ΕΘΝΙΚΟ ΚΑΙ ΚΑΠΟΔΙΣΤΡΙΑΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ
ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

Απειλές ασφάλειας, τεχνικές αντιμετώπισης επιθέσεων και νομοθεσία των τηλεπικοινωνιακών συστημάτων

Αθανασία-Αγγελική Δ. Δόδογλου
Αναστασία Ε. Ρήγα

Επιβλέπων: **Δημήτριος Βαρουτάς,** Επίκουρος Καθηγητής

ΑΘΗΝΑ

Φεβρουάριος 2017

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

Απειλές ασφάλειας, τεχνικές αντιμετώπισης επιθέσεων και νομοθεσία των τηλεπικοινωνιακών συστημάτων

Αθανασία-Αγγελική Δ. Δόδογλου

Α.Μ.: 1115201100051

Αναστασία Ε. Ρήγα

Α.Μ.: 1115200900196

ΕΠΙΒΛΕΠΟΝΤΕΣ: **Δημήτριος Βαρουτάς,** Επίκουρος Καθηγητής

ΠΕΡΙΛΗΨΗ

Η παρούσα πτυχιακή εργασία πραγματεύεται τους κινδύνους, τις απειλές καθώς και τους τρόπους επιθέσεων που αντιμετωπίζουν τα τηλεπικοινωνιακά συστήματα, λόγω της ραγδαίας προόδου της τεχνολογίας. Επίσης, αναλύονται οι σκοτεινές πλευρές του διαδικτύου, το επονομαζόμενο darknet και οι κίνδυνοι που κρύβει για τους χρήστες του. Εν συνεχεία, παρατίθενται οι λύσεις που προτείνει η Ευρωπαϊκή Ένωση για να εξασφαλίσει την προστασία των πολιτών των κρατών μελών της. Επιπλέον, μελετάται η ισχύουσα νομοθεσία για τις επικοινωνίες στην Ελλάδα και γενικά στην Ευρωπαϊκή Ένωση. Τέλος, θα εξεταστεί η νομοθεσία για υπηρεσίες cloud που ισχύει στην Ευρώπη και στην Αμερική καθώς υπάρχει μία διαμάχη ανάμεσα στις δύο για την ασφάλεια των προσωπικών δεδομένων των πολιτών τους.

ΘΕΜΑΤΙΚΗ ΠΕΡΙΟΧΗ: Ασφάλεια δικτύων

ΛΕΞΕΙΣ ΚΛΕΙΔΙΑ: Απειλές ασφάλειας, μεταδεδομένα, μαζική παρακολούθηση, σκοτεινό δίκτυο, νομοθεσία, υπολογιστικό νέφος

ABSTRACT

This thesis discusses the risks, the threats and the dangers faced telecommunication systems because of the rapid development of technology. Also analyses the dark side of the Internet, the so called Darknet and the risks that hides from its users. Subsequently, there are listed the solutions proposed by the European Union to ensure the protection of the citizens of the Member States. In addition, is studied the legislation on communications in Greece and the European Union in general. Finally, we examined cloud services and legislation in force in Europe and in America as there is a conflict between the two for the safety of citizens' personal data.

SUBJECT AREA: Network Security

KEYWORDS: security threats, metadata, mass surveillance, deep web, legislation, cloud

ΕΥΧΑΡΙΣΤΙΕΣ

Για τη διεκπεραίωση της παρούσας Πτυχιακής Εργασίας, θα θέλαμε να ευχαριστήσουμε τον επιβλέποντα, επίκουρο καθηγητή Δημήτριο Βαρουτά, για τη συνεργασία και την πολύτιμη συμβολή του στην ολοκλήρωση της.

ΠΕΡΙΕΧΟΜΕΝΑ

ΚΑΤΑΛΟΓΟΣ ΕΙΚΟΝΩΝ

ΚΑΤΑΛΟΓΟΣ ΠΙΝΑΚΩΝ

ΠΡΟΛΟΓΟΣ

Η παρούσα πτυχιακή εργασία διεξήχθει στην Αθήνα, κατά το ακαδημαικό ετος 2016-2017 υπό την επίβλεψη του επίκουρου καθηγητή Δημήτριου Βαρουτά, τον οποίο ευχαριστούμε θερμά για την συνεργασία του.

1.SECURITY THREATS

1.1 Πώς ορίζονται οι απειλές ασφάλειας (security threats)

Το security threat ορίζεται ως μια πιθανή παραβίαση ασφάλειας.

Ως παραβιάσεις ασφάλειας μπορούν να θεωρηθούν:

- Η μη εξουσιοδοτημένη αποκάλυψη πληροφοριών
- Η μη εξουσιοδοτημένη καταστροφή ή τροποποίηση δεδομένων, εξοπλισμού ή άλλων πόρων
- Η κλοπή, η αφαίρεση ή η απώλεια πληροφοριών.

Επιπλέον παραβιάσεις ασφαλείας θεωρούνται η διακοπή ή άρνηση των υπηρεσιών και η πλαστοπροσωπία ή μεταμφίεση ως εξουσιοδοτημένος φορέας.

1.2 Είδη απειλών ασφάλειας

Τα security threats χωρίζονται σε δύο κατηγορίες ως προς το είδος:

- **<u>Συμπτωματική ή εκ προθέσεως απειλή</u>**

  α)<u>Συμπτωματική απειλή (κάποιες φορές ονομάζονται και ακούσιες)</u>

  Μια συμπτωματική απειλή είναι αυτή η οποία δεν είχε καμία εκ προμελέτης πρόθεση, όπως για παράδειγμα μια δυσλειτουργία του συστήματος ή λογισμικού, ή μια υλική βλάβη.

  β) <u>Εκ προθέσεως απειλή</u>

  Μια εκ προθέσεως απειλή είναι αυτή η οποία πραγματοποιείται από κάποιον ο οποίος διαπράττει μια σκόπιμη πράξη. Οι σκόπιμες απειλές κυμαίνονται από συνηθισμένη εξέταση, χρησιμοποιώντας εύκολα διαθέσιμα εργαλεία παρακολούθησης, σε εξελιγμένες επιθέσεις που χρησιμοποιούν εξειδικευμένες γνώσεις συστήματος. Η εφαρμογή μιας εσκεμμένης απειλής ονομάζεται επίθεση.

- **<u>Ενεργητική ή παθητική απειλή</u>**

  α) <u>Ενεργητική απειλή</u>

  Μια ενεργή απειλή είναι αυτή η οποία έχει ως αποτέλεσμα την αλλαγή στην κατάσταση ή στην λειτουργία ενός συστήματος, όπως η αλλαγή δεδομένων ή η καταστροφή υλικού εξοπλισμού.

  β) <u>Παθητική απειλή</u>

  Σε αντίθεση με την ενεργητική, μια παθητική απειλή δεν περιλαμβάνει αλλαγή της κατάστασης, αλλά επικεντρώνεται σε υποκλοπές και παγίδευση γραμμών με κοριό.

1.3 Κατηγορίες Security Threats

Οι κύριες απειλές ασφάλειας που αντιμετωπίζει ο κλάδος των τηλεπικοινωνιών χωρίζονται σε δύο αλληλένδετες κατηγορίες.

Αρχικά στην πρώτη κατηγορία είναι οι απειλές οι οποίες στοχεύουν εταιρείες τηλεπικοινωνιών άμεσα και περιλαμβάνουν DDoS επιθέσεις, στοχευμένες επιθέσεις (APT εκστρατείες), τα τρωτά σημεία διαδικτυακών συσκευών και ανθρώπινες απειλές όπως για παράδειγμα η πρόσβαση εκ των έσω, η χειραγώγηση και το ρίσκο που επιτρέπει σε τρίτους να έχουν πρόσβαση σε πληροφορίες.

Στην δεύτερη κατηγορία ανήκουν οι απειλές που στοχεύουν τους συνδρομητές των υπηρεσιών τηλεπικοινωνιών, ιδιαίτερα τους πελάτες που τους παρέχεται κινητή τηλεφωνία (Cellular Service Providers (CSPs)) και υπηρεσίες Internet (Internet Service Providers (ISPs)). Οι απειλές αυτές περιλαμβάνουν κακόβουλο λογισμικό για συσκευές κινητής τηλεφωνίας, συλλογή δεδομένων του συνδρομητή, τρωτά σημεία συσκευών των τελικών χρηστών, και άλλα.

Αναλυτικότερα:

- Κατανεμημένες επιθέσεις άρνησης υπηρεσιών (**DDoS** attacks -Distributed Denial of Service attacks)

  Οι DDoS επιθέσεις συνεχίζουν να παρουσιάζουν αύξηση σε δύναμη και κλίμακα. Σύμφωνα με το Data Breach Investigations Report για το έτος 2016, ο τομέας των τηλεπικοινωνιών έχει λάβει πλήγμα ισχυρότερο από κάθε άλλο. Οι άμεσες DDoS επιθέσεις μπορούν να μειώσουν την χωρητικότητα του δικτύου, να υποβαθμίσουν την απόδοση, να αυξήσουν το κόστος ανταλλαγής πληροφορίας, να διακόψουν την διαθεσιμότητα της υπηρεσίας, ακόμα και να μειώσουν την πρόσβαση στο Internet εφόσον χτυπηθούν οι ISPs. Επιπλέον, μπορούν να είναι κάλυψη για μια βαθύτερη, πιο επιζήμια δευτερεύουσα επίθεση ή διαδρομή σε μια βασική επιχείρηση επίθεσης σε συνδρομητή ή σε λογισμικό μεγάλης κλίμακας.

- Εκμετάλλευση των τρωτών σημείων του δικτύου και των συσκευών των καταναλωτών

  Από τις βασικότερες απειλές για τα τηλεπικοινωνιακά συστήματα. Τα τρωτά σημεία σε συσκευές δικτύου, δικτύων φεμτοκυψελών επιχειρήσεων ή καταναλωτών, USBs και routers, καθώς και root exploits για τηλέφωνα Android, όλα παρέχουν νέους διαύλους για επιθέσεις, που περιλαμβάνουν κακόβουλο λογισμικό και τεχνολογίες που τα άτομα, οι οργανώσεις, ακόμα και οι βασικές λύσεις antivirus δεν μπορούν πάντα να τα αφαιρέσουν εύκολα.

- Phishing

  Μια συνήθης απειλή που παρουσιάζεται είναι η έκθεση των συνδρομητών μέσω χειραγώγησης, ηλεκτρονικού “ψαρέματος” (phishing), ή επιβλαβούς λογισμικού (malware). Εμφανίζονται συχνά με το πρόσχημα μηνυμάτων ηλεκτρονικού ταχυδρομείου σχεδιασμένο για να εμφανίζεται σαν να προέρχεται από νόμιμες πηγές.

  Αυτές οι κλασσικές τεχνικές παραμένουν δημοφιλείς και μπορεί εύκολα να τις κατέχει κάποιος εγκληματίας του κυβερνοχώρου, αν και το 2016 παρουσιάζονται αλλαγές και πιο εξελιγμένοι τρόποι με τους οποίους οι επιτιθέμενοι διεξάγουν τις εκστρατείες τους. Ένας αυξανόμενος αριθμός από κυβερνο-εισβολείς συνδυάζουν τα δεδομένα τους από διαφορετικές πηγές, συμπεριλαμβανομένων ανοιχτών πηγών, για να δημιουργήσουν λεπτομερείς εικόνες πιθανών στόχων για εκβιασμό ή χειραγώγηση.

- Εσωτερικές απειλές

  Τα τελευταία χρόνια έχει παρατηρηθεί η αύξηση των εσωτερικών απειλών στο διαδίκτυο. Τα λεπτομερή προφίλ των χρηστών –στόχων των επιθέσεων, χρησιμοποιούνται για την μύηση των έσω, δηλαδή άτομα τα οποία είναι γνώστες των λειτουργιών ενός γκρουπ, οργανισμού ή ιδρύματος, έτσι ώστε να βοηθήσουν στην διάπραξη του κυβερνο-εγκλήματος. Κάποιοι από αυτούς τους χρήστες είτε συνεργάζονται εθελοντικά είτε αναγκάζονται μέσω εκβιασμού. Οι χρήστες που εργάζονται σε εταιρείες που παρέχουν υπηρεσίες κινητής τηλεφωνίας, προσλαμβάνονται κυρίως για να παρέχουν πρόσβαση σε δεδομένα, ενώ το προσωπικό που εργάζεται για τους παρόχους υπηρεσιών διαδικτύου έχει επιλεγεί για να υποστηρίξει την χαρτογράφηση του δικτύου και για την επίθεση ενδιάμεσης οντότητας (man-in-the-middle attack).

- Κακόβουλο λογισμικό(Malware)

  Το malware είναι μια ποικιλία μορφών εχθρικού, ενοχλητικού ή επιθετικού λογισμικού ή κομμάτι κώδικα. Malware θα μπορούσε να είναι οι ιοί, τα «σκουλήκια» (worms) των υπολογιστών, Δούρειοι Ίπποι, κατασκοπευτικό λογισμικό (spyware) και κακόβουλο λογισμικό τύπου rootkits.

  - Πιο συγκεκριμένα, ο ιός των υπολογιστών είναι ένα μικρό κομμάτι λογισμικού που μπορεί να μεταδοθεί από έναν υπολογιστή σε έναν άλλο. Ο ιός μπορεί να φθείρει, να κλέψει και να διαγράψει δεδομένα στον υπολογιστή, ακόμα και να διαγράψει όλο το περιεχόμενο του σκληρού δίσκου. Επιπλέον, οι επιτιθέμενοι μπορούν να χρησιμοποιήσουν άλλα προγράμματα όπως το ηλεκτρονικό ταχυδρομείο έτσι ώστε να εξαπλωθεί ο ιός και σε άλλους υπολογιστές. Παρόμοια είναι και η λειτουργία του worm, δηλαδή το κακόβουλο λογισμικό μπορεί να αντιγράψει τον εαυτό του από υπολογιστή σε υπολογιστή χωρίς την ανθρώπινη αλληλεπίδραση.
  - Άλλη μορφή απειλής είναι το λογισμικό Trojan horse, που μπορεί να μολύνει τον υπολογιστή κάποιου χρήστη απλά κατεβάζοντας κάποια εφαρμογή που φαινομενικά δεν ήταν βλαβερή. Το λογισμικό αυτό μπορεί να κάνει τα πάντα, από το να λάβει κωδικούς μέσω της πληκτρολόγησης έως την παρακολούθηση και καταγραφή των κινήσεων του χρήστη μέσω της webcam του.
  - Αντίστοιχη δράση έχει και το κακόβουλο λογισμικό υποκλοπής spyware το οποίο χρησιμοποιείται για να περιγράψει την λειτουργία του Trojan horse, που έχει δημιουργηθεί από εγκληματίες του κυβερνοχώρου για να κατασκοπεύουν τους στόχους τους. Ένα παράδειγμα είναι το λογισμικό keylogger το οποίο καταγράφει κάθε πληκτρολόγηση του στόχου στο πληκτρολόγιό του, και περιοδικά στέλνει πίσω στον επιτιθέμενο τις καταγραφές. Παρόλα αυτά το keylogging λογισμικό είναι ευρέως διαθέσιμο στους γονείς ή στις εταιρείες που θέλουν να παρακολουθούν τα παιδιά τους ή την χρήση του Internet από τους εργαζομένους.

- Άλλες επιθέσεις που αντιμετωπίζουν οι εταιρείες τηλεπικοινωνιών συμπεριλαμβάνουν: στοχευμένες επιθέσεις, κακή ρύθμιση παραμέτρων ελέγχων πρόσβασης ιδίως όταν διεπαφές είναι διαθέσιμες στο κοινό και σε κάθε χρήστη του δικτύου, ανεπαρκή μέτρα ασφαλείας για 2G/3G επικοινωνίες, και το ρίσκο οι πάροχοι των τηλεπικοινωνιών να εμπλακούν σε άσχετες επιθέσεις που εκμεταλλεύονται τους πόρους των τηλεπικοινωνιών, και έτσι ως αποτέλεσμα να υποφέρουν τις παράπλευρες απώλειες.

1.4 Χρονολογίες δημιουργίας και δημοσίευσης των Security Threats

Τα security threats, παρότι δεν αποτελούν κάτι καινούριο στις μέρες μας, φαίνεται να προκαλούν μεγαλύτερη ζημιά από ποτέ. Ενώ οι μέθοδοι έχουν αλλάξει, οι επιτιθέμενοι έχουν ως στόχο να προκαλέσουν τόσο καταστροφικές συνέπειες όσο το δυνατόν περισσότερο.

Την δεκαετία του '60 οι άνθρωποι ξεκίνησαν να εκμεταλλεύονται τις τηλεπικοινωνίες. Τα πρώτα security threats δημιουργήθηκαν αρκετά νωρίτερα από την περίοδο που οι υπολογιστές άρχισαν να αποτελούν αναπόσπαστο κομμάτι της καθημερινότητας. Πράγματι, πριν από δεκαετίες οι εγκληματίες συχνά επιχειρούσαν να παγιδέψουν τηλεφωνικά συστήματα. Ξεκινώντας το 1960, η AT&T αποφάσισε να παρακολουθεί τις κλήσεις προκειμένου να πιάσει τους εγκληματίες. Μέσα στα επόμενα χρόνια πιάστηκαν εκατοντάδες άνθρωποι που θέλησαν να εξασφαλίσουν δωρεάν κλήσεις μέσω της χρήσης του ήχου που παράγουν τα "μπλε κουτιά".

Μέχρι το 1979 οι απειλές ως προς τους υπολογιστές είχαν πάρει άλλη μορφή. Οι ιοί και τα worms ήταν οι επόμενοι ένοχοι για της απειλές στον κυβερνοχώρο, αν και στην αρχή ήταν ακίνδυνα. Το πρώτο worm δημιουργήθηκε το 1979 σε ένα ερευνητικό κέντρο Xerox και ο αρχικός στόχος ήταν να βοηθήσει στην αποτελεσματικότητα των υπολογιστών. Παρόλα αυτά οι hackers πήραν τα worms και τα μετέτρεψαν έτσι ώστε να καταστρέφουν και να αλλάζουν δεδομένα. Μέχρι το 1988, η ζημία έγινε ευρέως διαδεδομένη, καθώς ένα worm απενεργοποίησε περίπου 6.000 υπολογιστές που ήταν συνδεδεμένοι με το Advanced Research Projects Agency Network. Από το 1990, δημιουργήθηκαν οι πρώτοι αυτο-τροποποιήσιμοι ιοί.

Στα μέσα τις δεκαετίας του 1990, το πρόβλημα των ιών έγινε διεθνές καθώς ο πρώτος ιός, με βάση το Microsoft Word χρησιμοποιώντας μακρο-εντολές, εξαπλώθηκε σε όλο τον κόσμο. Το 1998, έφηβοι hackers απέκτησαν τον έλεγχο περισσότερων από 500 κυβερνητικών, στρατιωτικών και ιδιωτικών υπολογιστικών συστημάτων μέσω των επιθέσεων "Solar Sunrise". Δύο χρόνια αργότερα, άλλοι hackers ήταν κατάφεραν να διακόψουν την λειτουργία των Amazon, Yahoo και eBay χρησιμοποιώντας DDoS επιθέσεις. Το 2001, το Code Red worm κατέληξε να προκαλέσει 2 δισεκατομμύρια δολάρια σε ζημιές, από τη μόλυνση του λογισμικού των Microsoft Windows NT και των Windows 2000. Οι επιθέσεις μεγάλης κλίμακας συνεχίστηκαν το 2006, όταν από 469.000 έως ένα εκατομμύριο υπολογιστές μολύνθηκαν με τον ιό Nyxem.

Στα μέσα της δεκαετίας του 2000, καθώς αυξήθηκε ο αριθμός των ανθρώπων που συνδέονται με το Διαδίκτυο, αντίστοιχα μεγάλωσαν και τα ποσοστά μόλυνσης. Ο ιός Storm Worm, το 2007 και ο ιός Koobface το 2008 χρησιμοποιήσαν τα μηνύματα ηλεκτρονικού ταχυδρομείου και τα Social Media για να εξαπλωθούν γρήγορα, μολύνοντας εκατομμύρια υπολογιστές. Επίσης το 2009, Hackers έκλεψαν τα δεδομένα με το worm Conficker. Το 2012 ανακαλύφθηκε το Heartbleed bug, το οποίο εκμεταλλεύτηκε ένα ελάττωμα στη βιβλιοθήκη λογισμικού ασφάλειας OpenSSL για να αποκτήσει πρόσβαση σε ευαίσθητα δεδομένα όπως κωδικούς πρόσβασης. Τέλος, το 2013 σημειώθηκε μια από τις πιο κακόφημες επιθέσεις, όταν hackers απέκτησαν πρόσβαση σε servers της Target, που οδήγησε στην κλοπή 70 εκατομμυρίων αρχείων πελατών[1],[2],[3].

1.5 Αντιμετώπιση των Security Threats από εταιρείες

Οι περισσότεροι από τους ιούς υπολογιστών που ο κώδικάς τους γράφτηκε στις αρχές και τα μέσα της δεκαετίας του 1980 ήταν περιορισμένοι σε αυτο-αναπαραγωγή και δεν είχαν καμία συγκεκριμένη ρουτίνα, για την βλάβη που προκαλούν, ενσωματωμένη στον κώδικα. Αυτό άλλαξε, όταν όλο και περισσότεροι προγραμματιστές

εξοικειώθηκαν με τον προγραμματισμό των ιών και δημιούργησαν ιούς που χειραγωγούν ή ακόμα και καταστρέφουν δεδομένα των μολυσμένων υπολογιστών.

Υπάρχουν ανταγωνιστικοί ισχυρισμοί ως προς το ποιος δημιούργησε το πρώτο προϊόν Antivirus[4],[5]. Ενδεχομένως η πρώτη δημόσια τεκμηριωμένη αφαίρεση ενός ιού υπολογιστών διεξήχθη από τον Bernd Fix το 1987. Υπήρχαν δύο εφαρμογές προστασίας από ιούς για την πλατφόρμα Atari ST οι οποίες αναπτύχθηκαν επίσης το 1987. Η πρώτη ήταν η G Data και η δεύτερη η UVK 2000. Ο Fred Cohen, ο οποίος δημοσίευσε ένα από τα πρώτα πανεπιστημιακά έγγραφα σχετικά με τους ιούς υπολογιστών το 1984, άρχισε να αναπτύσσει στρατηγικές για το λογισμικό προστασίας από ιούς το 1988, κάτι το οποίο συνεχίστηκε αργότερα από επόμενους προγραμματιστές. Το 1987, ο Cohen δημοσίευσε μια απόδειξη ότι δεν υπάρχει αλγόριθμος που μπορεί κάλλιστα να ανιχνεύσει όλους τους πιθανούς ιούς. Το 1987, ανακοινώθηκαν τα δύο πρώτα Antivirus: Flushot Plus από Ross Greenberg και Anti4us από Erwin Lanting.

Το 1988 μια λίστα με όνομα VIRUS-L ξεκίνησε στο δίκτυο BITNET/EARN, όπου συζητήθηκαν οι νέοι ιοί και οι δυνατότητες για την ανίχνευση και την εξουδετέρωσή τους. Κάποια από τα μέλη αυτής της λίστας όπως ο John McAfee και ο Eugene Kaspersky οι οποίοι αργότερα ίδρυσαν εταιρείες που ανέπτυξαν και πούλησαν λογισμικό προστασίας από ιούς.

Πριν η σύνδεση στο διαδίκτυο γίνει ευρύτατα διαδεδομένη, οι ιοί μεταδίδονταν από μολυσμένους δίσκους. Το antivirus είχε τεθεί μεν σε χρήση, αλλά ενημερωνόταν σχετικά σπάνια. Αυτό που έπρεπε να ελέγχεται, ήταν τα εκτελέσιμα αρχεία και οι τομείς εκκίνησης των δισκετών και των σκληρών δίσκων. Παρόλα αυτά όταν η χρήση του διαδικτύου έγινε ευρεία, οι ιοί άρχισαν να μεταδίδονται online.

Κατά τη διάρκεια των ετών, έχει γίνει απαραίτητο για το antivirus να ελέγχει μια αυξανόμενη ποικιλία αρχείων εκτός από μόνο τα εκτελέσιμα, για διάφορους λόγους, όπως το ότι οι ισχυρές μακροεντολές που χρησιμοποιήθηκαν στις εφαρμογές επεξεργαστών λέξεων, π.χ. Microsoft Word, παρουσίασαν κάποιο κίνδυνο[6]. Οι δημιουργοί ιών θα μπορούσαν να χρησιμοποιήσουν τις μακροεντολές για να γράψουν ιούς που θα ενσωματώνονται μέσα στα έγγραφα. Αυτό συνεπάγεται ότι οι υπολογιστές θα μπορούσαν να τίθενται σε κίνδυνο από μόλυνση με το άνοιγμα των εγγράφων με τις κρυμμένες συνημμένες μακροεντολές.

Με την πάροδο των χρόνων, όλο και περισσότερες εταιρείες ασχολήθηκαν με την ασφάλεια σε πολύ μεγαλύτερο βαθμό. Χαρακτηριστικά, η Microsoft τώρα πια με την εγκατάσταση των Windows παρέχει και το δικό της λογισμικό προστασίας. Άλλες εταιρείες-κυρίαρχες στο χώρο της πληροφορικής που εστίασαν σε αυτό το ζήτημα είναι οι Zerofox, Intel,IBM[7] και DELL[8].

2. ΤΕΧΝΙΚΕΣ ΠΑΡΑΚΟΛΟΥΘΗΣΗΣ ΚΑΙ ΑΝΑΛΥΣΗΣ ΜΕΤΑΔΕΔΟΜΕΝΩΝ ΤΩΝ ΧΡΗΣΤΩΝ

2.1. Μεταδεδομένα

Τα μεταδεδομένα είναι «δεδομένα που αφορούν τα δεδομένα» μιας επικοινωνίας. Τα μεταδεδομένα ουσιαστικά, είναι στοιχεία που παράγονται όταν χρησιμοποιούνται τα ηλεκτρονικά κανάλια επικοινωνίας, όπως Διαδίκτυο ή Τηλεφωνία, τα οποία παρέχουν πληροφορίες για τον χρόνο, την προέλευση, τον προορισμό, τη θέση, τη διάρκεια, και τη συχνότητα των επικοινωνιών.

2.2. Τύποι μεταδεδομένων

Υπάρχουν δύο τύποι μεταδεδομένων**:**

1.Μεταδεδομένα που παρέχουν τα στοιχεία όσον αφορά το περιεχόμενο: π.χ. οι ιδιότητες του αρχείου, ο δημιουργός ενός εγγράφου, η GPS τοποθεσία μιας φωτογραφίας.

2.Μεταδεδομένα της επικοινωνίας: Τα μεταδεδομένα επικοινωνίας μπορούν να υποδιαιρεθούν σε δύο διαφορετικούς τύπους:

α)Μεταδεδομένα Τηλεφωνίας: Αφορούν τις περιεκτικές επικοινωνίες που καθοδηγούν τις πληροφορίες. Δεν αφορούν το περιεχόμενο συζήτησης, το όνομα, ή τη διεύθυνση. Περιλαμβάνει την περιοχή των δεδομένων

β)Μεταδεδομένα Διαδικτύου: Επιτρέπουν την πρόσβαση των χειριστών μεταφορών δεδομένων και των παρόχων πληροφοριών στο τέλος των επικοινωνιών.

2.3. Έννομη παρακολούθηση των μεταδεδομένων επικοινωνίας

Η νόμιμη παρακολούθηση των μεταδεδομένων είναι μια στοχοθετημένη επιτήρηση από τις αρχές επιβολής του νόμου και δεν θεωρείται ως μαζική επιτήρηση.

Συγκεκριμένα:

-Στην Ευρώπη δεν υπάρχει καμιά υποχρεωτική περίοδος διατήρησης για τα μεταδεδομένα επικοινωνίας, έπειτα από την κατάργηση της Οδηγίας 2006/24/ΕΚ του Ευρωπαϊκού Κοινοβουλίου το 2014. Η οδηγία αυτή, έθετε μια περίοδο διατήρησης των μεταδεδομένων από 6 μήνες έως και 2 έτη.

-Το Ηνωμένο Βασίλειο ακολουθεί τη νομοθεσία για τη Διατήρηση και Διερεύνηση των Δεδομένων (DRIP Act – Data Retention and Investigatory Powers Act 2014) από το 2014. Η νομοθεσία αυτή ορίζει τη διατήρηση των μεταδεδομένων έως 12 μήνες και τη χρήση αυτών ως αποδείξεις σε δικαστικές υποθέσεις.

-Στην Αυστραλία , δεν υπάρχει προς το παρόν νομοθεσία για το ζήτημα των μεταδεδομένων. Παρόλα αυτά εξετάζεται η δημιουργία νομοθεσίας που θα προστάζει τους παρόχους υπηρεσιών να διατηρούν τα μεταδεδομένα τους εως και 2 χρόνια.

-Στις Ηνωμένες Πολιτείες, δεν υπάρχει νομοθεσία που να εστιάζει στη διατήρηση των μεταδεδομένων. Παρόλα αυτά οι αμερικανικές αρχές μπορούν να αποκτήσουν πρόσβαση στα μεταδεδομένα των παρόχων υπηρεσιών σύμφωνα με τη νομοθεσία SCA (Stored Communications Act), η οποία θεσπίζει επιτακτική

τη διατήρηση των μεταδεδομένων για 180 ημέρες εφόσον υπάρχει κυβερνητική εντολή.

2.4. Ανάλυση των μεταδεδομένων για σκοπούς μαζικής παρακολούθησης

Σήμερα, η ραγδαία ανάπτυξη της συλλογής δεδομένων και οι καινοτόμες προσεγγίσεις για την αναπαράσταση δεδομένων και μαθηματικών μοντέλων, συμπίπτουν με την ανάπτυξη ισχυρών τεχνολογιών βάσεων δεδομένων οι οποίες προσφέρουν εύκολη πρόσβαση σε γιγάντια ποσά αποθηκευμένων δεδομένων. Η δομημένη φύση των μεταδεδομένων είναι ιδανική για την ανάλυση με χρήση διαφόρων τεχνικών για εξόρυξη πληροφοριών από δεδομένα όπως Data Fusion, Pattern Recognition και Machine Learning. Η ανάλυση των μεταδεδομένων γίνεται μέσω Big Data.

Big Data*:* Ο όρος Big Data, περικλείει τη χρήση τεχνικών για να συλληφθεί, να γίνει αντικείμενο επεξεργασίας, να αναλυθεί και να απεικονιστεί ένα μεγάλο σύνολο δεδομένων σε μικρό χρονικό διάστημα, οι οποίες δεν είναι διαθέσιμες στις βασικές IT τεχνολογίες.

Η μετέπειτα ανάλυση των μεταδεδομένων επικοινωνίας μπορεί να αποκαλύψει πιο ιδιωτικές πληροφορίες για τον χρήστη και από το ίδιο το περιεχόμενο των επικοινωνιών του. Επιπλέον, μπορεί να αποκαλύψει ένα εξαιρετικό ποσό πληροφοριών για τις συνήθειες και τις σχέσεις των ανθρώπων. Ειδικά όταν η ανάλυση δεδομένων συνδυάζεται με συγκεκριμένα χρονικά πλαίσια ή άλλα datasets μπορεί να αποσπάσει περισσότερες προσωπικές πληροφορίες του χρήστη καθώς και λεπτομέρειες σχετικά με τους χρήστες που επικοινωνεί. Έτσι, η ανάλυση των μεταδεδομένων μας δίνει έναν γράφο (Social Graph) , ο οποίος απεικονίζει τις επικοινωνίες όλων των χρηστών μεταξύ τους , εκθέτοντας τους στον κίνδυνο της μαζικής παρακολούθησης.

Οι τεχνολογίες Big Data, έχουν κυρίαρχο ρόλο στο φαινόμενο των μαζικών παρακολουθήσεων αφού παρέχουν όλα τα εργαλεία που χρειάζονται για ανάλυση μεγάλου όγκου δεδομένων σε λογικά χρονικά πλαίσια.

2.5. Τρόποι μαζικής παρακολούθησης

- Internet Monitoring: Ο έλεγχος Διαδικτύου (Internet Monitoring) είναι η παρακολούθηση των πακέτων δεδομένων που ανταλλάσσονται μέσω του πρωτοκόλλου IP. Η υποδομή που υποστηρίζει το Διαδίκτυο περιλαμβάνει τη φυσική υποδομή (καλώδια οπτικών ινών που συνδέουν πολλά κράτη μεταξύ τους ώστε να συνδέονται στο παγκόσμιο δίκτυο) και τα ηλεκτρονικά συστήματα (όπως οι διακόπτες επικοινωνίας, οι δρομολογητές, οι κεντρικοί υπολογιστές, κ.λπ.) για να συνδεθούν οι χρήστες. Ο έλεγχος Διαδικτύου μπορεί να πραγματοποιηθεί πέρα από οποιοδήποτε σημείο αυτής της υποδομής, ανάλογα με το ποιες πληροφορίες θέλει κανείς να συλλέξει.

  Μετά τη διαρροή των μυστικών εγγράφων των αμερικανικών αρχών από τον Edward Snowden, αποκαλύφθηκε ότι η Εθνική Υπηρεσία Ασφάλειας των Ηνωμένων Πολιτειών (NSA) είχε στην κατοχή της αντίγραφα της κίνησης του διαδικτύου η οποία καταγράφεται μέσω των δικτύων καλωδίων οπτικών ινών. Τον Ιούνιο του 2013, ήρθαν στην επιφάνεια στοιχεία που αποδεικνύουν ότι και η Βρετανική Υπηρεσία Πληροφοριών (GCHQ) συγκέντρωνε, επεξεργάζονταν και αποθήκευε δεδομένα μέσω του δικτύου οπτικών ινών από όπου ρέει όλη η διαδικτυακή κίνηση.

Μέσω των καλωδίων οπτικών ινών είναι δυνατή η παρακολούθηση όλων των τηλεπικοινωνιακών δικτύων. Αν εστιάσουμε στο γεγονός ότι οι Ηνωμένες Πολιτείες της Αμερικής συνδέονται με 63 χώρες μέσω καλωδίων οπτικών ινών, η Γαλλία με 60 χώρες, η Πορτογαλία με 59 χώρες, το Ηνωμένο Βασίλειο με 57 χώρες, η Ιταλία με 47 χώρες, η Γερμανία με 40 χώρες και τέλος η Ελλάδα με 37 χώρες μπορούμε να διαμορφώσουμε μια εικόνα για την έκταση των μαζικών παρακολουθήσεων.

Πέρα από την παρακολούθηση της τηλεπικοινωνιακής κίνησης και τη συλλογή δεδομένων μέσω των καλωδίων οπτικών ινών, η μαζική παρακολούθηση γίνεται και μέσω του Cloud(υπολογιστικό νέφος).

Το υπολογιστικό νέφος είναι ένα μοντέλο το οποίο παρέχει τη δυνατότητα ευχερούς, βασισμένης στη ζήτηση διαδικτυακής πρόσβασης σε ένα διαμοιραζόμενο χώρο—που μπορεί να περιλαμβάνει δίκτυα, εξυπηρετητές πρόσβασης, υπολογιστικά συστήματα αποθήκευσης, συστήματα εφαρμογών και υπηρεσιών— και το οποίο μπορεί να παρασχεθεί προς χρήση ή/και να πάψει η χρήση του γρήγορα και χωρίς ιδιαίτερη διαχειριστική προσπάθεια και σύμφωνα με ορισμένη διαδικασία που προβλέπει ο πάροχος της υπηρεσίας υπολογιστικού νέφους(P. Mell, T. Grace, (2011), The NIST Definition of Cloud Computing, National Institute of Standards and Technology, Special Publication 800-145).

Το cloud computing, το οποίο είναι ραγδαία αναπτυσσόμενο, αποτελεί πλέον το χώρο αντικείμενο χρήσης όλων των χρηστών τεχνολογικών εφαρμογών συνειδητά ή όχι. Όλα τα δεδομένα τα οποία αποστέλλονται μέσω διαδικτύου, συμπεριλαμβανομένων των δεδομένων που ορίζουν την ταυτότητα και την τοποθεσία κάθε χρήστη, αποθηκεύονται στο cloud. Αυτή η αποθήκευση δεδομένων και μη διατιθέμενη δυνατότητα διαγραφής στοιχείων από το νέφος έχει βοηθήσει στην προσπάθεια εξάλειψης οποιαδήποτε εγκληματικής παρουσίας στο διαδίκτυο.

Παρόλα αυτά, οι υπηρεσίες cloud αποτέλεσαν το έναυσμα της διαμάχης μεταξύ εταιρειών των οποίων η βάση βρίσκεται στην Ευρώπη και συνδιαλέγονται αδρά με τις ΗΠΑ. Από τον Οκτώβριο του 2015 και έπειτα, ολοένα και περισσότερες εταιρείες τείνουν να αποφεύγουν τη χρήση υπηρεσιών cloud εντός των Ηνωμένων Πολιτείων της Αμερικής και να εστιάζουν σε εταιρείες που προσφέρουν υπηρεσίες όπου αποθηκεύουν τα δεδομένα τους σε κέντρα δεδομένων σε χώρες της Ευρωπαϊκής Ένωσης.

Η τολμηρή κίνηση της θυγατρικής εταιρείας της Deutsche Telekom, T-systems σε συνεργασία με την εταιρεία Huawei η οποία εδρεύει στην Κίνα, να προσφέρει υπηρεσίες cloud όπου τα δεδομένα θα αποθηκεύονται σε κέντρα δεδομένων εντός των συνόρων της Ευρωπαϊκής Ένωσης, δείχνει τη σημασία της προστασίας δεδομένων εταιριών και πολιτών που βρίσκονται στο cloud.

Λόγοι για τους οποίους οι Ηνωμένες Πολιτείες επιζητούν πρόσβαση σε δεδομένα Ευρωπαίων πολιτών:

1. Πολιτικοί λόγοι και συμφέροντα.

2. Έλεγχος των κινήσεων στο ευρωπαϊκό οικονομικό τοπίο για λόγους ανταγωνισμού.

3. Φόβος πιθανών τρομοκρατικών πράξεων.

Οι νομοθεσίες που ισχύουν σχετικά με τις υπηρεσίες Cloud σε Αμερική και Ευρώπη αναλύονται στο κεφάλαιο 6.

- Παρακολούθηση μέσω Cookies: Τα cookies είναι αρχεία κειμένου που αποθηκεύει μια ιστοσελίδα στο τοπικό δίσκο ενός χρήστη που την έχει επισκεφθεί. Τα cookies επιτρέπουν εξυπνότερη και γρηγορότερη πλοήγηση, και χρησιμοποιούνται συνήθως για την εξατομίκευση του περιεχομένου του ιστοχώρου, καθώς και των διαφημίσεων από τρίτους που αφορούν τον εκάστοτε χρήστη της σελίδας.

  Υπάρχουν 2 τύποι cookies ανάλογα με τη διάρκεια ζωής τους:

  1. **Session cookies:** Τα Cookies τα οποία αποθηκεύονται στη μνήμη προσωρινά και διαγράφονται όταν τελειώσει η σύνοδος ή όταν κλείσει ο browser.

  2. **Persistent cookies:** Τα Cookies τα οποία παραμένουν αποθηκευμένα στον τοπικό δίσκο του χρήστη ακόμα και όταν ο browser είναι κλειστός. Διαγράφονται όταν λήξει ο χρόνος ζωής τους.

  Ο σκοπός των Session Cookies είναι να διατηρήσουν πληροφορίες κατάστασης ανάμεσα στις συνόδους. Στον αντίποδα, τα Persistent Cookies χρησιμοποιούνται για τη συσχέτιση μεταγενέστερων συνόδων ή επισκέψεων σε μία ιστοσελίδα.

  Οι πληροφορίες που μπορούν να αποθηκευτούν και να εξαχθούν μέσα από τα cookies είναι διαφορετικές και κυμαίνονται από τις πληροφορίες εγγραφής και σύνδεσης του χρήστη και τις προτιμήσεις του μέχρι και πληροφορίες που μπορεί να ανακτηθούν σε μελλοντικές συνεδρίες συμπεριλαμβανομένων των προσωπικών πληροφοριών που παρέχονται στον ιστοχώρο από τον χρήστη.

  Τα Cookies, λόγω των πολλών δυνατοτήτων αποθήκευσης δεδομένων, αποτελούν μια ελκυστική τεχνική μαζικής παρακολούθησης από διαφημιστικούς οργανισμούς και οργανισμούς παρακολούθησης. Οι οργανισμοί αυτοί εκμεταλλεύονται τα Cookies για τους δικούς τους σκοπούς, αφού δε χρειάζεται καμία έγκριση για την πρόσβαση, τη συλλογή πληροφοριών και την παρακολούθηση του ιστορικού περιήγησης στο διαδίκτυο του χρήστη.

  Τα Cookies επίσης, έχουν τη δυνατότητα να συλλέγουν δεδομένα από εφαρμογές και συσκευές που έχουν μια μοναδική σύνοδο σύνδεσης. Μπορούν, δηλαδή μέσω των εφαρμογών να βρίσκουν την τοποθεσία του χρήστη της κινητής συσκευής και να παρακολουθούν τις αλλαγές που κάνει ο χρήστης στα στοιχεία λογαριασμού του σε διαφορετικές πλατφόρμες σύνδεσης.

- Παρακολούθηση βασισμένη στα κενά κρυπτογράφησης: Οι αποκαλύψεις του Edward Snowden περί μαζικής επιτήρησης δεδομένων, επισήμαναν την έλλειψη γνώσης των χρηστών του διαδικτύου για τις παραβιάσεις ασφαλείας λόγω λαθών στη χρήση της κρυπτογραφίας . Μετά την επίθεση της 11ης Σεπτεμβρίου 2011, οι αρχές άλλαξαν τη μέχρι τότε τακτική παρακολούθησης των επικοινωνιών η οποία επικεντρωνόταν σε συγκεκριμένους χρήστες σε μαζική παρακολούθηση όλων των χρηστών μετατρέποντας έτσι την κρυπτογραφία από ένα μέσο end-to-end κρυπτογραφίας για την προστασία των χρηστών σε ένα εργαλείο που εκθέτει σε κίνδυνο τα δεδομένα εκατομμυρίων χρηστών. Παραδείγματα αυτού του φαινομένου είναι τα Heartbleed και Go-to-fail bugs, τα οποία χρησιμοποιούνται

για να «σπάσουν» την κρυπτογραφία που χρησιμοποιείται για τα δεδομένα χρηστών σε διακομιστές και σε συσκευές. Άλλες μορφές επιθέσεων λόγω ελαττωμάτων κρυπτογράφησης είναι οι επιθέσεις που συνδέονται με τεχνικές social engineering και τεχνικές που επιτρέπουν την υποκλοπή των δεδομένων πριν αυτά κρυπτογραφηθούν.

Προβλήματα στην κρυπτογράφηση δεδομένων που εκθέτουν τους χρήστες στη μαζική παρακολούθηση :Σημαντικές επιθέσεις εμφανίζονται όταν δεν συμμορφώνονται πιστά οι εφαρμογές των τρεχουσών τεχνολογιών κρυπτογράφησης με τις προδιαγραφές τους, ή όταν bugs και «ελαττώματα» –μερικές φορές σκόπιμα- εγχέονται σε επίπεδο κώδικα. Ακόμα και ο open source κώδικας δεν εγγυάται να είναι χωρίς οποιαδήποτε ρωγμή λογισμικού. Οι ρωγμές λογισμικού στην εφαρμογή των αλγορίθμων κρυπτογράφησης (π.χ. στη διαπραγμάτευση, ή τις βασικές λειτουργίες ανταλλαγής) μπορούν να οδηγήσουν στις ευπάθειες που μπορούν να είναι εύκολα εκμεταλλεύσιμες, ανεξάρτητα από την πολυπλοκότητα, ή τη θεωρητική δύναμη και την ποιότητα της εφαρμοσμένης τεχνικής κρυπτογράφησης. Δεδομένου ότι η εφαρμογή είναι το κρίσιμο μέρος που καθορίζει τη γενική ποιότητα των λύσεων κρυπτογράφησης, μια διαδικασία για την ικανοποίηση αυτών των δεικτών πρέπει να εφαρμοστεί.

Επιθέσεις που οφείλονται σε κρυπτογραφικό περιεχόμενο:
1.“Goto fail” SSL vulnerability: Το Secure Socket Layer πρωτόκολλο χρησιμοποιείται για την κρυπτογράφηση και την πιστοποίηση αυθεντικότητας των συνδέσεων μεταξύ διακομιστών. Για την ασφάλεια της επικοινωνίας τους, ο διακομιστής και ο χρήστης μοιράζονται ένα κλειδί το οποίο κρυπτογραφείται από τον χρήστη και αποκρυπτογραφείται μόνο από τον διακομιστή. Το go-to-fail bug δημιουργούσε ένα διπλότυπό του στον πηγαίο κώδικα με αποτέλεσμα να επιτρέπει στον καθένα να αφουγκράζεται την επικοινωνία με μια απλή επίθεση man-in-the-middle.
2.Heartbleed: Security bug που εμφανίστηκε σε OpenSSL κρυπτογραφία και επιτρέπει την ανάγνωση περισσότερων δεδομένων από όσα επιτρέπεται δια νόμου.
3.Shellshock bug: Σφάλμα το οποίο εστιάζει σε συσκευές που χρησιμοποιούν λογισμικό Linux ή Mac OS και μπορεί να πάρει τον έλεγχο του συστήματος και να εκτελεί τυχαίες εντολές. Περισσότερες από 500 εκατομμύρια συσκευές έχουν μολυνθεί από αυτό το bug, το οποίο φαίνεται να υπάρχει από το 1989.
4.Phishing attacks: Οι επιθέσεις αυτές δε βασίζονται στις αποτυχίες κρυπτογράφησης, αλλά στο social engineering. Τα θύματα δέχονται emails τα οποία φαίνονται έντιμα και τα οποία ζητούν τα προσωπικά στοιχεία τους και απαντούν αποστέλλοντας τα στοιχεία τους χωρίς να ξέρουν ότι είναι εκτεθειμένοι σε επίθεση.
5.Botnets: Δίκτυα συσκευών που μολύνονται με κακόβουλο λογισμικό, οι οποίες έπειτα τίθενται υπό το χειρισμό των επιτιθέμενων. Τα botnets χρησιμοποιούνται ως εργαλεία για DDoS επιθέσεις.
6.Zero-day vulnerabilities: Είναι μια ατέλεια στο λογισμικό που είναι άγνωστη στον προμηθευτή του. Το λογισμικό έπειτα γίνεται εστία επιθέσεων μέχρι να εντοπιστεί και να επιλυθεί το πρόβλημα.
7.Brute Force attacks: Αυτές οι επιθέσεις είναι ευρέως γνωστές και εξετάζουν όλο το σύστημα του χρήστη μέχρι να βρουν κάποιο ελάττωμα το οποίο και θα εκμεταλλευτούν για να αποσπάσουν τα δεδομένα του χρήστη.

- Παρακολούθηση που οφείλεται σε σφάλματα σχεδίασης του λογισμικού: Δημοσιογραφικές αναφορές στρέφουν τα βέλη τους στους Ασιάτες

κατασκευαστές κατηγορώντας τους ότι συμπεριλαμβάνουν κενά διαφυγής πληροφοριών στα τσιπ τους εσκεμμένα. Πιο συγκεκριμένα, οι κατηγορίες αυτές βασίζονται ακαδημαϊκώς στην δημοσιευμένη έκθεση του σπουδαστή του πανεπιστημίου του Cambridge, Sergei Skorobogatov στην οποία αναφέρει ότι εντόπισε ένα κενό στο τσιπ ProASIC3 της εταιρίας Actel/Microsemi. Μετά από ενδελεχή έρευνα, αποδείχτηκε ότι το συγκεκριμένο σφάλμα που εντόπισε ο Skorobogatov εμπεριεχόταν στο σχεδιασμό του συγκεκριμένου τσιπ της εταιρίας Actel η οποία είναι αμερικάνικη.

Στα έγγραφα τα οποία διέρρευσε ο Edward Snowden, επιβεβαιώνεται ότι η NSA μυστικά εμφυτεύει εργαλεία μαζικής παρακολούθησης σε συσκευές που συνδέονται άμεσα στο διαδίκτυο, όπως servers, routers κα, τις επανασυσκευάζει και έπειτα τις στέλνει σε κράτη εκτός των Ηνωμένων Πολιτειών για χρήση. Με αυτόν τον τρόπο, η NSA αποκτά πρόσβαση σε δίκτυα και στους λογαριασμούς των χρηστών αυτών των δικτύων. Παρόλα αυτά δεν υπάρχει κάποια απόδειξη ότι οι προμηθευτές συνεργάζονται με την NSA για την τοποθέτηση των εργαλείων μαζικής παρακολούθησης χρηστών.

- <u>Παρακολούθηση των τηλεπικοινωνιών:</u>
  Στον τηλεπικοινωνιακό τομέα, από άποψη ασφαλείας υπάρχουν οι εξής κίνδυνοι για να γίνουν επιθέσεις παρακολούθησης:
  - Εξαγορά των παρόχων τηλεπικοινωνιακών υπηρεσιών από τις αρχές για την πρόσβαση στα δίκτυά τους. Σύμφωνα με την εφημερίδα Washington Post και το περιοδικό Forbes, η NSA πλήρωσε παρόχους τηλεπικοινωνιακών υπηρεσιών όπως οι Verizon και AT&T για να αποκτήσει πρόσβαση στο 81% όλων των υπερατλαντικών τηλεφωνημάτων που διεξάγονται εντός των ηνωμένων πολιτειών.
  - Επιθέσεις που βασίζονται στα τρωτά σημεία των δικτύων επικοινωνιών. Οι επιθέσεις αυτές συμβαίνουν όταν πρέπει να χρησιμοποιηθεί ο μηχανισμός για την εναλλαγή μιας σύνδεσης από 2G σε 3G δίκτυο, καθώς το πρωτόκολλο που χρησιμοποιείται παρουσιάζει πολλά κενά και μπορεί να παρακαμφθεί εύκολα.
  - Κακόβουλο λογισμικό σε συσκευές κινητών επικοινωνιών. Η εξέλιξη της τεχνολογίας των κινητών συσκευών επιφέρει και την εξέλιξη των ιών που μπορούν να προσβάλλουν τις συσκευές. Παράγοντες που αυξάνουν τον κίνδυνο των επιθέσεων είναι η κινητικότητα, το GPS και η χρήση της κάμερας ενός κινητού.

2.6 Τρόποι επιθέσεων στα δίκτυα κινητής τηλεφωνίας

Οι τρόποι επιθέσεων στα δίκτυα κινητής τηλεφωνίας σε ευρωπαϊκό επίπεδο είναι οι εξής:

α. Κρυπτογραφικές επιθέσεις
β. Επιθέσεις Over The Air (OTA)
γ. Επιθέσεις από τους παρόχους υπηρεσιών
δ. Επιθέσεις για την αλλοίωση της μνήμης
ε. Τρωτά σημεία πρωτοκόλλων επικοινωνίας

Η ευπάθεια των τηλεπικοινωνιακών πρωτοκόλλων όλων των γενιών, από το GSM μέχρι το 4G και του 5G μετέπειτα, σε συνδυασμό με τη μεγάλη, εκτεθειμένη σε επιθέσεις, επιφάνεια των κινητών συσκευών, τις καθιστούν εύκολο στόχο για επιθέσεις από χακερς.

Τα τρωτά σημεία των τηλεπικοινωνιακών δικτύων που θέτουν τις επικοινωνίες στον

κίνδυνο επιθέσεων είναι:

- Η κρυπτογράφηση των 3G δικτύων καλύπτει μόνο τη σύνδεση μεταξύ του χρήστη του τηλεφώνου και του σταθμού βάσης του παρόχου. Όλες οι υπόλοιπες επικοινωνίες δεν κρυπτογραφούνται.
- Είναι πιθανό να γίνεται αποκρυπτογράφηση των επικοινωνιών σε GSM σε πραγματικό χρόνο και να υποκλαπούν οι επικοινωνίες και τα δεδομένα του χρήστη. Το GSM χρησιμοποιεί πολλών ειδών πρωτόκολλα: πρωτόκολλα για την αναγνώριση του χρήστη, για τον έλεγχο αυθεντικότητας του χρήστη και για την μετάδοση φωνής και δεδομένων του χρήστη. Οι αλγόριθμοι αυτοί διαμοιράζονται ανάμεσα στον πάροχο υπηρεσιών GSM, στις συσκευές κινητών επικοινωνιών και στην κάρτα SIM που χρησιμοποιείται. Η Μετάδοση φωνής και δεδομένων γίνεται μέσω του πρωτοκόλλου A5, έπειτα από τον έλεγχο ταυτότητας του χρήστη από το δίκτυο. Το πρωτόκολλο A5 έχει 3 διαφορετικές εκδοχές: τα A5/1, A5/2 και A5/3. Το πρωτόκολλο A5/1 χρησιμοποιείται στο GSM και είναι υπεύθυνο για τη διατήρηση της ασφάλειας των τηλεπικοινωνιών κατά τη διάρκεια των συνδιαλέξεων.
- Τα πρότυπα των δικτύων 2G δεν ισχύουν πια κι έτσι υπάρχει ο κίνδυνος επιθέσεων κατά τη μεταπομπή των 2G κλήσεων σε 3G δίκτυα.
- Το 4G είναι ένα καινούριο πρωτόκολλο το οποίο υποστηρίζει όλες τις επικοινωνίες που βασίζονται στο πρωτόκολλο IP. Εφόσον το πρωτόκολλο του 4G βασίζεται στο TCP/IP πρωτόκολλο, αυτό σημαίνει ότι το πρωτόκολλο 4G υιοθετεί τις δυνατότητες και τις αδυναμίες του TCP/IP, τραβώντας τη προσοχή των πολλών χάκερ με γνώσεις του IP πρωτοκόλλου.
- Το πρωτόκολλο 4G είναι λιγότερο ασφαλές από τα προηγούμενα πρωτόκολλα κινητών επικοινωνιών.

2.7 Η μαζική παρακολούθηση ως μαζικό προϊόν προς πώληση

Η μαζική παρακολούθηση αποτελεί έναν επιχειρηματικό τομέα στον οποίο οι εταιρίες διαθέτουν προς πώληση εφαρμογές και εργαλεία λογισμικού για σκοπούς παρακολούθησης. Το αγοραστικό κοινό αυτής της βιομηχανίας είναι οργανισμοί οι οποίοι αποζητούν εξεζητημένες λύσεις για τη νόμιμη παρακολούθηση, συλλογή και ανάλυση δεδομένων μυστικών υπηρεσιών, υπηρεσιών εθνικής ασφάλειας καθώς και οργανισμών επιβολής των νόμων.

Η έννομη παρακολούθηση η οποία αποτελεί απόφαση δικαστηρίου βασισμένη σε αποδείξεις παράνομων ή τρομοκρατικών ενεργειών είναι απαραίτητο εργαλείο των αρχών του νόμου. Στις περιπτώσεις ,όμως, που δεν υφίσταται η συγκατάθεση δικαστηρίου, η παρακολούθηση των δεδομένων αποτελεί απειλή για τα δικαιώματα ελευθερίας του λόγου και της έκφρασης του ανθρώπου.

Οι τεχνικές μαζικής παρακολούθησης μπορούν να παρεμποδιστούν, αλλά μιλώντας με τεχνικούς όρους, δεν υπάρχει τεχνική για την πλήρη αποφυγή χρήσης τους. Γι' αυτό το λόγο, είναι επιτακτική η ανάγκη ισορροπίας μεταξύ των συμφερόντων των οργανισμών ασφαλείας και των δικαιωμάτων του ανθρώπου ο οποίος γίνεται το αντικείμενο παρακολούθησης.

Σύμφωνα με τον οργανισμό HRC (Human Rights Campaign), διακρίνονται 5 τύποι παρακολούθησης των τηλεπικοινωνιών:

1. Στοχευμένη παρακολούθηση των επικοινωνιών.
2. Μαζική παρακολούθηση των επικοινωνιών.
3. Πρόσβαση σε δεδομένα που χρησιμοποιούνται για την επικοινωνία.
4. Λογοκρισία μέσω του διαδικτύου.
5. Απαγορεύσεις της χρήσης του δικαιώματος της ανωνυμίας.

Σύμφωνα με παρουσίαση που έγινε στο συνέδριο ISS World Wide East το 2014, οι 10 πιο σοβαρές διαδικτυακές απειλές που αντιμετωπίζουν οι αρχές είναι οι εξής:

- Το εύρος ανάπτυξης των οπτικών ινών και συνάμα η αύξηση του εύρους των ανιχνευτών πληροφοριών μέσω των οπτικών ινών.
- Τα smartphones
- Η κρυπτογράφηση
- Η παρακολούθηση μέσω των social media
- Ο αυξανόμενος όγκος δεδομένων και η χρήση των τεχνολογιών Big Data ως λύση στο πρόβλημα
- Η παρακολούθηση της θέσης ενός χρήστη μέσω των κεραιών 3G και 4G δικτύων
- Όλες οι μελλοντικές υποδομές οι οποίες δε θα στηρίζονται στην ασφάλεια των καλωδίων αλλά σε τεχνολογίες cloud.
- Το σκοτεινό ίντερνετ (Dark Web) το οποίο αναλύεται εκτενώς σε επόμενο κεφάλαιο της εργασίας
- Τα dark emails
- Παραθυράκια στις νομοθεσίες που εγκρίνουν την παρακολούθηση των δεδομένων.

Πολλές από αυτές τις απειλές χρησιμοποιούνται για διαφημιστικούς λόγους από τους εμπόρους εργαλείων παρακολούθησης. Πιο συγκεκριμένα:

- Η εταιρία Verint με έδρα το Melville της Νέας Υόρκης, προωθεί ένα προϊόν το οποίο στην περιγραφή του παρουσιάζεται ως «Λύσεις μαζικής παρακολούθησης για δίκτυα εθνικής εμβέλειας και στρατηγικές λύσεις για την παρακολούθηση GSM δικτύων».
- Η εταιρία Nice Systems, παρουσιάζει το κέντρο μαζικής ανίχνευσης της (NiceTrack Mass Detection Center) ως μια ολοκληρωμένη πλατφόρμα η οποία παρέχει παρακολούθηση και ανάλυση δεδομένων σε εθνικό επίπεδο.
- Τέλος, η γαλλική εταιρία Amesys, πουλάει το σύστημα παρακολούθησης Eagle το οποίο έχει τη δυνατότητα νόμιμης και μαζικής παρακολούθησης.

Η πώληση αυτών των προϊόντων μαζικής παρακολούθησης απαγορεύεται να γίνεται σε τοπικές και κυβερνητικές αρχές και οι περισσότεροι από τους εμπόρους το θέτουν ως πολιτική για την πώληση των προϊόντων τους. Παρόλα αυτά, σύμφωνα με μελέτη του οργανισμού για τα ανθρώπινα δικαιώματα HRC, οι τεχνολογίες μαζικής παρακολούθησης πωλούνται σε χώρες όπου ο κίνδυνος καταπάτησης των δικαιωμάτων ελευθερίας των ανθρώπων μέσω παρακολούθησης των δεδομένων τους είναι μεγάλος. Τέτοιες χώρες είναι η Λιβύη, το Μπαχρέιν, η Συρία, η Αίγυπτος και η Τυνησία για τις οποίες υπάρχουν πολλές αναφορές χρήσης λογισμικού για την παρακολούθηση των πολιτών τους.

Οι παρακάτω εταιρείες αποτελούν τους μεγαλύτερους εμπόρους λογισμικού παρακολούθησης και κατηγορούνται για την προμήθεια τεχνολογίας παρακολούθησης σε χώρες οι οποίες παραβιάζουν επανειλημμένως τα ανθρώπινα δικαιώματα.

α. Gamma Group

Η Gamma Group είναι μια εταιρεία με έδρες στο Ηνωμένο Βασίλειο και τη Γερμανία, η οποία παρέχει εργαλεία παρακολούθησης σε εθνικές υπηρεσίες ερευνών και ασφαλείας σύμφωνα με την ιστοσελίδα της.

Το πιο περιζήτητο προϊόν της είναι το FinFisher kit, το οποίο παρουσιάζεται ως η πιο εξελιγμένη λύση για παρακολούθηση που υπάρχει στην αγορά. Το FinFisher, περιλαμβάνει ιούς Trojan με σκοπό να μολύνει τους υπολογιστές, τα κινητά τηλέφωνα , άλλες ηλεκτρονικές συσκευές καθώς και servers. Το λογισμικό FinSpy έπειτα, συλλέγει πληροφορίες από τον μολυσμένο υπολογιστή όπως

κωδικούς και επικοινωνίες μέσω Skype και στέλνει τις πληροφορίες πίσω στον server του FinFisher.

β.Hacking Team

Η εταιρία Hacking Team με έδρα το Μιλάνο, δίνει τη δυνατότητα παρακολούθησης χωρίς να χρειαστεί η αποκρυπτογράφηση των δεδομένων αφού εγκαθίσταται λογισμικό στη συσκευή το οποίο αποθηκεύει τα δεδομένα προτού κρυπτογραφηθούν. Αν και η πολιτική πώλησης του λογισμικού της εταιρίας τονίζει ότι δεν πωλούνται προϊόντα σε χώρες που βρίσκονται στη μαύρη λίστα των Ηνωμένων Πολιτειών, της Ευρώπης, των Ηνωμένων Εθνών και του ΝΑΤΟ, πολλές αναφορές και ειδικοί ασφάλειας τηλεπικοινωνιακών συστημάτων έχουν εντοπίσει ίχνη του λογισμικού αυτού σε χώρες που έχουν αμφισβητήσιμη θέση όσον αφορά τα ανθρώπινα δικαιώματα, όπως το Μαρόκο και τα Ηνωμένα Αραβικά Εμιράτα.

γ. Blue Coat

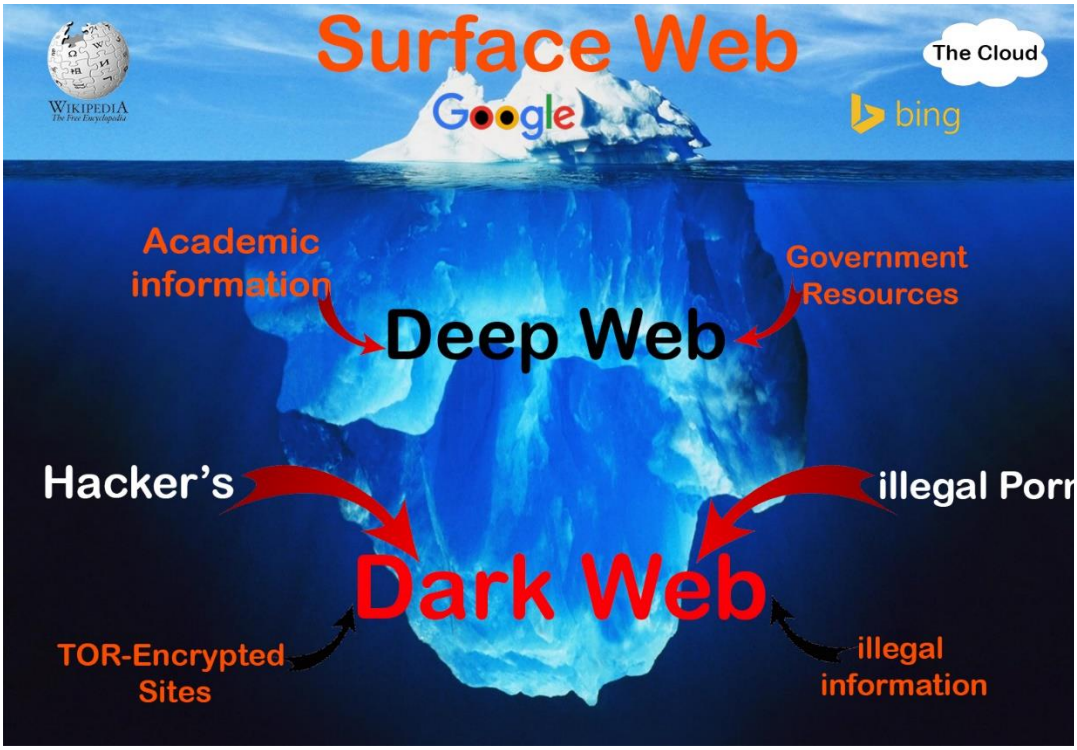
Η Blue Coat είναι αμερικάνικη εταιρία η οποία ειδικεύεται στην ανάπτυξη λογισμικού για την ασφάλεια των υπολογιστικών συστημάτων. Η φήμη της όμως εκτείνεται και στη δημιουργία και εμπορία λογισμικού παρακολούθησης. Ερευνητές του πανεπιστημίου του Τορόντο, ανακάλυψαν ότι οι συσκευές Blue Coat ProxySG και Blue Coat PacketShaper χρησιμοποιούνται για παρακολούθηση στις παρακάτω χώρες:

-61 συσκευές Blue Coat ProxySG σε: Αίγυπτο, Κουβέιτ, Κατάρ, Σαουδική Αραβία και Ηνωμένα Αραβικά Εμιράτα.

-316 συσκευές PacketShaper σε: Αφγανιστάν, Μπαχρέιν, Κίνα, Ινδία, Ινδονησία, Ιράκ, Κένυα, Κουβέιτ, Λίβανο, Μαλαισία, Νιγηρία, Κατάρ, Ρωσία, Σαουδική Αραβία, Νότια Κορέα, Σιγκαπούρη, Ταϊλάνδη, Τουρκία και Βενεζουέλα.

3. DEEP WEB

3.1. Επίπεδα του Web



Εικόνα 1: Δομή του διαδικτύου

Το ευρύ δίκτυο διαχωρίζεται σε δύο είδη δικτύου. Υπάρχει το επιφανειακό δίκτυο(Surface Web) που οι περισσότεροι άνθρωποι χρησιμοποιούν καθημερινά, το οποίο είναι εύκολα προσβάσιμο και οι ιστοσελίδες είναι όλες καταχωρημένες στις μηχανές αναζήτησης. Εκτός από το κανονικό δίκτυο υπάρχει και το βαθύ δίκτυο (deep web), δηλαδή κρυμμένες ιστοσελίδες που δεν εμφανίζονται χρησιμοποιώντας τις γνωστές μηχανές αναζήτησης.

Το surface web είναι το τμήμα του διαδικτύου που οι συμβατικές μηχανές αναζήτησης μπορούν να αναζητήσουν και οι web browsers μπορούν να έχουν πρόσβαση χωρίς την ανάγκη χρήσης ειδικού λογισμικού και διαμορφώσεων. Αυτό το προσβάσιμο κομμάτι του Internet ονομάζεται και Clearnet.

Σε αντίθεση με το surface web, το Deep Web μπορεί να προσεγγιστεί μόνο μέσω ειδικού λογισμικού. Σε αυτό συμπεριλαμβάνονται δυναμικές ιστοσελίδες, μπλοκαρισμένα site (όπως για παράδειγμα αυτά τα οποία ζητάνε την απάντηση σε ένα CAPTCHA), ασύνδετα site, ιδιωτικά site (όπως αυτά που απαιτούν διαπιστευτήρια σύνδεσης) και δίκτυα περιορισμένης πρόσβασης.

Τα δίκτυα περιορισμένης πρόσβασης καλύπτουν όλα εκείνα τα μέσα και τις υπηρεσίες που δεν θα ήταν κανονικά προσβάσιμα με ένα τυπικά διαμορφωμένο δίκτυο και έτσι προσφέρουν ενδιαφέρουσες δυνατότητες σε κακόβουλους παράγοντες να ενεργούν μερικώς ή ολικώς απαρατήρητα από την επιβολή του νόμου. Αυτά περιλαμβάνουν site με domain names που έχουν καταχωρηθεί στο Σύστημα Ονοματοδοσίας Διαδικτύου (Domain Name System -DNS), ρίζες που δεν διαχειρίζονται από τον Οργανισμό του Διαδικτύου για την Εκχώρηση Ονομάτων και Αριθμών (Internet Corporation for Assigned Names and Numbers-ICANN) και ως εκ τούτου, διαθέτουν

διευθύνσεις URL με μη τυπικά top-level domains (TLDs) που γενικά απαιτούν ένα συγκεκριμένο διακομιστή DNS για την σωστή επίλυση. Άλλα παραδείγματα είναι site τα οποία έχουν καταχωρημένο το domain name τους σε ένα τελείως διαφορετικό σύστημά από το πρότυπο DNS, όπως .BIT domains. Αυτά τα συστήματα όχι μόνο ξεφεύγουν τους κανονισμούς του DNS που επιβάλλει η ICANN, αλλά και η αυτοδιοίκητη φύση του εναλλακτικού DNS καθιστά πολύ δύσκολο να παγιδευτούν αν χρειαστεί.

Επίσης στα περιορισμένης πρόσβασης δίκτυα ανήκουν τα darknets[9]. Το Dark Web υπάρχει στα darknets τα οποία είναι δίκτυα επικάλυψης (overlay networks). Τα δίκτυα επικάλυψης υλοποιούνται «πάνω» από ένα άλλο δίκτυο. Στην περίπτωσή μας, τα darknets υλοποιούνται «πάνω» από το surface web αλλά αν κάποιος δε γνωρίζει δε μπορεί να έχει πρόσβαση σε αυτά καθώς απαιτούν τη χρήση ειδικού λογισμικού όπως π.χ. το Tor. Το μεγαλύτερο ενδιαφέρον στο deep web συγκεντρώνεται στις δραστηριότητες που συμβαίνουν στα darknets.

Παρόλο που ο διαχωρισμός του deep web και surface web είναι ξεκάθαρος, βρίσκεται μεγάλη σύγχυση όσον αφορά τον διαχωρισμό των deep web και dark web. Το dark web δεν είναι το deep web παρά μόνο ένα μέρος του. Το Dark Web βασίζεται σε darknets ή δίκτυα όπου οι συνδέσεις γίνονται μέσω έμπιστων peers. Παραδείγματα εργαλείων για πρόσβαση στο Dark Web είναι τα Tor, Freenet, ή Invisible Internet Project (I2P)[10].

3.2 Τρόποι εισόδου στο Deep και κατ' επέκταση στο Dark Web

Υπάρχουν αρκετοί τρόποι για αποκτηθεί πρόσβαση στο dark web, συμπεριλαμβανομένης της χρήσης των Tor, Freenet και I2P. Από αυτούς τους τρόπους, ο πιο δημοφιλής είναι το Tor (αρχικά ονομαζόταν The Onion Router), εν μέρει επειδή είναι ένα από τα ευκολότερα πακέτα λογισμικού προς χρήση[11]. Το Tor παρέχει μυστικότητα και ανωνυμία αφού διαδίδει μηνύματα από τον αποστολέα στον παραλήπτη μέσω μεσαζόντων, ειδικά διαμορφωμένων υπολογιστών. Το μήνυμα μεταφέρεται από τον ένα κόμβο στον άλλο και είναι κρυπτογραφημένο με έναν τρόπο ώστε ο κάθε μεσάζοντας να γνωρίζει μόνο για το μηχάνημα που έστειλε το μήνυμα και το μηχάνημα που αυτό θα σταλεί. Αντί για τις συμβατικές διευθύνσεις Web, το Tor χρησιμοποιεί «onion» διευθύνσεις, οι οποίες αποκρύπτουν περαιτέρω το περιεχόμενο. Υπάρχουν ακόμη και ειδικές εκδόσεις των μηχανών αναζήτησης όπως το Bing και Duck Duck Go, που επιτρέπουν onion διευθύνσεις οι οποίες υπάρχουν εξειδικευμένα για υπηρεσίες Tor. Παρόλα αυτά, είναι λάθος να θεωρείται ότι το Tor είναι εντελώς ανώνυμο. Αν ένα site είναι προσβάσιμο, ενδεχομένως κάποιος μπορεί να βρει πληροφορίες για το ποιος έχει πρόσβαση λόγω των πληροφοριών που μοιράζονται, καθώς και ονόματα χρηστών και ηλεκτρονικές διευθύνσεις μηνυμάτων. Εκείνοι που θέλουν να μείνουν εντελώς ανώνυμοι πρέπει να χρησιμοποιήσουν ειδικές υπηρεσίες ανωνυμίας για να κρύψουν την ταυτότητά τους σε αυτές τις περιπτώσεις.

Επίσης, άλλος ένας δημοφιλής τρόπος πρόσβασης στο dark web είναι μέσω της χρήσης του Freenet. Το Freenet είναι ελεύθερο λογισμικό που επιτρέπει στον χρήστη να μοιραστεί αρχεία ανώνυμα, να περιηγηθεί και να δημοσιεύσει "freesites" (web sites προσβάσιμα μόνο μέσω Freenet) και να κάνει chat στο φόρουμ, χωρίς το φόβο της λογοκρισίας. Το Freenet είναι αυτοδιοίκητο, ώστε να είναι λιγότερο ευάλωτο σε επιθέσεις, και αν χρησιμοποιείται σε Dark Web λειτουργία, όπου οι χρήστες συνδέονται μόνο με τους φίλους τους, είναι πολύ δύσκολο να ανιχνευθεί. Οι επικοινωνίες από τους κόμβους του Freenet είναι κρυπτογραφημένες και δρομολογούνται μέσω άλλων κόμβων ώστε να είναι εξαιρετικά δύσκολο να προσδιοριστεί το ποιος ζητά πληροφορίες και ποιο είναι το περιεχόμενό τους.Έχοντας σύνδεση μόνο με τους ανθρώπους που εμπιστεύονται, οι χρήστες μπορούν να μειώσουν σημαντικά την ευπάθειά τους, συνεχίζοντας όμως να μπορούν να συνδεθούν σε ένα παγκόσμιο δίκτυο μέσω φίλων

των φίλων τους. Αυτό επιτρέπει την χρήση του Freenet ακόμα και σε μέρη όπου μπορεί να είναι παράνομο, το κάνει πολύ δύσκολο ακόμα και για κυβερνήσεις να το μπλοκάρουν, και δεν βασίζεται στην ένωση με τον “ελεύθερο κόσμο”[12].

Τέλος, το I2P είναι ένα ανώνυμο δίκτυο επικάλυψης. Σκοπός του είναι να προστατεύσει την επικοινωνία από τις αρχές που αποσκοπούν την παρακολούθηση για εύρεση εγκληματικών ενεργειών και παρακολούθηση από τρίτους, όπως ISPs.Το I2P χρησιμοποιείται από πολλούς ανθρώπους που νοιάζονται για την ιδιωτικότητά τους όπως, ακτιβιστές, καταπιεσμένοι άνθρωποι, δημοσιογράφοι και πληροφοριοδότες, καθώς και το μέσο άτομο. Όπως προαναφέρθηκε, κανένα δίκτυο δεν μπορεί να είναι πλήρως ανώνυμο, παρόλα αυτά συνεχίζονται προσπάθειες ώστε να επιτευχθεί η ανωνυμία και να γίνει ισχυρότερη[13].

3.3 Χρησιμότητα του Deep Web

Ο κύριος σκοπός για τον οποίο κάποιος προτιμά να πλοηγηθεί στο σκοτεινό δίκτυο και όχι στο επιφανειακό είναι η προστασία της ιδιωτικότητάς του. Στο surface web, μια κοινή τεχνική παρακολούθησης είναι η «traffic analysis»(ανάλυση της κίνησης), η οποία χρησιμοποιείται για να ανακαλύψει ποιος συνδιαλέγεται με ποιόν σε ένα δημόσιο δίκτυο. Επίσης χρησιμοποιείται για να ορίσει την τοποθεσία και την online συμπεριφορά ενός χρήστη. Συνεπώς μια καλή λύση για αποφυγή της παρακολούθησης, είναι η περιήγηση στο deep web.

Ένας άλλος λόγος ο οποίος καθιστά το deep web θελκτικό, είναι η ανωνυμία που προσφέρει. Πολλοί δημοσιογράφοι χρησιμοποιούν το deep web για να έρθουν σε επαφή με άτομα τα οποία δεν πρέπει να βγει στο φως της δημοσιότητας ότι μιλάνε. Επιπλέον πολλές φορές κάποιος μπορεί να στείλει υλικό κατάλληλο για έρευνα σε δημοσιογράφους, χωρίς να αποκαλύψει την ταυτότητά του. Το deep web χρησιμοποιείται πολύ από πολιτικούς για λόγους ασφαλείας-δεν είναι άλλωστε λίγες οι περιπτώσεις διάρρευσης συνομιλιών και σκανδάλων από hackers που έλαβαν μέρος στο σκοτεινό μέρος του διαδικτύου.

Το deep web αποτελεί έναν ασφαλή χώρο για να μοιραστεί κάποιος δεδομένα και αρχεία, καθώς και να τα αποθηκεύσει. Η μεταφορά αρχείων μέσω του deep web, καθιστά πολύ δύσκολη την παρακολούθηση της διαδρομής από τον αποστολέα μέχρι τον παραλήπτη. Το deep web επιλέγεται λοιπόν από χρήστες οι οποίοι θέλουν να διατηρήσουν κρυφές τις ανταλλαγές δεδομένων τους. Πολλοί μάλιστα χρησιμοποιούν το deep web για αποθήκευση των δεδομένων τους, κάτι που δεν έχει εξακριβωθεί ακόμα ότι είναι πλήρως ασφαλές αφού είναι πιθανό κάποιος να διαγράψει αρχεία ενός άλλου χρήστη.

Το deep web μπορεί κάποιος να το χρησιμοποιήσει για ασφαλείς και κρυφές συναλλαγές. Επειδή το deep web χρησιμοποιείται για λόγους ανωνυμίας και ασφάλειας από παρακολουθήσεις, δε χρησιμοποιούνται λογαριασμοί για τις συναλλαγές, αλλά ένα εικονικό νόμισμα που ονομάζεται Bitcoin. Στην παρούσα φάση, υπάρχουν περίπου 11 εκατομμύρια bitcoins και κάθε ένα από αυτά έχει ένα μοναδικό online αριθμό εγγραφής. Οι αριθμοί αυτοί δημιουργούνται μέσω μιας διαδικασίας που ονομάζεται «mining» , που ουσιαστικά είναι ένας υπολογιστής ο οποίος λύνει ένα δύσκολο μαθηματικό πρόβλημα και για κάθε φορά που ένα πρόβλημα λύνεται σωστά, ο κάτοχος του υπολογιστή κερδίζει 25 bitcoins. Κάθε χρήστης, για να μπορεί να λαμβάνει και να στέλνει bitcoins, πρέπει να έχει μια διεύθυνση bitcoin, η οποία είναι μια ακολουθία από 27 έως 34 τυχαία επιλεγμένα γράμματα και αριθμούς. Αυτές οι διευθύνσεις δεν είναι καταχωρημένες πουθενά και κατά συνέπεια οι χρήστες μπορούν να κάνουν τις συναλλαγές τους ανώνυμα. Τέλος, οι διευθύνσεις αυτές αποθηκεύονται σε πορτοφόλια bitcoin , στα οποία κάποιος μπορεί να κάνει αποταμίευση καθώς λειτουργούν με τρόπο όμοιο σαν κρυφοί λογαριασμοί τραπέζης.

Τέλος, πολλοί άνθρωποι χρησιμοποιούν την πρόσβασή τους στο Deep web, για να συνδεθούν στους λογαριασμούς κοινωνικής δικτύωσής τους όπως το Facebook. Αυτό συμβαίνει διότι σε κάποιες χώρες όπως η Κίνα και το Ιράν, οι αρχές έχουν μπλοκάρει την πρόσβαση στο Facebook. Μέσω του Tor λοιπόν, ο καθένας σε όλο τον κόσμο μπορεί να έχει πρόσβαση στον προσωπικό του λογαριασμό στο Facebook (facebookcorewwwi.onion) χωρίς να ανησυχεί για το αν παρακολουθείται, αφού μέσω του Tor είναι εξαιρετικά δύσκολο να εντοπισθεί κάποιος.

3.4 Παραδείγματα παράνομης χρήσης του Deep Web

- Silk Road 1.0, 2.0, 3.0 και RAMP:

Το silk road [14] ιδρύθηκε το Φεβρουάριο του 2011 από τον Ross William Ulbricht και ήταν ουσιαστικά μια διαδικτυακή μαύρη αγορά. Η πρόσβαση στο silk road γινόταν μόνο μέσω του Tor αφού η σελίδα αυτή ήταν για ευνόητους λόγους τοποθετημένη στο Deep Web. Οι συναλλαγές γίνονταν με τη χρήση του εικονικού νομίσματος Bitcoin.

Το silk road ήταν ο παράδεισος των χρηστών και των διακινητών ναρκωτικών, αφού μπορούσες να βρεις οποιοδήποτε ναρκωτικό επιθυμούσες. Μέχρι τον Απρίλιο του 2013, όπου και συνελήφθη ο Ulbricht, το silk road απαριθμούσε 10.000 προϊόντα προς πώληση από τα οποία το 70% ήταν ναρκωτικά. Το υπόλοιπο 30% ήταν υλικό παιδικής και ενήλικης πορνογραφίας, συμβουλές για εξαπατήσεις, για παράδειγμα οδηγίες για το πώς να κλέψεις από ένα ATM, όπλα μαζικής καταστροφής, μέχρι και αγγελίες για πληρωμένους δολοφόνους. Για την ακρίβεια, ο ίδιος ο Ulbricht είχε αναρτήσει αγγελία όπου ζητούσε έναν εκτελεστή ο οποίος θα λάμβανε για πληρωμή το ποσό των 150.000 δολαρίων για να αφαιρέσει τη ζωή ενός καναδού χρήστη του Silk road με το όνομα χρήστη FriendlyChemist ο οποίος εκβίαζε τον Ulbricht, ο οποίος είχε το ψευδώνυμο Dread Pirate Roberts , ζητώντας του χρήματα για να μην αποκαλύψει τις ταυτότητες χιλιάδων χρηστών.

Εφόσον το Silk Road λειτουργούσε στο Deep Web, ήταν εξαιρετικά δύσκολο να εντοπιστεί και να συλληφθεί ο κάτοχός του. Όχι όμως και ακατόρθωτο. Ο Ulbricht, προσπαθώντας να προωθήσει το site του, ακολούθησε κάποιες γνωστές τακτικές για online marketing και εκεί έκανε το πρώτο του λάθος. Σε μία ανάρτησή του σε κάποιο site σχετικά με bitcoin, ζητούσε πληροφορίες και έδινε την αληθινή του διεύθυνση mail (). Έπειτα ήρθε και το δεύτερο λάθος, όπου στο γνωστό site Stack Overflow που ειδικεύεται σε θέματα προγραμματισμού, ο Ulbricht έθεσε ερώτημα σχετικά με τη δημιουργία κώδικα για site το οποίο είναι «κρυμμένο με Tor». Εκτός του ότι αρχικά χρησιμοποίησε το όνομά του στο Stack Overflow και όταν αντιλήφθηκε το λάθος του και το άλλαξε με το ψευδώνυμο Frosty ήταν πια αργά, ο Ulbricht αντέγραψε κώδικα τον οποίο βρήκε στο συγκεκριμένο site, στο silk road.

Μετά τη σύλληψη και φυλάκιση του Ulbricht, το silk road έκλεισε άλλα όχι οριστικά. Μετά από περίπου ένα μήνα, εμφανίστηκε η ιστοσελίδα Silk Road 2.0 η οποία ήταν υπό τη διαχείριση του δεύτερου administrator του πρώτου silk road. Το FBI χρησιμοποίησε DDoS επίθεση για να κλείσει το site και συνέλαβε τον διαχειριστή ο οποίος καταδικάστηκε σε 8 χρόνια φυλάκισης. Λίγες ώρες μετά το κλείσιμο του Silk road 2, εμφανίστηκε το Silk road 3, άλλη μια εναλλακτική λύση για τη Μαύρη Αγορά και ακόμα και αν αυτό κλείσει θα ακολουθήσουν και silk road 4,5, κ. ο. κ.

Υπάρχει όμως μια σελίδα που ειδικεύεται σε αγοραπωλησίες στη μαύρη αγορά η οποία έχει αντέξει στο χρόνο και παρόλες τις επιθέσεις δείχνει να αντιστέκεται στους

νόμους. Είναι το ρωσικό site RAMP(Russian Anonymous Marketplace)[15], το οποίο χρησιμοποιεί τη ρωσική γλώσσα, έχει πάνω από 14.000 μέλη, και βρίσκεται εν ενεργεία από το 2014.

Στο RAMP, η επικοινωνία για τις αγορές γίνεται ανάμεσα σε πωλητή και αγοραστή μέσω ενός κρυπτογραφημένου instant-messenger συστήματος γνωστό ως Off-the Record και οι πληρωμές γίνονται μέσω bitcoin και της ρωσικής υπηρεσίας πληρωμής QIWI. Για να γίνει πιο δύσκολος ο εντοπισμός τους, οι πωλητές αφήνουν το «δέμα» σε μια εγκαταλελειμμένη περιοχή από την οποία θα το παραλάβει αργότερα ο αγοραστής. Ο αγοραστής με τη σειρά του, δοκιμάζει το προϊόν και επιστρέφει στη σελίδα για να γράψει την κριτική του και να το προτείνει σε άλλους ενδιαφερόμενους. Επιπλέον, ο οποιοσδήποτε μπορεί να διαφημίσει το προϊόν του στη σελίδα αυτή εφόσον μπορεί με κάποιο ποσό να εξασφαλίσει χώρο στο πάνω μέρος της ιστοσελίδας.

Το RAMP, αν και λειτουργεί με την ίδια φιλοσοφία με το Silk Road, δεν επιτρέπει την παροχή των ίδιων αντικειμένων και υπηρεσιών. Πιο συγκεκριμένα, το RAMP απαγορεύει την πώληση όπλων, κλεμμένων πιστωτικών καρτών ακόμα και πορνογραφικό υλικό. Επίσης αν παρατηρηθεί δραστηριότητα που προωθεί τη βία και τον εθνικισμό, αυτομάτως ο χρήστης που είναι υπεύθυνος εκδιώκεται από τη σελίδα και δεν μπορεί να ξανά ανακτήσει πρόσβαση.

Το RAMP, σε αντίθεση με το Silk Road καταφέρνει να επιβιώνει και να παρακάμπτει τους νόμους επειδή είναι βασισμένο στην απλότητα. Χρησιμοποιεί μια πιο αποκεντρωμένη πολιτική, αφού όπως προαναφέρθηκε, η συζήτηση γίνεται κατευθείαν ανάμεσα στον πάροχο και τον ενδιαφερόμενο και τις περισσότερες φορές η συμφωνία ολοκληρώνεται εκτός της σελίδας. Επιπλέον, η σελίδα εδρεύει στη Ρωσία, όπου δυστυχώς πολλές φορές η δικαιοσύνη δεν ασχολείται με τις εγκληματικές ενέργειες στο χώρο του διαδικτύου. Η απλότητα, βοηθά ακόμα και στον τομέα του προγραμματισμού της σελίδας, διότι όσο λιγότερη πολυπλοκότητα, τόσο πιο δύσκολα θα βρουν οι αρχές κάποιο bug στον κώδικα για να επιτεθούν.

- <u>Δολοφονίες στο Dark Web:</u>

Η αναζήτηση πληρωμένων δολοφόνων είναι ένα θέμα που έχει αρχίσει να απασχολεί τις αρχές. Στο dark web έχουν κάνει την εμφάνισή τους πολλά site, στα οποία κάποιος μπορεί να βρει ένα δολοφόνο για να υλοποιήσει τα σχέδια του. Ονομαστικά μερικά sites είναι τα: Quick Killer, Contract killer, C'thulu, DeadPool, το silk road στο παρελθόν και το Assassination Market[16].

Συνήθως τα ονόματα στις λίστες των υποψήφιων θυμάτων είναι πολιτικά πρόσωπα, από τον επικεφαλής του NSA μέχρι τον πρόεδρο των Ηνωμένων Πολιτειών. Για να γίνει μια εκτέλεση, ένας χρήστης πρέπει να αναρτήσει το όνομα του θύματος στη σελίδα κι έπειτα γίνονται πλειοδοτήσεις ώστε να αυξηθεί το ποσό με σκοπό να γίνει θελκτικό στον δολοφόνο για να φέρει εις πέρας τη «δουλειά». Σε ένα άρθρο του περιοδικού Forbes, ένα πρόσωπο που συνεργάζεται με το Assassination Market έδωσε συνέντευξη, χρησιμοποιώντας ψευδώνυμο φυσικά και εξήγησε πώς ακριβώς γίνεται η συμφωνία ώστε να ανταμειφθεί ο εγκληματίας. Για να υπάρξει απόδειξη ότι η δολοφονία έχει επιτευχθεί, όλοι οι υποψήφιοι δολοφόνοι πρέπει να στείλουν στον administrator ένα αρχείο .txt πριν γίνει η δολοφονία, όπου θα καταγράφει την ημερομηνία την οποία έχουν διαλέξει για να γίνει η εκτέλεση κρυπτογραφημένη. Πριν τη δολοφονία, ο δολοφόνος πρέπει να κάνει δωρεά 1 bitcoin στον όνομα του θύματός του και αφού διαπράξει το έγκλημα να στείλει άλλο ένα .txt αρχείο όπου θα περιέχει τις πληροφορίες για την εκτέλεση που διαπράχθηκε. Ο administrator διασταυρώνει τις πληροφορίες και καταλήγει στο συμπέρασμα για το ποιος πρέπει να πάρει τα bitcoins.

- <u>Παιδική πορνογραφία στο Dark Web</u>

Ίσως το χειρότερο από όλα όσα μπορεί να βρει κάποιος στο Dark Web είναι sites που περιέχουν παιδική πορνογραφία. Μια τέτοια σελίδα, ονομαζόμενη Playpen κατάφερε να κλείσει το FBI το 2015 καθώς και να συλλάβει χιλιάδες χρήστες της σελίδας στους οποίους ασκήθηκαν ποινικές διώξεις. Το Playpen ήταν μάλιστα η μεγαλύτερη σελίδα παιδικής πορνογραφίας στο dark web που απαριθμούσε περίπου 215.000 μέλη, ενώ υπήρχαν συνολικά 117.000 δημοσιεύσεις οι οποίες περιείχαν εικόνες κακοποίησης παιδιών καθώς και συμβουλές προς θύτες παιδικής κακοποίησης για το πώς να αποφύγουν την παρακολούθηση από τις αρχές online.

Το FBI κατάφερε να βρει τον server ο οποίος διαχειριζόταν τη σελίδα, αποφάσισε να αναλάβει τη διαχείριση της σελίδας από τους δικούς του servers για 2 περίπου εβδομάδες ώστε να καταφέρει να μαζέψει στοιχεία για τους χρήστες της. Όταν πολλοί χρήστες άρχισαν να επισκέπτονται τη σελίδα, το FBI χρησιμοποίησε την τεχνική NIT(Network Investigative Technique) που ουσιαστικά είναι ένα εργαλείο για hacking και χρησιμοποίησε ένα μόνο ένταλμα για να ζητήσει πρόσβαση σε 1300 IP διευθύνσεις που θα τους οδηγούσαν στους χρήστες του site.

Ενώ το FBI είχε χρησιμοποιήσει αυτή την τεχνική ξανά στο παρελθόν, το δύσκολο σε αυτή την περίπτωση ήταν να παρακάμψει τους κανόνες του Tor, μέσω του οποίου κάποιος μπορούσε να έχει πρόσβαση στο Playpen. Όταν κάποιος επισκεπτόταν το site, ενώ οι κινήσεις του δεν καταγράφονταν, μια Flash εφαρμογή ενσωματωνόταν στον υπολογιστή του, η οποία κρυφά έστελνε δεδομένα για το χρήστη πίσω στο FBI χωρίς να περνάει καθόλου από το Tor. Το NIT, κατάφερε να ανακαλύψει την πραγματική IP διεύθυνση, τον τύπο του λειτουργικού συστήματος που χρησιμοποιούνταν, τη διεύθυνση MAC του υπολογιστή, το host name και το username καθώς και IP διευθύνσεις με τις οποίες ο χρήστης είχε ανταλλάξει υλικό.

Από αυτή την ενδελεχή έρευνα του FBI προέκυψαν περίπου 1500 υποθέσεις σε 8 πολιτείες των Η.Π.Α. που σχετίζονται με παιδική πορνογραφία. Το FBI δήλωσε ότι κάθε υπόθεση θα ερευνηθεί διεξοδικά και ήδη έχει αρχίσει η εκδίκαση των υποθέσεων[17].

- <u>Καρκινοπαθείς στρέφονται στο Dark Web για να βρουν τα φάρμακά τους</u>

Αμερικανοί πολίτες οι οποίοι δεν έχουν ασφάλεια ή αναζητούν φάρμακα τα οποία δεν έχουν εγκριθεί από την ομοσπονδία τροφίμων και φαρμάκων της Αμερικής (Food and Drug Administration -FDA), επιδιώκουν πρόσβαση στο Dark Web όπου τα φάρμακα για τη θεραπεία τους υπάρχουν σε μεγάλο απόθεμα και σε πολύ χαμηλές τιμές.

Πολλοί ασθενείς υποστηρίζουν ότι η φαρμακευτική αγορά στηρίζεται πάνω στους καρκινοπαθείς για να αυξήσει τα κέρδη της, θέτοντας τις τιμές των φαρμάκων για ασθένειες όπως ο καρκίνος σε εξωφρενικά υψηλές τιμές που καθιστούν αδύνατη την αγορά τους από το μέσο πολίτη. Συνεπώς, για τους περισσότερους ασθενείς, το να ψάξουν στο dark net να βρουν τα μέσα για τη θεραπεία τους είναι ζήτημα ζωής και θανάτου.

Από ιατρικής άποψης, τα πράγματα δεν είναι τόσο απλά. Οι ιατροί προειδοποιούν ότι τα φάρμακα που αγοράζονται στη μαύρη αγορά του διαδικτύου, μπορεί πολλές φορές να είναι πλαστά. Ειδικά αυτά που δεν έχουν λάβει έγκριση από το FDA, μπορεί να έχουν θανατηφόρες παρενέργειες[18].

4. ΛΥΣΕΙΣ ΓΙΑ ΤΟ ΠΡΟΒΛΗΜΑ ΤΗΣ ΜΑΖΙΚΗΣ ΠΑΡΑΚΟΛΟΥΘΗΣΗΣ ΣΕ ΕΥΡΩΠΑΙΚΟ ΕΠΙΠΕΔΟ

Το πρόβλημα παρακολούθησης των εθνικών δικτύων ειδικά από ξένες υπηρεσίες μπορεί να λυθεί με τους εξής τρόπους:

- **Συμφωνίες μεταξύ κρατών και κυρώσεις**: Από το 2011 η ΕΕ διαπραγματεύεται με την κυβέρνηση των ΗΠΑ για μια διεθνή συμφωνία ώστε να προστατεύονται τα δεδομένα που αφορούν νομικά ζητήματα μεταξύ των δυο.

Στην περίπτωση που οι πολιτικές συμφωνίες δεν είναι επιτυχής, τότε το κράτος θα πρέπει να βρει εναλλακτικούς τρόπους προστασίας των κρατικών μυστικών από τους εισβολείς.

Υπάρχουν 2 τρόποι προστασίας:

- **Μπλοκάρισμα φυσικής εισόδου(physical access) στο δίκτυο:** Σε αυτήν την περίπτωση, το κράτος θα πρέπει να διαχωρίσει το εθνικό του δίκτυο από τα υπόλοιπα, προστατεύοντας τις πύλες δεδομένων και το ποιος έχει πρόσβαση καθώς και να ασφαλίσει ότι τα καλώδια πρόσβασης δεν εκτείνονται εκτός της χώρας.
- **Μπλοκάρισμα λογικής εισόδου(logical access):** Η κρυπτογράφηση End-to-end είναι ο πιο αποτελεσματικός τρόπος για την προστασία των πληροφοριών από εξωτερικούς κινδύνους. Σε αυτού του είδους την κρυπτογράφηση, μόνο οι χρήστες του δικτύου μπορούν να έχουν πρόσβαση ενώ οι χρήστες που προσπαθούν να «εισβάλλουν» στο σύστημα απωθούνται από αυτό.

Σε αυτήν την ενότητα θα εξεταστούν όλες οι λύσεις που προτείνονται από το ευρωπαϊκό κοινοβούλιο για την προστασία των επικοινωνιών από εξωτερικές επιθέσεις και παρακολουθήσεις βραχυπρόθεσμα και μακροπρόθεσμα. Επίσης θα παρουσιαστούν τα μέτρα που θα πρέπει να ληφθούν για την επαρκή προστασία των δεδομένων σε υπηρεσίες cloud και στα μέσα κοινωνικής δικτύωσης καθώς και μέτρα προστασίας που μπορεί ο χρήστης να πάρει από μόνος του ώστε να εξασφαλίσει την ασφάλεια των δεδομένων του.

4.1 Βραχυπρόθεσμες λύσεις

1. Πρωτοβουλία της Ευρωπαϊκής Ένωσης για τη πιο διαλλακτική χρήση της κρυπτογραφίας: Η Ευρωπαϊκή Ένωση θα πρέπει να επενδύσει στην ύπαρξη διαφορετικών ειδών κρυπτογραφίας ανοιχτού κώδικα ώστε να χρησιμοποιούνται για τον έλεγχο και την επαλήθευση της ορθότητας της κρυπτογραφίας. Εφόσον όλες οι κρυπτογραφικές μέθοδοι θα είναι open source, οι χρήστες θα έχουν τη δυνατότητα να χρησιμοποιήσουν πιο δυνατά εργαλεία κρυπτογράφησης ώστε να προστατεύσουν τα δεδομένα τους από τυχόν παρακολουθήσεις.
2. Προώθηση των «ανοιχτών» πρωτοκόλλων, εφαρμογών και συστημάτων: Με τον όρο ανοιχτό πρωτόκολλο, νοείται ότι το πρωτόκολλο είναι διαθέσιμο στο κοινό για να το εξετάσει ενδελεχώς, να κρίνει αν ικανοποιεί τις ανάγκες του και να προτείνει βελτιώσεις. Η Ευρωπαϊκή Ένωση θα πρέπει να προωθήσει τη δημιουργία ανοιχτών πρωτοκόλλων και συστημάτων έτσι ώστε οι πολίτες να τα χρησιμοποιούν για τη διασφάλιση της ιδιωτικότητας των στοιχείων τους.

3. Ρύθμιση της τηλεπικοινωνιακής ασφάλειας και δημιουργία προτύπων κρυπτογράφησης: Η ΕΕ θα πρέπει να παροτρύνει πιο έντονα τους παρόχους τηλεπικοινωνιακών υπηρεσιών να εφαρμόσουν μηχανισμούς ασφάλειας με τη μορφή κρυπτογράφησης σε όλη την έκταση των δικτύων τους χωρίς να αφήσουν κενά τα οποία μπορούν να χρησιμοποιηθούν για παρακολούθηση.
4. Σωστή ενημέρωση των χρηστών για τη χρήση διαδικτυακών εφαρμογών: Η ΕΕ θα πρέπει να επενδύσει στην ενημέρωση των χρηστών του διαδικτύου σχετικά με τα διαδικτυακά ίχνη που αφήνουν κατά τη χρήση υπολογιστών είτε κινητών συσκευών και για το πώς μπορεί κάποιος να εκμεταλλευτεί αυτά τα στοιχεία για να βλάψει το χρήστη. Η ενημέρωση αυτή θα πρέπει να συμπεριλαμβάνει πληροφορίες για το πώς οι χρήστες μπορούν να ελαττώσουν το ψηφιακό τους αποτύπωμα ακολουθώντας συγκεκριμένους κανόνες συμπεριφοράς και συγκεκριμένα εργαλεία κρυπτογράφησης.
5. Αύξηση της χειραφέτησης των πολιτών επενδύοντας στην διαφάνεια των δεδομένων τους: Η ΕΕ θα πρέπει να επενδύσει και να προωθήσει τη διαφάνεια των δεδομένων των πολιτών έτσι ώστε αυτοί να αποφασίζουν για τη διαθεσιμότητα των δεδομένων τους. Έτσι, οι πολίτες θα έχουν τη δυνατότητα να ορίσουν οι ίδιοι σε ποιόν θα είναι διαθέσιμα τα στοιχεία τους καθώς και τι θα συμβαίνει με αυτά.
6. Επενδύσεις σε ολοκληρωμένες πλατφόρμες προστασίας και σε εφαρμογές προστασίας της ιδιωτικότητας των δεδομένων: Η ΕΕ πρέπει να κάνει επενδύσεις ώστε να υπάρχουν εφαρμογές για την προστασία των δεδομένων που ακόμα και ένας χρήστης με ελάχιστη εμπειρία θα μπορεί να χρησιμοποιήσει.
7. Δημιουργία κανονισμών που θα ορίζουν την μέγιστη προστασία δεδομένων σαν προκαθορισμένη επιλογή σε εφαρμογές: Η ΕΕ θα πρέπει να συγγράψει κανονισμούς που θα αναγκάζουν τους δημιουργούς εφαρμογών και τους παρόχους υπηρεσιών, ειδικά στο χώρο των νεφοϋπολογιστικών επιχειρήσεων, να εμπεριέχουν ως προκαθορισμένες επιλογές στις εφαρμογές τους ρυθμίσεις προστασίας και ιδιωτικότητας.

4.2 Μακροπρόθεσμες λύσεις για τη μείωση των μαζικών παρακολουθήσεων

Υπάρχουν 4 σενάρια για την προστασία ενάντια των μαζικών παρακολουθήσεων σε ευρωπαϊκό έδαφος. Αυτά τα σενάρια αναλύονται παρακάτω.

4.2.1 ΣΕΝΑΡΙΟ 1: Προώθηση

Σε αυτό το σενάριο, προτείνεται η προώθηση για την υιοθέτηση τεχνικών για την προστασία των δεδομένων από εισβολείς στα υπολογιστικά συστήματα.

- Προώθηση της από-άκρο-σε-άκρο κρυπτογράφησης(end-to-end encryption-E2E):

Η κρυπτογράφηση παίζει τον πρωταγωνιστικό ρόλο στην προστασία των δεδομένων των χρηστών. Η ελλιπής χρήση κρυπτογραφίας αποτελεί έναν από τους παράγοντες που υποβοηθούν τη μαζική παρακολούθηση των επικοινωνιών. Έτσι, η ΕΕ θα πρέπει:

- να παρέχει επαρκή πληροφόρηση των χρηστών για τη σημασία της E2E κρυπτογράφησης.

- να επιδιώξει την αύξηση του επιπέδου εκμάθησης των χρηστών, δημιουργώντας μια πλατφόρμα όπου οι χρήστες θα βρίσκουν ό,τι χρειάζονται για να μάθουν να χρησιμοποιούν τα εργαλεία κρυπτογράφησης.

- να προστάξει τη δημιουργία τεστ προστασίας των προϊόντων, ώστε να μπορεί ο χρήστης να επιλέγει σοφότερα ποιο πρόγραμμα θα χρησιμοποιήσει.

-να βοηθήσει ώστε η κρυπτογράφηση να γίνει μια διαδικασία πιο φιλική προς τον χρήστη. Αυτό μπορεί να γίνει με την προώθηση υπαρχόντων εργαλείων κρυπτογράφησης φιλικών προς το χρήστη για χρήση σε υπηρεσίες email και chat. Επιπλέον, η ΕΕ μπορεί να χρηματοδοτήσει προσπάθειες για τη δημιουργία κρυπτογραφικών λύσεων ανοιχτού κώδικα που η σχεδίαση τους επικεντρώνεται στην εύκολη χρήση από χρήστες χωρίς εμπειρία στον τομέα της κρυπτογραφίας.

- Προώθηση λογισμικού ανοιχτού κώδικα(OSS-Open Source Software):

Το λογισμικό ανοιχτού κώδικα αποτελεί ένα σημαντικό μέρος της στρατηγικής της ΕΕ για την αύξηση της ασφάλειας και την τεχνολογική της ανεξαρτησία. Έτσι, είναι απαραίτητη η χρηματοδότηση από την ΕΕ για υποστήριξη και συντήρηση σημαντικών OS λογισμικών. Αυτό θα επιτευχθεί με τη δημιουργία ενός ευρωπαϊκού προγράμματος χρηματοδότησης για OSS. Τέλος, είναι σημαντική η δημιουργία συστήματος ενός πιστοποίησης για open source λογισμικό έτσι ώστε να υπάρχει μια συγκεκριμένη κατηγορία λογισμικών τα οποία θα εγκρίνει η ΕΕ ότι είναι ασφαλή για χρήση.

- Προώθηση και τόνωση των ευρωπαϊκών τηλεπικοινωνιακών υπηρεσιών: Ειδικά των νεφοϋπολογιστικών υπηρεσιών, των μέσων κοινωνικής δικτύωσης και των μηχανών αναζήτησης. Θα πρέπει να γίνει επιβολή νομικών περιορισμών σχετικά με την εξαγωγή προσωπικών δεδομένων και επιβολή προστίμων σε περιπτώσεις παράβασης της νομοθεσίας στο χώρο της ΕΕ
- Προώθηση της ασφαλούς ανάπτυξης λογισμικού: Έργο της ΕΕ δε θα είναι μόνο η προώθηση των ήδη υπαρχουσών οδηγιών για την ασφάλεια των νέων λογισμικών, αλλά και για το σχεδιασμό, την ανάπτυξη και την διατήρηση των υπαρχόντων λογισμικών. Επιπλέον, μια επιλογή είναι η υιοθέτηση πολιτικής μιας πιστοποίησης του λογισμικού η οποία λόγω των σημερινών δεδομένων στη χρήση εφαρμογών κινητής τηλεφωνίας θα πρέπει να αρχίσει εστιάζοντας στις κινητές επικοινωνίες.

4.2.2 ΣΕΝΑΡΙΟ 2: Δημιουργία κλίματος εμπιστοσύνης

Η πολιτική του σεναρίου για τη δημιουργία κλίματος εμπιστοσύνης σε ευρωπαϊκό έδαφος, είναι η δημιουργία κατευθυντήριων γραμμών προστασίας (security baselines), έτσι ώστε οι χρήστες να νιώθουν ασφάλεια για την ακεραιότητα και την μυστικότητα των δεδομένων τους κατά τη χρήση λογισμικών. Επιπλέον, προβλέπεται η θέσπιση νόμων από το Ευρωπαϊκό Κοινοβούλιο για την έκθεση και διόρθωση τρωτών σημείων σε λογισμικά.

Η πολιτική δημιουργίας ευρωπαϊκών κατευθυντηρίων γραμμών ασφαλείας, με σκοπό τον προσδιορισμό βασικών θεμάτων ασφαλείας τα οποία δε μπορούν να λυθούν με τεχνικά μέσα έχει θετικές και αρνητικές εκβάσεις.

Θετικά αποτελέσματα της εφαρμογής των European Security Baselines:

1. Αύξηση του επιπέδου προστασίας στην Ευρωπαϊκή Ένωση.
2. Βελτίωση της συνεργασίας μεταξύ των κρατών μελών εφόσον θα υπάρχει πλήρης κατανόηση των απαιτήσεων ασφαλείας.

3. Καλύτερη προστασία σε μέχρι πρότινος αδύναμους συνδέσμους της ΕΕ.
4. Καλύτερος έλεγχος της ασφάλειας.

Αρνητικά αποτελέσματα της εφαρμογής των European Security Baselines:

- Με την αύξηση της προστασίας θα επέλθει και αύξηση των επιθέσεων στο δίκτυο, του cybercrime και γενικότερα οι εισβολείς θα δημιουργήσουν νέους τύπους επιθέσεων ώστε να καταφέρουν να διαπεράσουν το τοίχος ασφάλειας που δημιουργήθηκε βασιζόμενο στις γραμμές προστασίας της ΕΕ.
- Για την εφαρμογή των baselines είναι αναγκαία η δημιουργία ICT hardware και software τα οποία δεν υπάρχουν στις παρούσες συνθήκες κάτι που θα οδηγήσει στη μεγάλη αύξηση του κόστους εφαρμογής των γραμμών ασφαλείας.
- Δημιουργία πολιτικών συζητήσεων και διαμαχών ανάμεσα στα κράτη μέλη σχετικά με τα μέτρα που πρέπει να ληφθούν από κάθε κράτος για την προστασία του ευρωπαϊκού δικτύου.

4.2.3 ΣΕΝΑΡΙΟ 3: Διάσπαση (Διασπαστική Καινοτομία)

Υπάρχουν δύο μακροπρόθεσμες λύσεις οι οποίες θα συμβάλλουν στη μετρίαση των κατασκευαστικών κινδύνων που προκύπτουν από την εξάρτηση της Ευρώπης από την Αμερική και την Ασία σε θέματα υλικού και λογισμικού επικοινωνιών. Η πρώτη προτεινόμενη λύση αφορά τον καλύτερο προσδιορισμό του εξοπλισμού και του λογισμικού που προμηθεύεται η Ευρώπη από άλλες χώρες και η αξιολόγηση έτσι ώστε να εξακριβωθεί ότι ο εξοπλισμός δεν έχει αλλοιωθεί για σκοπούς παρακολούθησης. Η δεύτερη πρόταση αφορά τη δημιουργία ενός ευρωπαϊκού υποδικτύου το οποίο θα έχει ως αντίκτυπο την αποκοπή της Ευρώπης από το παγκόσμιο δίκτυο και τους κινδύνους που ελλοχεύουν σε αυτό.

4.2.3.α. Ευρωπαϊκή πιστοποίηση εξοπλισμού και λογισμικού εισαγόμενου από χώρες εκτός ΕΕ

Τα πρότυπα κρυπτογραφίας , το λογισμικό και ο εξοπλισμός μπορούν με τροποποιήσεις να αποτελέσουν όργανα μαζικής παρακολούθησης. Στην παρούσα φάση, δεν υπάρχουν ευρωπαϊκά πρότυπα σχεδίασης ώστε να αποφευχθεί ο κίνδυνος παρακολούθησης. Η πρόταση του ευρωπαϊκού κοινοβουλίου, παρουσιάζει τα παρακάτω θέματα σχετικά με την ανάγκη δημιουργίας ενός προτύπου πιστοποίησης της κρυπτογραφίας και του εξοπλισμού ώστε να αναπτερωθεί το αίσθημα ασφάλειας στους πολίτες της ΕΕ.

- Η προτυποποίηση της κρυπτογραφίας είναι ένα γεγονός εφικτό και αναγκαίο να υλοποιηθεί:

  Επί του παρόντος, η πλειοψηφία των προτύπων κρυπτογράφησης που υφίστανται, έχουν συνταχθεί από το Εθνικό Ινστιτούτο Προτυποποίησης και Τεχνολογίας (NIST).Το NIST αποτελεί ομοσπονδιακή αρχή του αμερικάνικου υπουργείου Εμπορίου και προφανώς όλα τα πρότυπα που δημιουργεί αφορούν την αμερικάνικη αγορά και ανταγωνισμό. Τα πρότυπα προστασίας, δημιουργούνται με βάση την αμερικάνικη νομοθεσία και όχι την παγκόσμια. Τέλος, το NIST έχει παραδεχτεί δημόσια τη συνεργασία του με την NSA για τη δημιουργία προτύπων κρυπτογραφίας, γεγονός που μειώνει την αξιοπιστία τους, δεδομένου της ανάμειξης της NSA στο σκάνδαλο μαζικής παρακολούθησης που έφερε στην επιφάνεια ο Snowden.

Η Ευρωπαϊκή Ένωση προς το παρόν δεν διαθέτει αντίστοιχη υπηρεσία του NIST. Έτσι τα κράτη μέλη και οι οργανισμοί της ΕΕ βασίζονται στα πρότυπα του NIST, παρά το γεγονός ότι διαθέτουν τους καλύτερους ερευνητές και τα καλύτερα ερευνητικά κέντρα που εστιάζουν στην κρυπτογραφία.

Η ευρωπαϊκή προτυποποίηση της κρυπτογραφίας είναι ένα θέμα που περιέχει θετικά και αρνητικά μέρη. Παρόλα αυτά, είναι εφικτό να δημιουργηθεί και λόγω της κυριαρχίας των Αμερικάνων στον παρόν τομέα είναι αναγκαίο.

- <u>Ο έλεγχος του εξοπλισμού (hardware) είναι αποδοτική λύση, αλλά όχι εφικτή:</u>

Το να αποδειχθεί ότι ο εξοπλισμός διαθέτει μόνο τις σχεδιασμένες λειτουργίες και δεν περιέχει κακόβουλο υλικό είναι εξαιρετικά δύσκολο. Για να εκτιμηθεί ότι η ασφάλεια του υλικού είναι η μέγιστη δυνατή, θα πρέπει όλες οι λειτουργίες σχεδιασμού και κατασκευής καθώς και η επιμελητεία να είναι ασφαλείς. Ειδικά σε περιπτώσεις μαζικής παραγωγής, κάτι τέτοιο είναι ακατόρθωτο.

Επιπλέον, ακόμα και αν γίνει έλεγχος κατά την παραγωγή του υλικού, υπάρχει η περίπτωση μεταποίησης του εξοπλισμού και πρόσθεση κακόβουλου υλικού σε αυτό κατά τη διάρκεια της αποστολής του στο χρήστη. Επομένως, ο έλεγχος του εξοπλισμού είναι πολύ δύσκολο να υλοποιηθεί σωστά.

- <u>Ο έλεγχος του λογισμικού είναι ανέφικτος και μη αποδοτικός:</u>

Ο έλεγχος του λογισμικού είναι μια διαδικασία άσκοπη, καθώς το λογισμικό μεταφέρεται ανεξέλεγκτα σε όλη την υφήλιο μέσω του διαδικτύου και σαν αποτέλεσμα μπορεί να αλλοιωθεί από τον οποιοδήποτε ,οπουδήποτε.

Η λύση του ελέγχου του λογισμικού μπορεί να εφαρμοστεί μόνο σε περιπτώσεις ανοιχτού κώδικα, όπου ο κώδικας μπορεί να αξιολογηθεί και να αλλάξει σε ύποπτες για την ασφάλεια περιπτώσεις.

- <u>Απαιτήσεις για την υλοποίηση της προτυποποίησης την κρυπτογραφίας:</u>

Η διαδικασία της προτυποποίησης θα πρέπει να είναι συστηματική, ανοιχτή, διαφανής, να ακολουθεί τους κανονισμούς και τις διαδικασίες και τέλος αποκριτική σε διεθνής ανησυχίες.

Αναλυτικότερα, η προτυποποίηση πρέπει να είναι ανοιχτή με την έννοια ότι ο καθένας θα μπορεί να συμμετέχει στη διαδικασία. Βασικό μέρος της όλης ενέργειας θα πρέπει να είναι εμπειρογνώμονες του κλάδου της κρυπτογραφίας και ακαδημαϊκοί. Επιπλέον, η προτυποποίηση θα πρέπει να είναι μια διαδικασία με διαφάνεια, εννοώντας ότι οι κρυπτογραφικοί διαγωνισμοί είναι ανοιχτοί και τα κριτήρια αξιολόγησης και εκτίμησης του αποτελέσματος είναι ξεκάθαρα. Όταν ένα πρότυπο τίθεται στη διάθεση του κόσμου για την αξιολόγησή του, θα πρέπει πάντα να διατίθενται οι αποδείξεις για την ασφάλεια του. Η διαδικασία της προτυποποίησης της κρυπτογραφίας θα πρέπει να είναι αποκριτική ως προς τις διεθνείς ανησυχίες αφού αυτά τα πρότυπα ουσιαστικά θα χτίσουν το τείχος ασφάλειας στα δικτυακά περιβάλλοντα. Τέλος, η προτυποποίηση θα πρέπει να είναι από μόνη της μια ασφαλής διαδικασία η οποία δε θα μπορεί να γίνει υποχείριο κακόβουλων πράξεων από εξωτερικούς παράγοντες.

- <u>Συνεργασία των μελών της ΕΕ:</u>

Για να στηθεί μια συστηματική, διαφανής, ανοιχτή και τεχνικά καίρια διαδικασία, η ΕΕ και τα κράτη μέλη της θα πρέπει να επενδύσουν στη δημιουργία μιας Ευρωπαϊκής ομάδας προτυποποίησης με επαρκείς γνώσεις και ικανότητες

καθώς και με εξαιρετικές διασυνδέσεις στον ακαδημαϊκό κόσμο και τη βιομηχανία.

Ο ρόλος της προστασίας μέσω των οργάνων επιβολής των νόμων είναι επίσης ένα σημαντικό ζήτημα για τη διαδικασία ορισμού των προτύπων. Η κρυπτογραφία, δεν είναι απλά ένα μέσο αντιμετώπισης του εγκλήματος και της τρομοκρατίας. Αποτελεί την καλύτερη αμυντική τεχνική απέναντι σε περιπτώσεις κυβερνοεγκλήματος και κατασκοπείας πράγμα που στρέφει το ενδιαφέρον των αρχών στην προτυποποίηση.

- Επιλογή πολιτικής της ΕΕ:

  Η κύρια πολιτική που πρέπει να ακολουθήσει η ΕΕ σχετικά με το σχεδιασμό τη κρυπτογράφησης είναι η σύσταση ενός Σώματος Ευρωπαϊκής Προτυποποίησης ή μιας αρχής πιστοποίησης της προτυποποίησης. Η αρχή αυτή ιδανικά, θα συνεργαζόταν με το NIST και με αντίστοιχες υπηρεσίες άλλων κρατών ώστε να θέσουν τους κανόνες και τις αρχές δημιουργίας των προτύπων χωρίς να υπάρξει διατάραξη της ισορροπίας των διεθνών σχέσεων.

4.2.3.β. Ευρωπαϊκό υποδίκτυο

Η σύσταση ενός ευρωπαϊκού υποδικτύου που θα συνεπάγεται την αποκοπή της Ευρώπης από το παγκόσμιο δίκτυο και τους κινδύνους που αυτό κρύβει είναι η δεύτερη πρόταση της ΕΕ για να εξασφαλίσει την προστασία των δικτύων της από επιθέσεις.

Ένα υποδίκτυο, είναι η συγκέντρωση πολλών συνδεδεμένων συσκευών οι οποίες κρατούν ένα σημαντικό μέρος της κίνησης των δεδομένων στο τοπικό δίκτυο. Ένα υποδίκτυο μπορεί να ανταλλάσσει δεδομένα με κάποιον άλλο χειριστή, ο οποίος μπορεί να επικοινωνήσει με άλλους πιο απομακρυσμένους χειριστές. Οι σχεδιαστές δικτύων χρησιμοποιούν τα υποδίκτυα ώστε να έχουν μεγαλύτερη ευκολία στη διαχείριση του δικτύου. Όταν τα υποδίκτυα χρησιμοποιούνται σωστά τότε η απόδοση και η ασφάλεια των δικτύων βελτιώνονται.

Το ευρωπαϊκό υποδίκτυο θα χρησιμοποιεί το πρωτόκολλο BGP (Border Gateway Protocol). Το πρωτόκολλο αυτό χρησιμοποιείται για τη σύνδεση μεταξύ των υποδικτύων και μάλιστα, η ασφάλεια των διασυνδέσεων εξαρτάται από την ασφάλεια του BGP. Το BGP όμως, λόγω του ότι δημιουργήθηκε στις απαρχές του ίντερνετ, τότε που δεν υπήρχε σαν ιδέα η έννοια του κυβερνοεγκλήματος, χωλαίνει σε πολλά σημεία γι' αυτό και όλα τα σφάλματα που σχετίζονται με διασυνδέσεις, οφείλονται στις αποτυχίες του BGP.

Η δημιουργία ενός ευρωπαϊκού υποδικτύου, το οποίο θα είναι φυσικά αποκομμένο από τα υπόλοιπα δίκτυα είναι μια περίπλοκη διαδικασία και είναι μια μέθοδος προστασίας από επιθέσεις που έχει πολλά μειονεκτήματα. Οι συνδέσεις από και προς την ΕΕ θα πρέπει να προστατεύονται, αναλύοντας διεξοδικά το περιεχόμενο όλων των δεδομένων που δέχονται και λαμβάνοντας τα απαραίτητα μέτρα. Επίσης, πρέπει είναι αναγκαία η εύρεση ενός τρόπου για την ανίχνευση παράνομων εξωτερικών συνδέσεων και τέλος να υπάρξει μια διαδικασία αναγνώρισης Ευρωπαϊκής ταυτότητας ώστε να αποτρέπεται η είσοδος πολιτών εκτός της Ευρωπαϊκής Ένωσης.

Τα μειονεκτήματα της σύστασης ενός υποδικτύου που εκτείνεται αποκλειστικά σε ευρωπαϊκό έδαφος είναι τα εξής:

- Η μεγάλη προσπάθεια που χρειάζεται για την υλοποίηση του και οι διαφορετικές οπτικές των κρατών- μελών σχετικά με τις ψηφιακές ταυτότητες που θα πρέπει να χρησιμοποιούν οι πολίτες.

- Υπάρχει ο κίνδυνος να αναπτυχθεί το παράνομο εμπόριο των ψηφιακών ταυτοτήτων σε κατοίκους που δεν ανήκουν στα κράτη μέλη της ΕΕ από κατοίκους της ΕΕ.
- Οι κάτοικοι της ΕΕ δε θα μπορούν αποθηκεύουν δεδομένα σε παρόχους υπηρεσιών cloud των ΗΠΑ, ακόμα και αν τα κέντρα δεδομένα τους είναι σε ευρωπαϊκό έδαφος, πράγμα που θα αυξήσει την αρνητική δημοσιότητα και τα αρνητικά σχόλια.
- Η μέθοδος αυτή θα επιφέρει πολλές οικονομικές διαμάχες όπως διεκδικήσεις για χαμένες επενδύσεις σε εγκαταστάσεις στην Ευρώπη.
- Θα πρέπει το φυσικό δίκτυο, δηλαδή τα καλώδια και οι υποδομές να είναι σε συνεχή επιτήρηση ώστε να αποτραπεί η έκθεση τους σε κίνδυνο τοποθέτησης εξοπλισμού υποκλοπών.

4.3. Λύσεις για την προστασία των δεδομένων που αποθηκεύονται σε υπηρεσίες cloud και σε υπηρεσίες κοινωνικής δικτύωσης σε ευρωπαϊκό έδαφος.

Η κεντρική ιδέα αυτής της πρότασης είναι η ανάπτυξη μηχανών αναζήτησης και κοινωνικών δικτύων που θα εδρεύουν στην Ευρώπη με σκοπό τα δεδομένα να μπορούν να αποθηκεύονται και να χρησιμοποιούνται σύμφωνα με την ευρωπαϊκή νομοθεσία.

Θετικά στοιχεία της πρότασης αυτής:

- Κανόνας δικαίου: Οι πολίτες της ΕΕ θεωρούνται ο τελευταίος τροχός της αμάξης σε ότι αφορά τον νόμο των US. Έτσι, αν οι υπηρεσίες εστιάζουν την προσοχή τους στους κατοίκους της ΕΕ και τα δεδομένα τους, τότε η επιβολή των νόμων της ΕΕ θα είναι πιο εύκολη.
- Ανεξαρτησία: Η τεχνολογία μεταβάλλεται διαρκώς κι έτσι ένας χρήστης ο οποίος εγγράφεται σε μια υπηρεσία, αύριο μπορεί να βρίσκεται στην ίδια υπηρεσία η οποία όμως ανήκει σε άλλη εταιρεία. Η ΕΕ εγγυάται ότι στις υπηρεσίες εντός του ευρωπαϊκού δικτύου κάτι τέτοιο δε θα γίνεται.
- Ευθύνες: Εδράζοντας τους χρήστες και τα δεδομένα τους σε ευρωπαϊκό έδαφος, δεν υπάρχει ο κίνδυνος αλλοίωσης της ιδιοκτησίας και των δεδομένων αφού δημιουργώντας μηχανές αναζήτησης και κοινωνικά δίκτυα που θα έχουν ως έδρα ευρωπαϊκές χώρες, αυτό σημαίνει ότι όλες αυτές οι υπηρεσίες θα ακολουθούν τη νομοθεσία της ΕΕ.

Αρνητικά:

- Ανεπάρκεια αγοράς: Οι ξένοι πάροχοι υπηρεσιών δε θα μπορούν να λειτουργήσουν στην ΕΕ ή να αλλάξουν τις υπηρεσίες τους για τους ευρωπαίους χρήστες , κάτι που θα δημιουργήσει εμπόδια στην αγορά και στην καινοτομία.
- Έλλειψη ζήτησης: Εφόσον υπάρχουν ήδη υπηρεσίες cloud και social media τα οποία είναι σε μεγάλη ζήτηση αφού προσφέρουν τις καλύτερες υπηρεσίες, δε θα υπάρξει μεγάλη ζήτηση για τις ίδιες υπηρεσίες της Ευρώπης.
- Προβλήματα με χρήση εκτός ΕΕ: Προβλήματα διαλειτουργικότητας μεταξύ συσκευών αλλά και χρηστών που είναι στο εξωτερικό.
- Αλληλεξάρτηση hardware και software από χώρες εκτός της ΕΕ αφού πολλά από τα μέσα αλλά και εργαζόμενοι προέρχονται από άλλες χώρες.

- Βαλκανιοποίηση: Το να περιορίζεται το ίντερνετ μόνο στην ΕΕ είναι ενάντια στην κύρια ιδέα πάνω στην οποία δημιουργήθηκε το ίντερνετ.
- Αλλαγή Βάσης: Πολλές εταιρείες και πολλοί χρήστες έχουν αποθηκευμένα τα δεδομένα τους σε υπηρεσίες cloud με έδρα τις Η.Π.Α και θα χρειαστεί μεγάλη προσπάθεια να μεταφέρουν όλα τα δεδομένα τους στην αντίστοιχη υπηρεσία της ΕΕ.
- Μικρή επίδραση στις επιθέσεις: Στη Google και τη Yahoo, έρευνες δείχνουν ότι οι προστασία ασφαλείας των Η.Π.Α. ερεύνησαν τις συνδέσεις για να βρουν πληροφορίες χρηστών που θεωρούσαν εχθρικούς. Στο ευρωπαϊκό δίκτυο δε μπορεί να εγγυηθεί κάποιος ότι δε θα υπάρξει το ίδιο φαινόμενο ειδικά αν οι ευρωπαϊκές υπηρεσίες συνεργάζονται με αυτές των ηνωμένων πολιτειών.

4.4 Τεχνικές προστασίας που μπορούν να χρησιμοποιηθούν από κάθε χρήστη για την ασφάλεια των δεδομένων του

Υπάρχουν πολλές τεχνικές τις οποίες οι πολίτες μπορούν να χρησιμοποιήσουν για να προστατεύσουν την ιδιωτικότητά τους όταν είναι συνδεδεμένοι στο διαδίκτυο. Αυτές οι τεχνικές βασίζονται στον τύπο της επικοινωνίας, στη συσκευή και στην πλατφόρμα που χρησιμοποιείται για επικοινωνία καθώς και τον χρόνο ζωής των δεδομένων που θα τεθούν υπό την προστασία των τεχνικών αυτών.

Ένας από τους πρώτους και πιο προφανείς τρόπους για την προστασία των χρηστών είναι ο περιορισμός της χρήσης των Cookies στο πρόγραμμα περιήγησης διαδικτύου που χρησιμοποιούν. Βέβαια, ο περιορισμός αυτός θα επηρεάσει την ποιότητα εμπειρίας του χρήστη αφού οι προτιμήσεις για συγκεκριμένες ιστοσελίδες και υπηρεσίες δε θα αποθηκεύονται πια χωρίς τα Cookies. Επιπλέον, με τον περιορισμό των Cookies ο χρήστης θα είναι ασφαλής μόνο στο τοπικό του δίκτυο, διότι για παράδειγμα, μια επισκεπτόμενη ιστοσελίδα εκτός του τοπικού δικτύου του χρήστη για να αναγνωριστεί πρέπει να ταιριάξει την IP διεύθυνση του χρήστη με μια διεύθυνση στον διακομιστή του τελικού σημείου.

Άλλες τεχνικές βασίζονται στο να κρύβεται η IP διεύθυνση του χρήστη όταν χρησιμοποιεί το διαδίκτυο και την εφαρμογή κρυπτογραφίας από-άκρο-σε-άκρο.

Οι πιο γνωστές τεχνικές προστασίας είναι:

1.Κρυπτογράφηση των αποθηκευμένων δεδομένων

- Κρυπτογράφηση του σκληρού δίσκου σε υπολογιστές: Η τεχνική αυτή συνίσταται την κρυπτογράφηση ολόκληρων μερών ενός σκληρού δίσκου ή στην κρυπτογράφηση μεμονωμένων αρχείων που είναι αποθηκευμένα σε ένα μέρος του σκληρού δίσκου. Παραδείγματα εργαλείων που χρησιμοποιούν αυτήν την τεχνική είναι το DiskCryptor, το TrueCrypt, το FileVault, το BitLocker, κα.
- Κρυπτογράφηση του σκληρού δίσκου ενός smartphone: Το λειτουργικό σύστημα Android της Google επιτρέπει στους χρήστες των smartphone να κρυπτογραφήσουν τον σκληρό δίσκο της συσκευής τους ενώ η Apple δεν επιτρέπει στους χρήστες τη χρήση κρυπτογραφικών εργαλείων. Παρόλα αυτά το λειτουργικό σύστημα OS κρυπτογραφεί τους κωδικούς των χρηστών και κάποια άλλα αρχεία αν χρησιμοποιηθεί κωδικός πρόσβασης στην συσκευή.
- Κρυπτογράφηση των δεδομένων στο υπολογιστικό νέφος: Οι τεχνολογίες αυτές επιτρέπουν στα δεδομένα να αποθηκευτούν κρυπτογραφημένα στο cloud, χρησιμοποιώντας ένα κλειδί κρυπτογράφησης το οποίο ανήκει στον χρήστη που ανήκουν τα δεδομένα και συνήθως το κλειδί αυτό είναι αποθηκευμένο στο

σκληρό δίσκο της συσκευής που συνδέεται στο cloud. Όλα τα αρχεία κρυπτογραφούνται με ασφάλεια στη συσκευή του χρήστη πριν μεταφερθούν στο cloud. Παραδείγματα τέτοιων τεχνολογιών είναι τα DropBox, Google Drive, SpiderOak, Wuala, BoxCryptor, κα.

2. Κρυπτογράφηση των δεδομένων που μεταφέρονται

- HTTP Everywhere: Το λογισμικό αυτό είναι το αποτέλεσμα της συνεργασίας μεταξύ των The Tor Project και του EFF(Electronic Frontier Foundation). Το λογισμικό αυτό, είναι μια επέκταση που μπορεί να προστεθεί στα Mozilla Firefox, Google Chrome και Opera η οποία κρυπτογραφεί τις επικοινωνίες με πολλές σημαντικές ιστοσελίδες, επιτρέποντας έτσι την ανώνυμη πλοήγηση του χρήστη.

3. Προστασία για υπηρεσίες ηλεκτρονικού ταχυδρομείου: Ενδεικτικά, εργαλεία που βοηθούν στην κρυπτογράφηση της ηλεκτρονικής αλληλογραφίας είναι:

- το πρωτόκολλο Prism-proof email(PPE) το οποίο επιτρέπει κρυπτογραφημένες συζητήσεις μέσω emails χρησιμοποιώντας κρυπτογράφηση δημοσίου κλειδιού.
- το πρωτόκολλο Bitmessage το οποίο εστιάζει σε peer-to-peer αποκεντρωμένες επικοινωνίες.
- η υπηρεσία Sendinc η οποία παρέχεται δωρεάν μέσω διαδικτύου και προσφέρει κρυπτογράφηση από-άκρο-σε-άκρο.
- η επέκταση Enigmail για Mozilla Thunderbird η οποία δίνει τη δυνατότητα συγγραφής και ανταλλαγής μηνυμάτων κρυπτογραφημένων με το πρότυπο OpenPGP και
- η επέκταση για Google Chrome kai Firefox, Mainvelope η οποία λειτουργεί με παρόμοιο τρόπο όπως η Enigmail.

4. Προστασία για επικοινωνίες φωνής και video: Εφαρμογές που προσφέρουν end-to-end κρυπτογράφηση στις επικοινωνίες για φωνή και βίντεο είναι οι: Cellcrypt, Celltrust, OSTN, Omnisec, SeeCrypt, κα.

5. Εργαλεία για την προστασία των δεδομένων κατά τη χρήση μηχανών αναζήτησης:

- DuckDuckGo: Δημοφιλής μηχανή αναζήτησης η οποία δε συλλέγει προσωπικά στοιχεία των χρηστών της και συνεπώς όλοι οι χρήστε λαμβάνουν τα ίδια αποτελέσματα κατά την αναζήτηση ενός όρου.
- Ixquick: Μηχανή αναζήτησης η οποία κρυπτογραφεί όλες τις αναζητήσεις χωρίς όμως να κάνει κρυπτογράφηση των δεδομένων των χρηστών της.
- Startpage: Ιστοσελίδα αναζητήσεων η οποία παρέχεται από την Ixquick και παρέχει έναν συνδυασμό των αποτελεσμάτων της αναζήτησης Google με την πολιτική προστασίας της ιδιωτικότητας της Ixquick.
- Ask: Η μηχανή αναζήτησης Ask επιτρέπει στο χρήστη να επεξεργαστεί τις ρυθμίσεις αναζήτησης. Επιπλέον, μετά από κάθε αναζήτηση διαγράφονται όλα τα Cookies.

5. ΙΣΧΥΟΥΣΕΣ ΝΟΜΟΘΕΣΙΕΣ ΓΙΑ ΤΗΝ ΠΡΟΣΤΑΣΙΑ ΤΩΝ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΤΩΝ ΧΡΗΣΤΩΝ ΕΦΑΡΜΟΓΩΝ ΤΟΥ ΔΙΑΔΙΚΤΥΟΥ

5.1 Νομοθεσία στην Ευρωπαϊκή Ένωση

Η Ευρωπαϊκή Ένωση από της απαρχές της σύστασής της είχε σαν κύριο μέλημα την προστασία των προσωπικών δεδομένων και το σεβασμό της ιδιωτικής ζωής των πολιτών της. Το ευρωπαϊκό κοινοβούλιο, ανέκαθεν αναγνώριζε την ανάγκη για μια ισορροπημένη προσέγγιση ανάμεσα στην ενίσχυση της ασφάλειας και τη διαφύλαξη των ανθρώπινων δικαιωμάτων συμπεριλαμβανομένης της ιδιωτικής ζωής και της προστασίας των προσωπικών δεδομένων ειδικά στον τεχνολογικό χώρο. Με την αύξηση της δημοφιλίας και της χρηστικότητας του διαδικτύου, επήλθαν αλλαγές και στη σχετική νομοθεσία που ψηφίζεται από το ευρωπαϊκό κοινοβούλιο [19]. Την παρούσα χρονική στιγμή ισχύουν οι νομοθεσίες που παραθέτονται περιγραφικά παρακάτω:

- Συνθήκη της Λισαβόνας: Η συνθήκη της Λισσαβόνας ψηφίστηκε το 2007 και είναι μια διεθνής συνθήκη που τροποποιεί τις ιδρυτικές συνθήκες της Ευρωπαϊκής Ένωσης. Στον τομέα της προστασίας των προσωπικών δεδομένων, η συνθήκη παρέχει πιο στέρεα βάση για την ανάπτυξη ενός σαφέστερου και πιο αποδοτικού νομοθετικού πλαισίου περί της προστασίας των προσωπικών δεδομένων και καθιστά το ευρωπαϊκό κοινοβούλιο ως συν νομοθέτη στον οποίοι προσδίδονται νέες εξουσίες. Πιο συγκεκριμένα, το άρθρο 16 της συνθήκης για τη λειτουργία της Ευρωπαϊκής Ένωσης, το οποίο ήταν και ένας από τους πυλώνες της σύστασης της συνθήκης της Λισαβόνας, προβλέπει ότι το Κοινοβούλιο και το Συμβούλιο έχουν το δικαίωμα θέσπισης κανόνων σχετικά με την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από τα θεσμικά και λοιπά όργανα και τους οργανισμούς της Ένωσης, καθώς και από τα κράτη μέλη κατά την άσκηση δραστηριοτήτων που εμπίπτουν στο πεδίο εφαρμογής του δικαίου της Ένωσης.

  -Άρθρο 16 (πρώην άρθρο 286 της ΣΕΚ)

  1. Κάθε πρόσωπο έχει δικαίωμα προστασίας των δεδομένων προσωπικού χαρακτήρα.

  2. Το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο, αποφασίζοντας σύμφωνα με τη συνήθη νομοθετική διαδικασία, θεσπίζουν τους κανόνες σχετικά με την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από τα θεσμικά και λοιπά όργανα και τους οργανισμούς της Ένωσης, καθώς και από τα κράτη μέλη κατά την άσκηση δραστηριοτήτων που εμπίπτουν στο πεδίο εφαρμογής του δικαίου της Ένωσης, και σχετικά με την ελεύθερη κυκλοφορία των δεδομένων αυτών. Η τήρηση των κανόνων αυτών υπόκειται στον έλεγχο ανεξάρτητων αρχών.

  Οι κανόνες που θεσπίζονται βάσει του παρόντος άρθρου δεν θίγουν τους ειδικούς κανόνες που προβλέπονται στο άρθρο 39 της Συνθήκης για την Ευρωπαϊκή Ένωση.

- Χάρτης των θεμελιωδών δικαιωμάτων της Ευρωπαϊκής Ένωσης:

  Τα άρθρα 7 και 8 του Χάρτη των Θεμελιωδών δικαιωμάτων της Ευρωπαϊκής Ένωσης, αναγνωρίζουν ως θεμελιώδη δικαιώματα το σεβασμό της ιδιωτικής ζωής και την προστασία των δεδομένων προσωπικού χαρακτήρα. Μάλιστα τονίζεται η στενή σύνδεση των δύο δικαιωμάτων αλλά και το γεγονός ότι είναι δύο ξεχωριστές έννοιες. Ο Χάρτης των Θεμελιωδών Δικαιωμάτων της Ε.Ε.,

είναι ενσωματωμένος στη Συνθήκη της Λισαβόνας η οποία αναλύθηκε εκτενώς προηγουμένως.

- ΟΔΗΓΙΑ 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του συμβουλίου της 24ης Οκτωβρίου 1995 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών:

  Η οδηγία της 24ης Οκτωβρίου του 1995 αποτελεί το βασικότερο νομοθέτημα που αφορά την προστασία των δεδομένων στην Ευρωπαϊκή Ένωση. Στην οδηγία αυτή:

  1. Καταγράφονται γενικοί κανόνες που ορίζουν τη νομιμότητα της επεξεργασίας δεδομένων προσωπικού χαρακτήρα.
  2. Καθορίζονται τα δικαιώματα των προσώπων των οποίων τα δεδομένα θέτονται προς επεξεργασία
  3. Ορίζεται η θέσπιση εθνικών ανεξάρτητων εποπτικών αρχών για την προστασία των δεδομένων εντός του κάθε κράτους μέλους.
  4. Ορίζεται ότι η επεξεργασία δεδομένων προσωπικού χαρακτήρα επιτρέπεται μόνο με την ρητή συγκατάθεση του ατόμου του οποίου τα δεδομένα αναφέρονται καθώς και με την πλήρη ενημέρωσή του προτού ξεκινήσει η διαδικασία της επεξεργασίας.

  Η οδηγία 95/46/ΕΚ θα βρίσκεται σε ισχύ μέχρι το Μάιο του 2018.

- Οδηγία 2002/58/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του συμβουλίου της 12ης Ιουλίου 2002 σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών (οδηγία για την προστασία ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες):

  Στη σύσταση αυτής της οδηγίας οδήγησε η ανάγκη για τη θέσπιση ειδικών κανονισμών για την προστασία των προσωπικών δεδομένων οι οποίοι θα εστιάζουν στην αντιμετώπιση των κινδύνων τους οποίους διατρέχουν οι χρήστες των τηλεπικοινωνιακών υπηρεσιών, καθώς τα σύγχρονα δίκτυα τηλεπικοινωνιών παρέχουν πρόσθετες τεχνικές δυνατότητες υποκλοπής και παρακολούθησης των επικοινωνιών. Η οδηγία εστιάζει στην προστασία προσωπικών δεδομένων όσον αφορά τα δημόσια δίκτυα ηλεκτρονικών επικοινωνιών.

  Τα δεδομένα τα οποία χρίζουν της προστασίας τους από την οδηγία της ΕΕ χωρίζονται σε 3 κατηγορίες:

  1. Δεδομένα που αποτελούν το περιεχόμενο των μηνυμάτων συνδιάλεξης κατά τη διάρκεια μίας ηλεκτρονικής επικοινωνίας: Άκρως απόρρητα δεδομένα.
  2. Δεδομένα κίνησης: Είναι τα δεδομένα τα οποία είναι απαραίτητα για την έναρξη και λήξη μιας δικτυακής επικοινωνίας, λόγου χάρη οι διευθύνσεις IP του καλούντα και του καλούμενου, ο χρόνος έναρξης της επικοινωνίας καθώς και η διάρκειά της.
  3. Δεδομένα Θέσης: Υποκατηγορία των δεδομένων κίνησης και αφορούν τα δεδομένα που σχετίζονται με τη θέση του χρήστη τη στιγμή της επικοινωνίας, ιδιαίτερα σημαντικά δεδομένα για επικοινωνίες που διεξάγονται μέσω κινητών συσκευών.

Η οδηγία επιτρέπει στους παρόχους τηλεπικοινωνιακών υπηρεσιών να κάνουν χρήση των δεδομένων κίνησης μόνο για λόγους χρέωσης του συνδρομητή και για την παροχή υπηρεσιών από τεχνική άποψη.

Στην περίπτωση των χρηστών, οδηγία επιτρέπει πάντα με τη συγκατάθεση του χρήστη την κοινοποίηση των δεδομένων για σκοπούς παροχής υπηρεσιών προστιθέμενης αξίας, όπως εφαρμογές που παρέχουν χάρτες και οδηγίες για την διευκόλυνση της κίνησης του χρήστη μέσα στην πόλη, εφαρμογές για την ενημέρωση των χρηστών σχετικά με τα καιρικά φαινόμενα στην περιοχή τους, κ.ο.κ.

Το 2009 έγινε τροποποίηση της οδηγίας με σκοπό την εξειδίκευση των διατάξεών της για την προστασία των προσωπικών δεδομένων στον χώρο των τηλεπικοινωνιών. Οι διατάξεις που προστέθηκαν είναι οι εξής:

α. Απαγορεύεται η αποστολή διαφημιστικών μηνυμάτων κάθε είδους (SMS,MMS) σε χρήστες τηλεπικοινωνιακών υπηρεσιών, χωρίς τη συγκατάθεσή τους. Αν δεν υφίσταται η συγκατάθεση του χρήστη, η αποστολή διαφημιστικών μηνυμάτων καθίσταται νόμιμη μόνο στην περίπτωση όπου ο λήπτης είναι πρώην πελάτης της εταιρείας (αποστολέας του μηνύματος), έχει ιδιοχείρως παραχωρήσει την ηλεκτρονική του διεύθυνση και δεν αντιτάσσεται στην αποστολή των διαφημιστικών μηνυμάτων.

β. Κάθε κράτος μέλος της Ευρωπαϊκής Ένωσης οφείλει να παρέχει ένδικα μέσα σε περίπτωση της παραβίασης της απαγόρευσης σχετικά με τις μη ζητηθείσες επικοινωνίες.

γ. Η εγκατάσταση cookies κρίνεται νόμιμη εφόσον γίνεται με τη συγκατάθεση του χρήστη. Οι τρόποι παροχής και λήψης της συγκατάθεσης του χρήστη για την επαρκή προστασία κατά την λήψη των cookies, τίθενται στην αρμοδιότητα της εθνικής νομοθεσίας του εκάστοτε κράτους.

δ. Σε περίπτωση παραβίασης προσωπικών δεδομένων λόγω πρόσβασης χωρίς άδεια είτε απώλειας ή καταστροφής δεδομένων, ενημερώνεται άμεσα η αρμόδια αρχή ελέγχου καθώς και οι συνδρομητές σε περίπτωση που έχουν υποστεί ζημία λόγω της παραβίασης.

- <u>Απόφαση πλαίσιο 2008/977/ΔΕΥ του συμβουλίου της 27ης Νοεμβρίου 2008 για την προστασία των δεδομένων προσωπικού χαρακτήρα που τυγχάνουν επεξεργασίας στο πλαίσιο της αστυνομικής και δικαστικής συνεργασίας σε ποινικές υποθέσεις:</u>

  Η απόφαση πλαίσιο 2008/977/ΔΕΥ αφορά μόνο αστυνομικά και δικαστικά δεδομένα που ανταλλάσσονται μεταξύ κρατών μελών, αρχών και συνδεδεμένων συστημάτων της Ευρωπαϊκής Ένωσης και δεν καλύπτει τα εγχώρια δεδομένα.

- <u>Οδηγία 2013/40/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 12ης Αυγούστου 2013 για τις επιθέσεις κατά συστημάτων πληροφοριών και την αντικατάσταση της απόφασης-πλαισίου 2005/222/ΔΕΥ του Συμβουλίου:</u>

  Η οδηγία αυτή προβλέπει νέους κανονισμούς οι οποίοι εναρμονίζουν την ποινικοποίηση και τις ποινές για σειρά αδικημάτων που στρέφονται κατά των συστημάτων πληροφοριών.

- Ευρωπαίος Επόπτης Προστασίας Δεδομένων (ΕΕΠΔ):

  Ο ρόλος του ΕΠΕΔ είναι να διασφαλίζει ότι κατά την επεξεργασία προσωπικών δεδομένων, τα όργανα και οι οργανισμοί της ΕΕ σέβονται το δικαίωμα των πολιτών για προστασία της ιδιωτικής ζωής [20]. Ο ΕΠΕΔ είναι μια ανεξάρτητη εποπτική αρχή η οποία συστάθηκε το 2004 και αρμοδιότητες του είναι οι εξής:

  1. Η εποπτεία της επεξεργασίας των προσωπικών δεδομένων που πραγματοποιούνται από τις υπηρεσίες της ΕΕ, ώστε να διασφαλιστεί η συμμόρφωση με τους κανόνες περί προστασίας της ιδιωτικής ζωής.
  2. Ο ΕΠΕΔ συμβουλεύει τα όργανα και τους οργανισμούς της Ευρωπαϊκής Ένωσης για τα θέματα επεξεργασίας προσωπικών δεδομένων, των συναφών πολιτικών και της νομοθεσίας.
  3. Η διεκπεραίωση καταγγελιών και η διενέργεια ερευνών.
  4. Ο ΕΠΕΔ παρακολουθεί νέες τεχνολογίες που θα μπορούσαν να έχουν επιπτώσεις στην προστασία των δεδομένων.

- Μεταρρύθμιση της προστασίας των δεδομένων της Ευρωπαϊκής Ένωσης:

  Η μεταρρύθμιση αποσκοπεί στην προστασία δεδομένων προσωπικού χαρακτήρα σε ολόκληρη την ΕΕ, ενισχύοντας τον έλεγχο των χρηστών επί των δεδομένων που τους αφορούν και περικόπτοντας το κόστος για τις επιχειρήσεις. Η ανάγκη για τη δημιουργία της μεταρρύθμισης αυτής προήλθε από το γεγονός ότι η τεχνολογική πρόοδος και η το φαινόμενο της παγκοσμιοποίησης εξελίσσονται τόσο ραγδαία ώστε ο τρόπος συλλογής, πρόσβασης και χρήσης δεδομένων έχει αλλάξει κατά κόρον. Επίσης, σημαντικός παράγοντας για την έναρξη των συζητήσεων των κρατών περί μεταρρύθμισης της υπάρχουσας νομοθεσίας υπήρξε η ανάγκη ενός ενιαίου νόμου σε όλα τα κράτη μέλη, αφού μέχρι τώρα , κάθε κράτος μέλος εφάρμοζε τους κανόνες του 1995 με διαφορετικό τρόπο.

  Μετά από διαπραγματεύσεις τριών ετών, τον Απρίλιο του 2016 δημοσιεύθηκαν οι νέοι κανόνες προστασίας των δεδομένων οι οποίοι θα τεθούν σε εφαρμογή από το Μάιο του 2018:

  1. Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων).
  2. Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ.

5.2 Νομοθεσία στην Ελλάδα

Η Ελλάδα όσον αφορά την προστασία στο χώρο των τηλεπικοινωνιών, ως ενεργό μέλος της Ευρωπαϊκής Ένωσης, εφαρμόζει τους νόμους που έχουν ψηφιστεί στο ευρωπαϊκό κοινοβούλιο για τη διαφύλαξη των προσωπικών δεδομένων [21].

- Νόμος 2472/1997 για την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα με ενσωματωμένες τις τροποποιήσεις:

  Αντικείμενο του νόμου είναι η θέσπιση των προϋποθέσεων για την επεξεργασία δεδομένων προσωπικού χαρακτήρα προς προστασία των δικαιωμάτων και των θεμελιωδών ελευθεριών των φυσικών προσώπων και ιδίως της ιδιωτικής ζωής.

  Στο άρθρο 4 του νόμου ορίζονται οι τρόποι με τους οποίους μπορούν να τίθεται σε επεξεργασία τα δεδομένα εφόσον ακολουθείται πάντα η νόμιμη οδός. Τονίζεται ότι τα δεδομένα πρέπει:

  1. Να συλλέγονται κατά τρόπο θεμιτό και νόμιμο για καθορισμένους, σαφείς και νόμιμους σκοπούς και να υφίστανται θεμιτή και νόμιμη επεξεργασία ενόψει των σκοπών αυτών.
  2. Να είναι συναφή, πρόσφορα, και όχι περισσότερα από όσα κάθε φορά απαιτείται εν όψει των σκοπών της επεξεργασίας.
  3. Να είναι ακριβή και, εφόσον χρειάζεται, να υποβάλλονται σε ενημέρωση.
  4. Να διατηρούνται σε μορφή που να επιτρέπει τον προσδιορισμό της ταυτότητας των υποκειμένων τους μόνο κατά τη διάρκεια της περιόδου που απαιτείται, κατά την κρίση της Αρχής, για την πραγματοποίηση των σκοπών της συλλογής τους και της επεξεργασίας τους. Μετά την παρέλευση της περιόδου αυτής, η Αρχή μμπορεί, με αιτιολογημένη απόφασή της, να επιτρέπει τη διατήρηση δεδομένων προσωπικού χαρακτήρα για ιστορικούς επιστημονικούς ή στατιστικούς σκοπούς, εφ΄ όσον κρίνει ότι δεν θίγονται σε κάθε συγκεκριμένη περίπτωση τα δικαιώματα των υποκειμένων τους ή και τρίτων.

  Στο άρθρο 5 απαριθμούνται οι προϋποθέσεις επεξεργασίας των προσωπικών δεδομένων. Η επεξεργασία δεδομένων προσωπικού χαρακτήρα επιτρέπεται μόνο έπειτα από τη συγκατάθεση του υποκειμένου του οποίου τα δεδομένα θα επέλθουν σε επεξεργασία.

  Η επεξεργασία δεδομένων χωρίς τη συγκατάθεση του υποκειμένου γίνεται κάτω από συγκεκριμένες συνθήκες. Αυτές είναι όταν:

  1. Η επεξεργασία είναι αναγκαία για την εκτέλεση σύμβασης, στην οποία συμβαλλόμενο μέρος είναι υποκείμενο δεδομένων ή για τη λήψη μέτρων κατόπιν αιτήσεως του υποκειμένου κατά το προσυμβατικό στάδιο.
  2. Η επεξεργασία είναι αναγκαία για την εκπλήρωση υποχρεώσεως του υπεύθυνου επεξεργασίας, η οποία επιβάλλεται από το νόμο.
  3. Η επεξεργασία είναι αναγκαία για τη διαφύλαξη ζωτικού συμφέροντος του υποκειμένου, εάν αυτό τελεί σε φυσική ή νομική αδυναμία να δώσει τη συγκατάθεσή του.
  4. Η επεξεργασία είναι αναγκαία για την εκτέλεση έργου δημόσιου συμφέροντος ή έργου που εμπίπτει στην άσκηση δημόσιας εξουσίας και εκτελείται από δημόσια αρχή ή έχει ανατεθεί από αυτή είτε στον υπεύθυνο επεξεργασίας είτε σε τρίτο, στον οποίο γνωστοποιούνται τα δεδομένα.

5. Η επεξεργασία είναι απολύτως αναγκαία για την ικανοποίηση του έννομου συμφέροντος που επιδιώκει ο υπεύθυνος επεξεργασίας ή ο τρίτος ή οι τρίτοι στους οποίους ανακοινώνονται τα δεδομένα και υπό τον όρο ότι τούτο υπερέχει προφανώς των δικαιωμάτων και συμφερόντων των προσώπων στα οποία αναφέρονται τα δεδομένα και δεν θίγονται οι θεμελιώδεις ελευθερίες αυτών.

- Νόμος 3917/2011 για τη διατήρηση δεδομένων που παράγονται ή υποβάλλονται σε επεξεργασία σε συνάρτηση με την παροχή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημόσιων δικτύων επικοινωνιών, χρήση συστημάτων επιτήρησης με τη λήψη ή καταγραφή ήχου ή εικόνας σε δημόσιους χώρους:

Με το νόμο 3917/2011 ενσωματώθηκε στην έννομη τάξη της Ελλάδας η Οδηγία 2006/24/ΕΚ της Ε.Ε. με στόχο την αποτελεσματικότερη καταπολέμηση της τρομοκρατίας και του οργανωμένου εγκλήματος. Όπως αναφέρεται και στο 1ο άρθρο του εν λόγω νόμου:

«Οι πάροχοι διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημόσιου δικτύου επικοινωνιών υποχρεούνται να διατηρούν τα δεδομένα του άρθρου 5 που παράγονται ή υποβάλλονται σε επεξεργασία από αυτούς, προκειμένου τα δεδομένα αυτά να καθίστανται διαθέσιμα στις αρμόδιες αρχές για τη διακρίβωση ιδιαίτερα σοβαρών εγκλημάτων, όπως αυτά ορίζονται στο άρθρο 4 του ν. 2225/1994»

Οι κατηγορίες δεδομένων τα οποία διατηρούνται είναι – όπως θεσπίζονται από το νόμο- οι εξής:

1. Δεδομένα αναγκαία για την ανίχνευση και τον προσδιορισμό της πηγής της επικοινωνίας (λ.χ. ο τηλεφωνικός αριθμός του καλούντος, η IP διεύθυνση του χρήστη, κοκ)
2. Δεδομένα αναγκαία για τον προσδιορισμό του προορισμού της επικοινωνίας(λ.χ. ο καλούμενος αριθμός τηλεφώνου, το ονοματεπώνυμο και η IP διεύθυνση του χρήστη, κτλ.)
3. Δεδομένα αναγκαία για τον προσδιορισμό της ημερομηνίας, ώρας και διάρκειας της επικοινωνίας.
4. Δεδομένα αναγκαία για τον προσδιορισμό του είδους επικοινωνίας(τηλεφωνική υπηρεσία, διαδικτυακή υπηρεσία)
5. Δεδομένα αναγκαία για τον προσδιορισμό του εξοπλισμού επικοινωνίας των χρηστών ή του φερόμενου ως εξοπλισμού επικοινωνίας τους.
6. Δεδομένα αναγκαία για τον προσδιορισμό της θέσης του εξοπλισμού κινητής τηλεφωνίας.

- Νόμος 4411/2016: Κύρωση της Σύμβασης του Συμβουλίου της Ευρώπης για το έγκλημα στον Κυβερνοχώρο και του Προσθέτου Πρωτοκόλλου της, σχετικά με την ποινικοποίηση πράξεων ρατσιστικής και ξενοφοβικής φύσης, που διαπράττονται μέσω Συστημάτων Υπολογιστών - Μεταφορά στο ελληνικό δίκαιο της Οδηγίας 2013/40/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τις επιθέσεις κατά συστημάτων πληροφοριών και την αντικατάσταση της

απόφασης – πλαισίου 2005/222/ΔΕΥ του Συμβουλίου, ρυθμίσεις σωφρονιστικής και αντεγκληματικής πολιτικής και άλλες διατάξεις.

Γενικά, η Ελλάδα, ακολουθεί τη νομοθεσία που θεσπίζεται από το Ευρωπαϊκό Κοινοβούλιο έχοντας πάντα τη βοήθεια της Α.Δ.Α.Ε. και της Αρχής Προστασίας Προσωπικών Δεδομένων για την εξασφάλιση της ασφάλειας των τηλεπικοινωνιών σε εθνικό επίπεδο.

- **Α.Δ.Α.Ε. (Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών)**

Πέρα από την ισχύ της νομοθεσίας, το όργανο που είναι αρμόδιο για την προστασία των τηλεπικοινωνιών στον ελληνικό χώρο, είναι η Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών (Α.Δ.Α.Ε.).

Η Α.Δ.Α.Ε. είναι ανεξάρτητη αρχή η οποία έχει διοικητική αυτοτέλεια. Συστάθηκε το 2003 με σκοπό την προστασία του απορρήτου των επιστολών, της ελεύθερης ανταπόκρισης ή επικοινωνίας με οποιονδήποτε άλλο τρόπο καθώς και την ασφάλεια των δικτύων και πληροφοριών. Η Α.Δ.Α.Ε. αποτελείται από πολλά υποτμήματα που ασχολούνται συγκεκριμένα με τις υπηρεσίες διαδικτύου, τις τηλεπικοινωνιακές υπηρεσίες, τις ταχυδρομικές υπηρεσίες, τις διοικητικές και οικονομικές υπηρεσίες, τις δημόσιες και διεθνείς σχέσεις καθώς και την άρση του απορρήτου. Ακολουθεί η ανάλυση των διευθύνσεων της Α.Δ.Α.Ε. που αφορούν την προστασία των δεδομένων, του απορρήτου και γενικά των τηλεπικοινωνιών.

Η διεύθυνση Διασφάλισης Υποδομών, Απορρήτου Υπηρεσιών και Εφαρμογών του Διαδικτύου είναι αρμόδια για τη μελέτη και τον σχεδιασμό της ασφάλειας των εφαρμογών διαδικτύου, για την καταγραφή και την αξιολόγηση των τεχνολογιών ασφαλείας, για την καταγραφή των κανόνων συμμόρφωσης που πρέπει να ακολουθούνται καθώς και την καταγραφή τεχνολογικών προτάσεων. Επίσης, στις αρμοδιότητές της είναι η χρήση πρωτοκόλλων και εφαρμογών, η προστασία των δεδομένων και η διασφάλιση του απορρήτου από τις δικτυακές υποδομές του διαδικτύου. Τέλος, είναι αρμόδια για την παροχή πιστοποίησης των υπολογιστικών συστημάτων, των τερματικών, των δικτυακών υποδομών και των συστημάτων μετάδοσης πληροφορίας.

Η διεύθυνση Διασφάλισης Υποδομών και Απορρήτου Τηλεπικοινωνιακών Υπηρεσιών είναι αρμόδια για την παρακολούθηση των τεχνολογιών ενσύρματων και ασυρμάτων συστημάτων μετάδοσης πληροφοριών καθώς και των παρεχόμενων υπηρεσιών, την καταγραφή των ευάλωτων σημείων για επικείμενη βελτίωση και για τη διασφάλιση του απορρήτου της επικοινωνίας. Πιο συγκεκριμένα, στις αρμοδιότητες της διεύθυνσης Διασφάλισης Υποδομών και Απορρήτου Τηλεπικοινωνιακών Υπηρεσιών εντάσσονται τα συστήματα κινητής τηλεφωνίας, οι επίγειες μικροκυματικές και δορυφορικές ζεύξεις καθώς και συστήματα ευρείας ζώνης. Τέλος, είναι αρμόδια για την καταγραφή και τη μελέτη της διασφάλισης του απορρήτου σε ενσύρματα τηλεπικοινωνιακά συστήματα και για τους τρόπους πιστοποίησης παροχής ασφαλών επικοινωνιών.

Η Α.Δ.Α.Ε. περιλαμβάνει ένα αυτοτελές τμήμα το οποίο είναι υπεύθυνο για τον έλεγχο της άρσης του απορρήτου. Το τμήμα Ελέγχου Άρσης του Απορρήτου προβαίνει στην κατάσχεση μέσων παραβίασης του απορρήτου που υποπίπτουν στην αντίληψη της Α.Δ.Α.Ε. κατά την ενάσκηση του έργου της και ορίζεται μεσεγγυούχος αυτών μέχρι να αποφανθούν τα αρμόδια δικαστήρια. Επιπλέον, αρμοδιότητα του τμήματος είναι να προβαίνει στην καταστροφή πληροφοριών ή στοιχείων ή δεδομένων τα οποία αποκτήθηκαν με παράνομη παραβίαση του απορρήτου των επικοινωνιών. Το τμήμα Ελέγχου Άρσης του Απορρήτου εξετάζει

καταγγελίες σχετικά με την προστασία των δικαιωμάτων των αιτούντων, όταν θίγονται από τον τρόπο και τη διαδικασία άρσης του απορρήτου και εξετάζει επίσης τη νομιμότητα των εντολών για την άρση του απορρήτου. [22]

- **Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ)**

  Αποστολή της Αρχής αποτελεί η προστασία των δικαιωμάτων της προσωπικότητας και της ιδιωτικής ζωής του ατόμου στην Ελλάδα, σύμφωνα με τις διατάξεις των Ν. 2472/1997 και 3471/2006.

  Πρωταρχικός σκοπός της Αρχής είναι η προστασία του πολίτη από την παράνομη επεξεργασία των προσωπικών του δεδομένων αλλά και η συνδρομή προς αυτόν σε κάθε περίπτωση που διαπιστώνεται παραβίαση των σχετικών δικαιωμάτων του σε κάθε επιχειρησιακό τομέα (χρηματοπιστωτικά, υγεία, ασφάλιση, εκπαίδευση, δημόσια διοίκηση, μεταφορές, ΜΜΕ, κ.ο.κ).

  Επίσης, σκοπός της Αρχής είναι η υποστήριξη και καθοδήγηση των υπεύθυνων επεξεργασίας στην εκπλήρωση των υποχρεώσεων τους απέναντι στο νόμο, λαμβάνοντας υπόψη τις νέες ανάγκες υπηρεσιών της ελληνικής κοινωνίας, καθώς και την διείσδυση των σύγχρονων ψηφιακών επικοινωνιών και δικτύων. Ως εκ τούτου, η Αρχή στρέφει ιδιαίτερα την προσοχή της μεταξύ άλλων στην παρατήρηση και αντιμετώπιση ζητημάτων που προκύπτουν με την εξέλιξη των νέων τεχνολογιών και εφαρμογών.

5.3 Νομοθεσία των Η.Π.Α για τις υπηρεσίες Cloud

- USA Patriot Act: Μετά τις επιθέσεις της 11ης Σεπτεμβρίου του 2011, το αμερικανικό κογκρέσο ψήφισε τη νομοθεσία USA Patriot Act , η οποία δημιουργήθηκε με σκοπό τη πρόληψη επερχόμενων τρομοκρατικών επιθέσεων. Μέσω αυτής της νομοθεσίας, οι αμερικανικές αρχές έχουν την άδεια να παρακολουθούν λογαριασμούς, δεδομένα καθώς και τηλεφωνικές συνομιλίες ανθρώπων που θεωρούν υπόπτους για τρομοκρατικές πράξεις.

  Αν και δημιουργήθηκε με σκοπό τη πρόληψη της τρομοκρατίας, υπάρχουν παράθυρα στο νόμο για έλεγχο δεδομένων που είτε είναι αποθηκευμένα σε αμερικανικό έδαφος , είτε μεταφέρονται από την Ευρώπη στις Η.Π.Α..

  Πιο συγκεκριμένα, η παράγραφος 217 του USA Patriot Act, δίνει το δικαίωμα στις αμερικανικές αρχές να προβούν σε online παρακολούθηση χρηστών. Αυτό συνεπάγεται στο ότι εφόσον οι πάροχοι υπηρεσιών έχουν δώσει την άδεια, οι αμερικανικές αρχές μπορούν να ζητήσουν πρόσβαση σε οποιαδήποτε πληροφορία αποθηκευμένη στις πλατφόρμες του US cloud(όπως οι Amazon, Google, Facebook ,κτλ.). Ακόμα και αν οι εταιρίες αποθηκεύουν τα δεδομένα σε ευρωπαϊκό cloud, εφόσον είναι υποκείμενες στην αμερικάνικη νομοθεσία, οι αμερικανικές αρχές έχουν το δικαίωμα να έχουν πρόσβαση στα δεδομένα τους. [23]

- Foreign Intelligence and Surveillance Act(FISA): Νομοθεσία που ψηφίστηκε το 1978, η οποία επιτρέπει τη φυσική και ηλεκτρονική παρακολούθηση και συλλογή πληροφοριών ανάμεσα σε Αμερικανούς πολίτες και μη καθώς και υπηρεσίες με σκοπό την προστασία από τρομοκρατικές επιθέσεις και την υπόνοια κατασκοπείας.

- Foreign Intelligence and Surveillance Amendments Act (FISAA): Είναι η τροποποίηση της νομοθεσίας FISA, η οποία ψηφίστηκε το 2008 και επιτρέπει σε πιο χαλαρά πλαίσια την παρακολούθηση των ηλεκτρονικών συσκευών χρηστών που θεωρούνται τρομοκράτες.

Στην τροπολογία 1881a του FISAA, αναφέρεται η πιθανότητα παρακολούθησης επικοινωνίας και πρόσβασης στα δεδομένα ξένων πολίτων που βρίσκονται εκτός αμερικανικού εδάφους, χωρίς να απαιτείται ένταλμα ή προειδοποίηση του χρήστη ώστε να συμβουλευτεί κάποιο νομικό πρόσωπο εφόσον τα δεδομένα έχουν αποθηκευτεί σε data center που υπόκειται στην αμερικάνικη δικαιοδοσία. Έτσι, ένας πολίτης της Ευρωπαϊκής Ένωσης για παράδειγμα μπορεί να βρεθεί να παρακολουθείται από τις αμερικανικές αρχές διότι έχει τα δεδομένα του αποθηκευμένα π.χ. στη Google.

5.4 Νομοθεσία της Ε.Ε. για υπηρεσίες cloud

Οι νόμοι για την προστασία των δεδομένων στην Ευρώπη είναι από τους πιο αυστηρούς παγκοσμίως. Κάθε χώρα μέλος της Ε.Ε υποχρεούται να έχει τη δική του νομοθεσία περί ιδιωτικότητας των δεδομένων για προστασία των δικαιωμάτων των πολιτών ενάντια στη συλλογή πληροφοριών και την παρακολούθηση από κυβερνητικά μέσα ή από ιδιωτικούς φορείς.

- BDSG: Η Γερμανία έχει την πιο αυστηρή νομοθεσία όσον αφορά τις υπηρεσίες cloud (γνωστή ως Bundesdatenschutzgesetz ή BDSG) η οποία απαγορεύει τη πρόσβαση σε δεδομένα χωρίς την άδεια του κατόχου τους. Επιπλέον, η άδεια πρόσβασης σε δεδομένα που παραχωρεί κάποιος προσδιορίζει το πώς και για πόσο χρονικό διάστημα θα χρησιμοποιηθούν τα δεδομένα. Η άδεια πρόσβασης στα δεδομένα ενός χρήστη μπορεί να ανακληθεί οποιαδήποτε στιγμή από τον εν λόγω κάτοχο. Τέλος, το υπουργείο εσωτερικών της Γερμανίας, εξέδωσε οδηγίες προς εταιρείες που παρέχουν υπηρεσίες cloud οι οποίες προστάζουν την υπογραφή συμφωνίας με τις γερμανικές αρχές για να διασφαλίσουν ότι τα δεδομένα τα οποία θα μπουν στο μικροσκόπιο των αρχών δε θα χρησιμοποιηθούν για λόγους κατασκοπείας.
- Safe Harbor: Το Safe Harbor ήταν μια νομοθεσία η οποία δημιουργήθηκε το 2000 από τις αμερικανικές αρχές και το ευρωπαϊκό κοινοβούλιο η οποία επέτρεπε την αποθήκευση δεδομένων ευρωπαϊκών πολιτών σε αμερικανικό cloud, με την προϋπόθεση ότι η εταιρεία εξ Αμερικής η οποία παρείχε το cloud, θα τηρούσε τη νομοθεσία σχετικά με την προστασία των δεδομένων.

  Τον Οκτώβριο του 2015, το ευρωπαϊκό δικαστήριο θεώρησε άκυρη τη νομοθεσία Safe Harbor έπειτα από μια καταγγελία του Max Schrems, ενός αυστριακού πολίτη ο οποίος ζήτησε να διεξαχθεί έρευνα σχετικά με την επάρκεια της ασφάλειας για τη μεταφορά των δεδομένων του σε αμερικανικό έδαφος μέσω Facebook.

Εν κατακλείδι, γίνεται κατανοητή η έντονη προσφυγή σε υπηρεσίες cloud των οποίων οι πάροχοι εδρεύουν σε ευρωπαϊκό έδαφος αφού εξετάζοντας τις ισχύουσες νομοθεσίες σε ΗΠΑ και ΕΕ, παρατηρεί κανείς ότι οι ευρωπαϊκοί κανονισμοί είναι πιο αυστηροί και δεν αφήνουν περιθώρια για παραβίαση των προσωπικών δεδομένων[24].

Παρόλα αυτά, ο λόγος δημιουργίας του υπολογιστικού νέφους ήταν να διευκολύνει τους χρήστες της τεχνολογίας και όχι να τους φέρει σε διαμάχη. Έτσι, τον Φεβρουάριο του 2016, η ευρωπαϊκή επιτροπή και οι Ηνωμένες Πολιτείες συμφώνησαν για ένα καινούριο νόμο-πλαίσιο για την υπερατλαντική μεταφορά δεδομένων.

Πλαίσιο ασπίδα προστασίας ΕΕ – ΗΠΑ για την ιδιωτικότητα. Η νομοθεσία αυτή περιλαμβάνει τα εξής:

- Αυστηρές υποχρεώσεις για τις επιχειρήσεις και σθεναρή επιβολή: Η νέα ρύθμιση είναι διαφανής και περιλαμβάνει αποτελεσματικούς μηχανισμούς εποπτείας,

ώστε να διασφαλιστεί ότι οι επιχειρήσεις τηρούν τις υποχρεώσεις τους. Ορίζεται η επιβολή κυρώσεων ή αποκλεισμού εάν οι εταιρείες δεν συμμορφώνονται. Οι νέοι κανόνες περιλαμβάνουν αυστηρότερους όρους για περαιτέρω διαβιβάσεις σε άλλους εταίρους από τις εταιρείες που συμμετέχουν στο σύστημα.

- Σαφείς διασφαλίσεις και υποχρεώσεις διαφάνειας όσον αφορά την πρόσβαση της κυβέρνηση των ΗΠΑ: Η κυβέρνηση των ΗΠΑ έδωσε στην ΕΕ γραπτή διαβεβαίωση από το Γραφείο Διευθυντή των Εθνικών Υπηρεσιών Πληροφοριών ότι οποιαδήποτε πρόσβαση των δημόσιων αρχών για σκοπούς εθνικής ασφάλειας θα υπόκειται σε σαφείς περιορισμούς, διασφαλίσεις και μηχανισμούς επίβλεψης, αποτρέποντας έτσι τη γενικευμένη πρόσβαση σε δεδομένα προσωπικού χαρακτήρα. Ο υπουργός Εξωτερικών των ΗΠΑ, κ. John Kerry, δεσμεύτηκε να θεσπίσει δυνατότητα προσφυγής στον τομέα της εθνικής υπηρεσίας πληροφοριών για τους Ευρωπαίους μέσω μηχανισμού συνηγόρου του πολίτη στο πλαίσιο του Υπουργείου Εσωτερικών, ο οποίος θα είναι ανεξάρτητος από τις εθνικές υπηρεσίες ασφάλειας. Ο συνήγορος θα δίνει συνέχεια σε καταγγελίες και ερωτήσεις που υποβάλλονται από μεμονωμένα πρόσωπα και θα ενημερώνει τους ενδιαφερομένους εάν έχουν τηρηθεί οι σχετικοί νόμοι. Αυτές οι γραπτές δεσμεύσεις θα δημοσιευτούν στο ομοσπονδιακό μητρώο των ΗΠΑ.
- Αποτελεσματική προστασία των δικαιωμάτων των πολιτών της ΕΕ με πολλές δυνατότητες προσφυγής: Οι καταγγελίες πρέπει να επιλύονται από τις εταιρείες σε διάστημα 45 ημερών. Θα παρέχεται δωρεάν λύση με εναλλακτικούς τρόπους επίλυσης διαφορών. Οι πολίτες της ΕΕ μπορούν να απευθυνθούν και στις εθνικές τους αρχές προστασίας δεδομένων, οι οποίες θα συνεργαστούν με την Ομοσπονδιακή Επιτροπή Εμπορίου ώστε να διασφαλίσουν ότι θα ερευνηθούν και θα διευθετηθούν οι εκκρεμείς καταγγελίες πολιτών της ΕΕ. Εάν δεν διευθετηθεί μια υπόθεση με άλλα μέσα, θα υπάρχει μηχανισμός διαιτησίας ως έσχατη λύση με τον οποίο θα διασφαλίζονται εκτελεστά διορθωτικά μέτρα. Επιπλέον, οι εταιρείες μπορούν να δεσμευτούν ότι θα συμμορφωθούν με συμβουλές από τις ευρωπαϊκές αρχές προστασίας δεδομένων. Αυτό αποτελεί υποχρέωση των εταιρειών που διαχειρίζονται δεδομένα ανθρώπινων πόρων.
- Ετήσιος κοινός μηχανισμός αξιολόγησης: Ο μηχανισμός θα παρακολουθεί τη λειτουργία της ασπίδας προστασίας για την ιδιωτικότητα, συμπεριλαμβανομένων των δεσμεύσεων και των διαβεβαιώσεων όσον αφορά την πρόσβαση σε δεδομένα για σκοπούς επιβολής του νόμου και εθνικής ασφάλειας. Η Ευρωπαϊκή Επιτροπή και το Υπουργείο Εμπορίου των ΗΠΑ θα προβαίνουν στην αξιολόγηση, στην οποία θα καλούν να συμμετάσχουν εθνικούς εμπειρογνώμονες των υπηρεσιών πληροφοριών από τις ΗΠΑ και τις ευρωπαϊκές αρχές προστασίας δεδομένων. Η Επιτροπή θα κάνει χρήση όλων των άλλων διαθέσιμων πηγών πληροφόρησης, συμπεριλαμβανομένων των εκθέσεων διαφάνειας από τις εταιρείες για την έκταση των απαιτήσεων κρατικής πρόσβασης. Η Επιτροπή θα διοργανώνει, επίσης, ετήσια διάσκεψη κορυφής για την ιδιωτικότητα με ενδιαφερόμενες ΜΚΟ και φορείς για να συζητούνται οι ευρύτερες εξελίξεις στον τομέα του δικαίου περί ιδιωτικότητας των ΗΠΑ και του αντίκτυπού τους στους Ευρωπαίους. Στο πλαίσιο της ετήσιας αξιολόγησης, η Επιτροπή θα δημοσιεύει έκθεση προς το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο.

6. ΣΥΜΠΕΡΑΣΜΑ

Η βιομηχανία των τηλεπικοινωνιών κρατά τον κόσμο συνδεδεμένο. Οι πάροχοι των τηλεπικοινωνιών δημιουργούν και διαχειρίζονται το πολύπλοκο σύστημα υποδομών που χρησιμοποιούνται για τη μετάδοση φωνής και δεδομένων. Επιπλέον, αποθηκεύουν μεγάλα ποσά ευαίσθητων δεδομένων, πράγμα που τους καθιστά τον κύριο στόχο για επιθέσεις από κυβερνοεγκληματίες.

Οι απειλές για την ασφάλεια των τηλεπικοινωνιακών συστημάτων παρουσιάζουν συνεχή εξέλιξη ανάλογη της εξέλιξης της τεχνολογίας. Οι νέες μορφές απειλών, έχουν ως αποτέλεσμα την επιτακτική ανάγκη για ανεύρεση νέων τρόπων προστασίας και αντιμετώπισης τυχόν επιθέσεων στα συστήματα.

Αντίστοιχα με τη δημιουργία των νέων τρόπων προστασίας των τηλεπικοινωνιών, δημιουργούνται και νέα νομοθετικά πλαίσια που διασφαλίζουν τη νομιμότητα της χρήσης των τεχνικών προστασίας των συστημάτων. Η Ευρωπαϊκή Ένωση, συνεχώς αναβαθμίζει τους νόμους της σχετικά με την ασφάλεια των προσωπικών δεδομένων των πολιτών της. Επίσης, τα τελευταία χρόνια αναπτύσσει ένα νέο νομοθετικό πλαίσιο το οποίο επικεντρώνεται στην προστασία των δεδομένων που αποθηκεύονται σε υπηρεσίες υπολογιστικού νέφους, καθώς με τη συνεχή χρήση του διαδικτύου όλοι στρέφονται στο cloud για την αποθήκευση των δεδομένων τους.

Παρόλα αυτά η νομοθεσία, όσο ισχυρή και αν είναι δεν αρκεί για να προστατευτεί κάποιος χρήστης του διαδικτύου. Ειδικά όταν οι χρήστες στρέφονται στο σκοτεινό διαδίκτυο (deep και dark web) είτε για να διατηρήσουν την ανωνυμία τους, είτε για αγορές προϊόντων που είναι δυσεύρετα στο επιφανειακό ίντερνετ, η ασφάλεια είναι ανύπαρκτη. Το dark web, το οποίο αποτελεί και το μεγαλύτερο μέρος του διαδικτύου, είναι άκρως επικίνδυνο για χρήστες χωρίς εμπειρία καθώς εκεί βρίσκονται οι περισσότεροι κυβερνοεγκληματίες, έμποροι παράνομων ουσιών και παιδεραστές.

Αυτή η μελέτη διεξήχθη με βάση τα δεδομένα της τελευταίας δεκαετίας, εξετάζοντας την πρόοδο των συστημάτων ως προς την αντιμετώπιση των νέων απειλών καθώς και την πρόοδο της νομοθεσίας που αφορά την προστασία των προσωπικών δεδομένων των χρηστών τηλεπικοινωνιακών υπηρεσιών. Ο χώρος των τηλεπικοινωνιών δικτύων είναι ένας τομέας ο οποίος συνεχώς θα εξελίσσεται ανά τα χρόνια και σίγουρα θα αποτελέσει το κύριο θέμα ερευνών και εργασιών πολλών ερευνητών και πανεπιστημιακών ιδρυμάτων, αφού η χρήση των δικτύων αποτελεί ένα μέρος της καθημερινότητας της πλειοψηφίας των ανθρώπων.

ΠΙΝΑΚΑΣ ΟΡΟΛΟΓΙΑΣ

Ξενόγλωσσος όρος	**Ελληνικός Όρος**
Security threats	Απειλές ασφάλειας
Phishing	Ηλεκτρονικό “ψάρεμα”
Malware	Επιβλαβές λογισμικό
Man in the middle attacks	Επίθεση ενδιάμεσης οντότητας
Worms	Σκουλήκια
Spyware	Κατασκοπευτικό λογισμικό
Trojan horse	Δούρειος Ίππος
Data Retention and Investigatory Powers	Διατήρηση και Διερεύνηση των Δεδομένων
Internet Monitoring	Έλεγχος Διαδικτύου
Cloud	Υπολογιστικό νέφος
Dark Web	Σκότεινό Ίντερνετ
Traffic analysis	Ανάλυση της κίνησης
Food and Drug Administration	Ομοσπονδία τροφίμων και φαρμάκων
Physical access	Φυσική είσοδος
Logical access	Λογική είσοδος
Domain Name System	Σύστημα Ονοματοδοσίας Διαδικτύου
Internet Corporation for Assigned Names and Numbers	Εκχώρηση Ονομάτων και Αριθμών
Overlay Networks	Δίκτυα Επικάλυψης
End-to-end encryption	Από-άκρο-σε-άκρο κρυπτογράφηση
Open Source Software	Λογισμικού ανοιχτού κώδικα
Security baselines	Γραμμές Προστασίας

ΣΥΝΤΜΗΣΕΙΣ – ΑΡΚΤΙΚΟΛΕΞΑ – ΑΚΡΩΝΥΜΙΑ

DDoS	Distributed Denial of Service
CSPs	Cellular Service Providers
ISPs	Internet Service Providers
DRIP	Data Retention and Investigatory Powers
SCA	Stored Communications Act
NSA	Εθνική Υπηρεσία Ασφάλειας των Ηνωμένων Πολιτειών
GCHQ	Βρετανική Υπηρεσία Πληροφοριών
NIST	National Institute of Standards and Technology
OTA	Over The Air
GSM	Global System for Mobile Communications
HRC	Human Rights Campaign
DNS	Domain Name System
ICANN	Internet Corporation for Assigned Names and Numbers
TLDs	Top-level domains
NIT	Network Investigative Technique
FDA	Food and Drug Administration
E2E	End-to-end encryption
OSS	Open Source Software
EFF	Electronic Frontier Foundation
PPE	Prism-proof email
ΕΕΠΔ	Ευρωπαίος Επόπτης Προστασίας Δεδομένων
ΑΔΑΕ	Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών
ΑΠΔΠΧ	Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα
FISA	Foreign Intelligence and Surveillance Act
FISAA	Foreign Intelligence and Surveillance Amendments Act
BDSG	Bundesdatenschutzgesetz

ΑΝΑΦΟΡΕΣ

[1] Υπηρεσία ερευνών του Ευρωπαϊκού Κοινοβουλίου (STOA unit), *Mass surveillance study (parts 1 and 3)*

[2] Georgia Institute of Technology, *Emerging cyber threats report 2016*

[3] Kaspersky labs, *Threat Intelligence report for the telecommunications industry*

[4] Πληροφορίες από την ιστοσελίδα: http://antivirussw.weebly.com/history.html

[5] Πληροφορίες από την ιστοσελίδα: http://www.cisco.com

[6] Πληροφορίες από την ιστοσελίδα: https://blogs.windows.com

[7] Πληροφορίες από την ιστοσελίδα: https://www.ibm.com

[8] Πληροφορίες από την ιστοσελίδα: http://www.dell.com/

[9] *"Explainer: what is the dark web?"* : http://theconversation.com/explainer-what-is-the-dark-web-46070

[10] Dr. Vincenzo Ciancaglini, Dr. Marco Balduzzi, Robert McArdle, and Martin Rösler , "Below the Surface: Exploring the Deep Web"

[11] *About Tor project* : https://www.torproject.org/

[12] *What is Freenet* : https://freenetproject.org/about.html

[13] *About I2P project*: https://geti2p.net/en/

[14] *"Silk Road: How FBI closed in on suspect Ross Ulbricht"*: http://www.bbc.com/news/technology-24371894

[15] *"How a Russian Dark Web Drug Market Outlived the Silk Road (And Silk Road 2)"*: https://www.wired.com/2014/11/oldest-drug-market-is-russian/

[16] *"Meet The 'Assassination Market' Creator Who's Crowdfunding Murder With Bitcoins"*: http://www.forbes.com/sites/andygreenberg/2013/11/18/meet-the-assassination-market-creator-whos-crowdfunding-murder-with-bitcoins/#4f778a511ac1

[17] *"FBI crack Tor and catch 1,500 visitors to biggest child pornography website on the dark web"*: http://www.ibtimes.co.uk/fbi-crack-tor-catch-1500-visitors-biggest-child-pornography-website-dark-web-1536417#

[18] *"Cancer Patients Driven to Darknet for Cheap Drugs"*: http://www.ibtimes.co.uk/cancer-patients-driven-darknet-cheap-drugs-1462358

[19] Περί ευρωπαϊκής νομοθεσίας όλοι οι νόμοι που αναφέρθηκαν προήλθαν από την ιστοσελίδα του Ευρωπαϊκού Κοινοβουλίου EUR-Lex: http://eur-lex.europa.eu/homepage.html

[20] *Ευρωπαϊκός Επόπτης Προστασίας Δεδομένων*: https://europa.eu/european-union/about-eu/institutions-bodies/european-data-protection-supervisor_el

[21] Περί ελληνικής νομοθεσίας όλοι οι νόμοι που αναφέρθηκαν προήλθαν από την Εφημερίδα της Κυβερνήσεως

[22] *Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών*: www.adae.gr/

[23] Stephanie Overby, *"The Patriot Act and Your Data: Should You Ask Cloud Providers About Protection?"*, http://www.cio.com/article/2400264/government/the-patriot-act-and-your-data--should-you-ask-cloud-providers-about-protection-.html

[24] *"Foreign clouds in the European sky: how US laws affect the privacy of Europeans"*: https://policyreview.info/articles/analysis/foreign-clouds-european-sky-how-us-laws-affect-privacy-europeans