
**ΕΘΝΙΚΟ ΚΑΙ ΚΑΠΟΔΙΣΤΡΙΑΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ**

**ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ**
**ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ**

**ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ**
**ΜΗΧΑΝΙΚΗ ΥΠΟΛΟΓΙΣΤΩΝ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ ΚΑΙ ΔΙΚΤΥΩΝ**


**ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ**

# Η υιοθέτηση του HTTPS υπό το πρίσμα του GDPR


**Αφροδίτη Η. Ιβανίδου**

**Επιβλέπων:** **Κωνσταντίνος Λιμνιώτης,** Εξωτερικός Διδάσκων



**ΑΘΗΝΑ**

**ΑΠΡΙΛΙΟΣ 2023**


**NATIONAL AND KAPODISTRIAN UNIVERSITY OF ATHENS**

**DEPARTMENT OF INFORMATICS & TELECOMMUNICATIONS**

**POSTGRADUATED STUDIES PROGRAM**
**COMPUTER, TELECOMMUNICATIONS AND NETWORK ENGINEERING**


**THESIS**

# The HTTPS adoption in light of the GDPR


**Afroditi I. Ivanidou**

**Supervisor:** **Konstantinos Limniotis,** External Instructor



**ATHENS**

**APRIL 2023**

**ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ**

# Η υιοθέτηση του HTTPS υπό το πρίσμα του GDPR

**Αφροδίτη Η. Ιβανίδου**

**ΑΜ:** EN.3.20.0005

**ΕΠΙΒΛΕΠΩΝ:** **Κωνσταντίνος Λιμνιώτης,** Εξωτερικός Διδάσκων

**ΕΞΕΤΑΣΤΙΚΗ ΕΠΙΤΡΟΠΗ:** **Δημήτριος Κατσιάνης**, Επίκουρος Καθηγητής
**Νικόλαος Πασσάς**, Εργαστηριακό Διδακτικό Προσωπικό (ΕΔΙΠ)

ΑΠΡΙΛΙΟΣ 2023

**THESIS**

# The HTTPS adoption in light of the GDPR

**Afroditi I. Ivanidou**

**AM:** EN.3.20.0005

**SUPERVISOR:** **Konstantinos Limniotis,** External Instructor

**SELECTION BOARD:** **Dimitrios Katsianis**, Assistant Professor
**Nikolaos Passas**, Laboratory Teaching Staff

**APRIL 2023**

# ΠΕΡΙΛΗΨΗ

Το πρωτόκολλο Transport Layer Security (TLS) αποτελεί το πιο διαδεδομένο μέσο κρυπτογραφημένης επικοινωνίας στο παγκόσμιο ιστό. Αναπτύχθηκε αρχικά από την Netscape Communications στα μέσα της δεκαετίας του 1990 και ήρθε να καλύψει κενά ασφαλείας του προκατόχου του, του πρωτοκόλλου Secure Sockets Layer (SSL). Από τότε μέχρι και σήμερα εξυπηρετεί δισεκατομμύρια χρήστες του διαδικτύου σε καθημερινή βάση. Η αυξανόμενη χρήση του πρωτοκόλλου το έχει καταστήσει στόχο επιθέσεων, γεγονός που έχει οδηγήσει στη βελτιστοποίηση του. Οι αδυναμίες που βρέθηκαν σε προηγούμενες εκδόσεις του ώθησε τον οργανισμό Internet Engineering Task Force (IETF) να αναπτύξει μια νέα έκδοση του, δηλαδή το TLS 1.3.

Με την ολοένα αυξανόμενη χρήση του διαδικτύου, η ανάγκη προστασίας των προσωπικών δεδομένων, που διακινούνται καθημερινά σε αυτό, ώθησε την Ευρωπαϊκή Ένωση (Ε.Ε.) να θεσπίσει ένα ενιαίο σύνολο κανόνων για όλα τα κράτη - μέλη της. Τον Απρίλιο του 2016 το Συμβούλιο της Ε.Ε. Και το Ευρωπαϊκό Κοινοβούλιο εξέδωσαν τον Γενικό Κανονισμό Προστασίας Δεδομένων (ΓΚΠΔ), ο οποίος τέθηκε σε ισχύ για όλα τα κράτη μέλη της Ε.Ε. από τις 25 Μαΐου 2018. Ο ΓΚΠΔ δίνει ιδιαίτερη έμφαση στην εφαρμογή κατάλληλων τεχνικών μέτρων για την εξασφάλιση των προσωπικών δεδομένων, σημαντικότερο από τα οποία είναι η χρήση της κρυπτογραφίας. Με αυτό τον τρόπο η χρήση του πρωτοκόλλου TLS έρχεται να αποτελέσει ένα από τα κύρια μέτρα προστασίας των προσωπικών δεδομένων κατά την περιήγηση μας στο διαδίκτυο.



**ΘΕΜΑΤΙΚΗ ΠΕΡΙΟΧΗ**: Το HTTPS υπό το Πρίσμα του ΓΚΠΔ

**ΛΕΞΕΙΣ ΚΛΕΙΔΙΑ**: HTTPS, TLS, Ασφάλεια στο Διαδίκτυο, ΓΚΠΔ

# ABSTRACT

The Transport Layer Security (TLS) protocol is the most widely used mean of encrypted communication on the World Wide Web. It was originally developed by Netscape Communications in the mid-1990s and came to fill security gaps in its predecessor, the SSL protocol. From then until today it serves billions of internet users on a daily basis. The increasing use of the protocol has made it a target for attacks, which has led to its optimization. Weaknesses found in previous versions of it prompted the Internet Engineering Task Force (IETF) to develop a new version of it, namely TLS 1.3.

With the ever-increasing use of the internet, the need to protect personal data, which is traded daily on it, prompted the European Union (EU) to establish a single set of rules for all its member states. In April 2016, the EU Council and the European Parliament issued the General Data Protection Regulation (GDPR), which came into force for all EU member states from 25 May 2018. The GDPR places particular emphasis on the application of appropriate technical measures to secure personal data, the most important of which is the use of cryptography. In this way, the use of the TLS protocol comes to be one of the main measures to protect personal data when browsing the Internet.



**SUBJECT AREA**: HTTPS in the Light of GDPR

**KEYWORDS**: HTTPS, TLS, Web Security, GDPR

# ΕΥΧΑΡΙΣΤΙΕΣ

Αρχικά θα ήθελα να εκφράσω τις ευχαριστίες μου στον επιβλέποντα της διπλωματικής μου εργασίας, τον Καθηγητή του Τμήματος Πληροφορικής και Τηλεπικοινωνιών του Εθνικού και Καποδιστριακού Πανεπιστημίου Αθηνών Κωνσταντίνο Λιμνιώτη, ο οποίος με καθοδήγησε στην έρευνα του θέματος της εργασίας μου και ήταν πάντα δίπλα μου όταν χρειάστηκα τη βοήθεια του. Επιπλέον θα ήθελα να ευχαριστήσω τους γονείς μου και όλους όσους με υποστήριξαν καθ'όλο το διάστημα των σπουδών μου και της εκπόνησης της διπλωματικής μου εργασίας. Δίχως την στήριξη τους τίποτα από όλα αυτά δεν θα ήταν εφικτό.

**Αφροδίτη Η. Ιβανίδου**

# ΠΕΡΙΕΧΟΜΕΝΑ

# ΚΑΤΑΛΟΓΟΣ ΕΙΚΟΝΩΝ

# ΚΑΤΑΛΟΓΟΣ ΠΙΝΑΚΩΝ

# 1. ΕΙΣΑΓΩΓΗ

Η παρούσα έρευνα έχει ως σκοπό την μελέτη της χρησιμοποίησης ασφαλών μεθόδων επικοινωνίας στο διαδίκτυο από φορείς του ελληνικού δημόσιου τομέα που παρέχουν διαδικτυακές υπηρεσίες. Συνακόλουθα εξετάζεται και η συμμόρφωση τους με βασικές αρχές που θέτει ο ΓΚΠΔ προς αυτή την κατεύθυνση και συγκεκριμένα η κρυπτογραφημένη διακίνηση των προσωπικών δεδομένων αλλά και η υποχρέωση διαφάνειας ως προς την επεξεργασία των δεδομένων. Στη συνέχεια παρουσιάζονται στατιστικά στοιχεία σχετικά με τη χρήση του πρωτοκόλλου TLS 1.3 υπό το πρίσμα του ΓΚΠΔ.

## 1.1 Κίνητρα και στόχοι

Η εκτεταμένη χρήση διαδικτυακών υπηρεσιών έχει ως αποτέλεσμα την διακίνηση τεράστιου όγκου προσωπικών δεδομένων στο διαδίκτυο. Η εξέλιξη αυτή στον τρόπο παροχής υπηρεσιών, όπως ήταν αναμενόμενο, έχει επηρεάσει και τον δημόσιο τομέα στη χώρα μας και έχει καταστήσει επιτακτική την ανάγκη προστασίας των δεδομένων αυτών με μεθόδους που συνάδουν με το ισχύον νομοθετικό πλαίσιο.

Σημαντικό ρόλο για την προστασία των δεδομένων παίζει η χρήση ασφαλών πρωτοκόλλων για τη διακίνηση τους στο διαδίκτυο, που δίνουν τη δυνατότητα κρυπτογράφησης τους με ισχυρούς αλγόριθμους. Το 2018 με τη θέση σε ισχύ του ΓΚΠΔ η χρήση κρυπτογράφησης θεωρήθηκε ένα από τα μέτρα που θα πρέπει να εξετάζεται ως προς την ανάγκη υιοθέτησής της, προκειμένου να εξασφαλίσει την προστασία των προσωπικών δεδομένων. Το πρωτόκολλου που ευρέως χρησιμοποιείται σήμερα στο διαδίκτυο και παρέχει τη μέγιστη δυνατή ασφάλεια είναι το TLS, η τελευταία έκδοση του οποίου είναι η 1.3.

Σε έρευνα που διεξήχθη το 2018 σχετικά με τη χρήση του Hypertext Transfer Protocol Secure (HTTPS) από δημοφιλής ελληνικές ιστοσελίδες, βρέθηκε πως από τις ιστοσελίδες του δημοσίου τομέα περίπου το 70% έκανε χρήση ασφαλούς πρωτοκόλλου επικοινωνίας στο διαδίκτυο εξασφαλίζοντας τη προστασία των προσωπικών δεδομένων που διακινούνταν. Το ποσοστό αυτό θα μπορούσε κανείς να θεωρήσει πως ήταν ικανοποιητικό, δεδομένης και της παράλληλης θέσης σε ισχύ εκείνη την χρονική περίοδο του ΓΚΠΔ, που έθεσε αυστηρά όρια σε σχέση με την προστασία των δεδομένων. Αξιοσημείωτα ωστόσο ήταν και τα αποτελέσματα σχετικά με την ευαισθητοποίηση των χρηστών για ασφαλή περιήγηση στο διαδίκτυο, όπου βρέθηκε πως μισοί περίπου από αυτούς που ερωτήθηκαν δεν γνώριζαν τη διαφορά ανάμεσα στο Hypertext Transfer Protocol (HTTP) με το HTTPS.

Σκοπός της παρούσας εργασίας είναι να γίνει εκ νέου έρευνα για τη χρήση του HTTPS από ιστοσελίδες του ελληνικού δημοσίου προκειμένου να συγκριθούν τα αποτελέσματα που προκύπτουν 4 έτη μετά την αρχική έρευνα και μετά τη θέση σε ισχύ του ΓΚΠΔ. Επιπλέον δίνεται έμφαση και στην ενημέρωση που παρέχεται πλέον στους χρήστες για την επεξεργασία προσωπικών τους δεδομένων και αν αυτή θεωρείται επαρκής και σύννομη. Οι θεματικές ενότητες που παρουσιάζονται είναι οι εξής:

1. Συνοπτική παρουσίαση του ΓΚΠΔ.
2. Παρουσίαση των πρωτοκόλλου TLS.
3. Ανάλυση της λειτουργίας του πρωτοκόλλου TLS .
4. Παρουσίαση των εκδόσεων του πρωτοκόλλου TLS.
5. Αναφορά σε γνωστές επιθέσεις στο πρωτόκολλο TLS.
6. Παρουσίαση προηγούμενων ερευνών σχετικά με την υιοθέτηση του HTTPS.
7. Ανάλυση αποτελεσμάτων ελέγχου για την υιοθέτηση του HTTPS από ιστοσελίδες του ελληνικού δημόσιου τομέα.
8. Αξιολόγηση κινδύνου σχετικά με την διακίνηση προσωπικών δεδομένων από ιστοσελίδες του ελληνικού δημόσιου τομέα.
9. Ανάλυση αποτελεσμάτων ελέγχου για την ενημέρωση χρηστών για την επεξεργασία προσωπικών τους δεδομένων από ιστοσελίδες του ελληνικού δημόσιου τομέα.

### 1.2 Ερευνητικά Ερωτήματα

Για να υλοποιηθεί ο στόχος που αναφέρεται παραπάνω χρειάστηκε να απαντηθούν ορισμένα ερευνητικά ερωτήματα, τα σημαντικότερα των οποίων αναγράφονται παρακάτω:

***"Πως επιτυγχάνεται η ασφάλεια των επικοινωνιών στο διαδίκτυο;"***

Η ασφάλεια των επικοινωνιών στο διαδίκτυο μπορεί να επιτευχθεί με εγκαθίδρυση ενός ασφαλούς καναλιού επικοινωνίας μεταξύ του Client και του Server. Ως ασφαλές κανάλι επικοινωνίας μπορεί να οριστεί το κανάλι όπου η πληροφορία διακινείται κρυπτογραφημένη ώστε ακόμα και να πέσει στα χέρια ενός κακόβουλου χρήστη να μην μπορεί να γίνει κατανοητή. Περαιτέρω, θα πρέπει να διασφαλίζεται ότι τα δεδομένα είναι ακέραια (δηλαδή ότι δεν έχουν αλλοιωθεί κατά τη μετάδοσή τους), καθώς επίσης και ότι τα ίδια τα μέλη της επικοινωνίας είναι αυθεντικοποιημένα.

***"Ποιο πρωτόκολλο ασφαλούς επικοινωνίας χρησιμοποιείται σήμερα στο διαδίκτυο;"***

Το πρωτόκολλο TLS είναι το πιο ευρέως χρησιμοποιούμενο πρωτόκολλο για κρυπτογραφημένη επικοινωνία στο Διαδίκτυο. Το TLS 1.0 κυκλοφόρησε το 1999, ακολουθούμενο από το TLS 1.1 το 2006, το TLS1.2 το 2008 και το TLS 1.3 το 2018. Το πρωτόκολλο TLS χρησιμοποιείται από το HTTPS. Το HTTP είναι πρωτόκολλο επιπέδου 7 (επίπεδο εφαρμογών). Το TLS είναι πρωτόκολλο επιπέδου 4 (μεταφοράς). Όταν στο επίπεδο μεταφοράς υλοποιείται το TLS, τότε αυτομάτως η υλοποίηση του HTTP στο επίπεδο 7 αποκαλείται πλέον HTTPS.

***"Πως οδηγηθήκαμε στη χρήση ενός ενιαίου κανονισμού για την προστασία των προσωπικών δεδομένων από όλα τα κράτη – μέλη της Ε.Ε.;"***

Η αυξανόμενη χρήση ηλεκτρονικών υπηρεσιών και η αλόγιστη διακίνηση δεδομένων στο διαδίκτυο γέννησε την ανάγκη αναθεώρησης του νομοθετικού πλαισίου για την προστασία των προσωπικών δεδομένων που ίσχυε σε κράτη – μέλη της Ε.Ε.. Για να αντιμετωπιστούν προβλήματα έλλειψής συνοχής στην εφαρμογή και την ερμηνεία από τα

κράτη – μέλη αποφασίστηκε η θέσπιση ενιαίου νομοθετικού πλαισίου, με το οποίο θα μπορούσε να εξασφαλιστεί μία συλλογική εναρμονισμένη προσέγγιση στα όρια της Ε.Ε..

***"Πως η χρήση του TLS σχετίζεται με την ασφάλεια των προσωπικών δεδομένων όπως ορίζεται στο ΓΚΠΔ;"***

Σύμφωνα με το ΓΚΠΔ ο υπεύθυνος επεξεργασίας προσωπικών δεδομένων θα πρέπει να εφαρμόζει κατάλληλα τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλίζεται το κατάλληλο επίπεδο ασφάλειας έναντι των κινδύνων, περιλαμβανομένων, μεταξύ άλλων, την ψευδωνυμοποίηση και την κρυπτογράφηση των δεδομένων προσωπικού χαρακτήρα. Παρόλο που ο ΓΚΠΔ δεν κάνει αναφορά στο πρωτόκολλο TLS η παραπάνω υποχρέωση των φορέων να λαμβάνουν τα πλέον κατάλληλα μέτρα ασφάλειας με βάση τους κινδύνους για τα δικαιώματα και τις ελευθερίες των προσώπων καθιστά, πρακτικά, τη χρήση του TLS υποχρεωτική σε πολλές περιπτώσεις.

***"Σε τι βαθμό έχουν συμμορφωθεί με τον ΓΚΠΔ οι υπεύθυνοι επεξεργασίας δεδομένων που ανήκουν στο δημόσιο τομέα και παρέχουν διαδικτυακές υπηρεσίες;"***

Το τελευταίο χρονικό διάστημα η πανδημία του Covid-19 δημιούργησε την ανάγκη παροχής περισσότερων ηλεκτρονικών υπηρεσιών. Τα εμπορικά καταστήματα προσαρμόστηκαν απευθείας στις νέες απαιτήσεις εκτοξεύοντας στα ύψη το ηλεκτρονικό εμπόριο. Ο δημόσιος τομέας έπρεπε με τη σειρά του να ακολουθήσει τις εξελίξεις παρέχοντας πλέον ηλεκτρονικές υπηρεσίες στους πολίτες. Χρονικά το πέρασμα σε μία νέα εποχή για τον δημόσιο τομέα, συνέπεσε με τη θέση σε ισχύ του ΓΚΠΔ. Από την αρχή το ποσοστό συμμόρφωσης των υπευθύνων επεξεργασίας με τις νέες απαιτήσεις ήταν ικανοποιητικό και δείχνει συνεχώς να αυξάνεται με το πέρασμα των χρόνων.

***"Είναι ενημερωμένα τα υποκείμενα των δεδομένων για τα δικαιώματα που έχουν σε σχέση με την επεξεργασία των προσωπικών τους δεδομένων από ιστοσελίδες στο διαδίκτυο;"***

Μία από τις απαιτήσεις του ΓΚΠΔ είναι και η ενημέρωση του υποκειμένου των δεδομένων για την επεξεργασία τους. Πολλοί δημόσιοι φορείς και ιδιωτικές επιχειρήσεις προσπαθώντας να καλύψουν τις απαιτήσεις του νέου νομοθετικού πλαισίου έδωσαν μεγάλη έμφαση στους τρόπους προστασίας των προσωπικών δεδομένων αφήνοντας στην άκρη την ενημέρωση των υποκειμένων των δεδομένων. Ακόμα και σήμερα εντοπίζονται ιστοσελίδες που δεν παρέχουν καθόλου ενημέρωση ή η ενημέρωση που παρέχουν δεν είναι σύμφωνα με όσα ορίζονται στο ΓΚΠΔ.

### 1.3 Δομή της εργασίας

Η παρούσα εργασία ξεκινάει με μία σύντομη παρουσίαση των κυριότερων σημείων του ΓΚΠΔ. Στη συνέχεια παρουσιάζονται τα πρωτόκολλα TLS και HTTPS που εξασφαλίζουν τη διακίνηση κρυπτογραφημένων δεδομένων στο διαδίκτυο.

Στο κύριο μέρος της εργασίας παρουσιάζονται προηγούμενες έρευνες σχετικά με την υιοθέτηση του πρωτοκόλλου HTTPS από ιστοσελίδες στο παγκόσμιο ιστό αλλά και από δημοφιλής ελληνικές ιστοσελίδες, οι οποίες κατηγοριοποιήθηκαν σε i) Ηλεκτρονικά καταστήματα, ii) Ενημερωτικού χαρακτήρα, iii) Πάροχοι τηλεπικοινωνιών, iv) Εκπαιδευτικές, v) Οικονομικού χαρακτήρα (συμπεριλαμβανομένου και ιστοσελίδες τραπεζών), vi) Άλλες εταιρείες, vii) Δημοσίου τομέα.

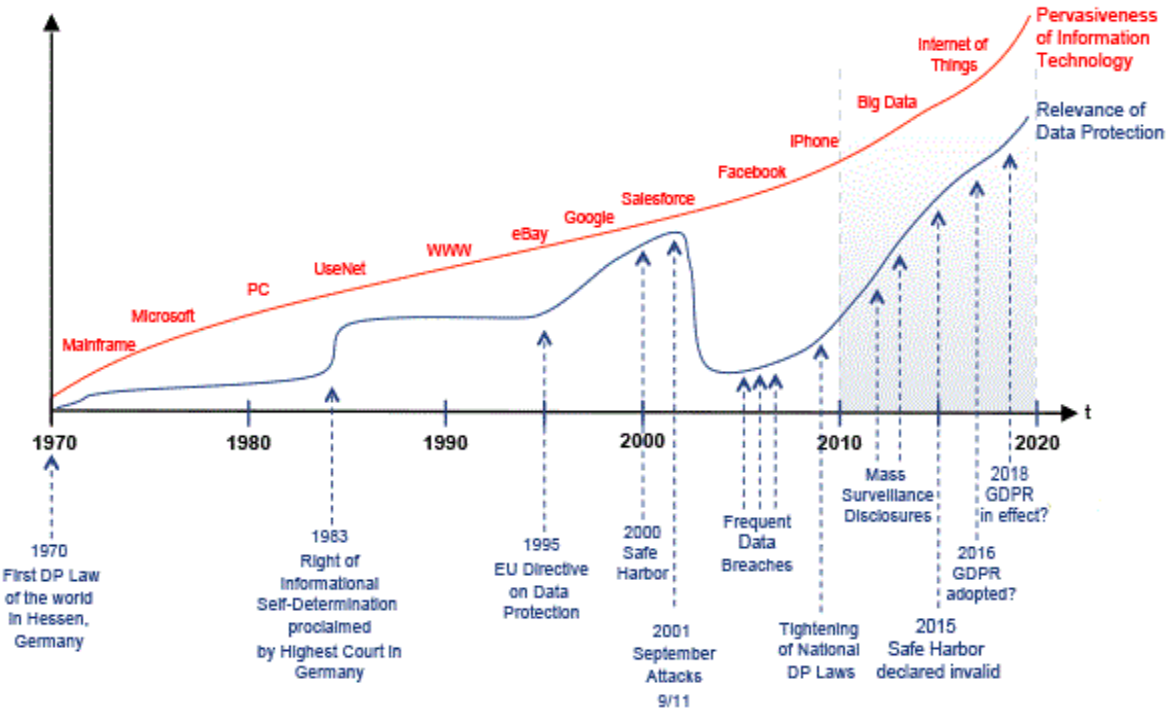
Εν συνεχεία παρουσιάζεται η έρευνα που έγινε για την υιοθέτηση του πρωτοκόλλου HTTPS από ιστοσελίδες του ελληνικού δημόσιου τομέα υπό το πρίσμα του ΓΚΠΔ. Ο έλεγχος πραγματοποιήθηκε για το χρονικό διάστημα από τον Ιούλιο του 2022 έως τον Οκτώβριο του 2022. Προκειμένου να γίνει αντιληπτή η αξία της χρήσης του HTTPS έγινε αξιολόγηση του κινδύνου σε περιπτώσεις ιστοσελίδων που βρέθηκαν να μη χρησιμοποιούν ασφαλή πρωτόκολλα περιήγησης στο διαδίκτυο. Τέλος έγινε έλεγχος της παροχής ενημέρωσης των χρηστών των εξεταζόμενων ιστοτόπων σχετικά με την επεξεργασία των προσωπικών τους δεδομένων. Προκειμένου να γίνουν αντιληπτά όσα παρουσιάζονται στα κεφάλαια 4-5-6-7 θα πρέπει να γίνουν κατανοητές οι έννοιες των κεφαλαίων 2-3-4.

# 2. ΓΕΝΙΚΟΣ ΚΑΝΟΝΙΣΜΟΣ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ (GDPR)

Σε αυτό το κεφάλαιο παρουσιάζονται ο δρόμος προς την υιοθέτηση ενός Κανονισμού για την προστασία των προσωπικών δεδομένων από όλα τα κράτη μέλη της Ε.Ε. και τα σημαντικότερα σημεία αυτού του Κανονισμού.

## 2.1 Ιστορικά στοιχεία

Η πρώτη προσπάθεια για την θέσπιση κανονισμών για την προστασία των προσωπικών δεδομένων στην Ε.Ε. χρονολογείται στην δεκαετία του 1970 μετά από ραγδαίες εξελίξεις στον τομέα της τεχνολογίας και των πληροφοριών. Το 1985 τέθηκε σε ισχύ η Σύμβαση 108 του Συμβουλίου της Ευρώπης για την προστασία προσωπικών δεδομένων και αργότερα το 1995 κυκλοφόρησε η Οδηγία της Ευρωπαϊκής Ένωσης 95/46/ΕΚ, η οποία περιείχε κανόνες για την επεξεργασία των προσωπικών δεδομένων εντός της Ε.Ε. αλλά και για την διακίνηση τους μεταξύ των κρατών μελών της. Το 2009 η Ευρωπαϊκή Επιτροπή ξεκίνησε την αναθεώρηση της παραπάνω οδηγίας ως προς ορισμένες πτυχές που θα μπορούσε να βελτιωθεί, όπως η θέσπιση μιας ενιαίας νομοθεσίας σχετικά με την προστασία των δεδομένων για όλα τα κράτη της Ε.Ε.. Τον Απρίλιο του 2016 το Συμβούλιο της Ε.Ε. Και το Ευρωπαϊκό Κοινοβούλιο ενέκριναν την πρόταση αναθεώρησης και εκδόθηκε ο ΓΚΠΔ, ο οποίος τέθηκε σε ισχύ για όλα τα κράτη μέλη της Ε.Ε. από τις 25 Μαΐου 2018.




**Εικόνα 1: Ιστορία του GDPR**

## 2.2 Βασικές αρχές που διέπουν την προστασία προσωπικών δεδομένων

Με την θέση σε ισχύ του Κανονισμού δόθηκε η δυνατότητα ελέγχου της ορθής χρήσης των προσωπικών δεδομένων τόσο από δημόσιους όσο και όσο ιδιωτικούς οργανισμούς. Η προστασία των δεδομένων θεωρήθηκε επιβεβλημένη λόγω της συνεχούς ανάπτυξης της ψηφιακής οικονομίας που είχε ως αποτέλεσμα την καθημερινή διακίνηση τεράστιου όγκου δεδομένων τόσο εντός όσο και εκτός της Ευρώπης.

Όπως ήταν αναμενόμενο δημιουργήθηκαν επιπλέον υποχρεώσεις για τους υπεύθυνους επεξεργασίας δεδομένων και νέα δικαιώματα για τα υποκείμενα των δικαιωμάτων. Με τον νέο Κανονισμό διευρύνθηκε η έννοια των προσωπικών δεδομένων περιλαμβάνοντας πλέον και πληροφορίες που θα μπορούσαν να χρησιμοποιηθούν για τον έμμεσο προσδιορισμό ατόμων όπως αριθμοί ταυτότητας, δεδομένα τοποθεσίας και ηλεκτρονικά αναγνωριστικά, συμπεριλαμβανομένων διευθύνσεων Internet Protocol (IP address) και cookies ιστού καθώς και πολλά άλλα.

Συγκριτικά με το προϊσχύον νομοθετικό πλαίσιο αίσθηση έχουν προκαλέσει τα διοικητικά πρόστιμα για την παραβίαση του Κανονισμού, τα οποία ανέρχονται πλέον σε 10.000.000 € ή έως 2% του ετήσιου τζίρου και σε 20.000.000 € ή έως το 4% του παγκόσμιου τζίρου για επιχειρήσεις με παγκόσμια παρουσία. Επιπλέον για οργανισμούς που διαχειρίζονται μεγάλο όγκο δεδομένων θεσπίζεται η υποχρέωση ορισμού Υπεύθυνου Προστασίας Δεδομένων, ο οποίος είναι υπεύθυνος για την εναρμόνιση του οργανισμού με τον Κανονισμό. Από την πλευρά των υποκειμένων των δικαιωμάτων θα πρέπει να υπάρχει η συγκατάθεσή τους για την επεξεργασία των δεδομένων τους και τους δίνεται το πολυσυζητημένο πλέον “δικαίωμα στην λήθη”. Τέλος τα προϊόντα και οι υπηρεσίες θα πρέπει να σχεδιάζονται εξαρχής λαμβάνοντας υπόψη την προστασία της ιδιωτικότητας (Privacy by design).

Ο Κανονισμός απαιτεί συνετή χρήση των προσωπικών δεδομένων από τους υπεύθυνους επεξεργασίας και η διαδικασία που πρέπει να ακολουθηθεί σε περίπτωση παραβίασης των δεδομένων στηρίζεται σε συγκεκριμένο μηχανισμό. Η επεξεργασία λοιπόν των δεδομένων θα πρέπει να ακολουθεί τις παρακάτω αρχές:

- Να είναι σύννομη και να προκύπτει από διαφανείς διαδικασίες.
- Η συλλογή δεδομένων να γίνεται για καθορισμένους, σαφείς και νόμιμους σκοπούς.
- Να συλλέγονται μόνο τα απαραίτητα δεδομένα για τους σκοπούς της επεξεργασίας.
- Να τηρούνται τα δεδομένα ενημερωμένα.
- Να διατηρούνται μόνο για όσο χρονικό διάστημα χρειάζεται.
- Η επεξεργασία τους να γίνεται με τέτοιο τρόπο ώστε να διασφαλίζεται η μέγιστη δυνατή ασφάλεια.

## 2.3 Δικαιώματα του υποκειμένου των δεδομένων

Μία από τις κύριες ιδέες πίσω από τον ΓΚΠΔ είναι ότι τα υποκείμενα των δικαιωμάτων πρέπει να ανακτήσουν τον έλεγχο των προσωπικών τους δεδομένων και να ενισχυθούν τα δικαιώματα τους σχετικά με την επεξεργασία τους. Με τον νέο αυτό Κανονισμό, προκειμένου να θεωρηθεί σύννομη η επεξεργασία των δεδομένων, θα πρέπει να ισχύει τουλάχιστον μία από τις προϋποθέσεις που ορίζονται στο άρθρο 6. Σύμφωνα λοιπόν με την παρ.1 του άρθρου 6 του ΓΚΠΔ η συναίνεση του υποκειμένου είναι μία από αυτές τις προϋποθέσεις. Η συγκατάθεση του υποκειμένου θα πρέπει να δίνεται μετά από ενημέρωση του με ξεκάθαρο τρόπο για το ποιος θα επεξεργαστεί τα δεδομένα του, για πόσο καιρό και για ποιόν λόγο. Σκοπός των κανόνων αυτών είναι να διασφαλιστεί ότι το υποκείμενο των δεδομένων κατανοεί για τι πραγματικά έχει δώσει τη συγκατάθεσή του. Αυτό σημαίνει ότι η συγκατάθεση πρέπει να δίνεται ελεύθερα, συγκεκριμένα και χωρίς ασάφειες με δήλωση διατυπωμένη σε απλή και κατανοητή γλώσσα.

Μετά τη συναίνεση, τα υποκείμενα των δικαιωμάτων έχουν το δικαίωμα διόρθωσης σχετικά με ανακριβείς πληροφορίες ή ανάκλησης προηγούμενης συγκατάθεσης ανά πάσα στιγμή. Επιπλέον, ο ΓΚΠΔ εισάγει το «δικαίωμα στη λήθη». Όταν δεν υπάρχουν πλέον λόγοι για την επεξεργασία των προσωπικών τους δεδομένων, τα υποκείμενα έχουν το δικαίωμα να ζητήσουν τη διαγραφή τους έτσι ώστε τα δεδομένα αυτά να μην υπόκεινται πλέον σε επεξεργασία. Τα υποκείμενα μπορούν επίσης να ζητήσουν πρόσβαση στα προσωπικά τους δεδομένα για να γνωρίζουν πώς και εάν αυτά τα δεδομένα επεξεργάζονται. Οι πολίτες έχουν τέλος δικαίωμα στη φορητότητα των δεδομένων με τη λήψη αντιγράφου τους σε δομημένο, κοινώς χρησιμοποιούμενο και αναγνώσιμο από μηχανήματα μορφότυπο, καθώς και το δικαίωμα να διαβιβάζουν τα εν λόγω δεδομένα σε άλλον υπεύθυνο επεξεργασίας. Εάν κάποιο από αυτά τα δικαιώματα παραβιαστεί, οποιοδήποτε άτομο έχει το δικαίωμα να υποβάλει καταγγελία στην εποπτική αρχή [2].

## 2.4 Υπεύθυνος προστασίας δεδομένων

Σύμφωνα με τον ΓΚΠΔ, είναι υποχρεωτικό για ορισμένους οργανισμούς να διορίζουν Υπεύθυνο Προστασίας Δεδομένων. Η υποχρέωση αυτή αφορά δημόσιες αρχές και οργανισμούς που επεξεργάζονται προσωπικά δεδομένα σε μεγάλη κλίμακα. Ο Υπεύθυνος Προστασίας Δεδομένων βρίσκεται στο επίκεντρο αυτού του νέου Κανονισμού καθώς ο ρόλος του είναι να παρακολουθεί τις λειτουργίες επεξεργασίας των δεδομένων, να διευκολύνει τη διαδικασία συμμόρφωσης και να λειτουργεί ως σημείο επαφής μεταξύ του οργανισμού των εποπτικών αρχών και των υποκειμένων των δεδομένων. Οι οργανισμοί μπορούν να διορίσουν έναν Υπεύθυνο Προστασίας Δεδομένων από κοινού ή να ορίσουν έναν εξωτερικό συνεργάτη [2].

## 2.5 Προστασία δεδομένων εκ σχεδιασμού και εξ ορισμού

Για τον μετριασμό των κινδύνων που συνεπάγεται η επεξεργασία και η αποθήκευση προσωπικών δεδομένων εισάγονται με τον ΓΚΠΔ οι έννοιες της προστασίας των δεδομένων εκ σχεδιασμού και εξ ορισμού. Με αυτό τον τρόπο παρέχεται το πλαίσιο

ανάπτυξης συστημάτων και εφαρμογών για την προστασία της ακεραιότητας των δεδομένων καθ' όλη τη διάρκεια του κύκλου ζωής ενός έργου.

Ορισμένες τέτοιες μέθοδοι προστασίας των δικαιωμάτων περιγράφονται στον ΓΚΠΔ:

- **Ελαχιστοποίηση δεδομένων (άρθρα 5 και 25 του ΓΚΠΔ):** Αναφέρεται στην έννοια της μη αποθήκευσης περισσότερων δεδομένων από ό,τι είναι απαραίτητο για την εκάστοτε εργασία. Επίσης, σημαίνει ελαχιστοποίηση των πραγματικών δεδομένων που ενδέχεται να ταυτοποιήσουν ένα άτομο σε μία βάση δεδομένων.

- **Έλεγχος πρόσβασης (άρθρο 29 του ΓΚΠΔ):** Θα πρέπει να έχουν πρόσβαση στα προσωπικά δεδομένα μόνο οι χρήστες που υπάρχει ανάγκη να έχουν πρόσβαση. Για αυτό το λόγο τα συστήματα που διαχειρίζονται προσωπικά δεδομένα θα πρέπει να διαθέτουν μηχανισμούς ελέγχου πρόσβασης.

- **Προστασία των δεδομένων:** Τα συστήματα πληροφορικής που επεξεργάζονται προσωπικά δεδομένα θα πρέπει να είναι ασφαλή καθ' όλη τη διάρκεια του κύκλου ζωής τους. Η χρήση τέτοιων λειτουργιών εκ των υστέρων, δηλαδή όταν ένα σύστημα έχει ήδη αναπτυχθεί, είναι δύσκολο και παράλληλα κοστοβόρο. Θα πρέπει λοιπόν ο αρχικός τους σχεδιασμός να λαμβάνει υπόψη την ασφάλεια των δεδομένων. Αυτό επιτυγχάνεται τις περισσότερες φορές όταν ενσωματώνεται σε ένα σύστημα η λειτουργία της κρυπτογράφησης. Από την πλευρά των χρηστών θα πρέπει να υπάρχουν σαφείς κανόνες και πολιτικές για την διαχείριση συμβάντων παραβίασης των δεδομένων καθώς και διαδικασίες για την ασφαλή καταστροφή των δεδομένων όταν δεν είναι πλέον απαραίτητη η τήρηση τους.

- **Φιλικά προς τον χρήστη συστήματα:** Συστήματα τα οποία μπορούν να χρησιμοποιηθούν για να καθοδηγήσουν τους χρήστες των συστημάτων να εργαστούν με τρόπο που προωθεί το απόρρητο από προεπιλογή, για παράδειγμα, μη συλλέγοντας υπερβολικά δεδομένα και μη εμφανίζοντας δεδομένα που δεν είναι απαραίτητα. Τα συστήματα που έχουν σχεδιαστεί για χρήση από το υποκείμενο των δεδομένων θα πρέπει να έχουν σαφής και κατανοητές πληροφορίες για τον λόγο που συλλέγονται τα δεδομένα και για το πως θα χρησιμοποιηθούν (άρθρο 4, παράγραφος 11 του ΓΚΠΔ).

### 2.6 Ασφάλεια δεδομένων

Ο όρος προστασία δεδομένων σχετίζεται με τη διαδικασία προστασίας δεδομένων τόσο από εσωτερικές όσο και από εξωτερικές απειλές. Το κλειδί για την προστασία των δεδομένων είναι η διασφάλιση της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας.

- Εμπιστευτικότητα: Για να διασφαλιστεί ότι τα δεδομένα δεν αποκαλύπτονται ή διατίθενται σε μη εξουσιοδοτημένους χρήστες.

- Ακεραιότητα: Για να διασφαλιστεί ότι τα δεδομένα παραμένουν στην αρχική τους κατάσταση, που σημαίνει ότι δεν μπορούν να τροποποιηθούν από μη εξουσιοδοτημένους χρήστες.

- Διαθεσιμότητα: Για να διασφαλιστεί ότι τα δεδομένα είναι διαθέσιμα ανά πάσα στιγμή και ότι το σύστημα που τα φιλοξενεί είναι πλήρως λειτουργικό χωρίς σφάλματα.

Σύμφωνα με το άρθρο 34 του ΓΚΠΔ σε περίπτωση παραβίασης, ο υπεύθυνος επεξεργασίας των δεδομένων δεν έχει υποχρέωση να ειδοποιήσει τα υποκείμενα των δικαιωμάτων εφόσον έχει εφαρμόσει τεχνικά μέτρα που διασφαλίζουν την εμπιστευτικότητα των δεδομένων, ένα από τα οποία είναι η κρυπτογράφηση. Επιπλέον σύμφωνα με το άρθρο 83 του ΓΚΠΔ για την επιβολή του προστίμου λαμβάνονται υπόψη τα τεχνικά και οργανωτικά μέτρα που έχουν εφαρμόσει ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία. Αυτό υποδεικνύει ότι η εφαρμογή κατάλληλων τεχνικών μέτρων και συγκεκριμένα η κρυπτογράφηση των δεδομένων πρέπει να είναι πρωταρχική λύση για την προστασία δεδομένων και ένα ουσιαστικό αντίμετρο ενάντια σε διάφορες απειλές και τρωτά σημεία.

Τα δεδομένα διακρίνονται σε δεδομένα που βρίσκονται αποθηκευμένα σε κάποιο συγκεκριμένο σημείο ενός συστήματος και σε δεδομένα που μεταφέρονται σε ένα δίκτυο. Για την προστασία των δεδομένων που διακινούνται στο διαδίκτυο έχουν αναπτυχθεί εικονικά ιδιωτικά δίκτυα (Virtual Private Networks - VPN). Υπάρχουν διαφορετικά πρωτόκολλα που μπορούν να χρησιμοποιηθούν για την κρυπτογράφηση των δεδομένων κατά την διακίνηση τους, όπως για παράδειγμα το TLS, το οποίο χρησιμοποιεί έναν συνδυασμό συμμετρικής και ασύμμετρης κρυπτογράφησης.

## 2.7 Εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων

Η εκτίμηση αντικτύπου είναι μια διαδικασία σχεδιασμένη για να περιγράψει την επεξεργασία προσωπικών δεδομένων και να αξιολογήσει την αναγκαιότητα αυτής της επεξεργασίας σε συνάρτηση με τους κινδύνους που προκύπτουν από αυτήν. Ο ΓΚΠΔ διευκρινίζει ότι όταν η επεξεργασία προσωπικών δεδομένων μπορεί να οδηγήσει σε υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των ατόμων, θα πρέπει να διενεργείται μελέτη εκτίμησης αντικτύπου για την αξιολόγηση των εγγενών κινδύνων μιας τέτοιας επεξεργασίας. Εάν υπάρχει οποιαδήποτε δραστηριότητα επεξεργασίας με εγγενείς υψηλούς κινδύνους για τους πολίτες και τα προσωπικά τους δεδομένα θα πρέπει να ζητείται η γνώμη των εποπτικών αρχών πριν από την επεξεργασία [2].

Η μελέτη εκτίμησης αντικτύπου αποτελεί εργαλείο για την οικοδόμηση και την επίδειξη συμμόρφωσης για τους οργανισμούς καθώς με αυτή μπορεί να αξιολογήσουν τους κινδύνους και να αποδείξουν ότι ελήφθησαν υπόψη τα κατάλληλα μέτρα για την επεξεργασία των δεδομένων. Με αυτή την αξιολόγηση των κινδύνων, οι οργανισμοί είναι καλύτερα προετοιμασμένοι στο να αποφύγουν παραβιάσεις δεδομένων, και κατ’επέκταση να αποφύγουν πιθανές επιβολές προστίμων.

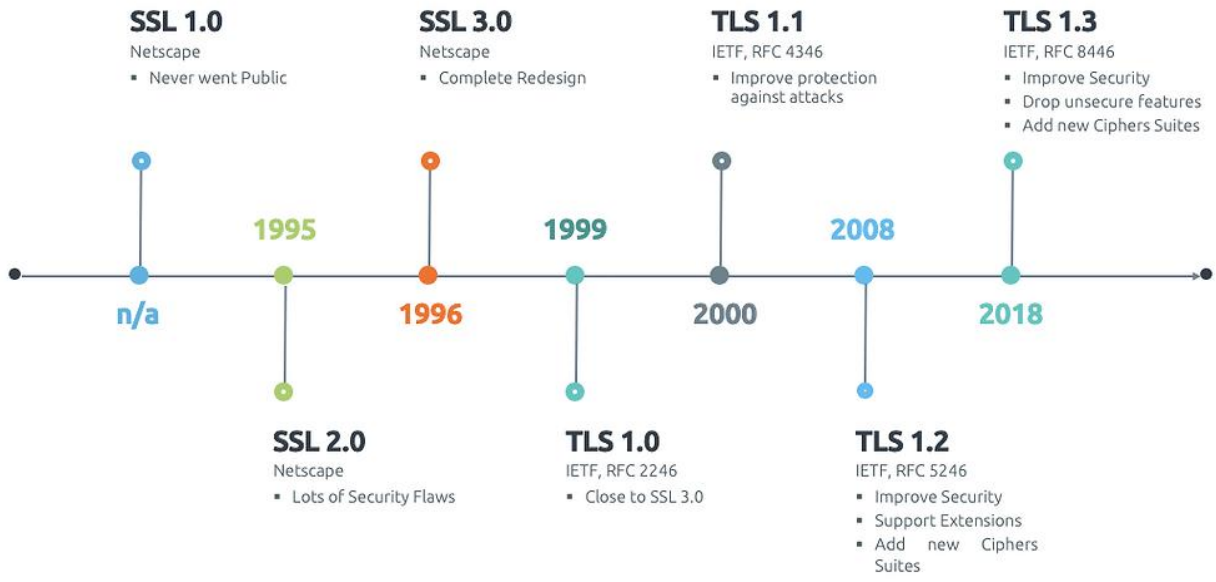
## 2.8 Επιπτώσεις μη συμμόρφωσης με τον Κανονισμό

Οι οργανισμοί που δεν συμμορφώνονται με τον ΓΚΠΔ ενδέχεται να υπόκεινται σε εκτεταμένα διοικητικά πρόστιμα σύμφωνα με ένα νέο σύστημα παραβάσεων που εισήχθη με τον Κανονισμό. Τα πρόστιμα που ενδέχεται να επιβληθούν στους οργανισμούς που παραβιάζουν τον Κανονισμό είναι σημαντικά και μπορούν να φτάσουν έως και το 4% των παγκόσμιων εσόδων ή τα 20 εκατομμύρια ευρώ εάν πρόκειται για σοβαρές παραβιάσεις. Για λιγότερο σημαντικές παραβάσεις μπορούν να επιβληθούν πρόστιμα που ανέρχονται έως και στο 2% των παγκόσμιων εσόδων ή σε 10 εκατομμύρια ευρώ [2].

Η Αρχή Προστασίας Δεδομένων έχει δώσει ιδιαίτερη σημασία στην εφαρμογή του ΓΚΠΔ, εκδίδοντας πλήθος αποφάσεων, γνωμοδοτήσεων και κατευθυντήριων οδηγιών. Συγκεκριμένα, σύμφωνα με σχετικά στατιστικά στοιχεία, για το χρονικό διάστημα από 25/5/18 έως και 24/5/22, γνωστοποιήθηκαν στην Αρχή 542 περιστατικά παραβίασης του ΓΚΠΔ και επιβλήθηκαν συνολικά πρόστιμα 11.190.500 ευρώ [28].

# 3. ΤΟ ΠΡΩΤΟΚΟΛΛΟ TLS

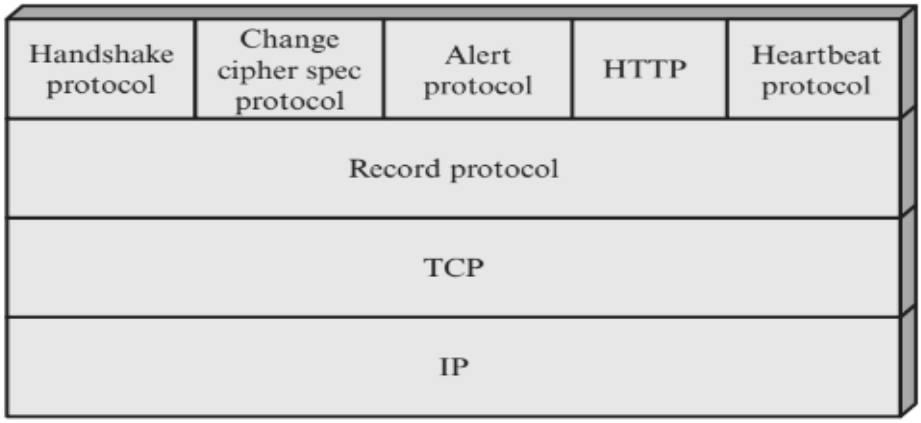
Σε αυτό το κεφάλαιο παρουσιάζονται οι λειτουργίες του πρωτοκόλλου TLS, οι εκδόσεις του και γνωστές επιθέσεις. Το πρωτόκολλο TLS είναι το πιο ευρέως χρησιμοποιούμενο πρωτόκολλο για κρυπτογραφημένη επικοινωνία στο Διαδίκτυο. Η Netscape Communications ανέπτυξε τον προκάτοχό του πρωτοκόλλου, το SSL τη δεκαετία του 1990. Η δεύτερη έκδοση του SSL κυκλοφόρησε το 1995, ακολουθούμενη από την τρίτη έκδοση το 1996. Αργότερα το ίδιο έτος ο οργανισμός IETF εισήγαγε το πρωτόκολλο TLS με σκοπό να τυποποιήσει μια έκδοση του SSL ως απάντηση στην αυξανόμενη ανάγκη για υποστήριξη ηλεκτρονικού εμπορίου και την αυξανόμενη υιοθέτηση του SSL. Το TLS 1.0 κυκλοφόρησε το 1999, ακολουθούμενο από το TLS 1.1 το 2006, το TLS1.2 το 2008 και το TLS 1.3 το 2018.




**Εικόνα 2: SSL/TLS Timeline**

## 3.1 Η λειτουργία του πρωτοκόλλου TLS 1.2

Το πρωτόκολλο TLS είναι ένα πρωτόκολλο σχεδιασμένο να παρέχει υπηρεσίες ασφαλείας για πρωτόκολλα που εκτελούνται στο επίπεδο εφαρμογής (application layer). Συγκεκριμένα, το TLS τρέχει πάνω από το πρωτόκολλο TCP (Transmission Control Protocol), ένα αξιόπιστο πρωτόκολλο δικτύου που διασφαλίζει την παράδοση των πακέτων δικτύου. Ο πρωταρχικός στόχος του TLS είναι να διευκολύνει την ίδρυση ενός ασφαλούς καναλιού επικοινωνίας μεταξύ του Client και του Server [4].



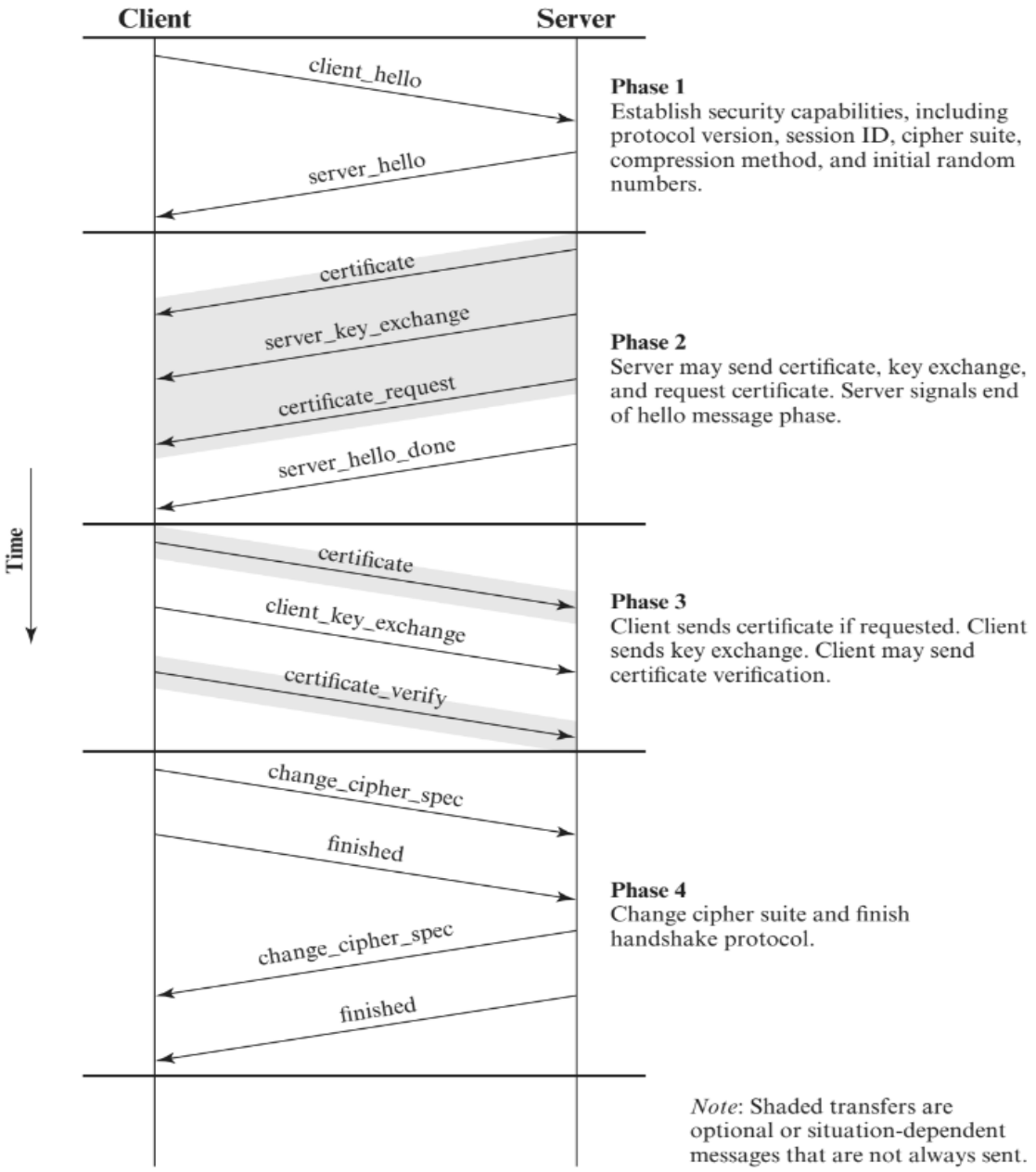

**Εικόνα 3: TLS Protocol Stack**

Το TLS παρέχει βασικές υπηρεσίες ασφαλείας σε πρωτόκολλα ανώτερων επιπέδων. Ειδικότερα, το HTTP, το οποίο παρέχει την υπηρεσία μεταφοράς δεδομένων μεταξύ ενός Client και ενός Web Server, μπορεί να λειτουργήσει πάνω από το TLS.

Όπως φαίνεται και στην Εικόνα 3 το πρωτόκολλο TLS αποτελείται από έναν αριθμό υποπρωτόκολλων, τα δύο πιο σημαντικά εκ των οποίων είναι το Handshake Protocol και το Record Protocol.

- Handshake Protocol

Το πιο περίπλοκο μέρος του TLS είναι το Handshake Protocol. Το Handshake Protocol χρησιμοποιεί κρυπτογραφία δημόσιου κλειδιού για να δημιουργήσει ένα κοινό μυστικό κλειδί μεταξύ του Server και του Client. Με αυτό τον τρόπο ο Server και ο Client μπορούν να επαληθεύουν ο ένας τον άλλον και να διαπραγματεύονται όλες τις κρυπτογραφικές παραμέτρους συμπεριλαμβανομένης της έκδοσης TLS, του ελέγχου ταυτότητας και της μεθόδου ανταλλαγής κλειδιών. Αυτό το πρωτόκολλο χρησιμοποιείται πριν από τη μετάδοση δεδομένων [5].




**Εικόνα 4: Handshake Protocol**

- Record Protocol

Το Record Protocol χρησιμοποιεί το μυστικό κλειδί που έχει καθιερωθεί στο Handshake Protocol για την προστασία της επικοινωνίας μεταξύ του Client και του Server. Το Record Protocol παρέχει δύο υπηρεσίες για συνδέσεις TLS:

■ Εμπιστευτικότητα: Το Handshake Protocol ορίζει ένα κοινό μυστικό κλειδί που χρησιμοποιείται για κρυπτογράφηση.

■ Ακεραιότητα μηνύματος: Το Handshake Protocol ορίζει επίσης ένα κοινό μυστικό κλειδί που χρησιμοποιείται για το σχηματισμό ενός κωδικού ελέγχου ταυτότητας μηνύματος (Message Authentication Code - MAC).

Το Record Protocol παίρνει ένα μήνυμα εφαρμογής προς μετάδοση, κατακερματίζει τα δεδομένα σε διαχειρίσιμα μπλοκ, προαιρετικά συμπιέζει τα δεδομένα, εφαρμόζει ένα MAC, κρυπτογραφεί, προσθέτει μια κεφαλίδα και μεταδίδει τη μονάδα που προκύπτει σε ένα TCP segment. Τα δεδομένα που λαμβάνονται αποκρυπτογραφούνται, επαληθεύονται, αποσυμπιέζονται και επανασυναρμολογούνται πριν παραδοθούν σε χρήστες υψηλότερου επιπέδου.

- Change Cipher Spec Protocol

Το πρωτόκολλο Change Cipher Spec Protocol είναι ένα από τα τέσσερα πρωτόκολλα ειδικά για το TLS που χρησιμοποιούν το Record Protocol του TLS, και είναι το απλούστερο. Αυτό το πρωτόκολλο αποτελείται από ένα ενιαίο μήνυμα, το οποίο αποτελείται από ένα μόνο byte με την τιμή 1. Ο μοναδικός σκοπός αυτού του μηνύματος είναι να προκαλέσει την αντιγραφή της κατάστασης σε εκκρεμότητα στην τρέχουσα κατάσταση, η οποία ενημερώνει τη σουίτα κρυπτογράφησης που θα χρησιμοποιηθεί σε αυτήν τη σύνδεση.

- Alert Protocol

Το πρωτόκολλο ειδοποίησης χρησιμοποιείται για τη μεταφορά ειδοποιήσεων που σχετίζονται με το TLS στην ομότιμη οντότητα. Όπως και με άλλες εφαρμογές που χρησιμοποιούν το TLS, τα μηνύματα ειδοποίησης συμπιέζονται και κρυπτογραφούνται, όπως καθορίζεται από την τρέχουσα κατάσταση.

Κάθε μήνυμα σε αυτό το πρωτόκολλο αποτελείται από δύο bytes. Το πρώτο byte παίρνει την τιμή “warning” (1) ή “fatal” (2) για να μεταφέρει τη σοβαρότητα του μηνύματος. Εάν το επίπεδο είναι fatal, το TLS τερματίζει αμέσως τη σύνδεση. Άλλες συνδέσεις στην ίδια περίοδο λειτουργίας μπορεί να συνεχιστούν, αλλά δεν επιτρέπεται η εγκαθίδρυση καμίας νέας σύνδεσης. Το δεύτερο byte περιέχει έναν κωδικό που υποδεικνύει τη συγκεκριμένη ειδοποίηση.

### 3.2 Το TLS 1.3

Με τις ανησυχίες να αυξάνονται για την ασφάλεια της TLS έκδοσης 1.2 λόγω των πολλών επιθέσεων, αλλά και με κίνητρο την επιθυμία να καταργηθούν οι παλιοί αλγόριθμοι, να ενισχυθεί το απόρρητο και να μειωθεί ο λανθάνοντας χρόνος δημιουργίας σύνδεσης, το 2014 η ομάδα εργασίας TLS του IETF ξεκίνησε μια πολυετή διαδικασία για την ανάπτυξη και την τυποποίηση μιας νέας έκδοσης του TLS, της έκδοσης 1.3. Από το 2014 έως το 2018 συνολικά δημοσιεύτηκαν 29 προσχέδια του TLS 1.3, με ενεργή ανατροφοδότηση από τη βιομηχανία και τον ακαδημαϊκό κόσμο. Το έγγραφο που τυποποιεί το TLS 1.3

είναι το RFC (Requests for Comments) 8446, το οποίο δημοσιεύτηκε τον Αύγουστο του 2018 και έχει λάβει πλέον ευρεία υιοθέτηση.

Η πιο σημαντική διαφορά του TLS 1.3 με τον προκάτοχο του είναι ότι μια χειραψία TLS της έκδοσης 1.3 απαιτεί λιγότερο χρόνο από μια χειραψία TLS έκδοσης 1.2. Τα οφέλη του TLS 1.3 περιλαμβάνουν [6]:

- Μείωση του round-trip time, με αποτέλεσμα ταχύτερη χειραψία.
- Βελτίωση των χρόνων καθυστέρησης με μείωση του αριθμού των round-trips.
- Βελτίωση της απόδοσης των ιστοσελίδων και ως εκ τούτου βελτίωση της εμπειρίας του χρήστη.
- Αφαίρεση ευάλωτων αλγορίθμων και κρυπτογράφησης.

**Απόδοση**

Οι ασφαλείς συνδέσεις μεταξύ client και server δημιουργούνται με αυτό που συνήθως αναφέρεται ως χειραψία SSL/TLS. Η χειραψία περιλαμβάνει μια σειρά βημάτων που απαιτούν επαλήθευση και έλεγχο ταυτότητας πριν από τη δημιουργία της ασφαλούς σύνδεσης. Ουσιαστικά, η χειραψία δημιουργεί ένα ασφαλές κανάλι επικοινωνίας μέσω του διαδικτύου.

Η χειραψία TLS 1.2 περιλαμβάνει πολλαπλές επικοινωνίες μεταξύ του Client και του Server πριν από την οριστικοποίηση μιας ασφαλούς σύνδεσης, επιβάλλοντας περιττή απόδοση και επιβάρυνση δικτύου. Το TLS 1.3 μειώνει τον αριθμό των επικοινωνιών κατά τη διάρκεια της χειραψίας. Η πιο σύντομη χειραψία έχει ως αποτέλεσμα πιο γρήγορες ασφαλείς συνδέσεις. Βελτιώνει επίσης την απόδοση του HTTPS μειώνοντας τους χρόνους φόρτωσης σελίδας σε κινητές συσκευές, γεγονός που μειώνει την καθυστέρηση και βελτιώνει την εμπειρία του χρήστη.

**Μυστικότητα**

Η κρυπτογράφηση είναι ένα χαρακτηριστικό του SSL/TLS που εμποδίζει έναν εισβολέα να μπορεί να αποκρυπτογραφήσει τα δεδομένα από περιόδους σύνδεσης, εάν είναι σε θέση να κλέψει τα ιδιωτικά κλειδιά που χρησιμοποιούνται σε μια συγκεκριμένη περίοδο λειτουργίας. Το απόρρητο προώθησης χρησιμοποιεί μοναδικά κλειδιά περιόδου λειτουργίας που δημιουργούνται συχνά και αυτόματα. Εμποδίζει έναν εισβολέα να πάρει το κλειδί της συνεδρίας αποκρυπτογραφώντας τα δεδομένα που αποστέλλονται κατά τη χειραψία.

**Ασφάλεια**

Η έκδοση TLS 1.3 είναι πιο ασφαλής από τις προηγούμενες εκδόσεις του πρωτοκόλλου. Για την ασφάλεια των δεδομένων που μεταφέρονται μέσω του Διαδικτύου, το TLS/SSL χρησιμοποιεί μία ή περισσότερες σουίτες κρυπτογράφησης. Μια σουίτα κρυπτογράφησης είναι ένας συνδυασμός αλγορίθμων κωδικού ελέγχου ταυτότητας, κρυπτογράφησης και ελέγχου ταυτότητας μηνυμάτων. Χρησιμοποιούνται κατά τη

διαπραγμάτευση των ρυθμίσεων ασφαλείας για μια σύνδεση TLS/SSL καθώς και για τη μεταφορά δεδομένων.

Ως μέρος της χειραψίας SSL/TLS, ο Server και ο Client συμφωνούν σχετικά με τη σουίτα κρυπτογράφησης που θα χρησιμοποιηθεί για κρυπτογραφημένη επικοινωνία. Το TLS 1.3 υποστηρίζει σουίτες κρυπτογράφησης που δεν περιλαμβάνουν αλγόριθμους ανταλλαγής κλειδιών και υπογραφών. Η έκδοση 1.2 του TLS χρησιμοποιεί κρυπτογράφηση με ευπάθειες. Οι ακόλουθες μη ασφαλείς λειτουργίες καταργήθηκαν από το TLS 1.3:

- SHA-1 (Secure Hash Algorithm 1)
- RC4 (Rivest Cipher 4)
- DES (Data Encryption Standard)
- 3DES
- AES-CBC (Advanced Encryption Standard - Cipher Block Chaining)
- MD5 (message-digest algorithm)

### 3.3 Κρυπτογραφικές σουίτες

Η ασφάλεια οποιασδήποτε σύνδεσης με SSL/TLS εξαρτάται σε μεγάλο βαθμό από την επιλογή αλγορίθμων κρυπτογράφησης από την πλευρά του client και του server. Το σύνολο των αλγορίθμων κρυπτογράφησης ονομάζεται κρυπτογραφική σουίτα (cipher suite). Το όνομα αυτού του συνόλου είναι αντιπροσωπευτικό των αλγορίθμων που το αποτελούν. Για να ξεκινήσει μια σύνδεση HTTPS, τα δύο μέρη (ο Server και ο Client) εκτελούν μια χειραψία SSL. Κατά τη διαδικασία της χειραψίας τα δύο μέρη συμφωνούν σε μια αμοιβαία σουίτα κρυπτογράφησης. Στη συνέχεια, η σουίτα κρυπτογράφησης χρησιμοποιείται για τη διαπραγμάτευση μιας ασφαλούς σύνδεσης HTTPS.

Οι αλγόριθμοι που συνθέτουν μια τυπική σουίτα κρυπτογράφησης είναι οι ακόλουθοι:

- **Αλγόριθμος ανταλλαγής κλειδιών:** Υπαγορεύει τον τρόπο με τον οποίο θα ανταλλάσσονται τα συμμετρικά κλειδιά [RSA (Rivest–Shamir–Adleman), DH (Diffie–Hellman), ECDH (Elliptic-curve Diffie–Hellman), ECDHE (Elliptic Curve Diffie-Hellman Ephemeral)].
- **Αλγόριθμος ελέγχου ταυτότητας:** Υπαγορεύει τον τρόπο με τον οποίο θα πραγματοποιηθεί ο έλεγχος ταυτότητας του server και εφόσον χρειάζεται ο έλεγχος ταυτότητας του client [RSA, DSA (Digital Signature Algorithm), ECDSA (Elliptic Curve Digital Signature Algorithm)].
- **Αλγόριθμος μαζικής κρυπτογράφησης:** Υπαγορεύει ποιος αλγόριθμος συμμετρικού κλειδιού θα χρησιμοποιηθεί για την κρυπτογράφηση των πραγματικών δεδομένων (AES).
- **Αλγόριθμος κωδικού ελέγχου ταυτότητας μηνυμάτων (MAC):** Υπαγορεύει τη μέθοδο που θα χρησιμοποιήσει η σύνδεση για τη διενέργεια ελέγχων ακεραιότητας δεδομένων (SHA-2, SHA-3).

Ένα παράδειγμα μιας τυπικής σουίτας κρυπτογράφησης του TLS 1.2 είναι το εξής:

TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384

Ξεκινώντας από τα αριστερά προς τα δεξιά, ο ECDHE καθορίζει ότι κατά τη διάρκεια της χειραψίας τα κλειδιά θα ανταλλάσσονται μέσω του αλγορίθμου ECDHE. Ο αλγόριθμος ψηφιακής υπογραφής ECDSA ή Elliptic Curve είναι ο αλγόριθμος ελέγχου ταυτότητας. Ο AES128-GCM είναι ο αλγόριθμος μαζικής κρυπτογράφησης. Τέλος, ο SHA-256 είναι ο αλγόριθμος κατακερματισμού.

Το πρωτόκολλο TLS 1.2 υποστηρίζει 37 διαφορετικές σουίτες κρυπτογράφησης. Ενδεδειγμένες σουίτες κρυπτογράφησης θεωρούνται οι εξής [23]:

- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256
- TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305
- TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
- TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305

Με την εισαγωγή του TLS 1.3, άλλαξαν πολλά πράγματα όσον αφορά τη βελτίωση και την ασφάλεια του πρωτοκόλλου. Οι μη ασφαλείς αλγόριθμοι που καταργήθηκαν είναι οι εξής:

- RC4
- DSA
- MD5
- SHA-1
- Weak Elliptic Curves
- RSA Key Exchange
- Static Diffie-Hellman (DH, ECDH)
- Block ciphers (CBC)
- Non-AEAD ciphers

Επιπλέον, οι σουίτες κρυπτογράφησης που υποστηρίζει το TLS 1.3 είναι πλέον πολύ μικρότερες από τις αντίστοιχες σουίτες του TLS 1.2. Στην περίπτωση του TLS 1.3 δεν αναφέρεται ο τύπος του πιστοποιητικού (RSA ή ECDSA) και ο μηχανισμός ανταλλαγής κλειδιών (DHE ή ECDHE). Ως εκ τούτου, ο αριθμός των διαπραγματεύσεων που απαιτούνται για τον προσδιορισμό των παραμέτρων κρυπτογράφησης έχει μειωθεί.

Ένα παράδειγμα μιας τυπικής σουίτας κρυπτογράφησης του TLS 1.3 είναι το εξής:

TLS_AES_128_GCM_SHA256

Οι υποστηριζόμενες σουίτες κρυπτογράφησης στο TLS 1.3 έχουν πλέον μειωθεί σε μόλις πέντε και είναι οι εξής:

- TLS_AES_256_GCM_SHA384
- TLS_CHACHA20_POLY1305_SHA256
- TLS_AES_128_GCM_SHA256
- TLS_AES_128_CCM_8_SHA256
- TLS_AES_128_CCM_SHA256

### 3.4 Γνωστές επιθέσεις στο TLS

Τα τελευταία χρόνια, σημειώνονται αρκετές σοβαρές επιθέσεις στο TLS, οι οποίες στοχεύουν είτε στους αλγόριθμους κρυπτογράφησης που χρησιμοποιεί είτε στην ίδια τη λειτουργία του πρωτοκόλλου. Όπως αναφέρθηκε παραπάνω το πρωτόκολλο αποτελείται από δύο φάσεις. Η πρώτη είναι η φάση της χειραψίας (Handshake Protocol), όπου γίνεται ο έλεγχος ταυτότητας και καθορίζονται οι παράμετροι της ασφαλείας αλλά και η κατάσταση της επικοινωνίας. Η δεύτερη φάση είναι η φάση της εγγραφής (Record Protocol), όπου ανταλλάσσονται κρυπτογραφημένα δεδομένα. Οι σημαντικότερες επιθέσεις που έχουν καταγραφεί για το TLS είναι οι εξής [7] [8]:

#### 3.4.1 SSL Stripping

Σε αυτή την επίθεση ο κακόβουλος χρήστης λειτουργεί ως man-in-the-middle και υποβαθμίζει τις συνδέσεις HTTPS σε HTTP αφαιρώντας το επιπλέον επίπεδο που κρυπτογραφεί τα δεδομένα έτσι ώστε εάν το θύμα ζητήσει ιστότοπους HTTPS, τα δεδομένα θα σταλούν σε απλό κείμενο, ώστε να καταστούν αναγνώσιμα από τον επιτιθέμενο [9].

#### 3.4.2 Επίθεση STARTTLS Command Injection

Το STARTTLS είναι μια επέκταση στα πρωτόκολλα απλής επικοινωνίας (plaintext) που προσφέρει έναν τρόπο αναβάθμισης μιας απλής σύνδεσης σε κρυπτογραφημένη (TLS ή SSL) αντί της χρήσης ξεχωριστής θύρας για κρυπτογραφημένη επικοινωνία. Ορισμένες υλοποιήσεις του STARTTLS περιέχουν μια ευπάθεια που θα μπορούσε να επιτρέψει σε έναν απομακρυσμένο κακόβουλο χρήστη χωρίς έλεγχο ταυτότητας να εισάγει εντολές

κατά τη φάση του πρωτοκόλλου απλού κειμένου, οι οποίες θα εκτελεστούν κατά τη φάση του πρωτοκόλλου κρυπτογραφημένου κειμένου [10].

### 3.4.3 BEAST

Το Browser Exploit Against SSL/TLS (BEAST) είναι μια επίθεση κατά των τρωτών σημείων δικτύου στο TLS 1.0 και σε παλαιότερα πρωτόκολλα (SSL). Η επίθεση εκτελέστηκε για πρώτη φορά το 2011 από τους ερευνητές ασφαλείας Thai Duong και Juliano Rizzo, αλλά η θεωρητική ευπάθεια ανακαλύφθηκε το 2002 από τον Phillip Rogaway. Το TLS αλλά και το SSL είναι κρυπτογραφικά πρωτόκολλα που επιτρέπουν τη χρήση διαφορετικής σουίτας κρυπτογράφησης για τη κρυπτογράφηση της επικοινωνίας μεταξύ του Client και του Server. Αυτό καθιστά αδύνατο για κάποιον να ακούσει την επικοινωνία και να κλέψει εμπιστευτικά δεδομένα. Οι επιτιθέμενοι ωστόσο μπορεί να έχουν τη δυνατότητα να υποκλέψουν αυτή την επικοινωνία χρησιμοποιώντας τεχνικές επίθεσης "man-in-the-middle". Αυτό ακριβώς συμβαίνει και με την επίθεση BEAST, όπου ερευνητές διαπίστωσαν ότι η κρυπτογράφηση του TLS 1.0 (και παλαιότερα) μπορεί να σπάσει γρήγορα, δίνοντας στον επιτιθέμενο την ευκαιρία να ακούσει τη συνομιλία [11].

### 3.4.4 Επιθέσεις Padding Oracle

Το Cipher Block Chaining (CBC) είναι ένας τρόπος λειτουργίας στον οποίο μια ακολουθία από bits είναι κρυπτογραφημένη ως ενιαία μονάδα ή μπλοκ, με ένα κλειδί κρυπτογράφησης που εφαρμόζεται σε ολόκληρο το μπλοκ. Το χρησιμοποιεί αυτό που είναι γνωστό ως διάνυσμα αρχικοποίησης (Initialization Vector - IV) συγκεκριμένου μήκους. Το Padding Oracle Attack εκμεταλλεύεται την ανάγκη κάθε μήνυμα να έχει συγκεκριμένο μήκος συνόλου. Εάν το αρχικό μήνυμα δεν είναι αρκετά μεγάλο, τότε πρέπει να προσθέσουμε padding για να λειτουργήσει η κρυπτογράφηση CBC. Επειδή υπάρχει το padding, ένας εισβολέας μπορεί να αφαιρέσει πληροφορίες στο κρυπτογραφημένο κείμενο, ένα byte τη φορά, αναλύοντας τα μηνύματα σφάλματος του παραλήπτη για τον αποστολέα, τον χρόνο απόκρισης και τη γενική συμπεριφορά [12].

### 3.4.5 Επιθέσεις στον RC4

Αυτού του τύπου οι επιθέσεις κατά του TLS επιτρέπουν στον επιτιθέμενο να ανακτήσει περιορισμένο αριθμό απλού κειμένου από μια σύνδεση TLS όταν χρησιμοποιείται κρυπτογράφηση RC4. Οι επιθέσεις προκύπτουν από στατιστικά ελαττώματα στη ροή κλειδιών που δημιουργούνται από τον αλγόριθμο RC4, τα οποία γίνονται εμφανή στα κρυπτογραφημένα κείμενα TLS όταν το ίδιο απλό κείμενο κρυπτογραφείται επανειλημμένα [13].

### 3.4.6 Επιθέσεις CRIME, TIME, και BREACH

Η επίθεση Compression Ratio Info-leak Made Easy (CRIME) μπορεί να εκτελεστεί έναντι των πρωτοκόλλων SSL/TLS και εκτελείται με παραβίαση των cookies της συνόδου ενός

χρήστη, ενώ εξακολουθεί να είναι αυθεντικοποιημένος σε έναν ιστότοπο. Αυτό είναι δυνατό μόνο εάν τα πρωτόκολλα έχουν ενεργοποιήσει ορισμένους τύπους μεθόδων συμπίεσης δεδομένων. Ενώ η συμπίεση μπορεί να είναι αρκετά βολική γενικά, ενέχει τον κίνδυνο ακούσιας αποκάλυψης ενδείξεων σχετικά με το περιεχόμενο της κρυπτογράφησης. Το Timing Info-leak Made Easy (TIME) είναι μια επιλεγμένη επίθεση απλού κειμένου στις αποκρίσεις HTTP. Το μοντέλο επίθεσης του CRIME δίνει πληροφορίες για το απλό κείμενο με βάση το μήκος των κρυπτογραφημένων και συμπιεσμένων δεδομένων. Το TIME χρησιμοποιεί αυτό το μοντέλο και πληροφορίες χρονισμού για να αναλύσει το μέγεθος του συμπιεσμένου ωφέλιμου φορτίου. Όπως η επίθεση CRIME, η επίθεση Browser Reconnaissance and Exfiltration via Adaptive Compression of Hypertext (BREACH) εκμεταλλεύεται τον συνδυασμό συμπίεσης και κρυπτογράφησης που χρησιμοποιείται για την αλληλεπίδραση μεταξύ του client και του web server [14].

### 3.4.7 Επιθέσεις σχετιζόμενες με τον RSA και τα πιστοποιητικά

Η επίθεση Return Of Bleichenbacher’s Oracle Threat (ROBOT) εκμεταλλεύεται μια παλιά ευπάθεια που ανακαλύφθηκε από τον Daniel Bleichenbacher το 1998. Η χρήση αυτής της επίθεσης παραβιάζει πλήρως την εμπιστευτικότητα του SSL/TLS όταν χρησιμοποιείται με κρυπτογράφηση RSA. Επιτρέπει στον επιτιθέμενο να εκτελεί λειτουργίες αποκρυπτογράφησης και υπογραφής RSA με το ιδιωτικό κλειδί ενός διακομιστή SSL/TLS. Ως αποτέλεσμα, είναι δυνατό να καταγράψει την κίνηση SSL/TLS και να την αποκρυπτογραφήσει αργότερα [15].

## 3.5 Το HTTPS

Το HTTPS είναι η ασφαλής έκδοση του HTTP, το οποίο είναι το κύριο πρωτόκολλο που χρησιμοποιείται για την αποστολή δεδομένων μεταξύ ενός web server και ενός ιστότοπου. Το HTTPS είναι κρυπτογραφημένο προκειμένου να αυξηθεί η ασφάλεια της μεταφοράς δεδομένων. Αυτό είναι ιδιαίτερα σημαντικό όταν οι χρήστες μεταδίδουν ευαίσθητα δεδομένα. Οποιοσδήποτε ιστότοπος και ειδικά εκείνοι που απαιτούν διαπιστευτήρια σύνδεσης, θα πρέπει να χρησιμοποιεί HTTPS. Στα σύγχρονα προγράμματα περιήγησης ιστού όπως το Chrome, οι ιστότοποι που δεν χρησιμοποιούν HTTPS επισημαίνονται ως μη ασφαλείς [4].

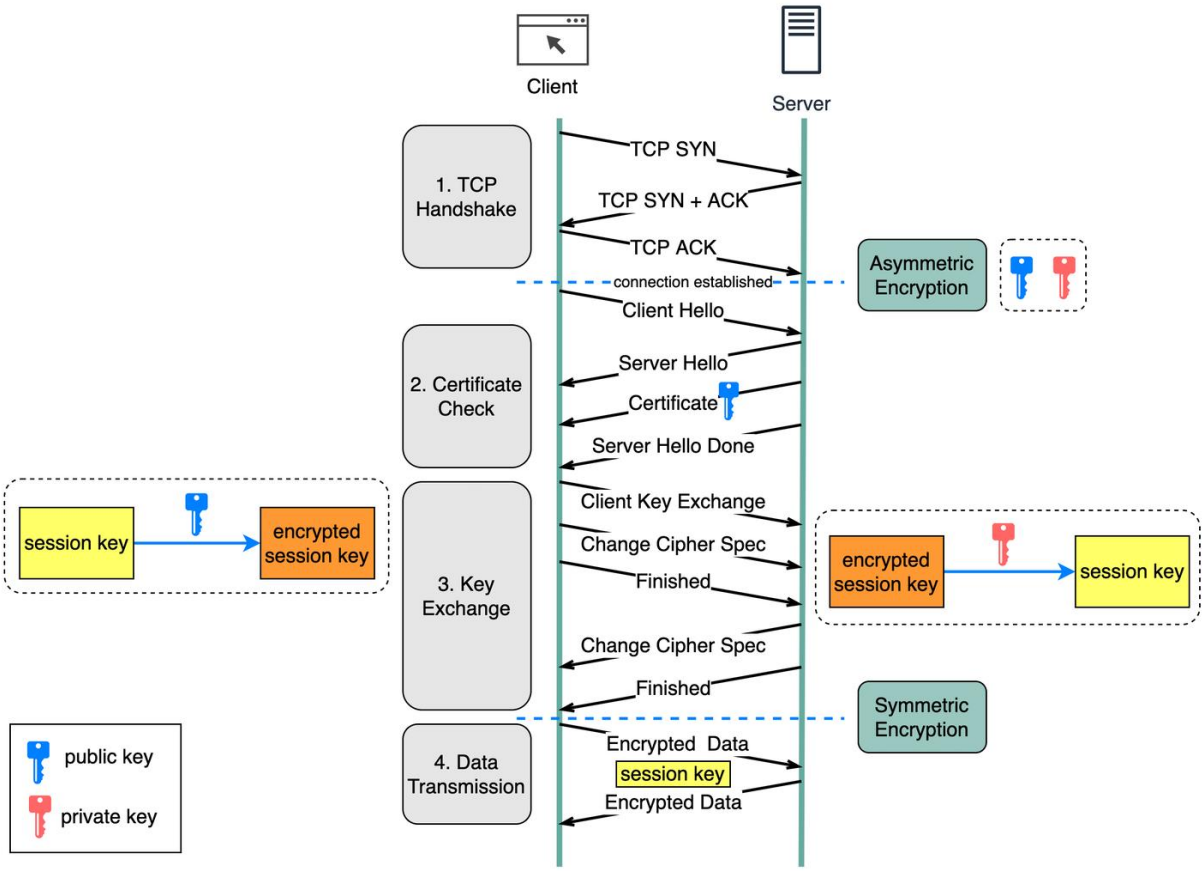
Το HTTPS χρησιμοποιεί το πρωτόκολλο TLS, το οποίο παλαιότερα ήταν γνωστό ως Secure Sockets Layer (SSL). Με αυτό το πρωτόκολλο κρυπτογραφείται η επικοινωνία με τη χρήση της υποδομής ασύμμετρου δημόσιου κλειδιού. Για την κρυπτογράφηση χρησιμοποιούνται δύο είδη κλειδιών:

- Το ιδιωτικό κλειδί

Αυτό το κλειδί ελέγχεται από τον κάτοχο ενός ιστότοπου και διατηρείται ιδιωτικό. Βρίσκεται αποθηκευμένο σε έναν web server και χρησιμοποιείται για την αποκρυπτογράφηση πληροφοριών που κρυπτογραφούνται από το δημόσιο κλειδί.

- Το δημόσιο κλειδί

Αυτό το κλειδί είναι διαθέσιμο σε όλους όσους θέλουν να αλληλεπιδράσουν με τον server με ασφαλή τρόπο. Οι πληροφορίες που είναι κρυπτογραφημένες από το δημόσιο κλειδί μπορούν να αποκρυπτογραφηθούν μόνο από το ιδιωτικό κλειδί.




**Εικόνα 5: Η λειτουργία του HTTPS**

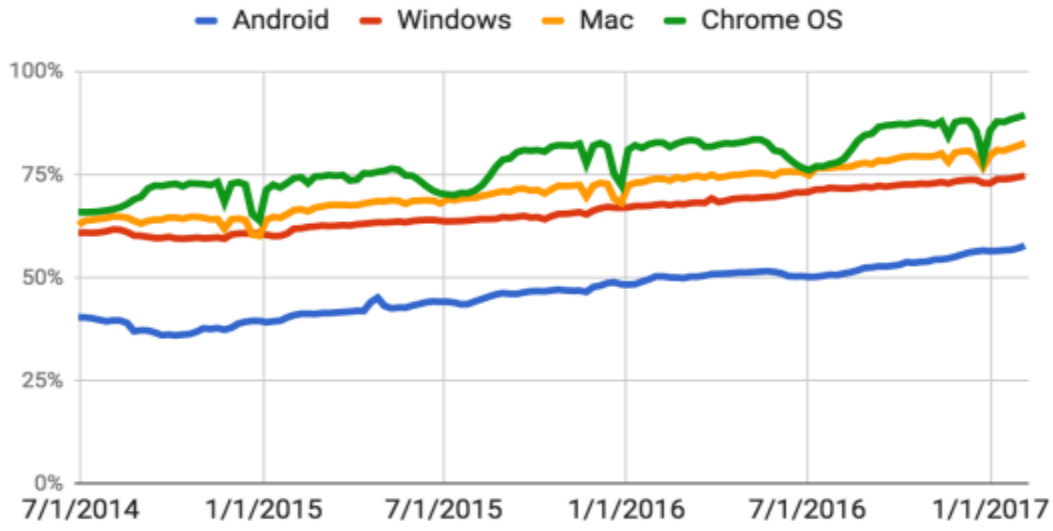
# 4. ΣΧΕΤΙΚΕΣ ΜΕΛΕΤΕΣ

Σε αυτό το κεφάλαιο παρουσιάζονται προηγούμενες μελέτες που έγιναν σχετικά με τον ρυθμό υιοθέτησης του HTTPS γενικά στο παγκόσμιο ιστό αλλά και ειδικά σε ελληνικούς ιστότοπους.

## 4.1 Η υιοθέτηση του HTTPS στο παγκόσμιο ιστό

Το 2017 οι Adrienne Porter Felt, Richard Barnes, April King, Chris Palmer, Chris Bentzel και Parisa Tabriz διεξήγαγαν μελέτη ως προς το βαθμό υιοθέτησης του πρωτοκόλλου HTTPS από τον παγκόσμιο ιστό μέσα στο διάστημα 2016-2017 [16]. Τα ποσοστά υιοθέτησης εξετάστηκαν από πολλές οπτικές γωνίες και αφορούν τόσο την πλευρά των clients όσο και των servers.

Από την έρευνα διαπιστώθηκε ότι η υιοθέτηση του HTTPS αυξήθηκε σημαντικά κατά τα τελευταία χρόνια. Οι περιηγήσεις μέσω επιτραπέζιων υπολογιστών γίνονται ως επί το πλείστον μέσω του HTTPS και τα ποσοστά αυτά αυξήθηκαν περίπου κατά 10 μονάδες μόνο το 2016. Ο αριθμός των κορυφαίων ιστοσελίδων που χρησιμοποιούν HTTPS από προεπιλογή διπλασιάστηκε μεταξύ των αρχών του 2016 και των αρχών του 2017. Ωστόσο, κατά την περίοδο της έρευνας βρέθηκαν οι μισοί από τους κορυφαίους ιστότοπους να εξακολουθούν να χρησιμοποιούν HTTP από προεπιλογή, και οι περισσότεροι servers να μην υποστηρίζουν καθόλου το HTTPS. Η περιήγηση στο Web για κινητά βρέθηκε να υστερεί σε σχέση με τους υπολογιστές και οι χώρες της Ανατολικής Ασίας παρουσίασαν σημαντικά χαμηλότερες τιμές σε σχέση με τα ποσοστά χρήσης του HTTPS από τον υπόλοιπο κόσμο.




**Εικόνα 6: Μετρήσεις για το HTTPS από το 2014 μέχρι το 2017 στον Chrome**

## 4.2 Η υιοθέτηση του HTTPS από ελληνικές ιστοσελίδες

Το 2018 οι Κοντογεώργης, Λιμνιώτης και Καντζάβελου διεξήγαγαν μελέτη και αξιολόγησαν για πρώτη φορά την υιοθέτηση του HTTPS από ιστοτόπους στην Ελλάδα [17]. Στα πλαίσια της μελέτης εξετάστηκαν συνολικά 241 ιστοσελίδες και χρησιμοποιήθηκαν δύο πολύ γνωστά εργαλεία το Qualy's SSL test και ο SSL/TLS server test από την εταιρεία High-Tech Bridge. Για τους σκοπούς της έρευνας οι ιστοσελίδες κατηγοριοποιήθηκαν σε i) Ηλεκτρονικά καταστήματα, ii) Ενημερωτικού χαρακτήρα, iii) Πάροχοι τηλεπικοινωνιών, iv) Εκπαιδευτικές, v) Οικονομικού χαρακτήρα (συμπεριλαμβανομένου και ιστοσελίδες τραπεζών), vi) Άλλες εταιρείες, vii) Δημοσίου τομέα. Σε δεύτερο επίπεδο εξετάστηκε μέσω ερωτηματολογίων το επίπεδο γνώσεων των χρηστών σχετικά με τη διαφορά του HTTP με το HTTPS καθώς και η επίγνωση των ελέγχων που θα πρέπει να κάνουν, από πλευράς ασφάλειας, πριν επισκεφθούν μία ιστοσελίδα.

Η παραπάνω μελέτη εστίασε στην βαθμολόγηση από τα εργαλεία των ιστοσελίδων, η οποία γίνεται σύμφωνα με την έκδοση του TLS που χρησιμοποιείται. Πέραν τούτου εξετάστηκαν και οι ευπάθειες που ενδεχομένως έχουν που προκύπτουν από την έκδοση του TLS που χρησιμοποιείται.

Σε σχέση με τα ηλεκτρονικά καταστήματα, από τις 58 ιστοσελίδες που ελέγχθηκαν σχεδόν όλες χρησιμοποιούν HTTPS πλην μιας μόνο ιστοσελίδας. Το 53% περίπου βαθμολογήθηκε από τα εργαλεία με την υψηλότερη βαθμολογία (A) ενώ μόλις το 10% βαθμολογήθηκε με F. Στις ιστοσελίδες ενημερωτικού χαρακτήρα από τις 33 που ελέγχθηκαν το 81.8% χρησιμοποιεί HTTPS. Σύμφωνα με τον έλεγχο των εργαλείων το 66.6% έλαβε την ανώτερη βαθμολογία ενώ το 14% βαθμολογήθηκε με F. Στις ιστοσελίδες τηλεπικοινωνιακού χαρακτήρα και οι 9 που εξετάστηκαν χρησιμοποιούν HTTPS. Όσον αφορά τη βαθμολογία των εργαλείων το 33.3% βαθμολογήθηκε με A ενώ το 22%, δηλαδή περίπου 2 στις 9 βαθμολογήθηκε με F. Στον τομέα της εκπαίδευσης από τις 33 ιστοσελίδες που ελέχθηκαν το 90% έκανε χρήση του HTTPS. Ωστόσο ακόμα και οι ιστοσελίδες που δεν υλοποιούσαν κάποιο πρωτόκολλο ασφαλείας είχαν διαδικασίες αυθεντικοποίησης χρηστών που απαιτούσαν την εισαγωγή διαπιστευτηρίων τους. Όσον αφορά τη συνολική βαθμολογία το 37% έλαβε την υψηλότερη βαθμολογία ενώ το 22.2% βαθμολογήθηκε με F. Στον οικονομικό τομέα το σύνολο των 21 ιστοσελίδων που εξετάστηκαν χρησιμοποιούν HTTPS. Στη βαθμολογία το 76% βαθμολογήθηκε με A ενώ μόλις το 5% με F. Σε άλλους οργανισμούς από τις 51 ιστοσελίδες που ελέγχθηκαν το 86.3% χρησιμοποιεί HTTPS. Ωστόσο αξίζει να σημειωθεί πως από τις υπόλοιπες ιστοσελίδες που χρησιμοποιούν HTTP οι 6 στις 7 δεν παρέχουν κάποια φόρμα αυθεντικοποίησης χρηστών. Στη συνολική βαθμολογία το 43% βαθμολογήθηκε με A ενώ το 18% με F. Τέλος στο δημόσιο τομέα από τις 39 ιστοσελίδες το 71.7% χρησιμοποιεί HTTPS. Ωστόσο μόνο 1 από τις υπόλοιπες παρέχει φόρμα αυθεντικοποίησης χρηστών χωρίς τη χρήση ασφαλούς πρωτοκόλλου επικοινωνίας. Στη τελική βαθμολογία το 46% έλαβε την υψηλότερη βαθμολογία ενώ το 25% την χαμηλότερη.

Τα τρωτά σημεία που εντοπίστηκαν παραπάνω δύναται να οδηγήσουν σε επιθέσεις κατά του TLS. Το μεγαλύτερο ποσοστό των ιστοτόπων του δημοσίου τομέα που εξετάστηκαν (35%), βρέθηκαν να είναι ευάλωτοι σε επιθέσεις στον RC4. Περίπου το 17% βρέθηκαν

να απειλούνται από επιθέσεις τύπου Poodle και να παρουσιάζουν αδυναμίες στον αλγόριθμο Diffie Hellman. Σε μικρότερο ποσοστό (10%) οι ιστότοποι βρέθηκαν ευάλωτοι σε επιθέσεις τύπου ROBOT και FREAK, ενώ ένας πολύ μικρός αριθμός, σε ποσοστό περίπου 7% φάνηκε να απειλείται από επιθέσεις DROWN. Οι τρωτότητες αυτές προέκυψαν από τη χρήση παλαιότερων εκδόσεων του TLS και κατ' επέκταση από τη χρήση παρωχημένων αλγορίθμων κρυπτογράφησης.

Σε σχέση με την ευαισθητοποίηση χρηστών ως προς την ασφαλή περιήγηση σε ιστοτόπους, μετά από ανάλυση 773 ερωτηματολογίων η έρευνα κατέληξε στο συμπέρασμα ότι 4 στους 10 χρήστες δεν γνωρίζουν τη διαφορά του HTTPS με το HTTP, ενώ 7 στους 10 χρήστες δεν έχουν ακούσει ποτέ για γνωστές επιθέσεις στο TLS.

# 5. ΕΛΕΓΧΟΣ ΤΩΝ ΙΣΤΟΣΕΛΙΔΩΝ

Σε αυτό το σημείο της εργασίας θα εξεταστεί η υιοθέτηση του HTTPS από ελληνικές ιστοσελίδες του δημόσιου τομέα. Λόγω του ότι πλέον η πλειοψηφία των ιστοσελίδων στο παγκόσμιο ιστό χρησιμοποιούν HTTPS αξίζει να μελετηθεί η έκδοση του πρωτοκόλλου TLS που χρησιμοποιείται.

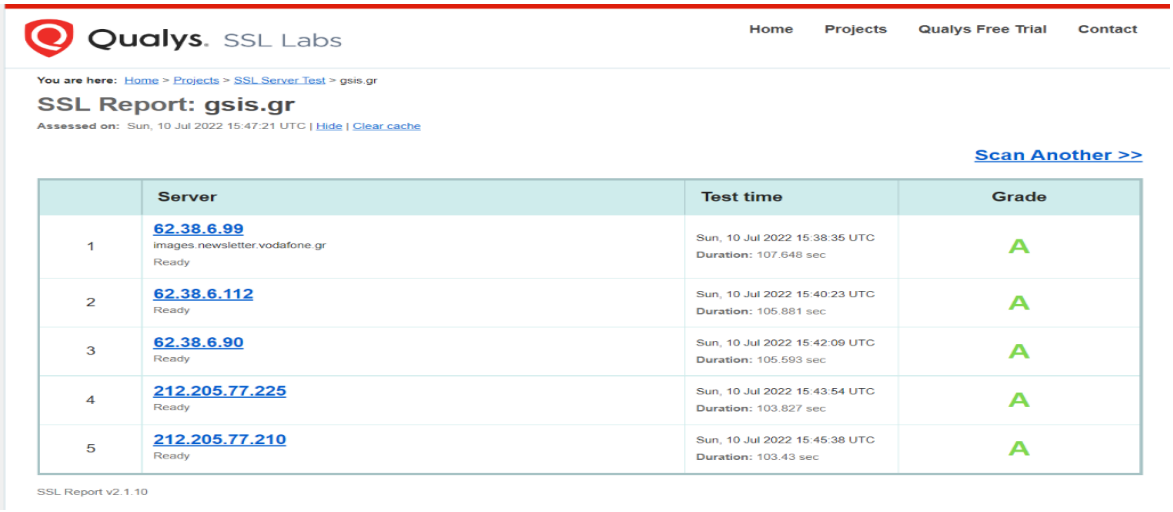
## 5.1 Μεθοδολογία

Για την ανάλυση εστιάσαμε στις 50 δημοφιλέστερες ιστοσελίδες του δημοσίου τομέα στην Ελλάδα. Οι ιστοσελίδες αντλήθηκαν από τον κατάλογο ελληνικών ιστοσελίδων που υπάρχει στο διαδίκτυο [18]. Ο έλεγχος πραγματοποιήθηκε από τον Ιούλιο του 2022 έως τον Οκτώβριο του 2022 και αντικατοπτρίζει την εικόνα των ιστοσελίδων για αυτή τη χρονική περίοδο.

Στόχος του ελέγχου ήταν η αποτύπωση της βαθμολογίας για κάθε ιστοσελίδα, εν συνεχεία η μελέτη της έκδοσης TLS που χρησιμοποιεί και κατ'επέκταση η αδυναμία που ενδεχομένως παρουσιάζει σε επιθέσεις που αναλύθηκαν παραπάνω. Στη συνέχεια της εργασίας θα αναλυθεί η ασφάλεια που παρέχεται στις κρατικές ιστοσελίδες σε συνάρτηση με τους κανόνες που θέτει ο ΓΚΠΔ σχετικά με την διασφάλιση των προσωπικών δεδομένων.

Για τον έλεγχο των ιστοσελίδων χρησιμοποιήθηκε το διαδικτυακό εργαλείο SSL Labs by Qualys, το οποίο είναι ένα από τα πιο δημοφιλή εργαλεία δοκιμών SSL τόσο για τον έλεγχο όλων των τρωτών σημείων αλλά και για τον έλεγχο εσφαλμένων ρυθμίσεων. Το εν λόγω εργαλείο ελέγχει:

- Τον εκδότη του πιστοποιητικού, την εγκυρότητα του και τον αλγόριθμο που χρησιμοποιείται για την υπογραφή του.
- Τις λεπτομέρειες του πρωτοκόλλου, τις σουίτες κρυπτογράφησης και προσομοίωση της χειραψίας.




**Εικόνα 7: Qualys SSL Report**

Ο έλεγχος του πιστοποιητικού SSL του ιστότοπου πραγματοποιείται σε πολλούς διακομιστές για να βεβαιωθεί ότι τα αποτελέσματα των δοκιμών είναι ακριβή. Στην παραπάνω εικόνα φαίνονται τα αποτελέσματα του ελέγχου.

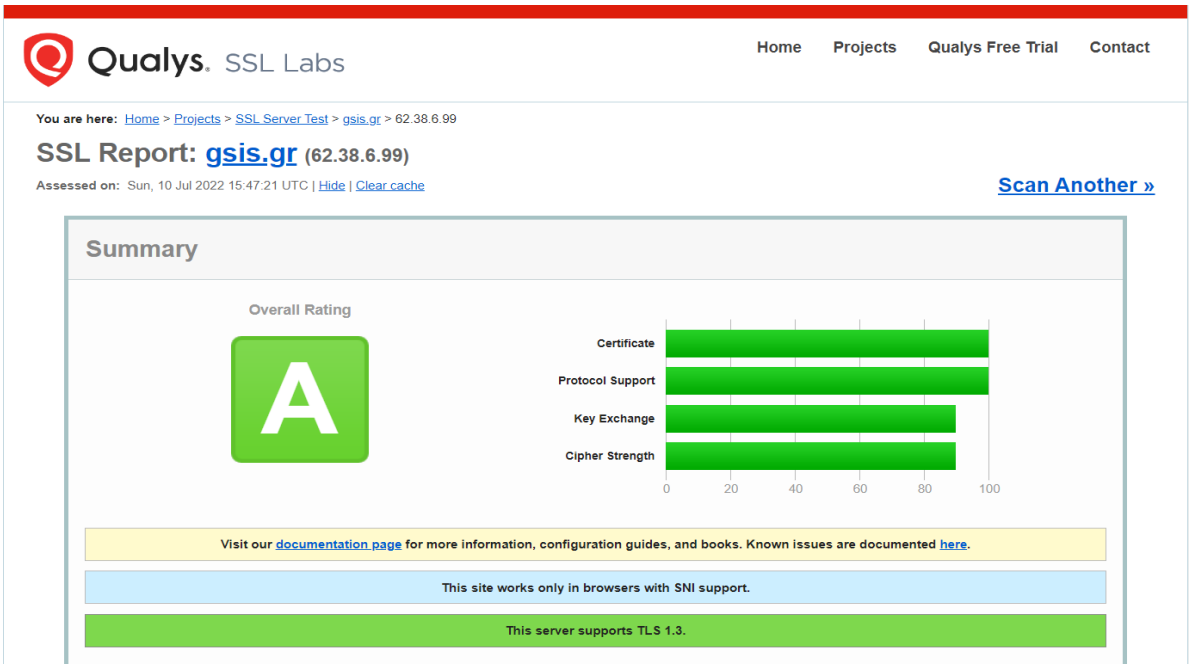
**Πίνακας 1: Κατάλογος Ιστοσελίδων Ελληνικού Δημόσιου Τομέα**

| A/A | Website | Description | Grade | TLS Version |
|---|---|---|---|---|
| 1 | Gsis.gr | Γενική Γραμματεία Πληροφοριακών Συστημάτων | A | TLS 1.3 |
| 2 | Aade.gr | Ανεξάρτητη Αρχή Δημοσίων Εσόδων | A | TLS 1.3 |
| 3 | Gov.gr | Ηλεκτρονική e-πλατφόρμα για το Δημόσιο | B | TLS 1.2 |
| 4 | Oaed.gr | Οργανισμού Απασχόλησης Εργατικού Δυναμικού | A | TLS 1.3 |
| 5 | Efka.gov.gr | Ηλεκτρονικός Εθνικός Φορέας Κοινωνικής Ασφάλισης | B | TLS 1.2 |
| 6 | Eopyy.gov.gr | Εθνικός Οργανισμός Παροχής Υπηρεσιών Υγείας | B | TLS 1.2 |
| 7 | Iep.edu.gr | Ινστιτούτο Εκπαιδευτικής Πολιτικής | B | TLS 1.3 |
| 8 | Diavgeia.gov.gr | Ιστοσελίδα Προγράμματος Δι@ύγεια | B | TLS 1.2 |
| 9 | Minedu.gov.gr | Ιστοσελίδα του Υπουργείου Παιδείας και Θρησκευμάτων | A | TLS 1.3 |
| 10 | Aftodioikisi.gr | Portal για τους ΟΤΑ και το Δημόσιο στην Ελλάδα | B | TLS 1.3 |
| 11 | Asep.gr | Ανώτατο Συμβούλιο Επιλογής Προσωπικού | B | TLS 1.2 |
| 12 | Ktimanet.gr | Ηλεκτρονικές Υπηρεσίες e - ΚΤΗΜΑΤΟΛΟΓΙΟ | B | TLS 1.3 |
| 13 | Mfa.gr | Ιστοσελίδα του Υπουργείου Εξωτερικών | A | TLS 1.3 |
| 14 | Elta.gr | Ιστοσελίδα των Ελληνικών Ταχυδρομείων | A | TLS 1.3 |
| 15 | Emvolio.gov.gr | Εμβολιασμός κατά της Covid-19 | A | TLS 1.3 |
| 16 | Web.tee.gr | Τεχνικό Επιμελητήριο Ελλάδος | B | TLS 1.2 |

| A/A | Website | Description | Grade | TLS Version |
|---|---|---|---|---|
| 17 | Et.gr | Εθνικό Τυπογραφείο | A | TLS 1.3 |
| 18 | Hcg.gr | Λιμενικό σώμα | A | TLS 1.3 |
| 19 | Eody.gov.gr | Εθνικός Οργανισμός Δημόσιας Υγείας | A | TLS 1.3 |
| 20 | Army.gr | Ιστοσελίδα του Γενικού Επιτελείου Στρατού | A | TLS 1.2 |
| 21 | Policenet.gr | Ειδησεογραφία, Νομοθεσία και εργαλεία για αστυνομικούς | B | TLS 1.3 |
| 22 | Grnet.gr | Εθνικό Δίκτυο Έρευνας και Τεχνολογίας | B | TLS 1.2 |
| 23 | Travel.gov.gr | Passenger Location Form | A | TLS 1.3 |
| 24 | Astynomia.gr | Ιστοσελίδα της Ελληνικής Αστυνομίας | A | TLS 1.3 |
| 25 | Emy.gr | Ιστοσελίδα της Εθνικής Μετεωρολογικής Υπηρεσίας | A | TLS 1.1 |
| 26 | Hcmr.gr | Ελληνικό Κέντρο Θαλάσσιων Ερευνών | B | TLS 1.1 |
| 27 | Ekt.gr | Ιστοσελίδα του Εθνικού Κέντρου Τεκμηρίωσης | A | TLS 1.3 |
| 28 | Moh.gov.gr | Υπουργείο Υγείας και Κοινωνικής Αλληλεγγύης | A | TLS 1.3 |
| 29 | Ktimatologio.gr | Εθνικό Κτηματολόγιο και Χαρτογράφηση Α.Ε | B | TLS 1.3 |
| 30 | Hellenicparliament.gr | Ιστοσελίδα της Βουλής των Ελλήνων | A | TLS 1.3 |
| 31 | Ypes.gr | Ιστοσελίδα του Υπουργείου Εσωτερικών | A | TLS 1.3 |
| 32 | Cityofathens.gr | Ιστοσελίδα του Δήμου Αθηναίων | A | TLS 1.3 |
| 33 | Opengov.gr | Υπουργείο Διοικητικής Μεταρρύθμισης & Ηλεκτρονικής Διακυβέρνησης | A | TLS 1.1 |
| 34 | Statistics.gr | Ιστοσελίδα της Ελληνικής Στατιστικής Αρχής | C | TLS 1.2 |

| A/A | Website | Description | Grade | TLS Version |
|---|---|---|---|---|
| 35 | Minagric.gr | Ιστοσελίδα του Υπουργείου Αγροτικής Ανάπτυξης και Τροφίμων | A | TLS 1.1 |
| 36 | Patt.gov.gr | Ιστοσελίδα της Περιφέρειας Αττικής | A | TLS 1.2 |
| 37 | Ypergasias.gov.gr | Ιστοσελίδα του Υπουργείου Εργασίας | A | TLS 1.3 |
| 38 | Minfin.gr | Ιστοσελίδα του Υπουργείου Οικονομικών | A | TLS 1.3 |
| 39 | Haf.gr | Ιστοσελίδα της Πολεμικής Αεροπορίας | A | TLS 1.3 |
| 40 | Eett.gr | Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων | B | TLS 1.2 |
| 41 | Efet.gr | Ενιαίος Φορέας Ελέγχου Τροφίμων | A | TLS 1.3 |
| 42 | Helexpo.gr | Διεθνής Έκθεση Θεσσαλονίκης | B | TLS 1.3 |
| 43 | Stratologia.gr | Ιστοσελίδα του Νομικού Σώματος Ενόπλων Δυνάμεων | B | TLS 1.3 |
| 44 | Geetha.mil.gr | Ιστοσελίδα του Γενικού Επιτελείου Εθνικής Άμυνας | A | TLS 1.3 |
| 45 | Hellenicnavy.gr | Ιστοσελίδα του Ελληνικού Πολεμικού Ναυτικού | B | TLS 1.3 |
| 46 | Visitgreece.gr | Ιστοσελίδα του Ελληνικού Οργανισμού Τουρισμού | A | TLS 1.3 |
| 47 | Mod.mil.gr | Ιστοσελίδα του Υπουργείου Εθνικής Άμυνας | A | TLS 1.3 |
| 48 | Odigostoupoliti.eu | Ιστοσελίδα Ενημέρωσης των Πολιτών | B | TLS 1.3 |
| 49 | E-katanalotis.gov.gr | Ιστοσελίδα της Γενικής Γραμματείας Εμπορίου και Προστασίας Καταναλωτή | B | TLS 1.3 |
| 50 | Businessportal.gr | Ιστοσελίδα του Υπουργείου Ανάπτυξης και Επενδύσεων | A | TLS 1.3 |

Τα αποτελέσματα των δοκιμών παρέχουν λεπτομερείς τεχνικές πληροφορίες και δύναται να χρησιμοποιηθούν από διαχειριστές συστημάτων προκειμένου να εντοπίσουν και να διορθώσουν τυχόν αδύναμες παραμέτρους.




**Εικόνα 8: Qualys SSL Summary**

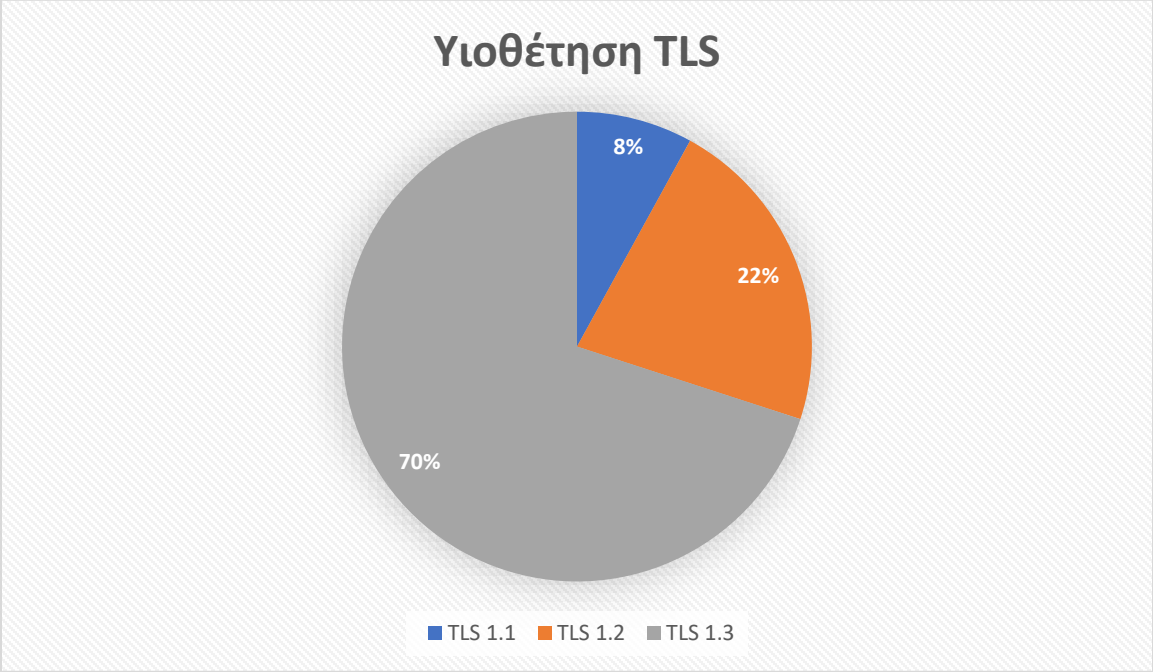
## 5.2 Αποτελέσματα Ελέγχων

Παρακάτω φαίνονται τα αποτελέσματα των ελέγχων:

Από το σύνολο των 50 κυβερνητικών ιστοσελίδων που εξετάστηκαν 4 μόνο από αυτές χρησιμοποιούν μη ασφαλή σύνδεση με HTTP. Από αυτές τις 4 ιστοσελίδες οι 2 είναι απλά ενημερωτικού χαρακτήρα, χωρίς να περιέχουν κάποια φόρμα συμπλήρωσης στοιχείων πολιτών (emy.gr, opengov.gr). Οι υπόλοιπες 2 (minagric.gr, army.gr) περιέχουν φόρμες συμπλήρωσης στοιχείων χωρίς να χρησιμοποιούν HTTPS, ωστόσο η ιστοσελίδα army.gr μεταφέρει το χρήστη σε ασφαλές περιβάλλον κατά τη συμπλήρωση προσωπικών στοιχείων (HTTPS). Σε σχέση με προηγούμενη έρευνα, που διεξήχθη το 2018 [17], όπου το 30% των κυβερνητικών ιστοσελίδων που εξετάστηκαν χρησιμοποιούσαν HTTP, φαίνεται πως σήμερα τα αποτελέσματα παρουσιάζουν βελτίωση με μόλις το 8% των κυβερνητικών ιστοσελίδων να χρησιμοποιούν το μη ασφαλές HTTP.

Όσον αφορά τη χρήση του πρωτοκόλλου TLS, το 22% χρησιμοποιεί TLS 1.2, το 70% TLS 1.3 και μόλις το 8% TLS 1.1. Παρατηρήθηκε ότι πολλές ιστοσελίδες ενώ χρησιμοποιούν τη τελευταία έκδοση του TLS έχουν ενεργοποιημένες και προηγούμενες εκδόσεις, γεγονός που επηρεάζει τη βαθμολογία τους από το εργαλείο SSL Labs by Qualys. Στη χρήση των πρωτοκόλλων φαίνεται πως δεν υπάρχει χρυσή τομή λόγω της ποικιλομορφίας των πελατών των ιστοτόπων. Αν και ιδανικό θα ήταν να έχει

απενεργοποιηθεί το HTTP καθώς και όλες οι εκδόσεις του TLS πέραν του TLS 1.3, αυτό θα σήμαινε πως πολλοί χρήστες δεν θα μπορούσαν να συνδεθούν.




**Εικόνα 9: Αξιολόγηση του TLS σε Ελληνικές Κυβερνητικές Ιστοσελίδες**

Σύμφωνα λοιπόν με το εργαλείο SSL Labs by Qualys, το 58% των ιστοσελίδων έλαβε την υψηλότερη βαθμολογία από A- μέχρι A+, το 40% έλαβε βαθμολογία C, ενώ η χαμηλότερη βαθμολογία που καταγράφηκε ήταν F, σε ποσοστό 2%.

Η διαδικασία βαθμολόγησης από το συγκεκριμένο εργαλείο αποτελείται από τέσσερα βήματα [27]:

1. Αρχικά εξετάζεται το πιστοποιητικό για να επαληθευτεί ότι είναι έγκυρο και αξιόπιστο.

2. Έπειτα ελέγχεται η διαμόρφωση του διακομιστή σε τρεις κατηγορίες:

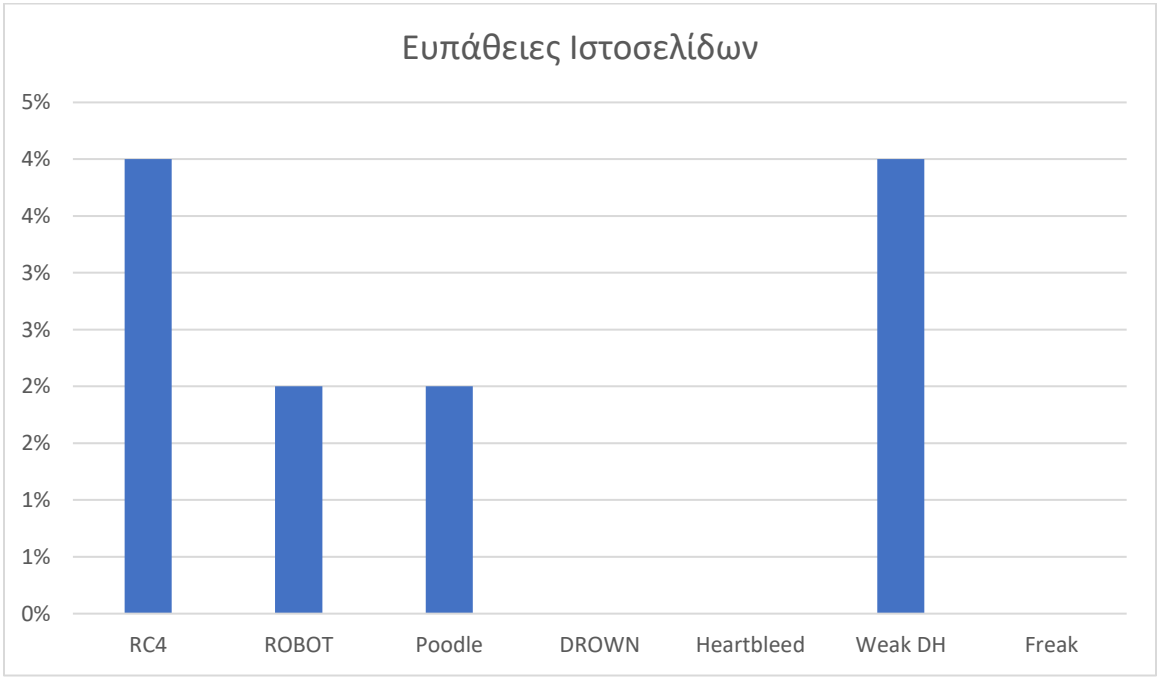
   - Υποστήριξη πρωτοκόλλου
   - Υποστήριξη ανταλλαγής κλειδιών
   - Υποστήριξη κρυπτογράφησης

3. Οι βαθμολογίες αυτής της κατηγορίας συνδυάζονται σε μια συνολική βαθμολογία (που εκφράζεται ως αριθμός μεταξύ 0 και 100).

4. Στη συνέχεια εφαρμόζεται μια σειρά κανόνων για να χειριστούν ορισμένες πτυχές της διαμόρφωσης διακομιστή που δεν μπορούν να εκφραστούν μέσω αριθμητικής βαθμολόγησης. Οι περισσότεροι κανόνες θα μειώσουν τον βαθμό (σε A-, B, C, D, E ή F)

εάν συναντήσουν ένα ανεπιθύμητο χαρακτηριστικό. Ορισμένοι κανόνες θα αυξήσουν τον βαθμό (σε A+), για να ανταμείψουν εξαιρετικές διαμορφώσεις.

Όσον αφορά τις επιθέσεις στο πρωτόκολλο TLS στις οποίες βρέθηκαν ευάλωτες οι ιστοσελίδες, παρατηρήθηκε αισθητή μείωση του ποσοστού σε σχέση με προηγούμενη έρευνα. Αυτό οφείλεται στην αναβάθμιση των εκδόσεων του TLS που χρησιμοποιούν πλέον οι ιστοσελίδες του ελληνικού δημόσιου τομέα σε σχέση με προηγούμενα έτη, γεγονός που αποτυπώνεται και στα αποτελέσματα που αναλύθηκαν παραπάνω. Οι τύποι επιθέσεων που μελετήθηκαν ήταν: επιθέσεις στον RC4, ROBOT, Poodle, DROWN, Heartbleed, Weak DH και Freak. Ένα πολύ μικρό ποσοστό των ιστοσελίδων (4%) βρέθηκαν να χρησιμοποιούν μη ισχυρό αλγόριθμο Diffie Hellman καθώς επίσης και τον μη ασφαλή αλγόριθμο RC4. Αυτές οι ιστοσελίδες χρησιμοποιούσαν παλαιότερες εκδόσεις του TLS, γεγονός που τις κατέστησε ευάλωτες στους αναφερόμενους τύπους επιθέσεων. Ένα επίσης χαμηλό ποσοστό ιστοσελίδων (2%) βρέθηκε ευάλωτο σε επιθέσεις ROBOT και Poodle, γεγονός που πάλι οφείλεται σε χρήση παρωχημένων εκδόσεων του πρωτοκόλλου TLS αλλά και του μη ασφαλούς πρωτοκόλλου SSL. Σε αντίθεση με προηγούμενη έρευνα το ποσοστό ευπάθειας σε επιθέσεις DROWN ήταν μηδενικό, ενώ για τις επιθέσεις Heartbleed και Freak τα ποσοστά παραμένουν ίδια με τα προηγούμενα έτη.




**Εικόνα 10: Επιθέσεις στο TLS σε ιστοσελίδες του ελληνικού δημόσιου τομέα**

# 6. Η ΨΗΦΙΑΚΗ ΔΙΑΚΥΒΕΡΝΗΣΗ ΚΑΙ Η ΠΡΟΣΤΑΣΙΑ ΤΩΝ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

Σε αυτό το κεφάλαιο θα γίνει λόγος για τους κινδύνους που ελλοχεύουν για τα προσωπικά δεδομένα στα πλαίσια της συνεχούς ψηφιοποίησης του δημόσιου τομέα στην Ελλάδα.

## 6.1 Εισαγωγή

Το δικαίωμα στην ιδιωτική ζωή και η προστασία των προσωπικών δεδομένων έχουν αποκτήσει μεγαλύτερη σημασία στην ψηφιακή εποχή που διανύουμε, με τις τεχνολογικές εξελίξεις να δίνουν την ευκαιρία στο δημόσιο τομέα να παρέχει ένα πλήθος ηλεκτρονικών υπηρεσιών αλλά και στους ιδιωτικούς οργανισμούς να δημιουργούν στοχευμένες διαφημίσεις ανάλογα με τις προτιμήσεις των πολιτών. Παραβιάσεις δεδομένων που αφορούν τη μη συναινετική συλλογή των προσωπικών δεδομένων δύναται να επιφέρουν πρόστιμα εκατομμυρίων σε ιδιωτικούς και δημόσιους οργανισμούς. Η ψηφιοποίηση του δημόσιου τομέα γέννησε επίσης την ανάγκη για ανταλλαγή δεδομένων μεταξύ των οργανισμών του δημόσιου τομέα.

Σύμφωνα με τα άρθρα 13 και 14 του ΓΚΠΔ το υποκείμενο των δικαιωμάτων έχει δικαίωμα ενημέρωσης είτε η επεξεργασία των δεδομένων γίνεται από το υποκείμενο των δεδομένων (άρθρο 13) είτε από τρίτο φορέα (άρθρο 14). Οι πληροφορίες που θα πρέπει να δίνονται είναι αρχικά η ταυτότητα και τα στοιχεία επικοινωνίας του υπευθύνου επεξεργασίας, τα στοιχεία επικοινωνίας του υπευθύνου προστασίας δεδομένων και ο σκοπός της επεξεργασίας. Επιπλέον τα φυσικά πρόσωπα θα πρέπει να ενημερώνονται για το χρονικό διάστημα τήρησης των δεδομένων αλλά και για τα δικαιώματα που έχουν απέναντι στον υπεύθυνο επεξεργασίας των δεδομένων. Όλες αυτές οι πληροφορίες θα πρέπει να είναι εύκολα προσβάσιμες και διατυπωμένες με σαφή, κατανοητή και απλή γλώσσα.

## 6.2 Ασφάλεια Προσωπικών Δεδομένων

Στο άρθρο 32 του ΓΚΠΔ ορίζεται ότι για την προστασία των προσωπικών δεδομένων θα πρέπει να εφαρμοστούν από τον υπεύθυνο επεξεργασίας κατάλληλα τεχνικά μέσα. Σύμφωνα με το ίδιο άρθρο ένα από αυτά τα μέτρα είναι η κρυπτογράφηση των δεδομένων. Προκειμένου να γίνει εκτίμηση του κινδύνου θα πρέπει να ληφθεί υπόψη η διαφορετική πιθανότητα επέλευσης κάποιων κινδύνων αλλά και η σοβαρότητα του κάθε κινδύνου. Στην περίπτωση των ιστοσελίδων του δημοσίου τομέα, που εξετάστηκαν και δεν χρησιμοποιούν ασφαλή πρωτόκολλα επικοινωνίας, θα πρέπει να λάβει κανείς υπόψη εάν αυτές οι ιστοσελίδες επεξεργάζονται προσωπικά δεδομένα αλλά και τί είδους προσωπικά δεδομένα χρησιμοποιούν.

Όπως αναφέρθηκε παραπάνω οι ιστοσελίδες που χρησιμοποιούν μη ασφαλή σύνδεση HTTP είναι ελάχιστες. Από αυτές μόνο 2 χρησιμοποιούν φόρμα συμπλήρωσης στοιχείων. Η μία ωστόσο από αυτές (ιστοσελίδα του Γενικού Επιτελείου Στρατού) μεταφέρει το χρήστη σε ασφαλή HTTPS σύνδεση όταν χρειάζεται να εισάγει προσωπικά του στοιχεία. Η έκδοση όμως TLS που χρησιμοποιεί είναι η TLS 1.2, η οποία παρουσιάζει ορισμένες ευπάθειες σε κάποια είδη επιθέσεων. Σε αυτή την περίπτωση η πιθανότητα εμφάνισης

κινδύνων δεν χαρακτηρίζεται ως υψηλή ωστόσο θα μπορούσαν να υπάρξουν σοβαρές επιπτώσεις σε περίπτωση παραβίασης των προσωπικών δεδομένων καθώς ενδέχεται ο ιστότοπος να αποθηκεύει δεδομένα που άπτονται θεμάτων εθνικής άμυνας.

Σε αντίθεση με την ιστοσελίδα του Γενικού Επιτελείου Στρατού, η ιστοσελίδα του Υπουργείου Ανάπτυξης και τροφίμων χρησιμοποιεί ακόμα και στο στάδιο εισαγωγής δεδομένων των χρηστών μη ασφαλή σύνδεση HTTP. Για να κάνει κάποιος εγγραφή και να μπορέσει να χρησιμοποιήσει τις ηλεκτρονικές υπηρεσίες της συγκεκριμένης ιστοσελίδας θα πρέπει να εισάγει προσωπικά του στοιχεία όπως ονοματεπώνυμο, email, διεύθυνση κατοικίας και αριθμό φορολογικού μητρώου. Σε αυτή την περίπτωση η πιθανότητα εμφάνισης κινδύνων θεωρείται υψηλή όπως επίσης και ο αντίκτυπος που θα έχει μία πιθανή παραβίαση στα προσωπικά δεδομένα.

Πέραν από τις κυβερνητικές ιστοσελίδες που χρησιμοποιούν μη ασφαλή σύνδεση HTTP, υπάρχουν και ιστοσελίδες που χρησιμοποιούν την έκδοση του TLS 1.2, η οποία χρησιμοποιεί κάποιους παρωχημένους αλγόριθμους κρυπτογράφησης, οι οποίοι την καθιστούν ευάλωτη σε συγκεκριμένα είδη επιθέσεων. Σύμφωνα με τα αποτελέσματα που παρουσιάστηκαν παραπάνω τη συγκεκριμένη έκδοση του TLS τη χρησιμοποιεί το 22% των ιστοσελίδων, δηλαδή 11 από τις συνολικά 50 ιστοσελίδες που εξετάστηκαν. Από αυτές τις 11 ιστοσελίδες μόνο μία δεν χρησιμοποιεί φόρμα καταχώρησης προσωπικών στοιχείων για την είσοδο σε κάποια ηλεκτρονική εφαρμογή. Οι ιστοσελίδες που χρησιμοποιούν φόρμα εισόδου για τις ηλεκτρονικές υπηρεσίες που παρέχουν χρησιμοποιούν τον ίδιο τύπο δεδομένων, δηλαδή ονοματεπώνυμο, διεύθυνση, email και σε ορισμένες περιπτώσεις αριθμό φορολογικού μητρώου. Στην περίπτωση λοιπόν της χρήσης του TLS 1.2 η πιθανότητα εμφάνισης κινδύνου θα μπορούσε να θεωρηθεί μεσαία. Η επίπτωση ωστόσο σε περίπτωση που γινόταν υποκλοπή δεδομένων θα ήταν υψηλή καθώς ο κακόβουλος χρήστης μέσω αυτής της παραβίασης θα μπορούσε να αποκτήσει πρόσβαση και να βλάψει πλήθος προσωπικών δεδομένων που έχουν στη διάθεση τους κρατικοί οργανισμοί. Ως τέτοιο παράδειγμα θα μπορούσε να αναφερθεί ο Εθνικός Οργανισμός Παροχής Υπηρεσιών Υγείας, που διαθέτει ακόμα και ευαίσθητα δεδομένα υγείας των πολιτών αλλά και η περίπτωση της ιστοσελίδας gov.gr, που αποτελεί την κεντρική πύλη παροχής ηλεκτρονικών υπηρεσιών του ελληνικού δημόσιου τομέα. Το ρίσκο λοιπόν σε αυτές τις περιπτώσεις για τα προσωπικά δεδομένα θεωρείται υψηλό.

Τέλος, μικρός αριθμός κυβερνητικών ιστοσελίδων χρησιμοποιεί την έκδοση του TLS 1.1. Από τις 4 ιστοσελίδες που κάνουν χρήση της εν λόγω έκδοσης του TLS μόνο η μία έχει φόρμα εισαγωγής δεδομένων για είσοδο σε ηλεκτρονικές υπηρεσίες. Με τη χρήση αυτής της παλαιότερης έκδοσης του TLS, η πιθανότητα εμφάνισης κινδύνου είναι υψηλή και αντίστοιχα και η επίπτωση σε πιθανή απώλειας δεδομένων θα μπορούσε να θεωρηθεί υψηλή.

# 7. ΕΝΗΜΕΡΩΣΗ ΧΡΗΣΤΩΝ ΓΙΑ ΤΗΝ ΕΠΕΞΕΡΓΑΣΙΑ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

Σε αυτό το κεφάλαιο θα αναλυθούν οι προϋποθέσεις που θέτει ο ΓΚΠΔ για την ενημέρωση των υποκειμένων των προσωπικών δεδομένων για την επεξεργασία τους και θα εξεταστεί το κατά πόσο οι προαναφερόμενες κυβερνητικές ιστοσελίδες πληρούν τα κριτήρια που θέτει ο νόμος.

## 7.1 Υποχρέωση διαφάνειας σύμφωνα με το ΓΚΠΔ

Η αρχή της διαφάνειας που εισάγεται στο άρθρο 5 του ΓΚΠΔ αποτελεί βασική αρχή του και επηρεάζει κυρίως τον τρόπο με τον οποίο οι επιχειρήσεις αλληλοεπιδρούν με τα υποκείμενα και το δικαίωμα που δίνεται από το νόμο στην ενημέρωση. Από την αρχή της διαφάνειας απορρέει η υποχρέωση σύνταξης ειδοποιήσεων ενημέρωσης για την επεξεργασία των δεδομένων. Η υποχρέωση αυτή περιλαμβάνει και την πολιτική απορρήτου που συναντάται στις περισσότερες ιστοσελίδες, η οποία θα πρέπει να περιλαμβάνει όλα τα στοιχεία που αναφέρονται στα άρθρα 13 και 14 του ΓΚΠΔ. Οι πληροφορίες που θα πρέπει να δίνονται στο υποκείμενο των δικαιωμάτων όταν επισκέπτεται μία ιστοσελίδα που επεξεργάζεται τα προσωπικά του δεδομένα θα πρέπει:

- να είναι κατανοητές και εύκολα προσβάσιμες
- να χρησιμοποιούν σαφή γλώσσα
- να παρέχονται δωρεάν
- να δίνονται γραπτώς ή με άλλα μέσα
- να περιέχουν όλες τις σχετικές πληροφορίες εντός εύλογου χρονικού διαστήματος

### 7.1.1 Απαιτήσεις ενημέρωσης

Σύμφωνα με όσα αναφέρονται στα άρθρα 13 και 14 του ΓΚΠΔ σε κάθε περίπτωση το υποκείμενο των δικαιωμάτων θα πρέπει να γνωρίζει τα στοιχεία αυτού που εκτελεί την επεξεργασία των δεδομένων του, το σκοπό της επεξεργασίας του αλλά και το αν τα δεδομένα διαβιβάζονται σε τρίτους. Στα πλαίσια της διαφανούς επεξεργασίας θα πρέπει επιπλέον η ενημέρωση να περιλαμβάνει:

- Ποιος είναι ο υπεύθυνος επεξεργασίας και ποιοι είναι οι τρόποι επικοινωνίας μαζί του;
- Ποιες κατηγορίες δεδομένων συλλέγονται και γιατί;
- Ποιος είναι ο αποδέκτης των δεδομένων;
- Τα δεδομένα διαβιβάζονται σε τρίτες χώρες; Ποιες είναι οι διασφαλίσεις;
- Για πόσο χρονικό διάστημα αποθηκεύονται τα δεδομένα;
- Ποια δικαιώματα έχει το υποκείμενο των δεδομένων;
- Ποια είναι η πηγή των δεδομένων;
- Υπάρχει χρήση αυτοματοποιημένης λήψης αποφάσεων;

Όσον αφορά την αρχή της διαφάνειας και κατ' επέκταση την ενημέρωση των υποκειμένων των δεδομένων έχουν δοθεί και κατευθυντήριες οδηγίες από την ομάδα εργασίας του άρθρου 29 [24]. Στις οδηγίες έχουν αποτυπωθεί και πρακτικά παραδείγματα προς διευκόλυνση των υπεύθυνων επεξεργασίας δεδομένων. Η διαφάνεια θα πρέπει να εφαρμόζεται σε όλα τα στάδια επεξεργασίας των δεδομένων, τόσο κατά τη συλλογή τους όσο και κατά τη διάρκεια της επεξεργασίας τους.

Οι πληροφορίες λοιπόν που παρέχονται θα πρέπει να έχουν τα εξής χαρακτηριστικά, όπως αναφέρθηκαν και παραπάνω [24]:

- Κατανοητές και εύκολα προσβάσιμες

Ο τρόπος με τον οποίο εκφράζονται οι πληροφορίες θα πρέπει να είναι διαφανής και εύπεπτος. Η "απόκρυψη" του σε μεγάλες σειρές κειμένων ή αναμεμειγμένη με άλλες πληροφορίες δεν είναι αποδεκτή. Θα πρέπει το υποκείμενο των δικαιωμάτων να μπορεί εύκολα να βρει τις σχετικές πληροφορίες. Οι πολυεπίπεδες ειδοποιήσεις, τα αναδυόμενα παράθυρα ή τα chatbots αποτελούν καλά παραδείγματα προσβασιμότητας και διαφάνειας.

- Σαφής γλώσσα

Η γλώσσα που χρησιμοποιείται πρέπει να είναι σαφής και απλή. Δεν έχει σημασία αν είναι σε γραπτή μορφή ή κάποια άλλη μορφή, ο κανόνας εξακολουθεί να ισχύει. Η αποφυγή σύνθετων προτάσεων και αφηρημένων ή ασαφών όρων είναι σημαντική. Θα πρέπει επίσης να αποφεύγεται η χρήση υπερβολικά τεχνικών, νομικών ή εξειδικευμένων όρων. Οι πληροφορίες θα πρέπει να είναι κατανοητές από τον αναγνώστη στον οποίο απευθύνονται. Αυτό είναι ιδιαίτερα σημαντικό εάν πρόκειται για παιδιά ή ιδιαίτερα ευάλωτο άτομο. Ο στόχος της χρήσης κατανοητής γλώσσας στο πλαίσιο της αρχής της διαφάνειας είναι να διασφαλιστεί ότι το υποκείμενο των δικαιωμάτων κατανοεί πως τα δεδομένα του υποβάλλονται σε επεξεργασία.

- Δωρεάν παροχή των πληροφοριών

Στο πλαίσιο της αρχής της διαφάνειας η ενημέρωση θα πρέπει να παρέχεται δωρεάν. Σε καμία περίπτωση δεν πρέπει η πληροφόρηση του υποκειμένου των δικαιωμάτων να εξαρτάται από την πληρωμή ή την αγορά ενός προϊόντος ή μιας υπηρεσίας.

- Γραπτώς ή με άλλα μέσα

Οι πληροφορίες θα πρέπει να παρέχονται είτε σε γραπτή μορφή είτε σε άλλη μορφή. Για παράδειγμα, μπορούν να παρέχονται και με οπτικοακουστικό τρόπο για άτομα με προβλήματα όρασης. Επιπλέον όλες οι πληροφορίες θα πρέπει να συγκεντρώνονται σε ένα μόνο σημείο για εύκολη πρόσβαση.

- Παροχή πληροφοριών εντός εύλογου χρονικού διαστήματος

Σε περίπτωση που συλλέγονται τα δεδομένα απευθείας από το υποκείμενο τους, πρέπει να δίνονται οι πληροφορίες κατά τη συλλογή τους. Εάν συλλέγονται από άλλη πηγή, ο

κανόνας είναι η παροχή των πληροφοριών εντός εύλογου χρονικού διαστήματος. Αυτό δεν μπορεί να είναι μεγαλύτερο από ένα μήνα.

Πέραν των παραπάνω όλες οι πληροφορίες θα πρέπει να παρέχονται με τα κατάλληλα μέτρα. Στον ΓΚΠΔ ωστόσο δεν καθορίζει το ακριβές μέτρο. Κατά πόσον ένα μέτρο είναι κατάλληλο καθορίζεται από διάφορους παράγοντες. Η εμπειρία κάθε χρήστη, ποια συσκευή χρησιμοποιείται και άλλοι παρόμοιοι παράγοντες είναι ιδιαίτερα σημαντικοί. Εάν χρησιμοποιούνται για παράδειγμα εικονίδια για την παροχή των σχετικών πληροφοριών στο θέμα, θα πρέπει να είναι τυποποιημένα και να μην υποκαθιστούν άλλες μορφές πληροφοριών. Επιπλέον όταν γίνονται σχετικές αλλαγές, τα υποκείμενα των δεδομένων θα πρέπει να ενημερώνονται. Παραδείγματα τέτοιων αλλαγών είναι οι αλλαγές στις πολιτικές απορρήτου, η αλλαγή του υπεύθυνου επεξεργασίας ή η αλλαγή του σκοπού επεξεργασίας. Τέλος ο υπεύθυνος επεξεργασίας έχει την ευθύνη να ενημερώνει το υποκείμενο για τα δικαιώματά του. Οι πληροφορίες αυτές πρέπει επίσης να πληρούν τις απαιτήσεις διαφάνειας. Επιπλέον, ο υπεύθυνος επεξεργασίας πρέπει να διευκολύνει την άσκηση των δικαιωμάτων του υποκειμένου.

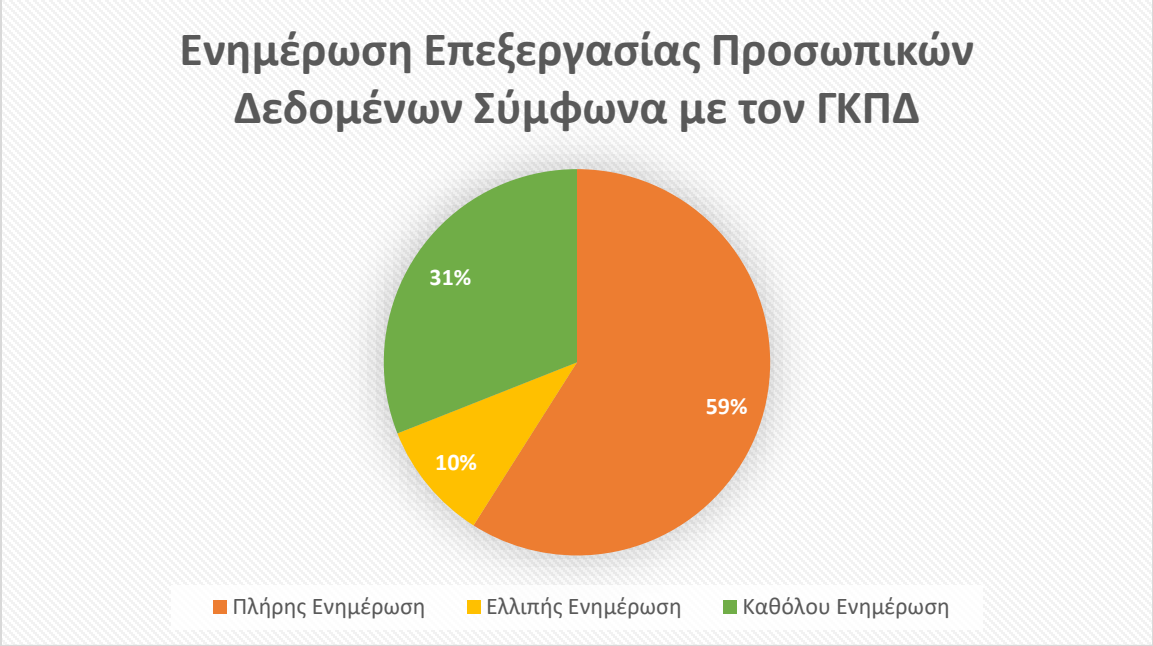
Σε όλα τα παραπάνω υπάρχουν και εξαιρέσεις στις οποίες δύναται ο υπεύθυνος επεξεργασίας να μην ενημερώσει το υποκείμενο των δικαιωμάτων. Η πρώτη εξαίρεση είναι όταν το υποκείμενο των δικαιωμάτων έχει ήδη τις πληροφορίες. Αυτό μπορεί να συμβεί μόνο σε περιπτώσεις που τα δεδομένα συλλέγονται απευθείας από το υποκείμενο. Εφόσον απαιτηθούν πρόσθετες πληροφορίες, θα πρέπει ακόμα και σε αυτή την περίπτωση να παρέχονται. Η δεύτερη εξαίρεση είναι όταν η ενημέρωση απαιτεί δυσανάλογη προσπάθεια ή θίγει τον σκοπό της επεξεργασίας. Αυτή η εξαίρεση χρησιμοποιείται κυρίως όταν η επεξεργασία των δεδομένων γίνεται για επιστημονικούς (ή παρόμοιους) σκοπούς. Η τρίτη εξαίρεση είναι όταν η επεξεργασία επιβάλλεται από το νόμο. Σε αυτή την περίπτωση ο υπεύθυνος επεξεργασίας θα πρέπει να διασφαλίζει ότι συμμορφώνονται με τη σχετική νομοθεσία. Τέλος η τέταρτη και τελευταία εξαίρεση είναι όταν η υποχρέωση απορρήτου σημαίνει ότι τα δεδομένα πρέπει να παραμείνουν εμπιστευτικά.

### 7.2 Ενημέρωση για προσωπικά δεδομένα σε ελληνικές κυβερνητικές ιστοσελίδες

Από το σύνολο των 50 κυβερνητικών ιστοσελίδων που εξετάστηκαν στην παρούσα εργασία σχεδόν οι μισές παρέχουν ηλεκτρονικές υπηρεσίες. Συγκεκριμένα το ποσοστό αυτό ανέρχεται στο 58% των ιστοσελίδων. Οι ηλεκτρονικές υπηρεσίες παρέχονται είτε με υλοποιημένα web services από τον ίδιο τον ιστότοπο είτε μέσω παραπομπής στην πύλη του gov.gr. Σε όλες τις περιπτώσεις συλλέγονται προσωπικά δεδομένα και απαιτείται κάποιου είδους εγγραφή των χρηστών. Στην περίπτωση των ηλεκτρονικών υπηρεσιών του ιστοτόπου gov.gr χρησιμοποιούνται διαπιστευτήρια taxisnet για τη σύνδεση και στη συνέχεια τη χρήση των ηλεκτρονικών υπηρεσιών. Πέραν του προαναφερόμενου είδους ηλεκτρονικών υπηρεσιών υπάρχουν ιστοσελίδες που δίνουν τη δυνατότητα ηλεκτρονικής υποβολής εντύπων ή υποβολής καταγγελιών. Σε αυτές τις περιπτώσεις ο χρήστης καλείται να συμπληρώσει σε φόρμα απαραίτητα κάποια προσωπικά του στοιχεία όπως για παράδειγμα ονοματεπώνυμο, διεύθυνση, ΑΦΜ κ.τ.λ..

Σύμφωνα με όσα αναφέρθηκαν παραπάνω θα πρέπει σε όλες αυτές τις περιπτώσεις να υπάρχει ενημέρωση στο υποκείμενο των δικαιωμάτων σύμφωνα με όσα ορίζει ο ΓΚΠΔ. Από τις 29 ιστοσελίδες που παρέχουν τις προαναφερόμενες ηλεκτρονικές υπηρεσίες οι 17 παρέχουν πλήρης ενημέρωση για τη χρήση προσωπικών δεδομένων, με όλες τις προϋποθέσεις που θέτει ο νόμος. Στην πλειοψηφία των περιπτώσεων τα στοιχεία της ενημέρωσης ήταν αναρτημένα σε εμφανές σημείο του ιστοτόπου και συμπεριλαμβάνονταν στους όρους χρήσης των ιστοσελίδων.

Πέραν αυτών των περιπτώσεων 3 ιστοσελίδες βρέθηκαν να παρέχουν ελλιπή ενημέρωση σχετικά με την επεξεργασία προσωπικών δεδομένων. Σε όλες τις περιπτώσεις στους όρους χρήσης περιλαμβάνονταν πληροφορίες για την επεξεργασία δεδομένων που δεν ήταν εναρμονισμένες με το ΓΚΠΔ αλλά με το προϊσχύον νομικό καθεστώς. Τέλος 9 από τις ιστοσελίδες που επεξεργάζονται προσωπικά δεδομένα δεν παρέχουν καμία ενημέρωση σχετικά με την επεξεργασία των δεδομένων και σύμφωνα με όσα ορίζει ο ΓΚΠΔ.




**Εικόνα 11: Ενημέρωση Επεξεργασίας Προσωπικών Δεδομένων**

# 8. ΣΥΜΠΕΡΑΣΜΑΤΑ

Στην παρούσα εργασία παρουσιάστηκε μία έρευνα για τη χρήση του πρωτοκόλλου HTTPS από σελίδες του ελληνικού δημόσιου τομέα. Επιπλέον εξετάστηκε η συμμόρφωση των φορέων με το νομικό πλαίσιο που έχει θεσπιστεί με τον ΓΚΠΔ ως προς την ενημέρωση και ως προς την ασφάλεια των ιστοσελίδων αναφορικά με το πρωτόκολλο TLS. Σε προγενέστερη έρευνα, σε δημοφιλείς ελληνικούς ιστότοπους, διαπιστώθηκε πως η υιοθέτηση του HTTPS δεν μπορεί να χαρακτηριστεί επαρκής καθώς υπήρχαν ιστοσελίδες που ακόμα χρησιμοποιούσαν το HTTP. Συγκεκριμένα στο δημόσιο τομέα διαπιστώθηκε πως περίπου το 72% των ιστοσελίδων χρησιμοποιεί HTTPS. Το ποσοστό αυτό σήμερα φαίνεται να έχει αυξηθεί και πλέον το 92% των ιστοσελίδων του δημόσιου φορέα χρησιμοποιεί το HTTPS. Όσον αφορά τη χρήση του TLS, το 70% των ιστοσελίδων χρησιμοποιεί την τελευταία έκδοση του πρωτοκόλλου γεγονός που σημαίνει πως οι υπόλοιπες ιστοσελίδες θεωρούνται ευάλωτες σε γνωστά είδη επιθέσεων σε προηγούμενες εκδόσεις του πρωτοκόλλου. Τα αποτελέσματα αυτά είναι ενθαρρυντικά σε σχέση με αυτά των προηγούμενων ετών καθώς μόνο ένα αμελητέο ποσοστό των ιστοσελίδων, που χρησιμοποιεί μη ασφαλή πρωτόκολλα επικοινωνίας, διαθέτει κάποιου είδους φόρμα συμπλήρωσης προσωπικών στοιχείων.

Έχοντας υπόψη το ΓΚΠΔ, ο οποίος έχει εισάγει ένα αυστηρότερο νομοθετικό πλαίσιο για την προστασία των προσωπικών δεδομένων που διακινούνται εντός Ε.Ε., συμπεραίνουμε πως ολοένα και περισσότεροι οργανισμοί προσπαθούν να συμμορφωθούν με όσα ορίζονται. Η χρήση του πρωτοκόλλου TLS, ανεξαρτήτως έκδοσης, έχει εξασφαλίσει από τη μία την κρυπτογράφηση των δεδομένων που διακινούνται στο διαδίκτυο, από την άλλη ωστόσο θα πρέπει να γίνει αντιληπτό πως πέραν αυτού του οργανωτικού μέτρου, θα πρέπει να εξασφαλιστεί περαιτέρω και η ασφάλεια των δεδομένων, με την χρήση τελευταίων εκδόσεων του πρωτοκόλλου.

Πέραν των ανωτέρω, σημαντική καθίσταται και η ενημέρωση των χρηστών ηλεκτρονικών υπηρεσιών του δημοσίου σχετικά με τα δικαιώματα που έχουν αναφορικά με την επεξεργασία των προσωπικών τους δεδομένων. Σε αυτή την περίπτωση τα αποτελέσματα είναι ενθαρρυντικά καθώς οι περισσότερες ιστοσελίδες του δημοσίου διαθέτουν πεδίο ενημέρωσης. Θα πρέπει ωστόσο να εναρμονιστεί το σύνολο των ιστοσελίδων του δημοσίου τομέα, δεδομένου και του χρονικού διαστήματος που έχει παρέλθει από τη θέση σε ισχύ του ΓΚΠΔ.

# 9. ΜΕΛΛΟΝΤΙΚΕΣ ΕΠΕΚΤΑΣΕΙΣ

Ως μελλοντικός ερευνητικός στόχος της παρούσας υλοποίησης προτείνεται η διεύρυνση του εξεταζόμενου στατιστικού δείγματος σε δημοφιλείς ιστοσελίδες του δημόσιου τομέα, σε ευρωπαϊκό επίπεδο, ώστε να μπορέσει να διεξαχθεί μία συγκριτική μελέτη για το επίπεδο συμμόρφωσης με το ΓΚΠΔ ανάμεσα στα κράτη-μέλη.

# ΑΚΡΩΝΥΜΙΑ

| | |
|---|---|
| AES-CBC | Advanced Encryption Standard - Cipher Block Chaining |
| BEAST | Browser Exploit Against SSL/TLS |
| BREACH | Browser Reconnaissance and Exfiltration via Adaptive Compression of Hypertext |
| CBC | Cipher Block Chaining |
| CRIME | Compression Ratio Info-leak Made Easy |
| DES | Data Encryption Standard |
| DH | Diffie–Hellman |
| DSA | Digital Signature Algorithm |
| ECDH | Elliptic-curve Diffie–Hellman |
| ECDHE | Elliptic Curve Diffie-Hellman Ephemeral |
| ECDSA | Elliptic Curve Digital Signature Algorithm |
| HTTP | Hypertext Transfer Protocol |
| HTTPS | Hypertext Transfer Protocol Secure |
| IETF | Internet Engineering Task Force |
| IP address | Internet Protocol address |
| IV | Initialization Vector |
| MAC | Message Authentication Code |
| MD5 | Message-Digest Algorithm |
| RC4 | Rivest Cipher 4 |
| RFC | Requests for Comments |
| ROBOT | Return Of Bleichenbacher’s Oracle Threat |
| RSA | Rivest–Shamir–Adleman |
| SHA-1 | Secure Hash Algorithm 1 |

| | |
|---|---|
| SSL | Secure Socket Layer |
| TCP | Transmission Control Protocol |
| TIME | Timing Info-leak Made Easy |
| TLS | Transport Layer Security |
| VPN | Virtual Private Networks |
| ΑΦΜ | Αριθμός Φορολογικού Μητρώου |
| ΓΚΠΔ | Γενικός Κανονισμός Προστασίας Δεδομένων |
| ΕΕ | Ευρωπαϊκή Ένωση |

# ΒΙΒΛΙΟΓΡΑΦΙΑ


[1] "A brief history of the General Data Protection Regulation (1981-2016)." https://iapp.org/resources/article/a-rief-history-of-the-general-data-protection-regulation/. Accessed 5 Feb. 2022.

[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 (Γενικός Κανονισμός για την Προστασία Δεδομένων).

[3] "How Decryption of Network Traffic Can Improve Security | Threatpost." 30 Nov. 2021, https://threatpost.com/decryption-improve-security/176613/. Accessed 30 Jun. 2022.

[4] Stallings W., 2017, “Cryptography and network security”, 4th ed., Boston, Mass: Pearson.

[5] Shbair, Wazen & Cholez, Thibault & François, Jérôme & Chrisment, Isabelle. (2016). A multi-level framework to identify HTTPS services.

[6] Dowling, Benjamin & Fischlin, Marc & Günther, Felix & Stebila, Douglas. (2015). A Cryptographic Analysis of the TLS 1.3 Handshake Protocol Candidates.

[7] Sheffer, Y., Holz, R. and Saint-Andre, P., 2015. Summarizing known attacks on transport layer security (TLS) and datagram TLS (DTLS).

[8] Efthymios Iosifidis and Konstantinos Limniotis. 2016. A Study of Lightweight Block Ciphers in TLS: The Case of Speck. In Proceedings of the 20th Pan-Hellenic Conference on Informatics (PCI ’16).

[9] Adjei, H.A., Shunhua, M.T., Agordzo, G.K., Li, Y., Peprah, G. and Gyarteng, E.S., 2021, February. SSL stripping technique (DHCP snooping and ARP spoofing inspection). In 2021 23rd International Conference on Advanced Communication Technology (ICACT) (pp. 187-193).

[10] W. Venema and M. Orlando. Vulnerability note VU#555316: STARTTLS plaintext command injection vulnerability, March 2011. http://www.kb.cert.org/vuls/id/555316. Accessed 4 Jul. 2022.

[11] Tomasz Andrzej Nidecki. "What Is the BEAST Attack - Acunetix." 21 May. 2020, https://www.acunetix.com/blog/web-security-zone/what-is-beast-attack/. Accessed 4 Jul. 2022.

[12] Team Sesame. "Padding Oracle Attacks - TLSeminar." 31 Jan. 2017, https://tlseminar.github.io/padding-oracle/. Accessed 4 Jul. 2022.

[13] I. Mantin. Attacking SSL when using RC4: Breaking SSL with a 13-year-old RC4 weakness. In Black Hat Asia, March 2015.

[14] Pratik Guha Sarkar, Shawn Fitzgerald. 2013. Attacks on SSL. A comprehensive study of BEAST, CRIME, TIME, BREACH, LUCKY 13 & RC4 BIASES.

[15] Bruce Morton."ROBOT Attack on RSA Encryption | Entrust Blog." 20 Dec. 2017, https://www.entrust.com/blog/2017/12/robot-attack-on-rsa-encryption/. Accessed 4 Jul. 2022.

[16] Adrienne Porter Felt, Richard Barnes, April King, Chris Palmer, Chris Bentzel, and Parisa Tabriz. 2017. Measuring HTTPS Adoption on the Web. In 26th USENIX Security Symposium. 1323–1338.

[17] Kontogeorgis, Dimitris & Limniotis, Konstantinos & Kantzavelou, Ioanna. (2018). An evaluation of the HTTPS adoption in websites in Greece: estimating the users awareness. PCI '18: Proceedings of the 22nd Pan-Hellenic Conference on Informatics. 46-51.

[18] "Ιστοσελίδες για: Κράτος & Οργανισμοί | greek-sites.gr." https://www.greek-sites.gr. Accessed 10 Jul. 2022.

[19] International Standard. ISO/IEC 27005:2018 Information technology – Security techniques - Information security risk management.

[20] Μεθοδολογία Αξιολόγησης Κινδύνου, [online] Available at: < https://www.enisa.europa.eu/risk-level-tool/methodology >. Accessed 22 Sep 2022.

[21] International Standard. ISO/IEC 27001 Information Security Management.

[22] International Standard. ISO/IEC 27002 Information Security Controls.

[23] An introduction to cipher suites, [online] Available at: < https://www.keyfactor.com/blog/cipher-suites-explained/>. Accessed 22 Sep 2022.

[24] Κατευθυντήριες γραμμές σχετικά με τη διαφάνεια βάσει του κανονισμού 2016/679, Ομάδα εργασίας του άρθρου 29, 29 Νοεμβρίου 2017.

[25] Dierks T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, August 2008.

[26] Ιστοσελίδες, ηλεκτρονικά καταστήματα (e-shops) και GDPR, [online] Available at: < https://www.lawspot.gr/nomika-blogs/magdalini_skondra/istoselides-ilektronika-katastimata-e-shops-kai-gdpr >. Accessed 10 Oct 2022.

[27] GitHub, “SSL Server Rating Guide”, [online] Available at: < https://github.com/ssllabs/research/wiki/SSL-Server-Rating-Guide>. Accessed 10 Oct 2022.

[28] 4 χρόνια GDPR στην Ελλάδα: 11 εκατ. ευρώ πρόστιμα και 699 παραβιάσεις, [online] Available at: < https://www.gdprgreece.com/article/147/4-hronia-gdpr-sthn-ellada-11-ekat-eyro-prostima-kai-699-paraviaseis>. Accessed 10 Oct 2022.

[29] Προστασία δεδομένων: Από τους πρώτους νόμους του ’70 στον GDPR, [online] Available at: < https://www.naftemporiki.gr/finance/100322/prostasia-dedomenon-apo-tous-protous-nomous-tou-70-ston-gdpr/>. Accessed 10 Oct 2022.

[30] Αρχή Προστασίας Δεδομένων, < https://www.dpa.gr/>. Accessed 10 Oct 2022.

[31] Stebila, D., Attacks on TLS, June 2020.