων ενεργειών και διαδικασιών παράγει αποτελέσματα για την ασφάλεια των πληροφοριών που πληρούν αυτές τις απαιτήσεις και τις προσδοκίες. Το Σχήμα 1 απεικονίζει επίσης τις συνδέσεις στις διαδικασίες που παρουσιάζονται στις επόμενες παραγράφους του προτύπου.



Σχήμα 2.1: Εφαρμογή του PDCA μοντέλου στις διαδικασίες του ΣΔΑΠ

Στον Πίνακα 1 παρουσιάζονται συνοπτικά οι βασικές έννοιες του μοντέλου PDCA.

Πίνακας 2.1: Παρουσίαση βημάτων μοντέλου PDCA

Σχεδίασε - Plan (καθορισμός του ΣΔΑΠ)	Καθορισμός της πολιτικής του ΣΔΑΠ, των στόχων, των διεργασιών και των διαδικασιών σχετικά με τη διαχείριση
Πράξε - Do (Υλοποίηση και	Εφαρμογή και λειτουργία της πολιτικής
Έλεγξε - Check (παρακολούθηση και αναθεώρηση του ΣΔΑΠ)	Υπολογισμός και μέτρηση της απόδοσης των διαδικασιών ως προς την πολιτική, τους στόχους, και την πρακτική εμπειρία του ΣΔΑΠ και
Πράξε - Act (Διατήρηση και βελτίωση του ΣΔΑΠ)	Λήψη διορθωτικών και προληπτικών μέτρων, με βάση τα αποτελέσματα του εσωτερικού ελέγχου του ΣΔΑΠ και της αναθεώρησης της διαχείρισης,

Αυτό το Διεθνές Πρότυπο είναι ευθυγραμμισμένο με τα πρότυπα ISO 9001:2000 και ISO 14001:2004, προκειμένου να στηριχθεί η συνεπής και ολοκληρωμένη εφαρμογή και λειτουργία με τα σχετικά πρότυπα διαχείρισης. Ένα κατάλληλα σχεδιασμένο σύστημα διαχείρισης μπορεί να ικανοποιήσει έτσι τις απαιτήσεις όλων αυτών των προτύπων.

Αυτό το Διεθνές Πρότυπο καλύπτει όλα τα είδη των οργανισμών (π.χ. εμπορικές επιχειρήσεις, κυβερνητικές υπηρεσίες, μη κερδοσκοπικούς οργανισμούς) και προδιαγράφει τις απαιτήσεις για τον καθορισμό, την υλοποίηση, τη λειτουργία, την παρακολούθηση, την αναθεώρηση, τη διατήρηση και τη βελτίωση ενός ΣΔΑΠ στο πλαίσιο των συνολικών επιχειρησιακών κινδύνων του οργανισμού. Η παρούσα οδηγία καθορίζει τις απαιτήσεις για την εφαρμογή των ελέγχων ασφαλείας προσαρμοσμένους στις ανάγκες των μεμονωμένων οργανισμών ή τμημάτων.

Το ΣΔΑΠ έχει σχεδιαστεί για να εξασφαλίσει την επιλογή κατάλληλων ελέγχων ασφαλείας που προστατεύουν τα πληροφοριακά αγαθά και να δίνουν εμπιστοσύνη στα ενδιαφερόμενα μέρη.

Για να μπορεί ένας οργανισμός να ισχυρίζεται συμμόρφωση με το πρότυπο πρέπει να μην εξαιρεί καμία από τις απαιτήσεις που ορίζονται από αυτό. Όταν εξαιρούνται μεμονωμένοι έλεγχοι, οι απαιτήσεις συμμόρφωσης σε αυτό το πρότυπο δεν είναι αποδεκτές, εκτός εάν οι εξαιρέσεις αυτές δεν επηρεάζουν την ικανότητα του οργανισμού, και/ή την ευθύνη του, για την παροχή ασφάλειας πληροφοριών η οποία να πληροί τις απαιτήσεις ασφαλείας που καθορίζονται από την εκτίμηση των κινδύνων και τις κανονιστικές απαιτήσεις.

2.3.2 Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών

Ο οργανισμός οφείλει να σχεδιάσει, υλοποιήσει, συντηρήσει και βελτιώσει ένα καταγεγραμμένο Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών (ΣΔΑΠ) σχετικό με τις επιχειρησιακές δραστηριότητες και τους κινδύνους που αντιμετωπίζουν. Η διαδικασία που χρησιμοποιείται για το ΣΔΑΠ βασίζεται στο μοντέλο PDCA.

2.3.2.1 Εγκαθίδρυση του ΣΔΑΠ

Ο οργανισμός θα πρέπει να κάνει τα ακόλουθα:

- Καθορισμό του πεδίου εφαρμογής και των ορίων του ΣΔΑΠ.
- Καθορισμό της πολιτικής του ΣΔΑΠ σχετικά με τα χαρακτηριστικά της επιχείρησης, τα αγαθά και την τεχνολογία που διαχειρίζεται.
- Καθορισμό της μεθόδου αξιολόγησης κινδύνων και αποδοχής αυτών.
- Προσδιορισμό των κινδύνων που αφορούν τα αγαθά και τις ευπάθειές τους καθώς και τον αντίκτυπο των κινδύνων αυτών.
- Καθορισμό του στόχου των ελέγχων και επιλογή κατάλληλων ελέγχων.
- Καταγραφή όλων αυτών.

2.3.2.2 Υλοποίηση και διαχείριση του ΣΔΑΠ

Ο οργανισμός θα πρέπει να κάνει τα ακόλουθα:

- Διατύπωση ενός συγκεκριμένου σχεδίου αντιμετώπισης κινδύνων και υλοποίηση του έτσι ώστε να επιτευχθούν οι στόχοι των ελέγχων.
- Καθορισμός του τρόπου μέτρησης της αποτελεσματικότητας των επιλεγμένων ελέγχων και πως οι μετρήσεις θα χρησιμοποιηθούν.
- Διαχείριση λειτουργιών και πόρων του ΣΔΑΠ και υλοποίηση διαδικασιών και ελέγχων για έγκαιρη ανίχνευση των περιστατικών.

2.3.2.3 Παρακολούθηση και αναθεώρηση του ΣΔΑΠ

Ο οργανισμός θα πρέπει να κάνει τα ακόλουθα:

- Να εκτελεί διαδικασίες και ελέγχους παρακολούθησης ώστε να γίνεται έγκαιρα η ανίχνευση λαθών και παραβιάσεων ασφαλείας.
- Να αναλαμβάνει τακτικές αναθεωρήσεις της αποτελεσματικότητας του ΣΔΑΠ και να μετράει την αποτελεσματικότητα των ελέγχων.
- Να αναθεωρεί τις αξιολογήσεις των κινδύνων και σε τακτικά χρονικά διαστήματα και μετά από διάφορες αλλαγές π.χ. στον οργανισμό, την τεχνολογία, τους στόχους, τις απειλές κλπ.
- Διεξαγωγή εσωτερικών ελέγχων και ενημέρωση σχεδίων ασφαλείας.

2.3.2.4 Συντήρηση και βελτίωση του ΣΔΑΠ

Ο οργανισμός θα πρέπει να κάνει τα ακόλουθα:

- Να εφαρμόζει τις καθορισμένες βελτιώσεις του ΣΔΑΠ.
- Να μαθαίνει από περιστατικά ασφάλειας του ίδιου ή άλλου οργανισμό.
- Να επικοινωνεί τις δράσεις του σε όλα τα ενδιαφερόμενα μέρη.
- Να διασφαλίζει ότι οι βελτιώσεις πετυχαίνουν τους στόχους τους.

2.3.2.5 Απαιτήσεις καταγραφής εγγράφων

Τα επίσημα έγγραφα περιλαμβάνουν καταγραφές για τις αποφάσεις της διοίκησης, που διασφαλίζουν ότι οι δράσεις είναι ανιχνεύσιμες σε αποφάσεις της διοίκησης και πολιτικές, και τα αποτελέσματα που καταγράφονται είναι επαναλήψιμα.

Τα έγγραφα ενός ΣΔΑΠ πρέπει να περιλαμβάνουν:

- Καταγεγραμμένες δηλώσεις της πολιτικής του ΣΔΑΠ και των στόχων.
- Περιγραφή της μεθοδολογίας ανάλυσης κινδύνων, καθώς και το σχέδιο αντιμετώπισης κινδύνων.
- Τη Δήλωση της Εφαρμοστικότητας (Statement of Applicability) που στην πραγματικότητα είναι ο κύριος σύνδεσμος μεταξύ της αξιολόγησης του κινδύνου και της θεραπείας με την εφαρμοζόμενη ασφάλεια πληροφοριών.

Τα επίσημα έγγραφα που απαιτούνται από το ΣΔΑΠ πρέπει να προστατεύονται και να ελέγχονται. Έτσι πρέπει να υλοποιηθεί μια αντίστοιχη διαδικασία που να ασχολείται με τη διανομή, συντήρηση και εμπιστευτικότητα των εγγράφων. Το ίδιο ισχύει και για τις καταγραφές που πρέπει να δημιουργούνται και να διατηρούνται για να προσκομίζουν αποδεικτικά στοιχεία συμμόρφωσης.

2.3.3 Διοικητική ευθύνη

Στην ενότητα αυτή παρουσιάζονται οι ευθύνες της διοίκησης ως προς τη δέσμευση της για τη δημιουργία του ΣΔΑΠ. Επίσης η ευθύνη ως προς την παροχή πόρων για την

υλοποίηση του ΣΔΑΠ και η εκπαίδευση, ενημέρωση και ο διαμοιρασμός αρμοδιοτήτων στο προσωπικό.

2.3.3.1 Δέσμευση της διοίκησης

Η Διοίκηση πρέπει να παρέχει αποδείξεις της δέσμευσης της ως προς την εγκατάσταση, λειτουργία, παρακολούθηση, αναθεώρηση, συντήρηση και βελτίωση του ΣΔΑΠ ακολουθώντας τα παρακάτω βήματα:

- Καθορισμός μιας πολιτικής ΣΔΑΠ και των αντίστοιχων στόχων.
- Καθορισμός των ρόλων και ευθυνών για την ασφάλεια πληροφοριών.
- Επικοινωνία εντός του οργανισμού σχετικά με τη σημαντικότητα της ασφάλειας πληροφοριών, τη συμμόρφωση με την αντίστοιχη πολιτική, τις νομικές υποχρεώσεις και την ανάγκη για συνεχή βελτίωση.
- Να αποφασίσει τα κριτήρια για αποδοχή κινδύνου και τα ανεκτά όρια.
- Να διεξάγει αναθεωρήσεις από την πλευρά της διοίκησης.

2.3.3.2 Διαχείριση των πόρων

Ο οργανισμός θα πρέπει να καθορίσει και να παρέχει τους πόρους που χρειάζονται για:

- Να υλοποιήσουν και να συντηρήσουν το ΣΔΑΠ.
- Να εξασφαλίσουν ότι οι διαδικασίες υποστηρίζουν τις επιχειρησιακές απαιτήσεις.
- Να εντοπίσουν και να αντιμετωπίσουν τις νομικές απαιτήσεις.
- Να εφαρμόζουν σωστά τους υλοποιημένους ελέγχους.
- Να πραγματοποιούν αναθεωρήσεις, και να αντιδρούν ανάλογα με τα αποτελέσματα και όταν απαιτείται να βελτιώνουν το ΣΔΑΠ.

Επίσης ο οργανισμός πρέπει να διασφαλίσει ότι όλο το προσωπικό που αναλαμβάνει ευθύνες ασφάλειας είναι ικανό να πραγματοποιήσει τις απαιτούμενες δραστηριότητες. Αυτό επιτυγχάνεται με τα παρακάτω:

- Τον καθορισμό των αναγκαίων δεξιοτήτων για το προσωπικό που εκτελεί εργασίες που πραγματοποιούν το ΣΔΑΠ.
- Παροχή εκπαίδευσης ή πρόσληψη προσωπικού με αυτές τις δεξιότητες.
- Καταγραφή της εκπαίδευσης, των ικανοτήτων και της εμπειρίας του προσωπικού.

2.3.4 Εσωτερικός έλεγχος του ΣΔΑΠ

Ο οργανισμός θα πρέπει να διεξάγει εσωτερικό έλεγχο του ΣΔΑΠ σε τακτά χρονικά διαστήματα ώστε να καθορίζεται κατά πόσον οι στόχοι των ελέγχων, οι έλεγχοι και οι διαδικασίες ενός ΣΔΑΠ συμμορφώνονται με τις απαιτήσεις των διεθνών προτύπων και της σχετικής νομοθεσίας αλλά και κατά πόσον λειτουργούν και συντηρούνται σωστά όπως αναμένεται.

Ένα πρόγραμμα ελέγχου πρέπει να σχεδιάζεται, λαμβάνοντας υπόψη την κατάσταση και τη σημασία των διαδικασιών και των περιοχών που πρόκειται να ελεγχθούν, καθώς και τα αποτελέσματα προηγούμενων ελέγχων. Θα πρέπει να οριστούν τα κριτήρια ελέγχου, το πεδίο εφαρμογής, η συχνότητα και οι μέθοδοι. Η επιλογή των ελεγκτών και η διενέργεια των ελέγχων πρέπει να εξασφαλίζουν την αντικειμενικότητα και την αμεροληψία της διαδικασίας ελέγχου. Οι ελεγκτές δεν πρέπει να ελέγχουν τη δική τους εργασία.

2.3.5 Επανεξέταση του ΣΔΑΠ από τη Διοίκηση

Η επανεξέταση θα περιλαμβάνει την αξιολόγηση ευκαιριών βελτίωσης και την ανάγκη για αλλαγές στο ΣΔΑΠ, συμπεριλαμβανομένης της πολιτικής και των στόχων της ασφάλειας πληροφοριών. Τα αποτελέσματα των αξιολογήσεων θα πρέπει να καταγράφονται σαφώς και τα έγγραφα πρέπει να διατηρούνται.

Η επανεξέταση αυτή δέχεται σαν είσοδο τα αποτελέσματα του εσωτερικού ελέγχου, την ανατροφοδότηση από τα ενδιαφερόμενα μέρη, την κατάσταση των αποτρεπτικών και διορθωτικών ενεργειών, τις ευπάθειες που δε διευθετήθηκαν επαρκώς στην

προηγούμενη ανάλυση κινδύνου, τις επακόλουθες δράσεις από προηγούμενη επανεξέταση και τέλος τις αλλαγές που θα μπορούσαν να επηρεάσουν το ΣΔΑΠ.

Το αποτέλεσμα της διοικητικής επανεξέτασης πρέπει να περιλαμβάνει αποφάσεις και δράσεις που σχετίζονται με τη βελτίωση της αποτελεσματικότητας, την ανανέωση του σχεδίου επανεξέτασης και αντιμετώπισης κινδύνων, και την τροποποίηση των διαδικασιών και των ελέγχων ώστε να ανταποκρίνονται σε εσωτερικά και εξωτερικά συμβάντα που έχουν αντίκτυπο στο ΣΔΑΠ.

2.3.6 Βελτίωση του ΣΔΑΠ

Η βελτίωση του ΣΔΑΠ μπορεί έχει τη μορφή της συνεχούς βελτίωσης ή της διορθωτικής ενέργειας ή της προληπτικής δράσης.

Ο οργανισμός πρέπει να βελτιώνει συνεχώς την αποτελεσματικότητα του ΣΔΑΠ μέσω της πολιτικής ασφάλειας πληροφοριών, των στόχων της ασφάλειας πληροφοριών, των αποτελεσμάτων ελέγχου και της ανάλυσης των περιστατικών που έχουν καταγραφεί.

Ο οργανισμός πρέπει να αναλάβει δράση για την εξάλειψη της αιτίας της μη συμμόρφωσης με τις απαιτήσεις του ΣΔΑΠ, προκειμένου να αποτραπεί η επανάληψη. Η καταγεγραμμένη διαδικασία για διορθωτικές ενέργειες θα πρέπει να καθορίζει απαιτήσεις για αναγνώριση μη συμμορφώσεων, καθορισμό των αιτιών τους, αξιολόγηση της ανάγκης για δράση, καταγραφή των αποτελεσμάτων των ενεργειών και επανεξέταση των διορθωτικών δράσεων που λήφθηκαν.

Ο οργανισμός πρέπει να προβαίνει σε ενέργειες για την εξάλειψη της αιτίας των πιθανών περιπτώσεων μη συμμόρφωσης με τις απαιτήσεις του ΣΔΑΠ, προκειμένου να αποφευχθεί η εμφάνισή τους. Οι προληπτικές δράσεις θα πρέπει να είναι κατάλληλες για τις επιπτώσεις των πιθανών προβλημάτων. Η καταγεγραμμένη διαδικασία για προληπτική δράση πρέπει να καθορίζει τις απαιτήσεις για:

- Εντοπισμό πιθανών μη συμμορφώσεων και των αιτιών τους.
- Αξιολόγηση της ανάγκης ανάληψης δράσης για την πρόληψη της εμφάνισης των περιπτώσεων μη συμμόρφωσης
- Καθορισμό και εφαρμογή των προληπτικών μέτρων που απαιτούνται.
- Καταγραφή των αποτελεσμάτων των και επανεξέταση της προληπτικής δράσης.

Η προτεραιότητα των προληπτικών ενεργειών θα πρέπει να καθορίζεται με βάση τα αποτελέσματα της αξιολόγησης του κινδύνου. Υπάρχει η σημείωση πως «Η δράση για την πρόληψη της μη συμμόρφωσης είναι συχνά πιο αποδοτική από τη διορθωτική ενέργεια».

2.3.7 Παραρτήματα του Προτύπου ISO/IEC 27001

Στο Πρότυπο ISO/IEC 27001 υπάρχει το παράρτημα Α όπου υπάρχει μια λίστα με αντιστοιχίες στόχων και ελέγχων οι οποίοι στόχοι προέρχονται από το πρότυπο ISO/IEC 17799:2005 όπου περιέχονται στις παραγράφους 2.2.4 έως 2.2.14 της παρούσας εργασίας. Σε ένα πίνακα λοιπόν παρουσιάζονται ένας προς έναν οι διάφοροι γενικοί στόχοι και ακολουθούν οι επιμέρους στόχοι και δίπλα ο αντίστοιχος έλεγχος.

Το παράρτημα Β παρουσιάζεται η αντιστοιχία των οδηγιών του OECD (Organisation for Economic Co-operation and Development) για την ασφάλεια δικτύων και πληροφοριακών προβλημάτων με το πρότυπο. Σε ένα πίνακα φαίνεται πως υλοποιούνται κάποιες από της αρχές του OECD χρησιμοποιώντας το μοντέλο PDCA.

Τέλος στο παράρτημα Γ παρουσιάζεται η αντιστοιχία του προτύπου με τα πρότυπα ISO 9001:2000 και ISO 14001:2004.

ΚΕΦΑΛΑΙΟ 3

Ρυθμιστικές Αρχές και Κανονιστική συμμόρφωση Τραπεζικών Ιδρυμάτων και το Προτυπο PCI DSS

Στο παρόν κεφάλαιο θα παρουσιάσουμε δύο ενότητες που αφορούν Ρυθμιστικές Αρχές στην Ελλάδα και την αντίστοιχη συμμόρφωση καθώς και μία ενότητα αφιερωμένη στο πρότυπο PCI DSS που αφορά τον τραπεζικό κλάδο. Στην πρώτη ενότητα παρουσιάζουμε την Πράξη Διοικητή ΤτΕ 2577 που αφορά την ασφαλή λειτουργία των Πληροφοριακών Συστημάτων σε Τραπεζικό Οργανισμό, και στη δεύτερη την Αρχή Προστασίας Προσωπικών δεδομένων και πως εφαρμόζεται το νομικό της πλαίσιο στον τραπεζικό κλάδο.

3.1. Πράξη Διοικητή Τράπεζας της Ελλάδος 2577

Περιλαμβάνει το πλαίσιο αρχών λειτουργίας και κριτηρίων αξιολόγησης της οργάνωσης και των Συστημάτων Εσωτερικού Ελέγχου των πιστωτικών και χρηματοδοτικών ιδρυμάτων και επίσης περιλαμβάνει τις σχετικές αρμοδιότητες των διοικητικών τους οργάνων. Αυτό που ενδιαφέρει για την ασφάλεια πληροφοριών και θα περιγράψουμε είναι το Παράρτημα 2: «ΑΡΧΕΣ ΑΣΦΑΛΟΥΣ ΚΑΙ ΑΠΟΤΕΛΕΣΜΑΤΙΚΗΣ ΛΕΙΤΟΥΡΓΙΑΣ ΤΩΝ ΣΥΣΤΗΜΑΤΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΣΤΑ ΠΛΑΙΣΙΑ ΤΗΣ ΔΙΑΧΕΙΡΙΣΗΣ ΤΟΥ ΛΕΙΤΟΥΡΓΙΚΟΥ ΚΙΝΔΥΝΟΥ ΑΠΟ ΤΑ ΠΙΣΤΩΤΙΚΑ ΙΔΡΥΜΑΤΑ»

Το παράρτημα αυτό θέτει ένα δομημένο και λεπτομερές πλαίσιο γενικών αρχών και κριτηρίων για την ασφαλή και αποτελεσματική λειτουργία των Πληροφοριακών Συστημάτων (ΠΣ), λαμβάνοντας παράλληλα υπόψη τις πλέον πρόσφατες εξελίξεις της πληροφορικής στον βαθμό που επηρεάζουν την λειτουργία των Πιστωτικών Ιδρυμάτων (ΠΙ).

Οι αρχές αυτές ομαδοποιούνται σε τέσσερις ενότητες και συγκεκριμένα στις:

- Οργάνωση και Διοίκηση Πληροφορικής, όπου γίνεται αναφορά στην Διακυβέρνηση της Πληροφορικής, στην οργάνωση της Υπηρεσιακής Μονάδας της Πληροφορικής και στις σχέσεις με τους Εξωτερικούς Συνεργάτες.

- Ανάπτυξη και Προμήθεια Συστημάτων, όπου γίνεται αναφορά στις μεθοδολογίες, πρότυπα και διαδικασίες ανάπτυξης και προμήθειας Πληροφοριακών Συστημάτων.
- Λειτουργία και Υποστήριξη, όπου γίνεται αναφορά στις διαδικασίες λειτουργίας των συστημάτων, στη φυσική και λογική τους ασφάλεια, καθώς και στη διασφάλιση της συνέχειας των εργασιών του ΠΙ.
- Έλεγχος Συστημάτων Πληροφορικής, όπου γίνεται αναφορά σε κανόνες και βασικές απαιτήσεις για την επαρκή και αποτελεσματική λειτουργία της Μονάδας Εσωτερικής Επιθεώρησης αναφορικά με τα Πληροφοριακά Συστήματα.

3.1.1 Οργάνωση και Διοίκηση Πληροφορικής

Σε αυτή την ενότητα αρχικά αναφέρεται η διακυβέρνηση της πληροφορικής ως ευθύνη της διοίκησης. Θα πρέπει να περιλαμβάνονται οι κατάλληλες διαδικασίες για την επίτευξη των στόχων του ιδρύματος, τη διαχείριση των πόρων, την αξιολόγηση των κινδύνων και άλλες λειτουργίες .

Για την επίτευξη όλων αυτών το ΠΙ θα πρέπει σύμφωνα με την Πράξη 2577:

- Να διαθέτει καταγεγραμμένη και εγκεκριμένη στρατηγική για την Πληροφορική, συμβατή με τη γενικότερη επιχειρησιακή στρατηγική του.
- Να διαθέτει Ειδική Συντονιστική Επιτροπή για την Πληροφορική (I.T. Steering Committee) όπου η σύνθεση και τα καθήκοντα της περιγράφονται.
- Να αξιολογεί, τους κινδύνους που απορρέουν από τη λειτουργία των Πληροφοριακών Συστημάτων.
- Να διαθέτει εγκεκριμένη από τη Διοίκηση πολιτική ασφάλειας.
- Να προβλέπει θέση υπευθύνου ασφαλείας Πληροφοριακών Συστημάτων ο οποίος αναφέρεται σε υψηλά κλιμάκια της ιεραρχίας.
- Να διαθέτει διαδικασίες για τη διαχείριση των έργων πληροφορικής, για τον εντοπισμό προβλημάτων και για την καταγραφή και κατηγοριοποίηση των γεγονότων που ενέχουν κίνδυνο.
- Να διαθέτει Σύστημα Διοικητικής Πληροφόρησης (MIS - Management Information System), κατάλληλο για την αποτελεσματική πληροφόρηση της διοίκησης.

- Να μελετά τα διεθνή πρότυπα ασφάλειας

Το Πιστωτικό Ίδρυμα θα πρέπει να διαθέτει εξειδικευμένη Υπηρεσιακή Μονάδα Πληροφορικής, λειτουργικά και διοικητικά ανεξάρτητη από τους τελικούς χρήστες των υπηρεσιών πληροφορικής, η οποία θα πρέπει:

- Να διαθέτει οργανόγραμμα όπου απεικονίζονται οι επιχειρησιακές ανάγκες, ο διαχωρισμός καθηκόντων και άλλες πληροφορίες.
- Να διαθέτει καταγεγραμμένες περιγραφές θέσεων εργασίας στις οποίες θα περιλαμβάνονται οι αρμοδιότητες κάθε θέσης.

Όταν το ΠΙ συνεργάζεται με εξωτερικούς συνεργάτες σε θέματα πληροφορικής θα πρέπει να λαμβάνονται υπόψη ειδικότερα τα εξής:

- Οι κίνδυνοι που προκύπτουν από τη χρήση εξωτερικών συνεργατών μερικοί εκ των οποίων είναι η έλλειψη ελέγχου στις υπηρεσίες, η εξάρτηση από τρίτους, η δυσκολία στο να προσαρμοστούν άμεσα στις ανάγκες των πελατών και η αδιαφανής κοστολόγηση των υπηρεσιών.
- Η σωστή επιλογή των εξωτερικών συνεργατών, καθώς και η κατάλληλη εποπτεία ως προς την ασφαλή λειτουργία. Για την επιλογή των εξωτερικών συνεργατών υπάρχουν κι άλλα κριτήρια είναι εκτός από την αξιολόγηση των υπηρεσιών όπως είναι η φήμη του στην αγορά, η οργανωτική δομή και η ποιότητα του ανθρωπίνου δυναμικού.
- Κατά την υπογραφή των συμβολαίων πρέπει να περιγράφονται αναλυτικά διάφορα σημαντικά θέματα όπως:
    - Τα δικαιώματα και οι υποχρεώσεις των συμβαλλομένων μερών.
    - Το συμφωνηθέν επίπεδο παροχής υπηρεσιών (Service Level Agreement - SLA) και ο τρόπος τιμολόγησής τους.
    - Η δυνατότητα επαναδιαπραγμάτευσης του συμβολαίου.
    - Και διάφορα άλλα όπως περιπτώσεις υπεργολαβίας, θέματα ιδιοκτησίας και αδειοδότησης, διαδικασίες επίλυσης διαφορών και διαδικασίες τερματισμού συμβολαίου.

Επίσης αναφορά στα συμβόλαια γίνεται στην ασφάλεια πληροφοριών, στην πιστοποίηση των δύο μερών, στη δυνατότητα διενέργεια ελέγχου από το ΠΙ ή από τρίτους, στις ποινικές ρήτρες για αθέτηση των συμφωνηθέντων και άλλα.

3.1.2 Ανάπτυξη και Προμήθεια Συστημάτων

Αρχικά αναφέρονται οι φάσεις του κύκλου ζωής ενός συστήματος. Τέτοιες φάσεις είναι η φάση της Μελέτης Σκοπιμότητας, της Ανάλυσης των Επιχειρησιακών Απαιτήσεων και του Καθορισμού των Προδιαγραφών, της Τεχνικής Ανάλυσης και του Σχεδιασμού, της Ανάπτυξης, των Δοκιμών, της Αποδοχής και της Μεταφοράς στην Παραγωγή, της Λειτουργίας και Υποστήριξης και τέλος της Απόσυρσης. Η μετάβαση από τη μία φάση στην άλλη προϋποθέτει την ανασκόπηση και έγκριση των αποτελεσμάτων της προηγούμενης.

Η εποπτεία του έργου της ανάπτυξης κάθε σημαντικού συστήματος πρέπει να ανατίθεται στη Συντονιστική Επιτροπή της Πληροφορικής (IT Steering Committee). Με την ολοκλήρωση της ανάπτυξης του συστήματος, η επιχειρησιακή και τεχνική του εποπτεία θα πρέπει να ανατίθεται στις αρμόδιες υπηρεσιακές μονάδες ή στελέχη.

3.1.2.1 Ανάπτυξη Συστημάτων

Όταν ο οργανισμός αναπτύξει εσωτερικά ένα πληροφοριακό σύστημα χωρίς δηλαδή να το προμηθευτεί από άλλη εταιρεία θα πρέπει να ληφθούν υπόψιν αρκετά ζητήματα μερικά εκ των οποίων είναι:

- Να ορισθεί Ομάδα Έργου που θα αναλάβει την διαχείριση του έργου.
- Να σχεδιαστεί χρονοδιάγραμμα υλοποίησης που να προσδιορίζει, μεταξύ άλλων, τις φάσεις, τη διάρκεια τους, και τους υπεύθυνους για την υλοποίηση της κάθε φάσης, καθώς και τα παραδοτέα.
- Να γίνεται εκτίμηση του όγκου των δεδομένων και του αριθμού των συναλλαγών που θα διαχειρίζεται το νέο σύστημα.

- Στις φάσεις της Τεχνικής Ανάλυσης και του Σχεδιασμού να διενεργείται ανάλυση κινδύνων και να καθορίζονται με λεπτομέρεια οι απαιτήσεις ασφαλούς λειτουργίας του συστήματος σύμφωνα με την πολιτική ασφάλειας του ιδρύματος.
- Οι αρχικές δοκιμές του συστήματος να διενεργούνται από το προσωπικό της Πληροφορικής σε ξεχωριστό περιβάλλον με προκαθορισμένα σενάρια. Σε δεύτερη φάση να διενεργούνται ολοκληρωμένες δοκιμές που περιλαμβάνουν δοκιμές επαναφοράς (recovery testing), δοκιμές ασφάλειας και δοκιμές αντοχής του συστήματος σε περίπτωση μεγάλου όγκου δεδομένων.
- Η Λειτουργία και Υποστήριξη του συστήματος να περιλαμβάνει διαδικασίες ελέγχου των αλλαγών (change control), ελέγχου των εκδόσεων του συστήματος (versioning), ελέγχου ενημερώσεων του συστήματος για την αντιμετώπιση προβλημάτων που εντοπίστηκαν (patching), ελέγχου της απόδοσης του συστήματος, λήψης και φύλαξης εφεδρικών αρχείων, συνέχειας των εργασιών, ενημέρωσης του Help Desk για την υποστήριξη των χρηστών του συστήματος, κ.α.
- Η φάση Απόσυρσης του Συστήματος να περιλαμβάνει διαδικασίες για διατήρηση των πληροφοριών σύμφωνα με τις νομικές οδηγίες.

3.1.2.2 Προμήθεια Συστημάτων

Στην περίπτωση προμήθειας ισχύουν επιπλέον των ζητημάτων για ανάπτυξη συστημάτων τα εξής:

- Η διαδικασία προμήθειας να χαρακτηρίζεται από διακριτές φάσεις, οι οποίες θα υλοποιούν πρότυπα, μεθοδολογίες και διαδικασίες επίσημα καταγεγραμμένες και εγκεκριμένες. Τέτοιες φάσεις, είναι αυτές της πρόσκλησης για υποβολή προτάσεων (Request For Proposal - RFP) με αναλυτική περιγραφή των αναγκών που θα καλύπτει το προς προμήθεια σύστημα, της επιλογής του εξωτερικού συνεργάτη, της σύναψης της συμφωνίας και της υπογραφής του συμβολαίου, της ένταξης και λειτουργίας των συστημάτων στην παραγωγή και, τέλος, της εποπτείας και του ελέγχου τους.
- Το είδος παρέμβασης του ΠΙ στο σύστημα να είναι εκ των προτέρων αυστηρά καθορισμένο και καταγεγραμμένο σε επίσημα έγγραφα.

- Να καθορίζονται τα χρονικά περιθώρια απόκρισης σε περίπτωση ανάγκης υποστήριξης από τον προμηθευτή.
- Να υπάρχει καταγραφή των δράσεων (logging) του εξωτερικού συνεργάτη σε περίπτωση εισόδου στο σύστημα.

3.1.3 Λειτουργία και Υποστήριξη

Η απρόσκοπτη λειτουργία και η αποτελεσματική υποστήριξη των Πληροφοριακών Συστημάτων προϋποθέτουν την τήρηση των πολιτικών, προτύπων και διαδικασιών του ΠΙ από όλες τις εμπλεκόμενες υπηρεσιακές μονάδες, αλλά και τους παρόχους υπηρεσιών πληροφορικής.

3.1.3.1 Λειτουργία Συστημάτων

Ο όρος «Λειτουργία Συστημάτων» αναφέρεται στο σύνολο των διαδικασιών που απαιτούνται για την καθημερινή λειτουργία των Πληροφοριακών Συστημάτων σε ένα Πιστωτικό Ίδρυμα. Για ένα αποδεκτό επίπεδο ασφαλούς και αποτελεσματικής λειτουργίας τους θα πρέπει να υφίστανται μεταξύ άλλων:

- Πλήρης και λεπτομερής καταγραφή του μηχανογραφικού εξοπλισμού, λογισμικού, καθώς και του ιστορικού των εκδόσεων και αδειών χρήσης.
- Υποστήριξη των υπαλλήλων, αλλά και των πελατών η οποία και θα πρέπει να ανατίθεται σε κατάλληλα οργανωμένες και στελεχωμένες υπηρεσιακές μονάδες (Help Desk).
- Διαδικασίες αποτροπής εγκατάστασης μη εγκεκριμένου λογισμικού.
- Συνεχής παρακολούθηση της διαθεσιμότητας των συστημάτων.
- Ειδικότερα, για τα συστήματα και τις υπηρεσίες Ηλεκτρονικής Τραπεζικής θα πρέπει να υφίστανται:
    - Επαρκής πληροφόρηση στο διαδικτυακό τόπο του ΠΙ για την εποπτεύουσα αρχή που παρέχει την άδεια λειτουργίας, πριν πραγματοποιήσουν τις ηλεκτρονικές τους συναλλαγές.

- Ενημέρωση των πελατών για την πολιτική εμπιστευτικότητας που εφαρμόζει το ΠΙ σε σχέση με τα προσωπικά τους δεδομένα.
- Αυτοματοποιημένα συστήματα παρακολούθησης συναλλαγών που να εντοπίζουν και καταγράφουν ασυνήθιστες συναλλακτικές συμπεριφορές και να παράγουν προειδοποιητικά μηνύματα.
- Αποτελεσματική αντιμετώπιση των κινδύνων νομιμοποίησης εσόδων από εγκληματικές δραστηριότητες (money laundering).

3.1.3.2 Φυσική Ασφάλεια

Η φυσική ασφάλεια αφορά την προστασία των συστημάτων από κινδύνους του περιβάλλοντος ή φυσική παραβίαση από ανθρώπους των χώρων των εγκαταστάσεων.

Στα μέτρα φυσικής ασφάλειας πρέπει να περιλαμβάνονται μεταξύ άλλων:

- Μηχανισμοί ελέγχου φυσικής πρόσβασης που να περιορίζουν και καταγράφουν την είσοδο και έξοδο του προσωπικού και επισκεπτών καθώς και τη διακίνηση εξοπλισμού και αποθηκευτικών μέσων.
- Μηχανισμοί πρόληψης και αντιμετώπισης καταστροφών από φυσικά αίτια (πλημμύρα, φωτιά, σεισμό).
- Μηχανισμοί πρόληψης και αντιμετώπισης κακόβουλων ενεργειών (διάρρηξη / κλοπή, βανδαλισμός, τρομοκρατική ενέργεια, κλπ).
- Η ασφαλής μεταφορά ευαίσθητων εγγράφων και μαγνητικών μέσων.

3.1.3.3 Λογική Ασφάλεια

Ενώ η φυσική ασφάλεια αφορά τη φυσική πρόσβαση στα συστήματα ή λογική ασφάλεια αφορά τον περιορισμό και έλεγχο πρόσβασης στους πόρους των συστημάτων όπως είναι τα δίκτυα, το λογισμικό και τα δεδομένα. Τα μέτρα αυτά μπορεί να αφορούν λειτουργικά συστήματα, εφαρμογές, συστήματα διαχείρισης βάσεων δεδομένων, συστήματα επικοινωνιών.

<u>Για την ασφάλεια των προσβάσεων στα συστήματα πρέπει:</u>

- Οι χρήστες να έχουν μοναδικό λογαριασμό πρόσβασης σε κάθε σύστημα.
- Να ελέγχονται οι δράσεις των χρηστών με αυξημένα δικαιώματα.
- Να πιστοποιείται κάθε χρήστης κατά την είσοδο μέσω ενός μηχανισμού ασφάλειας (πχ κωδικός, έξυπνη κάρτα, ψηφιακό πιστοποιητικό).
- Να χρησιμοποιούνται δύσκολα προβλέψιμοι κωδικοί και οι χρήστες να πρέπει να τους αλλάζουν συχνά.

Για την ασφάλεια των δεδομένων πρέπει:

- Να υπάρχει καταγεγραμμένη διαβάθμιση των δεδομένων.
- Να χρησιμοποιείται κρυπτογράφηση με υψηλής ασφάλειας κλειδί και να αναπτύσσεται στρατηγική υποδομής Δημοσίου Κλειδιού (Public Key Infrastructure) για τη διαχείριση των ψηφιακών πιστοποιητικών.
- Για της βάσεις δεδομένων πρέπει να υπάρχει καταγραφή του λογικού και φυσικού σχεδιασμού τους.

Για την προστασία των συστημάτων πρέπει:

- Να χρησιμοποιείται λογισμικό προστασίας από ιούς ή άλλο κακόβουλο λογισμικό και να ενημερώνεται τακτικά.
- Να απενεργοποιείται κάθε σύστημα ή λογισμικό αν δε χρησιμοποιείται.
- Να είναι ενεργές οι λειτουργίες καταγραφής και ελέγχου.
- Να υπάρχουν περιορισμοί στις ενέργειες των χρηστών του διαδικτύου.
- Να προστατεύονται αποτελεσματικά τα κρίσιμα συστήματα από κακόβουλες ενέργειες εξωτερικών ή εσωτερικών χρηστών. Προς αυτή την κατεύθυνση οφείλουν να υλοποιούνται διάφορες τεχνικές, όπως :
    - Η χρήση ειδικών συστημάτων (firewalls, filtering routers κλπ), τα οποία, ως σημεία ελέγχου των προσβάσεων, θα ρυθμίζουν και θα ελέγχουν την επικοινωνία από και προς περιοχές του δικτύου οι οποίες είναι συνήθως εκτεθειμένες σε αυξημένους κινδύνους.
    - Η δημιουργία στο δίκτυο ειδικών περιοχών (Demilitarized Zones – DMZ), ανάμεσα σε σημεία ελέγχου προσβάσεων, οι οποίες να λειτουργούν σαν απομονωμένο δίκτυο για τα προσβάσιμα από εσωτερικούς ή εξωτερικούς

χρήστες συστήματα του ΠΙ, προστατεύοντας έτσι αποτελεσματικά το υπόλοιπο δίκτυο από κακόβουλες ενέργειες.

Για την ασφάλεια της δικτυακής υποδομής και των επικοινωνιών πρέπει:

- Να ελέγχονται οι δίοδοι επικοινωνίας (gateways) με εξωτερικά δίκτυα.
- Να μην παραμένουν ανοιχτές λογικές θύρες επικοινωνίας (ports) σε κάθε συσκευή του δικτύου, αν δεν υποστηρίζουν αναγκαίες υπηρεσίες.
- Να μην παρέχεται η δυνατότητα απομακρυσμένης πρόσβασης στο δίκτυο, και όπου κρίνεται αναγκαία τέτοια πρόσβαση, να καταγράφεται και να ελέγχεται συστηματικά. Ειδικότερα, σε περίπτωση πρόσβασης στο δίκτυο χρηστών μέσω τηλεφωνικής σύνδεσης (dial up), αυτή να πραγματοποιείται κατόπιν διαδικασίας επιστροφής κλήσης (call back) ή άλλης κατάλληλης μεθόδου επαλήθευσης του καλούντος.
- Να υπάρχουν διαδικασίες και συστήματα παρακολούθησης, αποτροπής και αντιμετώπισης προσπαθειών παρείσφρησης στο δίκτυο ή γενικότερα προσπαθειών παραβίασης της ασφάλειας του δικτύου (intrusion detection/prevention systems).
- να διενεργούνται σε τακτική βάση, δοκιμαστικές απόπειρες παραβίασης της ασφάλειας του δικτύου (penetration tests), με στόχο την αξιολόγηση της επάρκειας της ασφάλειας του δικτύου.

3.1.3.4 Σχέδια Συνέχειας Εργασιών & Ανάκαμψης από Καταστροφή

Ο οργανισμός οφείλει να έχει σχέδιο σε περιπτώσεις βλάβης ή καταστροφής ώστε να συνεχίσει να λειτουργεί. Αυτά λέγονται Σχέδια Συνέχειας Εργασιών (ΣΣΕ), ή Σχέδια Ανάκαμψης από Καταστροφή (ΣΑΚ).

Πριν τη δημιουργία αυτών των σχεδίων πρέπει να γίνουν διάφορες δραστηριότητες όπως προσδιορισμός των κρίσιμων λειτουργιών, στάθμιση του λειτουργικού κόστους σε περίπτωση διακοπής ως προς το κόστος της ενεργοποίησης των ΣΣΕ και ΣΑΚ, και τέλος προσδιορισμός του χρόνου και του σημείου ανάκαμψης.

Σε βασικό επίπεδο η επιχειρησιακή συνέχεια συνίσταται στη διαχείριση των αντιγράφων ασφαλείας, στην ύπαρξη εφεδρικού υλικού και σε συσκευές παροχής αδιάλειπτης τάσης

(UPS). Ως προς τα αντίγραφα ασφαλείας πρέπει να λαμβάνονται υπ' όψιν ζητήματα όπως η συχνότητα δημιουργίας τους ως προς την κρισιμότητα των πληροφοριών, η ασφαλής φύλαξη τους, η αρχειοθέτηση του και η ανακύκλωση των μαγνητικών μέσων.

Σε δεύτερο επίπεδο, ένα ολοκληρωμένο και αποτελεσματικό ΣΣΕ και ΣΑΚ για τα Πληροφοριακά Συστήματα, πρέπει να περιλαμβάνει:

- Τη σαφή ιεραρχική δομή των στελεχών που συμμετέχουν στην εφαρμογή του, τις αρμοδιότητές τους, καθώς και τους υπεύθυνους λήψης αποφάσεων σε κάθε ομάδα έκτακτης ανάγκης.
- Τις διαδικασίες ενεργοποίησης του σχεδίου, ειδοποίησης των στελεχών και κινητοποίησης των ομάδων έκτακτης ανάγκης.
- Τους εναλλακτικούς χώρους εργασίας των χρηστών, τον εξοπλισμό που θα χρησιμοποιηθεί, καθώς και τις απαιτούμενες προδιαγραφές.
- Τις διαδικασίες εκπαίδευσης του προσωπικού σύμφωνα με τις αρμοδιότητες που αναλαμβάνουν κατά την υλοποίηση του Σχεδίου.
- Τις διαδικασίες εκτέλεσης δοκιμών όπου θα προσδιορίζεται η συχνότητα τους, οι στόχοι, η διεξαγωγή τους υπό συνθήκες που θα προσομοιώνουν έκτακτη ανάγκη, η σύνταξη έκθεσης αποτελεσμάτων και οι διορθώσεις στα σχέδια για τα προβλήματα που διορθώνονται.

Τέλος ένα Σχέδιο θα πρέπει να εξασφαλίσει την αποτελεσματική λειτουργία εναλλακτικού κέντρου που να μην επηρεάζεται από τους ίδιους κινδύνους με το κύριο κέντρο συστημάτων και να περιέχει τον κατάλληλο εξοπλισμό.

3.1.4 Έλεγχος Συστημάτων Πληροφορικής

Ο έλεγχος συστημάτων πληροφορικής πρέπει να εστιάζει στους κινδύνους που μπορεί να προκύψουν σε διάφορες φάσεις του κύκλου ζωής ενός συστήματος και να προτείνει τροποποιήσεις για καλύτερη επάρκεια των μηχανισμών ελέγχου. Επιπλέον εξετάζει αν οι μηχανισμοί ασφάλειας είναι σε συμφωνία με το νομοθετικό πλαίσιο, το επιχειρησιακό πλάνο, την πολιτική ασφάλειας του οργανισμού και τα διεθνή πρότυπα ασφάλειας.

Έτσι λοιπόν η μονάδα εσωτερικής επιθεώρησης του οργανισμού θα πρέπει:

- Να έχει επαρκή τεχνογνωσία για τη διενέργεια ελέγχων, οι οποίοι θα βασίζονται σε ανάλυση κινδύνων που έχει διενεργηθεί στα ΠΣ αλλά και σε ευρήματα προηγούμενων ελέγχων.
- Να παρακολουθεί τα θέματα που αφορούν στα ΠΣ, για να διαμορφώνει εικόνα για τους κινδύνους που υπάρχουν ή ενδέχεται να ανακύψουν.
- Να κάνει χρήση ειδικού ελεγκτικού λογισμικού.
- Να συμμετέχει στη φάση σχεδιασμού των συστημάτων για τη διαμόρφωση των κατάλληλων δικλείδων ασφαλείας, των ελεγκτικών αρχείων καταγραφής και αναφορών που παράγονται για τη διευκόλυνση του ελέγχου, καθώς και στη φάση των δοκιμών.
- Να μεριμνά σε περιπτώσεις σοβαρών προβλημάτων και περιστατικών για την άμεση και πλήρη ενημέρωση της αρμόδιας υπηρεσιακής μονάδας της Διεύθυνσης Εποπτείας Πιστωτικού Συστήματος της Τράπεζας της Ελλάδος, σύμφωνα με τις ισχύουσες διατάξεις.
- Να επικοινωνεί με τις διοικήσεις και ομάδες ελέγχου των θυγατρικών ή των δικτύων καταστημάτων εξωτερικού.
- Να μελετά, να αξιολογεί και να εφαρμόζει τα διεθνή πρότυπα και μεθοδολογίες ελέγχου Πληροφοριακών Συστημάτων.

Σε περίπτωση ύπαρξης εξωτερικού ελέγχου θα πρέπει να ξεκαθαριστεί ο ρόλος του αν είναι δηλαδή συμπληρωματικός του εσωτερικού προκειμένου να καλύψει περιπτώσεις που απαιτούν επιπλέον απαιτήσεις που δεν μπορούν να καλυφθούν ή αν θα λειτουργεί παράλληλα με τον εσωτερικό ώστε να υπάρχουν και τα δύο ανεξάρτητα ολοκληρωμένα πορίσματα.

3.2 Αρχή Προστασίας Προσωπικών Δεδομένων

Η προστασία των προσωπικών δεδομένων και της ιδιωτικής ζωής αποτελεί θεμελιώδες ανθρώπινο δικαίωμα. Ο νόμος παρέχει ορισμένα δικαιώματα στα φυσικά πρόσωπα (τα υποκείμενα των δεδομένων) και θέτει συγκεκριμένες υποχρεώσεις σε όσους τηρούν και επεξεργάζονται προσωπικά δεδομένα (τους υπευθύνους επεξεργασίας).

Η Αρχή Προστασίας Προσωπικών Δεδομένων, είναι συνταγματικά κατοχυρωμένη ανεξάρτητη διοικητική Αρχή. Ιδρύθηκε με τον Νόμο 2472/1997 «για την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα», ο οποίος ενσωματώνει στο ελληνικό δίκαιο την ευρωπαϊκή οδηγία 95/46/ΕΚ. Η οδηγία αυτή θέτει κανόνες για την προστασία των προσωπικών δεδομένων σε όλες τις χώρες μέλη της Ευρωπαϊκής Ένωσης. Η λειτουργία της Αρχής ξεκίνησε στις 10 Νοεμβρίου 1997.

3.2.1 Στόχος της Αρχής

Στόχος είναι ο σεβασμός και η προστασία της αξιοπρέπειας, της ιδιωτικής ζωής και της ελεύθερης ανάπτυξης της προσωπικότητας. Με την πάροδο του χρόνου, η τεράστια πρόοδος στον τομέα της πληροφορικής, η ανάπτυξη νέων τεχνολογιών, οι νέες μορφές διαφήμισης και ηλεκτρονικών συναλλαγών και η ανάγκη της ηλεκτρονικής οργάνωσης του κράτους έχουν σαν συνέπεια την αυξημένη ζήτηση προσωπικών πληροφοριών από τον ιδιωτικό και δημόσιο τομέα. Η ανεξέλεγκτη καταχώριση και επεξεργασία των προσωπικών δεδομένων σε ηλεκτρονικά και χειρόγραφα αρχεία υπηρεσιών, εταιρειών και οργανισμών μπορεί να προκαλέσει προβλήματα στην ιδιωτική ζωή του πολίτη.

Οι κίνδυνοι αυτοί αυξάνονται με τις νέες δυνατότητες ταχύτατης επεξεργασίας εκατομμυρίων δεδομένων μέσω ηλεκτρονικού υπολογιστή και μεταφοράς πληροφοριών παγκοσμίως μέσω του Ίντερνετ. Αποθήκευση και έρευνα μεγάλου όγκου δεδομένων που παλαιότερα θα απαιτούσε μεγάλους αποθηκευτικούς χώρους και επίπονη εργασία έχει πλέον απλοποιηθεί και γίνεται πολύ πιο εύκολα και ανέξοδα. Για την προστασία του ατόμου στην κοινωνία της πληροφορίας δεν επαρκούν οι παραδοσιακές θεσμικές εγγυήσεις και ρυθμίσεις, αλλά χρειάζεται ειδική αντιμετώπιση. Για τον σκοπό αυτό στην Ελλάδα, ιδρύθηκε με τον Νόμο 2472/1997 ως ανεξάρτητος διοικητικός φορέας η Αρχή Προστασίας Προσωπικών Δεδομένων, η οποία λειτουργεί από τον Νοέμβριο του 1997. Άλλες αρχές που εποπτεύουν την επεξεργασία προσωπικών δεδομένων είναι στην Ελλάδα η Αρχή Διασφάλισης Απορρήτου των Επικοινωνιών και στην Ευρώπη ο Ευρωπαίος Επόπτης Προστασίας Δεδομένων.

3.2.2 Προστασία Προσωπικών Δεδομένων σε Τραπεζικά Ιδρύματα

Στη σημερινή εποχή σχεδόν όλα μπορούν να αγοραστούν με πίστωση. Η χρήση των πιστωτικών καρτών διευκόλυνε την αύξηση της κατανάλωσης και του βιοτικού επιπέδου ζωής των χρηστών, αλλά είχε και σοβαρές συνέπειες για μεγάλο αριθμό καταναλωτών, οι οποίοι δεν ήταν σε θέση να αποπληρώσουν τα χρέη τους, με αποτέλεσμα να καταχωρούνται σε δυσμενείς λίστες οικονομικής συμπεριφοράς. Περαιτέρω, οι τράπεζες είναι σε θέση, με διασταύρωση στοιχείων που παίρνουν από τους ίδιους τους πελάτες τους, αλλά και από αρχεία οικονομικών πληροφοριών, να δημιουργήσουν το προφίλ των πελατών τους. Αυτή η μεγάλη συγκέντρωση πληροφοριών, σε συνδυασμό με τη μη σωστή ενημέρωση, ελλοχεύει κινδύνους για τα προσωπικά δεδομένα των προσώπων.

Οι τράπεζες οφείλουν να γνωστοποιούν τα αρχεία τους στην Αρχή. Πρέπει ακόμα να ενημερώνουν τα υποκείμενα των δεδομένων για το σκοπό επεξεργασίας των στοιχείων τους, από πού αντλούν τα στοιχεία τους, πού τα διαβιβάζουν (δηλαδή τους αποδέκτες, όπως είναι οι εταιρίες ενημέρωσης οφειλετών ή η ΤΕΙΡΕΣΙΑΣ Α.Ε.), και για τα δικαιώματα που τους παρέχει ο ν.2472/1997.

3.2.3 Προστασία Προσωπικών Δεδομένων στην ΤΕΙΡΕΣΙΑΣ Α.Ε.

Το Σύστημα Πληροφοριών της ΤΕΙΡΕΣΙΑΣ Α.Ε. αποτελεί μια κεντρική βάση δεδομένων με σκοπό τη συγκέντρωση και διάθεση στα χρηματοπιστωτικά ιδρύματα οικονομικών πληροφοριών με σκοπό επεξεργασίας την ελαχιστοποίηση των κινδύνων από τη σύναψη πιστωτικών συμβάσεων με αφερέγγυους πελάτες και, εν γένει, από τη δημιουργία επισφαλών απαιτήσεων. Τα σημαντικότερα αρχεία της ΤΕΙΡΕΣΙΑΣ παρουσιάζονται παρακάτω όπου το κάθε είδος έχει διαφορετική αντιμετώπιση ως προς την προστασία των δεδομένων σε συνάρτηση με την σοβαρότητα της πληροφορίας:

- Σύστημα Αθέτησης Υποχρεώσεων ΣΑΥ:

  Στο σύστημα τηρούνται δεδομένα, τα λεγόμενα δεδομένα της «μαύρης λίστας», δηλαδή δεδομένα που αφορούν ακάλυπτες επιταγές, απλήρωτες συναλλαγματικές, καταγγελίες συμβάσεων χορηγήσεων, διαταγές πληρωμής, προγράμματα πλειστηριασμών, κατασχέσεις και επιταγές του Ν.Δ.1923, πτωχεύσεις κ.ά. Τα δεδομένα τηρούνται χωρίς τη συγκατάθεση των υποκειμένων, μετά από ενημέρωση δια του Τύπου (απόφαση 24/2004 της Αρχής), για χρονικό διάστημα ανάλογα με το είδος τους.

- Σύστημα Συγκέντρωσης Χορηγήσεων ΣΣΧ:

Στο σύστημα αυτό εμπεριέχονται προσωπικά δεδομένα της «λευκής λίστας» σχετικά με προσωπικά, καταναλωτικά, ανοικτά και στεγαστικά δάνεια, υπεραναλήψεις και κάρτες. Σύμφωνα με τον πρόσφατο Νόμο 3746/2009 (άρθρο 70 παρ. 2) τροποποιήθηκε η απόφαση 86/2002 της Αρχής και τα δεδομένα του αρχείου διαβιβάζονται πλέον στην ΤΕΙΡΕΣΙΑΣ από τα πιστωτικά ιδρύματα στο σύνολό τους χωρίς τη συγκατάθεση των υποκειμένων. Η πρόσβαση των τραπεζών στο σύστημα γίνεται μετά από συγκατάθεση του πελάτη/υποψηφίου δανειολήπτη.

- Σύστημα Βαθμολόγησης Οικονομικής Συμπεριφοράς:

Είναι ένα σύστημα που αναπτύσσει η ΤΕΙΡΕΣΙΑΣ και αξιολογείται από κοινού με τα λοιπά κριτήρια που η τράπεζα χρησιμοποιεί στο εσωτερικό σύστημα αξιολόγησης και πιστοληπτικής διαβάθμισης (credit scoring). Σκοπός της επεξεργασίας είναι η μέτρηση της πιθανότητας αθέτησης της υποχρέωσης προς τις τράπεζες, η οποία αποτελεί βασικό στοιχείο για τον υπολογισμό του πιστωτικού κινδύνου. Στοιχεία βαθμολόγησης διαβιβάζονται μόνο στην τράπεζα που έχει την αίτηση του ενδιαφερόμενου και τη σχετική συγκατάθεση και δεν τηρούνται στο σύστημα μετά τη λειτουργία της δανειοδότησης ούτε ανακοινώνονται σε άλλους συμμετέχοντες στο σύστημα χωρίς ξεχωριστή συγκατάθεση.

- Σύστημα Ταυτοτήτων/Διαβατηρίων ΣΤΔ:

Λειτουργεί από το 2000 με σκοπό επεξεργασίας την προστασία των υποκειμένων από πιθανή απάτη λόγω απώλειας της ταυτότητας ή του διαβατηρίου τους. Με την απόφαση 11/2006 της Αρχής εγκρίθηκε πρόσφατα η διαβίβαση στην ΤΕΙΡΕΣΙΑΣ των αντίστοιχων στοιχείων από το αρχείο της Ελληνικής Αστυνομίας με on-line σύνδεση.

3.3 Πρότυπο PCI DSS

3.3.1: Εισαγωγή

Το Πρότυπο Ασφάλειας Δεδομένων (Data Security Standard – DSS) της Βιομηχανίας Πληρωμών με Κάρτα (Payment Card Industry – PCI) αναπτύχθηκε για να αναβαθμίσει και να εμπλουτίσει την ασφάλεια δεδομένων στις κάρτες πληρωμών και για να διευκολύνει την ευρεία και παγκόσμια αποδοχή συνεπών μεταξύ τους μέτρων ασφαλείας.

Το PCI DSS παρέχει ένα υπόβαθρο τεχνικών και επιχειρησιακών απαιτήσεων, σχεδιασμένο να προστατεύει τα δεδομένα των καρτών. Επίσης, εφαρμόζεται σε (και από) όλες τις οντότητες που συμμετέχουν με οιονδήποτε τρόπο στην επεξεργασία των καρτών, όπως εμπορικών επιχειρήσεων, διεκπεραιωτών, αγοραστών, εκδοτών, καθώς και άλλων οντοτήτων που αποθηκεύουν, επεξεργάζονται ή μεταδίδουν δεδομένα που αφορούν κάρτες. Επίσης, το PCI DSS περιέχει ένα ελάχιστο σύνολο απαιτήσεων για την προστασία των δεδομένων των καρτών, αλλά μπορεί και να εμπλουτιστεί από επιπλέον στοιχεία και πρακτικές για την περαιτέρω εξάλειψη των κινδύνων.

Οι απαιτήσεις που θέτει το PCI DSS είναι δώδεκα και χωρίζονται σε 6 κατηγορίες:

- <u>Δημιουργία και διατήρηση ενός ασφαλούς δικτύου</u>

  1. Εγκαθίδρυση και συντήρηση ρυθμίσεων που θα προστατεύουν τα δεδομένα των καρτών
  2. Αποφυγή χρησιμοποίησης κωδικών και άλλων παραμέτρων ασφαλείας, που παρέχει η εταιρεία παραγωγής του εξοπλισμού και του λογισμικού.

- <u>Προστασία των Δεδομένων των καρτών</u>

  3. Προστασία αποθηκευμένων δεδομένων καρτών
  4. Κρυπτογράφηση κατά τη μετάδοση δεδομένων καρτών πάνω από ανοιχτά, δημόσια δίκτυα

- <u>Εφαρμογή προγράμματος διαχείρισης ευπαθειών</u>

  5. Χρήση και συχνή ενημέρωση λογισμικού ασφαλείας
  6. Ανάπτυξη και διατήρηση ασφαλών συστημάτων και εφαρμογών

- <u>Εφαρμογή μέτρων αυστηρού ελέγχου πρόσβασης</u>

  7. Περιορισμός στην πρόσβαση στα δεδομένων των καρτών
  8. Απόδοση ενός μοναδικού αναγνωριστικού (ID) σε κάθε πρόσωπο με πρόσβαση σε υπολογιστή
  9. Περιορισμός σε φυσικό επίπεδο της πρόσβασης στα δεδομένων των καρτών

- <u>Τακτικός έλεγχος και δοκιμές του δικτύου και συνεχής παρακολούθηση</u>

10. Παρακολούθηση όλων των προσβάσεων στους πόρους του δικτύου και στα δεδομένα των καρτών
11. Τακτική δοκιμή της ασφάλειας των συστημάτων και των διεργασιών

- Εφαρμογή και διατήρηση πολιτικής για την ασφάλεια των Πληροφοριακών συστημάτων

12. Διατήρηση πολιτικής ασφαλείας που καθορίζει την ασφάλεια των πληροφοριών για όλο το προσωπικό.

3.3.2: Εφαρμοσιμότητα του PCI DSS

Το PCI DSS εφαρμόζεται οπουδήποτε δεδομένα λογαριασμών αποθηκεύονται, υπόκεινται σε επεξεργασία ή μεταδίδονται. Τα δεδομένα των λογαριασμών είναι τα δεδομένα των καρτών και τα ευαίσθητα δεδομένα αυθεντικοποίησης. Πιο συγκεκριμένα, αυτά περιλαμβάνουν:

Δεδομένα καρτών:

- Πρωτεύων Αριθμός Λογαριασμού (Primary Account Number – PAN)
- Όνομα κατόχου κάρτας
- Ημερομηνία Λήξης
- Κωδικός Υπηρεσίας (Service Code)

Ευαίσθητα Δεδομένα Αυθεντικοποίησης

- Πλήρως μαγνητισμένη κάρτα ή αντίστοιχό της σε chip
- CAV2/CVC2/CVV2/CID
- PINs/PIN blocks

Ο PAN είναι ο παράγοντας που καθορίζει την εφαρμοσιμότητα των απαιτήσεων του PCI DSS. Αυτές είναι εφαρμόσιμες μόνα αν το PAN αποθηκεύεται, υπόκειται σε επεξεργασία ή μεταδίδεται. Αν δεν γίνεται τίποτα από αυτά, τότε οι απαιτήσει του PCI DSS δεν εφαρμόζονται

Αν το όνομα του κατόχου της κάρτας, η ημερομηνία λήξης και/ή ο κωδικός υπηρεσίας αποθηκεύονται, υπόκειται σε επεξεργασία ή μεταδίδεται μαζί με το PAN ή,

εναλλακτικά, είναι παρόντα στο περιβάλλον των δεδομένων των καρτών, τότε πρέπει να προστατεύονται σύμφωνα με τις απαιτήσεις του PCI DSS.

Η χρήση μίας συμβατής με το PA-DSS εφαρμογής από μία οντότητα δεν την κάνει αυτόματα συμβατή με το PCI DSS, μιας και η εφαρμογή πρέπει να υλοποιηθεί μέσα σε ένα συμβατό με το PCI DSS περιβάλλον και σύμφωνα με τον Οδηγό Υλοποίησης του PA-DSS. Οι απαιτήσεις του Προτύπου Ασφάλειας Δεδομένων στις Εφαρμογές Πληρωμών (Payment Application Data Security Standard – PA-DSS) προκύπτουν από τις διευκολύνσεις που πρέπει να παρέχει μία εφαρμογή πληρωμών, ώστε να εξυπηρετεί κάποιον χρήστη, που τηρεί τις απαιτήσεις του PCI DSS.

Οι ασφαλείς εφαρμογές πληρωμών, όταν υλοποιούνται σε ένα συμβατό με το PCI DSS περιβάλλον, ελαχιστοποιούν τους πιθανούς κινδύνους που μπορεί να προκύψουν. Το PA-DSS εφαρμόζεται από τους δημιουργούς εφαρμογών σε εκείνες τις εφαρμογές που αποθηκεύουν, επεξεργάζονται ή μεταδίδουν δεδομένα καρτών, ως κομμάτι της αυθεντικοποίησης.

3.3.3: Συμμόρφωση με τις απαιτήσεις του PCI DSS

Οι απαιτήσεις ασφαλείας του PCI DSS εφαρμόζονται σε όλες τις συνιστώσες του συστήματος. Στο PCI DSS, με τον όρο “συνιστώσες συστήματος” εννοούμε κάθε κομμάτι του δικτύου, κάθε server ή εφαρμογή που περιλαμβάνεται ή συνδέεται με το περιβάλλον των δεδομένων των καρτών. Επίσης, μπορεί να περιλαμβάνονται εικονικές συσκευές, όπως routers και switches, εφαρμογές, κτλ.

Το περιβάλλον δεδομένων καρτών συνίσταται από ανθρώπους, διαδικασίες και τεχνολογίες που αποθηκεύουν, επεξεργάζονται ή μεταδίδουν δεδομένα καρτών ή ευαίσθητα δεδομένα αυθεντικοποίησης. Ο δικτυακός εξοπλισμός περιλαμβάνει firewalls, μεταγωγείς, δρομολογητές, ασύρματα σημεία πρόσβασης κ.α. Επίσης, όσον αφορά τους servers, υπάρχουν web, εφαρμογών, βάσεων δεδομένων, αυθεντικοποίησης, ηλεκτρονικού ταχυδρομείου, proxy, DNS κτλ.

Το πρώτο βήμα αποτίμησης κάθε PCI DSS είναι ο χρονικός καθορισμός των αξιολογήσεών του. Τουλάχιστον μία φορά το χρόνο και πριν την ετήσια αποτίμηση, θα πρέπει να αξιολογείται η συγκεκριμένη οντότητα, όσον αφορά τη συμμόρφωσή της με τις απαιτήσεις του PCI DSS. Για να επιβεβαιώσουμε την ακρίβεια και την καταλληλότητα του εύρους εφαρμογής του PCI DSS πρέπει να εκτελέσουμε τα ακόλουθα:

- Η αξιολογούμενη οντότητα θα πρέπει να ελέγξει και να καταγράψει την ύπαρξη δεδομένων καρτών στο περιβάλλον της και να εξακριβωθεί ότι κανένα δεδομένο καρτών δε βρίσκεται εκτός του καθορισμένου περιβάλλοντος δεδομένων καρτών (Cardholder Data Environment – CDE)
- Όταν η προηγούμενη διαδικασία εφαρμοστεί σε όλες τις οντότητες, η κάθε οντότητα χρησιμοποιεί τα αποτελέσματα για να επιβεβαιώσει ότι το εύρος εφαρμογής του PCI DSS είναι το κατάλληλο
- Η κάθε οντότητα θεωρεί ότι όλα τα δεδομένα καρτών που βρίσκονται εντός του εύρους εφαρμογής του PCI DSS, είναι μέρος του CDE
- Η κάθε οντότητα διατηρεί τεκμηριώσεις που αποδεικνύουν πώς το εύρος εφαρμογής του PCI DSS επιβεβαιώθηκε, ώστε να υπάρχει δυνατότητας εκ των υστέρων αναφοράς και ελέγχου.

Κατάτμηση Δικτύου

Η κατάτμηση δικτύου (network segmentation), δηλαδή η διαδικασία κατά την οποία τα δεδομένα των καρτών απομονώνονται από το υπόλοιπο της οντότητας, δεν είναι μέρος κάποιας απαίτησης του PCI DSS. Ωστόσο, είναι μία μέθοδος η οποία χρησιμοποιείται για να ελαχιστοποιηθούν τα ακόλουθα:

- Το εύρος εφαρμογής του PCI DSS
- Το κόστος του PCI DSS
- Το κόστος και η δυσκολία υλοποίησης και συντήρησης μονάδων ελέγχου του PCI DSS
- Οι κίνδυνοι.

Χωρίς κατάλληλη κατάτμηση δικτύου, το εύρος εφαρμογής του PCI DSS είναι όλο το δίκτυο. Επιτυγχάνεται με τη χρήση φυσικών συσκευών, όπως routers και firewalls, είτε με τη χρήση άλλων τεχνολογιών περιορισμού πρόσβασης. Απαραίτητο προαπαιτούμενο για την ελάττωση του μεγέθους του CDE είναι η βαθιά κατανόηση των αναγκών, αλλά και των διαδικασιών που σχετίζονται με την αποθήκευση, την επεξεργασία ή τη μετάδοση των δεδομένων των καρτών. Ο περιορισμός των σημείων όπου γίνεται η αποθήκευση

των δεδομένων, ίσως απαιτήσει τον επανασχεδιασμό πρακτικών που εφαρμόζονταν καιρό στον οργανισμό.

Χρήση ασύρματων δικτύων

Αν γίνεται χρήση ασύρματων τεχνολογιών για την αποθήκευση, επεξεργασία ή μετάδοση των δεδομένων των καρτών ή υπάρχουν ασύρματα δίκτυα που συνδέονται άμεσα με ή είναι μέρη του CDE, πρέπει να εφαρμόσουμε τις οδηγίες του PCI DSS που αφορούν τα ασύρματα δίκτυα.

Εξωτερικοί Συνεργάτες - Outsourcing

Οι παροχείς τεχνικών υπηρεσιών στο CDE που δεν ανήκουν στον οργανισμό, απαιτείται να υπόκεινται σε ετήσια αξιολόγηση, όσον αφορά τη συμμόρφωσή τους με τις απαιτήσεις του PCI DSS. Αυτό γίνεται επειδή μπορεί να υπάρχουν επιπτώσεις στην ασφάλεια του CDE, λόγω της συμμετοχής τρίτων μερών στις λειτουργίες που αφορούν την διατήρηση δεδομένων καρτών.

Σε αυτές τις περιπτώσεις πρέπει να υπάρχει σαφής καταγραφή του ρόλου του κάθε συνεργάτη σε μία Αναφορά Συμμόρφωσης (Report of Compliance – ROC), όπου εκεί θα αναλύονται οι απαιτήσεις που αφορούν τον συνεργάτη και εκείνες που αφορούν την οντότητα. Για να γίνει αυτό, υπάρχουν δύο επιλογές: είτε ο εξωτερικός συνεργάτης να υλοποιήσει από μόνος του μία αξιολόγηση για τη συμμόρφωση του με τις απαιτήσεις του PCI DSS, είτε, αν δεν το πράξει ο ίδιος, να αξιολογηθεί από τον ίδιο τον οργανισμό μας.

Δειγματοληπτικός έλεγχος στοιχείων του οργανισμού

Ο δειγματοληπτικός έλεγχος στοιχείων του οργανισμού δεν είναι απαίτηση του PCI DSS. Ωστόσο, λαμβάνοντας υπόψη το εύρος εφαρμογής του PCI DSS, καθώς και την πολυπλοκότητα του, ο αξιολογητής μπορεί να διαλέξει κάποια στοιχεία και να ελέγχει την υιοθέτηση των απαιτήσεων του PCI DSS. Η επιλογή, όμως, των αξιολογούμενων συστατικών δεν είναι τυχαία. Πρέπει να είναι αντιπροσωπευτικά όλων των τύπων και από όλες τις σχετιζόμενες υπηρεσίες του οργανισμού.
Κατά τον δειγματοληπτικό έλεγχο ο αξιολογητής θα πρέπει:

- Να δικαιολογήσει το μέγεθος της αξιολόγησης και τη λογική με την οποία επέλεξε τα απολογηθέντα στοιχεία
- Να καταγράψει την προτυποποιημένη PCI DSS διαδικασία που ακολούθησε

- Να εξηγήσει γιατί τα επιλεχθέντα στοιχεία θεωρούνται κατάλληλα και αντιπροσωπευτικά.

3.3.4: Ανάλυση των απαιτήσεων του PCI DSS

Στην παράγραφο 3.1 αναφέραμε τις 12 απαιτήσεις που θέτει το PCI DSS. Σε αυτήν την παράγραφο θα αναλύσουμε σε περισσότερο βάθος κάθε απαίτηση ξεχωριστά και θα παραθέσουμε αναλυτικά όλα τα βήματα που απαιτούνται για την εκπλήρωσή της.

Απαίτηση 1η: Εγκαθίδρυση και συντήρηση ρυθμίσεων που θα προστατεύουν τα δεδομένα των καρτών

Ένα firewall ελέγχει όλη τη δικτυακή κίνηση και απορρίπτει όποιο είδος κίνησης δεν συμβαδίζει με τα ορισμένα κριτήρια ασφαλείας. Όλα τα συστήματα πρέπει να είναι προστατευμένα από μη εξουσιοδοτημένη πρόσβαση που προέρχεται από μη ασφαλή δίκτυα. Έτσι, είτε πρόκειται για συσκευές firewall, είτε πρόκειται για συσκευές που επιτελούν παρόμοια λειτουργία, υπόκεινται στις απαιτήσεις της πρώτης απαίτησης:

1.1: Υλοποίηση των παραμετροποιήσεων των firewall και των router που περιλαμβάνουν τα ακόλουθα:

1.1.1: Επίσημη διαδικασία επιβεβαίωσης και δοκιμής όλων των δικτυακών συνδέσεων, καθώς και ενδεχόμενων αλλαγών

1.1.2: Πλήρες διάγραμμα της υφιστάμενης κατάστασης του δικτύου, που περιλαμβάνει όλες τις συνδέσεις στα δεδομένα των καρτών, συμπεριλαμβανομένων και των ασύρματων συνδέσεων.

1.1.3: Απαιτήσεις του firewall για κάθε σύνδεση στο Internet και για τη σύνδεση της DMZ με το εσωτερικό δίκτυο.

1.1.4: Περιγραφή των ομάδων, των ρόλων και των ευθυνών κάθε δικτυακού συστατικού

1.1.5: Καταγραφή όλων των services, πρωτοκόλλων και επιτρεπόμενων ports και σαφής δικαιολόγηση της χρησιμοποίησής τους.

1.1.6: Απαίτηση να επανελέγχεται το σύνολο των κανόνων του router και του firewall τουλάχιστον ανά εξάμηνο.

1.2: Υλοποίηση παραμετροποιήσεων των router και των firewall που περιορίζουν τις συνδέσεις μεταξύ μη εμπιστεύσιμων δικτύων και του CDE.

1.2.1: Περιορισμός εισερχόμενης και εξερχόμενης κίνησης, σε σημείο να επιτρέπεται μόνο η απολύτως απαραίτητη κίνηση.

1.2.2: Ασφάλιση και συγχρονισμός των αρχείων παραμετροποίησης των routers

1.2.3: Εγκατάσταση περιμετρικών firewalls μεταξύ κάθε ασύρματου δικτύου και του CDE, έτσι ώστε να απορρίπτεται ή να ελέγχεται όλη η κίνηση από αυτά.

1.3: Απαγόρευση απευθείας επικοινωνίας μεταξύ του Internet και των στοιχείων του CDE.

1.3.1: Υλοποίηση αποστρατικοποιημένης ζώνης (DMZ) για τον περιορισμό της εισερχόμενης κίνησης μόνο στα συστήματα τα οποία παρέχουν υπηρεσίες μετά από αυθεντικοποίηση.

1.3.2: Περιορισμός της εκ των έσω κίνησης προς το Internet, ώστε να ανακατευθύνονται προς IP διευθύνσεις εντός της DMZ.

1.3.3: Αποτρέπεται οποιαδήποτε απευθείας σύνδεση μεταξύ πόρων στο Internet και του CDE

1.3.4: Αποτρέπεται εσωτερικές IP διευθύνσεις να περνάνε από το Internet στην DMZ.

1.3.5: Αποτρέπεται μη εξουσιοδοτημένη πρόσβαση από το CDE στο Internet.

1.3.6: Υλοποίηση δυναμικού φιλτραρίσματος πακέτων, που σημαίνει ότι επιτρέπονται μόνο εγκατεστημένες συνδέσεις από και προς το δίκτυό μας.

1.3.7: Τοποθέτηση του εξοπλισμού όπου φυλάσσονται τα δεδομένα των καρτών σε κάποιο σημείο του εσωτερικού δικτύου, απομονωμένο από την DMZ και άλλα μη ασφαλή δίκτυα.

1.3.8: Απόκρυψη των εσωτερικών, ιδιωτικών IP διευθύνσεων και των δεδομένων δρομολόγησης σε μη εξουσιοδοτημένες οντότητες.

1.4: Εγκατάσταση προσωπικού λογισμικού firewall σε κάθε φορητό ή μη υπολογιστή, που έχει σύνδεση στο Internet.

<u>Απαίτηση 2η: Αποφυγή χρησιμοποίησης κωδικών και άλλων παραμέτρων ασφαλείας, που παρέχει η εταιρεία παραγωγής του εξοπλισμού και του λογισμικού.</u>

Κακόβουλοι χρήστες, εντός και εκτός ενός οργανισμού, συχνά χρησιμοποιούν τους default κωδικούς και άλλες default παραμετροποιήσεις στην προσπάθειά τους να

εισβάλουν σε ένα σύστημα. Αυτές οι default παράμετροι είναι ευρέως γνωστές και μπορούν εύκολα να έλθουν εις γνώση του επιτιθέμενου.

Απαιτήσεις:

2.1: Πάντα αλλάζουμε τις default παραμέτρους (passwords, accounts, κτλ), με τις οποίες ο εξοπλισμός ή το λογισμικό που αγοράζουμε είναι προ-ρυθμισμένος, πριν τα εγκαταστήσουμε και πριν τα συνδέσουμε στο δίκτυο μας.

2.1.1: Σε ασύρματα δίκτυα που συνδέονται στο CDE ή μεταδίδουν δεδομένα από και προς το CDE, αλλάζουμε όλα τα default, όπως κλειδιά κρυπτογράφησης, SSID, κωδικούς κτλ.

2.2: Ανάπτυξη προτύπων παραμετροποίησης για όλες τις συσκευές του δικτύου. Επιβεβαίωση ότι αυτές οι παραμετροποιήσεις αντιμετωπίζουν όλες τις γνωστές ευπάθειες και ότι είναι συμβατές με την πολιτική ασφαλείας του οργανισμού.

2.2.1: Σε κάθε server αποδίδουμε μόνο ένα ρόλο, ώστε να αποφεύγουμε πολλαπλές λειτουργίες και, σαν αποτέλεσμα αυτού, ενδεχόμενα διαφορετικά επίπεδα ασφαλείας.

2.2.2: Ενεργοποίηση μόνο τω απαραίτητων για την λειτουργία του συστήματος services, πρωτόκολλα κτλ.

2.2.3: Παραμετροποιούμε τις επιλογές ασφαλείας των συστημάτων, για να αποφεύγουμε λανθασμένους χειρισμούς από τους χρήστες.

2.2.4: Αφαίρεση όλων των αχρείαστων λειτουργιών, όπως scripts, drivers, περιττά χαρακτηριστικά προγραμμάτων κτλ.

2.3: Χρήση κρυπτογράφησης σε όλες τις μεθόδους που χρησιμοποιεί ο διαχειριστής μιας συσκευής, πλην της μεθόδου σύνδεσης με κονσόλα. Χρήση τεχνολογιών, όπως το SSH, το VPN, το SSL/TLS, κ.α.

2.4: Οι πάροχοι κοινών τόπων αποθήκευσης, όπως πχ cloud, πρέπει να ικανοποιούν συγκεκριμένες πρακτικές ασφαλείας.

Απαίτηση 3η: Προστασία αποθηκευμένων δεδομένων καρτών

Μέθοδοι προστασίας, όπως κρυπτογράφηση, κατακερματισμός κ.α., είναι απαραίτητές για την προστασία των δεδομένων των καρτών. Αν κάποιος εισβολέας καταστρατηγήσει κάποιες άλλες μεθόδους και αποκτήσει πρόσβαση στα

κρυπτογραφημένα δεδομένα, χωρίς όμως να κατέχει τα κλειδιά κρυπτογράφησης, θα πρέπει να μην μπορεί να διαβάσει αυτά τα δεδομένα.

Απαιτήσεις:

3.1: Προσπαθούμε να περιορίσουμε όσο το δυνατόν περισσότερο την αποθήκευση των δεδομένων, εφαρμόζοντας πολιτικές όπως:

3.1.1: Εφαρμογή πολιτικών συνοχής και διάθεσης όπως:

- Περιορισμός αποθηκευμένου όγκου δεδομένων και χρόνου διατήρησης των αποθηκευμένων δεδομένων, σύμφωνα με τις νομικές και κανονιστικές διατάξεις και σύμφωνα με τις επιχειρησιακές απαιτήσεις
- Διαδικασίες για ασφαλή διαγραφή δεδομένων, όταν δεν χρειάζονται πια
- Αυτόματες (ανά τρίμηνο) ή χειροκίνητες διαδικασίες, στις οποίες διαγράφονται δεδομένα καρτών που έχουν ξεπεράσει τα χρονικά όρια διατήρησής τους.

3.2: Αποφυγή αποθήκευσης ευαίσθητων δεδομένων αυθεντικοποίησης μετά τη φάση της εξουσιοδότησης.

3.2.1: Δεν αποθηκεύουμε δεδομένα που βρίσκονται στη μαγνητική ταινία της κάρτας ή στο chip της κάρτας

3.2.2: Δεν αποθηκεύουμε τον κωδικό επιβεβαίωσης της κάρτας ή τον κωδικό που χρησιμοποιείται σε συναλλαγές που δεν εμφανίζεται η κάρτα στην απτή της μορφή

3.2.3: Δεν αποθηκεύουμε το PIN ή το κρυπτογραφημένο PIN block

3.3: Όταν χρειάζεται να εμφανίζουμε το PAN καλύπτουμε τα ψηφία, αφήνοντας μόνο τα 6 πρώτα και τα 4 τελευταία

3.4: Κάνουμε το PAN να μην διαβάζεται οπουδήποτε και αν το αποθηκεύουμε.

3.4.1: Αν χρησιμοποιείται κρυπτογράφηση δίσκων, η λογική πρόσβαση πρέπει να είναι ανεξάρτητη από την πρόσβαση στο λειτουργικό σύστημα, ενώ τα κλειδιά αποκρυπτογράφησης δεν πρέπει να συνδέονται με λογαριασμούς χρηστών

3.5: Προστασία από αποκάλυψη ή λανθασμένη και κακόβουλη χρήση όλων των κλειδιών που χρησιμοποιούνται για την ασφάλεια των δεδομένων των καρτών

3.5.1: Περιορισμός πρόσβασης στα κρυπτογραφικά κλειδιά σε όσο το δυνατόν λιγότερα άτομα

3.5.2: Ασφαλής αποθήκευση των κρυπτογραφικών κλειδιών σε όσο το δυνατόν λιγότερα μέρη και σε όσο το δυνατόν λιγότερες μορφές

3.6: Πλήρης καταγραφή και εφαρμογή όλων των διεργασιών διαχείρισης των κλειδιών και των διαδικασιών κρυπτογράφησης των δεδομένων των καρτών

3.6.1: Δημιουργία ισχυρών κρυπτογραφικών κλειδιών

3.6.2: Ασφαλής διαμοιρασμός κρυπτογραφικών κλειδιών

3.6.3: Ασφαλής αποθήκευση κρυπτογραφικών κλειδιών

3.6.4: Αλλαγή των κρυπτογραφικών κλειδιών που έχουν φτάσει στο τέλος της περιόδου χρήσης τους

3.6.5: Κατάργηση ή αλλαγή των κλειδιών που η ακεραιότητά τους έχει κλονιστεί

3.6.6: Παρεμπόδιση της μη εξουσιοδοτημένης αντικατάστασης των κρυπτογραφικών κλειδιών

3.6.7: Οι διαχειριστές, οι δημιουργοί και οι γνώστες των κλειδιών πρέπει επισήμως να αναγνωρίζουν τις ευθύνες που φέρουν για τη διαφύλαξη της μυστικότητάς τους.

Απαίτηση 4η: Κρυπτογράφηση κατά τη μετάδοση δεδομένων καρτών πάνω από ανοιχτά, δημόσια δίκτυα

Οι ευαίσθητες πληροφορίες πρέπει να μεταδίδονται κρυπτογραφημένες πάνω από δίκτυα τα οποία είναι εύκολα προσβάσιμα από κακόβουλους χρήστες. Κακώς παραμετροποιημένα ασύρματα δίκτυα και οι ευπάθειες σε παλαιές μεθόδους κρυπτογράφησης και πρωτόκολλα αυθεντικοποίησης εξακολουθούν να είναι στόχοι επιθέσεων από άτομα τα οποία εκμεταλλεύονται αυτές τις ευπάθειες για να αποκτούν πρόσβαση υψηλού επιπέδου στα CDE.

4.1: Χρησιμοποίηση ισχυρής κρυπτογραφίας και πρωτοκόλλων ασφαλείας για τη διασφάλιση των ευαίσθητων δεδομένων των καρτών, κατά τη μετάδοσή τους πάνα από ανοιχτά, δημόσια δίκτυα

4.1.1: Διασφάλιση των ασύρματων δικτύων που μεταδίδουν δεδομένα καρτών ή είναι συνδεδεμένα στο CDE, χρησιμοποιώντας τα καλύτερα πρότυπα κρυπτογράφησης και αυθεντικοποίησης.

4.2: Δεν αποστέλλουμε ποτέ μη προστατευμένα PAN χρησιμοποιώντας λογισμικά συνομιλίας (messengers κτλ)

Απαίτηση 5η: Χρήση και συχνή ενημέρωση λογισμικού ασφαλείας

Το κακόβουλο λογισμικό (malware) περιλαμβάνει ιούς, σκουλήκια, δούρειους ίππους κ.α. Εισέρχεται στο δίκτυο μας μέσα από ενέργειες οι οποίες είναι, εν γένει, επιτρεπόμενες από εμάς. Τέτοιοι τρόποι είναι το e-mail, το Internet, USB sticks κτλ. Για αυτό το λόγο πρέπει να χρησιμοποιείται λογισμικό antivirus σε όλα τα συστήματα, ώστε αυτά να προστατεύονται από αυτές τις επικίνδυνες επιθέσεις.

5.1: Εγκατάσταση λογισμικού antivirus σε όλα τα συστήματα τα οποία συχνά προσβάλλονται από κακόβουλο λογισμικό.

5.1.1: Εξασφάλιση ότι το λογισμικό antivirus είναι σε θέση να προστατεύει από το κακόβουλο λογισμικό και επίσης να εντοπίζει και να εξαλείφει όλους τους κινδύνους που προκύπτουν από αυτό.

5.2: Διασφάλιση ότι όλοι οι μηχανισμοί antivirus είναι ενεργοί, πλήρως ενημερωμένοι και παράγουν αρχεία γεγονότων (logs).

Απαίτηση 6η: Ανάπτυξη και διατήρηση ασφαλών συστημάτων και εφαρμογών

Οι κακόβουλοι χρήστες χρησιμοποιούν τα κενά ασφαλείας για να αποκτήσουν πρόσβαση με υψηλά δικαιώματα στα συστήματα του οργανισμού. Πολλές από αυτές τις ευπάθειες λύνονται με βελτιωτικές εκδόσεις των προγραμμάτων ασφαλείας ή με συμπλήρωση και βελτίωση των ήδη υπαρχουσών, από τους ίδιους τους κατασκευαστές, τα λεγόμενα patches. Όλα τα συστήματα πρέπει να έχουν πάντα την τελευταία έκδοση του προγράμματος, συνοδευόμενο από τα απαραίτητα patches, ώστε να προστατεύεται ο οργανισμός από τους επιτιθέμενους.

6.1: Διασφάλιση ότι όλα τα συστήματα και το λογισμικό είναι προστατευμένα από όλες τις γνωστές ευπάθειες, έχοντας εγκατεστημένα όλα τα τελευταία patches ασφαλείας.

6.2: Δημιουργία διαδικασίας που θα αναγνωρίζει, θα εκτιμά και θα αξιολογεί τους νέους κινδύνους και τις νέες ευπάθειες που ανακαλύπτονται.

6.3: Ανάπτυξη εφαρμογών, εσωτερικών και εξωτερικών, που θα συνάδουν με τις απαιτήσεις του PCI DSS και με τις σύγχρονες, βέλτιστες πρακτικές του χώρου.

6.3.1: Αφαίρεση των λογαριασμών, των IDs των χρηστών και των κωδικών που φτιάχτηκαν από εμάς, πριν δοθεί η εφαρμογή στους χρήστες.

6.3.2: Επανέλεγχος του κώδικα που φτιάχτηκε από εμάς πριν αυτός δοθεί στους χρήστες, με σκοπό να εντοπιστούν πιθανές ευπάθειες.

6.4: Εφαρμογή διαδικασιών αλλαγής ελέγχου

6.4.1: Διαφορετικό περιβάλλον ανάπτυξης/δοκιμών και διαφορετικό περιβάλλον χρήσης

6.4.2: Διαχωρισμός καθηκόντων μεταξύ των περιβαλλόντων ανάπτυξης/δοκιμής και χρήσης.

6.4.3: Δεδομένα από το περιβάλλον χρήσης (υπαρκτά PAN) δε θα πρέπει να χρησιμοποιούνται στις φάσεις ανάπτυξης και δοκιμής των εφαρμογών

6.4.4: Αφαίρεση των δεδομένων που χρησιμοποιήθηκαν στη δοκιμής της εφαρμογής, πριν αυτή δοθεί για χρήση.

6.4.5: Δημιουργία διαδικασιών αλλαγής ελέγχου για την εγκατάσταση των patches και των αλλαγών στα προγράμματα. Οι διαδικασίες αυτές πρέπει να περιλαμβάνουν:

6.4.5.1: Καταγραφή της επίδρασης

6.4.5.2: Έγγραφη επιβεβαίωση αλλαγών από εξουσιοδοτημένη πηγή

6.4.5.3: Δοκιμή λειτουργικότητας για να επιβεβαιωθεί ότι η αλλαγή δεν επιφέρει ανεπιθύμητα αποτελέσματα.

6.4.5.4: Διαδικασίες αναίρεσης της αλλαγής σε περίπτωση σφάλματος

6.5: Ανάπτυξη εφαρμογών βασισμένες σε κατευθυντήριες οδηγίες ασφαλούς προγραμματισμού. Οι νέες εφαρμογές θα πρέπει να αποτρέπουν κοινές ευπάθειες όπως:

6.5.1: Injection flaws

6.5.2: Υπερχείλιση καταχωρητών (buffer overflow)

6.5.3: Μη ασφαλής αποθήκευση κρυπτογραφικών στοιχείων

6.5.4: Έλλειψη ασφάλειας στην επικοινωνία

6.5.5: Μη ορθός χειρισμός λαθών

6.5.6: Όλες οι σημαντικές ευπάθειες, όπως αυτές ορίζονται από την απαίτηση 6.2

6.5.7: Cross-site scripting (XSS)

6.5.8: Εσφαλμένος έλεγχος πρόσβασης

6.5.9: Cross-site request forgery (CSRF)

6.6: Για τις web εφαρμογές θα πρέπει να υπάρχει συνεχής ενημέρωση για νέους κινδύνους και ευπάθειες.

Απαίτηση 7η: Περιορισμός στην πρόσβαση στα δεδομένων των καρτών

Για να διασφαλίσουμε ότι στα κρίσιμα δεδομένα μπορεί να έχει πρόσβασή μόνο εξουσιοδοτημένο προσωπικό, τα συστήματα και οι διεργασίες πρέπει να είναι σε θέση να περιορίζουν την πρόσβαση, βασιζόμενα στις εργασιακές ευθύνες που έχει κάθε εργαζόμενος στον οργανισμό, κατά τέτοιον τρόπο, ώστε ο εργαζόμενος να έχει τα ελάχιστα δυνατά δικαιώματα, για να επιτελέσει την εργασία του.

7.1: Περιορισμός της πρόσβασης στα συστήματα και στα δεδομένα των καρτών μόνο σε εκείνα τα άτομα των οποίων η εργασία απαιτεί αυτού του επιπέδου την πρόσβαση. Οι περιορισμοί στην πρόσβαση μπορούν να περιλαμβάνουν:

7.1.1: Περιορισμός των δικαιωμάτων πρόσβασης στου χρήστες, ώστε κάθε χρήστης να έχει τα ελάχιστα δυνατόν δικαιώματα.

7.1.2: Η απόδοση του επιπέδου πρόσβασης και των αντίστοιχων δικαιωμάτων του κάθε χρήστη, βασίζεται στην ατομική εργασία που έχει να επιτελέσει το άτομο αυτό

7.1.3: Απαίτηση για έγγραφη επιβεβαίωση από εξουσιοδοτημένα άτομα, για την απόδοση των δικαιωμάτων πρόσβασης.

7.2: Εγκαθίδρυση ενός συστήματος ελέγχου πρόσβασης, για τα συστήματα που συνδέονται πολλοί χρήστες, όπου ο κάθε χρήστης δεν θα μπορεί να κάνει τίποτε, πέρα από αυτά που ρητά και συγκεκριμένα του επιτρέπονται. Αυτό το σύστημα ελέγχου πρόσβασης θα πρέπει να περιλαμβάνει:

7.2.1: Καθολική κάλυψη όλων των συστημάτων

7.2.2: Απόδοση των δικαιωμάτων σε άτομα ανάλογα με τη εργασία τους και τις απαιτήσεις της

7.2.3: Κανένας χρήστης δε μπορεί να κάνει τίποτα, πέρα από αυτά που ρητά του επιτρέπονται.

Απαίτηση 8η: Απόδοση ενός μοναδικού αναγνωριστικού (ID) σε κάθε πρόσωπο με πρόσβαση σε υπολογιστή

Με το να αποδίδουμε ένα μοναδικό ID σε κάθε πρόσωπου που έχει πρόσβαση, διασφαλίζουμε ότι το κάθε άτομο είναι αποκλειστικά υπεύθυνο και υπόλογο για τις πράξεις του. Κατ' αυτόν τον τρόπο, μπορούμε να ελέγχουμε τις πράξεις του κάθε ατόμου και το άτομο αυτό δεν μπορεί να αποποιηθεί τις ευθύνες του, καθώς μπορούμε να ακολουθήσουμε τα ψηφιακά του ίχνη και να οδηγηθούμε σε αυτό.

8.1: Απόδοση σε όλους τους χρήστες ενός μοναδικού ID πριν τους επιτρέψουμε την πρόσβαση στα συστήματα των δεδομένων των καρτών

8.2: Εκτός από το ID, χρησιμοποιούμε κάποια από τις ακόλουθες μεθόδους για να αυθεντικοποιήσουμε τους χρήστες:

- Κάτι που ξέρουν, όπως ένας κωδικός ή μια μυστική φράση
- Κάτι που έχουν, όπως μία έξυπνη κάρτα
- Κάτι που είναι, όπως κάποιο βιομετρικό χαρακτηριστικό

8.3: Για απόκτηση πρόσβασης από απόσταση, δηλαδή από κάποια θέση εκτός του δικτύου σε κάποιο πόρο του δικτύου, χρησιμοποιούμε αυθεντικοποίηση δύο παραγόντων, από αυτούς που αναφέρονται στην απαίτηση 8.2.

8.4: Κρυπτογραφούμε όλα τα passwords κατά τη μετάδοση τους, ώστε να μη μπορούν να διαβαστούν.

8.5: Εξασφαλίζουμε κατάλληλη αναγνώριση χρηστών και αυθεντικοποίηση για όλους τους διαχειριστές των συστημάτων.

8.5.1: Έλεγχος της πρόσθεσης, διαγραφής και αλλαγής των ID των χρηστών, των συνθηματικών τους και άλλων παραγόντων αναγνώρισης

8.5.2: Επιβεβαίωση της ταυτότητας των χρηστών, πριν προβούμε σε επαναφορά του κωδικού του

8.5.3: Καθορισμός ενός αρχικού password σε μία μοναδική τιμή και άμεση αλλαγή του μετά την πρώτη χρησιμοποίησή του

8.5.4: Άμεση ανάκληση του δικαιώματος πρόσβασης σε χρήστες που έφυγαν ή παύθηκαν από τον οργανισμό

8.5.5: Απομάκρυνση/διαγραφή μη ενεργών χρηστών, τουλάχιστον μία φορά το τρίμηνο

8.5.6: Ενεργοποίηση λογαριασμών που χρησιμοποιούνται από εξωτερικούς συνεργάτες μόνο κατά την περίοδο που αυτό είναι απαραίτητο. Παρακολούθηση των λογαριασμών αυτών κατά την περίοδο χρήσης τους.

8.5.7: Ενημέρωση όλων των χρηστών που έχουν πρόσβαση στα δεδομένα των καρτών, σχετικά με τις διαδικασίες αυθεντικοποίησης.

8.5.8: Αποφεύγεται η χρήση ομαδικών, κοινών ή διαμοιραζόμενων λογαριασμών και passwords.

8.5.9: Αλλαγή των passwords των χρηστών το πολύ κάθε 90 ημέρες

8.5.10: Τα passwords πρέπει να έχουν μήκος τουλάχιστον 7 χαρακτήρων

8.5.11: Χρησιμοποίηση passwords που έχουν και αριθμούς και γράμματα

8.5.12: Απαγόρευση στους χρήστες να δηλώνουν το ίδιο password με κάποιο προηγούμενό τους

8.5.13: Κλείδωμα των χρηστών μετά από το πολύ 6 αποτυχημένες εισαγωγές κωδικού.

8.5.14: Κλείδωμα του χρήστη που έδωσε λάθος κωδικούς για τουλάχιστον 30 λεπτά ή μέχρι να τον ξεκλειδώσει κάποιος διαχειριστής

8.5.15: Αν η σύνδεση κάποιου χρήστη παραμείνει ανενεργή για πάνω από 15 λεπτά, ο χρήστης θα πρέπει να αυθεντικοποιηθεί ξανά για να ξανασυνδεθεί

8.5.16: Αυθεντικοποίηση για κάθε πρόσβαση σε οποιαδήποτε βάση δεδομένων που περιέχει δεδομένα καρτών, συμπεριλαμβανομένων των διαχειριστών, των εφαρμογών και όλων των χρηστών.

Απαίτηση 9η: Περιορισμός σε φυσικό επίπεδο στο προσωπικό της πρόσβασης στα δεδομένων των καρτών

Κάθε είδους φυσική πρόσβαση στα συστήματα που περιέχουν τα δεδομένα των καρτών δίνει τη δυνατότητα στα συγκεκριμένα άτομα να γίνουν επικίνδυνα (αφαιρώντας π.χ. ευαίσθητα δεδομένα) και για αυτό θα πρέπει να τους απαγορεύονται τέτοιες ενέργειες. Με τον όρο “προσωπικό” εννοούμε όλους τους εργαζομένους, πλήρους ή μερικής απασχόλησης, συμβούλους, εξωτερικούς συνεργάτες κ.α. που μπορούν να έχουν φυσική παρουσία στους χώρους όπου υφίστανται τα συστήματα του οργανισμού.

Με τον όρο “επισκέπτης” εννοούμε κάποιον κατασκευαστή, τεχνικό ή προσκεκλημένο, που πρέπει να επισκεφθεί τις εγκαταστάσεις μας για μικρό χρονικό διάστημα. Τέλος, με τον όρο “Μέσα” (media) εννοούμε το σύνολο των γραπτών και ηλεκτρονικών μέσων, που περιέχουν δεδομένα καρτών.

9.1: Χρησιμοποίηση των κατάλληλων μεθόδων ελέγχου εισόδου στις εγκαταστάσεις του οργανισμού, με περιορισμό και παρακολούθηση της φυσικής πρόσβασης στα συστήματα του CDE.

9.1.1: Χρήση καμερών και/ή μηχανισμών ελέγχου φυσικής πρόσβασης και ανάλυση των καταγεγραμμένων δεδομένων. Αποθήκευση των δεδομένων για τουλάχιστον 3 μήνες, εκτός και αν απαιτείται διαφορετικά από το νόμο

9.1.2: Περιορισμός πρόσβασης από πριζάκια δικτύου που βρίσκονται στο χώρο φιλοξενίας και εργασίας των επισκεπτών .

9.1.3: Περιορισμός πρόσβασης των επισκεπτών σε ασύρματες συσκευές του δικτύου του οργανισμού

9.2: Ανάπτυξη διαδικασιών που θα διευκολύνουν το διαχωρισμό του προσωπικού του οργανισμού από τους επισκέπτες.

9.3: Εξασφάλιση ότι οι επισκέπτες θα πρέπει:

9.3.1: Να αυθεντικοποιούνται πριν εισέλθουν σε περιοχές, όπου φυλάσσονται δεδομένα καρτών

9.3.2: Να τους δίδεται μία κάρτα ή κάποιο σήμα, με ημερομηνία λήξης, που θα υποδηλώνει ότι πρόκειται για επισκέπτες και όχι μόνιμο προσωπικό.

9.3.3: Να τους ζητείται να παραδώσουν την κάρτα ή το σήμα που τους δόθηκε πριν εγκαταλείψουν τις εγκαταστάσεις του οργανισμού.

9.4: Καθιέρωση ενός ημερολογίου επισκεπτών, όπου θα καταγράφονται όλες οι φυσικές επισκέψεις. Θα πρέπει να καταγράφεται το όνομα του ατόμου, η εταιρεία για την όποια δουλεύει, καθώς και το όνομα του μονίμου προσωπικού που τον συνοδεύει. Διατήρηση αυτού του ημερολογίου για τουλάχιστον 3 μήνες.

9.5: Αποθήκευση των backups των Μέσων σε ασφαλή τοποθεσία, κατά προτίμηση σε άλλο κτίριο ή site. Έλεγχος της ασφάλειας αυτής της εγκατάστασης τουλάχιστον μια φορά το χρόνο.

9.6: Πλήρης φυσική ασφάλεια όλων των Μέσων.

9.7: Αυστηρός έλεγχος για πιθανή εσωτερική ή εξωτερική διαρροή Μέσων.

9.8: Εξασφάλιση από ανώτερα στελέχη ότι εγκρίνεται η μεταφορά Μέσων από κάποια ασφαλή περιοχή

9.9: Αυστηρός έλεγχος όσον αφορά την αποθήκευση και την προσβασιμότητα των Μέσων

9.9.1: Ορθή διατήρηση των logs που αφορούν τα Μέσα

9.10: Καταστροφή Μέσων που δεν είναι πια χρήσιμα

9.10.1: Καταστροφή ή αποτέφρωση των δεδομένων των καρτών που βρίσκονται σε έντυπη μορφή

9.10.2: Τα δεδομένα των καρτών θα πρέπει να μη μπορούν να ανακατασκευαστούν.

Απαίτηση $10^{η}$: Παρακολούθηση όλων των προσβάσεων στους πόρους του δικτύου και στα δεδομένα των καρτών

Οι μηχανισμοί καταγραφής του τι κάνει κάθε χρήστης, καθώς και η δυνατότητα να παρακολουθούμε τη δραστηριότητα αυτή των χρηστών, αποτελεί σημαντικότατο παράγοντα στην παρεμπόδιση, την ανίχνευση και τον περιορισμό της επίδρασης των επιθέσεων ή της κακής χρήσης. Η παρουσία των αρχείων καταγραφής συμβάντων (log files) σε όλα τα περιβάλλοντα, επιτρέπει την ενδελεχή παρακολούθηση, ετοιμότητα και ανάλυση ατυχών συμβάντων. Και αυτό γιατί ο προσδιορισμός της αιτίας των ατυχών συμβάντων είναι δύσκολος, αν όχι αδύνατος, χωρίς τη χρήση log αρχείων.

10.1: Υλοποίηση διαδικασίας για τη διασύνδεση όλων των προσβάσεων στα συστήματα

10.2: Υλοποίηση σε όλα τα συστήματα αυτόματων τρόπων παρακολούθησης των χρηστών, που θα καταγράφει:

10.2.1: Κάθε απόπειρα πρόσβασης στα δεδομένα των καρτών

10.2.2: Κάθε πράξη που έκανε κάποιος διαχειριστής

10.2.3: Κάθε απόπειρα πρόσβασης στα αρχεία καταγραφής συμβάντων

10.2.4: Μη επιτυχημένες προσπάθειες εισόδου στα συστήματα

10.2.5: Κάθε χρήση μηχανισμών αυθεντικοποίησης και ταυτοποίησης

10.2.6: Την αρχικοποίηση των αρχείων καταγραφής συμβάντων

10.2.7: Τη δημιουργία ή τη διαγραφή συστημικών αντικειμένων

10.3: Καταγραφή τουλάχιστον των ακόλουθων για κάθε σύστημα και για κάθε γεγονός:

10.3.1: Ταυτότητα του χρήστη

10.3.2: Είδος συμβάντος

10.3.3: Ημερομηνία και ώρα συμβάντος

10.3.4: Ένδειξη για τον αν η απόπειρα ήταν επιτυχημένη ή όχι

10.3.5: Από πού έγινε το γεγονός

10.3.6: Ταυτότητα ή όνομα των επηρεαζόμενων δεδομένων, συστήματος ή πόρου

10.4: Χρήση συντονισμού ώρας, με τη βοήθεια ενός κεντρικού ρολογιού, ώστε τα ρολόγια όλων των συστημάτων να έχουν την ίδια ώρα και ημερομηνία

10.4.1: Όλα τα συστήματα έχουν σωστή και συνεπή ώρα

10.4.2: Η χρονική σήμανση προστατεύεται και δεν αλλάζει.

10.4.3: Οι ρυθμίσεις της ώρας λαμβάνονται από γνωστές, έγκυρες και αξιόπιστες πηγές

10.5: Διασφάλιση των αρχείων καταγραφής, ώστε να μην μπορούν να αλλαχτούν

10.5.1: Περιορισμοί, ώστε μόνο συγκεκριμένα και εξουσιοδοτημένα άτομα να μπορούν να έχουν πρόσβαση σε αυτά τα αρχεία

10.5.2: Προστασία των αρχείων καταγραφής από μη εξουσιοδοτημένες αλλαγές

10.5.3: Αποθήκευση των αρχείων καταγραφής σε μια κεντροποιημένη τοποθεσία και σε συγκεκριμένα μέσα, ώστε να είναι δύσκολα προσβάσιμα και αδύνατον να αλλαχθούν

10.5.5: Χρησιμοποίηση λογισμικού παρακολούθησης ακεραιότητας αρχείων και ανίχνευσης αλλαγών, για τα αρχεία καταγραφής συμβάντων, ώστε να είναι αδύνατη η αλλαγή τους, χωρίς να υπάρξει η αντίστοιχη ειδοποίηση.

10.6: Εξέταση των αρχείων καταγραφής συμβάντων τουλάχιστον μία φορά τη μέρα. Αυτές οι επιθεωρήσεις πρέπει να περιλαμβάνουν εκείνους τους servers που επιτελούν λειτουργίες ασφαλείας, όπως αυθεντικοποίηση κτλ.

10.7: Διατήρηση των αρχείων καταγραφής για τουλάχιστον ένα έτος.

Απαίτηση 11η: Τακτική δοκιμή της ασφάλειας των συστημάτων και των διεργασιών

Κακόβουλοι χρήστες και ερευνητές στο πεδίο της ασφάλειας ανακαλύπτουν συνεχώς νέες ευπάθειες, είτε σε ήδη υπάρχοντα προγράμματα, είτε σε νέα. Όλα τα συστήματα, όλες οι διαδικασίες και όλα τα λογισμικά πρέπει να ελέγχονται συνεχώς, για να διατηρείται η ασφάλεια στα επιθυμητά επίπεδα.

11.1: Δοκιμή για την ύπαρξη ασύρματων σημείων πρόσβασης που δεν ανήκουν στον οργανισμό, τουλάχιστον μία φορά το τρίμηνο.

11.2: Έλεγχος τόσο στο εσωτερικό, όσο και στο εξωτερικό δίκτυο για ύπαρξη ευπαθειών, τουλάχιστον ανά τρίμηνο η μετά από κάποια σημαντική αλλαγή στο δίκτυο.

11.2.1: Εκτέλεση ελέγχων στο εσωτερικό δίκτυο ανά τρίμηνο

11.2.2: Εκτέλεση ανίχνευσης ευπαθειών στο εξωτερικό δίκτυο από κάποιον εγκεκριμένο κατασκευαστή μηχανισμών ασφαλείας (Approved Scanning Vendor) που να τον συστήνει το PCI SSC (Payment Card Industry Security Standards Council)

11.2.3: Εκτέλεση εσωτερικών και εξωτερικών ελέγχων μετά από κάθε σημαντική αλλαγή.

11.3: Εκτέλεση εσωτερικών και εξωτερικών δοκιμών διείσδυσης τουλάχιστον μία φορά το έτος ή μετά από κάθε σημαντική αλλαγή ή αναβάθμιση.

11.3.1: Δοκιμές διείσδυσης στο επίπεδο δικτύου

11.3.2: Δοκιμές διείσδυσης στο επίπεδο εφαρμογών

11.4: Χρησιμοποίηση Συστήματος Ανίχνευσης Εισβολών (Intrusion Detection System – IDS) σε συνδυασμό με τη χρησιμοποίηση Συστήματος Αποτροπής Εισβολών (Intrusion Prevention System - IPS), για την παρακολούθηση της κίνησης στην περίμετρο του CDE, καθώς και σε άλλα κρίσιμα σημεία του εσωτερικού μας δικτύου.

11.5: Χρησιμοποίηση εργαλείων παρακολούθησης ακεραιότητας αρχείων, για να ειδοποιείται το υπεύθυνο προσωπικό για μη εξουσιοδοτημένη πρόσβαση σε κρίσιμα συστημικά αρχεία ή αρχεία περιεχομένου.

Απαίτηση 12η: Διατήρηση πολιτικής ασφαλείας που καθορίζει την ασφάλεια των πληροφοριών για όλο το προσωπικό.

Μία ισχυρή πολιτική ασφαλείας θέτει το επίπεδο ασφαλείας όλου του οργανισμού και ενημερώνει το προσωπικό ποιες είναι οι απαιτήσεις από αυτούς. Όλο το προσωπικό του οργανισμού πρέπει να είναι ενήμερο για την ευαισθησία των δεδομένων, καθώς και τις ευθύνες που έχουν για την προστασία του.

12.1: Καθιέρωση, δημοσίευση, διατήρηση και γνωστοποίηση μίας πολιτικής ασφαλείας η οποία επιτυγχάνει τα ακόλουθα:

12.1.1: Υλοποιεί όλες τις απαιτήσεις του PCI DSS

12.1.2 Περιλαμβάνει μία ετήσια διαδικασία για την αναγνώριση των κινδύνων και των ευπαθειών, καθώς και τα αποτελέσματα, με μία επίσημη αποτίμηση ρίσκου

12.1.3: Περιλαμβάνει αναθεωρήσεις, τουλάχιστον μία φορά το χρόνο και μετά από κάθε μεγάλη αλλαγή στον οργανισμό.

12.2: Ανάπτυξη διαδικασιών που θα εκτελούνται καθημερινά και που είναι συμβατές με τις απαιτήσεις του PCI DSS

12.3: Ανάπτυξη πολιτικών χρήσης κρίσιμων τεχνολογιών, όπως για παράδειγμα ασύρματες τεχνολογίες, email, διαχείριση laptop και φορητών συσκευών, κτλ. Αυτές οι πολιτικές χρήσης θα πρέπει να περιλαμβάνουν:

12.3.1: Σαφή έγκριση από τους υπευθύνους

12.3.2: Αυθεντικοποίηση για χρήση των συγκεκριμένων τεχνολογιών

12.3.3: Λίστα με όλες τις συσκευές και του προσωπικού που θα έχει πρόσβαση

12.3.4: Προσθήκη ετικέτας σε όλες τις συσκευές για να καθορίζεται ο κάτοχος, ο σκοπός της χρήσης, κτλ.

12.3.5: Αποδεκτές και επιτρεπόμενες χρήσεις της κάθε τεχνολογίας

12.3.6: Αποδεκτές τοποθεσίες δικτύου για την κάθε τεχνολογία

12.3.7: Λίστα με προϊόντα που αποδέχεται ο οργανισμός

12.3.8: Αυτόματη αποσύνδεση συνόδων στις τεχνολογίες απομακρυσμένης πρόσβασης, μετά από κάποιο συγκεκριμένο χρονικό διάστημα

12.3.9: Ενεργοποίηση της απομακρυσμένης πρόσβασης για τους εξωτερικούς συνεργάτες του οργανισμού μόνο όταν χρειάζεται και άμεση απενεργοποίησή τους μετά το πέρας των εργασιών τους

12.3.10: Για το προσωπικό που αποκτά απομακρυσμένη πρόσβαση στα δεδομένα των καρτών, πρέπει να απαγορεύεται η αντιγραφή, η μετακίνηση και η αποθήκευση αλλού αυτών των δεδομένων.

12.4: Διασφάλιση ότι η πολιτική ασφαλείας και οι διαδικασίες καθορίζουν ξεκάθαρα τις ευθύνες του προσωπικού, όσον αφορά την ασφάλεια

12.5: Απόδοση σε κάθε άτομο ή ομάδα των ακόλουθων ευθυνών που αφορούν την διαχείριση της ασφαλείας:

12.5.1: Υλοποίηση, καταγραφή και διανομή των πολιτικών ασφαλείας και των διαδικασιών

12.5.2: Παρακολούθηση και ανάλυση των ειδοποιήσεων που αφορούν την ασφάλεια και ανάθεση των ενεργειών που πρέπει να γίνουν στο αρμόδιο προσωπικό

12.5.3: Καθιέρωση, καταγραφή και διανομή όλων των ενεργειών που πρέπει να εκτελέσει το προσωπικό σε περίπτωση περιστατικού ασφαλείας. Διασφάλιση ότι η αντίδραση θα είναι άμεση και αποτελεσματική

12.5.4: Διαχείριση των λογαριασμών των χρηστών, συμπεριλαμβανομένης της προσθήκης, διαγραφής ή αλλαγής τους.

12.5.5: Παρακολούθηση και έλεγχος κάθε πρόσβασης στα δεδομένα

12.6: Εφαρμογή επίσημου προγράμματος επιφυλακής που θα αφορά την ασφάλεια, ώστε όλο το προσωπικό να έχει πλήρη γνώση της σημαντικότητας της ασφάλειας των δεδομένων των καρτών

12.6.1: Εκπαίδευση του προσωπικού μετά την πρόσληψη και τουλάχιστον μία φορά το χρόνο

12.6.2: Απαίτηση από το προσωπικό να επιβεβαιώνει τουλάχιστον μία φορά το χρόνο, ότι έχει διαβάσει και κατανοήσει την πολιτική ασφαλείας και τις σχετικές διαδικασίες.

12.7: Έλεγχος του υπό πρόσληψη προσωπικού, ώστε να ελαχιστοποιούνται οι πιθανοί κίνδυνοι

12.8: Αν δεδομένα των καρτών χρησιμοποιούνται από κοινού ή διαμοιράζονται με άλλες οντότητες, τότε πρέπει να εφαρμόζονται πολιτικές και διαδικασίες που πρέπει να περιλαμβάνουν:

12.8.1: Τη λίστα με όλες αυτές τις οντότητες

12.8.2: Γραπτή συμφωνία που περιλαμβάνει αποδοχή της τρίτης οντότητας ότι είναι υπεύθυνη για την ασφάλεια των δεδομένων των καρτών

12.8.3: Διασφάλιση ότι υπάρχει διαδικασία για εκ των προτέρων δέσμευση της τρίτης οντότητας στις απαιτήσεις ασφαλείας του οργανισμού

12.8.4: Παρακολούθηση από τον οργανισμό του κατά πόσο οι συνεργάτες του και οι τρίτες οντότητες είναι συμβατές με τις απαιτήσεις ασφαλείας του PCI DSS.

12.9: Εφαρμογή σχεδίων αντιμετώπισης περιστατικών.

12.9.1: Δημιουργία σχεδίου αντιμετώπισης περιστατικών, το οποίο πρέπει να περιέχει τουλάχιστον τα ακόλουθα:

- Ρόλους, ευθύνες και στρατηγικές επικοινωνίας σε περίπτωση περιστατικού ασφαλείας
- Συγκεκριμένες διαδικασίας αντίδρασης σε περιστατικά
- Διαδικασίες ανάνηψης και επιχειρησιακής συνέχειας
- Διαδικασίες back-up δεδομένων
- Ανάλυση νομικών απαιτήσεων για τη δημοσιοποίηση επιθέσεων
- Κάλυψη και προστασία όλων των κρίσιμων συστημάτων

12.9.2: Δοκιμή του σχεδίου τουλάχιστον μια φορά το χρόνο

12.9.3: Ορισμός συγκεκριμένου προσωπικού που θα είναι διαθέσιμο κάθε ώρα της ημέρα για την αντιμετώπιση περιστατικών

12.9.4: Κατάλληλη εκπαίδευση του προσωπικού για αντίδραση σε περιστατικά ασφαλείας

12.9.5: Αναφορές από τα IPS, IDS και τα συστήματα παρακολούθησης

12.9.6: Δημιουργία διαδικασίας που θα ορίζει πώς θα εξελίσσονται οι διαδικασίες, με βάση αυτά που διδάχτηκε ο οργανισμός, είτε από κάποιο επίθεση, είτε από την προετοιμασία του.

ΚΕΦΑΛΑΙΟ 4

Πολιτικές Ασφάλειας σε Οργανισμό

Μια πολιτική ασφάλειας των πληροφοριών είναι ο ακρογωνιαίος λίθος ενός Προγράμματος Ασφάλειας Πληροφοριών. Θα πρέπει να αντικατοπτρίζει τους στόχους του οργανισμού για την ασφάλεια και τη συμφωνημένη με τη διοίκηση στρατηγική για την ασφάλιση πληροφοριών. Οι πολιτικές επιτρέπουν στους οργανισμούς να ρυθμίσουν τις πρακτικές και διαδικασίες που θα μειώσουν την πιθανότητα μιας επίθεσης ή ενός περιστατικού και θα ελαχιστοποιήσουν τη ζημία που προκλήθηκε από ένα τέτοιο περιστατικό αν αυτό συμβεί.

Πολλοί άνθρωποι βλέπουν τις πολιτικές σαν δευτερεύουσας σημασίας. Σαν μια νόστιμη «σάλτσα» για να προστεθεί σε μια πραγματική τεχνολογική «σαλάτα» από firewalls, ανιχνευτές ιών και VPNs. Αυτό είναι λάθος. Θα εξηγήσουμε γιατί οι πολιτικές θα πρέπει να είναι η βάση μιας ολοκληρωμένης στρατηγικής για την ασφάλεια των πληροφοριών, καθώς και το πώς οι πολιτικές μπορεί να είναι ένα αποτελεσματικό, πρακτικό μέρος των συστημάτων ψηφιακής άμυνας.

4.1 Επισκόπηση των Πολιτικών

Σε πρακτικό επίπεδο ασφάλειας, θα ορίσουμε μια πολιτική ως ένα δημοσιευμένο έγγραφο (ή σειρά εγγράφων) στο οποίο ορίζονται η φιλοσοφία του οργανισμού, η στρατηγική, οι πολιτικές και πρακτικές όσον αφορά την εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα των πληροφοριών και των συστημάτων πληροφοριών.

Έτσι, η πολιτική είναι ένα σύνολο από μηχανισμούς μέσω των οποίων μπορούν να καθορισθούν και να επιτευχθούν οι στόχοι ασφάλειας πληροφοριών. Ας εξετάσουμε εν συντομία κάθε μία από αυτές τις έννοιες. Πρώτον, έχουμε τους στόχους της ασφάλειας των πληροφοριών:

- Η εμπιστευτικότητα αφορά την εξασφάλιση ότι μόνο οι άνθρωποι που είναι εξουσιοδοτημένοι να αποκτήσουν πρόσβαση σε πληροφορίες μπορούνε να το πράξουν.

- Η ακεραιότητα αφορά τη διατήρηση της αξίας και της κατάστασης των πληροφοριών, πράγμα που σημαίνει ότι προστατεύονται από μη εξουσιοδοτημένη τροποποίηση. Η πληροφορία έχει αξία μόνο αν γνωρίζουμε ότι είναι σωστή. Ένας σημαντικός στόχος των πολιτικών ασφάλειας των πληροφοριών είναι, επομένως, να διασφαλιστεί ότι οι πληροφορίες δεν έχουν τροποποιηθεί ή καταστραφεί.
- Η διαθεσιμότητα αφορά την εξασφάλιση ότι οι πληροφορίες και τα συστήματα πληροφοριών είναι διαθέσιμα και λειτουργικά, όταν αυτό είναι απαραίτητο. Ένας βασικός στόχος της πολιτικής ασφάλειας των πληροφοριών θα πρέπει να είναι να διασφαλιστεί ότι οι πληροφορίες είναι πάντα διαθέσιμες για την υποστήριξη κρίσιμων επιχειρησιακών διαδικασιών.

Οι στόχοι αυτοί αναγνωρίζονται παγκοσμίως ως χαρακτηριστικό γνώρισμα κάθε ασφαλούς συστήματος.

Ενώ οι τεχνολογικοί έλεγχοι αφορούν τη διεύθυνση πληροφορικής ή τους διαχειριστές συστημάτων και δικτύων, η πολιτική ασφάλειας είναι ευθύνη της ανώτερης διοίκησης οι οποίοι έχουν και τη γενική ευθύνη απέναντι στους μετόχους για την προστασία των αγαθών και περιουσιακών στοιχείων του οργανισμού.

Σε ορισμένους κλάδους ο οργανισμός μπορεί να έχει νομικές υποχρεώσεις σε σχέση με την ακεραιότητα και την εμπιστευτικότητα ορισμένων πληροφοριών. Σε πολλές περιπτώσεις ο μόνος τρόπος που μπορούν να αποδείξουν τη δέουσα επιμέλεια (due diligence) στο θέμα αυτό είναι με αναφορά στις δημοσιευμένες πολιτικές. Επειδή η πολιτική αντανακλά τη φιλοσοφία και τη στρατηγική της διοίκησης του οργανισμού αποτελεί εύλογη απόδειξη της πρόθεσης της εταιρείας σχετικά με την ασφάλεια των πληροφοριών. Είναι ενδιαφέρον, ότι ο έλεγχος ως προς ένα πρότυπο ασφαλείας λειτουργεί με ακριβώς αυτή την αρχή της «πρόθεση».

Επειδή η πολιτική είναι συνήθως δημοσιευμένη, και επειδή αντιπροσωπεύει απόφαση της εκτελεστικής διοίκησης, μια πολιτική που μπορεί να είναι ακριβώς ό,τι χρειάζεται για να πείσει το δυνητικό πελάτη, συνεργάτη προς συγχώνευσης, ή επενδυτή για το πόσο σωστά λειτουργεί ο οργανισμός.

Η πολιτική αντανακλά τη φιλοσοφία και τη στρατηγική όσον αφορά τη διαχείριση ασφάλειας πληροφοριών. Ως εκ τούτου, είναι το τέλειο πρότυπο ως προς τον οποίο η τεχνολογία και οι λοιποί μηχανισμοί ασφαλείας μπορούν να μετρηθούν. Για παράδειγμα, αν θέλει κάποιος να ξέρει κατά πόσον αξίζει να αγοράσει ένα πανάκριβο εξοπλισμό ασφάλειας (π.χ. ένα firewall τελευταίας τεχνολογίας) μπορεί να ελέγξει αν υλοποιεί σωστά

τους ελέγχους που αναφέρονται στην πολιτική ασφάλειας. Επίσης, μπορεί μια σωστά σχεδιασμένη πολιτική να ενσωματωθεί στο συμβόλαιο των εργαζομένων έτσι ώστε σε περίπτωση παράβασης (π.χ. είσοδος σε ακατάλληλες ιστοσελίδες) να μπορεί να τιμωρηθεί βάσει της σύμβασης που θα έχει υπογράψει. Μια καλά εφαρμοζόμενη πολιτική βοηθά να εξασφαλιστεί η συνοχή των συστημάτων ασφαλείας, δίνοντας μια οδηγία και αναθέτοντας σαφώς την ευθύνης και επιπλέον ορίζοντας τις συνέπειες από τη μη εκπλήρωση αυτών των ευθυνών.

Οι άνθρωποι μπορεί να είναι ο πιο καθοριστικός παράγοντας σε ένα σύστημα ασφάλειας πληροφοριών. Με το να είναι καθορισμένο τι επιτρέπεται και τι όχι στους χρήστες και με το να διασφαλίζεται η εκπαίδευσή τους στα πρότυπα που εφαρμόζονται, η εταιρία τοποθετεί την ευθύνη σε αυτούς οι οποίοι δεν μπορούν να επικαλεστούν άγνοια σε περίπτωση παράβασης της πολιτικής. Επιπλέον μια πολιτική, ως μια οδηγία από την ανώτερη διοίκηση, δίνει στους διαχειριστές των συστημάτων και υπεύθυνους ασφαλείας τη δυνατότητα να επιβάλουν αποφάσεις που μπορεί να μην είναι δημοφιλής μεταξύ των χρηστών του συστήματος.

Τι προστατεύουν οι πολιτικές στην πραγματικότητα:

Πριν από τη λήψη αποφάσεων σχετικά με τη στρατηγική της Ασφάλειας Πληροφοριών οι οργανισμοί πρέπει να έχουν μια καλή κατανόηση του προφίλ κινδύνου τους. Ο κίνδυνος αποτελείται από ένα συνδυασμό πληροφοριακών πόρων που έχουν αξία και τα τρωτά σημεία τα οποία είναι εκμεταλλεύσιμα. Το μέγεθος του κινδύνου είναι το γινόμενο της αξίας των πληροφοριών επί το βαθμό στον οποίο η ευπάθεια μπορεί να αξιοποιηθεί.

Εφ 'όσον ο οργανισμός έχει πληροφορίες που έχουν αξία, αυτές οι πληροφορίες - και κατ' επέκταση, ο οργανισμός- θα υπόκεινται σε κίνδυνο. Η λειτουργία του κάθε μηχανισμού ελέγχου ασφάλειας πληροφοριών (τεχνικών ή διαδικαστικών) είναι να περιορίσει αυτόν τον κίνδυνο σε ένα αποδεκτό επίπεδο. Το ίδιο ισχύει και για τις πολιτικές. Οι πολιτικές είναι ένας μηχανισμός ελέγχου κινδύνου και ως εκ τούτου θα πρέπει να σχεδιαστούν και αναπτυχθούν για την αντιμετώπιση πραγματικών και συγκεκριμένων κινδύνων. Έτσι, μια πλήρης και αναλυτική αξιολόγηση των κινδύνων πρέπει να είναι η πρώτη φάση της διαδικασίας ανάπτυξης πολιτικής. Η εκτίμηση κινδύνου πρέπει να προσδιορίζει τις ασθενέστερες περιοχές του συστήματος και μπορεί να χρησιμοποιηθεί για τον καθορισμό συγκεκριμένων στόχων.

Φυσικά, η προσέγγιση της χρήσης γενικών εγγράφων πολιτικής που είναι ελεύθερα διαθέσιμα στο Διαδίκτυο και από διάφορες εμπορικές πηγές. Αν και υπάρχει μια σειρά από ζητήματα που πράγματι μπορούν να αντιμετωπιστούν με ένα γενικό τρόπο, θα

πρέπει να είμαστε πολύ προσεκτικοί με αυτή την προσέγγιση. Μια πολιτική που λέει πάρα πολύ δεν είναι καλύτερη από μία που δεν λέει τίποτα. Οι οργανισμοί πρέπει να είναι έτοιμοι να επιβάλουν κάθε διάταξη που υπάρχει στην πολιτική ασφάλειας, έτσι λοιπόν οι πολιτικές πρέπει να είναι στοχευμένες και συγκεκριμένες.

Οι διαχειριστές ασφαλείας πρέπει να καθορίσουν συγκεκριμένους στόχους για τον οργανισμό, με βάση την αξία των εν λόγω πληροφοριών και τους συγκεκριμένους κινδύνους που αντιμετωπίζουν οι πληροφορίες.

4.2 Δημιουργία ενός υποστηρικτικού περιβάλλοντος

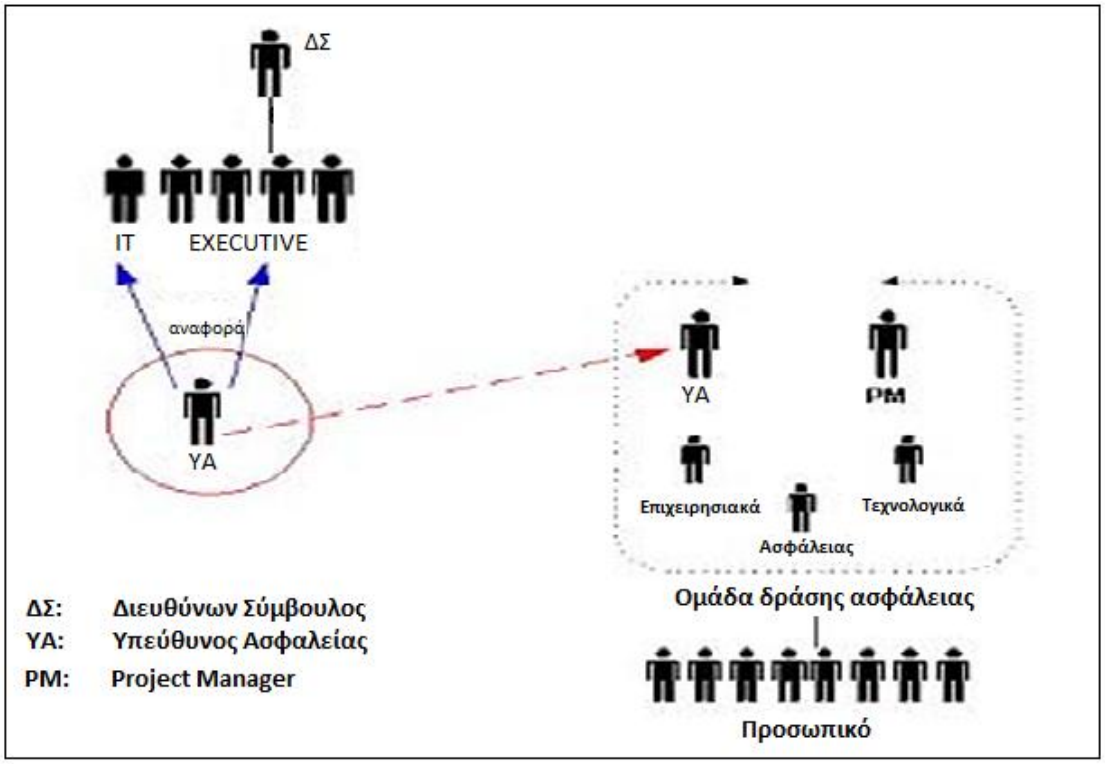
Σε αυτή την ενότητα θα δείξουμε μερικά από τα πράγματα που μπορούν να γίνουν για να διασφαλιστεί ότι στις πολιτικές ασφαλείας δίνεται πλήρη στήριξη από τη διοίκηση του οργανισμού, ώστε να αυξηθεί η αποτελεσματικότητα των πολιτικών.

Ανεξάρτητα από το μέγεθος του οργανισμού, μια πολιτική θα πρέπει να έχει πάντα έναν ιδιοκτήτη. Αν και οι τίτλοι ή τα ακρωνύμια μπορεί να διαφέρουν από οργανισμό σε οργανισμό, οι ρόλοι, τα καθήκοντα και οι υποχρεώσεις πρέπει να είναι παρεμφερή. Για λόγους ευκολίας ανάγνωσης, στην ενότητα αυτή θα καλούμε αυτό το άτομο «Υπεύθυνος Ασφάλειας» ή «ΥΑ». Είναι ευθύνη του ΥΑ για να επιβλέπει τη δημιουργία, τη διανομή, και την εφαρμογή των πολιτικών ασφαλείας. Με αυτή την έννοια, ο ΥΑ παίζει το ρόλο του διαμεσολαβητή μεταξύ της διοίκησης και της βάσης των χρηστών. Είναι προφανές λοιπόν ότι ο ΥΑ θα πρέπει να αναφέρεται άμεσα στο διοικητικό συμβούλιο ή ακόμη και στο διευθύνων σύμβουλο.

Σε μεγάλους οργανισμούς που είναι ακόμα νωρίς στον κύκλο της ασφάλειας προτείνεται η δημιουργία μιας ομάδας ασφαλείας να αναλάβει την ευθύνη για την ασφάλεια της διαδικασίας. Αυτή η ομάδα αποτελείται συνήθως από το ΥΑ, έναν διαχειριστής έργου (Project Manager - PM) και μια ομάδα εξειδικευμένων στελεχών ως προς ζήτημα επιχειρησιακά, τεχνολογικά και ασφάλειας. Οι λειτουργίες της ομάδας περιλαμβάνουν:

- Καθορισμός της στρατηγικής ασφάλειας.
- Δημιουργία ενός πλάνου έργου και μιας δήλωσης αποστολής.
- Καθορισμός της εταιρικής πολιτικής ασφάλειας.
- Καθορισμός πολιτικών συγκεκριμένων συστημάτων.

- Ένα πρόγραμμα ευαισθητοποίησης των χρηστών.
- Το διορισμό της ελεγκτών ασφάλειας. Η δομή της ομάδας απεικονίζεται στο παρακάτω διάγραμμα:



Σχήμα 4.1: Ομάδα δράσης Ασφάλειας

Σε ένα σύστημα ασφαλείας ο πιο αδύναμος κρίκος είναι ο ανθρώπινος παράγοντας. Ακόμα κι αν ελέγχεται η κίνηση του στο διαδίκτυο υπάρχουν μηχανισμοί για να αψηφήσει (bypass) το firewall. Οπότε είναι απαραίτητο να δημιουργηθεί μια κουλτούρα ως προς την ασφάλεια και η τρόποι για να ενισχυθεί είναι μέσω εκπαίδευσης των χρηστών, επιστράτευση των προϊσταμένων για ενημέρωση, επιβολή της κουλτούρας είτε θετικά με επιβράβευση είτε αρνητικά με κυρώσεις και τέλος με ενυπόγραφη δέσμευση των υπαλλήλων.

Συστήματα ταξινόμησης πληροφορίας

Κατά την ανάπτυξη των πολιτικών ασφάλειας των πληροφοριών, το προσωπικό ασφαλείας θα πρέπει να είναι σε θέση να διακρίνει μεταξύ διαφόρων ομάδων ανθρώπων, υπολογιστών και πληροφοριών που έχουν διαφορετική αξία και διαφορετικές απαιτήσεις όσον αφορά την ασφάλεια. Για αυτό το λόγω πρέπει να χρησιμοποιηθεί ένα σύστημα ταξινόμησης με το οποίο στις πηγές πληροφόρησης και στα άτομα αποδίδονται επίπεδα

ταξινόμησης τα οποία στη συνέχεια χρησιμοποιούνται για να περιγράψουν από ποιούς ανθρώπους θα πρέπει να επιτρέπεται η πρόσβαση σε ποιές ταξινομήσεις των πόρων.

Δυο χαρακτηριστικά παραδείγματα μοντέλων συστημάτων ταξινόμησης πληροφοριών είναι το στρατιωτικό μοντέλο και το μοντέλο Bell-Lapadula. Το στρατιωτικό μοντέλο εφαρμόζει τη γνωστή κατηγοριοποίηση των εγγράφων σε πέντε κατηγορίες: αδιαβάθμητα, περιορισμένα, εμπιστευτικά, απόρρητα και άκρως απόρρητα. Αντίστοιχη ταξινόμηση υπάρχει για τους χρήστες όπου καθορίζει ποιά έγγραφα μπορεί να δει κάποιος. Το μοντέλο Bell-Lapadula είναι μια εκδοχή του στρατιωτικού που περιγράφει ένα σύνολο κανόνων ελέγχου πρόσβασης οι οποίοι χρησιμοποιούν ετικέτες ασφαλείας σε αντικείμενα και δικαιώματα σε χρήστες. Τα δικαιώματα πρόσβασης που προβλέπονται πρέπει να καταγράφονται στον πίνακα προστασίας και επίσης ισχύουν ιδιότητες που εξασφαλίζουν τη γενική αρχή του μοντέλου «no read up, no write down», δηλαδή οι χρήστες με χαμηλά δικαιώματα δεν διαβάζουν έγγραφα με υψηλή εμπιστευτικότητα και αντίθετα οι χρήστες με υψηλά δικαιώματα δεν μπορούν να γράψουν σε έγγραφα με χαμηλή κλάση εμπιστευτικότητας (τα οποία μπορούν να τα διαβάσουν οι πιο πολλοί).

Μια τέτοια επίσημη προσέγγιση πιθανότατα να μην είναι απαραίτητη σε όλους τους οργανισμούς. Οι υπεύθυνοι για την ανάπτυξη πολιτικών για την ασφάλεια θα πρέπει να αναπτύξουν ένα σύστημα ταξινόμησης, καθώς και ένα υποστηρικτικό σύνολο κανόνων που θα υποστηρίξει τις απαιτήσεις και τους στόχους του οργανισμού.

Ταξινόμηση

Όλα τα δεδομένα έχει μια προεπιλεγμένη ταξινόμηση, αλλά με επαρκή αιτιολόγηση, ο ιδιοκτήτης των δεδομένων μπορεί να αλλάξει την ταξινόμηση. Οι υπολογιστές ταξινομούνται κατά παρόμοιο τρόπο με τα δεδομένα. Κάθε υπολογιστής έχει έναν ιδιοκτήτη όπου τέτοιος ορίζεται ο επικεφαλής του τμήματος που ζητά την εγκατάσταση του εξοπλισμού και είναι έπειτα υποχρέωση του ιδιοκτήτη του εξοπλισμού να ταξινομήσει όλες τις συσκευές υπό τον έλεγχο του. Η κατάταξη γίνεται με συνεννόηση του ιδιοκτήτη (ή του αντιπροσώπου που διορίστηκε) με τον Διαχειριστή Ασφαλείας, αλλά ο Διαχειριστής Ασφαλείας πρέπει να λάβει την τελική απόφαση. Μπορεί να υπάρχει μια προκαθορισμένη λίστα ταξινομήσεων για τους υπολογιστές στην πολιτική ασφάλειας του δικτύου. Εκτός από τους ίδιους τους υπολογιστές, ειδικές υπηρεσίες ή διεργασίες μπορούν επίσης να ταξινομηθούν. Για παράδειγμα, σε ένα UNIX μηχάνημα που χρησιμοποιείται για να φιλοξενήσει ένα δημόσιο web site, ο web server μπορεί να ταξινομηθεί με έναν τρόπο, ενώ ο telnet server να έχει ένα πολύ υψηλότερο επίπεδο ασφάλειας.

Τέλος, όλοι οι χρήστες και οι δυνητικοί χρήστες πρέπει να ταξινομηθούν. Η ταξινόμηση ενός χρήστη ονομάζεται Επίπεδο Εκκαθάρισης και χρησιμοποιείται για να καθορίσει σε ποια στοιχεία και πόρους ένας χρήστης μπορεί να έχει πρόσβαση. Σε γενικές γραμμές, η πρόσβαση επιτρέπεται μόνο όταν η εκκαθάριση είναι στο ίδιο επίπεδο ή υψηλότερη από την κατάταξη του στοιχείου που έχει πρόσβαση (δεδομένα, εξοπλισμός ή φυσική τοποθεσία).

Επίπεδα Ασφάλειας

Θα πρέπει να καθοριστούν και να περιγραφούν τα επίπεδα της ταξινόμησης που έχουν νόημα και είναι κατάλληλα για τον οργανισμό. Μια προσέγγιση μπορεί να είναι ως εξής:

- Αδιαβάθμητο: Θεωρούνται προσβάσιμα στο κοινό. Δεν υπάρχουν απαιτήσεις για τον έλεγχο της πρόσβασης ή της εμπιστευτικότητας.
- Διαμοιραζόμενο: Πόροι που μοιράζονται σε ομάδες ή με άτομα εκτός οργανισμού. Τα δεδομένα στα οποία υπάρχει πρόσβαση από άτομα ή ομάδες που βρίσκονται εκτός οργανισμού μπορούν να ταξινομηθούν ως διαμοιραζόμενα. Επίσης οι χρήστες από εξωτερικούς οργανισμούς που έχουν νόμιμη πρόσβαση στους εσωτερικούς πόρους θα μπορούσαν επίσης να χαρακτηριστούν ως διαμοιραζόμενοι.
- Ενδοεταιρικό: Η πρόσβαση πρέπει να περιορίζεται σε εσωτερικούς υπαλλήλους μόνο.
- Εμπιστευτικό: Η πρόσβαση πρέπει να περιορίζεται σε μια συγκεκριμένη λίστα των ανθρώπων. Για να έχει κάποιος πρόσβαση στα δεδομένα ή πόρους που χαρακτηρίζονται ως «εμπιστευτικά» θα πρέπει να έχει επίπεδο εκκαθάρισης σε αυτό το επίπεδο και θα πρέπει να συμπεριληφθεί στον κατάλογο πρόσβασης για αυτόν τον πόρο. Ο ιδιοκτήτης του αντικειμένου (ή των δεδομένων του υπολογιστή) είναι υπεύθυνη για τη διαχείριση των καταλόγων πρόσβασης.

Ένα παράδειγμα πίνακα πρόσβασης

Μόλις ολοκληρωθεί το σύστημα ταξινόμησης ένας απλός πίνακας πρόσβασης μπορεί να συνταχθεί:

Πίνακας 4.1: Παράδειγμα πίνακα πρόσβασης

Πίνακας Ελέγχου Πρόσβασης

Υποκείμενο(χρήστης)	Αντικείμενο (Δεδομένα, εξοπλισμός, Φυσική τοποθεσία)			
	Αδιαβάθμητο	Διαμοιραζόμενο	Ενδοεταιρικό	Εμπιστευτικό
Αδιαβάθμητο	Επιτρέπεται	Απαγορεύεται	Απαγορεύεται	Απαγορεύεται
Διαμοιραζόμενο	Επιτρέπεται	Επιτρέπεται	Απαγορεύεται	Απαγορεύεται
Ενδοεταιρικό	Επιτρέπεται	Επιτρέπεται	Επιτρέπεται	Απαγορεύεται
Εμπιστευτικό	Επιτρέπεται	Επιτρέπεται	Επιτρέπεται	Αναφορά στη λίστα πρόσβασης

Ένας πίνακας, όπως ο παραπάνω μπορεί να αποτελέσει έναν οδηγό για το γράψιμο μιας πολιτικής. Τα παραδείγματα πολιτικών που δίνονται παρακάτω κάνουν χρήση αυτού του συστήματος.

4.3 Δόμηση πολιτικών ασφάλειας

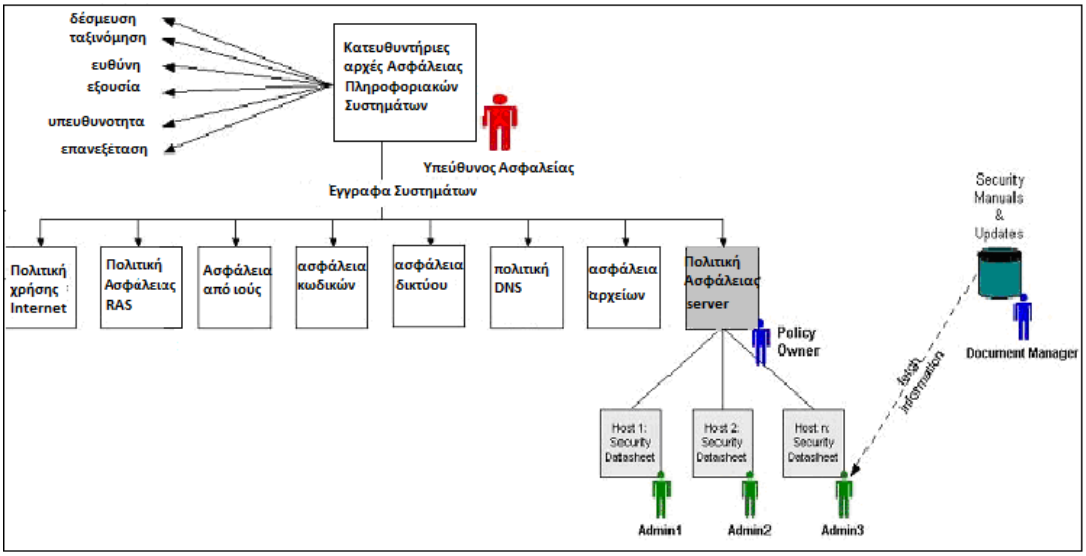
Ένα αποτελεσματικό σύστημα ταξινόμησης μπορεί να βοηθήσει στο να καταστήσει τις πολιτικές ασφαλείας απλούστερες και ευκολότερες για να αναπτυχθούν. Ωστόσο, αν πρόκειται να εφαρμοστεί σε ένα μεγάλο οργανισμό που χρησιμοποιεί μια ποικιλία τεχνολογιών, η ανάπτυξη των πολιτικών, θα απαιτήσει πολλή δουλειά. Είναι σημαντικό οι πολιτικές να δομούνται κατά τέτοιο τρόπο ώστε να είναι όσο το δυνατόν πιο ελαφριές, χωρίς να λείπουν κάποια σημαντικά ζητήματα. Με το «ελαφριά» για μια πολιτική ασφάλειας εννοούμε ότι θα πρέπει να είναι:

- Ελαφριά, χωρίς τη χρήση πολλών δέντρων.
- Απλή και πρακτική.
- Εύκολη στη διαχείριση και τη συντήρηση.
- Εύκολη στην πρόσβαση από ανθρώπους που αναζητούν συγκεκριμένη πληροφορία.

Για να επιτευχθούν τα παραπάνω θα πρέπει η πολιτική να χωριστεί σε έναν αριθμό από επιμέρους πολιτικές που θα οργανώνονται σε ιεραρχική δομή.

Το έγγραφο πλαισίου ασφαλείας

Παρότι κάθε επιμέρους πολιτική θα γράφεται από διαφορετικό συγγραφέα, πρέπει όλες οι επιμέρους πολιτικές να συμφωνούν σε κάποιες θεμελιώδεις αρχές. Αυτές οι αρχές, που αποτελούν και τη φιλοσοφία της ασφάλειας του οργανισμού, πρέπει να καταγράφονται σε ένα μοναδικό έγγραφο γνωστό και ως Έγγραφο Πλαισίου Ασφάλειας. Σε αυτό, πέρα από το σύστημα ταξινόμησης, δημιουργείται ένα πλαίσιο αξιών και αρχών πάνω στις οποίες θα βασιστεί κάθε άλλο έγγραφο. Επίσης λειτουργεί και σαν προεπιλεγμένη πολιτική σε περίπτωση που κάποιο σύστημα δεν καλύπτεται από κάποιο επιμέρους έγγραφο πολιτικής. Όλη αυτή η ιδέα παρουσιάζεται στο Σχήμα 3.



Σχήμα 4.2: Παράδειγμα Εγγράφου Πλαισίου Ασφάλειας

Ας εξετάσουμε κάθε στοιχείο αυτού του πλαισίου με τη σειρά:

Το Έγγραφο Πλαισίου Ασφαλείας ορίζει ένα ελάχιστο σύνολο κατευθυντήριων αρχών ασφαλείας που εφαρμόζονται για τη διοίκηση, το προσωπικού και τους εξωτερικούς συνεργάτες. Το έγγραφο ορίζει ένα σύνολο εννοιών και αρχών που έχουν σχεδιαστεί για να εξασφαλίζουν την προστασία των πληροφοριακών αγαθών, και τις τεχνολογίες που χρησιμοποιούνται για την αποθήκευση και τη μετάδοση τους. Καμία απόφαση σχετικά με την ασφάλεια των πληροφοριών και της τεχνολογίας των πληροφοριών, δεν θα πρέπει να γίνει χωρίς προσεκτική εξέταση, και σωστή συμμόρφωση με τις έννοιες και τις αρχές που περιγράφονται στο έγγραφο-πλαίσιο ασφαλείας.

Το Έγγραφο Πλαισίου Ασφαλείας πρέπει να καλύπτει τουλάχιστον τα εξής σημαντικά σημεία:

1. Την αξία των πληροφοριών και τη δέσμευση του οργανισμού για την ασφάλεια των πληροφοριών.
2. Το σύστημα ταξινόμησης.
3. Την αρχή της ευθύνης που αναφέρει σαφώς ότι οι χρήστες και οι διαχειριστές θα πρέπει να λογοδοτήσουν για συμπεριφορά που επηρεάζει την ασφάλεια των πληροφοριών.
4. Τον ορισμό της εξουσίας στον υπεύθυνο ασφαλείας.
5. Την αρχή της ατομικής ευθύνης όλων των χρηστών του συστήματος για την ασφάλεια των πληροφοριακών πόρων.
6. Την προσέγγιση του οργανισμού στους ελέγχους ασφαλείας. Για παράδειγμα, πόσο συχνά γίνονται και από ποιούς.

Ιδιοκτήτης Πολιτικής

Ο ιδιοκτήτης της πολιτικής είναι το πρόσωπο που είναι υπεύθυνο για τη συντήρηση και την ακεραιότητα ενός συγκεκριμένου εγγράφου πολιτικής. Καμία αλλαγή δεν μπορεί να γίνει σε ένα έγγραφο χωρίς τη ρητή άδεια του ιδιοκτήτη πολιτικής. Το όνομα του πρέπει να εμφανίζεται σαφώς στο έγγραφο και το έγγραφο θα πρέπει πάντα να χρονολογείται και υπογράφεται από αυτόν. Έχοντας έναν ιδιοκτήτη για την πολιτική διασφαλίζεται η συνέπεια της.

Τεχνικές προδιαγραφές ασφαλείας

Συνίσταται κάθε πληροφοριακό σύστημα να έχει ένα έγγραφο τεχνικών προδιαγραφών ασφαλείας (security datasheet). Το έγγραφο αυτό παραθέτει ειδικές ρυθμίσεις και παραμέτρους που εξασφαλίζουν την ασφάλεια του συστήματος. Ενώ το έγγραφο πλαισίου ασφαλείας και τα διάφορα επιμέρους έγγραφα αφορούν την πολιτική εν γένει, το έγγραφο τεχνικών προδιαγραφών παρουσιάζει τις λεπτομέρειες που πρέπει να εφαρμόζονται για κάθε σύστημα.

Είναι ευθύνη των ιδιοκτητών και των χρηστών πληροφοριών και τεχνολογίας να λάβουν τα σχετικά έγγραφα από τον ΥΑ ή την ομάδα ασφαλείας και να διασφαλίσουν ότι τα πρότυπα που ορίζονται σ 'αυτό έχουν εφαρμοστεί σωστά στα συστήματα που ελέγχουν.

Τεχνικοί Οδηγοί

Οι τεχνικοί οδηγοί είναι ένα άλλο σύνολο από χρήσιμα έγγραφα, αν και δεν είναι στην πραγματικότητα πολιτικές. Οι τεχνικοί οδηγοί περιγράφουν την υλοποίηση, τη λειτουργία, τη διαμόρφωση και διαχείριση των συγκεκριμένων συστημάτων. Μπορούν να αγοραστούν έτοιμοι ή ο οργανισμός μπορεί να προσλάβει ειδικούς για να τους γράψουν. Μπορούν να αποθηκευτούν μαζί με τις πολιτικές και να αναφέρονται από τα επιμέρους έγγραφα. Για παράδειγμα, αντί να χρησιμοποιεί ένα επιμέρους έγγραφο να περιγράψει πώς ακριβώς ο Solaris Apache Web server θα πρέπει να ρυθμιστεί, ο οργανισμός μπορεί να γράψει ή ακόμη και να αγοράσει έναν οδηγό που καλύπτει ακριβώς αυτό.

Τι θα έπρεπε να λένε τα επιμέρους έγγραφα

- Πεδίο εφαρμογής - ακριβώς το ζήτημα, οργανωτική μονάδα ή τεχνολογικό σύστημα.
- Διάρκεια ισχύος - κάθε πολιτική πρέπει να έχει περιορισμένη διάρκεια ζωής και να αναθεωρείται σε τακτική βάση.
- Ιδιοκτησία - το όνομα και τα στοιχεία επικοινωνίας για τον «ιδιοκτήτη» του εγγράφου, όπως περιγράφεται παραπάνω σε αυτό.
- Ευθύνες - μια περιγραφή του ποιος είναι υπεύθυνος για ποιά στοιχεία της ασφάλειας συστήματος ή θέματος που καλύπτεται. Αυτό είναι σημαντικό αν κάποιος θέλει να επιβάλει λογοδοσία.
- Τεκμηρίωση - μια αναφορά σε άλλα έγγραφα υψηλότερα ή χαμηλότερα στη δομή της πολιτικής, για παράδειγμα, το έγγραφο πλαισίου ασφαλείας ή ένας συγκεκριμένος τεχνικός οδηγός.
- Δήλωση θέσης - αυτό που πραγματικά θέλω να πω για το θέμα.
- Αξιολόγηση - αν, πότε και πώς θα πραγματοποιηθούν αξιολογήσεις ασφαλείας στα εν λόγω συστήματα.
- Συμμόρφωση - μια δήλωση σχετικά με τις συνέπειες της μη συμμόρφωσης με την πολιτική.

Αξιολογώντας τις πολιτικές

Όταν ένας οργανισμός έχει ένα σύστημα πολιτικών ασφάλειας εγκατεστημένο, θα είναι αναγκαίο να προσδιοριστεί η αποτελεσματικότητα των πολιτικών στο πλαίσιο του οργανισμού. Ο σωστός τρόπος για να γίνει αυτό είναι, βεβαίως, είναι μέσω μιας ακόμα άσκησης αξιολόγησης κινδύνου, ολοκληρώνοντας έτσι τον κύκλο της ασφάλειας. Ωστόσο, μπορεί να είναι δυνατό να εκτιμηθούν σωστά οι πολιτικές, χωρίς να χρειάζεται να

περάσουν από την όλη διαδικασία αξιολόγησης του κινδύνου. Το παρακάτω είναι μια λίστα με απλές ερωτήσεις που το προσωπικό ασφαλείας μπορεί να χρησιμοποιήσει για να αξιολογήσει πόσο αποτελεσματική είναι η πολιτική. Αυτές είναι συνήθως οι ερωτήσεις που οι ελεγκτές και αναλυτές ασφαλείας χρησιμοποιούν, καθώς επανεξετάζουν τους μηχανισμών ασφαλείας:

- Έχει η πολιτική ένα σαφώς προσδιορισμένο πεδίο εφαρμογής; Είναι σαφές σε ποιά συστήματα και ανθρώπους μπορεί να εφαρμοστεί;
- Καλύπτονται επαρκώς όλα τα συστήματα και τα ζητήματα;
- Η πολιτική καθορίζει με σαφήνεια τις ευθύνες; Είναι σαφές για τον τελικό χρήστη και τους διάφορους διαχειριστές τι ακριβώς είναι οι ευθύνες; Είναι σαφές ποιος είναι υπεύθυνος για τις διάφορες πτυχές της ασφάλειας;
- Μπορεί να εφαρμοστεί η πολιτική σε ένα συγκεκριμένο τρόπο, έτσι ώστε η συμμόρφωση είναι μετρήσιμο;
- Είναι η πολιτική προσαρμόσιμη; Μπορεί εύκολα να αλλάξει για να αντιμετωπίσει νέους κινδύνους και νέες τεχνολογίες;
- Είναι η πολιτική που έχει τα επιθυμητά αποτελέσματα του;
- Είναι η πολιτική παγκοσμίως γνωστή και κατανοητή μέσα στην οργάνωση; Η πολιτική διανέμεται σωστά, υπάρχει κατάλληλη επίγνωση της πολιτικής υπάρχει και είναι κατανοητό το περιεχόμενό της;
- Η πολιτική συμμορφώνονται με τη νομοθεσία και με καθήκοντα σε τρίτους; Πληροί ο οργανισμός τις νόμιμες υποχρεώσεις της;

<u>Παγκοσμίως βέλτιστη πρακτική: Μέτρηση πολιτικών ως προς τα Διεθνή Πρότυπα.</u>

Ένας καλός λόγος για έναν οργανισμό να έχει τις πολιτικές ασφάλειας είναι να εμφανίσει ότι λαμβάνει όλα τα εύλογα μέτρα για να εξασφαλίσει την εμπιστευτικότητα και την ακεραιότητα των πληροφοριακών αγαθών του. Δεδομένου ότι η ασφάλεια γίνεται περισσότερο από ένα πρόβλημα δημοσίων σχέσεων, μεγάλοι οργανισμοί θα απαιτήσουν από τους e-business εταίρους τους να συμμορφώνονται με ένα σύνολο κανόνων λειτουργίας που διασφαλίζουν ότι διατηρούνται τα κατάλληλα επίπεδα ασφάλειας. Για παράδειγμα, οι ηγέτες του κλάδου όπως η VISA έχουν ήδη ξεκινήσει τη διαδικασία αυτή με τους συνεργάτες τους.

Εάν εφαρμοστεί σωστά, ένα πρότυπο όπως το ISO 17799 μπορεί να προωθήσει σημαντικά τους στόχους ασφάλειας του IT ενός οργανισμού, αλλά οι αναγνώστες θα

πρέπει να γνωρίζουν ότι αυτό δεν είναι το μόνο διαθέσιμο πρότυπο ασφαλείας σήμερα. Είναι σημαντικό για έναν οργανισμό που ξεκινά την μακρά και σκληρή (και ακριβή!) διαδρομή προς την πιστοποίηση να καταλάβει ποιο είναι η προβλεπόμενο πρότυπο ασφάλειας που θα προσφέρει στον οργανισμό και τους επιχειρηματικούς εταίρους σε μακροπρόθεσμη βάση.

Εάν ένας οργανισμός εξετάζει τη διάρθρωση των πολιτικών του, στο πλαίσιο ενός προτύπου ασφαλείας όπως ISO 17799, εδώ είναι μερικά ζητήματα που θα πρέπει να το εξετάσει:

- Αναγνώριση - Εάν ένας κύριος σκοπός της πιστοποίησης για έναν οργανισμό είναι να εξασφαλίσει στους πελάτες του την ετοιμότητα ως προς την ασφάλεια, η πιστοποίηση που θα επιλεγεί θα πρέπει να έχει φήμη στην αγορά Αυτό είναι πιθανώς ο πιο σημαντικός παράγοντας.
- Εστίαση - Τα διάφορα προγράμματα πιστοποίησης έχουν την τάση να εστιάζουν σε διαφορετικές πτυχές της ασφάλειας IT. Για παράδειγμα, η GMITS παίρνει μια προσέγγιση προσανατολισμένη στην επιχείρηση, ενώ η ITSEC εστιάζει στην τεχνολογία. Μια διαδρομή πιστοποίησης θα πρέπει να επιλέγεται έτσι ώστε να είναι συμβατή με τους στόχους ασφάλειας του οργανισμού σας.
- Τοπική παρουσία - Εκτός από το κυρίως μέρος των προτύπων η διαδικασία πιστοποίησης συνήθως απαιτεί τη συμμετοχή των δύο άλλων μερών - τον σύμβουλο διαδικασίας που θα καθοδηγεί μέσα στην πιστοποίηση και τους αξιολογητές οι οποίοι κάνουν την πιστοποίηση.
- Κόστος - Το κόστος της πιστοποίησης πρέπει να σταθμίζεται σε σχέση με την τιμή που προσφέρει.
- Αντοχή - Η διαδικασία πιστοποίησης πρέπει να έχει μακροπρόθεσμα οφέλη που αντισταθμίζουν το κόστος. Αυτό σημαίνει:
    - Τα αποτελέσματα της διαδικασίας θα πρέπει να είναι απτά.
    - Η διαδικασία δεν θα πρέπει να επαναληφθεί πολλές φορές
- Αντικειμενικότητα - Δεν είναι γενικά μια καλή ιδέα να ελεγχθεί επίσημα ένας οργανισμός από τις εταιρείες που πωλούν επίσης τα προϊόντα ασφάλειας.

4.4 Ένα δείγμα πολιτικής ασφάλειας

Αυτή είναι το τέταρτο μέρος της ανάλυσης για τις πολιτικές ασφάλειας. Στο πρώτο, εξετάσαμε τι είναι πολιτικές και τι μπορούν να επιτύχουν. Στο δεύτερο μέρος είδαμε την υποστήριξη που απαιτείται από τον οργανισμό για την υλοποίηση επιτυχημένων πολιτικών ασφάλειας. Στο τρίτο συζητήθηκε το πώς αναπτύσσεται και να δομείται μια πολιτική ασφαλείας. Σε αυτό το μέρος θα ρίξουμε μια ματιά σε μερικά παραδείγματα πολιτικών ασφαλείας.

Παράδειγμα πολιτικής ασφαλείας IP Network

Αυτή η ενότητα περιέχει ένα παράδειγμα ενός εγγράφου πολιτικής ενός δικτύου IP για μια φανταστική εταιρεία που θα ονομάζουμε "Foobar". Η πολιτική που καταγράφεται εδώ κάνει εκτεταμένη χρήση του συστήματος ταξινόμησης που εξηγήθηκε στο δεύτερο μέρος του κεφαλαίου.

Ο σκοπός αυτής της πολιτικής είναι να διασφαλιστεί ότι όλα τα συστήματα που έχουν εγκατασταθεί στο δίκτυο του οργανισμού διατηρούνται σε κατάλληλα επίπεδα ασφάλειας, ενώ ταυτόχρονα δεν παρεμποδίζουν την δυνατότητα των χρηστών της Foobar και του προσωπικού υποστήριξης να εκτελούν την εργασία τους. Ο σκοπός είναι:

- να καθοριστεί που πρέπει να τοποθετείται στο δίκτυο ο εξοπλισμός.
- να οριστεί ποιος μπορεί να έχει πρόσβαση στον εξοπλισμό δικτύου.
- να καθοριστεί πως ο τρόπος πρόσβασης στον εξοπλισμό θα πρέπει να ελέγχεται.
- να καθοριστεί πώς τα δεδομένα που ταξιδεύουν μέσω του δικτύου πρέπει να προστατεύονται.

Αυτή η πολιτική ισχύει για:

- Όλα τα δίκτυα IP (υφιστάμενων και μελλοντικών) στα οποία είναι συνδεδεμένος εξοπλισμός δικτύου της Foobar.
- Όλο τον εξοπλισμό που συνδέεται με τα δίκτυα.
- Όλα τα IP δίκτυα στα οποία τα δεδομένα τις Foobar ταξιδεύουν.
- Τους διαχειριστές δικτύου που χειρίζονται τον εξοπλισμό.
- Τους επικεφαλής έργων που απαιτούν το νέο εξοπλισμό που πρόκειται να συνδεθεί με το δίκτυο

- Όλους οι χρήστες που χρησιμοποιούν τον εξοπλισμό που είναι συνδεδεμένος με το δίκτυο.

Αυτό περιλαμβάνει, μεταξύ άλλων, το χρήστη στο LAN, το server, τον backup server, όλες τις υπηρεσίες κορμού, switches, ADSL κλπ, και τέλος τα απομακρυσμένα sites.

Η πολιτική αυτή θα ισχύει και για όλες τις συσκευές που συνδέονται με τα δίκτυα που αναφέρονται πιο πάνω, καθώς και για όλους τους εργαζόμενους που χρησιμοποιούν κάποιον από αυτόν τον εξοπλισμό.

Η πολιτική ασφαλείας βασίζεται στις αρχές και στις κατευθυντήριες γραμμές που περιγράφονται στο έγγραφο πλαισίου ασφάλειας πληροφοριών του οργανισμού. Όλος ο εξοπλισμός δικτύου (δρομολογητές, servers, σταθμοί εργασίας κλπ.) πρέπει να κατατάσσεται σύμφωνα με το πρότυπο σύστημα ταξινόμησης του οργανισμού και τοποθετείται σε ένα τμήμα του δικτύου που αντιστοιχεί στο επίπεδο της ταξινόμησης. Η πρόσβαση σε ένα τέτοιο τμήμα θα πρέπει να ελέγχεται με κατάλληλο τρόπο. Κάθε φορά που τα δεδομένα ταξιδεύουν πάνω από μια κατάτμηση του δικτύου χαμηλότερης διαβάθμισης ασφαλείας τότε τα δεδομένα θα πρέπει να προστατεύονται κατά τρόπο που να αρμόζει στο επίπεδο της ταξινόμησης.

Ταξινόμηση

Σύμφωνα με το έγγραφο πλαισίου ασφάλειας, όλοι οι χρήστες και τα δεδομένα θα πρέπει να χαρακτηριστούν σε κάποιο από τα επίπεδα ασφάλειας: 1 (μη ταξινομημένο), 2 (διαμοιραζόμενο), 3 (ενδοεταιρικό) ή 4 (εμπιστευτικό). Όλα τα φυσικά τμήματα του δικτύου, IP υποδίκτυα και άλλοι φορείς της IP κίνησης πρέπει να κατατάσσονται με τον ίδιο τρόπο. Όλα τα δεδομένα που ταξιδεύουν σε ένα δίκτυο IP θα πρέπει να ταξινομηθούν, και όλοι οι χρήστες που χρησιμοποιούν τον εξοπλισμό του δικτύου ή ζητούν δεδομένα μέσω του δικτύου πρέπει να τους εκχωρηθεί ένα επίπεδο εκκαθάρισης σύμφωνα με το ίδιο σύστημα.

Κατάτμηση δικτύου

- Όλα τα τμήματα δικτύου ταξινομούνται ως Επίπεδο 1 – Αταξινόμητα, εκτός αν αναφέρεται κάτι άλλο στο έγγραφο πλαισίου ασφάλειας.
- Η ταξινόμηση των τμημάτων του δικτύου δίδεται παρακάτω στην ενότητα στην παράγραφο Συζήτηση για τις Ταξινομήσεις.
- Ένα τμήμα του δικτύου μπορεί να χαρακτηριστεί ως ένα άλλο επίπεδο ασφαλείας μόνο με την έγκριση του Διευθυντή Ασφαλείας. Το νέο επίπεδο διαβάθμισης

πρέπει να καταγράφεται σε αυτό το έγγραφο και όλοι οι προϊστάμενοι τμημάτων πρέπει να ενημερώνονται.

- Όταν ένα τμήμα του δικτύου συνδέεται με ένα άλλο τμήμα του δικτύου με ένα διαφορετικό επίπεδο ασφάλειας, τότε η σύνδεση μεταξύ των δύο δικτύων θα πρέπει να ελέγχεται από ένα αξιόπιστο εγκεκριμένο σημείο. Ένα αξιόπιστο σημείο είναι εξοπλισμός ικανός να ρυθμίζει την ροή της κυκλοφορίας μεταξύ των δύο τμημάτων του δικτύου με τρόπο κατάλληλο για την κατάταξη των δικτύων. Τα αξιόπιστα σημεία καλύπτονται λεπτομερώς στην παράγραφο που ακολουθεί.
- Δεν μπορεί να συνδεθεί εξοπλισμός δικτύου σε ένα τμήμα του δικτύου που δεν είναι του ίδιου επιπέδου ασφάλειας με αυτόν.
- Ο ΥΑ του οργανισμού μπορεί επίσης να επιλέξει να διαχωρίσει δύο δίκτυα του ίδιου επιπέδου ασφάλειας.

Αξιόπιστα σημεία

- Το αξιόπιστο σημείο που χρησιμοποιείται μεταξύ των δύο τμημάτων δικτύου θα πρέπει να είναι κατάλληλο για το δίκτυο με το υψηλότερο επίπεδο ασφάλειας.
- Η προεπιλεγμένη συμπεριφορά τους είναι να αρνούνται όλες τις IP κίνησης μεταξύ των τμημάτων του δικτύου που προστατεύει.
- Κατά την κρίση του Διευθυντή Ασφαλείας Foobar, η προεπιλεγμένη (default) συμπεριφορά της εμπιστοσύνης σημείο μπορεί να είναι να επιτρέψει σε όλους τους κίνηση έξω από το δίκτυο με το υψηλότερο επίπεδο ασφάλειας, ενώ αρνείται κάθε κίνηση μέσα.
- Κατά την κρίση του ΥΑ, η default συμπεριφορά θα μπορούσε να είναι να επιτρέπεται η εξερχόμενη κίνηση από το δίκτυο με το μεγαλύτερο επίπεδο ασφάλειας ενώ η εισερχόμενη κίνηση να απορρίπτεται.
- Όλα τα αξιόπιστα σημεία θα πρέπει να είναι πλήρως υπό τον έλεγχο του ΥΑ και η πρόσβαση σε οποιοδήποτε αξιόπιστο σημείο πρέπει να χορηγούνται μόνο με τη ρητή άδεια του.
- Υπάρχει ένας αριθμός τεχνολογιών που μπορούν να δράσουν ως αξιόπιστα σημεία. Αυτά χωρίζονται στις ακόλουθες κατηγορίες:
    - Έλεγχος Επιπέδου Δικτύου: TCP wrappers, host. allow λίστες, δρομολογητές, firewalls επιπέδου δικτύου, V-LAN switches κλπ.

- Έλεγχος επιπέδου χρήστη: proxy εφαρμογής, firewalls σε επίπεδο χρήστη, πιστοποιητικά κλπ.

- Κάθε φορά που υπάρχει μια σύνδεση που παρακάμπτει ένα επίπεδο ασφάλειας πρέπει να χρησιμοποιείται ισχυρός έλεγχος σε επίπεδο χρήστη. Ακόμα και αν χρησιμοποιείται ισχυρός έλεγχος χρήστη, η σύνδεση δεν πρέπει να παραλείπει περισσότερα από ένα επίπεδο.
- Ο έλεγχος της κυκλοφορίας πρέπει να ασκείται με τον τρόπο που αναφέρεται παρακάτω:

Πίνακας 4.2: Για συνδέσεις σε τμήματα με ταξινόμηση: Μη ταξινομημένο

Από	Τύπος Ελέγχου
Μη ταξινομημένο	Κανένας Έλεγχος
Διαμοιραζόμενο	Κανένας Έλεγχος
Ενδοεταιρικό	Κανένας Έλεγχος
Εμπιστευτικό	Κανένας Έλεγχος

Πίνακας 4.3: Για συνδέσεις σε τμήματα με ταξινόμηση: Διαμοιραζόμενο

Από	Τύπος Ελέγχου
Μη ταξινομημένο	Κανένας Έλεγχος
Διαμοιραζόμενο	Κανένας Έλεγχος
Ενδοεταιρικό	Κανένας Έλεγχος
Εμπιστευτικό	Κανένας Έλεγχος

Πίνακας 4.4: Για συνδέσεις σε τμήματα με ταξινόμηση: Ενδοεταιρικό

Από	Τύπος Ελέγχου
Μη ταξινομημένο	Μέσω ενός proxy: Έλεγχος επιπέδου δικτύου από και προς τον proxy Άμεση: Ισχυρός έλεγχος επιπέδου χρήστη

Διαμοιραζόμενο	Έλεγχος επιπέδου δικτύου
Ενδοεταιρικό	Κανένας Έλεγχος
Εμπιστευτικό	Κανένας Έλεγχος

Πίνακας 4.5: Για συνδέσεις σε τμήματα με ταξινόμηση: Εμπιστευτικό

Από	**Τύπος Ελέγχου**
Μη ταξινομημένο	Δεν επιτρέπεται
Διαμοιραζόμενο	Δεν επιτρέπεται
Ενδοεταιρικό	Ισχυρός έλεγχος επιπέδου χρήστη
Εμπιστευτικό	Κανένας Έλεγχος

Τα δεδομένα κατά τη μεταφορά

- Δεδομένα που διακινούνται στο δίκτυο μεταξύ οποιωνδήποτε δύο στοιχείων του δικτύου θεωρείται ότι είναι "δεδομένα κατά τη μεταφορά". Αυτό περιλαμβάνει τις συνεδρίες ελέγχου και διαχείρισης.
- Όλες οι τεχνολογίες δικτύου θεωρούνται είτε "ασφαλείς" είτε "μη ασφαλείς" σε φυσική κατάσταση (δηλαδή χωρίς κρυπτογράφηση). Τα μόνα δίκτυα που θεωρούνται ως ασφαλείς από τον οργανισμό είναι τα Frame Relay-PVC και τα switched Ethernet LANs. Όλοι οι άλλοι τύποι δικτύου θεωρείται επισφαλή.
- Όλα τα δεδομένα που διέρχονται πάνω από ένα μη ασφαλές τμήμα του δικτύου που έχει μια κατάταξη χαμηλότερη από την ταξινόμηση των δεδομένων θα πρέπει να προστατεύονται από κρυπτογράφηση δεδομένων. Τα δεδομένα που διέρχονται πάνω από ασφαλές τμήμα του δικτύου μπορεί να κρυπτογραφούνται αναλόγως την κρίση του ΥΑ.
- Η κρυπτογράφηση των δεδομένων κατά τη μεταφορά μπορεί να λάβει οποιαδήποτε από τις ακόλουθες μορφές:
    - Κρυπτογράφηση δικτύου, όπου τα δεδομένα κρυπτογραφούνται στο IP στρώμα (για παράδειγμα, με το IPSec)

- κρυπτογράφηση συνεδρίας, στην οποία τα δεδομένα κρυπτογραφούνται σε ένα στρώμα TCP (π.χ. με SSL)
- κρυπτογράφηση μηνύματος, όπου κομμάτια των δεδομένων είναι κρυπτογραφημένα πριν σταλούν (π.χ. με SMIME)
- κρυπτογράφηση δεδομένων, όπου ολόκληρο το πακέτο δεδομένων είναι κρυπτογραφημένο πριν σταλεί (π.χ. με κρυπτογράφηση αρχείων)

- Τα συστήματα κρυπτογράφησης που χρησιμοποιούνται πρέπει να προσφέρουν ισχυρή κρυπτογράφηση (κλειδιά κρυπτογράφησης με πάνω από 100 bit) και να χρησιμοποιούν διεθνώς αναγνωρισμένους αλγόριθμους κρυπτογράφησης. Η επιλογή του κρυπταλγόριθμου είναι ευθύνη του ΥΑ και καταγράφεται στο έγγραφο πολιτικής του οργανισμού για κρυπτογραφία.

Συζήτηση για τις Ταξινομήσεις

Ταξινόμηση χρηστών:

Κάθε χρήστης ορίζεται ως μη ταξινομημένος μέχρι να αλλάξει ρητά την κατάταξη του/της με έγγραφη έγκριση ο ΥΑ. Όταν ένας νέο υπάλληλος προσληφθεί ο προϊστάμενος του ζητάει από τον ΥΑ να του αποδώσει ένα επίπεδο εκκαθάρισης. Συνήθως, επιλέγεται η κλάση Ενδοεταιρικό, αφού όμως έχει υπογράψει συμφωνία μη αποκάλυψης πληροφοριών.

Ταξινόμηση του εξοπλισμού:

- Σε όλο τον εξοπλισμό πληροφορικής πρέπει να δοθεί μια κατάταξη από τον ΥΑ.
- Οι ταξινομήσεις για τον υπάρχοντα εξοπλισμό έχουν ως εξής:
  - Όλοι οι σταθμοί εργασίας χρηστών, servers αρχείων/εκτυπωτών κτλ θα πρέπει να χαρακτηριστούν ως «Ενδοεταιρικά"
  - Όλοι οι διακομιστές LAN και άλλοι κόμβοι του δικτύου που χρησιμοποιούνται για τη διαχείριση της υποδομής εσωτερικού δικτύου ή του δικτύου κορμού θα πρέπει να χαρακτηριστούν ως «Εμπιστευτικό»
  - Όλος ο εξοπλισμός κορμού (συμπεριλαμβανομένων των switches, servers απομακρυσμένης πρόσβασης, υλικό για ADSL κλπ) που δεν βρίσκεται στο χώρο του οργανισμού θα πρέπει να χαρακτηριστεί ως "Διαμοιραζόμενο"
  - Όλος ο εξοπλισμός που χρησιμοποιείται για τη μεταφορά δεδομένων προς και από το Internet θα χαρακτηριστεί ως " Διαμοιραζόμενο ".

- Ο ΥΑ πρέπει να διατηρεί μια πλήρη λίστα των ταξινομήσεων του συνόλου του εξοπλισμού πληροφορικής στο δίκτυο και στον κορμό του οργανισμού.

Ταξινόμηση των Δικτύων:

Ο ΥΑ πρέπει να ταξινομεί κάθε τμήμα του δικτύου που αποτελεί μέρος της υποδομής. Οι ταξινομήσεις για τα τμήματα του δικτύου έχουν ως εξής:

- Το LAN χρηστών του οργανισμού έχει ταξινομηθεί ως Ενδοεταιρικό.
- Οι servers & backup servers του LAN ταξινομούνται ως Εμπιστευτικοί.
- Το δίκτυο κορμού Frame Relay έχει ταξινομηθεί ως Διαμοιραζόμενο.
- Οι απομακρυσμένες περιοχές ταξινομούνται ως Διαμοιραζόμενο.

Ταξινόμηση δεδομένων:

Τα καινούργια δεδομένα πρέπει αρχικά να ταξινομούνται σαν «Ενδοεταιρικά» μέχρι να αναταξινομηθούν από κάποιον χρήστη ο οποίος φέρει και την ευθύνη για αυτή την αλλαγή. Οι ταξινομήσεις για τα υπάρχοντα δεδομένα του οργανισμού δίνονται παρακάτω:

- Οι επιχειρηματικές πληροφορίες του οργανισμού (υπομνήματα, οικονομικά έγγραφα, έγγραφα σχεδιασμού κλπ) θα πρέπει να χαρακτηριστεί ως «Ενδοεταιρικά»
- Τα δεδομένα των πελατών του οργανισμού (στοιχεία επικοινωνίας, συμβάσεις, κλπ.) πρέπει να χαρακτηριστούν ως «Ενδοεταιρικά»
- Τα δεδομένα του δικτύου διαχείρισης (IP διευθύνσεις, κωδικούς πρόσβασης, τα αρχεία ρυθμίσεων, κλπ.) πρέπει να χαρακτηριστούν ως «Εμπιστευτικό»
- Οι πληροφορίες ανθρωπίνου δυναμικού (συμβάσεις εργασίας, πληροφορίες αμοιβών, κλπ.) θα πρέπει να ταξινομείται «Εμπιστευτικό»
- Οι δημοσιευμένες πληροφορίες (φυλλάδια, εκθέσεις για τις επιδόσεις, υλικό μάρκετινγκ, κλπ.) θα πρέπει να ταξινομείται «Διαμοιραζόμενο»
- Τα e-mail μεταξύ των εργαζομένων ταξινομούνται ως «Ενδοεταιρικά»
- Τα e-mail μεταξύ των εργαζομένων του οργανισμού και εργαζομένων εξωτερικών μερών θα πρέπει να θεωρούνται ως «Αταξινόμητα».

<u>Ρόλοι και ευθύνες</u>

- Είναι ευθύνη του χρήστη να:
    - γνωρίζει το δικό του επίπεδο εκκαθάρισης και να κατανοήσει τα δικαιώματα και τους περιορισμούς που συνδέονται με αυτό
    - βεβαιωθεί ότι όλα τα δεδομένα που αυτός λειτουργεί έχουν σωστά ταξινομηθεί
    - διασφαλίσει ότι αντιλαμβάνεται τους περιορισμούς που σχετίζονται με τα δεδομένα που αυτός εργάζεται
    - βεβαιωθεί ότι στεγάζονται και προστατεύονται κατάλληλα όλα τα δεδομένα με τα οποία αυτός ή αυτή εργάζεται.
- Είναι ευθύνη των ιδιοκτητών και διαχειριστών του συστήματος να:
    - προσδιορίσουν το επίπεδο ασφάλειας ενός χρήστη, πριν του παραχωρηθεί πρόσβαση σε οποιοδήποτε σύστημα
    - ελέγχουν την ταξινόμηση του εξοπλισμού που διαχειρίζονται
    - βεβαιωθούν ότι ο εξοπλισμός έχει εγκατασταθεί και προστατεύεται σύμφωνα με την κατάταξή του
- Είναι ευθύνη του κάθε διευθυντή τμήματος να:
    - λάβει την έγκριση για τους υπαλλήλους του τμήματα της?
    - αποσαφηνίσει την ταξινόμηση των στοιχείων σχετικά με τα συστήματα κάτω από τον έλεγχο του
    - αποσαφηνίσει την ταξινόμηση του εξοπλισμού στο πλαίσιο του ελέγχου και να διασφαλίσει ότι τα εν λόγω συστήματα έχουν εγκατασταθεί σωστά
    - εξασφαλίσει ότι όλοι οι εργαζόμενοι στο εν λόγω τμήμα κατανοούν και να εφαρμόζουν αυτή την πολιτική
- Είναι η ευθύνη του Υπευθύνου Ασφαλείας να:
    - εγκρίνει όλες τις ταξινομήσεις
    - τηρεί κατάλογο όλων των ταξινομήσεων
    - εγκρίνει την τελική διαμόρφωση του δικτύου κορμού
    - ελέγχει και να διαχειρίζεται όλα των αξιόπιστα σημεία

- καθορίζει το είδος της κρυπτογράφησης που πρέπει να χρησιμοποιηθεί για την προστασία των δεδομένων κατά τη μεταφορά

Συμμόρφωση

- Κάθε χρήστης με πρόσβαση σε δεδομένα, εξοπλισμό ή μια φυσική τοποθεσία, αν δεν έχει επαρκή εκκαθάριση μπορεί να αντιμετωπίσει πειθαρχικές κυρώσεις, απόλυση και ποινικές διώξεις.
- Κάθε χρήστης που επιτρέπει την πρόσβαση σε ένα σύστημα, που ελέγχεται από αυτόν, για κάποιον με ανεπαρκή εκκαθάριση μπορεί να αντιμετωπίσει πειθαρχικές κυρώσεις, απόλυση και ποινικής δίωξη.
- Κάθε πρόσωπο που συνδέει εξοπλισμό που δεν έχει ταξινομηθεί με το δίκτυο ή συνδέει εξοπλισμό σε ακατάλληλο μέρος του δικτύου ή σε ακατάλληλη θέση μπορεί να αντιμετωπίσει πειθαρχικές κυρώσεις, απόλυση και ποινική δίωξη.
- Κάθε πρόσωπο που μεταδίδει δεδομένα σε οποιοδήποτε δίκτυο χωρίς την κατάλληλη προστασία κρυπτογράφησης για τα δεδομένα αυτά μπορεί να αντιμετωπίσει πειθαρχικές κυρώσεις, απόλυση και ποινική δίωξη.
- Κάθε πρόσωπο που μεταβάλλει την κατάταξη των δεδομένων με τρόπο που να είναι επικίνδυνος, ανεύθυνος ή επιζήμιος για τον οργανισμό, τους μετόχους ή τους πελάτες ενδέχεται να αντιμετωπίσει πειθαρχικές κυρώσεις, απόλυση και ποινική δίωξη.

4.5 Συμπέρασμα

Εδώ θα κάνουμε μια σύνοψη των σημαντικών σημείων που πρέπει να κρατήσει κανείς για τις πολιτικές ασφάλειας:

- Εάν οι πολιτικές εφαρμόζονται σωστά, μπορούν να γίνουν ένα αποτελεσματικό και αποδοτικό μέρος του οπλοστασίου της ασφάλειας πληροφοριών. Επειδή οι πολιτικές ασφαλίζουν το «ανθρώπινο στοιχείο», αντιμετωπίζουν ένα στοιχείο του κινδύνου που σπάνια αγγίζεται από την τεχνολογία.

- Οι πολιτικές θα πρέπει να γραφτούν για την αντιμετώπιση συγκεκριμένου προφίλ κινδύνου και όχι γενικά κι αόριστα και θα πρέπει να βασίζονται στα ευρήματα της ανάλυσης του κινδύνου ασφάλειας.
- Οι πολιτικές μπορεί να είναι αποτελεσματικές μόνο σε ένα εταιρικό περιβάλλον που κάνει την ασφάλεια πληροφοριών να αποτελεί υψηλή προτεραιότητα.
- Οι πολιτικές πρέπει να είναι εύκολες ως προς την πρόσβαση, τη χρήση και την κατανόηση. Για να διευκολυνθεί αυτό, τα έγγραφα πρέπει να δομηθούν σε ένα ιεραρχικό τρόπο με έγγραφα που έχουν διαφορετικά επίπεδα λεπτομέρειας.
- Παρά το γεγονός ότι το πραγματικό περιεχόμενο των εγγράφων πολιτικής θα πρέπει να διαφέρει ριζικά από οργανισμό σε οργανισμό, υπάρχουν κάποιες θεμελιώδεις αρχές που κάθε πολιτική πρέπει να εφαρμόζει.

Μόλις οι πολιτικές έχουν εφαρμοστεί θα έχουμε ένα δομημένο, επίσημο πλαίσιο για την καθοδήγηση της στρατηγικής ασφαλείας και σύμφωνα με το οποίο η πρόοδος της διαδικασίας μπορεί να μετρηθεί.

ΚΕΦΑΛΑΙΟ 5

Τεχνική Ανάλυση Κινδύνων και Μηχανισμών Προστασίας

5.1 Κίνδυνοι, Ευπάθειες και Επιθέσεις

5.1.1 Επιθέσεις στο δίκτυο

Μία επίθεση σε κάποιον οργανισμό εκτυλίσσεται σε πολλά στάδια. Στα αρχικά στάδια ο επιτιθέμενος έχει λιγοστές πληροφορίες σχετικά με τον στόχο.

Ένα από τα πρωταρχικά μελήματα του επιτιθέμενου είναι η συλλογή πληροφοριών για τις ευπάθειες του στόχου. Αυτού του είδους οι επιθέσεις ονομάζονται εξερευνητικές επιθέσεις (reconnaissance attacks) και σκοπός τους είναι η μη εξουσιοδοτημένη συλλογή πληροφοριών για τις ευπάθειες του συστήματος ή, εν γένει, του οργανισμού. Αυτό το πετυχαίνει με ανιχνευτές πακέτων (packet sniffers), με σάρωση των ports (port scan), με συνεχή pings (ping sweep) και με ερωτήματα (internet information queries) όπως, για παράδειγμα, DNS ερωτήματα.

Για να αντιμετωπιστούν αυτού του είδους οι επιθέσεις χρησιμοποιούμε διάφορες τεχνικές. Κατ' αρχήν τα pings και τα port scans δεν είναι παράνομο να γίνουν, οπότε πρέπει να βρούμε εξυπνότερους τρόπους αντιμετώπισης. Όσον αφορά τα pings, αποτρέπουμε τις συσκευές που βρίσκονται στις παρυφές του δικτύου μας να απαντούν σε pings, ενώ για τα port scans χρησιμοποιούμε συστήματα IPS/IDS, που θα αναλυθούν σε ύστερο κεφάλαιο.

Ένα άλλο είδος επιθέσεων είναι οι επιθέσεις άρνησης παροχής υπηρεσιών (Denial of Service attacks και Distributed Denial of Service attacks). Εδώ ο επιτιθέμενος δεν χρειάζεται να έχει βαθιά γνώση του συστήματος στο οποίο επιτίθεται. Μία DoS επίθεση σε κάποιον εξυπηρετητή περιλαμβάνει την αποστολή τεράστιου αριθμού αιτημάτων σε αυτόν, με αποτέλεσμα να μειώσει δραματικά την απόδοση του και να μην μπορεί να εξυπηρετήσει τα αιτήματα καλόβουλων χρηστών. Οι DDoS επιθέσεις είναι η επόμενη

γενιά επιθέσεων DoS, καθώς οι συγκεκριμένες επιθέσεις γίνονται από πολλαπλές πηγές, πιθανώς από ανύπαρκτες IP διευθύνσεις ή από υπολογιστές που έχουν υποστεί επιθέσεις.

Η αντιμετώπιση τέτοιου είδους επιθέσεων είναι δύσκολη και αδύνατο να εξαλειφθεί. Έτσι, σκοπός μας είναι ο περιορισμός τους. Για αυτό το λόγο, χρησιμοποιούμε τα anti-spoofing και anti-DoS εργαλεία στους routers και στα firewalls, καθώς και με περιορισμό στο ρυθμό μεταφοράς συγκεκριμένων ειδών κινήσεων. Για παράδειγμα, περιορίζουμε στο ελάχιστο το ποσοστό του bandwidth μας που μπορεί να καταληφθεί από το πρωτόκολλο ICMP που αφορά τα pings.

Τέλος, υπάρχουν οι επιθέσεις πρόσβασης (access attacks), οι οποίες εκμεταλλεύονται γνωστές ευπάθειες σε διάφορους τομείς, όπως υπηρεσίες αυθεντικοποίησης, FTP και WEB εξυπηρετητές κ.α. Σε αυτές περιλαμβάνονται επιθέσεις σε passwords, εκμετάλλευση εμπιστοσύνης, ανακατεύθυνση ports, man-in-the-middle επιθέσεις και υπερχείλιση καταχωρητών.

5.1.2 Επιθέσεις στους τερματικούς σταθμούς

Στην προηγούμενη παράγραφο ασχοληθήκαμε με τις επιθέσεις που έχουν ως στόχο τη συλλογή πληροφοριών ή την απόκτηση πρόσβασης στο δίκτυό μας. Σε αυτήν την παράγραφο θα εξετάσουμε πιο εξελιγμένες μεθόδους που διαθέτουν νοημοσύνη. Βασίζονται είτε σε κακόβουλο κώδικα, είτε σε πληροφορίες που έχουν συγκεντρωθεί σε προγενέστερο χρόνο, είτε στη χρήση πρόσβασης που αποκτήθηκε εκ των έσω. Οι τερματικοί σταθμοί είναι ιδιαίτερα ευάλωτοι, αν δεν προστατεύονται όπως πρέπει. Κι αυτό γιατί έχουν να αντιμετωπίσουν τρεις κατηγορίες επιθέσεων: σκουλήκια (worms), ιούς (viruses) και δούρειους ίππους (Trojan Horses).

Ο ιός είναι ένα κακόβουλο πρόγραμμα, που προσκολλά τον εαυτό του σε κάποιο άλλο πρόγραμμα και εκτελεί ανεπιθύμητες ενέργειες σε κάποιον υπολογιστή. Η διάδοσή του γίνεται μολύνοντας άλλα προγράμματα στον ίδιο υπολογιστή. Η επίδραση του μπορεί να περιορίζεται σε απλή ενόχληση στο χρήστη, μέσω της προβολής ενός ενοχλητικού μηνύματος, μέχρι την πρόκληση σοβαρότατων ζημιών, όπως τη διαγραφή δεδομένων ολόκληρων δίσκων. Οι ιοί δεν μπορούν να διαδοθούν χωρίς ανθρώπινη παρέμβαση, κα διαδίδονται με ενέργειες όπως το άνοιγμα ενός αρχείου σε κάποιο USB stick ή σε κάποιο e-mail.

Ο Δούρειος Ίππος ένας γενικός όρος που αναφέρεται σε προγράμματα που, εν πρώτοις και φαινομενικά, είναι επιθυμητά, αλλά στην πραγματικότητα είναι επικίνδυνα. Μπορούν να επιτελούν ζημιογόνες ενέργειες ή να φέρουν τα ίδια κάποιον ίο ή worm.

Ένα worm περιέχει και εκτελεί κακόβουλο κώδικα και εγκαθίσταται στη μνήμη του μολυσμένου υπολογιστή. Από εκεί μπορεί να μολύνει και κάποιον άλλον υπολογιστή. Παρόλο που και το worm είναι πρόγραμμα, όπως ο ιός, και μπορεί να διαδοθεί και σε άλλους υπολογιστές, έχουν μία σημαντική διάφορα: το worm το πετυχαίνει αυτό χωρίς την ανθρώπινη παρέμβαση.

Η αντιμετώπιση των ιών και των Δούρειων Ίππων μπορεί να γίνει με πολλούς τρόπους. Ενδεικτικά αναφέρουμε τη χρησιμοποίηση αντιϊκού λογισμικού με όλα τα τελευταία updates, με τη χρήση συστημάτων πρόληψης εισβολής (Intrusion Prevention Systems, IPS) και φροντίζοντας να είμαστε ενημερωμένοι για την παρούσα κατάσταση, όπως συνηθισμένες επιθέσεις, νέες μεθόδους κτλ.Όσον αφορά τα worms, τα πράγματα εδώ γίνονται πιο περίπλοκά, λόγω της φύσης τους. Αρχικά θα πρέπει να περιορίσουμε τη διάδοσή τους. Στη συνέχεια θα πρέπει να εγκαταστήσουμε όλες τις τελευταίες ενημερώσεις του αντιβιοτικού και του λειτουργικού μας συστήματος, σε όλα τα συστήματα που χρησιμοποιούμε. Έπειτα, θα πρέπει να βάλουμε σε καραντίνα τα ήδη μολυσμένα συστήματα, απομονώνοντάς τα από το δίκτυο ή και κλείνοντάς τα. Τέλος, προχωράμε σε πλήρη εξάλειψη των worms στα μολυσμένα μηχανήματα. Εξυπακούεται ότι έχουμε λάβει όλα τα απαραίτητα μέτρα πριν συμβεί η επίθεση. Επίσης, αφού αντιμετωπίσουμε μια τέτοιου είδους επίθεση, στη συνέχεια προσπαθούμε να εντοπίσουμε τις ευπάθειες εκείνες που εκμεταλλεύτηκε το worm και τις εξαλείφουμε.

5.1.3 Άλλες Ευπάθειες - Επιθέσεις

Στην παράγραφο αυτή θα περιγράψουμε ένα πλήθος συνηθισμένων επιθέσεων που εκμεταλλεύονται ευπάθειες του δευτέρου επιπέδου δικτύωσης, δηλαδή επιθέσεις που αφορούν κυρίως τα switches.

MAC Flooding Attack: Είναι μία αρκετά συνηθισμένη επίθεση, που προκαλεί υπερχείλιση στον πίνακα του switch που αποθηκεύονται οι MAC διευθύνσεις, το λεγόμενο MAC table. Αυτή η υπερχείλιση επιτυγχάνεται με τη συνεχή αποστολή πακέτων από μη υπαρκτές MAC διευθύνσεις. Πλέον, το CAM table δεν μπορεί να αποθηκεύσει άλλες MAC και έτσι, αν έρθει ένα πακέτο για κάποιον υπαρκτό υπολογιστή, αυτό θα διοχετευτεί σε όλα τα

ports του switch. Έτσι, αφενός δημιουργείται πολλή, αχρείαστη κίνηση και αφετέρου ο επιτιθέμενος θα μπορεί να λαμβάνει πακέτα τα οποία δεν προοριζόντουσαν για αυτό, λόγω του flooding. Η συγκεκριμένη επίθεση αντιμετωπίζεται με το port security.

VLAN Hopping: Είναι η επίθεση κατά την οποία κάποιος τερματικός σταθμός λαμβάνει ή στέλνει πακέτα σε κάποιο VLAN που δεν είναι μέλος του. Αυτό επιτυγχάνεται είτε σημαδεύοντας (tagging) κάποια κίνηση με κάποιο συγκεκριμένο VLAN ID, είτε μέσω της διαπραγμάτευσης (negotiation) σε ένα trunk και τη ρύθμισή να στέλνει και να λαμβάνει κίνηση από VLANs που έχει πρόσβαση ο επιτιθέμενος. Για να αντιμετωπίσουμε αυτή την επίθεση, όποιο port δεν είναι trunk το ρυθμίζουμε ως access port, απενεργοποιούμε όλα τα μη χρησιμοποιούμενα ports και ρυθμίζουμε συγκεκριμένα VLANs που θα χρησιμοποιούμε και όχι όλα που είναι το default.

DHCP Spoof Attack: Η συγκεκριμένη επίθεση χρησιμοποιεί την τεχνική man-in-the-middle. Όταν ένας τερματικός σταθμός ζητάει IP διεύθυνση από κάποιον DHCP server στέλνει το μήνυμα ως broadcast, δηλαδή μπορεί να παραληφθεί από όλους. Αυτό μπορεί να το εκμεταλλευτεί κάποιος κακόβουλος και να προσποιηθεί ότι εκείνος είναι ο νόμιμος DHCP server και πλέον, μιας και γνωρίζει τις εσωτερικές IP διευθύνσεις, μπορεί ανεμπόδιστα να παρακολουθεί την κίνηση στο δίκτυο. Η συγκεκριμένη επίθεση αντιμετωπίζεται με μία λειτουργία του switch, που ονομάζεται DHCP snooping και, μέσω αυτής, ορίζουμε από ποια ports του switch μπορεί να προέλθει μία DHCP απάντηση. Έτσι, κάποιος κακόβουλος DHCP server θα αποτραπεί από το να στείλει απάντηση στον τερματικό σταθμό που αιτείται IP.

Telnet: Το Telnet έχει αρκετά μειονεκτήματα, τα οποία είναι: τα username, τα passwords και τα δεδομένα στέλνονται με τη μορφή απλού κειμένου. Κάποιος χρήστης με πρόσβαση σε μία συσκευή μπορεί να αποκτήσει περισσότερα δικαιώματα. Επίσης, κάποιος κακόβουλος μπορεί να “ρίξει” το telnet, αποτρέποντας νόμιμους χρήστες να μην μπορούν να συνδεθούν. Έτσι, είναι σώφρον, αντί να χρησιμοποιούμε telnet, να χρησιμοποιούμε SSH. Για το SSH θα αναφερθούμε εκτενέστερα σε επόμενη παράγραφο.

5.2 Διαχείριση λογαριασμών/κωδικών πρόσβασης

5.2.1 Κωδικοί πρόσβασης στο δικτυακό εξοπλισμό

Σε αυτή την πρώτη παράγραφο θα εξετάσουμε μερικές καλές πρακτικές που οφείλουμε να ακολουθούμε, για να διασφαλίζουμε όσο το δυνατόν περισσότερο την πρόσβαση στο δικτυακό εξοπλισμό. Τα passwords είναι ο κυριότερος τρόπος αποτροπής απόκτησης πρόσβασης σε οποιοδήποτε είδος εξοπλισμού. Ο καλύτερος τρόπος διαχείρισης των passwords είναι με κάποιον AAA server. Όμως, η βέλτιστη πρακτική είναι να τηρείται παράλληλα και ένα password configuration σε κάθε δικτυακή συσκευή.

Τα passwords μπορούν να έχουν μήκος ενός έως εικοσιπέντε χαρακτήρων. Μπορούν να περιλαμβάνουν αλφαριθμητικά σύμβολα, μεγάλα και μικρά γράμματα, σύμβολα και κενά. Δεν επιτρέπεται η χρήση αριθμού ως πρώτος χαρακτήρας. Τα κενά που προηγούνται του password αγνοούνται, όχι, όμως, και αυτά που έπονται.

Εξυπακούεται ότι τα passwords πρέπει να αλλάζουν τακτικά. Θα πρέπει να περιλαμβάνουν όλα τα είδη χαρακτήρων που αναφέρθηκαν. Επίσης, δεν πρέπει να χρησιμοποιούνται λέξεις που μπορούν να βρεθούν σε λεξικό, καθώς έτσι καθίστανται ευάλωτα σε λεξικογραφικές επιθέσεις (dictionary attacks).

Οι τρόποι που μπορεί ένας διαχειριστής δικτύου να αποκτήσει πρόσβαση σε κάποια δικτυακή συσκευή είναι: μέσω του control port, με telnet, με ssh και με SNMP.

Όπως προείπαμε, δύναται η δυνατότητα πέρα από τη χρήση ενός server για τη διαδικασία της αυθεντικοποίησης, να παρέχουμε εναλλακτικά ή σαν τελευταία επιλογή την αυθεντικοποίηση με τη βοήθεια του router. Αυτό είναι ιδιαίτερα χρήσιμο σε περιπτώσεις που έχει χαθεί η συνδεσιμότητα με το υπόλοιπο δίκτυο, αλλά η συσκευή είναι λειτουργική η στην περίπτωση που η συσκευή είναι καινούρια και πρέπει να ρυθμιστεί.

Μπορούμε να το πετύχουμε τη ρύθμιση ενός τοπικού λογαριασμού στο router με τις εντολές enable password και enable secret. Έτσι δημιουργούμε ένα τοπικό λογαριασμό, κοινό για όλους και γνωστό μόνο σε όσους χρειάζεται. Οι δύο εντολές πετυχαίνουν ακριβώς το ίδιο: δημιουργούν ένα κρυπτογραφημένο password. Ωστόσο, η εντολή enable secret χρησιμοποιεί ισχυρότερο μηχανισμό κρυπτογράφησης. Επίσης, μπορούμε να χρησιμοποιήσουμε τις συγκεκριμένες εντολές με την επιλογή level, ώστε να δηλώνουμε για ποιο privilege level ορίζουμε κωδικό. Τέλος, καλό θα ήταν να κρυπτογραφούμε τα συγκεκριμένα passwords στις εντολές show, ώστε να μην είναι προφανή σε κάποιον επιτιθέμενο.

Αφού δημιουργήσουμε τα passwords, θα πρέπει να τα χρησιμοποιήσουμε για να ασφαλίσουμε την είσοδο στις συσκευές μας. Έτσι, μπορούμε να τα τοποθετήσουμε στο

console port, στο auxiliary port και στα vty lines. Πλέον, οποιοσδήποτε προσπαθήσει να συνδεθεί μέσω αυτού του port. Επίσης, μας δίνεται η δυνατότητα να ρυθμίζουμε τον αριθμό τον αποτυχημένων προσπαθειών εισαγωγής password, το χρονικό διάστημα που θα παραμένει κλειδωμένη η συσκευή μέχρι να επιτραπεί ξανά στο χρήστη να δοκιμάσει να εισέλθει, καθώς και η δυνατότητα να καταχωρείται κάθε προσπάθεια εισόδου, αποτυχημένη ή επιτυχημένη.

Επιπροσθέτως, είναι καλή πρακτική να χρησιμοποιούμε μηνύματα εισόδου (banners), δηλαδή μηνυμάτων που θα τα βλέπει ο χρήστης πριν ή αφού αποκτήσει πρόσβαση στη συσκευή. Χρησιμοποιούνται για να δείξουν στους επίδοξους εισβολείς ότι δεν είναι επιθυμητοί στο δίκτυό μας. Επίσης, είναι σημαντικά και από νομικής απόψεως, καθώς, στο παρελθόν, εισβολείς έχουν αθωωθεί επειδή δεν υπήρχε κάποιο προειδοποιητικό μήνυμα και ισχυριζόμενοι ότι δεν ήταν εις γνώση τους ότι έκαναν κάτι κολάσιμο.

5.2.2 AAA

Η μη εξουσιοδοτημένη πρόσβαση σε οτιδήποτε αφορά ή κατέχει ο οργανισμός ελλοχεύει κινδύνους, που σχετίζονται με την εκμετάλλευση πόρων, συστημάτων και πληροφοριών. Επομένως, είναι εκ των ουκ άνευ η ασφάλεια που αφορά τον δικτυακό εξοπλισμό και αφορά τους μηχανικούς δικτύου και τους διαχειριστές (administrators).

Η αρχιτεκτονική που περιγράφει τη διάρθρωση των λειτουργιών του συγκεκριμένου μοντέλου ονομάζεται AAA από τα αρχικά των λέξεων Authentication (αυθεντικοποίηση), Authorization (εξουσιοδότηση), Accounting-Auditing (Λογιστική-Έλεγχος). Πιο συγκεκριμένα:

- **Αυθεντικοποίηση:** Απαιτεί από τους χρήστες να αποδείξουν την ταυτότητά τους, να δείξουν ότι όντως πρόκειται για αυτούς που ισχυρίζονται ότι είναι. Η αυθεντικοποίηση μπορεί να γίνει με πολλούς τρόπους: με τη χρήση username και password, με μία μέθοδο πρόκλησης-απάντησης, με τη χρήση κάποιου «κουπονιού» (token) ή με βιολογικά και ανθρωπιστικά χαρακτηριστικά.
- **Εξουσιοδότηση:** Μετά την αυθεντικοποίηση του χρήστη, με τη βοήθεια της εξουσιοδότησης, αποφασίζεται σε ποιους πόρους μπορεί να έχει πρόσβαση και ποιες ενέργειες του επιτρέπεται να εκτελέσει σε αυτούς.

- **Λογιστική-Έλεγχος:** Η λογιστική καταγράφει ποιες ενέργειες πραγματοποίησε ο χρήστης, σε ποιον πόρο και για πόση ώρα. Οι πληροφορίες αυτές αποθηκεύονται σε ειδικά αρχεία, τα λεγόμενα log files.

Τα πρωτόκολλα AAA που εφαρμόζονται στους routers σήμερα είναι τα TACACS+ (Cisco proprietary) και RADIUS (IETF). Οι διαφορές τους είναι αρκετές, κάτι που μας εξυπηρετεί στο να χρησιμοποιούμε κάθε ένα από αυτά στην κατάλληλη περίσταση. Οι διαφορές τους φαίνονται στον παρακάτω πίνακα:

Πίνακας 5.1: Διαφορές TACACS+ και RADIUS

	TACACS+	**RADIUS**
Πρωτόκολλο $3^{ου}$ Επιπέδου	TCP/IP	UDP/IP
Κρυπτογράφηση	Πλήρης	Μόνο το password
Χρήση	Μόνο σε Cisco συσκευές	Οπουδήποτε

Εκτός από τις παραπάνω διαφορές, το TACACS+ μας προσφέρει και δύο επιπλέον, ιδιαίτερα χρήσιμες, λειτουργίες. Η πρώτη είναι ότι επιτρέπει την παραμετροποίηση του επιπέδου εξουσιοδότησης για κάθε χρήστη. Έτσι, κατ' αυτόν τον τρόπο, δημιουργούμε μία διαβάθμιση στο ποιος μπορεί να κάνει τι και επιτρέπουμε, για παράδειγμα, στον αρχαιότερο administrator να κάνει τα πάντα, ενώ σε κάποιον πιο αρχάριο δίνουμε λιγότερα δικαιώματα, ώστε να ελαττώνονται οι πιθανότητες λαθών. Η δεύτερη λειτουργία που καθιστά το TACACS+ ιδιαίτερα ελκυστικό σε σχέση με το RADIUS, είναι ότι το TACACS+ διαχωρίζει τις διαδικασίες αυθεντικοποίησης και εξουσιοδότησης. Έτσι, μπορούμε να χρησιμοποιήσουμε τον router για εξουσιοδότηση και έλεγχο και να χρησιμοποιήσουμε κάποια άλλη μέθοδο για αυθεντικοποίηση, όπως, π.χ., το Kerberos.

Η διαδικασία αυθεντικοποίησης του χρήστη μέσω RADIUS έχει ως ακολούθως: ο πόρος που του ζητείται πρόσβαση (router, switch, κτλ) ζητά από το χρήστη username και password. Ο χρήστης τα εισάγει και στη συνέχεια ο πόρος τα μεταφέρει στον RADIUS server για αυθεντικοποίηση και απαντά με ένα μήνυμα αποδοχής ή απόρριψης της αίτησης σύνδεσης στον πόρο. Η ασφάλεια που παρέχεται με τη χρήση RADIUS είναι η

κρυπτογράφηση των passwords με MD5 αλγορίθμους και η αυθεντικοποίηση των πακέτων πάλι με MD5.

Με τη χρήση TACACS+ η παραπάνω διαδικασία αλλάζει. Όταν ο χρήστης προσπαθήσει να αποκτήσει πρόσβαση σε κάποιον πόρο, ο πόρος απευθύνεται στον TACACS+ server και του ζητά το prompt που πρέπει να δείξει στο χρήστη, ώστε να καταλάβει ότι του ζητείται το username. Ο πόρος εμφανίζει το prompt στο χρήστη και ο χρήστης εισάγει το username. Στη συνέχεια γίνεται το ίδιο και για το password. Τέλος, ο TACACS+ server απαντά στον πόρο αν τα στοιχεία που δόθηκαν είναι αποδεκτά.

Στη διαδικασία αυθεντικοποίησης ορίζουμε λίστες αυθεντικοποίησης και δηλώνουμε ποιος server θα είναι υπεύθυνος για την επεξεργασία τους. Επίσης δηλώνουμε ποιες άλλες μέθοδοι θα χρησιμοποιηθούν σε περίπτωση αποτυχίας κάποιας που προηγείται.

Στη διαδικασία εξουσιοδότησης οι εντολές ενός router μπορούν να ταξινομηθούν κατά τέτοιο τρόπο, ώστε να χωριστούν σε privilege levels. Κάθε Privilege Level περιέχει εντολές που μπορούν να εκτελεστούν μόνο από κάποιο άτομο που έχει εξουσιοδοτηθεί να ανήκει στο συγκεκριμένο privilege level.

Στη διαδικασία ελέγχου ορίζουμε τι θα ελέγχουμε (χρήστες ή χρήση), πότε θα ξεκινάει και πότε θα σταματάει η καταγραφή των συμβάντων και ποιος θα είναι υπεύθυνος για τον έλεγχο. Η ενεργοποίηση των εντολών που αφορούν τον έλεγχο προϋποθέτει την εκτέλεση των εντολών που αφορούν την αυθεντικοποίηση και την εξουσιοδότηση.

Παρακάτω φαίνεται ένα πλήρες configuration AAA σε έναν router. Ακολουθεί επεξήγηση κάθε εντολής. Τα βήματα 1-5 αφορούν τη δήλωση των IP διευθύνσεων των servers και των κλειδιών κρυπτογράφησης, τα βήματα 6-8 αφορούν την αυθεντικοποίηση, τα βήματα 9-11 αφορούν την εξουσιοδότηση, ενώ το βήμα 12 αφορά τον έλεγχο.

Πίνακας 5.2: Configuration AAA σε router

1.	Router(config)#aaa new-model
2.	Router(config)#tacacs-server host 1.1.1.1
3.	Router(config)#radius-server host 1.1.1.2
4.	Router(config)#tacacs-server key key1
5.	Router(config)#radius-server key key2
6.	Router(config)#aaa authentication login my_list group tacacs+

```
local
7.  Router(config)#line vty 0 4
8.  Router(config-line)#login authentication my_list
9.  Router(config)#aaa authorization exec default group tacacs+ local
10. Router(config)#aaa authorization commands 1 default group tacacs+ local
11. Router(config)#aaa authorization commands 15 default group tacacs+ local
12. Router(config)#aaa accounting exec default start-stop group tacacs+
```

1: Δημιουργούμε ένα νέο AAA configuration

2: Ορίζουμε την IP διεύθυνση του TACACS+ server

3: Ορίζουμε την IP διεύθυνση του RADIUS server

4: Δημιουργούμε το κλειδί κρυπτογράφησης για τον TACACS+ server

5: Δημιουργούμε το κλειδί κρυπτογράφησης για τον RADIUS server

6: Δημιουργούμε τη λίστα my_list, η οποία θα καλείται σε κάθε περίπτωση login και θα υπερκερά τη default. Το local δηλώνει ποια μέθοδος θα χρησιμοποιηθεί αν αποτύχει η αυθεντικοποίηση μέσω TACACS+, με το local να δηλώνει τη χρήση τοπικών συνθηματικών, αν ο TACACS+είναι μη προσβάσιμος. Θα μπορούσαμε να προσθέσουμε και άλλες, οι οποίες θα ενεργοποιούνταν αν οι προηγούμενες είχαν αποτύχει.

7-8: Πάμε στο interface στο οποίο θα συνδεόμαστε εξ αποστάσεως και δηλώνουμε ότι για αυθεντικοποίηση θα χρησιμοποιείται η λίστα my_list.

9: Καθορίζει αν ο χρήστης έχει πρόσβαση στο να εκτελέσει εντολές στο exec shell. Αυτό θα διαπιστωθεί μέσω του TACACS+ server και να δεν καταστεί εφικτό αυτό, τοπικά.

10-11: Ορίζουμε τα privilege levels 1 και 15, ενώ η πρόσβαση δίνεται από TACACS+ server ή, αν αποτύχει, τοπικά.

12: Ορίζουμε έλεγχο στο exec shell, που θα ελέγχεται μέσω του TACACS+. Το start-stop είναι μία επιλογή δηλώνει την έναρξη του ελέγχου με την έναρξη της διαδικασίας και τη λήξη του ελέγχου με τον τερματισμό της.

5.2.3 Active Directory - Kerberos

Μέχρι τώρα σε αυτό το κεφάλαιο ασχοληθήκαμε με εξοπλισμό που είναι διαχειρίσιμος από εξειδικευμένο προσωπικό, όπως μηχανικούς και διαχειριστές δικτύου. Σε αυτήν την παράγραφο θα εστιάσουμε στις προσβάσεις που έχουν οι απλοί χρήστες στους τερματικούς σταθμούς.

Κάθε οργανισμός οφείλει να έχει μια πολιτική για τα passwords που χρησιμοποιούν οι χρήστες του και να επιβάλει συγκεκριμένους περιορισμούς. Πιο συγκεκριμένα, θα πρέπει η πολιτική αυτή να ορίζει το μήκος του password, την πολυπλοκότητά του, κάθε πότε πρέπει να αλλάζεται, τον ελάχιστο χρόνο ζωής του κ.α. Η πολιτική αυτή θα πρέπει να εφαρμόζεται σε όλο το πλάτος του domain και, ενδεχομένως, θα πρέπει να είναι αυστηρότερη στα άτομα που χειρίζονται ευαίσθητο εξοπλισμό, όπως servers.

Το Kerberos είναι ένα πρωτόκολλο δικτυακής αυθεντικοποίησης. Χρησιμοποιείται για να παρέχει ισχυρή αυθεντικοποίηση για εφαρμογές client/server, χρησιμοποιώντας κρυπτογράφηση μυστικού κλειδιού. Υλοποιήθηκε από το MIT και σήμερα είναι διαθέσιμο σε πολλές εμπορικές εφαρμογές.

Είναι πολύ εύκολο για κάποιον ωτακουστή να παρακολουθεί τα πακέτα που μεταφέρονται από ένα δίκτυο. Συνεπώς, αν σε αυτά τα πακέτα περιέχονται passwords σε απλό κείμενο, είναι εξίσου εύκολο να τα υποκλέψει. Το Kerberos χρησιμοποιεί πολύ ισχυρή κρυπτογράφηση, ώστε ο πελάτης να αποδεικνύει την ταυτότητα του στο server και το αντίστροφο, χρησιμοποιώντας ένα μη ασφαλές κανάλι. Αφού ο client και ο server έχουν αυθεντικοποιηθεί, έχουν τη δυνατότητα να κρυπτογραφήσουν και την υπόλοιπη επικοινωνία τους, για να διασφαλίσουν την ιδιωτικότητα και την ακεραιότητα που επιθυμούν.

Σχεδόν όλη η παραμετροποίηση του Keberos είναι κρυφή από το χρήστη, καθιστώντας ασύνηθες φαινόμενο την επικοινωνία με το πρωτόκολλο. Παρόλα αυτά, κάθε φορά που εισάγουμε τους κωδικούς μας σε κάποιον υπολογιστή που συνδέεται με το Active Directory ή κάθε φορά που αποκτούμε πρόσβαση σε κάποιον δικτυακό δίσκο ή εφαρμογή, ερχόμαστε σε επαφή με το Kerberos.

Όταν συνδεόμαστε σε κάποιον υπολογιστή ξεκινάει μία σειρά συναλλαγών με τον Domain Controller, που, αν είναι επιτυχής, θα καταλήξει στο να μας αποδοθεί ένα «κουπόνι» (ticket-graning ticket). Από εκείνη τη στιγμή και μετά, κάθε φορά που θέλουμε να χρησιμοποιήσουμε κάποιο service, όπως πρόσβαση σε κάποια εφαρμογή, χρησιμοποιούμε αυτό το κουπόνι.

5.3 Προστασία στο Επίπεδο Πρόσβασης

5.3.1 Port Security

Κάθε switch έχει ως διαθέσιμο χαρακτηριστικό το port security. Το port security περιορίζει το ποιες MAC διευθύνσεις μπορεί να δεχθεί ένα port. Αυτές οι MAC διευθύνσεις μπορούν να γίνουν γνωστές είτε δυναμικά-αυτόματα, είτε χειροκίνητα-στατικά. Πλέον, το συγκεκριμένο port θα επιτρέπει τη διέλευση πλαισίων (frames) μόνο από τις συγκεκριμένες MAC διευθύνσεις. Αν, όμως, το port επιτρέπει πλαίσια από πέντε MAC διευθύνσεις και δεν έχει δηλωθεί καμία, τότε το port επιτρέπει τα πλαίσια οποιονδήποτε πέντε MAC διευθύνσεων, που θα μάθει δυναμικά.

Η υλοποίηση του σε ένα switch είναι εύκολη και η διαδικασία φαίνεται στον παρακάτω πίνακα:

Πίνακας 5.3: Port Security

1.	Switch(config-if)#switchport port-security
2.	Switch(config-if)#switchport port-security maximum 5
3.	Switch(config-if)#switchport port-security mac-address 1111.2222.3333
4.	Switch(config-if)#switchport port-security violation shutdown
5.	Switch (config-if)#switchport port-security mac-address sticky

1.: Εφαρμόζουμε το port-security σε ένα port του switch

2.: Δηλώνουμε ότι επιτρέπουμε μόνο 5 MAC διευθύνσεις να συνδέονται στο συγκεκριμένο port

3.: Δηλώνουμε μία MAC address που επιτρέπεται στο port (προαιρετικό)

4.: Υποδεικνύουμε στο port να απενεργοποιηθεί αν διαπιστώσει τη σύνδεση συσκευής με μη επιτρεπτή MAC. Έχουμε επίσης την επιλογή να απορρίπτουμε πλαίσια από την μη αποδεκτή MAC και να δημιοθργείται ή όχι καταγραφή στο log αρχείο.

5.: Χρησιμοποιούμε την επιλογή sticky. Κατ' αυτόν τον τρόπο περιορίζουμε την πρόσβαση σε μία MAC διεύθυνση. Έτσι, μία MAC που μαθεύτηκε δυναμικά, μετατρέπεται και αντιμετωπίζεται σαν να τη δηλώσαμε στατικά.

5.3.2 802.1x

Το πρότυπο 802.1x αποτρέπει μη εξουσιοδοτημένους τερματικούς σταθμούς να συνδεθούν στο εσωτερικό μας δίκτυο, χρησιμοποιώντας ports του switch διαθέσιμα και προσβάσιμα σε όλους. Ο authentication server αυθεντικοποιεί κάθε τερματικό σταθμό που συνδέεται στο switch, πριν μπορέσει να αποκτήσει πρόσβαση στις υπηρεσίες και τις εφαρμογές που προσφέρει το δίκτυο.

Μέχρι να αυθεντικοποιηθεί ένας τερματικός σταθμός, το 802.1x επιτρέπει μόνο ένα είδος κίνησης να περνάει μέσα από το port: κίνηση EAPOL (Extensible Authentication Protocol over LAN). Αν στη συνέχεις αυθενικοποιηθεί, τότε και μόνον τότε επιτρέπεται και άλλων ειδών κίνηση.

Στο 802.1x υπάρχουν τρεις ρόλοι: ο πελάτης (client), ο εξυπηρετητής αυθεντικοποίησης (authentication server) και το switch, που καλείται εναλλακτικά και αυθεντικοποιητής (authenticator). Ας δούμε τι έργο επιτελεί ο καθένας.

Ο πελάτης, δηλαδή ο τερματικός σταθμός, είναι εκείνος που ζητάει πρόσβαση στο LAN και είναι εκείνος που απαντά στα αιτήματα του switch. Επίσης θα πρέπει το λειτουργικό του να υποστηρίζει και να είναι συμβατό με το 802.1x.

Ο Authentication Server επιτελεί το έργο της αυθεντικοποίησης του πελάτη, ελέγχοντας την εγκυρότητα της ταυτότητας του πελάτη και ενημερώνει το switch για το αν ο χρήστης αυθεντικοποιήθηκε ή όχι. Επειδή το switch ενεργεί ως μεσάζων η διαδικασία αυθεντικοποίησης είναι τελείως ανεπαίσθητη στον πελάτη.

Το switch είναι εκείνο που ελέγχει τη φυσική πρόσβαση στο δίκτυο, βασιζόμενο στο αν ο πελάτης έχει αυθεντικοποιηθεί ή όχι. Όπως προείπαμε, λειτουργεί σαν μεσάζων μεταξύ του πελάτη και του server, ζητώντας πληροφορίες από το χρήστη, επιβεβαιώνοντάς τες με τον server και επιστρέφοντας την απάντηση στον πελάτη.

Η κατάσταση του port καθορίζει αν ο πελάτης έχει πρόσβαση στο δίκτυο. Ξεκινάει από την κατάσταση μη-εξουσιοδότησης (unauthorized state), όπου εδώ το port απαγορεύει όλη την εισερχόμενη και εξερχόμενη κίνηση, πλην τα πακέτα του 802.1x. Αν ο πελάτης αυθεντικοποιηθεί, τότε γίνεται η μετάβαση στην εξουσιοδοτημένη κατάσταση (authorized state) και όλα τα πλαίσια επιτρέπονται στο συγκεκριμένο port. Αν ο πελάτης δεν αυθεντικοποιηθεί, τότε το port μπαίνει σε unauthorized state, όμως η αυθεντικοποίηση μπορεί να επιχειρηθεί ξανά. Τέλος, αν ο server δεν απαντήσει, τότε δεν υπάρχει αυθεντικοποιήση και, συνεπώς, δεν επιτρέπεται η πρόσβαση στο δίκτυο.

Η ενεργοποίηση του 802.1x σε ένα Cisco switch φαίνεται στον παρακάτω πίνακα:

Πίνακας 5.4: 802.1x σε Cisco switch

1.	Switch(config)#aaa new-model
2.	Switch(config)#radius-server 10.10.10.11 key new_key
3.	Switch(config)#aaa authentication dot1x default group radius
4.	Switch(configf)#dot1x system-auth-control
5.	Switch(config)#int e 1/1
6.	Switch (config-if)#dot1x port-control auto

1: Για να ενεργοποιήσουμε το 802.1x απαιτείται η ενεργοποίηση του AAA

2: Δηλώνουμε ποιος είναι ο authentication server

3: Δημιουργούμε μία λίστα για 802.1x αυθεντικοποίηση

4: Ενεργοποιούμε το 802.1x σε όλο το switch

5-6: Ενεργοποιούμε το dot.1x σε κάποιο interface.

5.3.3 Ασύρματα Δίκτυα

Μέχρι τώρα, ασχοληθήκαμε με ενσύρματα δίκτυα, που είναι προτιμητέα από τις επιχειρήσεις και τους οργανισμούς λόγω της ασφάλειας που προσφέρουν. Ωστόσο, στις σύγχρονες επιχειρήσεις, όπου το outsourcing, δηλαδή η ανάθεση δύσκολων και επίπονων έργων σε εξωτερικούς συνεργάτες, είναι κοινός τόπος, απαιτείται η παρουσία προσωπικού που δεν ανήκει στις τάξεις του οργανισμού. Επίσης, λόγω της φύσης της

δουλειάς απαιτείται συνεχής και απρόσκοπτη πρόσβαση είτε σε μέρη του εταιρικού δικτύου, είτε στο Internet με περιορισμένη ή απεριόριστη πρόσβασης. Τέλος, λόγω της νομαδικότητας και των συνεχών μετακινήσεων των συγκεκριμένων χρηστών, αλλά και για την εξυπηρέτηση των εργαζομένων στον ίδιο τον οργανισμό, πολλοί καταφεύγουν στη χρησιμοποίηση ασύρματων δικτύων. Η ασφάλεια στα ασύρματα δίκτυα περιστρέφεται γύρω από δύο άξονες: την αυθεντικοποίηση και την κρυπτογράφηση.

Ένα ασύρματο δίκτυο έχει να αντιμετωπίσει πλήθος απειλών, διαφορετικής φύσεως και κλιμακούμενων συνεπειών. Στη συνέχεια θα αναφερθούμε στις σημαντικότερες εξ' αυτών και κατόπιν θα παραθέσουμε το αμυντικό μας οπλοστάσιο.

5.3.3.1 Απειλές σε Ασύρματα Δίκτυα

Τα ασύρματα δίκτυα είναι εκ φύσεως επισφαλή λόγω του μέσου που χρησιμοποιούν για τη μετάδοση των σημάτων (αέρας), αλλά και λόγω της φύσης του σήματος, που είναι ηλεκτρομαγνητικό και διαδίδεται προς όλες τις διευθύνσεις και όχι στοχευόμενα και άρα είναι προσιτό σε όποιον διαθέτει κεραία και στοιχειώδη εξοπλισμό.

Ένα ασύρματο δίκτυο παρουσιάζει πολλές εγγενείς ευπάθειες. Αυτές είναι:

SSID: Το SSID είναι το όνομα του ασύρματου δικτύου. Είναι παραμετροποιήσιμο και πρέπει να το μοιράζονται τόσο ο πελάτης (client) όσο και το σημείο πρόσβασης (access point). Το πρότυπο 802.11, που αφορά τα ασύρματα δίκτυα, απαιτεί η ασύρματη κάρτα δικτύου του χρήστη να έχει το ίδιο SSID με το access point, για να εγκαθιδρυθεί η επικοινωνία. Τα περισσότερα access points διαμοιράζουν ανοιχτά το SSID τους. Επίσης, η ζωή των επίδοξων hackers γίνεται ευκολότερη από το γεγονός ότι πολλοί διαχειριστές δικτύων δεν αλλάζουν καν το SSID κα διατηρούν και διαμοιράζουν το default SSID. Ακόμη, όλα τα σύγχρονα λειτουργικά συστήματα κάνουν αυτόματη αναζήτηση ασύρματων δικτύων, χωρίς καν να το ζητήσει άμεσα ο χρήστης. Αλλά ακόμα και αν απενεργοποιήσουμε το διαμοιρασμό του SSID, ο hacker μπορεί να περιμένει απλά να συνδεθεί κάποιος στο ασύρματο δίκτυο.

MAC Filtering: Κατά τη διαδικασία σύνδεσης σε ένα access point ο πελάτης πρέπει να αυθεντικοποιηθεί. Πολλά ασύρματα δίκτυα αυθεντικοποιούν τους χρήστες μέσω των MAC διευθύνσεων. Ωστόσο είναι πολύ εύκολο για τον hacker να αλλάξει τη MAC κατά βούληση, με μία άλλη ανύπαρκτη (MAC spoofing). Συνεπώς το MAC filtering δεν πρέπει να λογίζεται σαν χαρακτηριστικό ασφαλείας ενός ασύρματου δικτύου.

Automatic DHCP: Τα περισσότερα ασύρματα δίκτυα χρησιμοποιούν DHCP για να ορίζουν IP διευθύνσεις στους χρήστες που συνδέονται αυτά. Όμως, η απόδοση IP διευθύνσεων δεν περιλαμβάνει μόνο τους επιθυμητούς χρήστες, αλλά και τους hackers. Από τη στιγμή που θα αποδοθεί μία IP στον hacker, μπορεί να δει οποιονδήποτε άλλον συνδεδεμένο στο ασύρματο δίκτυο, καθώς επίσης και κοινούς πόρους ή αρχεία.

WEP: Το WEP (Wired Equivalent Privacy) είναι μία μέθοδος κρυπτογράφησης των πακέτων σε ένα ασύρματο δίκτυο, που κρυπτογραφεί ολόκληρο το πακέτο χρησιμοποιώντας τον αλγόριθμο κρυπτογράφησης RC4. Ο RC4 επεκτείνει ένα μικρού μήκους κλειδί και το μετατρέπει σε ένα ψευδοτυχαίο μεγάλο κλειδί. Ο αποστολέας κρυπτογραφεί το πακέτο και ο παραλήπτης χρησιμοποιεί το ίδιο κλειδί για να αποκρυπτογραφήσει το πακέτο. Όμως, ένας hacker μπορεί πολύ εύκολα, και σε ελάχιστο χρόνο (λιγότερο από δύο λεπτά) να «σπάσει» το WEP κλειδί, χρησιμοποιώντας έτοιμο λογισμικό. Επίσης, οι περισσότερες κάρτες δικτύου δημιουργούν μόνιμα WEP κλειδιά που αποθηκεύονται στην κάρτα. Άρα, σε δύο μόλις λεπτά μπορούμε να παρακολουθούμε για πάντα την αποστολή των πακέτων (εκτός και αν αλλαχθεί χειροκίνητα το WEP key).

Initialization Vector Attack: Για να αποφευχθεί η περίπτωση δύο πακέτα να κρυπτογραφηθούν με το ίδιο WEP κλειδί, το WEP χρησιμοποιεί έναν Πίνακα Αρχικοποίησης (Initialization Vector) για να επεκτείνει το μυστικό κλειδί και κάθε πακέτο να κρυπτογραφηθεί με διαφορετικό RC4 κλειδί. Αν ο IV μεταδοθεί σαν απλό κείμενο, τότε ένας επιτιθέμενος που παρακολουθεί την κίνηση στο δίκτυο, μπορεί να το καταγράψει. Στη συνέχεια, αν επανειλημμένα χρησιμοποιηθεί ο ίδιος IV με το ίδιο WEP κλειδί, μπορεί να εξάγει συμπεράσματα για αυτά και να τα υπολογίσει. Ο τρόπος αντιμετώπισης είναι να αλλάζουμε συχνά WEP κλειδιά, ώστε και να συνάγει πληροφορίες ο επιτιθέμενος, να του είναι άχρηστες.

«Σπάσιμο» Κωδικών: Τα περισσότερα συστήματα αυθεντικοποίησης με τη χρήση passwords μπορούν να δεχτούν είτε online, είτε offline λεξικογραφικές επιθέσεις, δηλαδή μία επίθεση «ωμής δύναμης» (brute force), όπου δοκιμάζεται κάθε δυνατός κωδικός, μέχρι να βρεθεί ο σωστός. Αν ο κωδικός είναι απλός είναι ευκολότερο και να σπάσει. Αν είναι πολύπλοκος, είναι δυσκολότερο. Συνεπώς, πρέπει να προτιμάμε πολύπλοκα passwords. Επίσης, μπορούμε να χρησιμοποιούμε το κλείδωμα της πρόσβασης, μετά από έναν μικρό αριθμό προσπαθειών. Στις offline λεξικογραφικές επιθέσεις ο επιτιθέμενος υποκλέπτει την πρόκληση και την απάντηση και μετά έχει όσο χρόνο θέλει να υπολογίσει αυτό που τα συνδέει.

Man-in-the-Middle Attacks: Αυτού του είδους οι επιθέσεις εφαρμόζονται όχι μόνο στα ενσύρματα δίκτυα, αλλά και στα ενσύρματα δίκτυα. Ο επιτιθέμενος παρακολουθεί τα πλαίσια που στέλνονται και από τις δύο πλευρές σε ένα ασύρματο δίκτυο. Έτσι, μπορεί να συνάγει πληροφορίες σχετικά με το access point, τις IP διευθύνσεις, το SSID κ.α. Στη συνέχεια, μπορεί να εγκαταστήσει ένα δικό του access point και να εξαναγκάσει το χρήστη να εγκαθιδρύσει σύνδεση με αυτόν. Το 802.11 δεν αυθεντικοποιεί το access point, οπότε, αν το κακόβουλο access point έχει ισχυρότερο σήμα, θα προτιμηθεί. Επίσης, αν το κακόβουλο access point έχει ρυθμιστεί και με το σωστό WEP κλειδί, τότε τα δεδομένα του χρήστη θα μπορούν να διαβαστούν. Ακόμη, μπορεί ένας κακόβουλος χρήστης να αποκτήσει με αυτόν τον τρόπο πρόσβαση στο δίκτυο.

DoS Attacks: Όπως και οι man-in-the-middle attacks, οι DoS attacks εφαρμόζονται τόσο στα ενσύρματα, όσο και στα ασύρματα δίκτυα. Σκοπός τους είναι να υπερφορτώσουν τα ασύρματες κάρτες δικτύου, εκμεταλλευόμενοι το γεγονός ότι στο πρότυπο 802.11 αν μία κάρτα εντοπίσει RF κίνηση, σταματάει να μεταδίδει.

5.3.3.2 Ασφάλεια στα Ασύρματα Δίκτυα

Η ασφάλεια στα ασύρματα δίκτυα πέρασε από τρεις φάσεις: την φάση χρήσης του WEP, την εξέλιξή της με τη χρήση WPA και τη σημερινή κατάσταση όπου προτιμάται το ασφαλέστερο WPA2. Φυσικά, υπάρχουν και περιπτώσεις που δεν χρειάζεται να υπάρχει ασφάλεια, όπως σε περιπτώσεις δωρεάν ασύρματης σύνδεσης σε πλατείες αεροδρόμια, λιμάνια κτλ. Η μη χρήση καμίας ασφάλειας ονομάζεται ανοικτή αυθεντικοποίηση (open authentication) και λογίζεται ως η τέταρτη επιλογή ασφαλείας: καθόλου ασφάλεια! Στην παρούσα εργασία δε θα μας απασχολήσει, απλά αναφέρεται για εγκυκλοπαιδικούς λόγους.

Για το WEP μιλήσαμε εκτενώς στην προηγούμενη παράγραφο. Συνοψίζοντας, τα ελαττώματά του είναι ότι δεν παρέχει ισχυρή αυθεντικοποίηση, χρησιμοποιεί στατικά και εύκολα υπολογίσιμα κλειδιά και, ως λύση, δεν είναι εύκολα επεκτάσιμη. Παρόλο που έχουν προταθεί βελτιώσεις του WEP, όπως η ασφαλής παραγωγή κλειδιών και η χρήση δυναμικών WEP κλειδιών, το WEP έχει εγκαταλειφτεί σε περιπτώσεις που η ασφάλεια στα ασύρματα δίκτυα είναι εκ των ουκ άνευ.

Η ασφάλεια του WEP ενισχύεται με τη χρήση WPA ή WPA2, που περιλαμβάνουν βελτιωμένη ασφάλεια και κρυπτογράφηση. Επίσης, πέρα από την ισχυρότερη

αυθεντικοποίηση, μπορούμε να επιβάλουμε πολιτικές στους χρήστες, βασιζόμενοι στις συναλλαγές αυθεντικοποίησης. Βασίζοντας την αυθεντικοποίηση στο χρήστη, αντί στον τερματικό σταθμό, μειώνουμε τον κίνδυνο σύνδεσης κλεμμένου υπολογιστή ή MAC spoof επίθεσης. Επίσης, μπορούμε να χρησιμοποιήσουμε και το 802.1x, που παρουσιάστηκε σε προηγούμενη παράγραφο, δίνοντάς μας το πλεονέκτημα να επιτρέπουμε τη διανομή δυναμικών κλειδιών κρυπτογράφησης σε κάθε χρήστη, κάθε φορά που αυθεντικοποιείται από το δίκτυο.

Το WPA παρέχει δύο βελτιώσεις σε σχέση με το WEP, όσον αφορά την κρυπτογράφηση: το TKIP και το MIC. Το TKIP (Temporal Key Integrity Control) περιέχει τις ακόλουθες βελτιώσεις: κατακερματισμό για το κλειδί (key hashing) ή κλειδί για κάθε πακέτο, έλεγχο ακεραιότητας του μηνύματος (MIC – Message Integrity Check) και εναλλαγή του κλειδιού που διανέμεται. Ουσιαστικά, το TKIP αποτρέπει τον επιτιθέμενο να αντλήσει πληροφορίες μέσα από τη σύγκριση των πακέτων. Το MIC μας προστατεύει από επιθέσεις στις οποίες ζητείται από το σύστημα να στείλει είτε δεδομένα που αφορούν το κλειδί, είτε κάποια απάντηση και μέσω αυτών των δεδομένων, να συναχθούν πληροφορίες για το κλειδί. Το MIC προσθέτει ένα επιπλέον πεδίο 8 bytes και προστατεύει τόσο τα δεδομένα, όσο και τις επικεφαλίδες. Εν τέλει, το WPA επιλύει τα προβλήματα των ασθενών επικεφαλίδων και ενισχύει την ακεραιότητα του μηνύματος χρησιμοποιώντας το TKIP.

Βέβαια, το WPA παρουσιάζει και ατέλειες. Εν πρώτοις, χρησιμοποιεί TKIP, που χρησιμοποιεί τον ίδιο αλγόριθμο με το WEP, δηλαδή το RC4. Επίσης, δεν εξαλείφει πλήρως τα μειονεκτήματα του WEP, καθώς αποτελεί συμβιβαστική λύση στο πρόβλημα της ασφάλειας. Ακόμη, απαιτείται αναβάθμιση του λογισμικού, τόσο στους clients, όσο και στα access points, ενώ πρέπει να υποστηρίζεται και από το λειτουργικό σύστημα του client. Τέλος, είναι ευάλωτο σε νέα είδη DoS επιθέσεων, ενώ έχουν ανακαλυφθεί αδυναμίες του, όταν χρησιμοποιούνται preshared κλειδιά.

Το WPA περιλαμβάνει λύσεις που αντιμετώπιζαν όλα τα προβλήματα που ήταν γνωστά μέχρι και το 2003. Το WPA2 περιλαμβάνει όλα τα χαρακτηριστικά ασφαλείας του WPA και μερικές αναβαθμίσεις επιπλέον.

Κατ’ αρχήν το WPA2 χρησιμοποιεί τον αλγόριθμο AES. Ο AES είναι ισχυρότερος από τον RC4 που χρησιμοποιούν το WEP και το WPA, αλλά απαιτεί μεγαλύτερη επεξεργαστική ισχύ, και, συνεπώς, θα πρέπει να αναβαθμίσουμε τον εξοπλισμό μας για να διασφαλίσουμε την ίδια ποιότητα υπηρεσιών.

Μία ακόμα καινοτομία με το WPA2 είναι η εισαγωγή του 802.1x. Ο χρήστης πρώτα αυθεντικοποιείται και στη συνέχεια παράγεται ένα πρωτεύον κλειδί (master key) που μοιράζονται ο server και ο client. Αυτό το πρωτεύον κλειδί είναι που χρησιμοποιείται για την παραγωγή των κλειδιών κρυπτογράφησης και δεν χρησιμοποιείται άμεσα.

Επίσης, ο Initialization Vector γίνεται 48 bits, ενώ ήταν 24. Έτσι αποφεύγουμε επαναχρησιμοποίηση του ίδιου διανύσματος και κατ' επέκταση καθιστούμε πιο δύσκολο τον υπολογισμό του κλειδιού. Επίσης, αλλάζουμε συχνά το broadcast κλειδί με αποτέλεσμα ο επιτιθέμενος να μην μπορεί να συλλέξει αρκετά πακέτα, ώστε να καταλάβει ποιο είναι το κλειδί.

Τέλος, δύο ακόμη βελτιώσεις του WPA2 είναι η υποστήριξη σε προληπτικής αποθήκευσης κλειδιών (Proactive Key Caching – PKC) και η προ-αυθεντικοποιήση, ενώ προστίθεται και IDS (Intrusion Detection System) για την αναγνώριση και την αντιμετώπιση επιθέσεων. Πιο συγκεκριμένα, το ασύρματο IDS επιλύει προβλήματα όπως: εντοπισμός και αποκλεισμός κακόβουλων συσκευών, εντοπισμός και διαχείριση παρεμβολών, εντοπίζει διάφορα είδη επιθέσεων, επιτρέπει ανάλυση μετά τις επιθέσεις με τη συλλογή στοιχείων κ.α.

Στα μειονεκτήματα του WPA2 περιλαμβάνονται η απαίτηση για ειδικό οδηγό (driver) στον client και η απαίτηση περισσότερης υπολογιστικής ισχύος, ενδεχομένως και νέου hardware, για την υλοποίηση της AES κρυπτογράφησης.

5.4 Προστασία στα Επίπεδα Δικτύου-Μεταφοράς

5.4.1 VPN

Τα εικονικά ιδιωτικά δίκτυα (Virtual Private Networks – VPN) χρησιμοποιούν εξελιγμένες τεχνικές κρυπτογράφησης, που επιτρέπουν σε έναν οργανισμό να εγκαθιστά ασφαλή, από άκρο σε άκρο ιδιωτικές, δικτυακές συνδέσεις, χρησιμοποιώντας δίκτυο που δεν τους ανήκει, όπως το Internet ή το δίκτυο κάποιου παρόχου.

Ένα VPN, ως έννοια, περιγράφει πώς θα δημιουργήσουμε ένα ιδιωτικό δίκτυο, χρησιμοποιώντας μία δημόσια δικτυακή υποδομή, έχοντας, ταυτόχρονα, εμπιστευτικότητα και ασφάλεια. Τα VPNs χρησιμοποιούν κρυπτογραφικά πρωτόκολλα σηράγγωσης (tunneling), για να παρέχουν αυθεντικοποίηση του αποστολέα, ακεραιότητα

του μηνύματος και εμπιστευτικότητα και λειτουργούν στα επίπεδα 2, 3 και 4 του μοντέλου OSI.

Τα απαραίτητα συστατικά για τη δημιουργία μίας VPN υποδομής είναι:

- Ένα υπάρχον δίκτυο με servers και τερματικούς σταθμούς
- Σύνδεση στο Internet
- VPN Gateways (routers, firewalls, κ.α.) που χρησιμεύουν ως σημεία τερματισμού των συνδέσεων
- Λογισμικό για τη δημιουργία και τη διαχείριση των VPN tunnels.

Υπάρχουν τρεις τοπολογίες VPN για να επιλέξει ένας οργανισμός: VPNs απομακρυσμένης πρόσβασης (remote access VPNs), VPNs από μία θέση σε κάποια άλλη θέση του ιδιωτικού μας δικτύου (site-to-site Intranet VPNs) και VPNs από μία θέση σε κάποια άλλη θέση εκτός του ιδιωτικού μας δικτύου (site-to-site Extranet VPNs).

Τα remote access VPNs επιτρέπουν σε απομακρυσμένους χρήστες πρόσβαση στο εσωτερικό δίκτυο ενός οργανισμού και είναι ιδιαίτερα χρήσιμα σε περιπτώσεις εργαζομένων που είναι αναγκασμένοι να μετακινούνται συνεχώς. Το VPN gateway του οργανισμού συνδέεται με το VPN λογισμικό του εν κινήσει χρήστη με οποιοδήποτε είδος γραμμής, από ISDN μέχρι και DSL. Τα tunnels δημιουργούνται είτε με IPSEC (IP Security), είτε με PPTP (Point to Point Tunneling Protocol), είτε με L2TP (Layer 2 Tunneling Protocol), είτε με L2F (Layer 2 Forwarding).

Τα site-to-site Intranet VPNs συνδέουν τα κεντρικά γραφεία, τα απομακρυσμένα γραφεία και τα καταστήματα του δικτύου στο εσωτερικό δίκτυο του οργανισμού, χρησιμοποιώντας αποκλειστικές συνδέσεις πάνω από μία κοινή υποδομή (Internet ή ISP). Τα Intranet VPNs διαφέρουν από τα Extranet VPNs στο γεγονός ότι τα πρώτα επιτρέπουν την πρόσβαση μόνο σε έμπιστους υπαλλήλους.

Ένα site-to-site Extranet VPN συνδέει εξωτερικούς πελάτες, προμηθευτές, συνεργάτες με το δίκτυο του οργανισμού, χρησιμοποιώντας αποκλειστικές συνδέσεις πάνω από μία κοινή υποδομή. Χρησιμοποιούνται σε συνδυασμό με firewalls, ώστε να αποτρέπεται η είσοδος σε περιοχές του δικτύου που δεν πρέπει να έχουν πρόσβαση.

Σηράγγωση (tunneling) είναι η μετάδοση δεδομένων μέσω ενός δημοσίου δικτύου, με τέτοιο τρόπο που οι ενδιάμεσες συσκευές που επιτελούν τη μετάδοση του πακέτου δεν έχουν καμία απολύτως γνώση των δεδομένων που μεταφέρονται. Τα VPNs υλοποιούν τα

tunnels ενθυλακώνοντας την πληροφορία, κατά τέτοιο τρόπο, που τα δεδομένα που μεταφέρουν από το tunnel είναι ακατάληπτα σε κάποιον πιθανό ωτακουστή. Εναλλακτικά, θα μπορούσαμε να ορίσουμε το tunneling ως τη διαδικασία ενθυλάκωσης ενός πακέτου σε ένα άλλου και της αποστολής του δεύτερου πακέτου πάνω από κάποιο δημόσιο δίκτυο.

Στη διαδικασία υλοποίησης ενός tunnel συμμετέχουν τρία είδη πρωτοκόλλων: τα πρωτόκολλα-φορείς (carrier protocols) που είναι τα πρωτόκολλα στα οποία ταξιδεύει η πληροφορία (Frame Relay, ATM, MPLS). Τα πρωτόκολλα ενθυλάκωσης (encapsulation protocols), που είναι τα πρωτόκολλα που περιέχουν μέσα τους τα αυθεντικά δεδομένα (GRE, IPSec, L2TP, L2F, PPTP). Και, τέλος, τα μεταφορικά πρωτόκολλα (passenger protocols), που είναι τα πρωτόκολλα τα οποία μεταφέρουν τα αρχικά δεδομένα (IPv4, IPv6, IPX, AppleTalk)

5.4.2 IPSEC

Το IPSec παρέχει ένα μηχανισμό για ασφαλή μεταφορά δεδομένων πάνω από ένα IP δίκτυο, διασφαλίζοντας την εμπιστευτικότητα, την ακεραιότητα και την αυθεντικότητα των δεδομένων διαμέσου μη ασφαλών δικτύων, όπως είναι το Internet. Περικλείει πρωτόκολλα και δεν είναι ταυτισμένο με κάποια συγκεκριμένα πρωτόκολλα κρυπτογράφησης ή αυθεντικοποίησης, ούτε με τεχνικές παραγωγής κλειδιών, ούτε και με σχέσεις ασφαλείας (security associations). Αντίθετα, παρέχει τους κανόνες και το πλαίσιο λειτουργίας, χρησιμοποιώντας υπάρχοντα πρωτόκολλα για όλες τις λειτουργίες του.

Το IPSec προσφέρει ασφαλή tunnels μεταξύ δυο πλευρών, όπως για παράδειγμα δύο routers. Ο αποστολέας καθορίζει ποια πακέτα χρειάζονται ασφάλεια και πρέπει να σταλούν μέσα από το tunnel και μετά καθορίζει τις παραμέτρους που χρειάζονται για να προστατευθούν αυτά τα πακέτα. Πιο συγκεκριμένα, αυτά τα tunnels είναι σύνολα security associations (SA) που εγκαθίστανται μεταξύ δύο πλευρών που χρησιμοποιούν IPSec. Τα SA καθορίζουν ποια πρωτόκολλα και ποιοι αλγόριθμοι θα πρέπει να χρησιμοποιηθούν για να διασφαλιστούν τα ευαίσθητα πακέτα. Τα SA δεν είναι αμφίδρομα, είναι, δηλαδή, μονοκατευθυντικά και εγκαθιδρύονται από το πρωτόκολλο ασφαλείας που χρησιμοποιείται (AH ή ESP).

5.4.2.1 Πρωτόκολλα του IPSEC

Για να δημιουργήσει ένα πλαίσιο ασφαλείας, το IPSec χρησιμοποιεί τα εξής πρωτόκολλα:

IKE: Παρέχει το πλαίσιο διαπραγμάτευσης των παραμέτρων ασφαλείας και εγκαθιδρύει τα αυθεντικοποιημένα κλειδιά. Το IPSec χρησιμοποιεί αλγορίθμους συμμετρικής κρυπτογραφίας, που είναι πιο αποτελεσματικοί και πιο εύκολα υλοποιήσιμοι. Αυτοί οι αλγόριθμοι, όμως, χρειάζονται μία ασφαλή μέθοδο ανταλλαγής των κλειδιών. Το IKE παρέχει αυτή ακριβώς τη δυνατότητα.

AH: Η αυθεντικοποίηση επικεφαλίδων (Authentication Header – AH) παρέχει ακεραιότητα και αυθεντικοποίηση της πηγής των δεδομένων και, προαιρετικά, προστασία από επιθέσεις επανάληψης (replay attacks). Η AH ενσωματώνεται στα δεδομένα που πρέπει να προστατευτούν. Πλέον, η AH έχει αντικατασταθεί, στις περισσότερες των περιπτώσεων, από το ESP.

ESP: Το ESP (Encapsulating Security Payload) παρέχει ένα πλαίσιο για κρυπτογράφηση, αυθεντικοποίηση και ασφάλιση δεδομένων. Επίσης, προσφέρει ιδιωτικότητα δεδομένων, προαιρετική αυθεντικοποίηση δεδομένων και εργαλεία για αντιμετώπιση επιθέσεων επανάληψης. Οι περισσότερες υλοποιήσεις IPSec στις μέρες μας χρησιμοποιούν ESP.

Επίσης, το IPSec περιλαμβάνει διάφορες επιλογές για την κρυπτογράφηση των δεδομένων: DES (Data Encryption Standard), 3DES (Triple Data Encryption Standard) ή AES (Advanced Encryption Standard). Ακόμη, προσφέρει και αρκετές μεθόδους για κατακερματισμό: HMAC (Hash-based Message Authentication Code), MD5 (Message Digest 5) ή SHA-1 (Secure Hash Algorithm).

Το IPSec έχει δύο μεθόδους για προώθηση δεδομένων σε ένα δίκτυο: το tunnel mode και το transport mode, τα οποία διαφέρουν στις περιπτώσεις στις οποίες εφαρμόζονται και στο πόσα επιπλέον bytes (overhead) προσθέτουν.

Στο tunnel mode ενθυλακώνεται και προστατεύεται ένα ολόκληρο IP πακέτο. Επειδή έτσι κρύβεται η IP επικεφαλίδα του πακέτου, πρέπει να προστεθεί μία νέα IP επικεφαλίδα, ώστε να προωθηθεί σωστά το πακέτο στον προορισμό του. Αυτή την νέα IP επικεφαλίδα ανήκει στις συσκευές που υλοποιούν την κρυπτογράφηση. Το tunnel mode μπορεί να χρησιμοποιήσει είτε το ESP,είτε το AH, είτε και τα δύο και, συνολικά, αυξάνει το μέγεθος ενός πακέτου κατά 20 περίπου bytes, λόγω της νέας επικεφαλίδας.

Αν στο δίκτυο μας μετακινούμε συνήθως μικρά πακέτα, π.χ. voice, ενδέχεται να προκύψει σημαντική επιβάρυνση λόγω των 20 bytes που προστίθενται σε κάθε πακέτο. Για αυτό

χρησιμοποιούμε το transport mode, όπου εισάγουμε την ESP επικεφαλίδα μεταξύ της IP επικεφαλίδας και του πρωτοκόλλου του επιπέδου μεταφοράς, π.χ. TCP. Και οι δύο IP διευθύνσεις των δύο δικτυακών κόμβων, των οποίων η κίνηση προστατεύεται, είναι ορατές. Ακόμη, προσφέρει μικρότερη επέκταση του πακέτου. Το transport mode μπορεί να χρησιμοποιήσει είτε το ESP,είτε το AH, είτε και τα δύο, ενώ συνεργάζεται πολύ καλά και με το GRE, επειδή το GRE ήδη αποκρύπτει τις διευθύνσεις των τερματικών σταθμών προσθέτοντας μία επικεφαλίδα.

5.4.2.2 IKE

Για να υλοποιηθεί σωστά η κρυπτογράφηση σε ένα VPN θα πρέπει το κλειδί να αλλάζει περιοδικά. Αν δεν γίνεται αυτό, το VPN γίνεται ευάλωτο σε επιθέσεις «ωμής δύναμης». Στο IPSec Tunnel το πρόβλημα αυτό λύνεται με το IKE. Το IKE με τη σειρά του χρησιμοποιεί δύο άλλα πρωτόκολλα για να αυθεντικοποιεί την άλλη πλευρά και για να δημιουργεί τα κλειδιά. Κύρια δουλειά του IKE είναι να διαπραγματεύεται ένα SA, που, ουσιαστικά, είναι μια συμφωνία μεταξύ δύο πλευρών και περιλαμβάνει τη συμφωνία σε συγκεκριμένες παραμέτρους που είναι απαραίτητες για την εγκαθίδρυση της επικοινωνίας. Συνοπτικά, το IPSec χρησιμοποιεί το IKE για να πετύχει τα ακόλουθα: διαπραγμάτευση των χαρακτηριστικών του SA, την αυτόματη δημιουργία κλειδιών, την αυτόματη ανανέωση των κλειδιών και όλα αυτά, με έναν εύκολο και διαχειρίσιμο τρόπο.

Επίσης το IKE περιλαμβάνει τα ακόλουθα χαρακτηριστικά:

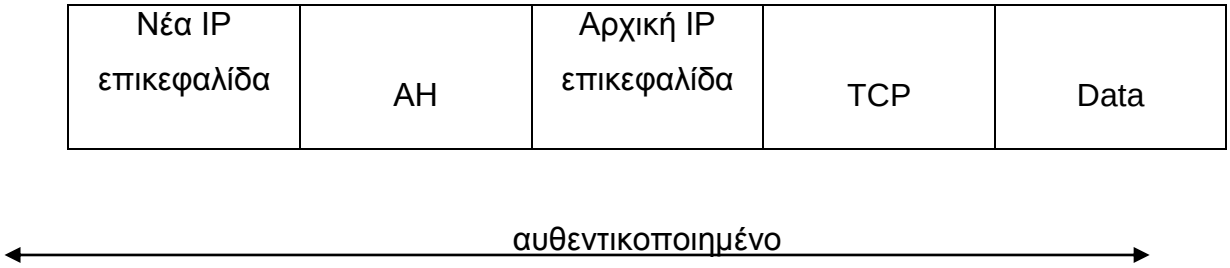
- Εξαλείφει την ανάγκη για χειροκίνητο καθορισμό όλων των παραμέτρων ασφαλείας μεταξύ των δύο πλευρών
- Επιτρέπει τον καθορισμό της χρονικής διάρκειας ενός SA
- Επιτρέπει την κρυπτογράφηση των κλειδιών κατά την διάρκεια των IPSec συνόδων
- Επιτρέπει στο IPSec να προσφέρει προστασία στις επιθέσεις επανάληψης
- Επιτρέπει την χρησιμοποίηση Certification Authorities
- Επιτρέπει την δυναμική αυθεντικοποίηση των δύο πλευρών.

Η εκτέλεση του IKE περιλαμβάνει δύο φάσεις και μία ενδιάμεση προαιρετική. Στην πρώτη φάση γίνεται η αρχική διαπραγμάτευση για το SA που θα ισχύσει μεταξύ των δύο πλευρών. Επίσης, προαιρετικά, μπορεί να περιλάβει και μία διαδικασία αυθεντικοποίησης. Στη συγκεκριμένη φάση, ακόμη και αν υπάρχει ωτακουστής, δεν υπάρχει πρόβλημα ή κάποιος κίνδυνος ασφαλείας. Στην ενδιάμεση, προαιρετική φάση δίνεται η δυνατότητα για περαιτέρω αυθεντικοποίηση των συμμετεχόντων πλευρών, μέσω του πρωτοκόλλου Xauth (Extended Authentication). Τέλος, στη δεύτερη φάση γίνεται η διαπραγμάτευση του SA, για λογαριασμό του IPSec. Επειδή τα SAs που χρησιμοποιεί το IPSec είναι μονοκατευθυντικά, θα πρέπει να γίνουν ξεχωριστές ανταλλαγές κλειδιών.

5.4.2.3 AH

Το AH δεν προστατεύει τα δεδομένα με τη συνήθη έννοια, δηλαδή αποκρύπτοντας τα δεδομένα, αλλά «σφραγίζοντας» με μία σφραγίδα ασφαλείας τα δεδομένα. Επίσης προστατεύει πεδία της IP επικεφαλίδας. Ωστόσο, το AH δεν πρέπει να χρησιμοποιείται μόνο του όταν μας ενδιαφέρει η εμπιστευτικότητα. Οι αλγόριθμοι κατακερματισμού που υποστηρίζει το AH είναι ο MD5 και ο SHA-1

Παρακάτω φαίνεται σχηματικά ένα πακέτο στο οποίο έχει εφαρμοστεί AH σε tunnel mode.



Σχήμα 5.1: Πακέτο που έχει εφαρμοστεί AH σε tunnel mode

Η διαδικασία που ακολουθείται, όταν χρησιμοποιείται AH είναι η εξής:

1. Η IP επικεφαλίδα και τα δεδομένα περνάνε μέσα από μία συνάρτηση κατακερματισμού

2. Το αποτέλεσμα του hashing χρησιμοποιείται για την δημιουργία της AH επικεφαλίδας, που προστίθεται στο αρχικό πακέτο
3. Το νέο πακέτο μεταφέρεται στον router της άλλης πλευρά του IPSec tunnel
4. Ο router της άλλης πλευράς κατακερματίζει και αυτός την IP επικεφαλίδα και τα δεδομένα και
5. Ο router αφαιρεί το μεταδοθέν hash από την AH επικεφαλίδα
6. Ο router συγκρίνει τα δύο hashes, που πρέπει να είναι ακριβώς τα ίδια.

5.4.2.4 ESP

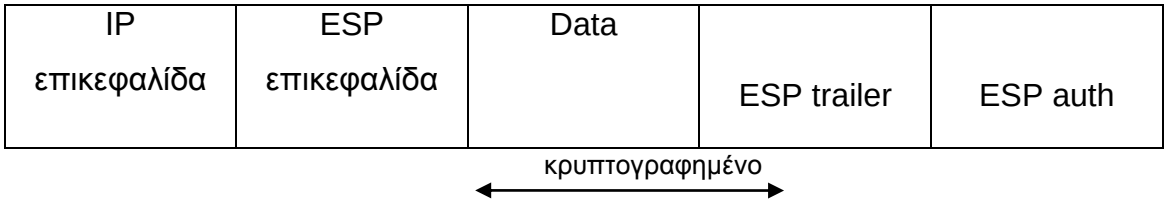
Το ESP, σε συνδυασμό με μία μέθοδο κρυπτογράφησης ή ένα SA, προστατεύει τα δεδομένα, κάνοντάς μη αποκρυπτογραφήσιμα. Προστατεύει μόνο το κομμάτι των δεδομένων του πακέτου, και όχι της επικεφαλίδες και μπορεί να προσφέρει αυθεντικοποίηση των προστατευμένων δεδομένων. Μία ESP επικεφαλίδα στην αρχή και ένα trailer στο τέλος προστίθενται στο ήδη κρυπτογραφημένο πακέτο. Έτσι, στην αυθεντικοποίηση του ESP, τόσο το αρχικό κρυπτογραφημένο πακέτο, όσο και η επικεφαλίδα και το trailer περιλαμβάνονται στη διαδικασία κατακερματισμού. Τέλος, προστίθεται μία νέα IP επικεφαλίδα στην αρχή του πακέτου, που χρησιμοποιείται για να δρομολογηθεί το πακέτο στο Internet.

Αν εφαρμόσουμε και αυθεντικοποιήση και κρυπτογράφηση, τότε η κρυπτογράφηση πραγματοποιείται πριν την αυθεντικοποίηση. Ο λόγος που γίνεται αυτό είναι για να έχουμε γρήγορο εντοπισμό και απόρριψη επανειλημμένων και/ή ύποπτων πακέτων. Πριν την αποκρυπτογράφηση, λοιπόν, το παραλήπτης μπορεί να αυθεντικοποιήσει τα εισερχόμενα πακέτα, ελαχιστοποιώντας την πιθανότητα εμφάνισης προβλημάτων, όπως, για παράδειγμα μια DoS επίθεση.

Το transport mode είναι εκεί που χρησιμοποιείται by default στο IPSec και χρησιμοποιείται μεταξύ δύο τερματικών σταθμών. Το transport mode προστατεύει τα δεδομένα και τις επικεφαλίδες ανωτέρου επιπέδου, αλλά αφήνει απροστάτευτη την IP επικεφαλίδα, η οποία χρησιμοποιείται για τη δρομολόγηση. Όταν χρησιμοποιείται tunnel mode, τότε παρέχεται προστασία σε όλο το IP πακέτο. Εφαρμόζεται σε περιπτώσεις επικοινωνίας μεταξύ ενός τερματικού σταθμού και ενός security gateway ή μεταξύ security gateways.

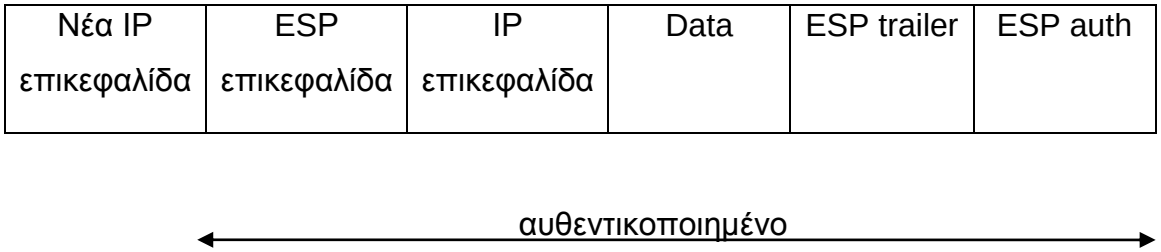
Παρακάτω παρουσιάζεται σχηματικά η δομή του πακέτου με ESP, τόσο σε transport όσο και σε tunnel mode.

Transport mode



Σχήμα 5.2: Πακέτο που έχει εφαρμοστεί ESP σε transport mode

Tunnel mode



Σχήμα 5.3: Πακέτο που έχει εφαρμοστεί ESP σε tunnel mode

5.4.2.5 Hashing Πρωτόκολλα

Όταν μεταφέρονται δεδομένα σε ένα VPN πάνω από το Internet, υπάρχει το ενδεχόμενο κάποιος να μπορέσει να τα υποκλέψει και να τα αλλάξει. Για να προφυλαχτούμε από αυτό, προσθέτουμε στο τέλος κάθε μηνύματος ένα hash. Το hash μας δίδει έναν τρόπο να εγγυηθούμε την ακεραιότητα του αρχικού μηνύματος. Έτσι, αν το μεταδοθέν hash είναι ίδιο με το παραληφθέν hash, το μήνυμα δεν έχει αλλαχθεί.

Ένα πρωτόκολλο παραγωγής hash είναι το HMAC. Το HMAC μπορεί να χρησιμοποιηθεί σε συνδυασμό με κάθε επαναληπτική κρυπτογραφική συνάρτηση κατακερματισμού, όπως το MD5 και στο SHA-1, μαζί με κάποιο διαμοιραζόμενο κλειδί. Η κρυπτογραφική ισχύς του HMAC εξαρτάται από τις συναρτήσεις κατακερματισμού που χρησιμοποιεί.

Το MD5 παράγει έξοδο 128 bit, ενώ το SHA-1 παράγει έξοδο 160 bit, από τα οποία μόνο τα 96 χρησιμοποιούνται στο IPSec. Επίσης, το SHA-1 μπορεί να είναι πιο αργό στο να υπολογιστεί από το MD5, ωστόσο είναι ασφαλέστερο.

5.4.2.6 Υλοποίηση ενός VPN Tunnel

Η λειτουργία του IPSec μπορεί να αναλυθεί σε πέντε επιμέρους βήματα. Αυτά είναι:

1. Ανίχνευση της ευαίσθητης και/ή ενδιαφέρουσας κίνησης και έναρξη της IPSec διαδικασίας. Αν η κίνηση δεν είναι ευαίσθητη και/ή ενδιαφέρουσα, αποστέλλεται ως απλό κείμενο.
2. Πρώτη φάση του IKE, όπου το IKE αυθεντικοποιεί τους συναλλασσόμενους και διαπραγματεύεται την εγκαθίδρυση ενός SA. Εγκαθίσταται ένα ασφαλές κανάλι επικοινωνίας.
3. Το IKE διαπραγματεύεται τις παραμέτρους του SA και εγκαθιστά στις συναλλασσόμενες πλευρές ταιριαστές SA.
4. Μεταφορά δεδομένων.
5. Κατάργηση του tunnel.

Για να υλοποιήσουμε ένα site-to-site VPN σε δύο Cisco routers θα πρέπει να ακολουθήσουμε τα εξής βήματα στους δύο routers:

1. Ρύθμιση της ISAKMP πολιτικής που είναι απαραίτητη για την εγκαθίδρυση του IKE tunnel

2. Ορισμός του transform set, δηλαδή των παραμέτρων του IPSec, όπως οι αλγόριθμοι κρυπτογράφησης και ακεραιότητας.

3. Δημιουργία μιας ACL (access list) η οποία θα είναι αυτή που αναγνωρίζει την ενδιαφέρουσα κίνηση που πρέπει να κρυπτογραφηθεί.

4. Δημιουργία ενός crypto map, για να συνδυάσουμε όλες τις προηγούμενες ρυθμίσεις και να δηλώσουμε τις διευθύνσεις της άλλης πλευράς.

5. Εφαρμόζουμε το crypto map στη διεπαφή εξόδου του VPN gateway

6. Δημιουργία μιας ACL και εφαρμογή της στο interface για να επιτρέπεται να περνάνε τα πρωτόκολλα του IPSec.

Παρακάτω φαίνεται μία υλοποίηση VPN σε έναν Cisco router και έπεται ανάλυση των βημάτων. Στη συνέχεια παρατίθεται και το configuration του router της άλλης πλευράς του VPN.

Πίνακας 5.5: VPN σε Cisco router

```
1.  R1(config)#crypto isakmp policy 1
2.  R1(config-isakmp)#authentication pre-share
3.  R1(config-isakmp)#hash sha
4.  R1(config-isakmp)#encryption aes 256
5.  R1(config-isakmp)#group 2
6.  R1(config)#crypto isakmp key SECRET address 172.16.171.20
255.255.255.255
7.  R1(config)#crypto ipsec transform-set AES-SHA esp-aes 128
esp-sha-hmac
8.  R1(cfg-crypto-trans)#access-list 101 permit ip 10.1.1.0 0.0.0.255
10.1.2.0 0.0.0.255
9.  R1(config)#crypto map VPN_to_R2 10 ipsec-isakmp
10. R1(config-crypto-map)#set peer 172.16.171.20
11. R1(config-crypto-map)#match address 101
12. R1(config-crypto-map)#set transform-set AES-SHA
13. R1(config)#int fa0/0
14. R1(config-if)#ip address 172.16.172.10 255.255.255.0
15. R1(config-if)#crypto map VPN_to_R2
16. R1(config)#ip route 10.1.2.0 255.255.255.0 172.16.171.20
17. R1(config)#access-list 102 permit ah host 172.16.172.10 host
172.16.171.20
18. R1(config)#access-list 102 permit esp host 172.16.172.10 host
172.16.171.20
19. R1(config)#access-list 102 permit udp host 172.16.172.10 host
```

```
172.16.171.20 eq isakmp
```

1.: Δημιουργούμε την ISAKMP policy 1

2.: Επιλέγουμε ως μέθοδο αυθεντικοποίσης

3.: Επιλέγουμε τη μέθοδο κατακερματισμού

4.: Επιλέγουμε τον αλγόριθμο κρυπτογράφησης

5.: Επιλέγουμε το Diffie-Hellman group

6.: Ορίζουμε ως κλειδί τη λέξη SECRET και στη συνέχεια δίνουμε την IP διεύθυνση του tunnel της άλλης πλευράς.

7.: Ορίζουμε το transform-set AES-SHA, που ουσιαστικά καθορίζουμε τις παραμέτρους του IPSec tunnel.

8.: Δηλώνουμε ποια κίνηση θεωρούμε ενδιαφέρουσα. Εδώ επιλέγουμε ως ενδιαφέρουσα κάθε είδους κίνηση από το δίκτυο 10.1.1.0 στο 10.1.2.0

9.: Δημιουργούμε ένα crypto map με όνομα VPN_to_R2. Ουσιαστικά δηλώνουμε τις παραμέτρους του SA

10.: Δίνουμε την IP διεύθυνση του tunnel της άλλης πλευράς

11.: Δηλώνουμε στο router ποια κίνηση θα πρέπει να θεωρεί ενδιαφέρουσα

12.: Δηλώνουμε στον router ποιο transform-set να χρησιμοποιήσει, στην περίπτωσή μας αυτό που φτιάξαμε, το AES-SHA.

13-14.:Δίνουμε IP διεύθυνση στο interface που θα αποστέλλει την κρυπτογραφημένη κίνηση

15.: Δηλώνουμε στο interface ποιο crypto map θα χρησιμοποιεί

16.: Φτιάχνουμε μία στατική διαδρομή προς τον router της άλλης πλευράς (θα μπορούσαμε να έχουμε και routing protocol)

17.-18.-19.: Επιτρέπουμε στα πρωτόκολλα του IPSec να περνάνε ελεύθερα.

Στη συνέχεια δίνουμε και το configuration που πρέπει να υλοποιήσουμε στον router της άλλης πλευράς του VPN.

Πίνακας 5.6: Configuration στην άλλη πλευρά του VPN

```
1.  R1(config)#crypto isakmp policy 1
2.  R1(config-isakmp)#authentication pre-share
3.  R1(config-isakmp)#hash sha
4.  R1(config-isakmp)#encryption aes 256
5.  R1(config-isakmp)#group 2
6.  R1(config)#crypto isakmp key SECRET address 172.16.171.10
255.255.255.255
7.  R1(config)#crypto ipsec transform-set AES-SHA esp-aes 128 esp-sha-
hmac
8.  R1(cfg-crypto-trans)#access-list 101 permit ip 10.1.2.0 0.0.0.255
10.1.1.0 0.0.0.255
9.  R1(config)#crypto map VPN_to_R1 10 ipsec-isakmp
10. R1(config-crypto-map)#set peer 172.16.171.10
11. R1(config-crypto-map)#match address 101
12. R1(config-crypto-map)#set transform-set AES-SHA
13. R1(config)#int fa0/0
14. R1(config-if)#ip address 172.16.172.20 255.255.255.0
15. R1(config-if)#crypto map VPN_to_R1
16. R1(config)#ip route 10.1.1.0 255.255.255.0 172.16.171.10
17. R1(config)#access-list 102 permit ah host 172.16.172.20 host
172.16.171.10
18. R1(config)#access-list 102 permit esp host 172.16.172.20 host
172.16.171.10
19. R1(config)#access-list 102 permit udp host 172.16.172.20 host
172.16.171.10 eq isakmp
```

5.4.3 SSL

Σχεδόν κάθε οργανισμός στις μέρες μας διαθέτει και ιστοσελίδα. Επίσης, ο αριθμός των χρηστών με πρόσβαση στο Internet αυξάνει ραγδαία, ενώ το ίδιο ραγδαία αυξάνει και η επιθυμία των επιχειρήσεων να πουλήσουν τα προϊόντα τους μέσω του Διαδικτύου. Όμως, το Διαδίκτυο δεν είναι ασφαλές.

Η αντιμετώπιση για αυτό το πρόβλημα είναι η εφαρμογή μεθόδων ασφαλείας μεταξύ του επιπέδου transport (layer 4 του OSI) και του επιπέδου εφαρμογών (layer 7 του OSI). Η πλέον δημοφιλής λύση είναι η χρησιμοποίηση του Secure Sockets Layer (SSL). Σε αυτό το σημείο έχουμε δύο επιλογές υλοποίησης: είτε το SSL να είναι κομμάτι του υποκείμενου επιπέδου και, συνεπώς, αόρατο για τις εφαρμογές, είτε να ενσωματώνεται σε συγκεκριμένα πακέτα. Για παράδειγμα, ο Internet Explorer και το Netscape έχουν ενσωματωμένο το SSL, όπως και πολλές ιστοσελίδες.

Όταν πλοηγούμαστε στο Internet το SSL δεν είναι πάντα ενεργό. Ενεργοποιείται κατά την πρόσβασή μας σε σελίδες **Error! Hyperlink reference not valid.**, ενώ η πρόσβαση σε σελίδες **Error! Hyperlink reference not valid.** γίνεται χωρίς τη χρήση SSL. Με το που θα εισάγουμε ένα σύνδεσμο https, ο φυλλομετρητής (browser) ξεκινάει μία σύνοδο (session) με τον server στο TCP port 443. Το SSL ξεκινάει τότε να διαπραγματεύεται την εγκαθίδρυση μιας ασφαλούς σύνδεσης για να μεταφερθούν μέσω αυτής τα δεδομένα. Αν η διαπραγμάτευση αποτύχει, δεν αποστέλλονται δεδομένα. Η επιτυχής διαπραγμάτευση γίνεται γνωστή στο χρήστη. Για παράδειγμα στον IE εμφανίζεται ένα λουκέτο χαμηλά στο παράθυρο.

Το SSL είναι σχεδιασμένο να χρησιμοποιεί το TCP για να παρέχει μία αξιόπιστη, από άκρο σε άκρο, ασφαλή μεταφορά δεδομένων. Δεν είναι ένα απλό πρωτόκολλο, αλλά δύο επίπεδα πρωτοκόλλων.

Το SSL Record πρωτόκολλο παρέχει βασικές υπηρεσίες ασφαλείας σε διάφορα πρωτόκολλα ανώτερων επιπέδων, όπως για παράδειγμα στο Handshake Protocol. Πιο συγκεκριμένα, προσφέρει εμπιστευτικότητα, μέσω της κρυπτογράφησης των δεδομένων της εφαρμογής και ακεραιότητα δεδομένων, μέσω του κωδικού αυθεντικοποίησης μηνύματος (Message Authentication Code - MAC).

Το HTTP, που υλοποιεί την μεταφορά σε client/server WEB εφαρμογές, μπορεί να λειτουργήσει αξιοποιώντας ο SSL. Τρία πρωτόκολλα ανωτέρων επιπέδων ορίζονται ως μέρος του SSL: το πρωτόκολλο χειραψίας (Handshake Protocol), το Change CipherSpec πρωτόκολλο και το πρωτόκολλο ειδοποίησης (Alert Protocol). Αυτά τα τρία πρωτόκολλα,

που χρησιμοποιούνται αποκλειστικά από το SSL, ελέγχουν τις συναλλαγές που απαιτούνται για την υλοποίηση του SSL.

Το Handshake Protocol υλοποιεί την αυθεντικοποίηση του client και του server και διαπραγματεύεται τη μέθοδο κρυπτογράφησης, το MAC, τα κλειδιά, κ.α. Λειτουργεί πριν ξεκινήσει η μεταφορά των δεδομένων και υλοποιείται με τη αποστολή σειράς μηνυμάτων, τόσο από το client, όσο και από τον server.

Το Change CipherSpec Protocol υλοποιείται με την αποστολή ενός μηνύματος ενός byte με την τιμή 1. Ο μοναδικός σκοπός που εξυπηρετείται είναι μετάβαση από την κατάσταση αναμονής στην παρούσα κατάσταση, το οποίο ενημερώνει ότι θα χρησιμοποιηθεί η CipherSuite. Ουσιαστικά είναι ένα σήμα που στέλνει ο client στον server και ο server στον client. Όταν και οι δύο πλευρές το έχουν παραλάβει, όλα τα επόμενα μηνύματα στέλνονται χρησιμοποιώντας τα συμφωνηθέντα κλειδιά.

Το Alert Protocol χρησιμοποιείται για να μεταφέρει ειδοποιήσεις που αφορούν το SSL στην άλλη πλευρά. Τα μηνύματα αυτά αποστέλλονται συμπιεσμένα και κρυπτογραφημένα.

Δύο βασικές έννοιες που διέπουν το SSL είναι η SSL σύνδεση (SSL connection) και η SSL σύνοδος (SSL session). Μία SSL connection είναι μία λογική client/server σύνδεση που παρέχει ένα συγκεκριμένο τύπο υπηρεσίας. Για το SSL αυτή η σύνδεση είναι μεταξύ δύο ομότιμων οντοτήτων (peer-to-peer). Αυτές οι συνδέσεις είναι πρόσκαιρες και συνδέονται με ένα session. Ένα SSL session είναι μία συσχέτιση μεταξύ ενός client και ενός server. Τα sessions δημιουργούνται από το Handshake Protocol και ορίζουν ένα σύνολο κρυπτογραφικών παραμέτρων ασφαλείας, που μπορούν να χρησιμοποιηθούν από πολλά connections. Ουσιαστικά, τα sessions μας βοηθάνε να αποφεύγουμε τη συνεχή διαπραγμάτευση των παραμέτρων ασφαλείας κάθε σύνδεσης.

Μεταξύ ενός client και ενός server, μπορούν να υπάρχουν πολλαπλές συνδέσεις. Για την ακρίβεια, μπορούν να υπάρχουν πολλά sessions. Ωστόσο αυτό αποφεύγεται στην πράξη.

Η λειτουργία του SSL μπορεί να αναλυθεί σε επιμέρους βήματα. Το πρώτο βήμα είναι η κατάτμηση (fragmentation) των δεδομένων σε διαχειρίσιμα blocks, μεγέθους 16384 bytes ή λιγότερα. Στη συνέχεια, μπορεί προαιρετικά να υπάρξει συμπίεση. Το επόμενο βήμα είναι να υπολογιστεί το MAC των συμπιεσμένων δεδομένων. Για αυτό το λόγο χρησιμοποιείται ένα διαμοιρασμένο, μυστικό κλειδί. Ο παραλήπτης, χρησιμοποιώντας το ίδιο κλειδί, θα ακολουθήσει την αντίστροφη διαδικασία. Το συμπιεσμένο μήνυμα συν το

MAC κρυπτογραφούνται χρησιμοποιώντας συμμετρική κρυπτογραφία, επιλέγοντας από μία πληθώρα αλγορίθμων κρυπτογράφησης, όπως ο DES ή ο 3DES. Το τελευταίο βήμα είναι η τοποθέτηση μίας SSL επικεφαλίδας.

Η SSL επικεφαλίδα περιέχει τα εξής πεδία:

- **Περιεχόμενο (8bits):** το πρωτόκολλο ανωτέρου επιπέδου που έκανε χρήση του SSL.
- Major Version (8 bits): για το SSLv3, είναι 3.
- **Minor Version (8 bits)**: για το SSLv3, είναι 0.
- **Συμπιεσμένο μέγεθος (16 bits)**: Το μέγεθος του συμπιεσμένου block ή του block απλού κειμένου, αν δεν υπάρχει συμπίεση.

5.5 Προστασία από επιθέσεις

5.5.1 DMZ

Μία DMZ είναι ένα φυσικό ή λογικό υποδίκτυο ενός οργανισμού, που περιέχει και παρέχει σε ένα μεγαλύτερο, μη εμπιστεύσιμο δίκτυο (συνήθως το Internet), όλες εκείνες τις υπηρεσίες που είναι απαραίτητες, ώστε να έρθει σε επαφή με τον έξω κόσμο και να επιτελέσει ορθά το έργο του. Η ονομασία της προκύπτει από την σύντμηση των λέξεων Demilitarized Zone (αποστρατικοποιημένη ζώνη), που στην καθημερινή ζωή περιγράφει μία περιοχή μεταξύ δύο εμπόλεμων πλευρών στην οποία δεν επιτρέπονται εχθροπραξίες. Σκοπός της DMZ σε ένα δίκτυο είναι να προσθέσει ένα επιπλέον επίπεδο ασφαλείας στο εσωτερικό δίκτυο του οργανισμού και έτσι η DMZ είναι το απώτατο σημείο που μπορεί να φτάσει κάποιος εξωτερικός επιτιθέμενος.

Τα πλέον ευάλωτα συστήματα σε ένα δίκτυο υπολογιστών είναι αυτά που παρέχουν υπηρεσίες στους χρήστες έξω από το τοπικό δίκτυο. Τέτοιες υπηρεσίες είναι τα e-mail, DNS services, web ιστοσελίδες, κ.α. Επειδή, λοιπόν, υπάρχει μεγάλη πιθανότητα να δεχτούν επίθεση, για αυτό απομονώνουμε αυτό το κομμάτι του δικτύου από το υπόλοιπο δίκτυο, ώστε να περιορίσουμε εκεί τις όποιες συνέπειες και να αποτρέψουμε την είσοδο στα ενδότερα του δικτύου μας.

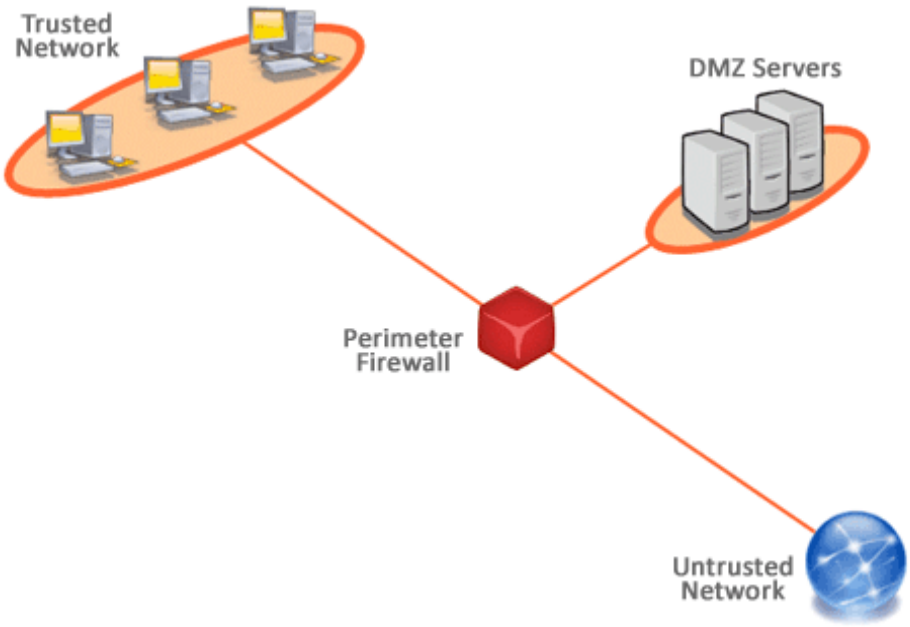
Η συνδεσιμότητα των χρηστών και των υπηρεσιών που βρίσκονται στη DMZ είναι περιορισμένη προς το εσωτερικό δίκτυο και αφορά συγκεκριμένους χρήστες. Αντίθετα, η επικοινωνία με άλλους χρήστες και servers στην DMZ και στον έξω κόσμο είναι ελεύθερη.

Αυτό επιτρέπει την παροχή υπηρεσιών τόσο στο εσωτερικό, όσο και στο εξωτερικό δίκτυο. Επίσης, μία DMZ προστατεύει από εξωτερικές επιθέσεις, αλλά δεν προστατεύει (και δεν είναι δουλειά της να το κάνει) από εσωτερικές επιθέσεις, όπως υποκλοπές επικοινωνιών, spoofing διευθύνσεων κτλ.

Συνήθως, ό, τι υπηρεσία παρέχεται σε χρήστες στο εξωτερικό δίκτυο, βρίσκεται στην DMZ. Αυτές οι υπηρεσίες περιλαμβάνουν web services, mail services, FTP services, VoIP service, Internet Banking κτλ.

Υπάρχουν πολλοί τρόποι να σχεδιαστεί και να υλοποιηθεί μία DMZ. Ωστόσο, δύο είναι οι βασικές μέθοδοι που έχουν επικρατήσει: η πρώτη υλοποιείται με τη χρήση ενός firewall και η δεύτερη με δύο firewall. Και στις δύο περιπτώσεις υπάρχουν 3 οδεύσεις από τον firewall: μία προς το εξωτερικό δίκτυο, μία προς το εσωτερικό δίκτυο και μία προς την DMZ.

Παρακάτω φαίνεται το σχηματικό για μία υλοποίηση με ένα firewall.

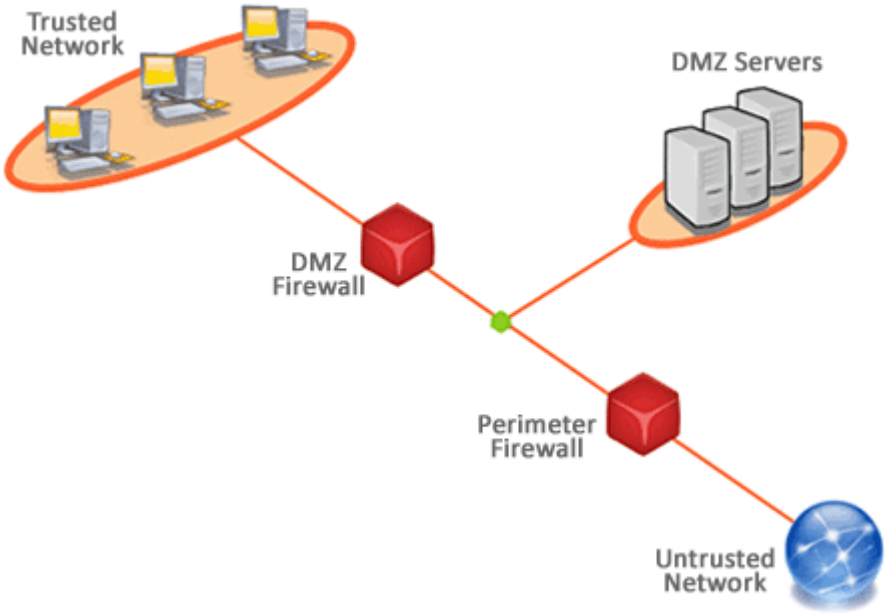


Σχήμα 5.4: Υλοποίηση με firewall

Για να δημιουργήσουμε την DMZ του παραπάνω σχήματος, θα πρέπει να χρησιμοποιήσουμε έναν firewall με τουλάχιστον τρεις διεπαφές. Η μία θα καταλήγει στον router του παρόχου, η άλλη στο εσωτερικό μας δίκτυο και η τρίτη στη DMZ. Το μειονέκτημα αυτής της υλοποίησης είναι ότι ο firewall πλέον αποτελεί μοναδικό σημείο αποτυχίας (single point of failure), δηλαδή αν τεθεί εκτός λειτουργίας δεν υπάρχει

εναλλακτική λύση. Επίσης, πρέπει να είναι αρκετά ισχυρός για να διαχειριστεί όλον αυτόν τον φόρτο.

Παρακάτω φαίνεται το σχηματικό για μία υλοποίηση με δύο firewalls.



Σχήμα 5.5: Υλοποίηση με χρήση δύο firewalls

Ο ένας firewall, ο λεγόμενος απώτατος ή εξωτερικός firewall (front-end firewall) ρυθμίζεται έτσι, ώστε να επιτρέπει την κίνηση που έχει ως προορισμό την DMZ. Ο δεύτερος firewall, ο back-end firewall, επιτρέπει την κίνηση από την DMZ προς το εσωτερικό δίκτυο.

Η υλοποίηση αυτή είναι ασφαλέστερη, μιας και δύο συσκευές πρέπει να τεθούν εκτός λειτουργίας ή να δεχθούν επίθεση για να καταρρεύσει το σύστημα. Επίσης, προτείνεται η χρήση firewalls από διαφορετικό κατασκευαστή ο καθένας, μιας και έτσι ελαχιστοποιούνται οι ευπάθειες, αλλά και τα λάθη στη ρύθμισή τους. Είναι προφανές, βέβαια, ότι πρόκειται και για πιο κοστοβόρα λύση.

Η σύγχρονη τάση στη δημιουργία DMZ είναι να δημιουργούμε πολλαπλές DMZ, δηλαδή να έχουμε μία DMZ για κάθε service. Έτσι, δεν έχουμε σημεία ελέγχου μόνο μεταξύ εξωτερικού και εσωτερικού δικτύου, αλλά, πλέον, και μεταξύ των διαφορετικών services. Με αυτόν τον τρόπο, μία επιτυχής επίθεση σε κάποιον server του οργανισμού θα επηρεάσει μόνο το συγκεκριμένο service και όχι την πλήρη λειτουργία του οργανισμού.

Συμπερασματικά, τα οφέλη που προσφέρει μια καλοσχεδιασμένη DMZ είναι τα ακόλουθα:

- Τα σημεία φιλτραρίσματος της κίνησης (είτε routers, είτε firewalls) αρχικά προστατεύουν τα services, και, αν αυτά εκτεθούν σε κίνδυνο, να περιορίσουν τις δυνατότητες του επιτιθέμενου να διεισδύσει περισσότερο.
- Οι δημόσιοι servers που βρίσκονται στη DMZ ασφαλίζονται όσο το δυνατόν περισσότερο, με σκοπό να δυσκολέψουν όσο το δυνατόν περισσότερο τον επιτιθέμενο.
- Η τοποθέτηση proxy servers στην DMZ εξομαλύνουν την κίνηση, ειδικά όσον αφορά τον φόρτο που προέρχεται από το εσωτερικό δίκτυο με κατεύθυνση προς το Internet.

5.5.2 Firewalls

5.5.2.1 Hardware Firewalls

Ένα firewall μπορεί να υλοποιείται είτε με υλικό (hardware-based), είτε με λογισμικό (software-based) χρησιμοποιείται στην ασφάλεια των δικτύων. Πρωταρχικός του στόχος είναι να ελέγχει την εισερχόμενη και την εξερχόμενη κίνηση, αναλύοντας τα πακέτα δεδομένων και αποφασίζοντας αν πρέπει να επιτρέψει τη διέλευσή τους, με βάση ένα προαποφασισμένο σύνολο κανόνων. Με άλλα λόγια, ένα firewall αποτελεί μία γέφυρα μεταξύ του εσωτερικού και του εξωτερικού δικτύου, η οποία γέφυρα είναι ασφαλής και εμπιστεύσιμη.

Υπάρχουν τρεις τύποι firewall τεχνολογιών: το packet filtering, οι ALGs και το stateful packet filtering.

Το packet filtering περιορίζει τα πακέτα που εισέρχονται σε ένα δίκτυο, βασιζόμενος στην πληροφορία που υπάρχει στις επικεφαλίδες των πακέτων. Υλοποιείται συνήθως από τους routers μέσω access lists για να καθορίζεται ποια κίνηση επιτρέπεται και ποια όχι. Αν η κίνηση επιτρέπεται, στέλνεται στον προορισμό της. Διαφορετικά, απορρίπτεται. Η προώθηση ή απόρριψη των πακέτων γίνεται με βάση τις IP διευθύνσεις και τα port numbers πηγής-προορισμού ή με βάση τον τύπο του πακέτου. Κάθε συσκευή που υλοποιεί ACLs μπορεί να επιτελέσει packet filtering.

Παρόλο που το packet filtering είναι πολύ αποτελεσματικό και παντελώς διάφανο στους χρήστες, παρουσιάζει ορισμένα μειονεκτήματα. Καταρχήν, είναι ευάλωτο σε επιθέσεις spoofing, καθώς με αλλαγή των διευθύνσεων σε κάποιες τιμές που πληρούν τα κριτήρια εισόδου, επιτρέπεται η είσοδος σε ύποπτα πακέτα. Επίσης, δεν φιλτράρουν καλά κατατετμημένα πακέτα, επειδή σε αυτά η TCP επικεφαλίδα βρίσκεται μόνο στο πρώτο πακέτο. Έτσι, φιλτράρεται το πρώτο πακέτο, ενώ επιτρέπονται όλα τα υπόλοιπα. Τέλος, για πολύπλοκες ACLs και πολύπλοκες υλοποιήσεις, ο φόρτος εργασίας για τη δημιουργία, συντήρηση, παρακολούθηση και φινίρισμα είναι υπερβολικός και δυσβάσταχτος.

Οι ALGs λειτουργούν στο επίπεδο εφαρμογών. Είναι ένα ειδικό λογισμικό που είναι σχεδιασμένο να μεταφέρει αιτήσεις και απαντήσεις επιπέδου εφαρμογών. Λειτουργεί σαν διαμεσολαβητής μεταξύ ενός πελάτη και ενός server. Για τον πελάτη, ο ALG είναι ένας εικονικός server. Για τον server, ο ALG είναι ένας εικονικός client.

Τα μειονεκτήματα των ALGs είναι ότι πρέπει να αξιολογούν πολλή πληροφορία, σε πολλά πακέτα, με αποτέλεσμα να δημιουργούν καθυστερήσεις. Επίσης, ένα ALG σχεδιάζεται για να φιλτράρει μία εφαρμογή. Αν θέλουμε να φιλτράρουμε και άλλες εφαρμογές, θα πρέπει να εγκαταστήσουμε και άλλα ALGs. Ακόμη, αποτελούν μοναδικό σημείο αποτυχίας για το δίκτυο, καθώς αν τεθεί εκτός λειτουργίας ένα ALG, τότε διακυβεύεται η ασφάλεια όλου του δικτύου.

Το stateful packet filtering είναι η πιο διαδεδομένη τεχνολογία firewalling στις μέρες μας. Είναι μία μέθοδος φιλτραρίσματος πακέτων, η οποία, όμως, είναι και ενήμερη για το επίπεδο εφαρμογών. Συντηρεί έναν πίνακα καταστάσεων για να παρακολουθεί όλα τα ενεργά sessions που διαπερνάν το firewall, ενώ παρακολουθεί και την κίνηση των πακέτων. Ο πίνακας καταστάσεων αλλάζει δυναμικά, ανάλογα με την κίνηση που παρατηρεί. Αν τα πακέτα έχουν τις αναμενόμενες ιδιότητες, με βάση τον πίνακα καταστάσεων, τότε προωθούνται, αλλιώς απορρίπτονται. Δηλαδή, σε αντίθεση με το packet filtering που φιλτράρει πακέτο-πακέτο την κίνηση, το stateful packet filtering ελέγχει το σύνολο της σύνδεσης. Με άλλα λόγια, «θυμάται» συγκεκριμένα χαρακτηριστικά της κίνησης και τα αποθηκεύει. Διατηρεί, δηλαδή, την κατάσταση του firewall και της κίνησης. Επίσης έχει την ικανότητα να προσαρμόζει τη λειτουργία του, με βάση την κίνηση που καταγράφει. Ακόμη, αναγνωρίζει τις εφαρμογές και ξέρει ποιες επιπρόσθετες συνδέσεις θα χρειαστούν μεταξύ δυο πλευρών.

Με βάση τα παραπάνω, προτιμητέο είναι το stateful packet filtering, γιατί:

- Φιλτράρει με βάση και τα πακέτα, αλλά και με βάση τη σύνδεση.

- Λειτουργεί σε υψηλότερο OSI layer σε σχέση με τις δύο άλλες μεθόδους.
- Διατηρεί την κατάσταση της κίνησης και του συστήματος.

Λόγω της σπουδαιότητας της συγκεκριμένης μεθόδου, αλλά και της, εν γένει ευρείας χρήσης της, θα εμμείνουμε λίγο παραπάνω στον τρόπο λειτουργίας της, ξεκινώντας από τον πίνακα καταστάσεων.

Ο πίνακας καταστάσεων (state table) είναι σημαντικότατο μέρος της δομής που υλοποιεί το stateful packet filtering. Εκτός από αυτό, με επιπρόσθετο έλεγχο των πακέτων, μπορούν να ξεχωρίζουν και ποια εφαρμογή αφορούν. Επιθεωρώντας ένα session πιο ενδελεχώς, μπορούν να αναγνωρίζουν ροές δεδομένων που αποστέλλει μία εφαρμογή και να τις συνδυάζουν με την αρχική εγκαθίδρυση αυτού του session. Με τον όρο session εννοούμε τις συνόδους που σχετίζονται με το TCP και το UDP, αν και το firewall μπορεί να παρακολουθεί την κατάσταση και άλλων πρωτοκόλλων, όπως το ICMP ή το GRE.

Κατά κανόνα, ένα stateful packet filtering firewall δεν αλλάζει τις επικεφαλίδες των πακέτων. Απλά τις ελέγχει και τις συγκρίνει. Όμως, προαιρετικά, μπορεί να επιτελέσει αλλαγή των διευθύνσεων, για λόγους εφαρμογής NAT (Network Address Translation) ή PAT (Port Address Translation). Ωστόσο, θεωρείται ως άλλου είδους εργασία από το καθεαυτό φιλτράρισμα.

Το stateful packet filtering firewall, όπως είπαμε, χειρίζεται διαφορετικά τα διάφορα πρωτόκολλα. Πρωτόκολλα όπως το GRE, το IPSec, κ.α, χειρίζονται όπως θα χειρίζονταν και από ένα stateless packet filtering firewall, δηλαδή πακέτο-πακέτο. Έτσι, αν μία ροή δεδομένων για κάποιο πρωτόκολλο επιτραπεί αρχικά, τότε όλα τα πακέτα που ανήκουν σε αυτή τη ροή επιτρέπονται, μέχρι να περάσει ένα διάστημα αδράνειας.

Όσον αφορά την TCP κίνηση, τα πράγματα είναι λίγο πιο πολύπλοκα. Όταν ένα firewall επιτρέπει ένα TCP session, δημιουργεί μία καταχώρηση στον πίνακα κατάστασης. Κάθε επόμενο πακέτο ελέγχεται με βάση την κατάσταση στον πίνακα. Πιο συγκεκριμένα, ελέγχεται η πληροφορία του πακέτου που αφορά τη ροή της πληροφορίας και επιχειρείται να βρεθεί κάποια αντιστοίχιση σε κάποια εγγραφή του πίνακα κατάστασης. Συνηθέστερα, ελέγχονται τα TCP flags (SYN και ACK) για να επιβεβαιωθεί ότι έχει γίνει η κατάλληλη χειραψία. Αφού ολοκληρωθεί η μεταφορά των δεδομένων, η σύνδεση διακόπτεται και αφαιρείται η εγγραφή από τον πίνακα κατάστασης.

Η UDP κίνηση δεν περιέχει αρκετή πληροφορία ώστε να έχουμε εύρωστη παρακολούθηση ροών δεδομένων. Μόλις επιτραπεί η είσοδος σε μία ροή UDP,

προστίθεται μία εγγραφή στον πίνακα κατάστασης και ορίζεται ένας χρονοδιακόπτης αδράνειας. Αν δεν ανιχνευθεί κίνηση αυτής της ροής σε αυτό το διάστημα, η εγγραφή διαγράφεται από τον πίνακα κατάστασης.

Ακόμη, δυναμικές εφαρμογές, όπως το FTP, το SQLnet, voice και video εφαρμογές, και, εν γένει, οποιαδήποτε κίνηση που γίνεται μέσω συνήθων ports, μπορεί να ελεγχθούν από ένα stateful packet filtering firewall.

Τέλος, ένα firewall, ανεξαρτήτως είδους, οφείλει να παράγει ειδοποιήσεις και να καταχωρεί τα συμβάντα σε πραγματικό χρόνο. Τα μηνύματα αυτά πρέπει να παρέχουν αρκετές πληροφορίες, ώστε να είναι εφικτό στον διαχειριστή του firewall να δράσει άμεσα και αποτελεσματικά.

Η ρύθμιση ενός firewall περιλαμβάνει τα εξής βήματα:

1. Ορισμός εσωτερικής και εξωτερικής διεπαφής.
2. Ρύθμιση ACLs στις διεπαφές.
3. Καθορισμός κανόνων ελέγχου και παρακολούθησης.
4. Εφαρμογή των παραπάνω στις διεπαφές.
5. Έλεγχος και αξιολόγηση

5.5.2.2 Software Firewalls

Μέχρι τώρα σε αυτό το κεφάλαιο μιλούσαμε για firewalls συσκευές, που τοποθετούνται στα όρια του ιδιωτικού δικτύου του οργανισμού. Πρόκειται είτε για συσκευές που επιτελούν αποκλειστικά φιλτράρισμα των πακέτων, είτε για routers που αναλαμβάνουν, μεταξύ άλλων, και καθήκοντα ελέγχου της κίνησης.

Εκτός, όμως, από αυτά τα firewalls, υπάρχουν και άλλα, τα οποία αποτελούν κομμάτι του λειτουργικού συστήματος και υλοποιούνται στους τερματικούς σταθμούς. Δεν έχουν σκοπό να προστατέψουν όλον τον οργανισμό, αλλά μόνον τον υπολογιστή στον οποίον είναι εγκατεστημένα. Το scope τους, δηλαδή, είναι περιορισμένο στον υπολογιστή, σε αντίθεση με τα firewalls της προηγούμενης παραγράφου, που το scope τους αφορούσε τον οργανισμό στο σύνολό του.

Παρόλα αυτά, δεν θα πρέπει να αμφισβητηθεί η σημαντικότητά τους. Κι αυτό γιατί δεν είναι μόνο ότι αποτρέπουν εισερχόμενη κακόβουλη κίνηση. Είναι και μία από τις

τελευταίες γραμμές άμυνας του οργανισμού. Επίσης, τα firewalls δεν αποτρέπουν μόνο την εισερχόμενη κίνηση, αλλά και την εξερχόμενη. Έτσι, αφενός, προστατεύουμε τον μη εξειδικευμένο χρήστη από την έκθεση σε ένα επικίνδυνο περιβάλλον, όπως το Internet, και αφετέρου προστατεύουμε από πιθανή μόλυνση τους υπόλοιπους υπολογιστές του δικτύου, σε περίπτωση που κάποιο worm ή ιός μολύνει τον υπολογιστή. Τέλος, μειώνουμε την απόσπασή του από σελίδες ψυχαγωγίας ή κοινωνικών δικτύων.

Τα firewall στους τερματικούς σταθμούς είναι πιο κοντά στην ανθρώπινη λογική. Δηλαδή, υπάρχουν εφαρμογές που επιτρέπουμε η απαγορεύουμε, και όχι τόσο IP διευθύνσεις ή είδη κινήσεων. Έτσι, απαγορεύουμε ή επιτρέπουμε συγκεκριμένες εφαρμογές ή συγκεκριμένα ports, χωρίς αυτό να σημαίνει ότι δεν μπορούμε να ορίσουμε και πιο πολύπλοκους κανόνες. Ακόμη, μας δίνεται η δυνατότητα να χρησιμοποιήσουμε έτοιμα profiles και έτοιμους κανόνες και εμείς απλά να τους προσαρμόσουμε και να τους τελειοποιήσουμε με βάση τα δικά μας κριτήρια.

Το σημαντικότερο, όμως, στοιχείο είναι ότι μπορούμε να ασφαλίσουμε μαζικά τους υπολογιστές, αφού πρώτα τους έχουμε κατηγοριοποιήσει και ομαδοποιήσει. Αυτό το πετυχαίνουμε φτιάχνοντας ένα group policy, το οποίο να συνάδει με τις πολιτικές ασφαλείας του οργανισμού, και το οποίο να εφαρμόσουμε σε όλους ανεξαιρέτως τους υπολογιστές και τους servers του οργανισμού.

Τέλος, και εδώ δε θα πρέπει να παραλείψουμε την καταγραφή των συμβάντων και των περιστατικών ασφαλείας.

5.5.3 IPS-IDS

5.5.3.1 Γενικά

Το Σύστημα Ανίχνευσης Εισβολών (Intrusion Detection System – IDS) είναι ένα σύστημα που παρακολουθεί παθητικά τη δικτυακή κίνηση. Μπορεί να είναι είτε βασισμένη σε υλικό, είτε σε λογισμικό. Το IDS δε βρίσκεται στο μονοπάτι που περνάει η δικτυακή κίνηση, ωστόσο παρακολουθεί ανεξαιρέτως όλη αυτήν την κίνηση. Κανονικά, μόνο μία διεπαφή αρκεί για την παρακολούθηση όλης της κίνησης ενός δικτύου, αν και με την χρήση και άλλων διεπαφών μπορεί να επιτευχθεί η παρακολούθηση περισσοτέρων δικτύων. Όταν το IDS ανιχνεύσει ύποπτη δικτυακή κίνηση, στέλνει μία ειδοποίηση, γιατί

έχει περιορισμένες αποτρεπτικές δυνατότητες. Αν ρυθμιστεί κατάλληλα, μπορεί να μπλοκάρει αυτή την ύποπτη κίνηση, ρυθμίζοντας με τη σειρά του άλλες συσκευές, όπως routers. Όμως, μέρος της επικίνδυνης κίνησης έχει ήδη εισέλθει και μόνο η επόμενη κίνηση μπορεί να μπλοκαριστεί. Επίσης, το IDS έχει τη δυνατότητα να τερματίζει επικίνδυνες TCP συνδέσεις.

Το Σύστημα Αποτροπής Εισβολών (Intrusion Prevention System - IPS) είναι μια ενεργητική συσκευή, που τοποθετείται στο μονοπάτι που μεταφέρεται η δικτυακή κίνηση, παρακολουθώντας την κίνηση, και επιτρέπει η απορρίπτει ροές κινήσεων να εισέλθουν στο εσωτερικό δίκτυο. Όλη η κίνηση διέρχεται από το IPS για έλεγχο από μία διεπαφή και εξέρχεται από μία άλλη.

Όταν το IPS αντιληφθεί επικίνδυνη κίνηση, αφού στείλει ειδοποιήσεις, μπορεί να ρυθμιστεί, ώστε να απορρίπτει αμέσως τη συγκεκριμένη κίνηση. Έτσι, προλαβαίνει και αποτρέπει και την αρχική αλλά και την επικίνδυνη κίνηση που έπεται. Αυτό είναι πολύ σημαντικό χαρακτηριστικό του IPS, γιατί, μιας και οι μηχανισμοί επιθέσεων γίνονται όλο και πιο εξελιγμένοι, επιβάλλεται η προληπτική αντιμετώπιση και προστασία απέναντι σε ιούς, worms, κακόβουλο λογισμικό κτλ.

Συμπερασματικά, το IPS μπλοκάρει και απορρίπτει κάθε κίνηση που θεωρεί ύποπτη. Δεν θα πρέπει, όμως, να εμποδίζει την επιθυμητή κίνηση και για αυτό θα πρέπει να το ρυθμίζουμε σωστά, ώστε να αποφεύγουμε διακοπές στην επικοινωνία. Το IDS συμπληρώνει τις λειτουργίες του IPS, επιβεβαιώνοντας ότι το IPS βρίσκεται σε λειτουργία, ειδοποιώντας για την ανίχνευση ύποπτης κίνησης και να αναλαμβάνει τις “γκρίζες ζώνες”, δηλαδή κινήσεων που το IPS επέτρεψε να περάσουν, αλλά ενδεχομένως να αποτελούν κίνδυνο για το δίκτυό μας.

5.5.3.2 Τύποι IPS και IDS

Όταν εγκαθιστούμε μία υποδομή IPS και IDS στο δίκτυό μας, πρέπει να αποφασίσουμε για δύο πράγματα: αφενός τον τρόπο ανάπτυξης και αφετέρου τον τρόπο που το IPS και το IDS θα εντοπίζουν την ύποπτη κίνηση. Όσον αφορά τον τρόπο ανάπτυξης έχουμε δύο επιλογές: είτε Network-based, όπου παρακολουθούμε την κίνηση προς πολλούς hosts, είτε Host-based, όπου ένας agent παρακολουθεί όλες τις λειτουργίες ενός λειτουργικού συστήματος.

Στα Host-based IPS (εφεξής HIPS) το IPS ελέγχει την κίνηση σε κάθε ξεχωριστό τερματικό σταθμό ή host. Το HIPS έχει πλήρη πρόσβαση στις πληροφορίες ενός τερματικού σταθμού και μπορεί να συσχετίζει την εισερχόμενη κίνηση με τις εργασίες που επιτελούνται εκείνη την ώρα στον υπολογιστή, για να αναγνωρίζει το περιεχόμενο της κίνησης. Επίσης, αν έχουμε υλοποιήσει VPNs, ο μόνος τρόπος να εξετάσουμε την κίνηση σε μορφή απλού κειμένου είναι με HIPS. Παρόλα αυτά, το HIPS λειτουργεί με συγκεκριμένο λειτουργικό σύστημα και δε μπορεί να παράσχει προστασία στα επίπεδα 1 έως 3 του μοντέλου OSI. Επίσης, ο επίμονος επιτιθέμενος είναι σε θέση να καταλάβει την ύπαρξή του.

Στα Network-based IPS (εφεξής NIPS) το IPS ελέγχει μεμονωμένα πακέτα που κινούνται στο δίκτυο. Είναι σε θέση να εντοπίζει επικίνδυνα πακέτα, που δεν έχουν εντοπιστεί από το φιλτράρισμα του firewall. Το NIPS τοποθετείται μέσα στο δίκτυο και παρέχει επιβεβαίωση της όλης της δικτυακής κίνησης, ή, τουλάχιστον, των κρίσιμων περιοχών. Επίσης, προστατεύει από επιθέσεις χαμηλότερου επιπέδου, αλλά δεν μπορεί να ελέγξει κρυπτογραφημένη κίνηση, ούτε και επιθέσεις που εκτυλίσσονται στα εσωτερικά των hosts, αφού το απασχολεί το δίκτυο στο σύνολό του.

Εν κατακλείδι, τα δύο συστήματα έχουν φτιαχτεί για να συμπληρώνει το ένα το άλλο. Το NIPS εστιάζει στον εντοπισμό υπερχείλισης buffers, επιθέσεις σε web servers, εξερευνητικές επιθέσεις και DoS επιθέσεις. Από την άλλη, το HIPS εστιάζει στην ασφάλεια εφαρμογών και πόρων συστήματος των hosts.

Ας εξετάσουμε τώρα τους τρόπους με τους οποίους τα IPS και IDS εντοπίζουν την ύποπτη.

5.5.3.3 Τρόποι Ανίχνευσης Επικίνδυνης Κίνησης

Συνολικά, τα IPS και IDS μας παρέχουν τέσσερις τρόπους για να ανιχνεύουμε ύποπτη και/ή επικίνδυνη κίνηση : Signature-based, Policy-based, Anomaly-based και Honeypot-based.

Τα signature-based IPS και IDS λειτουργούν ψάχνοντας προκαθορισμένο περιεχόμενο ή σταθερές ακολουθίες σε ένα πακέτο και το συγκρίνει με ήδη υπάρχουσες ακολουθίες, τα signature patterns, τα οποία είναι επικίνδυνα. Στις περισσότερες των περιπτώσεων, έχουμε ταύτιση μόνο αν το ύποπτο πακέτο σχετίζεται με κάποιο συγκεκριμένο service ή με κάποιο συγκεκριμένο port. Κατ' αυτόν τον τρόπο μειώνουμε σημαντικά τον έλεγχο που

κάνουμε σε κάθε πακέτο, αλλά αντιμετωπίζουμε δυσκολίες με κίνηση σε ports τα οποία δεν είναι από τα γνωστά. Αρχικά, ίσως στέλνονται πολλές ειδοποιήσεις, που οι πιο πολλές από αυτές δε θα ενέχουν κίνδυνο, μέχρις ότου να ρυθμιστεί το σύστημα στις απαιτήσεις και τις ιδιαιτερότητες του δικτύου μας.

Όπως καταλαβαίνουμε, τα signature-based IPS και IDS ανιχνεύουν επιθέσεις που έχουν εισαχθεί σε μία βάση δεδομένων και άρα δεν μπορούν να αντιμετωπίσουν καινούρια είδη επιθέσεων. Η ενημέρωση των βάσεων δεδομένων με τις επιθέσεις, γίνεται είτε με έκδοση updates από τον κατασκευαστή, είτε από τον ίδιο το διαχειριστή.

Τα policy-based IPS και IDS χρησιμοποιούν έναν αλγόριθμο για να εντοπίζουν τις επιθέσεις και απαιτείται η ύπαρξη μίας βάσεως δεδομένων με πολιτικές. Σε περίπτωση που συμβεί κάποια παραβίαση πολιτικής, τότε ή στέλνει ειδοποιήσεις ή μπλοκάρει την κίνηση. Οι πολιτικές αυτές μπορούν να είναι ένα σύνολο από permissions που περιέχουν ποια δίκτυα μπορούν να επικοινωνούν με ποια και με τη χρήση ποιων πρωτοκόλλων.

Τα anomaly-based IPS και IDS ψάχνουν για δικτυακή κίνηση η οποία παρεκκλίνει από την κίνηση που θεωρείται “κανονική”. Το πρόβλημα εδώ είναι τι θεωρούμε ως κανονική κίνηση. Μερικά συστήματα έχουν εκ κατασκευής ενσωματωμένα “κανονικά” μοντέλα κίνησης. Άλλα συστήματα είναι σχεδιασμένα να μαθαίνουν από μόνα τους τι είναι “κανονική” κίνηση, αλλά εδώ παρουσιάζεται το πρόβλημα ενδεχόμενης λάθος αξιολόγησης. Συνεπώς, είναι απλό να εγκαταστήσουμε τέτοιου είδους συστήματα σε μικρά περιβάλλοντα, αλλά δύσκολο έως αδύνατο σε μεγάλα.

Η διάγνωση για την ύπαρξη ανωμαλιών στην κίνηση μπορεί να γίνει είτε στατιστικά, είτε μη στατιστικά. Τα στατιστικά συστήματα παρακολουθούν το δίκτυο για κάποια περίοδο και με βάση αυτή την παρατήρηση μπορούν να αποφανθούν αν είχαμε παρέκκλιση από την κανονική λειτουργία. Τα μη στατιστικά συστήματα έχουν προκαθορισμένο ορισμό του τι είναι “κανονική” κίνηση (συνήθως εκ κατασκευής) και με βάση αυτό γίνεται η σύγκριση.

Τέλος, τα honeypot-based IPS και IDS προσφέρουν στον επιτιθέμενο έναν dummy server για να προσελκύει τις επιθέσεις. Η φιλοσοφία που διέπει αυτό το είδος συστημάτων είναι η απόσπαση του επιτιθέμενου από τον πραγματικό στόχο. Προσφέρει τη δυνατότητα ανάλυσης των επιθέσεων και έτσι τα συστήματά μας “εκπαιδεύονται” σε αυτού του είδους τις επιθέσεις. Η προσέλκυση του επιτιθέμενου γίνεται με τη ρύθμισή τους ως λιγότερο ασφαλή ή με περισσότερες ευπάθειες. Εναλλακτικά, μπορούμε να τα κάνουμε πολύ ενδιαφέροντα, αλλά με πολύ καλή άμυνα, ώστε ο επιτιθέμενος να χρειαστεί να αφιερώσει χρόνο και έτσι να δοθεί σε μας το χρονικό περιθώριο για να αντιδράσουμε.

5.5.3.4 Υπογραφές

Μία υπογραφή (signature) ανιχνεύει επαναλαμβανόμενες ακολουθίες (patterns) που θα πρέπει να δημιουργήσουν μία ειδοποίηση ή να οδηγήσει στην απόρριψη των πακέτων. Ο μηχανισμός του IPS που ταιριάζει τις υπογραφές με τα δεδομένα των πακέτων ονομάζεται μικρομηχανή (microengine). Ένα IPS περιέχει πολλές microengines και κάθε microengine χειρίζεται ένα σύνολο υπογραφών, οργανωμένες με βάση κοινά χαρακτηριστικά.

Υπάρχουν τέσσερα είδη υπογραφών:

- **Exploit signatures:** Αναγνωρίζουν κινήσεις που αφορούν ένα συγκεκριμένο και μοναδικό κενό ασφαλείας.
- **Connection signatures:** Ενεργοποιούνται σε περιπτώσεις που ανιχνευθούν ύποπτες συνδέσεις.
- **String signatures:** Υποστηρίζουν ταίριασμα με συγκεκριμένες εκφράσεις
- **DoS signatures:** Περιλαμβάνουν περιγραφές συμπεριφοράς χαρακτηριστικές των DoS.

Όσον αφορά τα exploit signatures, αυτά αντιστοιχούν τις επιθέσεις σε κάποιο επίπεδο του OSI layer. Για παράδειγμα, στο Application layer έχουμε DoS, worms, ιούς, Δούρειους Ίππους κ.α. Στο Transport layer έχουμε port sweeps, port scans κτλ.

Όταν περνάει ύποπτη κίνηση μέσα από τον αισθητήρα του IPS ή του IDS, εκείνο πρέπει να αποφασίσει ποια microengine θα το αναλάβει. Αυτό καθορίζεται με βάση το δικτυακό πρωτόκολλο, τον τύπο του λειτουργικού συστήματος, το port ή το είδος της επίθεσης.

5.5.4 ACLs

Σε πολλά σημεία αναφερθήκαμε στη χρήση των ACLs. Χρησιμοποιήσαμε ACLs στην εγκατάσταση του IPSec για να καθορίσουμε την ενδιαφέρουσα κίνηση. Χρησιμοποιήσαμε ACLs στα firewalls ως κανόνες. Γενικά, σε έναν router οι ACLs είναι το πλέον χρησιμοποιούμενο εργαλείο, γιατί έχει πάμπολλες χρήσεις και γιατί είναι ένας πολύ αποδοτικός τρόπος να μεταφέρουμε στο router ποια κίνηση επιθυμούμε να επεξεργαστούμε. Σε αυτή την παράγραφο δεν θα ασχοληθούμε γενικά με τις ACLs, αλλά

θα δούμε γιατί αποτελούν ένα από τα χρησιμότερα εργαλεία στην επιβολή οποιασδήποτε μορφής ασφάλειας.

Όταν πρέπει να αποφασίσουμε για το πώς θα χειριστούμε τα services, τα ports και τα πρωτόκολλα του router, με γνώμονα την ασφάλεια, θα πρέπει να έχουμε κατά νου δύο πράγματα: την απενεργοποίηση όλων των μη χρησιμοποιούμενων και τον περιορισμό της πρόσβασης στα services, στα ports και στα πρωτόκολλα. Κι εδώ έγκειται η σημαντικότητα των ACLs, γιατί λειτουργούν ως φίλτρα ανάμεσα στο εταιρικό δίκτυο και στο Internet, ενώ είναι από τα κύρια μέσα επιβολής της πολιτικής ασφαλείας του οργανισμού.

Παρόλη τη χρησιμότητα και τη χρηστικότητα των ACLs, καλό θα είναι κάποιες στιγμές να κοιτάμε και την ελάττωση του διαχειριστικού βάρους. Έτσι, αν επιθυμούμε να μην υπάρχει καμία πρόσβαση στο Service, μπορούμε αντί να αποκόπτουμε την πρόσβαση στο service με ACLS, να απενεργοποιούμε τελείως το ίδιο το service. Αν επιθυμούμε, όμως, μερική ή περιορισμένη πρόσβαση, η μόνη λύση είναι η χρήση ACLs.

Πέρα, λοιπόν, από την προστασία services, ports και πρωτοκόλλων, οι ACLs μας χρησιμεύουν στον να αντιμετωπίζουμε πολλούς κινδύνους, όπως:

- Spoofing IP διευθύνσεων και προς τις δύο κατευθύνσεις
- DoS TCP SYN επιθέσεις
- DoS Smurf επιθέσεις
- DDoS επιθέσεις
- Reconnaissance επιθέσεις με χρήση ICMP και προς τις δύο κατευθύνσεις
- Φιλτράρισμα του εργαλείου traceroute.

Το να γράψουμε μία ACL είναι πολύ εύκολο. Απλά ορίζουμε ποια κίνηση/πρωτόκολλο αφορά η ACL και ορίζουμε διευθύνσεις πηγής και προορισμού συν κάποιες άλλες προαιρετικές λεπτομέρειες. Το δύσκολο, ωστόσο, είναι να τις γράψουμε με τέτοιο τρόπο και να τις τοποθετήσουμε σε εκείνο το σημείο, ώστε να εξυπηρετούν τις ανάγκες μας και τις πολιτικές ασφαλείας μας, χωρίς να εμποδίζουν τη θεμιτή κίνηση.

Στο σχεδιασμό των ACLs πρέπει να λάβουμε πολλά πράγματα υπ’ όψιν, που αν δε το κάνουμε, ενδέχεται να δημιουργηθούν προβλήματα στη λειτουργία του δικτύου μας.

Κατ αρχήν, κάθε ACL, στο τέλος της περιέχει ένα implicit deny, δηλαδή αφού επιτραπούν ή αποτραπούν τα πακέτα με τους κανόνες που ορίσαμε στην ACL, ότι δεν αναφέρθηκε

ρητά, απλά απορρίπτεται. Αυτό το “deny all” δεν φαίνεται πουθενά, αλλά υφίσταται εξ ορισμού σε κάθε ACL.

Η εκτέλεση των ACLs είναι ακολουθιακή. Δηλαδή εκτελείται πρώτα η πρώτη εντολή της και ούτω καθεξής. Συνεπώς, η θέση στην ACL που βρίσκεται κάποια εντολή είναι ιδιαίτερα σημαντική. Για αυτό, πάντα τοποθετούμε τις πιο συγκεκριμένες ACL ψηλά, ώστε να εκτελεστούν πριν πιο γενικές ACLs, γιατί αν βάλουμε μία πολύ συγκεκριμένη ACL που αφορά έναν host μετά από μία ACL που αφορά το δίκτυο που βρίσκεται ο host, η συγκεκριμένη ACL που αφορά τον host δε θα εκτελεστεί ποτέ.

Επίσης, πολύ σημαντική παράμετρος στον ορισμό μιας ACL είναι η κατευθυντικότητα του φιλτραρίσματος, δηλαδή αν ο κανόνας θα εφαρμόζεται στα πακέτα που φτάνουν ή στα πακέτα που φεύγουν. Τέλος, πρέπει να είμαστε πολύ προσεκτικοί στο να μη φιλτράρεται σημαντική κίνηση.

Παρακάτω, παραθέτουμε ένα παράδειγμα για αποφυγή ενός κινδύνου που αναφέραμε παραπάνω, με τη χρήση ACL, όπου θα εξηγήσουμε και τη σύνταξη της αλλά και τη λειτουργία της.

Πίνακας 5.7: Χρήση ACL

```
1.  R1(config)#access-list 101 permit ip 10.2.1.0 0.0.0.255 any
2.  R1(config)#access-list 101 deny ip any any log
3.  R1(config)#int fa0/0
4.  R1(config-if)#ip access-group 101 in
```

Με την παραπάνω σειρά εντολών εξαλείφουμε το πρόβλημα του IP spoofing εσωτερικών IP διευθύνσεων.

1. Ορίζουμε την ACL 101. Αυτή επιτρέπει όλη την κίνηση που προέρχεται από το εσωτερικό μας δίκτυο, το 10.2.1.0. Το 0.0.0.255 είναι η wildcard mask και υποδηλώνει ότι επιθυμούμε όλες τις IP διευθύνσεις (0-255) του υποδικτύου που προηγείται. Με άλλα λόγια, θα επιτρέπεται οποιοιδήποτε IP κίνηση, των hosts 10.2.1.0-10.2.1.255 προς οποιοδήποτε προορισμό. Το “προς οποιοδήποτε προορισμό” δηλώνεται από το “any”.
2. Απορρίπτουμε οποιαδήποτε IP κίνηση, πλην της προαναφερθείσας

3. Πηγαίνουμε στο interface που συνδέεται στο δίκτυο 10.2.1.0 και
4. Εφαρμόζουμε την ACL στην εισερχόμενη κίνηση.

5.5.5 NAP

Ας επεξεργαστούμε το ακόλουθο σενάριο: στην παρούσα χρονική περίοδο, ένα worm έχει κατακλύσει το Internet. Ο οργανισμός μας έχει πάρει όλα τα απαραίτητα μέτρα ασφαλείας στην περίμετρο του δικτύου μας. Ένας κινούμενος εργαζόμενος, με laptop, βρισκόμενος σε εξωτερική δουλειά, κολλάει το worm. Την επόμενη μέρα επιστρέφει στην εταιρεία. Ανοίγει τον υπολογιστή του και σε μερικές ώρες έχει μολύνει εκατοντάδες υπολογιστές του οργανισμού μας. Πώς θα μπορούσε να αποφευχθεί αυτό; Θα μπορούσε να αποφευχθεί με τη χρήση της Προστασίας Πρόσβασης Δικτύου (Network Access Protection – NAP) , το οποίο είναι ένα πρόσθετο χαρακτηριστικό στον Windows Server 2008.

Η συλλογιστική του είναι απλή: όταν ένας υπολογιστής συνδέεται στο εσωτερικό μας δίκτυο θα πρέπει να πληροί συγκεκριμένα κριτήρια ασφαλείας και υγείας, όπως ενημερωμένο antivirus, όλα τα πρόσφατα updates κτλ. Αν δεν τα διαθέτει αυτά, τότε θα μεταφερθεί σε ένα άλλο υποδίκτυό μας, όπου και θα τοποθετηθεί σε καραντίνα και όπου θα μπορεί να προβεί σε όλες τις απαραίτητες ενέργειες, ώστε να είναι ασφαλής η είσοδός του στο δίκτυο.

Πιο συγκεκριμένα, πέρα από το ιδιωτικό μας δίκτυο, δημιουργούμε ένα δίκτυο για τους επισκέπτες (guest network) και ένα δίκτυο εξυγίανσης (remediation network). Έτσι, αν θέλουμε να εξυγιαίνουμε τους υπολογιστές, και ιδιαίτερα τα laptops, θα πρέπει να διαθέσουμε επιπλέον εξοπλισμό, ειδικό για αυτά, όπως DHCP server, Active Directory Server, WSUS server για τα updates κτλ.

Οι τρόποι που επιβάλλεται το NAP ποικίλλουν:

- **IPSec Connection Security:** Αυτός ο τρόπος επιβολής, απαιτεί από τον client να εκτελέσουν ένα check-up, ώστε να αποκτήσουν ένα πιστοποιητικό που δηλώνει ότι είναι υγιείς. Χωρίς αυτό το πιστοποιητικό, ο client δεν μπορεί να συνδεθεί με hosts που προστατεύονται από το IPSec.
- **802.1x Access Points:** Η μέθοδος επιβολής περιλαμβάνει τη χρήση switches και/ή ασύρματων access points, που υποστηρίζουν αυθεντικοποίηση με 802.1x.

Αν κάποιος client αυθεντικοποιηθεί με 802.1x και διαπιστωθεί ότι είναι υγιής, του δίνεται η ανάλογη πρόσβαση.

- **VPN Server:** Αν έχουμε υλοποιήσει έναν VPN server, που θα συγκεντρώνει και θα εξυπηρετεί όλα τα VPNs που εγκαθιδρύονται, μπορούμε μέσω αυτού να επιβάλουμε τις πολιτικές ασφαλείας που υπαγορεύει το NAP. Επίσης, μας δίδεται η δυνατότητα να περιορίσουμε τις προσβάσεις του client, στις απολύτως απαραίτητες, δηλαδή μόνο στο δίκτυο εξυγίανσης.
- **DHCP Server:** Μπορούμε έμμεσα να επιβάλλουμε το NAP μέσω του DHCP server, δίνοντας σε clients πλήρη πρόσβαση μόνον εάν πληρούν τις προϋποθέσεις. Διαφορετικά, τους δίνεται μία IP, με subnet mask 255.255.255.255 και καθόλου default gateway. Εναλλακτικά, μπορούμε να δώσουμε τέτοιο default gateway που να κατευθύνει τον client στην περιοχή εξυγίανσης.

Δύο βασικές έννοιες, όσον αφορά το NAP, είναι οι SHA και οι SHV. Οι Διαχειριστές Υγείας Συστήματος (System Health Agents - SHA) είναι τα client συστατικά του NAP και περιλαμβάνονται στα λειτουργικά συστήματα Windows XP SP 3 και μετά και περιέχουν μία πλήρη περιγραφή της κατάστασης υγείας του υπολογιστή. Επίσης, είναι εφικτό να δημιουργήσουμε και τα δικά μας SHAs. Οι Επικυρωτές Υγείας Συστήματος (System Health Valdiators – SHV) είναι τα server συστατικά του NAP και αναλύουν τα δεδομένα που τους στέλνονται από του SHAs. Με βάση αυτό καθορίζεται το επίπεδο προσβάσεων του client.

5.5.6 Antivirus

5.5.6.1Antivirus Προσωπικού Υπολογιστή

Ένα antivirus πρόγραμμα χρησιμοποιείται για να εκτελεί ελέγχους των αρχείων του υπολογιστή, να ανιχνεύει και να εξαλείφει ιούς και άλλο κακόβουλο λογισμικό. Για να το πετύχει αυτό χρησιμοποιεί δύο τεχνικές: πρώτον, διαθέτοντας μία λίστα με όλους τους γνωστούς ιούς (virus dictionary), ψάχνει τα αρχεία σε έναν υπολογιστή προσπαθώντας να τους εντοπίσει, αν υπάρχουν και, δεύτερον, ανιχνεύοντας ύποπτη συμπεριφορά από κάποιο πρόγραμμα, το οποίο μπορεί να υποδηλώνει την ύπαρξη κακόβουλου λογισμικού.

Στην πρώτη περίπτωση, το antivirus πρόγραμμα, όταν εκτελεί τον έλεγχο ενός αρχείου, αναφέρεται σε μία λίστα με όλους τους γνωστούς ιούς. Αν αναγνωρίσει ως μέρος του προγράμματος ύποπτο κώδικα, τότε έχει τρεις επιλογές: ή να το διαγράψει ή να το βάλει σε καραντίνα, καθιστώντας το μη προσβάσιμο, ή να επιχειρήσει να επιδιορθώσει τη βλάβη, εξαλείφοντας τον ιό. Ο έλεγχος αυτός γίνεται στο άνοιγμα και στο κλείσιμο του αρχείου, πριν και μετά την αποστολή του με e-mail ή σε τακτά, προγραμματισμένα διαστήματα. Είναι εύκολα κατανοητό, ότι για να είναι αποδοτική αυτή η προσέγγιση θα πρέπει η λίστα να εμπλουτίζεται συνεχώς. Παρόλο που η παραπάνω μέθοδος θεωρείται αρκετά αποτελεσματική, οι δημιουργοί των ιών καταφεύγουν στη δημιουργία πολυμορφικών ιών, η οποίοι κρυπτογραφούν δεδομένα τους ή τα αλλάζουν κατά τέτοιο τρόπο που να περνάν απαρατήρητα.

Με τη δεύτερη τεχνική, δεν έχουμε σκοπό να εντοπίσουμε κάποιον γνωστό ιό, καθώς το παραπάνω πρόβλημα θα έχει επιλυθεί με την προηγούμενη διαδικασία. Αντίθετα, παρακολουθείται η εκτέλεση των προγραμμάτων για ύποπτη δραστηριότητα, όπως προσπάθεια εγγραφής δεδομένων σε κάποιο εκτελούμενο πρόγραμμα. Τότε, ή το antivirus δρα αυτοβούλως ή ενημερώνεται ο χρήστης και του ζητείται να αποφασίσει επ' αυτού. Ωστόσο, θα πρέπει να υπάρχει ισορροπία, ώστε ο χρήστης να μην κατακλύζεται από ειδοποιήσεις και, έτσι, να παύει να δίνει την δέουσα προσοχή σε αυτά τα warnings.

Σε ορισμένες περιπτώσεις, χρησιμοποιείται και η τεχνική του sandbox. Ένα sandbox προσομοιώνει το λειτουργικό σύστημα και εκτελεί το ύποπτο πρόγραμμα μέσα του. Αφού ολοκληρωθεί η εκτέλεση του προγράμματος, αναλύονται τα χαρακτηριστικά της εκτέλεσής του για τον εντοπισμό ύποπτης δραστηριότητας. Εν γένει η μέθοδος αυτή αποφεύγεται λόγω χρησιμοποίησης πολλών πόρων.

5.5.6.2 Antivirus Υποδομή Οργανισμού

Μέχρι τώρα αναλύσαμε πώς δουλεύει ένα antivirus πρόγραμμα σε έναν απλό, αυτόνομο υπολογιστή. Πώς, όμως θα αναπτύξουμε μία antivirus υποδομή που θα καλύπτει όλον τον οργανισμό; Ποιες είναι οι βέλτιστες πρακτικές και τι πρέπει να έχουμε κατά νου;

Κατ αρχήν ένα σύγχρονο antivirus πρόγραμμα δεν περιορίζεται απλά στο να εντοπίζει ιούς. Οι περισσότεροι κατασκευαστές προτείνουν ολοκληρωμένες λύσεις στις οποίες, πέρα από τα αυτονόητα, περιέχονται και λύσεις αντιμετώπισης hackers και απώλειας δεδομένων, αλλά και έλεγχο της πρόσβασης.

Μία καλή πρακτική είναι να έχουμε μία antivirus σουίτα που θα επιτελεί όλα τα παραπάνω. Τα σημερινά μεγέθη των επιχειρήσεων, το εύρος των επιθέσεων, το πλήθος των προγραμμάτων, η ταχύτητα ανάπτυξης νέων μεθόδων επίθεσης και άμυνας, καθιστά πολύ δύσκολη τη διατήρηση και διαχείριση πολλών εξειδικευμένων εργαλείων, ένα για κάθε κατηγορία κινδύνων, χωρίς να ξεχνάμε βέβαια και το επιπλέον κόστος.

Επίσης, η σουίτα που χρησιμοποιούμε θα πρέπει να μην επιφέρει προβλήματα στην απόδοση των υπολογιστών. Οι σύγχρονες σουίτες, πέρα από την βέλτιστη αξιοποίηση των πόρων, προσφέρουν και επιλογές στο διαχειριστή του προγράμματος, που τον βοηθάνε να προσαρμόσει στις δικές του ανάγκες και στο δικό του επίπεδο εξοπλισμού το antivirus πρόγραμμα. Ακόμη, θα πρέπει να είναι εύκολα διαχειρίσιμο και οι αναφορές που δημιουργεί να είναι ακριβείς, αναλυτικές και ευανάγνωστες.

Μία ακόμη νέα τάση τον τελευταίο καιρό, που θα πρέπει να ενσωματώνεται στην υποδομή μας είναι η χρησιμοποίηση του ελέγχου των εφαρμογών (application control) ή, αλλιώς, white-listing. Το white-listing είναι μία μέθοδος στην οποία οι διαχειριστές διατηρούν μία λίστα με όλες τις επιτρεπόμενες εφαρμογές για το περιβάλλον του, απαγορεύοντας την εκτέλεση κάθε άλλης εφαρμογής. Το white-listing αποτελεί σημαντική εξέλιξη, καθώς μέχρι τώρα τα antivirus προγράμματα λειτουργούσαν με τη λογική του black-listing, δηλαδή προσπαθούσαμε να κόψουμε κάθε τι επικίνδυνο. Η πληθώρα, όμως των κινδύνων, και το εύρος των σύγχρονων εφαρμογών, μας οδήγησαν στην υιοθέτηση του white-listing.

Επιπροσθέτως, πρέπει να έχουμε υπόψη ότι καμία μηχανή ελέγχου και ανίχνευσης δεν είναι τέλεια. Για αυτό το λόγο, χρησιμοποιούνται πολλές μηχανές ανίχνευσης ταυτόχρονα, ώστε να αυξάνονται οι πιθανότητες εντοπισμού των κινδύνων. Ακόμη, σύμφωνα με έρευνες, όταν ένα antivirus πρόγραμμα έρθει αντιμέτωπο με έναν πρωτόγνωρο κίνδυνο, κατά 50% θα αποτύχει να τον αντιμετωπίσει. Για αυτό το λόγο, θα πρέπει να είμαστε εκ των προτέρων προετοιμασμένοι, απαγορεύοντας εγγραφές στη registry, στο root ή στο φάκελο συστήματος, μιας και η πλειοψηφία των επιθέσεων επιχειρεί ακριβώς αυτό.

Ακόμη, το ότι εντοπίστηκε ένας ιός, δε σημαίνει και ότι αντιμετωπίστηκε. Για παράδειγμα, υπάρχουν ιοί και γενικότερα malware που καθιστούν το αρχείο συνεχώς ανοιχτό, και άρα αδύνατο να διαγραφεί. Παλαιότερα, θα έπρεπε να μπούμε στο safe-mode του λειτουργικού συστήματος, για να εξαλείψουμε τον κίνδυνο. Πλέον, με τα εξελιγμένα εργαλεία που διαθέτουμε, δεν χρειάζεται να το κάνουμε αυτό.

Τελευταίο, αλλά όχι και λιγότερο σημαντικό, είναι το κόστος απόκτησης της σουίτας αλλά και των αδειών για κάθε τερματικό ξεχωριστά. Για να μειώσουμε το κόστος, χωρίς να

έχουμε επιπτώσεις στην ασφάλεια, θα πρέπει να καταφύγουμε σε μία ολοκληρωμένη λύση που θα μας καλύπτει σε όσο το δυνατόν περισσότερους τομείς.

5.5.7 EFS-Bitlocker

Σε αυτήν την παράγραφο θα αναφερθούμε σε δύο εργαλεία κρυπτογράφησης αρχείων που χρησιμοποιεί το λειτουργικό σύστημα των Windows. Το εργαλείο EFS, το οποίο χρησιμοποιείται για την κρυπτογράφηση αρχείων και το εργαλείο Bitlocker που χρησιμοποιείται για την κρυπτογράφηση ολόκληρων δίσκων. Τα εργαλεία αυτά μπορούν να δουλέψουν είτε αυτόνομα, είτε σε συνδυασμό.

5.5.7.1 Encrypting File System

Το EFS είναι συστατικό του συστήματος αρχείων NTFS και επιτρέπει διάφανη στο χρήστη κρυπτογράφηση και αποκρυπτογράφηση αρχείων, χρησιμοποιώντας εξελιγμένους αλγορίθμους. Χρησιμοποιεί συμμετρική κρυπτογραφία για να κρυπτογραφήσει τα αρχεία και ασύμμετρη κρυπτογραφία για να προστατευτεί το κλειδί κρυπτογράφησης.

Το EFS εκτελείται σε χαμηλό επίπεδο και για αυτό το λόγο η λειτουργία του είναι ανεπαίσθητη στο χρήστη. Αν ένας φάκελος επιλεχθεί να κρυπτογραφηθεί, τότε κάθε αρχείο μέσα του και κάθε αρχείο που θα μετακινηθεί σε αυτόν, θα είναι κρυπτογραφημένο. Οι εφαρμογές δε χρειάζεται να έχουν γνώση του EFS. Άλλωστε, με το EFS προστατεύουμε τα αρχεία μας από μη εξουσιοδοτημένους χρήστες, οι οποίοι αν επιχειρήσουν να ανοίξουν ένα τέτοιο αρχείο θα τους αρνηθεί η πρόσβαση.

Όπως είπαμε, το συμμετρικό κλειδί κρυπτογράφησης κρυπτογραφείται με τη σειρά του με το δημόσιο κλειδί ενός ζεύγους κλειδιών ασύμμετρης κρυπτογραφίας. Το ζεύγος ιδιωτικού και δημοσίου κλειδιού συνδέονται άμεσα με το χρήστη. Αν το ιδιωτικό κλειδί χαθεί ή καταστραφεί, τότε η μόνη περίπτωση να αποκτήσουμε ξανά πρόσβαση στα αρχεία μας είναι με τη χρήση κάποιο recovery agent. Ακόμη, τα κλειδιά μπορούν να αποθηκευτούν σε κάποιο άλλο φορητό, αποθηκευτικό μέσο και να ασφαλιστούν, για την περίπτωση που προκύψει ανυπέρβλητο πρόβλημα.

Τα κλειδιά του EFS προστατεύονται από το password του χρήστη. Αν κάποιος υποκλέψει το password μας, τότε συνδεόμενος θα μπορεί να αποκτήσει πρόσβαση στα αρχεία μας. Συνεπώς, απαιτούνται ισχυρά passwords και σωστή ενημέρωση και εκπαίδευση των χρηστών.

Μια επιπλέον σημαντική παράμετρος είναι ότι κρυπτογραφημένα αρχεία, όταν μεταφέρονται, μεταφέρονται σε μορφή απλού κειμένου, ακόμα και αν αποθηκεύονται σε κάποιον κρυπτογραφημένο φάκελο. Η κρυπτογράφηση θα γίνει κατά αφού ολοκληρωθεί η μεταφορά τους.

Πέραν όλων των άλλων, ο οργανισμός μας θα πρέπει να διαθέτει και μία πολιτική ανάκτησης κρυπτογραφημένων αρχείων. Τι γίνεται, για παράδειγμα, σε περίπτωση απώλειας ή καταστροφής του ιδιωτικού κλειδιού; Το EFS προσφέρει και ανάκτηση δεδομένων σε περίπτωση απώλειας κλειδιού και ανάκτηση κλειδιού. Η πρώτη περίπτωση λύνεται εύκολα. Μέσω του recovery agent certificate, με το οποίο είναι συνδεδεμένος ο χρήστης, επιτυγχάνεται αποκρυπτογράφηση του αρχείου, το οποίο στη συνέχεια αποστέλλεται στο χρήστη. Για να μπορούμε να προχωρήσουμε και σε ανάκτηση κλειδιών κρυπτογράφησης, θα πρέπει να έχουμε υλοποιήσει στον οργανισμό μας και έναν επιπλέον ρόλο του Windows Server, αυτόν των Certificate Services.

5.5.7.2 Bitlocker

Το Bitlocker είναι ένα εργαλείο κρυπτογράφησης συστημικών δίσκων στο λειτουργικό σύστημα των Windows. Χρησιμοποιεί τον αλγόριθμο κρυπτογράφησης AES με κλειδί μήκους 128 Bits. Με το Bitlocker εξασφαλίζεται και η ακεραιότητα των περιοχών από τις οποίες ξεκινάει ο υπολογιστής (boot sector, BIOS, κτλ) και κατ’ αυτόν τον τρόπο διασφαλίζουμε ότι δε θα κινδυνεύσουμε από τέτοιου είδους επιθέσεις.

Το μόνο που έχουμε να κάνουμε για να ενεργοποιήσουμε την κρυπτογράφηση ενός δίσκου, είναι απλά να ενεργοποιήσουμε το Bitlocker. Αυτό, βέβαια, μόνο αν έχουμε κάποια περιοχή στον υπολογιστή αρκετά ασφαλή, για να αποθηκεύσουμε το κλειδί κρυπτογράφησης. Αυτή η περιοχή ονομάζεται Εμπιστεύσιμη Πλατφόρμα (Trusted Platform Module - TPM). Χρησιμοποιώντας TPM έχουμε το πλεονέκτημα ότι η όλη διαδικασία είναι τελείως διαφανής στο χρήστη. Διαφορετικά θα πρέπει να αποθηκεύσουμε το κλειδί σε κάποιο USB stick και κάθε φορά που θέλουμε να ανοίξουμε τον υπολογιστή θα πρέπει να το εισάγουμε στην αντίστοιχη θύρα. Μία τρίτη μέθοδος είναι

με τη χρήση PIN που ζητείται στο χρήστη πριν την εκκίνηση του λειτουργικού, ωστόσο αυτή η μέθοδος είναι ευάλωτη σε επιθέσεις.

Το Bitlocker χρησιμοποιεί τον αλγόριθμο κρυπτογράφησης AES με κλειδί μήκους 128 Bits και κρυπτογραφεί ολόκληρους δίσκους ή ολόκληρα διαμερίσματα δίσκων (partitions). Ο χρόνος που απαιτείται για την κρυπτογράφηση είναι αρκετά μεγάλος. Ενδεικτικά, ένας υπολογιστής με διπύρηνο επεξεργαστή θα χρειαστεί περίπου 12 ώρες για να κρυπτογραφήσει έναν δίσκο 500 GB, κάτι πολύ λογικό, μιας και κάθε κομμάτι του δίσκου πρέπει να διαβαστεί, να κρυπτογραφηθεί και να γραφτεί στο δίσκο. Ωστόσο, η διαδικασία κρυπτογράφησης γίνεται στο background.

Πέρα από τα προφανή πλεονεκτήματα ασφαλείας που προσφέρει, το Bitlocker έχει ακόμα δύο, σε σχέση με άλλες μεθόδους κρυπτογράφησης δίσκων, ειδικά για την περίπτωσή μας, που θέλουμε να το εφαρμόσουμε κατά βούληση σε συγκεκριμένους υπολογιστές του οργανισμού. Το πρώτο είναι ότι τα κλειδιά κρυπτογράφησης αποθηκεύονται στο Active Directory και το δεύτερο ότι μπορεί να εφαρμοστεί ως κομμάτι κάποιας Group Policy.

5.6 Certification Authorities

Στην πρώτη παράγραφο του κεφαλαίου αυτού θα αναλύσουμε και θα εξηγήσουμε τι είναι και πώς υλοποιείται μία υποδομή δημοσίου κλειδιού στο Internet και στο δεύτερο μέρος του κεφαλαίου θα παρουσιάσουμε πώς μπορούμε να υιοθετήσουμε αυτό το μοντέλο πιστοποιήσεων και στον οργανισμό μας. Σε μία υποδομή δημοσίου κλειδιού δεσπόζουσα θέση κατέχει η αρχή πιστοποίησης. Στο δεύτερο μέρος θα δείξουμε πώς μπορούμε να δημιουργήσουμε τη δική μας, ενδοεταιρική αρχή πιστοποίησης.

5.6.1 Public Key Infrastructure

Μία υποδομή δημοσίου κλειδιού (Public Key Infrastructure – PKI) επιτρέπει στους χρήστες του Internet να ανταλλάσσουν ασφαλώς και με ιδιωτικότητα δεδομένα και χρήματα, χρησιμοποιώντας ένα ζεύγος δημοσίου και ιδιωτικού κλειδιού, το οποίο αποκτάται και μοιράζεται από μία πιστοποιημένη και εμπιστεύσιμη αρχή. Το PKI παρέχει

ένα ιεραρχικό πλαίσιο χειρισμού ψηφιακών οντοτήτων, οι οποίες χρησιμοποιούνται στην ασφάλεια των επικοινωνιών.

Τα συστατικά του PKI περιλαμβάνουν τους χρήστες του ασφαλούς δικτύου, τουλάχιστον μία Αρχή Πιστοποίησης (Certification Authority – CA), ψηφιακά πιστοποιητικά που περιέχουν πληροφορίες (όπως την ταυτότητα του χρήστη, τη χρονική διάρκεια πιστοποίησης, κτλ), ένα μηχανισμό διαμοιρασμού (LDAP, HTTP) και προαιρετικά μία Αρχή Καταχώρησης (Registration Authority – RA) που θα ελαφρύνει την CA από το επεξεργαστικό βάρος έκδοσης των πιστοποιητικών.

Το PKI παρέχει στους πελάτες του ένα εύκολα κλιμακούμενο και ασφαλή μηχανισμό για διανομή, διαχείριση και ανάκληση πιστοποιητικών σε ένα ασφαλές δίκτυο. Κάθε οντότητα που παίρνει μέρος (άνθρωπος ή συσκευή) εγγράφεται στο PKI μέσω μίας διαδικασίας, κατά την οποία η οντότητα δημιουργεί ένα ζεύγος κλειδιών RSA (ένα ιδιωτικό και ένα δημόσιο) και στη συνέχεια πιστοποιείται η ταυτότητά της από μία CA.

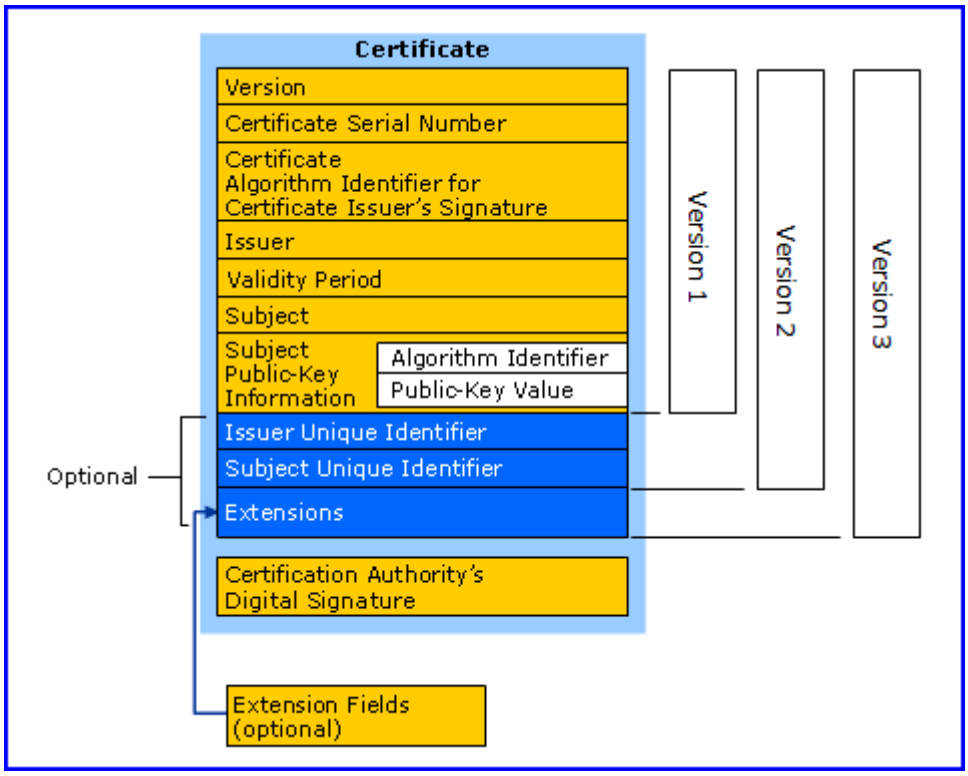
Από τη στιγμή που η οντότητα θα εγγραφεί στο PKI, λαμβάνει ένα ψηφιακό πιστοποιητικό, που εκδίδεται από την CA. Όταν δύο οντότητες θα πρέπει να διαπραγματευθούν ένα ασφαλές κανάλι επικοινωνίας, ανταλλάσσουν τα ψηφιακά πιστοποιητικά τους. Βασισμένη στις πληροφορίες που φέρει το πιστοποιητικό, η οντότητα μπορεί να επιβεβαιώσει την ταυτότητα της άλλης πλευράς και να εγκαθιδρύσει μία κρυπτογραφημένη σύνοδο (session) με τα δημόσια κλειδιά που περιλαμβάνονται στο πιστοποιητικό.

Η Αρχή Πιστοποίησης (CA) διαχειρίζεται τις αιτήσεις για πιστοποιητικά και τα εκδίδει. Αυτό παρέχει κεντροποιημένη διαχείριση κλειδιών για όλες τις εμπλεκόμενες πλευρές. Η οντότητα εμπιστεύεται απόλυτα την CA στο να πιστοποιεί ταυτότητες και να δημιουργεί πιστοποιητικά. Πριν ξεκινήσει το PKI οποιαδήποτε δραστηριότητα, η CA πρέπει να εκδώσει και για τον εαυτό της ένα δημόσιο κλειδί και ένα CA πιστοποιητικό υπογεγραμμένο από την ίδια.

Οι CAs οργανώνονται ιεραρχικά. Στην κορυφή βρίσκεται η root CA, που κατέχει ένα πιστοποιητικό υπογεγραμμένο από την ίδια. Η εμπιστοσύνη ολόκληρης της ιεραρχίας πηγάζει από το ζεύγος κλειδιών RSA της root CA. Το επόμενο επίπεδο CAs πιστοποιούνται από τη root CA και αυτό με τη σειρά του πιστοποιεί το αμέσως κατώτερο επίπεδο και ούτω καθεξής. Μέσα σε ένα ιεραρχικό PKI όλες οι CA μπορούν να πιστοποιήσουν τα πιστοποιητικά όλων των άλλων CAs της ιεραρχίας.

Οι λόγοι που οδηγούμαστε να δημιουργήσουμε πολλές CAs και να τις οργανώσουμε ιεραρχικά είναι δύο. Αφενός τα μεγάλα και ενεργά δίκτυα, που απαιτούν συχνές εκδόσεις και ανακλήσεις πιστοποιητικών, είναι δύσκολο να διαχειριστούν από μία μόνο CA. Αφετέρου, επειδή η ασφάλεια όλου του PKI βασίζεται στην root CA, αποτελεί συνήθη πρακτική να την έχουμε αποσυνδεδεμένη, ώστε να μην μπορεί να γίνει στόχος επίθεσης, και απλά να την επαναφέρουμε όταν χρειάζεται να εκδώσει πιστοποιητικό για κάποια CA κατωτέρου επιπέδου.

Παρακάτω φαίνεται η δομή ενός πιστοποιητικού.



Σχήμα 5.6: Δομή Πιστοποιητικού

5.6.2 Αρχές πιστοποίησης στον Οργανισμό

Ο Windows Server 2008 βασίζεται στο Active Directory Certificate Services (ADCS) για διαχειρίζεται την υποδομή των δημοσίων κλειδιών και τα αντίστοιχα πιστοποιητικά. Με το ACDS μπορούμε να δημιουργήσουμε μία PKI ιεραρχία για να εξυπηρετήσουμε τις ανάγκες του οργανισμού για έκδοση και διαχείριση πιστοποιητικών.

Τα συστατικά του ADCS είναι τα ακόλουθα:

- **Certificate Authorities (CA)**: Οι CAs είναι οι servers που εκδίδουν και διαχειρίζονται τα πιστοποιητικά. Λόγω της ιεραρχικής φύσης του PKI, το ADCS υποστηρίζει τόσο root CAs, όσο και δευτερεύουσες CAs.
- **CA Web Enrollment**: Με τη χρήση της έκδοσης πιστοποιητικού μέσω Web (Web Enrollment), οι χρήστες μπορούν να συνδέονται μέσω του web browser τους σε μία CA και να ζητάνε πιστοποιητικά ή να ανακτούν τις λίστες ανακλημένων πιστοποιητικών (Certificate Revocation Lists – CRLs).
- **Online Responder**: Με τη χρησιμοποίηση ενός Online Responder, ο χρήστης δε χρειάζεται να αποκτήσει ένα πλήρες CRL. Το μόνο που έχει να κάνει είναι να υποβάλει μία αίτηση στον OR για να διευκρινιστεί αν κάποιο συγκεκριμένο πιστοποιητικό είναι έγκυρο. Η χρήση OR είναι ταχύτερη και αποδοτικότερη από τη χρήση CRLs.
- **Network Device Enrollment Service**: Μέσω του NDES δίνεται η δυνατότητα σε συσκευές κατωτέρων επιπέδων, όπως οι routers και τα switches να γίνουν μέρος της PKI ιεραρχίας, παρόλο που δεν μπορούν να γίνουν μέρος του ADCS.

Το ADCS υποστηρίζει δύο τύπους CA:

- **Standalone CA**: Μία CA δε χρειάζεται απαραίτητα να βρίσκεται μέσα στο Active Directory. Μπορούν να βρίσκονται και σε αυτόνομους servers. Οι αυτόνομες CAs χρησιμοποιούνται συνήθως ως root CAs και τίθενται εκτός σύνδεσης για λόγους ασφαλείας. Η έκδοση και η αποδοχή πιστοποιητικών γίνεται χειροκίνητα και τα πιστοποιητικά δεν μπορούν να αλλαχτούν.
- **Enterprise CA**: Μία Enterprise CA αποτελεί μέρος του Active Directory. Συνήθως είναι δευτερεύουσες CAs, κατωτέρων επιπέδων της ιεραρχίας, είναι συνήθως online και είναι αυτές που εκδίδουν τα πιστοποιητικά. Επειδή αποτελούν μέρος του AD εκδίδουν και εγκρίνουν άμεσα πιστοποιητικά στα μέλη του. Τα templates των πιστοποιητικών είναι πιο επιτηδευμένα και μπορούν να προσαρμοστούν.

Οι CAs οργανώνονται ιεραρχικά. Η root CA πρέπει να είναι όσο το δυνατόν ασφαλέστερη, γιατί τυχόν παραβίαση της ασφάλειάς της, οδηγεί σε αυτόματη παραβίαση της ασφάλειας όλων των CAs των κατωτέρων επιπέδων. Για αυτό το λόγο μία κοινή πρακτική είναι να βγάζουμε εκτός σύνδεσης τις CAs των ανωτέρων επιπέδων, ακριβώς

για να μη διακυβεύεται η ασφάλεια τους. Το μέγεθος της ιεραρχίας, τόσο σε πλάτος, όσο και σε βάθος εξαρτάται από πολλούς παράγοντες, όπως το μέγεθος του οργανισμού και η γεωγραφική του διασπορά.

Όσον αφορά βέλτιστες πρακτικές ανάπτυξης του ACDS, κατ αρχήν θα πρέπει να αποφεύγουμε ιεραρχίες ενός επιπέδου, καθώς είναι πολύ δύσκολο να προστατευτούν. Σε περιπτώσεις ιεραρχικής δομής πολλών επιπέδων, θα πρέπει μόνον οι CAs του κατωτέρου επιπέδου να είναι συνδεδεμένες στο δίκτυο, ενώ η root CA και οι ενδιάμεσες CAs θα πρέπει να τίθενται εκτός δικτύου.

Επίσης, λόγω της φύσης τους, οι CAs είναι εξαιρετικοί υποψήφιοι για υλοποίηση με virtualization. Αν η υλοποίησή μας γίνει έτσι, θα πρέπει να αφαιρούμε τα αρχεία της VM CA και να τα αποθηκεύουμε σε κάποιο ασφαλές σημείο. Για ακόμα μεγαλύτερη ασφάλεια, μπορούμε να χρησιμοποιούμε VMs που δεν έχουν καθόλου κάρτες δικτύου, και άρα σύνδεση με τις υπόλοιπες CAs. Η μεταφορά των πιστοποιητικών θα γίνεται με USB sticks.

Οι διαχειριστές της CA ιεραρχίας θα πρέπει να είναι άτομα απολύτου εμπιστοσύνης, καθώς σε αυτούς επαφίεται η ασφάλεια των CA και κατ επέκταση η αξιοπιστία ολόκληρου του οργανισμού. Επίσης, ελάχιστα πράγματα μπορούν να αλλάξουν στην ιεραρχία από τη στιγμή που θα δημιουργηθεί. Για παράδειγμα, το όνομα ενός server δεν μπορεί να αλλάξει, ούτε μπορεί μια standalone CA να γίνει Enterprise CA και το αντίθετο. Συνεπώς, θα πρέπει να είμαστε απολύτως σίγουροι κατά το σχεδιασμό της ιεραρχίας και να έχουμε κάνει τις προβλέψεις μας, όχι μόνο για το άμεσο, αλλά και για το απώτατο μέλλον.

ΚΕΦΑΛΑΙΟ 6

Πολιτική Ελέγχου Πληροφοριακών Συστημάτων για τον Τραπεζικό Τομέα

6.1 Εισαγωγή

Ο Έλεγχος των Πληροφοριακών Συστημάτων (Information Systems Auditing – ISA) είναι η συστηματική, ανεξάρτητη εξέταση των πληροφοριακών συστημάτων και του περιβάλλοντός τους, για να εξακριβωθεί αν οι στόχοι που έχουν θεσπιστεί επιτυγχάνονται ή όχι. Επίσης ο ISA μπορεί να περιγραφεί σαν η συνεχής προσπάθεια για συμμόρφωση. Οι ελεγκτές δεν χρειάζεται απαραιτήτως να ελέγχουν εξ ολοκλήρου το σύστημα. Ενδεχομένως να αρκεί η εξέταση μέρους ή μερών του. Ο έλεγχος πρωταρχικά καλύπτει τις παρακάτω ευρείες περιοχές:

α) Συλλογή πληροφοριών

β) Σύγκριση πληροφοριών

γ) Αναζήτηση αιτιών.

Υπάρχουν πολλοί τύποι ελέγχων. Οι δύο κυριότεροι είναι ο Έλεγχος Συστημάτων (Systems Audit) και ο Έλεγχος Συμμόρφωσης (Compliance Audit). Θα μπορούσαμε, επίσης, να κατηγοριοποιήσουμε τα είδη του ελέγχου με βάση τα επίπεδα ελέγχου: εσωτερικός, εξωτερικός και τρίτων. Οι πιο συνηθισμένοι τύποι ελέγχων είναι ο έλεγχος οικονομικών (Financial Audit), ο έλεγχος συμμόρφωσης και συστημάτων που προαναφέραμε και ο επιχειρησιακός έλεγχος (Operations Audit).

Στον τραπεζικό, αλλά και γενικότερα στον οικονομικό τομέα, ο κίνδυνος (risk) ενυπάρχει εξ ορισμού. Οι κίνδυνοι που υφίστανται σε ένα περιβάλλον, όπου οι υπολογιστές και η δικτύωσή του είναι εκ των ουκ άνευ, είναι οι ακόλουθοι:

1. Επιχειρησιακοί Κίνδυνοι (Operational Risks): Προκύπτουν από τα προβλήματα που αφορούν την αξιοπιστία και την ακεραιότητα των ΠΣ. Η έκταση των συγκεκριμένων κινδύνων εξαρτάται από τα χαρακτηριστικά ασφαλείας, το σχεδιασμό και την υλοποίηση πολιτικών και διαδικασιών, κ.α. Μερικές από τις παραμέτρους ασφαλείας

που πρέπει να αντιμετωπιστούν είναι η ασφάλεια του δικτύου και των βάσεων δεδομένων, η ακεραιότητα των δεδομένων, η αποφυγή κακής χρήσης των πληροφοριών και των πόρων, κτλ.

2. Κίνδυνοι Υπόληψης (Reputational Risks): Είναι απόλυτα συνυφασμένος με τα υπόλοιπα είδη κινδύνων. Οι αποτυχίες, οι απάτες, η μη ορθή ή η καθόλου παροχή πληροφοριών στους πελάτες, η απώλεια χρημάτων των πελατών, η έλλειψη προσωπικής επαφής και ενδιαφέροντος, οι αντιδικίες κτλ, είναι παράγοντες που επηρεάζουν αρνητικά την φήμη και την υπόληψη του οργανισμού. Η έλλειψη ή απώλεια της καλής φήμης της εταιρείας ή του οργανισμού είναι πολύ σημαντικό πρόβλημα και δεν είναι λίγες οι φορές που οφείλεται σε αστοχίες στην ασφάλεια στα πληροφοριακά συστήματα, σε αργή ή αναποτελεσματική αντιμετώπιση περιστατικών ή σε επιθέσεις από κακόβουλους.
3. Νομικοί Κίνδυνοι (Legal Risks): Πηγάζουν από διαφόρους παράγοντες, όπως η έλλειψη σαφούς και κατάλληλου νομικού πλαισίου, από ανάρμοστη, αναποτελεσματική ή κακόβουλη χρήση των ΠΣ, λόγω ανεπαρκούς πολιτικής ασφαλείας, λόγω διακρατικών συναλλαγών με χώρες χωρίς παρόμοιο (συνήθως ανεπαρκέστερο) νομικό καθεστώς και λόγω έλλειψης προβλέψεων νομικής φύσεως σε θέματα διακρατικών επικοινωνιών, όπως το Ίντερνετ.
4. Πιστωτικοί Κίνδυνοι (Credit Risks): Παρουσιάζονται όταν οι δανειολήπτες δεν αποπληρώνουν τα δάνεια και/ή τους τόκους. Σε ένα περιβάλλον όπου τα ΠΣ κατέχουν δεσπόζων ρόλο, οι πιστωτικοί κίνδυνοι είναι μεγάλης σημασίας, γιατί τα ΠΣ και η υποδομή δικτύου έχουν και διανέμουν την πληροφορία αυτή.
5. Κίνδυνοι Ρευστότητας (Liquidity Risks): Παρουσιάζεται όταν μία οντότητα αδυνατεί να τηρήσει τις υποχρεώσεις πληρωμής που έχει, εντός των χρονικών πλαισίων που έχουν οριστεί. Οι τράπεζες, που παρέχει την υποδομή για το ηλεκτρονικό χρήμα (πιστωτικές κάρτες) πρέπει να είναι σε θέση να το χρησιμοποιεί άπταιστα, καθώς κάθε λάθος μπορεί να οδηγήσει σε έλλειψη ρευστότητας και σε νομικά προβλήματα.
6. Κίνδυνοι Επιτοκίων (Interest Rate Risks): Προκύπτουν από την διαφοροποίηση της τιμής των επιτοκίων. Στην περίπτωση των τραπεζών, κάθε διακύμανση του επιτοκίου επηρεάζει όλες τις λειτουργικές οικονομικές πτυχές της, με αποτέλεσμα να ενδέχεται να προκληθούν σημαντικές οικονομικές απώλειες για αυτήν.
7. Κίνδυνοι Διακρατικών Συναλλαγών (Cross-border Transactions Risks): Με την ηλεκτρονική παροχή τραπεζικών υπηρεσιών (e-banking) δημιουργούμε ένα κόσμο οικονομικών υπηρεσιών που δεν θα γνωρίζει σύνορα. Διαφορετικές τιμές επιτοκίων σε διαφορετικές χώρες, διαφορετικά νομίσματα, παρουσία σε πολλές χώρες κτλ,

σημαίνει ότι οι τράπεζες πρέπει να αναλύουν όχι μόνο τις συναλλαγές στις χώρες τους, αλλά διεθνώς. Οι κίνδυνοι της συγκεκριμένης κατηγορίας προκύπτουν από την αυξομείωση των επιτοκίων σε κάποια χώρα, από προβλήματα στην αποπληρωμή των δανείων λόγω κοινωνικών, οικονομικών ή πολιτικών αναταραχών σε κάποια χώρα, κ.α.

Όλοι οι παραπάνω κίνδυνοι αναδεικνύουν την ανάγκη για εμπεριστατωμένο έλεγχο του συνόλου του οργανισμού. Στη συνέχεια θα αναλύσουμε τα είδη των ελέγχων που προαναφέραμε.

1) Έλεγχος Οικονομικών (Financial Audit)

Ο Έλεγχος των Οικονομικών είναι η εξέταση της οικονομικής κατάστασης του οργανισμού. Ο οικονομικός έλεγχος, όπως και τα υπόλοιπα είδη ελέγχου, πρέπει να εκτελείται από κάποιον ανεξάρτητο ελεγκτή. Οι ελεγκτές δεν αρκεί να είναι ανεξάρτητοι, αλλά πρέπει και να φαίνεται ότι είναι ανεξάρτητοι.

Η έννοια “έλεγχος” περιλαμβάνει την έρευνα που πρέπει να διεξάγουν οι ελεγκτές και η οποία θα αποτελέσει τη βάση για την μετέπειτα ανάλυση. Επίσης, στα πλαίσια του οικονομικού ελέγχου, οι ελεγκτές θα πρέπει να λάβουν υπόψη και να αποτιμήσουν τις εσωτερικές διαδικασίες του οργανισμού. Ακόμη, οι ελεγκτές συλλέγουν ενδείξεις και πληροφορίες για να επαληθεύσουν την οικονομική κατάσταση της εταιρείας. Τέλος, οι ελεγκτές υλοποιούν διαδικασίες, σχεδιασμένες έτσι ώστε η οικονομική κατάσταση και οι συνοδευτικές σημειώσεις να είναι πλήρεις από κάθε άποψη.

Μετά την ολοκλήρωση του ελέγχου, οι ελεγκτές εκφράζουν την εμπεριστατωμένη γνωμάτευσή τους, σχετικά με την οικονομική κατάσταση του οργανισμού. Αυτή η γνωμάτευση έχει τη μορφή αναφοράς ελέγχου (audit report). Οι αναφορές ελέγχου δεν εγγυώνται την ακρίβεια της οικονομικής κατάστασης, αλλά την ακρίβεια της οικονομικής κατάστασης βάσει των στοιχείων που δόθηκαν στου ελεγκτές.

Ο πρωταρχικός σκοπός του οικονομικού ελέγχου είναι να ελέγξει την ακρίβεια και την ευμάρεια της οικονομικής κατάστασης του οργανισμού και όχι η ανίχνευση κάποιων ή όλων των καταδολιεύσεων. Οι περισσότερες διαδικασίες ελέγχου είναι προτυποποιημένες και βάσει δειγμάτων και, συνεπώς, μπορεί να μην είναι εφικτό στου ελεγκτές να εξακριβώσουν όλες τις συναλλαγές. Για αυτό το λόγο, οι απάτες που αποπροσανατολίζουν τον οικονομικό έλεγχο απαιτούν την εφαρμογή και άλλων μεθόδων ελέγχου.

Ο οικονομικός έλεγχος σε τράπεζες και οικονομικούς οργανισμούς οφείλει να προσαρμόζεται στα νέα δεδομένα που δημιουργούνται. Η χρήση της Πληροφορικής έχει

φέρει την επανάσταση στον τραπεζικό και στον οικονομικό τομέα, κυρίως στον τρόπο με τον οποίο παρέχουν τις υπηρεσίες τους στους πελάτες τους. Επίσης, οικονομικές υπηρεσίες, όπως το e-banking, το tele-banking, η μεταφορά χρημάτων, τα εμβάσματα, οι πιστωτικές κάρτες, οι έξυπνες κάρτες κτλ, συνεχώς κερδίζουν έδαφος. Με άλλα λόγια, η Πληροφορική έχει βοηθήσει τις τράπεζες και τους οικονομικούς οργανισμούς να υλοποιήσουν πιο αποδοτικά συστήματα, σε συνδυασμό με αυτοματοποιημένες μεθόδους ελέγχου και ανάλυσης κινδύνου.

Η οικονομική κατάσταση του οργανισμού αντικατοπτρίζει την οικονομική του υγεία. Δουλειά του ελεγκτή είναι να προσδιορίσει αν η οικονομική κατάσταση έχει ορθώς παρουσιαστεί. Για να επιτευχθεί αυτό, ο ελεγκτής θα πρέπει να ορίσει τους σκοπούς του ελέγχου, να σχεδιάσει τις διαδικασίες και να συλλέξει πληροφορίες και αποδείξεις που επιβεβαιώσουν ή θα διαψεύσουν τους ισχυρισμούς του οργανισμού.

Ο οικονομικός έλεγχος υλοποιείται σε τρεις φάσεις. Στην πρώτη φάση καθορίζεται το πλάνο του ελέγχου. Στη δεύτερη φάση δοκιμάζονται τα στοιχεία εσωτερικού ελέγχου, όπως πχ διαδικασίες, πολιτικές κτλ. Τέλος, στην Τρίτη φάση υλοποιούνται επιλεκτικά πιο εξειδικευμένες δοκιμασίες, επιλεγμένες από το σύνολο των συναλλαγών που υλοποιεί ο οργανισμός.

2) Έλεγχος Συμμόρφωσης (Compliance Audit)

Οι λειτουργίες ενός οργανισμού υπόκεινται σε ένα σύνολο νόμων και κανονισμών. Η παραβίαση αυτών έχει σαν αποτέλεσμα την επιβολή ποινών και την καταβολή προστίμων. Η συμμόρφωση του οργανισμού με αυτούς τους κανόνες και νόμους παρακολουθείται από ρυθμιστικές αρχές μέσω του ελέγχου συμμόρφωσης.

Ο έλεγχος συμμόρφωσης των ηλεκτρονικών συναλλαγών είναι δύσκολος και πολύπλοκος. Πρέπει να υπάρχει συστηματικός έλεγχος των συναλλαγών ή έστω ένα ικανό δείγμα τους. Μέσω του ελέγχου συμμόρφωσης θα πρέπει να ληφθεί υπόψη ένας κυκεώνας νόμων, κανονισμών και κανόνων και κάθε αλλαγή σε κάποια εφαρμογή ή δεδομένα θα πρέπει να υπόκειται σε έλεγχο.

Ο έλεγχος συμμόρφωσης αποτελείται και αυτός από τρία στάδια. Το σχεδιασμό, όπου μελετώνται και καταγράφονται οι κανόνες, οι κανονισμοί, οι νόμοι και τα διατάγματα και τον σχεδιασμό δοκιμών για την εξακρίβωση της συμμόρφωσης με αυτούς. Δεύτερο στάδιο είναι η δοκιμή και ο έλεγχος της συμμόρφωσης του οργανισμού, μέσω των δοκιμών που σχεδιάστηκαν στο πρώτο στάδιο. Τρίτο και τελευταίο στάδιο είναι ο έλεγχος της συμμόρφωσης επιλεκτικά σε κάποιες από τις συναλλαγές.

Τέλος, όσον αφορά τον έλεγχο συμμόρφωσης στους τραπεζικούς οργανισμούς ελέγχεται η συμμόρφωση με τους κανόνες που θέτουν θεσμοί, όπως η Κεντρική Τράπεζα, το Κράτος, κ.α.

3) Έλεγχος Πληροφοριακών Συστημάτων (Information Systems Audit - ISA)

Ο έλεγχος των πληροφοριακών συστημάτων είναι μια συστηματική διεργασία συλλογής και αξιολόγησης πληροφοριών που αφορούν την ορθή υλοποίηση, λειτουργία και έλεγχο των πληροφοριακών συστημάτων. Ο ISA μπορεί να θεωρηθεί ως μέρος του οικονομικού ελέγχου. Συνεπώς, απαιτείται ένα λογικό πλαίσιο για τη διεξαγωγή του ελέγχου στο πληροφοριακό περιβάλλον, ώστε να αναγνωριστούν όλες οι σημαντικές διεργασίες και αρχεία δεδομένων.

Ο ISA υλοποιείται σε τρία στάδια, ανάλογα με αυτά του οικονομικού ελέγχου. Στην πρώτη φάση γίνεται ο σχεδιασμός και ο ελεγκτής των πληροφοριακών συστημάτων εντοπίζει τους διάφορους κινδύνους και ευπάθειες και ορίζει τους τρόπους αντιμετώπισής τους. Επίσης σχεδιάζονται λεπτομερώς οι δοκιμές που θα χρειαστεί να εκτελεστούν στη δεύτερη φάση. Τέλος, στην τρίτη φάση δοκιμάζονται και ελέγχονται επιλεκτικά διάφορες συναλλαγές. Σε αυτή τη φάση ο ελεγκτής χρησιμοποιεί εκτεταμένα εργαλεία έλεγχου μέσω υπολογιστή.

4) Έλεγχος Πληροφοριακών Συστημάτων για τον Τραπεζικό και τον Οικονομικό τομέα

Ο Έλεγχος είναι ένα από τα κύρια εργαλεία παρακολούθησης του μάνατζμεντ στις τράπεζες και του οικονομικούς οργανισμούς. Σε ένα μηχανογραφημένο περιβάλλον, ο ISA είναι πολύ αποτελεσματικός, αλλά και απαραίτητος. Στους τραπεζικούς και οικονομικούς οργανισμούς συνήθως αυτό γίνεται με την υιοθέτηση διαφορετικών μεθόδων, τόσο εσωτερικά, όσο και από εξωτερικούς συνεργάτες. Στην πρώτη περίπτωση, ο ISA απαιτεί την δημιουργία ομάδας ελεγκτών, που θα συμμετέχουν εσωτερικοί αλλά και εξωτερικοί ελεγκτές. Ωστόσο, προτιμητέα είναι η δεύτερη περίπτωση, όπου ο ISA διεξάγεται με τη βοήθεια εξειδικευμένων εξωτερικών συνεργατών, οι οποίοι προσφέρουν και αντικειμενικότητα.

Οι τεχνικές και τα εργαλεία που χρησιμοποιούνται για τον έλεγχο είναι οι εξής:

α) Μέθοδος Δοκιμής Δεδομένων: Αυτή η μέθοδος χρησιμοποιείται για να ελεγχθεί η ακεραιότητα και η ορθότητα των εφαρμογών, χρησιμοποιώντας ειδικά προετοιμασμένα

δεδομένα. Τα αποτελέσματα της κάθε δοκιμής συγκρίνονται με τα αναμενόμενα αποτελέσματα.

β) Αξιολόγηση του Συστήματος σε βασικές συναλλαγές: Σε αυτή τη μέθοδο, ένα σύνολο βασικών συναλλαγών προετοιμάζεται συ συνδυασμό με τα αναμενόμενα αποτελέσματα. Το σύνολο αυτό είναι περιεκτικό και περιλαμβάνει όλα τα είδη των συναλλαγών. Όταν ολοκληρωθούν οι δοκιμές, τα αποτελέσματα συγκρίνονται με τα αναμενόμενα και στη συνέχεια εξάγονται τα συμπεράσματα.

γ) Παρακολούθηση Ροής Δεδομένων σε Εφαρμογή: Με αυτή τη μέθοδο, δοκιμαστικά δεδομένα που επιλέξαμε καθοδηγούνται, ώστε να περάσουν από όλα τα λογικά στάδια της εφαρμογής. Στο τέλος εξάγονται όλες οι εντολές που εκτελέστηκαν κατά τη διάρκεια επεξεργασίας των δεδομένων.

δ) Ολοκληρωμένη Δοκιμή της Εγκατάστασης: Η συγκεκριμένη δοκιμή είναι αυτοματοποιημένη και σε αυτήν ο έλεγχος ενσωματώνεται στην εκάστοτε εφαρμογή, ως ένα επιπλέον module της. Έτσι, προγραμματίζουμε την εφαρμογή, ώστε ο έλεγχος να αποτελεί μέρος της τυπικής λειτουργίας της.

ε) Παράλληλη Προσομοίωση: Σε αυτή τη μέθοδο απαιτείται από τον ελεγκτή να υλοποιήσει μία δικιά του εφαρμογή, η οποία θα προσομοιώνει τη λειτουργία της εφαρμογής και, εν τέλει, συγκρίνονται τα αποτελέσματα εκτέλεσης των δύο εφαρμογών.

Σε περιπτώσεις που χρειαζόμαστε έλεγχο πραγματικού χρόνου, ενσωματώνουμε ένα στοιχείο ελέγχου (audit module) το οποίο χρησιμοποιείται για την αναγνώριση των σημαντικών συναλλαγών, καθώς αυτές εκτελούνται και αντίγραφα αυτών συναλλαγών εξάγονται σε πραγματικό χρόνο. Ακόμη, προκαθορίζονται κάποιες συνθήκες για όλες τις εφαρμογές, οι οποίες πρέπει να πληρούνται.

Πολύ σημαντικό κομμάτι του ISA σε έναν τραπεζικό οργανισμό είναι ο έλεγχος των βάσεων δεδομένων. Η δομή των βάσεων δεδομένων ποικίλει, από απλά αρχεία μέχρι δομές βάσεων δεδομένων. Για να ελεγχθούν αποτελεσματικά οι βάσεις, είναι απαραίτητη μια διεργασία κανονικοποίησης. Η κανονικοποίηση είναι μία διεργασία καθαρά τεχνικής φύσεως και η δημιουργία της είναι ευθύνη των διαχειριστών της. Ωστόσο, και οι ελεγκτές πρέπει να έχουν γνώση της. Ο ελεγκτής πρέπει να διαπιστώσει αν τα συστημικά αρχεία και οι βάσεις δεδομένων είναι ορθώς κανονικοποιημένα και ότι δεν υπάρχει σημαντικός πλεονασμός και εξαρτήσεις, γιατί μια μη κανονικοποιημένη βάση δεδομένων ενδέχεται να επηρεάσει την ακεραιότητα των δεδομένων. Επίσης, θα πρέπει να ελεγχθούν και οι περιορισμοί της βάσεως δεδομένων.

Μέχρι τώρα αναφερόμασταν στο ρόλο του ελεγκτή. Εκτός από τον ελεγκτή (auditor), βασικό ρόλο στον έλεγχο των τραπεζικών και οικονομικών οργανισμών έχει ο ρυθμιστής (regulator). Καθήκον του ρυθμιστή είναι να διασφαλίζει την ομαλότητα στις αγορές και τα οικονομικά συστήματα και να προσπαθεί για την ανάπτυξή τους. Ακόμη, ο ρυθμιστής εκδίδει κανονισμούς και οδηγίες που οι εμπλεκόμενοι στις οικονομικές δραστηριότητες οφείλουν να ακολουθούν. Ουσιαστικά, ο ρόλους του ρυθμιστή περικλείει εκείνον του ελεγκτή. Ο ρυθμιστής ορίζει το γενικότερο πλαίσιο λειτουργίας και ο ελεγκτής διασφαλίζει την αποδοτικότητα, την ταχύτητα και την ευρυθμία των τραπεζικών οργανισμών, καθώς και την αποτροπή καταδολιεύσεων.

Για όλα τα παραπάνω είναι απαραίτητο ένα σύνολο προτύπων (standards), πρακτικών και διαδικασιών και τα οποία υιοθετούνται από κάθε οργανισμό στον τραπεζικό και οικονομικό τομέα και που αφορούν κάθε πτυχή της μηχανογράφησης των οργανισμών, συμπεριλαμβανομένων των δικτυακών τοπολογιών, εφαρμογών, βάσεων δεδομένων, χαρακτηριστικών ασφαλείας, χαρακτηριστικά ελέγχου και λογιστικής, κ.α. Τα πρότυπα αυτά πρέπει να είναι ανοικτά, γενικά και σύντομα και θα πρέπει να διασφαλίζουν ότι οι τραπεζικοί και οικονομικοί οργανισμοί μπορούν να ελεγχθούν ενδελεχώς και τεχνηέντως. Επίσης, θα πρέπει να περιέχουν και εκείνες τις δικλείδες ασφαλείας που θα ενισχύουν τη σθεναρότητα των μηχανισμών ασφαλείας, ώστε να μειώνεται ο κίνδυνος ηλεκτρονικών εγκλημάτων, όπως το hacking, το spamming, η μη εξουσιοδοτημένη πρόσβαση και η καταστροφή ή κακή χρήση δεδομένων.

6.2: Ανατομία ενός ελέγχου

Η εμφάνιση τα τελευταία χρόνια προβλημάτων ευρείας κλίμακας σε οργανισμούς (περιλαμβανομένων και των τραπεζικών), ανάγκασε τους οργανισμούς να εστιάσουν σε αυτά και ειδικότερα στον χειρισμό και διακυβέρνηση των πληροφοριακών συστημάτων. Η προστασία όλων των στοιχείων του ενεργητικού του οργανισμού είναι ευθύνη της διοίκησής του. Για να αποφορτιστεί κάπως από αυτή την ευθύνη, καθώς και για να εκπληρώσει τις προσδοκίες του, η διοίκηση πρέπει να υλοποιήσει ένα επαρκές σύστημα εσωτερικών μηχανισμών ελέγχου. Επίσης, πρέπει να καταστεί σαφές ότι το εύρος του ISA περιλαμβάνει και τη διοίκηση, τόσο του οργανισμού, όσο και των πληροφοριακών συστημάτων.

Κάθε οργανισμός πρέπει να δίδει τις ακόλουθες πληροφορίες στον ελεγκτή πληροφοριακών συστημάτων:

- Τα άτομα του προσωπικού που είναι υπεύθυνα για τα πληροφοριακά συστήματα
- Πληροφορίες από αυτά τα άτομα που τους επιτρέπει να αποφορτιστούν από αυτή την ευθύνη
- Πλαίσιο ελέγχου, υιοθετημένο από τη διοίκηση του οργανισμού, ως μέρος της πολιτικής.

Οι στόχοι του ελέγχου ενδέχεται να προσαρμόζονται στις εκάστοτε ανάγκες και ιδιορρυθμίες του ελεγχόμενου οργανισμού, στους εθνικούς νόμους και τους κανονισμούς και το προβλεπόμενο βάθος που θα έχει. Οι στόχοι αυτοί είναι:

- Καταγραφή του συστήματος διοίκησης και ελέγχου των πληροφοριακών συστημάτων
- Καταγραφή και ανάλυσης της αποδοτικότητας του συστήματος διοίκησης και ελέγχου
- Προσμέτρηση ή όχι των πληροφοριακών συστημάτων που επιτελούν οικονομικές εργασίες
- Προσμέτρηση ή όχι των πληροφοριακών συστημάτων που δεν έχουν σχέση με τις οικονομικές εργασίες.

Το εύρος του ελέγχου θα πρέπει σίγουρα να περιλαμβάνει τα ακόλουθα:

- Τα δεδομένα
- Τα συστήματα εφαρμογών
- Τις διάφορες τεχνολογίες που χρησιμοποιούνται
- Τις εγκαταστάσεις
- Τους εργαζομένους

Για να ολοκληρωθεί ο έλεγχος και για να θεωρείται αποδοτικός και ορθός θα πρέπει να συμπεριληφθούν τουλάχιστον τα ακόλουθα:

1) Σκοπός του ελέγχου και στόχοι που πρέπει να εκπληρωθούν
2) Εκτίμηση των κινδύνων σε αντιδιαστολή με την χρήση των πληροφοριακών συστημάτων από τον οργανισμό
3) Στρατηγική του ISA, συνοδευόμενη από το πλάνο εφαρμογής του
4) Κόστος των πληροφοριακών συστημάτων και τα αντίστοιχα budgets.
5) Πολιτικές υψηλού επιπέδου για τα πληροφοριακά συστήματα
6) Έγκριση σημαντικών συμβολαίων και παρακολούθηση της τήρησής τους
7) Παρακολούθηση της απόδοσης των SLA (Service Level Agreement)

8) Επίδραση εξωτερικών οντοτήτων, όπως το Ίντερνετ, στα πληροφοριακά συστήματα
9) Έλεγχος των αναφορών αυτό-αξιολόγησης
10) Πλάνο Συνέχισης Λειτουργίας (Business Continuity Plan). Δοκιμή και αξιολόγησή του
11) Συμμόρφωση με το νομικό και κανονιστικό πλαίσιο

Μία άλλη σημαντική πτυχή της εργασίας του ελεγκτή είναι ο έλεγχος και η αξιολόγηση των πολιτικών που διέπουν τη λειτουργία του οργανισμού. Επίσης, θα πρέπει να διασφαλίσει ότι καλύπτουν όλες τις πτυχές του οργανισμού. Οι πολιτικές που τουλάχιστον πρέπει να υπάρχουν, είναι:

1) Πολιτική Ασφαλείας
2) Πολιτική Ανθρώπινου Δυναμικού
3) Πολιτική Κατοχής Δεδομένων
4) Πολιτική Χρησιμοποίησης Υπολογιστών από τον Τελικό χρήστη
5) Πολιτική Copyright
6) Πολιτική Διατήρησης Δεδομένων
7) Πολιτική Απόκτησης Συστημάτων και Εγκατάστασης τους
8) Πολιτική για Εξωτερικούς Συνεργάτες (Outsourcing)

Για όλες τις παραπάνω πολιτικές ο ελεγκτής θα πρέπει να αποφανθεί ότι είναι οι κατάλληλες και ότι πληρούν τις προϋποθέσεις που θέτει ο οργανισμός. Επίσης, θα πρέπει να ελέγξει το κατά πόσον οι πολιτικές εφαρμόζονται και αν, φυσικά εφαρμόζονται σωστά. Ακόμη, απαραίτητος είναι ο έλεγχος και η ανάλυση των θέσεων και των ατόμων που απαρτίζουν το Τμήμα Πληροφορικής του οργανισμού και να διαπιστώσει αν είναι η διάρθρωσή του είναι σωστή, αν υπάρχουν αντικρουόμενα καθήκοντα για κάποιους κτλ.
Όταν ολοκληρωθεί ο έλεγχος, ο ελεγκτής θα πρέπει να συντάξει την αναφορά του προς τους υπευθύνους του οργανισμού και θα πρέπει να περιλαμβάνει:
α) Μία δήλωση ότι η διοίκηση είναι υπεύθυνη για τα πληροφοριακά συστήματα και τους μηχανισμούς ελέγχου τους.

β) Μία δήλωση ότι οι μηχανισμοί ελέγχου μπορούν να προσδώσουν αρκετή αλλά όχι πλήρη διασφάλιση απέναντι στις απώλειες και λανθασμένη χρήση.

γ) Περιγραφή των σημαντικότερων διαδικασιών που η διοίκηση έχει εγκρίνει και υιοθετήσει και αφορούν τους εσωτερικούς μηχανισμούς ελέγχου.

δ) Πληροφορίες σχετικά με την ενδεχόμενη μη συμμόρφωση με τους εθνικούς ή τους κλαδικούς νόμους και κανονισμούς.

ε) Πληροφόρηση σχετικά με μη ελεγχόμενους κινδύνους.

στ) Πληροφόρηση για μη αποτελεσματικές δομές ελέγχου, μαζί με οδηγίες και προτάσεις για βελτίωσή τους.

ζ) Συνολικά συμπεράσματα του ελεγκτή των πληροφοριακών συστημάτων που διεξήγαγε τον ISA.

Τέλος, μετά την ολοκλήρωση του ελέγχου, ο ελεγκτής οφείλει να παρακολουθεί τον οργανισμό και να παρατηρεί αν οι όποιες ατέλειες και αδυναμίες διευθετούνται και αν όχι, να προτείνει λύσεις και βελτιώσεις.

6.3: Στόχοι του Ελέγχου Πληροφοριακών Συστημάτων

Οι βασικοί στόχοι του ISA περιλαμβάνουν, μεταξύ άλλων, τα ακόλουθα:

1) Προστασία των Πληροφοριακών συστημάτων και των πόρων του οργανισμού
2) Διατήρηση της Ακεραιότητας των Δεδομένων
3) Διατήρηση της Αποτελεσματικότητας των Συστημάτων
4) Διασφάλιση της Αποδοτικότητας των Συστημάτων

6.3.1: Προστασία των Πληροφοριακών συστημάτων και των πόρων του οργανισμού

Τα πληροφοριακά συστήματα του οργανισμού πρέπει να προστατεύονται από ένα σύστημα εσωτερικού ελέγχου, που θα περιλαμβάνει προστασία του υλικού (hardware) γιατί μπορεί να καταστραφεί, του λογισμικού (software) γιατί μπορεί να κλαπεί, τις εγκαταστάσεις, το ανθρώπινο δυναμικό και την τεχνογνωσία του, τα αρχεία δεδομένων γιατί μπορεί να αλλαχθούν ή διαγραφούν, τις προμήθειες κτλ. Ο ελεγκτής των πληροφοριακών συστημάτων θα πρέπει να ελέγξει τη φυσική ασφάλεια των κτιριακών εγκαταστάσεων, είτε από ηθελημένη επέμβαση, είτε από ατυχήματα, τη συνολική ασφάλεια του λειτουργικού των συστημάτων και την καταλληλότητα και πληρότητα των στοιχείων εσωτερικού ελέγχου.

6.3.2: Ακεραιότητα Δεδομένων

Η διατήρηση της ακεραιότητας των δεδομένων περιλαμβάνει την προστασία από μη εξουσιοδοτημένη πρόσθεση, διαγραφή, αλλαγή ή αντικατάσταση δεδομένων. Τα πληροφοριακά συστήματα χρησιμοποιούνται για να αποθηκεύουν, να επεξεργάζονται και να μεταδίδουν δεδομένα με ασφαλή και αποτελεσματικό τρόπο. Η έμφαση δίδεται στην ακρίβεια των δεδομένων και στην ασφαλή μετάδοσή τους.

Τα δεδομένα πρέπει να έχουν τα εξής χαρακτηριστικά:

- Να είναι ακριβή: Μη ακριβή δεδομένα μπορεί να οδηγήσουν σε λανθασμένες αποφάσεις που θα βλάψουν τον οργανισμό.
- Να είναι εμπιστευτικά: Τα δεδομένα πρέπει να προστατεύονται από την ανάγνωση ή την αντιγραφή τους από μη εξουσιοδοτημένα άτομα.
- Να είναι πλήρη: Μη πλήρη δεδομένα, χάνουν τη σημασία τους και τη χρησιμότητά τους
- Να είναι ενημερωμένα: Τα δεδομένα πρέπει να ενημερώνονται τακτικά. Αν δεν γίνεται αυτό, δημιουργούν εσφαλμένη εικόνα του οργανισμού.
- Να είναι αξιόπιστα: Τα δεδομένα πρέπει να είναι αξιόπιστα, γιατί σημαντικές αποφάσεις λαμβάνονται με βάση αυτά
- Να είναι συνεχώς και αδιαλείπτως διαθέσιμα: Τα δεδομένα πρέπει να είναι συνεχώς διαθέσιμα στους εξουσιοδοτημένους χρήστες και πάντα απροσπέλαστα από τους μη εξουσιοδοτημένους.
- Να είναι αποτελεσματικά: Τα δεδομένα πρέπει να εμπεριέχουν τις πληροφορίες που απαιτούνται, χωρίς πλεονασμό, αλλά και χωρίς ελλείψεις.

6.3.3: Αποτελεσματικότητα Συστημάτων

Ένα αποτελεσματικό Πληροφοριακό Σύστημα συνεισφέρει σημαντικότατα στην επίτευξη των στόχων του οργανισμού. Συνεπώς, ένας από τους στόχους του ISA πρέπει να είναι ο έλεγχος της αποτελεσματικότητάς του και θα περιγράφει πότε, τι και πώς το σύστημα πρέπει να βελτιωθεί, ώστε η αποτελεσματικότητά του να μεγιστοποιηθεί.

Όσον αφορά τα πληροφοριακά συστήματα σε έναν τραπεζικό οργανισμό, πρέπει να πετυχαίνουν τους στόχους τους αποτελεσματικά και αποδοτικά. Ευθύνη του ελεγκτή είναι να αποφανθεί το πώς αυτά συνεισφέρουν στην εύρυθμη λειτουργία του οργανισμού και πώς βοηθούν στην επίτευξη των πραγματικών του στόχων.

Οι βασικοί στόχοι της μηχανογράφησης ενός οργανισμού είναι:

α) Βελτίωση στην επίτευξη των στόχων του οργανισμού: Τα πληροφοριακά συστήματα πρέπει να αυξάνουν και να βοηθούν στην αύξηση της παραγωγικότητας των εργαζομένων.

β) Βελτίωση στην ποιότητα των υπηρεσιών: Τα πληροφοριακά συστήματα πρέπει να συνεπικουρούν στην βελτίωση της ποιότητας της δουλειάς και των παρεχόμενων υπηρεσιών.

γ) Επιχειρησιακή αποτελεσματικότητα: Τα πληροφοριακά συστήματα πρέπει να είναι αποτελεσματικά και εύκολα στη χρήση. Αυτό θα πρέπει να αναγνωρίζεται και από τους εργαζομένους και τους χειριστές τους.

δ) Αποτελεσματικότητα των πληροφοριακών συστημάτων: Τα πληροφοριακά συστήματα πρέπει να είναι κατάλληλα εξοπλισμένα και να αναβαθμίζονται συχνά.

ε) Αποτελεσματικότητα όσον αφορά το κόστος τους: Τα πληροφοριακά συστήματα πρέπει να χρησιμοποιούνται πλήρως. Τα οφέλη που αποκομίζουμε από αυτά πρέπει να υπερβαίνουν το κόστος απόκτησης, λειτουργίας και συντήρησής τους.

6.3.4: Αποδοτικότητα των Συστημάτων

Οι πόροι που χρησιμοποιούν τα πληροφοριακά συστήματα, όπως συσκευές, περιφερειακά, λογισμικό κτλ, είναι περιορισμένοι και κοστίζουν. Ένα αποδοτικό πληροφοριακό σύστημα χρησιμοποιεί όσο το δυνατόν λιγότερους πόρους για να επιτύχει το επιθυμητό αποτέλεσμα. Επίσης, είναι σημαντικό να γνωρίζουμε αν οι δυνατότητες ενός συστήματος έχουν εξαντληθεί ή αν η παρούσα κατανομή των πόρων δημιουργεί συμφόρηση.

Η αποδοτικότητα ενός συστήματος ορίζεται ως ο λόγος της εξόδου προς την είσοδο. Αν τα παραγόμενα αποτελέσματα είναι περισσότερα με τους ίδιους ή λιγότερους πόρους, τότε έχουμε ένα αποδοτικό σύστημα. Επίσης, είναι πολύ σημαντικός ο καθορισμός του φόρτου εργασίας, σε σχέση πάντα με τον διαθέσιμο εξοπλισμό.

Συνεπώς, οι ελεγκτές των πληροφοριακών συστημάτων θα πρέπει να εξετάσουν πόσο αποδοτικά είναι, σε σχέση με το φόρτο εργασίας και το πλήθος των εργαζομένων, με απώτερο στόχο ο οργανισμός να έχει το μέγιστο αποτέλεσμα σε ποσότητα και ποιότητα υπηρεσιών, χρησιμοποιώντας το δυνατόν λιγότερους πόρους.

6.3.5: Λοιποί Στόχοι του ISA

Παρακάτω ακολουθούν και κάποιοι περαιτέρω στόχοι του ISA:

- Αναγνώριση των κινδύνων που αντιμετωπίζει ο οργανισμός και ιεράρχησή τους.
- Σύμπνοια της υλοποίησης των πληροφοριακών συστημάτων με τις διάφορες πολιτικές του οργανισμού.
- Εξακρίβωση του κατά πόσο οι διαδικασίες και οι πολιτικές έχουν σχεδιαστεί για να καλύπτουν όλο το εύρος του οργανισμού και του συνόλου των συστημάτων του
- Διακρίβωση ότι κατάλληλες πολιτικές και διαδικασίες ασφαλείας εφαρμόζονται κατά γράμμα.
- Προσπάθεια για ελαχιστοποίηση της πιθανότητας εμφάνισης κακής χρήσης και/ή καταδολιεύσεων, που θα χρησιμοποιούν κάποιο από τα συστήματα του οργανισμού.
- Παροχή συστάσεων για τη βελτίωση των μηχανισμών ελέγχου των συστημάτων
- Συμμόρφωση με τις ισχύουσες νόρμες και κανόνες δεοντολογίας, για τη διασφάλιση ποιοτικού και συνεπούς έλεγχου πληροφοριακών συστημάτων.

6.4: Προσεγγίσεις Ελέγχου Πληροφοριακών Συστημάτων

Υπάρχουν τρεις προσεγγίσεις για τη διεξαγωγή του ελέγχου των πληροφοριακών συστημάτων:

1) Έλεγχος χωρίς να δίδεται έμφαση στον υπολογιστή
2) Έλεγχος συμπεριλαμβάνοντας τον υπολογιστή
3) Έλεγχος χρησιμοποιώντας τον υπολογιστή

6.4.1: Έλεγχος χωρίς να δίδεται έμφαση στον υπολογιστή

Σε αυτήν την προσέγγιση η έμφαση δίδεται στον έλεγχο της ορθότητας των εξαγόμενων δεδομένων και εγγράφων σε αντιδιαστολή με τα εισερχόμενα δεδομένα, χωρίς να εμβαθύνουμε στην επεξεργασία που μεσολάβησε. Η προσέγγιση αυτή προτιμάται όταν οι ελεγκτές δεν έχουν το απαιτούμενο επίπεδο τεχνικών δεξιοτήτων, ώστε να υιοθετήσουν τις άλλες πρακτικές. Είναι επίσης προτιμητέα όταν ο οργανισμός βασίζεται κυρίως στο προσωπικό που χειρίζεται τα συστήματα για την ασφάλειά τους και όχι τόσο στα συστήματα τα ίδια.

Η συγκεκριμένη προσέγγιση ελέγχου μπορεί να χρησιμοποιηθεί στις ακόλουθες περιστάσεις:

- Όταν το σύστημα εφαρμογών είναι απλό, λογικό και άμεσο και υπάρχει σαφής διαδρομή που μπορεί να ακολουθήσεις ο έλεγχος
- Όταν το σύστημα εφαρμογών έχει ακολουθήσει την πεπατημένη άλλων συστημάτων, τα οποία είναι διεξοδικά δοκιμασμένα και/ή παρέχονται από κάποια πολύ αξιόπιστη εταιρεία, και άρα εμπίπτουν στη γενικότερη κατηγορία δοκιμασμένων συστημάτων.
- Όταν ανατίθεται πρωτίστως στους χρήστες και δευτερευόντως στα ίδια τα συστήματα η διαφύλαξή τους.

Η πρώτη αυτή προσέγγιση είναι απλή και δεν παρέχει πληροφόρηση σχετικά με το αν είναι σε θέση να ανταπεξέλθει σε αλλαγές. Επίσης, δεν μπορούμε να χρησιμοποιήσουμε αυτή τη μεθοδολογία σε πολύπλοκα συστήματα.

6.4.2: Έλεγχος συμπεριλαμβάνοντας τον υπολογιστή

Σε αυτήν την προσέγγιση ελέγχου απαιτείται πολύ καλή γνώση του λειτουργικού συστήματος και του hardware, καθώς και τεχνικές γνώσεις της ανάπτυξης των συστημάτων. Στόχοι αυτής της προσέγγισης αποτελούν τα προγράμματα και τα δεδομένα. Ουσιαστικά, ελέγχεται η συμμόρφωση και εκτελούνται δοκιμές στο σύστημα, στο λογισμικό και στα δεδομένα. Οι ελεγκτές μπορούν να χρησιμοποιήσουν και υπολογιστές για να ελέγξουν τη λογική μέσα στα συστήματα, καθώς και τις εγγραφές τους.

6.4.3: Έλεγχος χρησιμοποιώντας τον υπολογιστή

Σε αυτήν την προσέγγιση το υπολογιστικό σύστημα και τα προγράμματά του χρησιμοποιούνται σαν εργαλεία στη διαδικασία ελέγχου. Ο απώτερο σκοπός είναι να διεξαχθούν ουσιαστικές δοκιμές χρησιμοποιώντας τους υπολογιστές και τα προγράμματα. Τα δεδομένα από τα συστήματα του ελεγχομένου μεταφέρονται σε ένα ανεξάρτητο περιβάλλον. Εκεί διενεργούνται από τους ελεγκτές αναλύσεις τους, χρησιμοποιώντας εξειδικευμένα προγράμματα.

Η συγκεκριμένη μέθοδος χρησιμοποιείται όταν:

- Τα συστήματα εφαρμογών έχουν μεγάλο όγκο εισερχόμενων δεδομένων, παράγουν μεγάλο όγκο εξερχόμενων δεδομένων και εν γένει όταν είναι δύσκολο να ελεγχθεί τόσο μεγάλος όγκος δεδομένων.
- Η λογική του συστήματος είναι ιδιαίτερα περίπλοκη.
- Υφίστανται σημαντικά κενά στη διαδικασία ελέγχου.

Οι υπολογιστές, όπως προαναφέραμε, είναι ιδιαίτερα χρήσιμοι, ειδικά στις δοκιμές που αφορούν τις συναλλαγές. Μερικά από τα προγραμματιστικά εργαλεία που χρησιμοποιούνται για αυτό τον σκοπό είναι τα ακόλουθα:

1) Εργαλεία Ελέγχου Υποβοηθούμενα από Υπολογιστές (Computer Assisted Audit Tools – CAAT): Είναι αποτελεσματικά και αποδοτικά εργαλεία για τον έλεγχο των αρχείων που παράγονται από το σύστημα, τις εγγραφές και τα έγγραφα.
2) Λογισμικό Ελέγχου: Είναι ένα πρόγραμμα, που χρησιμοποιείται από τους ελεγκτές, για την επεξεργασία των δεδομένων που έχουν ιδιαίτερη σημασία για τον έλεγχο. Υπάρχουν τρεις τύποι τέτοιων προγραμμάτων:
    - Προγράμματα τα οποία είναι σχεδιασμένα να επεξεργάζονται δεδομένα και να δημιουργούν αρχεία και αναφορές στη μορφή που επιθυμεί ο ελεγκτής.
    - Προγράμματα ειδικού σκοπού, που εκτελούν τον έλεγχο σε συγκεκριμένες καταστάσεις
    - Προγράμματα εφαρμογών, που εκτελούν συνήθεις επεξεργασίες δεδομένων.

3) Τεχνικές δοκιμής δεδομένων: Ένα δείγμα συναλλαγών δίνεται ως είσοδος στο σύστημα του ελεγχόμενου και τα αποτελέσματα συγκρίνονται με αυτά που είχαν προβλεφθεί
4) Γενικό Λογισμικό Ελέγχου: Είναι η πιο διαδεδομένη τεχνική, όταν εκτελείται ο ISA. Το ACL (Audit Command Language – ACL) είναι ένα τέτοιο λογισμικό και είναι ένα εργαλείο για ανάλυση δεδομένων. Τα πλεονεκτήματα του ACL είναι τα εξής:
    - Δημιουργεί ευέλικτες αναφορές και αποτελέσματα
    - Οι ελεγκτές είναι διαφορετικά πρόσωπα από τους ειδικούς στα τεχνικά θέματα
    - Αυξάνεται η κάλυψη του ελέγχου
    - Εξοικονομείται χρόνος, χρήματα και προσπάθεια
    - Αυξάνεται η αξιοπιστία του ελέγχου

6.5: Μεθοδολογία Ελέγχου Πληροφοριακών Συστημάτων

Ο ISA περιλαμβάνει, όπως είδαμε, χειροκίνητες διαδικασίες, διαδικασίες υποβοηθούμενες από υπολογιστές και πλήρως αυτοματοποιημένες διαδικασίες. Η διαδικασία ελέγχου χωρίζεται για ευκολία και αποτελεσματικότητα σε πέντε βασικά βήματα:

1) Σχεδιασμός
2) Δοκιμή εργαλείων ελέγχου
3) Δοκιμές συναλλαγών
4) Δοκιμή ισολογισμών
5) Ολοκλήρωση ελέγχου.

Σχεδιασμός: Ο σχεδιασμός είναι το πρώτο στάδιο του ελέγχου. Ο ελεγκτής αρχικά πρέπει να κατανοήσει πλήρως τη δομή και την οργανωτική διάρθρωση του οργανισμού, να κατανοήσει τους στόχους του, να ορίσει τους στόχους του ελέγχου, να συλλέξει πληροφορίες, να συνομιλήσει με το προσωπικό, να αναγνωρίσει τους πιθανούς κινδύνους, κ.α. Όσον αφορά την ανάλυση των κινδύνων, θα πρέπει να εντοπιστούν τα συστήματα που αντιμετωπίζουν το μεγαλύτερο κίνδυνο και να αποφασίσουν τη λεπτομέρεια της ανάλυσης και της δοκιμής του.

Δοκιμή εργαλείων ελέγχου: Κατά τη διάρκεια αυτής της φάσης του ελέγχου δοκιμάζονται τα εσωτερικά στοιχεία ελέγχου, με απώτερο σκοπό να αξιολογηθεί η αξιοπιστία τους και να εντοπιστούν τυχόν αδυναμίες. Κατά την εκτέλεση αυτής της φάσης, ο ελεγκτής θα πρέπει να ικανοποιήσει τις ακόλουθες συνθήκες:

- Αναγνώριση των στοιχείων ελέγχου, ώστε να μειωθεί η πιθανότητα παράνομων συμβάντων
- Υλοποίηση των αναγνωρισμένων στοιχείων ελέγχου
- Εξακρίβωση λειτουργίας. Μερικές φορές, παρόλο που έχουν υλοποιηθεί τα στοιχεία ελέγχου, δεν είναι λειτουργικά. Για παράδειγμα, μπορεί να έχει οριστεί η αλλαγή των κωδικών ανά τρίμηνο, αλλά αυτό να μη συμβαίνει
- Έγγραφη καταγραφή των στοιχείων ελέγχου.
- Διατήρηση και συντήρηση των στοιχείων ελέγχου, όπως για παράδειγμα η τακτική συντήρηση της παροχής ρεύματος των συστημάτων.
- Παρακολούθηση των στοιχείων ελέγχου και προληπτικές δράσεις.

Δοκιμές συναλλαγών: Οι δοκιμές των συναλλαγών γίνονται για να διαπιστωθεί αν λανθασμένες συναλλαγές έχουν οδηγήσει σε στρεβλώσεις των οικονομικών πληροφοριών και αν οι συναλλαγές χειρίζονται αποτελεσματικά και αποδοτικά. Ο στόχος εδώ είναι να ελεγχθεί η ακεραιότητα των δεδομένων. Μερικές από αυτές τις δοκιμές θα περιλαμβάνουν την εξέταση αρχείων, τον έλεγχο της υπολογιστικής ακρίβειας, κτλ. Τα CAAT είναι ιδιαίτερα χρήσιμα σε αυτές τις δοκιμές.

Δοκιμή ισολογισμών: Κατά τη διάρκεια του ISA γίνεται η τελική κρίση σχετικά με το βαθμό των απωλειών που προκύπτουν από την αδυναμία διασφάλισης των ενεργητικών του οργανισμού, από τη διασφάλισης της ακεραιότητας των δεδομένων και από την έλλειψη αποτελεσματικότητας και αποδοτικότητας. Όσον αφορά τα δύο πρώτα, η τυπική δοκιμή είναι η επιβεβαίωση των ληφθέντων και η επιβεβαίωση ότι βρίσκονται στην κατοχή μας. Όσον αφορά την αποδοτικότητα και την αποτελεσματικότητα, οι δοκιμές πρέπει να γίνονται κατά τη φάση της ανάπτυξης του συστήματος.

Ολοκλήρωση ελέγχου: Στο τελικό αυτό στάδιο του ελέγχου οι ελεγκτές καλούνται να εκφέρουν τη σαφώς τη γνώμη τους, παρουσιάζοντας τα ευρήματά τους και τις συστάσεις τους. Τα αποτελέσματα του ελέγχου, μαζί με τα προτερήματα και τις συστάσεις των ελεγκτών, πρέπει να γνωστοποιούνται στα υπεύθυνα στελέχη του οργανισμού. Όλα τα

στοιχεία του ελέγχου πρέπει να είναι πολύ καλά οργανωμένα, καθαρογραμμένα και να διευθετούν όλες τις πτυχές που περιλήφθησαν στον έλεγχο.

Κατά την εκτέλεση του ISA ο ελεγκτής έρχεται αντιμέτωπος με πολύπλοκα συστήματα. Για να κατανοήσει καλύτερα κάποιο τέτοιο σύστημα, είναι συνετό να χωρίσει το σύστημα σε υποσυστήματα. Υποσύστημα είναι ένα συστατικό του αρχικού συστήματος, το οποίο επιτελεί κάποιες βασικές λειτουργίες, οι οποίες είναι απαραίτητες για να εκτελέσει το αρχικό σύστημα τους στόχους του. Από τη στιγμή που θα διαχωρίσει το αρχικό σύστημα σε υποσυστήματα, ο ελεγκτής πρέπει:

α) Να αξιολογήσει την αποτελεσματικότητα των στοιχείων ελέγχου του αρχικού συστήματος
β) Να ξεκαθαρίσει τις επιπτώσεις που έχει η αξιοπιστία κάθε υποσυστήματος στην γενικότερη λειτουργία του αρχικού συστήματος.

Υπάρχουν δύο βασικά είδη συστημάτων, που απαιτούν τον διαχωρισμό τους σε υποσυστήματα για να διεξαχθεί ο ISA: Τα συστήματα διαχείρισης (management systems) Και τα συστήματα εφαρμογών (application systems).

Συστήματα Διαχείρισης: Τα συστήματα διαχείρισης παρέχουν μία σταθερή και βασική υποδομή, πάνω στην οποία εδράζονται τα πληροφοριακά συστήματα και μπορούν να είναι λειτουργικά. Τα συστήματα διαχείρισης μπορούν να υποδιαιρεθούν σε υποσυστήματα που θα επιτελούν τις εξής λειτουργίες:

- Διαχείριση Υψηλού Επιπέδου: Καθορίζει τις μακροπρόθεσμες αποφάσεις που αφορούν τη χρήση των πληροφοριακών συστημάτων στον οργανισμό
- Διαχείριση Πληροφοριακών Συστημάτων: Επιτελεί το σχεδιασμό και τον έλεγχο των πληροφοριακών συστημάτων του οργανισμού.
- Διαχείριση Ανάπτυξης Συστημάτων: Σχεδιασμός, υλοποίηση και συντήρηση των συστημάτων εφαρμογών
- Διαχείριση Προγραμμάτων: Προετοιμάζει προγράμματα για νέα συστήματα, συντηρεί τα παλιά και παρέχει υποστηρικτικό λογισμικό
- Διαχείριση Δεδομένων: Σχεδιασμός και έλεγχος των βάσεων δεδομένων
- Διαχείριση Διασφάλισης Ποιότητας: Διασφαλίζει ότι η ανάπτυξη, υλοποίηση, και συντήρηση των πληροφοριακών συστημάτων, συμβαδίζει με τα ποιοτικά πρότυπα του οργανισμού

- Διαχείριση Ασφαλείας: Έλεγχος πρόσβασης και ασφάλεια σε φυσικό επίπεδο των πληροφοριακών συστημάτων
- Διαχείριση Λειτουργιών: Σχεδιασμός και έλεγχος της καθημερινής λειτουργίας των πληροφοριακών συστημάτων.

Συστήματα Εφαρμογών: Τα συστήματα εφαρμογών είναι εκείνα που αναλαμβάνουν την διεκπεραίωση των συναλλαγών. Μπορούν να διαχωριστούν σε υποσυστήματα τα οποία μπορούν να είναι:

- Υποσυστήματα διεπαφών: Αποτελούνται από τα συστατικά που εγκαθιδρύουν τη διεπαφή μεταξύ του συστήματος και του τελικού χρήστη
- Υποσυστήματα εισροής: Αποτελούνται από τα συστατικά που δέχονται, ετοιμάζουν και εισάγουν εντολές και δεδομένα στο σύστημα
- Υποσυστήματα επικοινωνιών: Αποτελούνται από τα συστατικά που μεταδίδουν δεδομένα μεταξύ των συστημάτων και των υποσυστημάτων
- Υποσυστήματα επεξεργασίας: Περιλαμβάνουν τα συστατικά που επιτελούν τη λήψη αποφάσεων, υπολογισμούς, ταξινόμηση και περίληψη των δεδομένων στο σύστημα
- Υποσυστήματα βάσεων δεδομένων: Αποτελούνται από τα συστατικά που καθορίζουν προσθέτουν, αλλάζουν και διαγράφουν δεδομένα στο σύστημα
- Υποσυστήματα εκροής: Αποτελούνται από τα συστατικά που εντοπίζουν και παρουσιάζουν δεδομένα του συστήματος στους χρήστες.

6.6: Πλήρες πλαίσιο εργασίας για τη διενέργεια ενός ISA

Ένα πλήρες πλαίσιο εργασίας μπορεί να δημιουργηθεί από τους βασικού στόχους ενός ISA. Ο ISA κάνει μία εκτίμηση της δομής του οργανισμού και της ποιότητα της διαχείρισης. Πρέπει να τονιστεί ότι ο ISA δεν περιορίζεται απλά στην εκτέλεση κάποιων διαδικασιών, αλλά ο ελεγκτής πρέπει να έχει τα μάτια του και τα αυτιά του ανοιχτά.

Τα βασικά ενδιαφέροντα του ISA, όπως αυτά προκύπτουν από τους στόχους του, είναι:

1) Φύλαξη και ασφάλεια όλων των στοιχείων του ενεργητικού του οργανισμού

Ένας από του βασικούς στόχους κάθε ελέγχου είναι ότι τα στοιχεία του ενεργητικού του οργανισμού (assets) πρέπει να προστατεύονται. Τα στοιχεία αυτά περιλαμβάνουν το

υλικό, το λογισμικό, τα δεδομένα και τους χρήστες. Θα πρέπει, λοιπόν, να υπολογιστούν οι επιπτώσεις που θα υπάρξουν για τον οργανισμό αν καταστραφεί, κλαπεί, δεν αξιοποιείται πλήρως, δεν παρέχει υπηρεσίες ή χρησιμοποιηθεί λανθασμένα (επίτηδες ή από λάθος) κάποιο στοιχείο του ενεργητικού.

Για να διαπιστώσει ο ελεγκτής αν τα στοιχεία ενεργητικού του οργανισμού είναι ασφαλή, θα πρέπει να ελέγξει, μεταξύ άλλων, και τα εξής:

- Περιβαλλοντική Ασφάλεια
- Μη διακοπτόμενη παροχή ηλεκτρικού ρεύματος
- Ηλεκτρική καλωδίωση
- Δομημένη καλωδίωση
- Πυροπροστασία
- Ασφάλιση
- Συμβόλαια ετήσιου ελέγχου και συντήρησης
- Μέθοδοι ασφαλείας, τόσο σε φυσικό, όσο και σε λογικό επίπεδο

2) Ακεραιότητα Δεδομένων

Τα δεδομένα είναι ο πιο σημαντικός πόρος ενός μηχανογραφημένου οργανισμού και πρέπει να ναι ακριβή, πλήρη, συνεπή, ενημερωμένα και αυθεντικά. Οι ελεγκτές πρέπει να ελέγξουν αν παρατηρείται απόκλισης από αυτούς τους στόχους και να επιβεβαιώσουν ότι η ακεραιότητα δεδομένων ενυπάρχει και διατηρείται.

Για την ακεραιότητα των δεδομένων πρέπει να ελεγχθούν τα παρακάτω σημεία:

- Στοιχεία ελέγχου κατά την εισαγωγή των δεδομένων
- Στοιχεία ελέγχου κατά την επεξεργασία των δεδομένων
- Προγράμματα επιδιόρθωσης (patch programms)
- Εκκαθάριση των δεδομένων από πληροφορία που δεν είναι πια απαραίτητη
- Backup των δεδομένων
- Επαναφορά δεδομένων σε περιπτώσεις σφάλματος

3) Πλάνο Επιχειρησιακής Συνέχειας

4) Αποτελεσματικότητα Συστήματος

Από τα πληροφοριακά συστήματα περιμένουμε να αναβαθμίζουν την συνολική ποιότητα σε όλες τις λειτουργίες του οργανισμού, όπως ακρίβεια και ταχύτητα στην εκτέλεσή τους.

Επίσης, πρέπει να είναι φιλικά προς το χρήση. Δουλειά του ελεγκτή είναι να κρίνει πόσο αποτελεσματικό είναι ένα σύστημα στο να πετυχαίνει τους παραπάνω στόχους.

5) Αποδοτικότητα Συστήματος

Οι ελεγκτές θα πρέπει να ελέγχουν το κατά πόσον κάθε υπολογιστικός πόρος λειτουργεί στο μέγιστο των δυνατοτήτων του.

6) Οργάνωση και Διαχείριση

Η αποδοτικότητα των λειτουργιών εξαρτάται από την αποδοτικότητα του προσωπικού που χειρίζεται τα πληροφοριακά συστήματα. Το προσωπικό αυτό πρέπει να εκτελεί τις εργασίες του πλήρως, εντός εύλογου χρονικού διαστήματος, με ακρίβεια και με όσο το δυνατόν λιγότερους πόρους, ενώ με το αποτέλεσμα πρέπει να μεγιστοποιείται τόσο ποσοτικά όσο και ποιοτικά.

Ο ελεγκτής πρέπει να επιληφθεί, ώστε να υπάρξει καταμερισμός των καθηκόντων, περιγραφή του, κατάλληλη εκπαίδευση του προσωπικού, διπλός έλεγχος σε ιδιαίτερα σημαντικές εργασίες, ύπαρξη εφεδρικών σχεδίων κτλ.

ΚΕΦΑΛΑΙΟ 7

Πραγματικά Περιστατικά Ασφάλειας και Επιχειρησιακή Συνέχεια

7.1 Πραγματικά Περιστατικά Ασφάλειας

Στην ενότητα αυτή θα παρουσιάσουμε μερικά γνωστά περιστατικά ασφάλειας σε παγκόσμιο επίπεδο που αφορούν χρηματοπιστωτικούς αλλά και άλλου τύπου οργανισμούς.

7.1.1 Παραβίαση της Heartland Payment Systems

Η Heartland Payment Systems είναι ένας σημαντικός διαχειριστής πληρωμών μέσω πιστωτικής κάρτα και εδρεύει στο Princeton, New Jersey στις ΗΠΑ. Διαχειρίζεται περισσότερα από 11 εκατομμύρια συναλλαγές την ημέρα, και πάνω από $ 80 δισεκατομμύρια σε συναλλαγές ετησίως, καθιστώντας την το 5ο μεγαλύτερο επεξεργαστή πληρωμών στις Ηνωμένες Πολιτείες, και 9ο στον κόσμο.

Τον Οκτώβριο του 2008, άρχισε να λαμβάνει ειδοποιήσεις από τις Visa και MasterCard για παράνομη δραστηριότητα σχετικά με τις πιστωτικές κάρτες που είχαν υποστεί επεξεργασία μέσω του δικτύου πληρωμών της Heartland.

Κατά τη διάρκεια αυτών των αναφορών απάτης, η Heartland πίστευε ότι θα μπορούσε να έχει «χακευθεί», αλλά δεν ήταν σε θέση να το πει με βεβαιότητα, και αν ναι, ποια δεδομένα μπορεί να έχουν παραβιαστεί.

Λαμβάνοντας υπόψη ότι οι μέσοι όροι για τη Heartland είναι πάνω από 300 εκατομμύρια συναλλαγές κάθε μήνα (συνολικά πάνω από 6,5 δισεκατομμύρια δολάρια), καταλαβαίνει κανείς ότι το παραμικρό ίχνος «εισβολής» ή «απάτης» θα προκαλέσει μια τεράστια ανταπόκριση από παντού. Ωστόσο, η Heartland σιωπούσε για αρκετούς μήνες σχετικά με αυτή την «εν δυνάμει» εισβολή στο σύστημα επεξεργασίας της. Με τη βοήθεια ειδικών αποκαλύφθηκε τελικά η απάτη την οποία αποκάλυψε ο οργανισμός με μεγάλη καθυστέρηση.

Η πλειονότητα των δεδομένων που παραβιάστηκαν περιλαμβάνει αριθμούς πιστωτικών καρτών και ημερομηνίες λήξης, και σε ορισμένες περιπτώσεις, τα ονόματα των κατόχων της κάρτας. Επιπλέον, η παραβίαση περιελάμβανε στοιχεία που βρίσκονταν στις μαγνητικές ταινίες των πιστωτικών και χρεωστικών καρτών, το οποίο κατέστησε ευκολότερο για τους εγκληματίες να δημιουργήσουν πλαστές πιστωτικές/χρεωστικές κάρτες. Ο αριθμός των καρτών για τις οποίες οι εισβολείς απέκτησαν κάποια δεδομένα έφτανε τα 130 εκατομμύρια κάτι που αποτελεί και τη μεγαλύτερη παραβίαση δεδομένων στις Ηνωμένες Πολιτείες.

Πως όμως έγινε η παραβίαση;

Όπως κάθε έμπειρος χάκερ, οι εισβολείς της Heartland ακολούθησαν μια «πολυεπίπεδη» προσέγγιση για να επιτεθούν και να θέσουν σε κίνδυνο τα συστήματα του οργανισμού. Πρώτα, επικεντρώθηκαν στην επίθεση της περιμέτρου, και να αποκτήσουν πρόσβαση στο εταιρικό δίκτυο της Heartland. Παρότι θεωρείται πολύ εξεζητημένη επίθεση, η παραβίαση του εταιρικού δικτύου έγινε με την πολύ βασική τεχνική του SQL injection. Η «κεκρόπορτα» ήταν ένα παλιό κομμάτι κώδικα για μια web form που περιείχε μια ευπάθεια που δεν έγινε ποτέ αντιληπτή από τον εσωτερικό και εξωτερικό έλεγχο, και επιπλέον αυτός ο κώδικας παρείχε πρόσβαση στο ξεχωριστό δίκτυο επεξεργασίας πληρωμών.

Αφού ξεπέρασαν αυτό το πρώτο εμπόδιο, και «μπήκαν» στο Εταιρικό Δίκτυο της Heartland, πιστεύεται ότι οι hackers στη συνέχεια πέρασαν αρκετούς από τους επόμενους μήνες στο να καλύψουν τυχόν «ίχνη» που μπορεί να είχαν αφήσει, ενώ εισέβαλαν στο εταιρικό δίκτυο.

Από εκεί και πέρα, οι hackers μπήκαν στο Σύστημα Επεξεργασίας.

Για να σπάσει το Σύστημα Επεξεργασίας, οι hackers εγκατέστησαν αρχικά έναν καταγραφέα, ο οποίος «έπιανε» ό,τι πληκτρολογούσε κάποιος στο μολυσμένο σύστημα. Αυτό επέτρεψε στους εισβολείς να αποκτήσουν πρόσβαση σε ευαίσθητα δεδομένα όπως κωδικούς πρόσβασης και ονόματα χρηστών του συστήματος, τα οποίο μπορούσαν να χρησιμοποιηθούν στη συνέχεια για να διεισδύσουν περαιτέρω στο σύστημα επεξεργασίας. Στη συνέχεια, οι hackers εγκαταστήσει ένα «sniffer», που καταγράφει όλες τις επικοινωνίες δεδομένων στο δίκτυο, συμπεριλαμβανομένων των αριθμών των πιστωτικών καρτών, ημερομηνίες λήξης, ονόματα κατόχου της κάρτας, και ούτω καθεξής.

Αντίκτυπος

Η Heartland παρότι θεωρητικά είχε συμμόρφωση ως προς το πρότυπο PCI, τελικά παραβιάστηκε από μια στοιχειώδη επίθεση “SQL injection”. Αυτή η τεράστια παραβίαση αποτέλεσε ένα «ξύπνημα» για όλες τις εταιρίες του κλάδου.

7.1.2 Εισβολή στην τράπεζα της Ινδίας (Bank of India)

Ο χειρότερος εφιάλτης για έναν επαγγελματία της ασφάλειας πληροφοριών: Η ιστοσελίδα σας είναι hacked, και οι λογαριασμοί χρηστών είναι σε κίνδυνο.

Το 2007 πραγματοποιήθηκε επίθεση στης ιστοσελίδα της Bank of India μέσω 30 κομματιών κακόβουλου λογισμικού. Αφότου η σελίδα φορτώθηκε με κακόβουλο λογισμικό κάθε επισκέπτης που έμπαινε από το PC του μέσω unpatched browsers μολύνθηκε.

Το κακόβουλο λογισμικό στην ιστοσελίδα της Τράπεζας της Ινδίας αποτελούταν από ένα σκουλήκι (worm), πέντε Trojan downloaders, τρεις rootkits και διάφορες εφαρμογές υποκλοπής κωδικού πρόσβασης.

Σύμφωνα με την εγκληματολογική έρευνα και από τα στοιχεία που μπόρεσαν να συλλέξουν οι αρχές, βασικοί ύποπτοι δείχνουν να είναι η συμμορία του διαβόητου ρωσικού Δικτύου Επιχειρήσεων (Russian Business Network - RBN). Αυτοί θεωρούνται ως οι πλέον επικίνδυνοι κακοποιοί του διαδικτύου και εμπλέκονται σε υποθέσεις όλων των ειδών από spamming, phishing και denial-of-service επιθέσεις έως και την ώθηση παιδικής πορνογραφίας μέσω του Διαδικτύου.

Η συγκεκριμένη επίθεση εκμεταλλεύθηκε μια ευπάθεια του Internet Explorer και όλοι οι χρήστες του browser αυτού που δεν είχαν κάνει αναβάθμιση επηρεάστηκαν.

7.1.3 Απώλεια δεδομένων για την Τράπεζα της Νέας Υόρκης Mellon

Αυτό το περιστατικό διαφέρει από τα άλλα καθώς αναφέρεται σε απώλεια κρίσιμων πληροφοριών χωρίς να γίνει κάποια εισβολή στο σύστημα από hackers.

Η Bank of New York Mellon το 2008 έχασε μια μη κρυπτογραφημένη εφεδρική ταινία εκθέτοντας ενδεχομένως πληροφορίες για 4,5 εκατομμύρια πελάτες της. Η τράπεζα έδωσε μια εφεδρική ταινία χωρίς κρυπτογράφηση σε μια επιχείρηση αποθήκευσης, την

Archive Systems Inc, για να μεταφερθεί σε εγκατάσταση αποθήκευσης. Όταν το όχημα της εταιρείας φύλαξης έφτασε στις εγκαταστάσεις αποθήκευσης, η ταινία έλειπε. Οι άλλες εννέα ταινίες έφτασαν στην εγκατάσταση με ασφάλεια.

Η ταινία που έλειπε περιείχε αριθμούς κοινωνικής ασφάλισης και πληροφορίες για τραπεζικούς λογαριασμούς για 4,5 εκατομμύρια πελάτες - συμπεριλαμβανομένων αρκετές εκατοντάδες χιλιάδες καταθέτες και επενδυτές της People's United Bank, η οποία είχε δώσει στην Bank of New York Mellon τις πληροφορίες ώστε να μπορούσε να προσφέρει σε αυτούς τους καταναλωτές μια επενδυτική ευκαιρία.

Η εταιρία προσπάθησε να μπαλώσει το πρόβλημα αλλά η ζημιά για τη φήμη της ήταν δύσκολο να αποκατασταθεί καθώς χάθηκε η αξιοπιστία ως προς τους πελάτες της.

Το περιστατικό αυτό ανέδειξε το πρόβλημα της διατήρησης μη κρυπτογραφημένων αντιγράφων που τότε ήταν η συνήθης πρακτική.

7.1.4 Stuxnet

Το Stuxnet είναι μια από τις πιο περίπλοκες απειλές που έχουν εμφανιστεί ποτέ και, ταυτόχρονα, έχει προσελκύσει το ενδιαφέρον τόσο των ερευνητών, όσο και του τύπου, αποτελείται από πολλά διαφορετικά συστατικά και επιτελεί πολλές λειτουργίες. Στοχεύει στον επαναπρογραμματισμό συστημάτων ελέγχου της βιομηχανικής παραγωγής, όπως πχ σε εργοστάσια παραγωγής ηλεκτρικού ρεύματος. Πιο συγκεκριμένα ο απώτατος στόχος του είναι ο επαναπρογραμματισμός των βιομηχανικών συστημάτων ελέγχου (Industrial Control Systems – ICS), αλλάζοντας τον κώδικα των προγραμματίσιμων λογικών ελεγκτών (Programmable Logic Controllers - PLC), ούτως ώστε να τους αναγκάσει να δουλέψουν με τον τρόπο που επιθυμεί ο επιτιθέμενος, ενώ παράλληλα αυτό δεν θα είναι εμφανές στον διαχειριστή του εξοπλισμού. Οι στόχοι της επίθεσης (λέγεται ότι) βρίσκονται στο Ιράν (για αυτό άλλωστε και η πλειοψηφία των μολυσμένων συστημάτων βρίσκεται εκεί), το λογισμικό και ο εξοπλισμός που δέχτηκε την επίθεση ήταν συγκεκριμένης εταιρείας (Siemens) και οι δημιουργοί του Stuxnet (λέγεται ότι) είναι οι Ηνωμένες Πολιτείες Αμερικής και το Ισραήλ.

Για να επιτευχθεί αυτός ο στόχος οι δημιουργοί του Stuxnet συγκέντρωσαν ένα πλήθος συστατικών, για να αυξήσουν τις πιθανότητες επιτυχίας του. Έτσι, περιλαμβάνονται zero-day exploits, ένα rootkit για τα Windows, ένα rootkit για τα PLC, τεχνικές αποφυγής του

antivirus, πολύπλοκες διεργασίες για να επιτευχθεί η μόλυνση, διεπαφές εντολών και ελέγχου κ.α.

Τα κυριότερα χαρακτηριστικά και δυνατότητες του Stuxnet είναι:

- Αυτο-αναπαραγωγή σε αφαιρούμενα μέσα, εκμεταλλευόμενο ευπάθειες που επιτρέπουν την αυτόματη εκτέλεση (autorun)
- Εξάπλωση μέσω LAN, εκμεταλλευόμενο ευπάθεια στο Print Spooler των Windows
- Αντιγραφή και εκτέλεση σε απομακρυσμένους υπολογιστές, μέσω κοινών φακέλων
- Αντιγραφή και εκτέλεση σε απομακρυσμένους υπολογιστές που λειτουργούν ως WinCC database servers
- Ενημερώνεται αυτόματα σε ένα LAN μέσω peer-to-peer μηχανισμών
- Εκμετάλλευση ευπαθειών των Windows για απόκτηση περισσοτέρων δικαιωμάτων
- Χρήση Windows rootkit για απόκρυψη των δυαδικών του αρχείων (binaries)
- Χρήση του PCL rootkit για απόκρυψη του αλλαγμένου κώδικα στα PCL
- Παράκαμψη αντιβιοτικών και άλλων χαρακτηριστικών ασφαλείας.

Δεν υπάρχουν στοιχεία για το πώς εξαπολύθηκε η επίθεση. Ωστόσο, μπορούν να γίνουν εικασίες με βάση τα τεχνικά χαρακτηριστικά του Stuxnet. Στη συνέχεια θα παρουσιάσουμε ένα σενάριο επίθεσης, το οποίο, όμως, δεν απέχει και πολύ από την πραγματικότητα.

Ο χειρισμός των ICS είναι δυνατός μέσω κώδικα που βρίσκεται στα PLC και ο οποίος μοιάζει πολύ στη μορφή με assembly. Ο προγραμματισμός των PLC γίνεται με υπολογιστές με Windows οι οποίοι δεν είναι συνδεδεμένοι στο Internet. Επίσης, και τα ICS είναι απίθανο να είναι συνδεδεμένα στο Internet.

Πώς, λοιπόν, επιτίθεσαι σε κάτι που δεν είναι online; Αρχικά οι επιτιθέμενοι διεξήγαγαν μια εξερευνητική επίθεση (reconnaissance attack). Μιας και το κάθε PLC είναι παραμετροποιημένο με μοναδικό τρόπο, ο επιτιθέμενος θα χρειαστεί να έχει στην κατοχή του το σχηματικό των ICS. Αυτό μπορεί να γίνει ή με κάποια πρώιμη έκδοση του Stuxnet ή με τη χρήση άλλου malware σε προγενέστερο χρόνο ή εκ των έσω. Όταν οι επιτιθέμενοι απέκτησαν στην κατοχή τους τα συγκεκριμένα έγγραφα και, συνεπώς, τη γνώση που απαιτείται, ανέπτυξαν την τελευταία έκδοση του Stuxnet, όπου κάθε στοιχείο

του δημιουργήθηκε για συγκεκριμένο λόγο και με απώτατο σκοπό το σαμποτάρισμα του ICS.

Οι επιτιθέμενοι θα χρειάστηκε να δημιουργήσουν ένα ακριβώς ίδιο περιβάλλον (mirrored environment) που θα περιελάμβανε όλο τον εξοπλισμό, όπως τα ICS, τα PLC, τα περιφερειακά, ώστε να γίνουν οι δοκιμές του κώδικα και να είναι όσο το δυνατόν ρεαλιστικότερες. Η διαδικασία αυτή μπορεί να διήρκεσε έως και 6 μήνες και να απαιτήθηκε εργασία από 10 τουλάχιστον προγραμματιστές, χωρίς να συμπεριλαμβάνουμε στον υπολογισμό αυτό τυχόν βοηθητικό προσωπικό.

Επίσης, τα δυαδικά αρχεία που περιέχουν το malware θα πρέπει να ήταν ψηφιακά υπογεγραμμένα, ώστε να μην κινήσουν υποψίες. Για αυτό το λόγο οι επιτιθέμενοι χρησιμοποίησαν δύο ψηφιακά πιστοποιητικά, τα οποία ήρθαν στην κατοχή τους μέσω συνεργού τους ο οποίος διείσδυσε στις εγκαταστάσεις του δεχόμενου την επίθεση. Για να γίνει η μόλυνση του στόχου, το πιο πιθανό είναι να μολύνθηκε πρώτα κάποιος τρίτος, όπως πχ μια συνεργαζόμενη με τον στόχο εταιρεία που παρείχε κάποιες υπηρεσίες στον στόχο και άρα είχε πρόσβαση σε αυτόν ή κάποιος εργαζόμενος, και οι οποίοι εν αγνοία τους εισήγαγαν το λογισμικό στα συστήματά τους. Η αρχική μόλυνση μάλλον έγινε με τη χρήση αφαιρούμενης συσκευής (USB stick).

Από τη στιγμή που το Stuxnet μόλυνε έναν υπολογιστή, άρχισε να διαδίδεται στα PG, τα οποία είναι υπολογιστές που τρέχουν Windows, αλλά χρησιμοποιούνται για να προγραμματίζουν τα PLC. Επειδή οι περισσότεροι από αυτούς τους υπολογιστές δεν είναι συνδεδεμένοι σε κάποιο δίκτυο, το Stuxnet διαδόθηκε σε άλλους υπολογιστές στο τοπικό δίκτυο, εκμεταλλευόμενο zero-day ευπάθειες και μέσω αφαιρούμενων αποθηκευτικών μέσων. Η διάδοση μέσω LAN ήταν μάλλον το πρώτο βήμα εξάπλωσης του Stuxnet, ενώ τα επόμενα βήματα ήταν με τα αφαιρούμενα αποθηκευτικά μέσα, έτσι ώστε να μολυνθούν και οι μη δικτυωμένοι υπολογιστές που είχαν τα PG.

Οι επιτιθέμενοι μπορούσαν να ελέγχουν το Stuxnet μέσω ενός server ελέγχου και εντολών. Όμως, ο βασικός υπολογιστής που έπρεπε να μολυνθεί δεν είχε σύνδεση στο Internet. Συνεπώς, το ίδιο το εκτελέσιμο του Stuxnet ήταν εκείνο που θα έπρεπε να έχει ενσωματωμένη όλη εκείνη τη λειτουργικότητα που απαιτούνταν για την κατάληψη του συστήματος. Επίσης, μέσω peer-to-peer μεθόδων που εγκαταστάθηκαν από το ίδιο το Stunt, κατέστη δυνατή η ενημέρωσή του με διάφορα updates.

Τελικά, όταν το Stuxnet βρήκε τους συγκεκριμένους υπολογιστές, άλλαξε τον κώδικα στο PLC. Τα θύματα της επίθεσης δεν μπορούσαν να εντοπίσουν το πρόβλημα, δηλαδή τα αλλαγμένα PLC, γιατί το Stuxnet έκρυβε πολύ καλά τις αλλαγές που είχε κάνει. Ακόμη, το

Stuxnet, όπως είπαμε, χρησιμοποιούσε τεχνικές αυτό-αναπαραγωγής. Αυτό είχε σαν αποτέλεσμα, πέρα από τον εντοπισμό των PG, να προξενήσει πολλές παράπλευρες ζημιές, μολύνοντας υπολογιστές εκτός του οργανισμού στον οποίο εκδηλώθηκε η επίθεση. Οι επιτιθέμενοι απλά θεώρησαν αυτές τις παράπλευρες ζημιές ως αναγκαιότητα, ώστε να φτάσουν και να επιτεθούν αποτελεσματικά στο στόχο τους. Επίσης, όταν πια αποκαλύφτηκε η επίθεση, το πιο πιθανό είναι οι επιτιθέμενοι να είχαν ολοκληρώσει το έργο τους.

Το 60% των υπολογιστών που μολύνθηκαν από το Stunt βρίσκονταν στο Ιράν, κάτι που δείχνει ότι ήταν μάλλον και ο κύριος στόχος της επίθεσης.

7.1.5 TJX

Η TJX Companies, Incorporated είναι η μεγαλύτερη διεθνής εταιρεία στο χώρο της ένδυσης και της διακόσμησης εσωτερικού χώρου στις Ηνωμένες Πολιτείες. Εδρεύει στη Μασαχουσέτη και ξεκίνησε τη λειτουργία της το 1976.

Στις 17 Ιανουαρίου 2007 η ίδια η TJX ανακοίνωσε ότι είχε πέσει θύμα επίθεσης, με εισβολή μη εξουσιοδοτημένων χρηστών στα συστήματά της. Αποκάλυψε το Δεκέμβριο του 2006 ανακάλυψε ότι τα συστήματα ασφαλείας της είχαν παραβιαστεί και ότι είχαν κλαπεί δεδομένα πελατών. Η επίθεση, όμως, είχε ξεκινήσει από το Ιούλιο του 2005 και απλά έγινε αντιληπτή τόσους μήνες μετά. Οι επιτιθέμενοι απέκτησαν πρόσβαση στο σύστημα διαχείρισης και αποθήκευσης των δεδομένων των πιστωτικών και χρεωστικών καρτών, των επιταγών και άλλων συναλλαγών. Η επίθεση αυτή κρατήθηκε κρυφή, μετά από εισαγγελική εντολή. Επίσης, ανέφερε ότι ήδη συνεργαζόταν με τις διάφορες εταιρείες, όπως η IBM για την βελτίωση της ασφάλειας των συστημάτων της.

Μέχρι το Μάρτιο του 2007, περίπου 45.7 εκατομμύρια πελάτες της εταιρείας είχαν επηρεαστεί, καθιστώντας την συγκεκριμένη επίθεση ως τη μεγαλύτερη, από πλευράς έκτασης, μέχρι τότε στα χρονικά. Για 451.000 περίπου καταναλωτές ανακτήθηκαν και άλλα προσωπικά στοιχεία, όπως οι αριθμοί κοινωνικής ασφάλισης και άδειας οδήγησης. Ωστόσο, άλλοι υπολογισμοί ανεβάζουν το συνολικό αριθμό των χρηστών που επηρεάστηκαν στο διπλάσιο, δηλαδή στα 94 εκατομμύρια καταναλωτές.

Η επίθεση και η ανάκτηση των δεδομένων κατέστη εφικτή μέσω του μη ασφαλισμένου ασύρματου δικτύου ενός καταστήματος της εταιρείας. Υπολογίζεται ότι η επίθεση διήρκεσε πάνω από 18 μήνες. Πιο συγκεκριμένα, συμφωνα με την μετέπειτα έρευνα,

προέκυψε ότι οι επιτιθέμενοι μπόρεσαν και υπέκλεψαν συναλλαγές μέσω ασύρματου δικτύου μεταξύ δύο καταστημάτων που βρίσκονταν στο Μαϊάμι. Η παρακολούθηση αυτή των συναλλαγών, όχι μόνο έδωσε τη δυνατότητα στου επιτιθέμενους να αποκτήσουν πρόσβαση στις βάσεις δεδομένων της TJX, αλλά και αυτή η πρόσβαση να είναι μη ανιχνεύσιμη.

Ο ακριβής αριθμός των επιτιθέμενων δεν έχει διευκρινιστεί επακριβώς, ωστόσο για τη συγκεκριμένη επίθεση συνελήφθησαν έντεκα άτομα και ένα από αυτά καταδικάστηκε, με πολλαπλές κατηγορίες να τον βαραίνουν. Ένας άλλος συλληφθείς, πριν δικαστεί, αυτοκτόνησε, όντας σίγουρος για την καταδίκη του. Ωστόσο, όλοι οι συλληφθέντες απλά χρησιμοποίησαν δεδομένα που είχαν κλαπεί για να πραγματοποιήσουν αγορές και δεν αποδείχτηκε ποτέ ότι ήταν εκείνοι που εξαπέλυσαν την επίθεση.

Τα αποτελέσματα όλων αυτών ήταν πολλαπλά. Κατ αρχήν το κόστος για την εταιρεία ανήλθε σε περίπου 5 εκατομμύρια δολάρια, χωρίς, όμως, να υπολογίζονται παράπλευρα κόστη, όπως κλονισμός της αξιοπιστίας της κτλ. Τα στοιχεία των καρτών χρησιμοποιήθηκαν για την αγορά ηλεκτρονικών συσκευών από συγκεκριμένη αλυσίδα καταστημάτων (Wal-Mart) και οι αγορές αυτές ανήλθαν στα 8 εκατομμύρια δολάρια. Επίσης, δεκάδες τράπεζες αναγκάστηκαν να ακυρώσουν και να επανεκδώσουν όλα αυτά τα εκατομμύρια των καρτών για τα οποία κλάπηκαν τα στοιχεία, ενώ οι τράπεζες κινήθηκαν νομικά κατά της TJX διεκδικώντας αποζημίωση. Το ίδιο έπραξαν και οι πελάτες της TJX των οποίων τα στοιχεία κλάπηκαν, και το πιθανότερο είναι η δικαίωσή τους και η αποζημίωσή τους με εκπτωτικά κουπόνια και/ή μετρητά. Λόγω του μεγάλου χρονικού διαστήματος που οι επιτιθέμενοι εκτελούσαν την επίθεση, οι επιπτώσεις της εξαπλώθηκαν μέχρι το Χονγκ Κονγκ και τη Σουηδία, όπου πραγματοποιήθηκαν αγορές με στοιχεία καρτών που εκλάπησαν κατά τη συγκεκριμένη επίθεση.

7.1.6 Operation Aurora

Η Επιχείρηση Aurora (Operation Aurora) είναι ένα χαρακτηριστικότατο παράδειγμα ενός νέου και διαδεδομένου τύπου κατευθυνόμενων και περίπλοκων επιθέσεων, των Εξελιγμένων Επίμονων Επιθέσεων (Advanced Persistent Threat – APT). Οι APT χρησιμοποιούν ύπουλες τεχνικές για την απόκτηση πρόσβασης σε συστήματα, καθώς και για τη διατήρηση της πρόσβασης αυτής, έως ότου επιτευχθούν οι στόχοι του επιτιθέμενου.

Η συγκεκριμένη επίθεση ξεκίνησε από την Κίνα στα μέσα του 2009 και συνεχίστηκε μέχρι και το τέλος του ίδιου έτους. Στόχοι της ήταν πασίγνωστες εταιρείες πληροφορικής, και όχι μόνο, όπως η Google, η Adobe, η Juniper, η Yahoo, η Symantec, η Morgan Stanley κ.α. Συνολικά, πάνω από 30 εταιρείες δέχθηκαν επίθεση. Αργότερα, η εταιρεία παροχής πιστοποιητικών VeriSign ισχυρίστηκε ότι η επίθεση διαπράχθηκε είτε από στελέχη της κινεζικής κυβέρνησης, είτε από proxies στην Κίνα.

Επιπροσθέτως, πηγές της αμερικανικής πρεσβείας στην Κίνα διέρρευσαν πληροφορίες από κινεζικές πηγές, οι οποίες ισχυρίζονταν ότι όλη η επίθεση χειραγωγήθηκε από την κινεζική κυβέρνηση και ότι σκοπός της ήταν η εισβολή στα υπολογιστικά συστήματα της Google. Ακόμη, ότι η Aurora ήταν μέρος μιας γενικευμένης επιχείρησης, η οποία εκτελέστηκε από κυβερνητικές υπηρεσίες σε συνεργασία με κινέζους hackers, οι οποίοι επιστρατεύτηκαν για αυτό το λόγο. Απώτατος σκοπός της όλης επιχείρησης ήταν η απόκτηση πρόσβασης σε υπολογιστικά συστήματα της αμερικανικής κυβέρνησης.

Η Aurora δρούσε σε έξι βήματα, τα οποία όλα ήταν διαφανή στο χρήστη. Έτσι, μιας και δεν υπήρχε κάποιο προφανές σημάδι στο χρήστη, μπορούσε ανεξέλεγκτη να ολοκληρώσει τους κακόβουλους στόχους της. Τα έξι βήματα που περιελάμβανε ήταν:

1. Ο χρήστης λαμβάνει ένα σύνδεσμο (URL) με mail ή μέσω instant messaging από μία εμπιστεύσιμη πηγή.
2. Ο χρήστης κάνει κλικ στο σύνδεσμο και οδηγείται σε μια ιστοσελίδα που φιλοξενείται στην Ταιβάν, η οποία εμπεριέχει κακόβουλο κώδικα JavaScript.
3. Ο browser του χρήστη κατεβάζει και εκτελεί τον κακόβουλο κώδικα, ο οποίος εκμεταλλευόταν και ένα κενό ασφαλείας του Internet Explorer.
4. Μέσω αυτού του κενού ασφαλείας, αποθηκευόταν ένα binary αρχείο προερχόμενο από τους servers της Ταιβάν, το οποίο ήταν στη μορφή αρχείου εικόνας, και στη συνέχεια εκτελούνταν ο κακόβουλος κώδικας.
5. Η εκτέλεση του κακόβουλου κώδικα οδηγούσε στη δημιουργία μίας κερκόπορτας (backdoor), μέσω της οποίας ο υπολογιστής συνδεόταν στους servers καθοδήγησης και ελέγχου στην Ταιβάν.
6. Πλέον, οι επιτιθέμενοι είχαν πλήρη πρόσβαση στα εσωτερικά συστήματα. Στόχος τους ήταν τα συστήματα στα οποία βρίσκεται η πνευματική ιδιοκτησία των εταιρειών, όπως τα SCM συστήματα (Software Configuration Management systems), τα οποία ήταν προσβάσιμα από τους μολυσμένους υπολογιστές και μέσω αυτών των συστημάτων ήταν εφικτή και η περαιτέρω διείσδυση στο δίκτυο.

Θα πρέπει να σημειώσουμε εδώ ότι με τον όρο πνευματική ιδιοκτησία (Intellectual Property) εννοούμε όλη εκείνη την πληροφορία που κατέχει ένας οποιοσδήποτε οργανισμός, όπως εταιρικά μυστικά, στοιχεία πνευματικής ιδιοκτησίας, φόρμουλες, σήματα κατατεθέντα, πατέντες, πηγαίοι κώδικες κτλ.

Η ίδια η Google με δήλωσή της επισήμανε ότι μέρος της πνευματικής της ιδιοκτησίας εκλάπη. Συγκεκριμένα, δήλωσε ότι οι επιτιθέμενοι έδειξαν ιδιαίτερο ενδιαφέρον στην απόκτηση πρόσβασης σε λογαριασμούς Gmail, με αντιγραφή των περιεχομένων τους.

Η εκδήλωση της επίθεσης αποκαλύφθηκε δύο μέρες μετά και επισημάνθηκε ότι εκμεταλλεύτηκε ευπάθειες και κενά ασφαλείας του Internet Explorer. Μία εβδομάδα αργότερα, η Microsoft παρουσίασε τη λύση του προβλήματος και παραδέχθηκε ότι το κενό ασφαλείας το οποίο εκμεταλλεύτηκαν οι επιτιθέμενοι ήταν ήδη γνωστό σε αυτήν. Στο ενδιάμεσο διάστημα μέχρι να γίνει διαθέσιμο το fix για την επίλυση του προβλήματος, κυβερνήσεις συνέστησαν στους πολίτες τη χρήση άλλου browser.

7.2 Επιχειρησιακή Συνέχεια

Πολλοί οργανισμοί μαθαίνουν πώς να ανταποκρίνονται σε περιστατικά ασφαλείας κατά την εξέλιξη αυτών των περιστατικών. Έτσι, οι επιθέσεις αυτές καταλήγουν να είναι πολύ περισσότερο επιζήμιες και κοστοβόρες, από το αν είχαν αντιμετωπιστεί σωστά ευθύς εξ αρχής.

7.2.1 Πλάνο Επιχειρησιακής Συνέχειας

Ένα Πλάνο Επιχειρησιακής Συνέχειας (Business Continuity Plan – BCP) είναι ένα σχέδιο προληπτικών ενεργειών που πρέπει να έχει και να εφαρμόζει ένας οργανισμός, ώστε να διασφαλίζεται ότι οι κρίσιμες λειτουργίες του και/ή τα προϊόντα του θα συνεχίσουν να υφίστανται, χωρίς διακοπή, ανεξαρτήτως περιστάσεων. Κάθε BCP θα πρέπει να περιλαμβάνει:

- Σχέδια, μέτρα και διαδικασίες που να διασφαλίζουν την απρόσκοπτη λειτουργία κρίσιμων εργασιών του οργανισμού, έτσι ώστε να είναι σε θέση να αναρρώνει μετά από ατυχή περιστατικά ή επιθέσεις.

- Αναγνώριση των απαραίτητων πόρων του οργανισμού, συμπεριλαμβανομένων του προσωπικού, των πληροφοριών, του εξοπλισμού, της υποδομής, κτλ.

Ένα BCP ενισχύει το προφίλ ενός οργανισμού και στους εργαζομένους σε αυτόν και στους μετόχους και στους πελάτες, επιδεικνύοντας μια υπεύθυνη και προληπτική πολιτική. Επίσης, αυξάνει τη συνολική αποδοτικότητα του οργανισμού, με την αναγνώριση των σχέσεων που διέπουν τους πόρους του οργανισμού με τον ανθρώπινο παράγοντα.

Κάθε οργανισμός έρχεται αντιμέτωπος με διάφορες επικίνδυνες για αυτόν καταστάσεις, οι οποίες περιλαμβάνουν:

- Φυσικές καταστροφές (πλημμύρες, σεισμοί, κτλ)
- Ατυχήματα
- Σαμποτάζ
- Διακοπές ηλεκτροδότησης
- Περιβαλλοντικές καταστροφές (μόλυνση από ραδιενέργεια κτλ)
- Κυβερνοεπιθέσεις και επιθέσεις από hackers.

Ένα BCP αποτελείται από πέντε μέρη, τα όποια θα αναλύσουμε στη συνέχεια:

1. Ηγεσία του BCP (BCP Governance)
2. Ανάλυση επίδρασης στις λειτουργίες του οργανισμού (Business Impact Analysis - BIA)
3. Σχέδια, μέτρα και διεργασίες για επιχειρησιακή συνέχεια
4. Διαδικασίες Ετοιμότητας
5. Μέθοδοι ελέγχου ποιότητας (ασκήσεις ετοιμότητας, auditing, κτλ)

BCP Governance

Ένα BCP θα πρέπει να περιγράφει τη μορφή και την ιεραρχία μιας ομάδας ή επιτροπής και να καθορίζει τους ρόλους των μετεχόντων σε αυτήν ομάδα. Αυτή η ομάδα είναι υπεύθυνη για την επίβλεψη, την εκκίνηση, το σχεδιασμό, την έγκριση, τη δοκιμή και την παρακολούθηση του BCP. Είναι επίσης αυτή που εφαρμόζει το BCP, συντονίζει τις ενέργειες, εγκρίνει την BIA, επιβλέπει το σχεδιασμό των σχεδίων και αναλύει τα αποτελέσματα

Οι ηγέτες αυτής της ομάδας αναλαμβάνουν τις εξής ευθύνες:

- Έγκριση της δομής και της ιεραρχίας της BCP ομάδας
- Αποσαφήνιση των ρόλων των συμμετεχόντων
- Επίβλεψη των επιμέρους ομάδων
- Ορισμός της στρατηγικής κατεύθυνσης και των αρχών που τη διέπουν
- Έγκριση των αποτελεσμάτων της BIA
- Έγκριση των σχεδίων επιχειρησιακής συνέχειας που θα εκπονηθούν
- Επίλυση πιθανών αντικρουόμενων απαιτήσεων και καθορισμός προτεραιοτήτων.

Η BCP ομάδα συνήθως έχει τα ακόλουθα μέλη:

- Υπεύθυνος εκτέλεσης του BCP: Έχει την ευθύνη για όλη την ομάδα και είναι ο καθοδηγητής της.
- Συντονιστής του BCP: Υπολογίζει τους απαιτούμενους πόρους, αναπτύσσει την πολιτική, συντονίζει και επιβλέπει την BIA διαδικασία, διασφαλίζει την αποτελεσματικότητα των μελών, συντονίζει και επιβλέπει τα σχέδια και τις διαδικασίες, ορίζει τις επιμέρους ομάδες και καθορίζει τις αρμοδιότητές τους, συντονίζει την εκπαίδευση όλων των μελών και παρέχει συνεχώς την αξιολόγηση του BCP.
- Υπεύθυνος Ασφαλείας: Συνεργάζεται με το συντονιστή του BCP, ώστε να διασφαλιστεί ότι όλες οι παράμετροι του BCP ακολουθούν τις πολιτικές ασφαλείας του οργανισμού
- Επικεφαλής του IT: Συνεργάζεται με το συντονιστή και την Υπηρεσία Πληροφορικής για την υλοποίηση των σχεδίων
- Στελέχη του οργανισμού που παρέχουν τα δεδομένα και αξιολογούν τα αποτελέσματα της BIA.

7.2.2 Ανάλυση Επιχειρησιακών Επιπτώσεων

Ο σκοπός της Ανάλυσης Επιχειρησιακών Επιπτώσεων (**Business Impact Analysis – BIA**) είναι να αναγνωριστούν τα απαραίτητα και κρίσιμα για τον οργανισμό προϊόντα και υπηρεσίες, να καθοριστεί η σημαντικότητα του καθενός και να δοθεί η αντίστοιχη προτεραιότητα επαναφοράς και να αναγνωριστούν οι επιπτώσεις της διακοπής ομαλής λειτουργίας του οργανισμού.

Αρχικά θα πρέπει να αναγνωριστούν τα προϊόντα και οι υπηρεσίες, που πρέπει σε κάθε περίπτωση να προσφέρονται από τον οργανισμό. Επ' αυτού, μπορούν να αντληθούν πληροφορίες από την αποστολή του οργανισμού και από νομικούς περιορισμούς. Αν ο οργανισμός προσφέρει πολλά προϊόντα ή υπηρεσίες, θα πρέπει να ιεραρχηθούν με βάση την ελάχιστη αποδεκτή παραγωγή του προϊόντος και το μέγιστο χρονικό διάστημα μη προσφοράς της υπηρεσίας, πριν ο οργανισμός αντιμετωπίσει σοβαρότατα προβλήματα.

Στη συνέχεια πρέπει να προσδιοριστούν οι επιπτώσεις της διακοπής των παρεχόμενων προϊόντων και υπηρεσιών. Θα πρέπει, δηλαδή, να διαπιστωθεί για πόσο χρόνο ο οργανισμός μπορεί να λειτουργήσει χωρίς κάποιο από αυτά και ποιο είναι το χρονικό διάστημα διακοπής λειτουργίας, που οι πελάτες του οργανισμού μπορούν να αποδεχθούν. Επίσης, σημαντική παράμετρος είναι και το χρονικό διάστημα που θα περάσει μέχρι οι πελάτες του οργανισμού να αναγνωρίσουν ότι υφίσταται πρόβλημα.

Ακόμη, θα πρέπει να εντοπιστούν εκείνες οι διεργασίες και οι λειτουργίες του οργανισμού, η διακοπή των οποίων έχει τη μεγαλύτερη οικονομική επίπτωση. Για παράδειγμα, αν διακοπεί μία λειτουργία, θα υπάρξει απώλεια εσόδων; Και αν ναι, πόση είναι αυτή; Αν ο πελάτης δεν μπορούν να έχουν πρόσβαση σε συγκεκριμένα προϊόντα και υπηρεσίες, θα απευθυνθούν σε κάποιον ανταγωνιστή προξενώντας περαιτέρω απώλειες; Ενδεχομένως να χρειαστεί πρόσληψη νέου προσωπικού και η κλήση εξωτερικών συνεργατών, εξειδικευμένων σε επίλυση τέτοιου είδους προβλημάτων. Πόσο θα είναι το επιπλέον κόστος; Θα υπάρξουν ποινές και πρόστιμα λόγω νομικών υποχρεώσεων ή συμφωνιών του οργανισμού; Πέρα, βέβαια, από τις μετρήσιμες απώλειες εσόδων, υπάρχουν και ζημιές οι οποίες δεν ποσοτικοποιούνται. Αυτές είναι οι επιπτώσεις στη φήμη, η μείωση της ανταγωνιστικότητας, οι απώλειες στην τιμή των μετοχών και γενικότερα η υποβάθμιση της προς τα έξω εικόνας του οργανισμού.

Σημαντική παράμετρος της BIA είναι η ιεράρχηση των κρίσιμων υπηρεσιών και των σημαντικότερων προϊόντων, που γίνεται αφού ολοκληρωθεί η συλλογή των πληροφοριών που τα αφορούν. Η ιεράρχηση γίνεται με βάση τις πιθανές απώλειες εσόδων, τον χρόνο επαναφοράς και τη σημαντικότητα της ζημιάς που θα προξενηθεί. Ακολούθως,

καθορίζονται τα ελάχιστα επίπεδα εξυπηρέτησης και οι μέγιστοι χρόνοι μη παροχής προϊόντων-υπηρεσιών.

7.2.3 Προληπτικά μέτρα

Σχεδιασμός επιχειρησιακής συνέχειας

Σε αυτό το βήμα προετοιμάζουμε λεπτομερώς τα σχέδια αντίδρασης και επαναφοράς, που διασφαλίζουν την επιχειρησιακή συνέχεια. Κατ αρχήν οι κίνδυνοι και οι απειλές θα πρέπει να περιγράφονται είτε στην BIA, είτε σε μία πλήρη και αναλυτική εκτίμηση απειλών-κινδύνων. Επίσης, η μείωση της πιθανότητας εμφάνισης αυτών των κινδύνων πρέπει να είναι συνεχής διαδικασία και να γίνεται ακόμα και αν το BCP δεν έχει ενεργοποιηθεί. Για παράδειγμα, αν η παραγωγή μας βασίζεται στην ηλεκτρική ενέργεια, μπορούμε να μειώσουμε την πιθανότητα η εταιρεία μας να διακόψει την παραγωγή λόγω διακοπής ρεύματος, αγοράζοντας μια γεννήτρια.

Στη συνέχεια θα πρέπει να δημιουργήσουμε τα σχέδια συνέχειας, βασιζόμενοι στα αποτελέσματα της BIA. Αυτά θα πρέπει να είναι κλιμακούμενα, ανάλογα με τη σοβαρότητα του περιστατικού που αντιμετωπίζεται. Για παράδειγμα, αλλιώς θα αντιμετωπιστεί μία πλημμύρα με νερό στάθμης ενός εκατοστού, αλλιώς μισού μέτρου. Με βάση αυτά τα σχέδια θα πρέπει να δημιουργηθούν ομάδες με συγκεκριμένες αρμοδιότητες και υποχρεώσεις και να εκπαιδευθούν σχετικά με το πώς πρέπει να αντιδράσουν σε περίπτωση εφαρμογής του BCP.

Ειδικά σε περιπτώσεις οργανισμών που κατέχουν σημαντικό αριθμό πληροφοριακών συστημάτων, η βέλτιστη πρακτική είναι να υπάρχει και ένα δεύτερο site, όπου θα υπάρχει και εκεί εξοπλισμός (disaster site). Υπάρχουν τρεις τύποι disaster site:

- Cold Site: ένα εναλλακτικό site, που δεν είναι άμεσα λειτουργικό, αλλά θα πρέπει να περάσει αρκετό διάστημα (μέρες) μέχρι να γίνει πλήρως λειτουργικό. Είναι η φθηνότερη λύση.
- Warm Site: σχεδόν απολύτως εξοπλισμένο και σχεδόν άμεσα (εντός ωρών) λειτουργικό. Αποτελεί μια μέση λύση.
- Hot Site: πλήρως εξοπλισμένο, άμεσα λειτουργικό, και συχνά πλήρως επανδρωμένο. Μπορούν να ενεργοποιηθούν εντός λεπτών, αλλά είναι και η ακριβότερη λύση.

Διαδικασίες ετοιμότητας

Στην απευκταία περίπτωση που πρέπει να ενεργοποιηθεί το BCP, αυτό μπορεί να εκτελεστεί ομαλά και αποδοτικά αν προηγουμένως έχουμε ενημερώσει όλους τους εργαζομένους και το προσωπικό σχετικά με τα περιεχόμενα του BCP και είναι πλήρως ενημερωμένοι σχετικά με τις ατομικές τους αρμοδιότητες. Επίσης, το συγκεκριμένο προσωπικό θα πρέπει να είναι εκπαιδευμένο σχετικά με τις αρμοδιότητες του και θα πρέπει να είναι όσο το δυνατόν περισσότερο ενημερωμένο για τις εργασίες των υπόλοιπων ομάδων.

Αφού ολοκληρωθεί η ενημέρωση και η εκπαίδευση των στελεχών, θα πρέπει να προγραμματιστούν και να εκτελεστούν ασκήσεις ετοιμότητας, ώστε να επιτευχθούν τα επιθυμητά επίπεδα ετοιμότητας. Παρόλο που είναι αρκετά χρονοβόρα και κοστοβόρα, είναι ο καλύτερος τρόπος για να ελεγχθεί η αποτελεσματικότητα ενός BCP.

Μέθοδοι ελέγχου ποιότητας

Μετά το σχεδιασμό και τη δοκιμαστική εκτέλεση του BCP θα πρέπει να αξιολογηθεί η ακρίβεια και η αποτελεσματικότητά του. Επίσης, θα πρέπει να διευκρινιστεί ποια είναι τα σημεία του BCP που επιδέχονται βελτίωσης. Υπάρχουν δύο τρόποι για να επιτευχθεί αυτό: είτε με εσωτερική αξιολόγηση, είτε με εξωτερικό έλεγχο.

Όσον αφορά την εσωτερική αξιολόγηση, συνίσταται ο οργανισμός να αξιολογεί το BCP:

- Σε τακτά χρονικά διαστήματα (μία ή δύο φορές το χρόνο)
- Όταν διαπιστώνονται αλλαγές στους κινδύνους του περιβάλλοντος
- Όταν συμβούν σημαντικές αλλαγές στον οργανισμό
- Μετά από κάποια άσκηση, για να εφαρμοστούν οι αλλαγές.

Σε περίπτωση εξωτερικού ελέγχου, οι σύμβουλοι που προσλαμβάνουμε επιβεβαιώνουν:

- Τις διαδικασίες που χρησιμοποιούνται για να καθορίσουν τις κρίσιμες υπηρεσίες και διεργασίες
- Τη μεθοδολογία, την ακρίβεια και την διεξοδικότητα του BCP.

7.2.4 Μέτρα αντιμετώπισης περιστατικού

Μέχρι τώρα αναλύσαμε τις ενέργειες στις οποίες πρέπει να προβεί προληπτικά ο οργανισμός πριν προκύψει κάποιο ατυχές περιστατικό. Τι πρέπει να κάνει, όμως, αφού βρεθεί σε αυτή τη δυσχερή θέση;

Όταν συμβεί κάποια διατάραξη στην ομαλή λειτουργία του οργανισμού, θα πρέπει να ακολουθηθούν τρία βήματα:

1. Αντίδραση
2. Συνέχιση των κρίσιμων και σημαντικών διεργασιών
3. Ανάνηψη και επαναφορά σε κατάσταση ομαλής λειτουργίας.

Ας δούμε τώρα αναλυτικότερα αυτά τα επιμέρους βήματα.

Αντίδραση

Αρχικά θα πρέπει συσταθούν οι ομάδες και να αναπτυχθούν τα μέτρα, τα σχέδια και οι διαδικασίες. Σε αυτή τη φάση, τη φάση της αντίδρασης, εκτελούνται τα εξής:

- Διαχείριση του περιστατικού: περιλαμβάνει την ενημέρωση όλου του προσωπικού, τον υπολογισμό της έκτασης του προβλήματος και του εύρους των ζημιών, την εφαρμογή των σχεδίων, την εξακρίβωση πιθανών διακοπών λειτουργίας εξοπλισμών-διαδικασιών και το συντονισμό τόσο των εσωτερικών, όσο και των εξωτερικών υποστηρικτικών ομάδων.
- Επικοινωνιακή Διαχείριση: Είναι απαραίτητη για τον περιορισμό των φημών, την επικοινωνία με τα Μέσα Μαζικής Ενημέρωσης, τους προμηθευτές και τους πελάτες και τον καθησυχασμό των εργαζομένων, των πελατών και εν γένει της κοινής γνώμης.
- Διαχείριση Ενεργειών: Μπορούμε να δημιουργήσουμε ένα Κέντρο Έκτατων Επιχειρήσεων (Emergency Operation Center – EOC) για να διαχειριστούμε καλύτερα τις ενέργειες που πρέπει να γίνουν. Έχοντας ένα κεντροποιημένο EOC, όπου οι πληροφορίες και οι πόροι μπορούν ευκολότερα να συντονιστούν, να διαχειριστούν και να καταγραφούν, επιτυγχάνουμε τη διασφάλιση αποτελεσματικής και ακριβούς αντίδρασης.

Συνέχιση των κρίσιμων και σημαντικών διεργασιών

Στο δεύτερο βήμα διασφαλίζουμε ότι όλες οι χρονικά ευαίσθητες και κρίσιμες υπηρεσίες ή προϊόντα του οργανισμού συνεχίζουν να προσφέρονται απρόσκοπτα και δεν διακόπτονται για χρονικό διάστημα πέραν του προαποφασισθέντος.

Ανάνηψη και επαναφορά σε κατάσταση ομαλής λειτουργίας

Ο στόχος της ανάνηψης και επαναφοράς των λειτουργιών περιλαμβάνει:

- Την επανατοποθέτηση του προσωπικού
- Την απόφαση για το αν πρέπει να επιδιορθωθούν οι εγκαταστάσεις, αν πρέπει να μεταφερθούν αλλού ή αν πρέπει να φτιαχτούν άλλες
- Την απόκτηση επιπλέον πόρων απαραίτητων για την επαναφορά των λειτουργιών του οργανισμού

Επαναφορά σε κανονική λειτουργία, όπως ήταν πριν τη διακοπή τους.

ΚΕΦΑΛΑΙΟ 8

Σύνοψη, η κατάσταση στις Ελληνικές τράπεζες και οι μελλοντικές τάσεις στο χώρο της ασφάλειας

8.1 Σύνοψη

Στα προηγούμενα κεφάλαια παρουσιάσαμε αρκετές πτυχές του προβλήματος της ασφάλειας πληροφοριών σε οργανισμούς και ιδιαίτερα σε τραπεζικούς οργανισμούς.

Στο Κεφάλαιο 1 κάναμε μια εισαγωγή στην ασφάλεια πληροφοριών και περιγράψαμε την κατάσταση στην ασφάλεια τραπεζικών ιδρυμάτων. Στη συνέχεια παρουσιάσαμε τις κυριότερες απειλές για τους οργανισμούς όπως εμφανίζονται βάσει μελετών και αναλύσαμε τη σημασία της ασφάλειας για την υπηρεσία του internet banking. Τέλος εντοπίσαμε τις διαφοροποιήσεις που έχει η μελέτη της ασφάλειας σε τραπεζικούς οργανισμούς σε σχέση με άλλα είδη οργανισμών, π.χ. τηλεπικοινωνίες, και τους λόγους που πρέπει να δίνεται ιδιαίτερη σημασία στην ασφάλεια χρηματοπιστωτικών ιδρυμάτων.

Στο Κεφάλαιο 2 αναλύουμε τα διεθνή πρότυπα ασφάλειας οργανισμών που εφαρμόζονται σε κάθε είδους οργανισμό. Αρχικά κάνουμε μια εισαγωγή στις έννοιες όπου πρωτοεμφανίζεται και ο όρος ΣΔΑΠ δηλαδή Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών. Στη συνέχεια αναλύουμε το πρότυπο ISO/IEC 17799 (ή αλλιώς ISO/IEC 27002) που αποτελεί τον Κώδικα Πρακτικής για υλοποίηση ενός ΣΔΑΠ, και έπειτα παρουσιάζουμε το ISO/IEC 27001 που αποτελεί πρότυπο πάνω στο οποίο μπορεί να γίνει πιστοποίηση του οργανισμού από εξωτερικό φορέα.

Στο Κεφάλαιο 3 παρουσιάζονται ζητήματα που αφορούν καθαρά τον τραπεζικό κλάδο. Αυτά είναι η κανονιστική συμμόρφωση με την Πράξη Διοικητή ΤτΕ 2577, η Αρχή Προστασίας Προσωπικών Δεδομένων, και το διεθνές πρότυπο PCI DSS που αφορά τραπεζικές συναλλαγές με χρήση κάρτας.

Στο Κεφάλαιο 4 παρουσιάζονται οι πολιτικές ασφάλειας σε έναν οργανισμό που πρέπει να βασίζονται στα διεθνή πρότυπα και στην όποια κανονιστική συμμόρφωση. Αρχικά δημιουργείται ένα υποστηρικτικό περιβάλλον για να υλοποιήσει τις πολιτικές αυτές τις οποίες πρέπει στη συνέχεια να δομήσει ο οργανισμός αναλύοντας τους κινδύνους και

αναθέτοντας τις ευθύνες. Στο τέλος του κεφαλαίου δημιουργούμε μια τέτοια πολιτική έχοντας ως παράδειγμα την πολιτική ασφάλειας του IP Network.

Στο Κεφάλαιο 5 γίνεται μια πιο τεχνική ανάλυση των κινδύνων αλλά και των μηχανισμών προστασίας που έχουν εμφανιστεί σε πραγματικά πληροφοριακά συστήματα. Ενδεικτικά αναφέρονται τεχνολογίες όπως Active directory-Kerberos, Port security, VPN, IPSEC, SSL, DMZ, Firewalls, IPS-IDS, Antivirus, EFS-Bitlocker, PKI, CAs.

Στο Κεφάλαιο 6 παρουσιάζονται θέματα εσωτερικού ελέγχου όπως είναι οι μεθοδολογίες που χρησιμοποιούνται, ο διαχωρισμός των κινδύνων, τα πεδία ελέγχου, οι στόχοι του ελέγχου και οι διάφορες προσεγγίσεις.

Τέλος στο Κεφάλαιο 8 αρχικά αναφέρουμε κάποια γνωστά περιστατικά ασφάλειας και στη συνέχεια παρουσιάζουμε ζητήματα επιχειρησιακής συνέχειας.

8.2 Οι Ενέργειες των Ελληνικών Τραπεζών

Οι τραπεζικοί οργανισμοί στην Ελλάδα όπως και σε όλες τις προηγμένες χώρες προσπαθούν να αυξήσουν το επίπεδο ασφάλειας πληροφοριών επενδύοντας μεγάλα ποσά για την υλοποίηση πολιτικών ασφαλείας, ΣΔΑΠ, την ύπαρξη προσωπικού για την εφαρμογή των πολιτικών, τους ειδικούς ασφάλειας για πιστοποίηση των οργανισμών, τον απαραίτητο τεχνολογικό εξοπλισμό, και για τον εσωτερικό έλεγχο των διαδικασιών ασφάλειας.

Σχεδόν όλες οι ελληνικές τράπεζες από τις πιο μεγάλες έως και τις πιο μικρές έχουν αποκτήσει πιστοποίηση από αναγνωρισμένους οργανισμούς πιστοποίησης ως προς το πρότυπο ISO 27001 με πρώτης από όλες την Eurobank. Αυτό είναι σημαντικό για την εικόνα τους και ενδιαφέρει και τους πελάτες αλλά και τους μετόχους. Για παράδειγμα η TÜV HELLAS έχει πιστοποιήσει την Τράπεζα Πειραιώς αλλά και την Αχαϊκή Συνεταιριστική Τράπεζα. Η Εθνική έχει πιστοποιηθεί μέσω της θυγατρικής της ETHNODATA από την TUV Rheinland. Όλες οι άλλες τράπεζες (π.χ. Alpha, Emporiki κλπ.) έχουν επίσης πιστοποίηση 27001.

Ως προς το πρότυπο PCI DSS που αφορά την ασφάλεια συναλλαγών με κάρτα, η μόνη τράπεζα που έχει πιστοποιηθεί είναι η τράπεζα Πειραιώς. Αυτό μπορεί να της κόστισε και σε χρήμα και σε ευελιξία ως προς τις υπηρεσίες, όμως παράλληλα της δίνει ένα επιπλέον κύρος στην αγορά ως πρωτοπόρος στην ασφάλεια πληροφοριών. Το πρότυπο PCI DSS

θα επιτρέψει στην Τράπεζα να εξασφαλίσει την άμεση πιστοποίηση της πλειοψηφίας των εμπόρων, επιχειρήσεων και οργανισμών που συνεργάζονται μαζί της στον τομέα της εκκαθάρισης ηλεκτρονικών συναλλαγών χωρίς κάποια περαιτέρω ενέργεια εκ μέρους τους, ενώ την ίδια στιγμή έχει ήδη ξεκινήσει διαδικασία ενημέρωσης όσων εκ των συνεργατών της Τράπεζας έχουν υλοποιήσει πιο σύνθετες λύσεις ηλεκτρονικών πληρωμών που απαιτούν πιστοποίηση PCI DSS και από τους ιδίους. Η πιστοποίηση κατά PCI DSS διενεργήθηκε από την TrustWave Ltd, από τους κορυφαίους παρόχους λύσεων ασφάλειας και πιστοποιήσεων.

Ως προς τις τεχνολογίες οι οργανισμοί προσπαθούν να υλοποιήσουν όσο περισσότερους μηχανισμούς προστασίας μπορούν ώστε να αυξήσουν το επίπεδο ασφάλειας. Δεδομένη θεωρείται από όλες τις τράπεζες η χρήση SSL για το internet banking. Επίσης σημαντική χρήση έχουν και οι τεχνολογίες ασφάλειας όπως VPN, Firewalls και PKI.

Τέλος, δεδομένη θεωρείται η κανονιστική συμμόρφωση των οργανισμών με την Πράξη Διοικητή 2577 και με την Αρχή Προστασίας Προσωπικών Δεδομένων όπως επίσης δεδομένη είναι η χρήση ελεγκτικών μηχανισμών τόσο από ειδικό τμήμα του οργανισμού όσο και από εξωτερικούς φορείς.

8.3 Οι μελλοντικές τάσεις στο χώρο της ασφάλειας

Η τεχνολογική υποδομή γίνεται όλο και πιο πολύπλοκη, πιο δύσκολη να την ελέγξει κανείς, και γεμάτη από «μαύρα κουτιά» που συχνά δεν είναι κατανοητά για τους χρήστες. Παρακάτω παρουσιάζονται σχετικές νέες τάσεις που έχουν επιπτώσεις στην ασφάλεια των πληροφοριών και της ιδιωτικής ζωής. Μερικές από αυτές δεν είναι απαραίτητα νέες αλλά έχουν ήδη μεγάλη ιστορία αλλά παράλληλα έχουν και μέλλον.

1. *Η αύξηση της αλληλεξάρτησης μεταξύ των κοινωνικών διαδικασιών και των συστημάτων πληροφοριών.* Η όλο και μεγαλύτερη ενσωμάτωση της τεχνολογίας της πληροφορικής στην καθημερινότητά των πολιτών δημιουργεί εξάρτηση μεταξύ των υποδομών και των κοινωνικών διαδικασιών. Όσο πιο πολύπλοκη και τρωτή από κινδύνους γίνεται η τεχνολογία αντίστοιχα συμβαίνει και με την καθημερινότητά μας.
2. *Αναδύονται νέες αλληλεξαρτήσεις μεταξύ των οργανισμών και του κράτους.* Για παράδειγμα, αν οι κρίσιμες λειτουργίες των δημόσιων οργανισμών διασκορπίζονται γύρω από διάφορες χώρες και εξετάζονται από διάφορες

ιδιωτικές εταιρείες (για παράδειγμα, ως συνέπεια της εξωτερικής ανάθεσης), τα δημόσια ιδρύματα θα εξαρτώνται από την καταλληλότητα των πρακτικών άλλων φορέων. Εδώ, επίσης, οι διαφορετικές κανονιστικές πολιτικές και νομικές δομές μπορεί να έχουν σημαντική επίδραση στην αυτονομία των δράσεων των θεσμικών οργάνων.

3. *Τα θέματα ασφάλειας των πληροφοριών γίνονται πιο διεθνή.* Η παγκοσμιοποίηση της ασφάλειας των πληροφοριών γίνεται παράλληλα με τις οικονομικές και κοινωνικές διαδικασίες της παγκοσμιοποίησης.

4. *Αυξάνεται η ανάγκη για διαχείριση ιδιωτικών ή εμπιστευτικών πληροφοριών σε πληροφοριακά περιβάλλοντα.* Η δημιουργία ψηφιακού περιεχομένου από τη μία πλευρά και των ψηφιακών αποτυπωμάτων από την άλλη επεκτείνονται, ενώ οι αρχικοί συγγραφείς έχουν συχνά λίγο έλεγχο πάνω στη μεταγενέστερη χρήση των πληροφοριών τους. Τα άτομα παράγουν περιεχόμενο και ίχνη, αλλά θα μπορούσαν επίσης να είναι αντικείμενα των ενεργειών άλλων ατόμων (για παράδειγμα, σε εικόνες που λαμβάνονται από άλλους).

5. *Η προστασία των δεδομένων προσωπικού χαρακτήρα γίνεται ένα σημαντικό πολιτικό ζήτημα.* Στις μελλοντικές συζητήσεις πιθανότατα θα τεθούν ερωτήσεις για το πώς να υλοποιηθούν τα νομικά και ηθικά δικαιώματα στο γρήγορα εξελισσόμενο περιβάλλον των επικοινωνιών, και εάν τα νομικά και τεχνικά μέσα γενικά είναι επαρκή. Η υλοποίηση των δικαιωμάτων προσωπικών δεδομένων μπορεί να απαιτεί τα άτομα να γνωρίζουν εκ των πραγμάτων, τι πληροφορίες γι αυτούς πρέπει να αποθηκεύονται, που αποθηκεύονται, και πώς γίνεται η επεξεργασία και διανομή. Οι απαιτήσεις αυτές θα μπορούσαν να ικανοποιηθούν, για παράδειγμα, με νέες τεχνολογικές λύσεις και υπηρεσίες για τη διαχείριση προσωπικών δεδομένων.

6. *Γίνεται όλο και πιο δύσκολο να εξασφαλισθεί η ορθότητα των πληροφοριών*. Ο αυξανόμενος όγκος των πληροφοριών, οι πολλές διαφορετικές πηγές και η μεγάλη πολυπλοκότητα κάνουν πιο δύσκολο να ελεγχθεί η ορθότητα.

7. *Η ορθότητα των πληροφοριών γίνεται ολοένα και πιο σημαντική*.

8. *Αυξάνεται η συγκέντρωση δεδομένων.* Πολλά από τα δεδομένα (διαφόρων ειδών) είναι διαθέσιμα για διάφορους κοινωνικούς φορείς, όπως επιχειρήσεις, δημόσιες αρχές κ.λπ. Οι νέες πληροφορίες παρέχουν ευκαιρίες για την ανάπτυξη υπηρεσιών και επιχειρηματικών δράσεων. Δεδομένου ότι οι πληροφορίες που

συλλέγονται αποδεικνύονται πολύτιμες από οικονομική άποψη ή για τη δημόσια διαχείριση, αυξάνονται τα κίνητρα για τη χρήση των πληροφοριών ώστε να αποκτήσει κανείς κοινωνικά, οικονομικά ή πολιτικά οφέλη.

9. *Αυξάνεται ο συνδυασμός δεδομένων από διάφορες πηγές.* Αυτό παρέχει νέες ευκαιρίες για εμπορικούς σκοπούς και την ανάπτυξη υπηρεσιών, αλλά μπορεί κάλλιστα να απειλήσει την ιδιωτική ζωή.

10. *Αυξάνεται η ικανότητα εντοπισμού των προσώπων και των αγαθών*. Η ιχνηλασιμότητα των προσώπων και των αγαθών αυξάνεται λόγω των νέων τεχνολογιών αισθητήρων και τις αυξανόμενες τάσεις στην συλλογή και αποθήκευση δεδομένων, τα συστήματα επιτήρησης και με τη χρήση υπηρεσιών που περιλαμβάνουν τεχνολογία πληροφορικής. Η ικανότητα εντοπισμού των ατόμων (π.χ. πελάτες) και των αγαθών είναι μια πιθανή πηγή για οικονομική αποδοτικότητα και νέες καινοτόμες υπηρεσίες. Όμως, η νομική προστασία της ιδιωτικής ζωής και οι απαιτήσεις προστασίας των δεδομένων θα μπορούσε να περιορίσει τη χρήση της τεχνολογίας ΙΤ για σκοπούς εντοπισμού.

11. *Αυξάνονται οι κακόβουλες ενέργειες κατά συστημάτων πληροφοριών.* Οι επιθέσεις κακόβουλου λογισμικού αυξάνονται συνεχώς και γίνονται όλο και πιο σύνθετες. Νέες μορφές επιθέσεων εμφανίζονται όπως ακτιβισμός (hactivism), κυβερνοπόλεμος (cyberwar) και άλλα. Έτσι και η ασφάλεια πρέπει να προσαρμοστεί σε τέτοιου είδους επιθέσεις.

12. *Ζητήματα ποιότητας και ασφάλειας λαμβάνονται όλο και περισσότερο υπόψη στην ανάπτυξη λογισμικού.*

13. *Τα συστήματα Αυτοματισμού / αυτόνομα συστήματα χρησιμοποιούνται όλο και περισσότερο για την επίτευξη της ασφάλειας*. Τα συστήματα αυτά χρησιμοποιούνται όλο και πιο πολύ ώστε να εξαλειφθεί ο ανθρώπινος παράγοντας με τις αρνητικές επιπτώσεις που έχει για την ασφάλεια. Όμως τελικά αυτά τα συστήματα έχει γίνει πλέον εύκολο να τα εκμεταλλευτούν οι εισβολείς. Η πρόκληση για αυτούς είναι να αποφύγουν τον εντοπισμό τους.

14. Η διαθεσιμότητα των κυβερνητικών, δημοτικών και άλλων ειδών πληροφοριών που συλλέγονται από δημόσιους οργανισμούς αυξάνει όσο οι δημόσιες πηγές πληροφόρησης είναι ανοιχτές για τους πολίτες, τους ερευνητές και για εμπορικούς σκοπούς.

15. *Εμπορικά συμφέροντα οδηγούν φορείς στο να περιορίσουν την πρόσβαση σε ιδιόκτητες πηγές πληροφόρηση.*
16. *Η διακυβέρνηση της πρόσβασης σε πόρους πληροφοριών σε οργανισμούς γίνεται όλο και πιο δύσκολη.*

ΟΡΟΛΟΓΙΑ

Consumerization	Η εφαρμογή των προϊόντων πληροφορικής από τους καταναλωτές στους οργανισμούς
Mobile banking	Κινητή τραπεζική
Internet banking	Διαδικτυακή τραπεζική
Information Technology	Τεχνολογία Πληροφοριών
Trade-off	Αντιστάθμιση θετικών και αρνητικών παραγόντων
endpoints	Τερματικά σημεία
Patch	«Μπάλωμα» λογισμικού
hacker	Εισβολείς στα πληροφοριακά συστήματα
man-in-the-browser attack	Τύπος επίθεσης με χρήση «Δούρειου Ίππου»
Trojan Horse	Δούρειος Ίππος
botnet	Δίκτυο ελεγχόμενο από χάκερς
Malware	Κακόβουλο λογισμικό
phising	Υποκλοπή – «ψάρεμα» εμπιστευτικών πληροφοριών όπως username και password
vishing	Phising μέσω φωνής
smishing	Phising μέσω SMS
spear phishing	Επιθέσεις phising σε μεμονωμένα άτομα ή οργανισμούς
account takeover	Απόκτηση ελέγχου λογαριασμού
insider	Εσωτερικός παράγοντας κινδύνου
Laptop	Φορητός υπολογιστής
WEB 2.0	Κατηγορία τεχνολογιών διαδικτύου νέας γενιάς
SQL injection	Επίθεση «έγχυσης» SQL κώδικα
Code of Practice	Κώδικας Ορθής Πρακτικής

outsourcing	Ανάθεση έργου σε εξωτερικό φορέα
Plan-Do-Check-Act model	Μοντέλο Σχεδίασε-Κάνε-Έλεγξε-Πράξε
Assets	Αγαθά / Περιουσιακά Στοιχεία του οργανισμού
documentation	Το σύνολο των εγγράφων ενός συστήματος
treatment	Αντιμετώπιση (κινδύνου)
test systems	Συστήματα δοκιμών
Worm	σκουλήκι
Back-up	Αντίγραφο ασφαλείας
denial-of-service	Άρνηση διαθεσιμότητας υπηρεσίας
instant messaging	Άμεση επικοινωνία μέσω μηνυμάτων (π.χ. msn)
host	υποδοχέας
logs	καταγραφικά αρχεία
session	σύνοδος
buffer overflow	Υπερχείλιση καταχωρητών (τύπος επίθεσης)
International Organization for Standardization	Διεθνής Οργανισμός Πιστοποίησης
International Electrotechnical Commission	Διεθνής Ηλεκτροτεχνική Επιτροπή
Firewall	Τοίχος προστασίας
Statement of Applicability	Δήλωση της Εφαρμοστικότητας
Steering Committee	συντονιστική επιτροπή
Management Information System	Σύστημα Διαχείρισης Πληροφοριών
Service Level Agreement	Συμφωνία Επιπέδου Παροχής της Υπηρεσίας
versioning	έκδοση
Help Desk	Τμήμα επίλυσης προβλημάτων
Request For Proposal	Πρόσκληση για υποβολή αιτήσεων από παρόχους
money laundering	ξεπλύματος παράνομου χρήματος

Public Key Infrastructure	Υποδομή Δημοσίου Κλειδιού
Demilitarized Zones	Αποστρατικοποιημένες ζώνες
gateways	Πύλες Επικοινωνίας
ports	θύρες
dial up	τηλεφωνική σύνδεση
call back	Διαδικασία επιστροφής κλήσης
intrusion detection	ανίχνευσης εισβολής
prevention systems	συστήματα πρόληψης
penetration tests	δοκιμές διείσδυσης
credit scoring	βαθμολόγησης πιστοληπτικής ικανότητας
Payment Card Industry	Βιομηχανία Πληρωμών μέσω Κάρτας
Data Security Standard	Πρότυπο Ασφάλειας Δεδομένων
Primary Account Number	Πρωτεύων Αριθμός Λογαριασμού
Proxy server	Διαμεσολαβητής εξυπηρέτης
Cardholder Data Environment	Περιβάλλον δεδομένων κατόχων καρτών
network segmentation	Κατάτμηση του δικτύου
Report of Compliance	Αναφορά Συμμόρφωσης
default password	προεπιλεγμένος κωδικός πρόσβασης
media	“Μέσα”: το σύνολο των γραπτών και ηλεκτρονικών μέσων, που περιέχουν δεδομένα καρτών
log files	Αρχεία καταγραφής συμβάντων
Project Manager	Διαχειριστής έργου
security datasheet	έγγραφο τεχνικών προδιαγραφών ασφαλείας
e-business	Ηλεκτρονικό Επιχειρείν
reconnaissance attacks	εξερευνητικές επιθέσεις
packet sniffers	ανιχνευτές πακέτων
port scan	σάρωση των θυρών

ping sweep	Συνεχή pings
internet information queries	Ερωτήματα πληροφοριών διαδικτύου (π.χ. DNS)
Distributed Denial of Service attacks	Κατανεμημένες επιθέσεις άρνησης παροχής υπηρεσιών
man-in-the-middle attacks	Επιθέσεις ενδιάμεσου κόμβου
viruses	ιοί
MAC Flooding Attack	Επίθεση πλημμύρας MAC
dictionary attacks	Λεξικογραφικές επιθέσεις
privilege level	Προνομιακό επίπεδο
Authentication	Αυθεντικοποίηση
Authorization	Εξουσιοδότηση
Accounting-Auditing	Λογιστική-Έλεγχος
token	κουπόνι
administrator	Διαχειριστής
client/server	Πελάτης/εξυπηρέτης
Extensible Authentication Protocol over LAN	Επεκτάσιμο πρωτόκολλο ελέγχου ταυτότητας πάνω από LAN
authentication server	εξυπηρετητής αυθεντικοποίησης
(un-)authorized state	(μη-)εξουσιοδοτημένη κατάσταση
access point	σημείο πρόσβασης
Initialization Vector Attack	Επίθεση Πίνακα Αρχικοποίησης
Temporal Key Integrity Control	Έλεγχος ακεραιότητας προσωρινού κλειδιού
Message Integrity Check	Έλεγχος ακεραιότητας μηνύματος
master key	πρωτεύον κλειδί
Virtual Private Networks	Εικονικά ιδιωτικά δίκτυα
tunneling	σηράγγωση
encapsulation protocols	πρωτόκολλα ενθυλάκωσης

security associations	σχέσεις ασφαλείας
Authentication Header	Επικεφαλίδα αυθεντικοποίησης
replay attacks	επιθέσεις επανάληψης
security gateway	Πύλη ασφαλείας
Secure Sockets Layer	Στρώμα ασφαλούς υποδοχής
fragmentation	κατάτμηση
Handshake Protocol	Πρωτόκολλο χειραψίας
single point of failure	μοναδικό σημείο αποτυχίας
Network Address Translation	Μετάφραση Διεύθυνσης Δικτύου
guest network	δίκτυο επισκεπτών
remediation network	δίκτυο εξυγίανσης
Systems Audit	Έλεγχος Συστημάτων
Compliance Audit	Έλεγχος Συμμόρφωσης
Operations Audit	Επιχειρησιακός έλεγχος
Reputational Risks	Κίνδυνοι Υπόληψης
Operational Risks	Επιχειρησιακοί Κίνδυνοι
Legal Risks	Νομικοί Κίνδυνοι
Credit Risks	Πιστωτικοί Κίνδυνοι
Liquidity Risks	Κίνδυνοι Ρευστότητας
Interest Rate Risks	Κίνδυνοι Επιτοκίων
Cross-border Transactions Risks	Κίνδυνοι Διακρατικών Συναλλαγών
Information Systems Audit	Έλεγχος Πληροφοριακών Συστημάτων
Business Continuity Plan	Πλάνο Συνέχισης Λειτουργίας
Computer Assisted Audit Tools	Εργαλεία Ελέγχου με χρήση Υπολογιστή
Programmable Logic Controllers	Προγραμματίσιμοι λογικοί ελεγκτές
peer-to-peer	Σχηματισμός ομοτίμων

Business Impact Analysis	Ανάλυση Επιχειρησιακών Επιπτώσεων
disaster site	Τοποθεσία εξοπλισμού σε περίπτωση καταστροφής

ΣΥΝΤΜΗΣΕΙΣ – ΑΡΚΤΙΚΟΛΕΞΑ – ΑΚΡΩΝΥΜΙΑ

IT	Information Technology
SQL	Structured Query Language
SMS	Short Message
PC	Personal Computer
ISO	International Organization for Standardization
IEC	International Electrotechnical Commission
ISMS	International Security Management System
ΣΔΑΠ	Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών
ΕΣΥΔ	Ελληνικό Σύστημα Διαπίστευσης
PDCA	Plan-Do-Check-Act
CD	Compact Disc
UPS	Uninterruptible Power Supply
DVD	Digital Video Disc
VPN	Virtual Private Network
OECD	Organization for Economic Co-operation and Development
PCI DSS	Payment Card Industry – Data Security Standard
ΠΣ	Πληροφοριακά Συστήματα
ΠΙ	Πιστωτικά Ιδρύματα
MIS	Management Information System
SLA	Service Level Agreement
RFP	Request For Proposal
DMZ	Demilitarized Zones
ΣΣΕ	Σχέδια Συνέχειας Εργασιών
ΣΑΚ	Σχέδια Ανάκαμψης από Καταστροφή

ΣΑΥ	Σύστημα Αθέτησης Υποχρεώσεων
ΝΔ	Νομοθετικό Διάταγμα
ΣΣΧ	Σύστημα Συγκέντρωσης Χορηγήσεων
ΣΤΔ	Σύστημα Ταυτοτήτων και Διαβατηρίων
ID	Identification
PAN	Primary Account Number
CID	Card Identification Number
CVC	Card Verification Code
CVV	Card Verification Value
PIN	Personal Identification Number
PA-DSS	Payment Application Data Security Standard
CDE	Cardholder Data Environment
ROC	Report of Compliance
IP	Internet Protocol
SSH	Secure Shell
SSL	Secure Sockets Layer
TLS	Transport Layer Security
USB	Universal Serial Bus
XSS	Cross-Site Scripting
CSRF	Cross-Site Request Forgery
PCI SSC	Payment Card Industry Security Standards Council
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
ΥΑ	Υπεύθυνος Ασφαλείας
PM	Project Manager
ΔΣ	Διευθύνων Σύμβουλος

GMITS	Guidelines for the Management of Information Technology Security
LAN	Local Area Network
ADSL	Asymmetric Digital Subscriber Line
VLAN	Virtual Local Area Network
TCP	Transmission Control Protocol
PVC	Permanent Virtual Circuit
IPSec	Internet Protocol Security
SMIME	Secure Multipurpose Internet Mail Extensions
DNS	Domain Name System
DoS	Denial of Service
DDoS	Distributed Denial of Service
ICMP	Internet Control Message Protocol
FTP	File Transfer Protocol
MAC	Media Access Control
DHCP	Dynamic Host Configuration Protocol
AAA	Authentication Authorization Accounting
SNMP	Simple Network Management Protocol
TACACS	Terminal Access Controller Access-Control System
IETF	Internet Engineering Task Force
RADIUS	Remote Authentication Dial In User Service
MD5	Message Digest 5
AD	Active Directory
MIT	Massachusetts Institute of Technology
EAPOL	Extensible Authentication Protocol Over LAN
SSID	Service Set Identification

WEP	Wired Equivalent Privacy
IV	Initialization Vector
WPA	WI-fi Protected Access
TKIP	Temporal Key Integrity Control
MIC	Message Integrity Check
AES	Advanced Encryption Standard
PKC	Proactive Key Caching
ISDN	Integrated Services Digital Network
PPTP	Point to Point Tunneling Protocol
L2TP	Layer 2 Tunneling Protocol
L2F	Layer 2 Forwarding
ISP	Internet Service Provider
ATM	Asynchronous Transfer Mode
SA	Security Associations
AH	Authentication Header
ESP	Encapsulating Security Payload
IKE	Internet Key Exchange
DES	Data Encryption Standard
HMAC	Hash-based Message Authentication Code
SHA	Secure Hash Algorithm
CA	Certification Authority
ISAKMP	Internet Security Association and Key Management Protocol
OSI	Open Systems Interconnection
IE	Internet Explorer
HTTP	Hypertext Transfer Protocol
ALG	Application Level Gateway

GRE	Generic Routing Encapsulation
UDP	User Datagram Protocol
NAT	Network Address Translation
PAT	Port Address Translation
HIPS	Host-based Intrusion Prevention System
NIPS	Network-based Intrusion Prevention System
ACL	Access Control List
NAP	Network Access Protection
WSUS	Windows Server Update Services
SHA	System Health Agent
SHV	System Health Validator
EFS	Encrypting File System
NTFS	New Technology File System
BIOS	Basic Input Output System
TPM	Trusted Platform Module
PKI	Public Key Infrastructure
LDAP	Lightweight Directory Access Protocol
RA	Registration Authority
RSA	Rivest Shamir Adleman (Επίθετα ονομάτων)
ADCS	Active Directory Certificate Services
CRL	Certificate Revocation List
OR	Online Responder
NDES	Network Device Enrollment Service
VM	Virtual Machine
ISA	Information Systems Auditing
BCP	Business Continuity Plan

CAAT	Computer Assisted Audit Tools
ACL	Audit Command Language
RBN	Russian Business Network
ICS	Industrial Control Systems
PLC	Programmable Logic Controllers
TJX	Όνομα Εταιρείας
APT	Advanced Persistent Threat
URL	Uniform Resource Locator
SCMS	Software Configuration Management System
BIA	Business Impact Analysis
EOC	Emergency Operation Center

ΒΙΒΛΙΟΓΡΑΦΙΚΕΣ ΑΝΑΦΟΡΕΣ

1. www.cisco.com
2. www.microsoft.com
3. Cisco Networking Academy Program
4. Microsoft Official Course: Configuring, Managing and Maintaining Windows Server 2008
5. http://web.mit.edu/kerberos/
6. http://www.windowsitpro.com/article/kerberos/kerberos-in-active-directory
7. http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_1-1/ssl.html
8. http://en.wikipedia.org/wiki/DMZ_(computing)
9. http://www.antivirusworld.com/articles/antivirus.php
10. http://www.net-security.org/article.php?id=485
11. http://4sysops.com/archives/review-windows-7-bitlocker/
12. http://www.csoonline.com/article/499041/how-to-evaluate-compare-and-implement-enterprise-antivirus
13. http://technet.microsoft.com/library/bb457116.aspx
14. http://en.wikipedia.org/wiki/DMZ_(computing)
15. Introduction to Information Security - Author: Linda Pesante Copyright 2008 Carnegie Mellon University
16. Information Security in Banking and Financial Industry - Vishal R. Ambhire, Prakash S. Teltumde Computer Department, V.J.T.I.,Mumbai, Maharashtra, India
17. http://banktechindia.com/news/12-01-25/Mitigating_security_risks_for_the_banking_and_financial_sector.aspx
18. http://en.wikipedia.org/wiki/Information_security
19. http://www.bankinfosecurity.com/top-8-security-threats-2010-a-2019/op-1
20. http://en.wikipedia.org/wiki/ISO/IEC_27001

21. INTERNATIONAL STANDARD ISO/IEC FDIS 17799

22. INTERNATIONAL STANDARD ISO/IEC FDIS 27001

23. http://www.itgovernance.co.uk/files/download/Infosec_101v1.3.pdf

24. http://www.dpa.gr

25. Πράξη διοικητή ΤτΕ - Παράρτημα 2 - ΑΡΧΕΣ ΑΣΦΑΛΟΥΣ ΚΑΙ ΑΠΟΤΕΛΕΣΜΑΤΙΚΗΣ ΛΕΙΤΟΥΡΓΙΑΣ ΤΩΝ ΣΥΣΤΗΜΑΤΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΣΤΑ ΠΛΑΙΣΙΑ ΤΗΣ ΔΙΑΧΕΙΡΙΣΗΣ ΤΟΥ ΛΕΙΤΟΥΡΓΙΚΟΥ ΚΙΝΔΥΝΟΥ ΑΠΟ ΤΑ ΠΙΣΤΩΤΙΚΑ ΙΔΡΥΜΑΤΑ

26. http://el.wikipedia.org/wiki/%CE%91%CF%81%CF%87%CE%AE_%CE%A0%CF%81%CE%BF%CF%83%CF%84%CE%B1%CF%83%CE%AF%CE%B1%CF%82_%CE%94%CE%B5%CE%B4%CE%BF%CE%BC%CE%AD%CE%BD%CF%89%CE%BD_%CE%A0%CF%81%CE%BF%CF%83%CF%89%CF%80%CE%B9%CE%BA%CE%BF%CF%8D_%CE%A7%CE%B1%CF%81%CE%B1%CE%BA%CF%84%CE%AE%CF%81%CE%B1

27. http://www.csoonline.com/article/495017/how-to-write-an-information-security-policy?page=1

28. http://www.symantec.com/connect/articles/introduction-security-policies-part-one-overview-policies

29. http://en.wikipedia.org/wiki/Information_technology_audit

30. Basel Committee on Banking Supervision - Consultative document. The internal audit function in banks, December 2011

31. Information systems audit policy for the banking and financial sector Department of Information Technology Reserve Bank Of India Mumbai October, 2001

32. http://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard

33. Payment Card Industry (PCI) Data Security Standard Navigating PCI DSS, “Understanding the Intent of the Requirements”, October 2010

34. http://searchfinancialsecurity.techtarget.com/definition/PCI-DSS-Payment-Card-Industry-Data-Security-Standard

35. http://www.fas.org/irp/threat/cyber/docs/infosec.htm

36. Olli Pitkänen, Risto Sarvas, Asko Lehmuskallio, Miska Simanainen, Vesa Kantola, “Future Information Security Trends”, Kasi Research Project, Tekes Safety and Security Research Program. Final Report, March 11, 2011
37. http://www.datanymity.com/breaches/heartland_payment_systems.php
38. http://www.bankinfosecurity.com/bank-india-hack-a-560
39. http://www.bankinfosecurity.com/bank-new-york-mellon-investigated-for-lost-data-tape-a-862/op-1
40. http://www.piraeusbank.gr/ecpage.asp?id=300941&nt=78&lang=1
41. http://www.insurancedaily.gr/blog/%CF%80%CE%B9%CF%83%CF%84%CE%BF%CF%80%CE%BF%CE%AF%CE%B7%CF%83%CE%B7-%CE%B1%CF%83%CF%86%CE%B1%CE%BB%CE%B5%CE%AF%CE%B1%CF%82-%CE%B3%CE%B9%CE%B1-%CF%84%CE%B9%CF%82-%CE%B7%CE%BB%CE%B5%CE%BA%CF%84%CF%81/
42. http://www.capital.gr/news.asp?id=871938
43. http://www.ethnodata.gr/Announcements.aspx?Id=0