Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μεταπτυχιακή Διατριβή
Στην Ασφάλεια Υπολογιστών και Δικτύων

Προστασία προσωπικών δεδομένων στο διαδίκτυο (HTTPS) με έμφαση τον επιχειρησιακό κόσμο της Κύπρου

Όνομα Επώνυμο
Λοΐζος Σολωμού

Επιβλέπων Καθηγητής
Αδαμαντίνη Περατικού

Μήνας Έτος
2018-2019

Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μεταπτυχιακή Διατριβή

Στην Ασφάλεια Υπολογιστών και Δικτύων

Προστασία προσωπικών δεδομένων στο διαδίκτυο (HTTPS) με έμφαση τον επιχειρησιακό κόσμο της Κύπρου

Όνομα Επώνυμο
Λοΐζος Σολωμού

Επιβλέπων Καθηγητής
Αδαμαντίνη Περατικού

Η παρούσα μεταπτυχιακή διατριβή υποβλήθηκε
προς μερική εκπλήρωση των απαιτήσεων για απόκτηση
μεταπτυχιακού τίτλου σπουδών
στην Ασφάλεια Υπολογιστών και Δικτύων
από τη Σχολή Θετικών και Εφαρμοσμένων Επιστημών
του Ανοικτού Πανεπιστημίου Κύπρου.

Μήνας Έτος
2018-2019

Περίληψη

Οι στόχοι της μεταπτυχιακής διατριβής είναι να γίνουν οι ανάλογες έρευνες για να διαπιστωθεί κατά πόσο οι επιχειρήσεις στη Κύπρο συμμορφώνονται με τον Γενικό Κανονισμό Προστασίας Δεδομένων (GDPR) και εκτελούνται τα κατάλληλα μέτρα προστασίας των προσωπικών δεδομένων στο διαδίκτυο. Επίσης αξιολογείται η χρησιμοποίηση του πρωτοκόλλου HTTPS στις ιστοσελίδες των επιχειρήσεων ώστε να υλοποιείται σωστά για να διασφαλίζονται τα προσωπικά δεδομένα που διακινούνται στο διαδίκτυο. Οι μέθοδοι που ακολουθήθηκαν για τον εντοπισμό σημαντικών πληροφοριών και αποτελεσμάτων ήταν διαμέσου διαδικτυακού ερωτηματολογίου με την συμμετοχή 55 συμμετεχόντων, εκπροσωπώντας τις επιχειρήσεις που εργάζονται. Τα αποτελέσματα της μεταπτυχιακής διατριβής αυτής έδειξαν ότι οι περισσότερες επιχειρήσεις υλοποιούν το πρωτόκολλο HTTPS για να προστατεύσουν και να κρυπτογραφήσουν τις ιστοσελίδες τους από τυχόν παρεμβάσεις και αλλοιώσεις δεδομένων. Η έλευση του νέου κανονισμού έχει επηρεάσει τις επιχειρήσεις όμως με την εφαρμογή του προσδίδει αρκετά ωφελήματα τόσο στην ευκολία διαχείρισης των δεομένων όσο και στην προστασία τους. Τα τεχνικά και οργανωτικά μέτρα τηρούνται σε ένα πολύ καλό επίπεδο όμως σε κάποια σημεία χρειάζεται βελτίωση των οποίων τα πιο σημαντικά είναι η κρυπτογραφία, διαδικασίες περιστατικών ασφαλείας και λογισμικό πρόσληψης διαρροών δεδομένων.

Summary

The aims of the dissertation are to investigate whether the businesses in Cyprus comply with the General Data Protection Regulation (GDPR) and if they implement the appropriate measures to protect personal data on the Internet. In addition, there is an evaluation on the use of the HTTPS protocol in the businesses' websites, to be implemented correctly, in order to safeguard the personal data which are transporting on the Internet. The methods used to identify important information and results were through an online questionnaire, with the participation of 55 participants, representing the companies that work. The results of this dissertation shown that most of the businesses are implemented the HTTPS protocol to protect and to encrypt their web pages from any interventions and data alterations. The advent of the new regulation had an influence to the businesses, but after its implementation, it offers several benefits in terms of both ease of data management and their protection. The technical and organizational measures are observed to a very good level, but there are some points which need to be improved, who's most important is the cryptography, the procedures of security incidents and the leakage data capture software.

Ευχαριστίες

Ευχαριστώ πολύ την επιβλέποντα καθηγήτρια μου κυρία Αδαμαντίνη Περατικού για τις εξαιρετικές συμβουλές, υποδείξεις και φέρνοντας εις πέρας αυτήν την μεταπτυχιακή διατριβή στο τέλος της ώστε να είναι πλήρης. Εκφράζω την ευγνωμοσύνη μου στους καθηγητές του μεταπτυχιακού προγράμματος για τις πολύτιμες γνώσεις και καθοδήγηση που μου πρόσφεραν. Επιπλέον θερμές ευχαριστίες στους συναδέλφους και φίλους μου για την οποιανδήποτε βοήθεια και συμβουλή κατά την εκπόνηση της μεταπτυχιακής μου διατριβής. Τέλος θέλω να αφιερώσω αυτήν την μεταπτυχιακή διατριβή στην σύζυγο και στην οικογένεια μου για την απέραντη συμπαράσταση, ενθάρρυνση και αγάπη που μου έδωσαν με τόσο ξεχωριστό τρόπο όλο αυτό το διάστημα για την ολοκλήρωση της. Όλο αυτό τον καιρό έχω κερδίσει και μάθει πολλά όπως και το γεγονός να εκτιμώ περισσότερο τη ζωή.

Περιεχόμενα

Κεφάλαιο 1
Εισαγωγή

Η γενική κατεύθυνση του θέματος της παρούσας μεταπτυχιακής διατριβής είναι να διερευνήσει την προστασία των προσωπικών δεδομένων στο διαδίκτυο και συγκεκριμένα στον επιχειρησιακό κόσμο της Κύπρου. Έχει σκοπό να αξιολογήσει τη χρήση του HTTPS και να γίνει μια σειρά από έρευνες για να διαπιστωθεί κατά πόσο χρησιμοποιούνται σωστά οι τρόποι προστασίας των προσωπικών δεδομένων. Επίσης θα συμπληρωθούν ερωτηματολόγια διαδικτυακά σε διάφορες επιχειρήσεις για την εξεύρεση χρήσιμων πληροφοριών και αποτελεσμάτων, που έχουν σχέση με τον πιο πάνω σκοπό.

1.1 Εισαγωγή στην προστασία προσωπικών δεδομένων στις επιχειρήσεις

Ο επιχειρησιακός κόσμος στην Κύπρο έχει να αντιμετωπίσει μια τεράστια πρόκληση όσον αφορά την προστασία των προσωπικών δεδομένων και ιδιαίτερα το 2018 με την άφιξη του GDPR. Στη σύγχρονη εποχή η διαχείριση των προσωπικών δεδομένων στις επιχειρήσεις αυξάνεται με αποτέλεσμα οι κίνδυνοι που παραμονεύουν να είναι πολύ περισσότεροι. Έτσι δημιουργείται η ανάγκη για μια ολοκληρωμένη και σίγουρη προστασία των προσωπικών δεδομένων των επιχειρήσεων μέσω του διαδικτύου.

1.2 Σκοπός έρευνας

Ο απώτερος σκοπός της ασφάλειας των προσωπικών δεδομένων - πληροφοριών είναι να μειώσει τους κινδύνους της επιχειρηματικής δραστηριότητας. Αποτελεί μέρος της διαχείρισης και μείωσης του λειτουργικού κινδύνου, κάτι που πολλές επιχειρήσεις ειδικά στην Κύπρο το αγνοούν. Προφυλάγοντας τις πληροφορίες από πρόσβαση, αποκάλυψη, τροποποίηση σε μη εξουσιοδοτημένους χρήστες μπορείς να αποτρέψεις τους λειτουργικούς κινδύνους που μπορούν να υπάρξουν. Για αυτούς τους λόγους έχει δημιουργηθεί το GDRP, το οποίο απαιτεί άμεση και αποτελεσματική αλλαγή κουλτούρας στον επιχειρησιακό κόσμο. [02]

Αυτή η μεταπτυχιακή διατριβή μελετά την προστασία των προσωπικών δεδομένων στις επιχειρήσεις στην Κύπρο (τρόποι προστασίας των προσωπικών δεδομένων). Τα αποτελέσματα θα δείξουν κατά πόσο οι επιχειρήσεις στην Κύπρο έχουν ικανά επίπεδα προστασίας των προσωπικών δεδομένων και πόσο προετοιμασμένες είναι για αυτό. Το GDPR θα εφαρμοστεί ως μέτρο αξιολόγησης του επιπέδου προστασίας των προσωπικών δεδομένων στις ιστοσελίδες των επιχειρήσεων, για να ελεγχθεί κατά πόσο χρησιμοποιείται σωστά το HTTPS.

Ο τρόπος με τον οποίο οι επιχειρήσεις πρέπει να αντιλαμβάνονται τις αρχές νομιμότητας του GDPR για την προστασία των προσωπικών δεδομένων τόσο των δικών τους όσο και των πελατών τους είναι η ακόλουθη:

1. Διερεύνηση και σύγκριση λειτουργικών πλαισίων και διαδικασιών προστασίας των προσωπικών δεδομένων οι οποίες πρέπει να ακολουθούνται πιστά και με ευλάβεια. Οι διαδικασίες αυτές θα ήταν καλό να υπάρχουν έτσι ώστε να προβλέπουν ότι έχουν να κάνουν με την παραβίαση, χρήση και συγκέντρωση των προσωπικών δεδομένων.

2. Η διαχείριση των προσωπικών δεδομένων πρέπει να συμμορφώνεται σύμφωνα με τις πολιτικές των επιχειρήσεων και να μην χρησιμοποιούνται παράνομες πολιτικές οι οποίες μπορούν να εκτεθούν ή και να υπάρξουν απώλειες προσωπικών δεδομένων. Κάποιες πρακτικές όπως unmanaged file storage σε cloud (όπως Drobox, Google Drive, Box) δεν εμπίπτουν στην πολιτική της επιχείρησης και παραβιάζονται οι κανόνες ασφάλειας. Επίσης άλλοι κίνδυνοι που πρέπει να καταπολεμηθούν είναι το file sharing, υπηρεσίες αποθήκευσης οι οποίες δεν είναι εγκεκριμένες, δεδομένα εξαφανίζονται κατά την μεταφορά μεταξύ των sites και των συστημάτων επιχειρήσεων, η διαχείριση των δεδομένων δεν είναι η κατάλληλη κ.ά. Η υιοθέτηση μιας στρατηγικής για την ασφάλεια πληροφοριών και την αποτελεσματική υλοποίηση των βασικών αρχών της ασφάλειας πληροφοριών είναι η μόνη σωστή αντιμετώπιση.

3. Να έχουν καθοριστεί και καταγραφεί τα βασικά δεδομένα των επιχειρήσεων και έχουν ληφθεί κατάλληλα μέτρα προστασίας τους (στα πληροφοριακά συστήματα που προστατεύουν τα προσωπικά δεδομένα).

4. Τα πληροφοριακά συστήματα να είναι συμβατά ως προς τις ανάγκες της νομοθεσίας.

5. Καθορίζονται καθήκοντα και υποχρεώσεις όσον αφορά στην προστασία των προσωπικών δεδομένων.

6. Να υπάρχει ένα αρχείο το οποίο θα καταγράφει όλες τις ενέργειες που γίνονται.

Οι επιχειρήσεις στην Κύπρο θα αξιολογηθούν κατά πόσο έχουν συμμορφωθεί δηλαδή ευαισθητοποιηθεί, διεκπεραιώσει τις ανάλογες ενημερώσεις και εκπαιδεύσεις για την

προστασία των προσωπικών δεδομένων στον κυβερνοχώρο και σε ποιο βαθμό με βάση το GDRP ως πρότυπο. Άρα χρειάζεται να υπάρχει η κατάλληλη πληροφόρηση και εκπαίδευση για την νέα νομοθεσία των προσωπικών δεδομένων σχετικά με την ασφάλεια της προστασίας των προσωπικών δεδομένων έτσι ώστε να υπάρχει η επαρκής προετοιμασία για την αντιμετώπιση των σχετικών κινδύνων που μπορεί να υπάρξουν. Επίσης θα διερευνηθούν οι επιχειρήσεις για να διαπιστωθεί αν εφαρμόζεται το HTTPS για την ασφαλή προστασία των προσωπικών δεδομένων στο διαδίκτυο.

1.3 Βασικά ερευνητικά ερωτήματα

1. Πώς επηρεάζει η νέα νομοθεσία προστασίας των προσωπικών δεδομένων (GDPR) τις επιχειρήσεις στην Κύπρο;

2. Είναι πράγματι διασφαλισμένα τα προσωπικά δεδομένα σε βαθμό ώστε να διατηρούνται ασφαλή, ιδιωτικά και ακέραια;

3. Κατά πόσο εφαρμόζεται το HTTPS για την προστασία των προσωπικών δεδομένων στις ιστοσελίδες των επιχειρήσεων στην Κύπρο;

4. Υπάρχει η κατάλληλη εφαρμογή της νομοθεσίας περί προστασίας προσωπικών δεδομένων (GDPR);

1.4 Αναγκαιότητα και σπουδαιότητα της έρευνας

Η τεχνολογία έχει κάνει σημαντικά βήματα προόδου και αυτό επέφερε τη χρήση του διαδικτύου για καταχώρηση των προσωπικών δεδομένων. Αυτό όμως οδήγησε στην αναγκαιότητα δημιουργίας μέτρων προστασίας αυτών των δεδομένων. Σαν αποτέλεσμα αυτού επιβάλλεται η υποχρέωση ενός νέου πειθαρχημένου νομοθετικού πλαισίου που έχει να κάνει με την προστασία των προσωπικών δεδομένων με την ονομασία Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων (GDPR) και έχει πραγματοποιηθεί στις 25 Μαΐου του 2018.

Έτσι τώρα με το νέο νομοθετικό σχέδιο της Ευρωπαϊκής Ένωσης το οποίο είναι αυστηρότερο στο θέμα της ασφάλειας των προσωπικών δεδομένων οι επιχειρήσεις καλούνται να επενδύσουν στην προστασία αυτών των προσωπικών δεδομένων για να μην έχουν ποινικές επιβαρύνσεις με τη μη τήρηση των απαιτήσεων που προνοεί το νομοσχέδιο.

Η τήρηση του νομοσχεδίου έχει θετικό αντίκτυπο στις επιχειρήσεις γιατί εκτός του ότι δεν θα υποστούν κυρώσεις θα διατηρήσουν υψηλά επίπεδα παραγωγικότητας, αφού ανυψώνεται η εταιρική φήμη κερδίζοντας την αξιοπιστία και την εμπιστοσύνη προς στους πελάτες (επενδυτές και μετόχους) ικανοποιώντας τις προσδοκίες τους [02].
Επιπρόσθετα πρέπει να διοριστεί αρμόδιο πρόσωπο για να έχει τον έλεγχο και την προστασία των προσωπικών δεδομένων (Data Protection Officer –DPO). Τα

προβλήματα με τα δίκτυα συνεχίζονται να αυξάνονται συνεχώς και έτσι γεννιέται η ανάγκη να υφίσταται η παρακολούθησή τους.

Οι υποκλοπές των δεδομένων δεν περιορίζονται και για αυτό το λόγο η συγκεκριμένη μεταπτυχιακή διατριβή θα διερευνήσει την αφύπνιση στις επιχειρήσεις (κάποιες επιχειρήσεις δεν έχουν πλήρη αντίληψη) για να παρθεί σωστός προγραμματισμός, έλεγχος, αξιολόγηση και λήψη των κατάλληλων μέτρων προστασίας (ετοιμότητα του επιπέδου προστασίας).

Ο κανονισμός του GDPR γίνεται σε πράξη με την εκπαίδευση (χρειάζεται να γίνει εκπαίδευση με κατάλληλους ανθρώπους οι οποίοι είναι γνώστες στο αντικείμενο) και πιστοποίηση γνώσεων (τα στελέχη που θα εκπαιδευτούν να έχουν τις απαιτούμενες γνώσεις και προσόντα). Επίσης στις επιχειρήσεις που θα υλοποιείται να γίνονται οι ανάλογες έρευνες και ενέργειες γνησιότητας της εφαρμογής. Απαραίτητοι είναι και οι κατάλληλοι άνθρωποι (σύμβουλοι) που ειδικεύονται σε νομικά, τεχνικά αλλά και επιχειρησιακά θέματα. [02]

Το πρωτόκολλο HTTPS έχει μια ουσιαστικής σημασίας ρόλο στην ασφάλεια δεδομένων στο διαδίκτυο, αν και η εφαρμογή του συνίσταται εδώ και χρόνια σε πολλές επιχειρήσεις εντούτοις εξακολουθούν να το αγνοούν ή να το χρησιμοποιούν λανθασμένα. Με βάση το νομοσχέδιο και τους κανόνες συμμόρφωσης που προτείνονται στο GDRP η λειτουργία του HTTPS στις επιχειρήσεις στην Κύπρο χρειάζεται να αξιολογηθεί.

Κεφάλαιο 2
Βιβλιογραφική Επισκόπηση

Η βιβλιογραφική επισκόπηση χωρίζεται σε δύο μέρη. Στο πρώτο μέρος γίνεται ανάλυση της νομοθεσίας GDPR, μέσω διαφόρων πηγών και ακολούθως γίνεται μια εκτενής ανάλυση της βιβλιογραφίας γύρω από το πρωτόκολλο HTTPS.

2.1 GDPR

Το GDPR είναι ένας κανονισμός ο οποίος επηρεάζει τους ανθρώπους ή τις επιχειρήσεις που συλλέγουν και επεξεργάζονται πληροφορίες όσον αφορά τους πολίτες της Ευρωπαϊκής Ένωσης ανεξάρτητα από τον χώρο στον οποίο βρίσκονται τα δεδομένα. Επίσης καθιερώνει υποχρεωτική κοινοποίηση παραβίασης και οι επιχειρήσεις που υπόκεινται σε παραβιάσεις πρέπει να διαφωτίζουν τις αρχές προστασίας δεδομένων σε διάστημα 72 ωρών. Οι κανονισμοί είναι πολύ αυστηροί και για αυτό οι επιχειρήσεις που δεν συμμορφώνονται υπόκεινται σε κυρώσεις οι οποίες μπορεί να φτάσουν σε μεγάλα ποσά των εσόδων τους. [26]

Υπάρχουν διάφοροι λόγοι που οδήγησαν στη δημιουργία μιας καινούργιας νομοθεσίας. Η αρχική οδηγία του 1995 είχε εφαρμοστεί με τα πρότυπα μιας τεχνολογίας, η οποία πλέον έχει εξελιχθεί, αφού το διαδίκτυο στη σημερινή εποχή είναι αρκετά δημοφιλές αφού ευνοείται και με τη χρήση των έξυπνων τηλεφώνων (smartphones) και των μέσων κοινωνικής δικτύωσης κ.ά. Στη σημερινή πραγματικότητα οι πλείστες πληροφορίες βρίσκονται στο διαδίκτυο σε ηλεκτρονική μορφή κάτι που δυσκολεύει την προστασία τους. [26]

Οι επιχειρήσεις που χρησιμοποιούν το GDPR θα πρέπει να υλοποιήσουν τεχνολογικές και επιχειρησιακές προφυλάξεις και ελέγχους απορρήτου για την προστασία των προσωπικών δεδομένων. Επίσης πρέπει να παρθούν κατάλληλα εσωτερικά μέτρα που θα πληρούν τα κριτήρια για τις αρχές προστασίας των δεδομένων. Το GDPR επιβάλλει στις επιχειρήσεις να προστατευτούν από τυχόν απειλές που μπορεί να προκύψουν ώστε να διασφαλίσουν τον κυβερνοχώρο τους, όσον αφορά την στρατηγική, τη νομοθεσία και τις λειτουργίες που πρέπει να ακολουθήσουν. Όταν συμβούν αυτές οι απειλές θα πρέπει να βρίσκονται σε ετοιμότητα και να έχουν μια συνεχή ανθεκτικότητα. Η προστασία και η πρόληψη είναι άκρως σημαντικές, ενώ την ίδια στιγμή η κρυπτογράφηση αποτελεί ιδανική μέθοδο προστασίας των προσωπικών δεδομένων, που οδηγεί στη σωστή κατεύθυνση για την προφύλαξή τους. Επίσης οι επιχειρήσεις θα πρέπει να αναπροσαρμοστούν σε ότι έχει να κάνει με τις διευθετήσεις και τους περιορισμούς αυτής της νομοθεσίας. Οι απαιτήσεις που πρέπει να τηρούν οι επιχειρήσεις με τη νέα νομοθεσία είναι [ΒΛΕΠΕ ΠΑΡΑΡΤΗΜΑ Δ.1]:

1. Είναι δικαίωμα από όλους να διαγράψουν δεδομένα και να μην υπάρχουν πλέον διαθέσιμα (the right to be forgotten). [18]

2. Για την επεξεργασία των δεδομένων απαιτείται αποδοχή από τον δικαιούχο που αφορούν τα δεδομένα. [18]

3. Το δικαίωμα σύντομης και εύκολης μεταφοράς δεδομένων από έναν προμηθευτή υπηρεσιών σε ένα άλλο. [18]

4. Να εκλεγεί ένας υπεύθυνος επεξεργασίας δεδομένων. Ο αντιπρόσωπος θα πρέπει να ενεργεί εκ μέρους του υπεύθυνου επεξεργασίας δεδομένων και θα πρέπει να είναι σε επικοινωνία με τις εποπτικές αρχές. [18]

5. Η επεξεργασία των δεδομένων πρέπει να επιτυγχάνεται διαμέσου διαδικασιών οι οποίες θα τεκμηριώνονται. [18]

2.1.1 Στόχοι GDPR

Ο καινούργιος κανονισμός του GDPR έχει σαν μέλημα να υποβάλλει τα πάντα που περιστρέφονται γύρω από τα προσωπικά δεδομένα από όπου και αν είναι τοποθετημένα. Η έλλειψη συμμόρφωσης θα έχει συνέπειες στις επιχειρήσεις οι οποίες θα είναι αναγκασμένες να πληρώσουν προστίματα σύμφωνα με τα κέρδη τους, ενώ παράλληλα θα αποκτούν διεθνή κακή φημολογία. [18]

Η Ευρωπαϊκή Ένωση παρέχει δύο εργαλεία τα οποία είναι ο κώδικας συμπεριφοράς και δεύτερο η πιστοποίηση (a code of conduct and certification). Ο κανονισμός προσπαθεί να ωθήσει διάφορους φορείς ώστε να εκπαιδευτούν σε κώδικες συμπεριφοράς οι οποίοι θα δώσουν το έναυσμα στη σωστή υλοποίηση του κανονισμού. Οι κώδικες αυτοί πρέπει να είναι ξεκάθαροι και θεμιτοί στην επεξεργασία δεδομένων. Το GDPR θεσπίζει μηχανισμούς πιστοποίησης, σφραγίδες και σήματα επεξεργασίας δεδομένων δίνοντας τη δυνατότητα στα άτομα στα οποία ανήκουν τα δεδομένα να κρίνουν αν είναι ικανοποιητικό το επίπεδο προστασίας των δεδομένων που τους παρέχεται. Το GDPR ασχολείται με ενέργειες που γίνονται στην πράξη όσον αφορά πως διαχειρίζονται, κατανέμονται και χρησιμοποιούνται τα προσωπικά δεδομένα.

Οι συντονιστές που θα είναι υπεύθυνοι για την μετάβαση στο GDPR θα πρέπει να στηρίζονται σε επαγγελματίες όπως δικηγορικές εταιρείες, χρήση νομικών εργαλείων στο διαδίκτυο, συμβουλευτικές εταιρείες οι οποίες θα είναι σε θέση να δώσουν αναλύσεις και συμβουλές για τη σωστή διαχείριση της ψηφιακής μετάβασης. Επίσης συμβουλές παρέχονται και από εταιρικούς αρχιτέκτονες οι οποίοι θα δώσουν τη σωστή καθοδήγηση βασιζόμενη στο σύνολο της επιχείρησης και όχι αποκλειστικά στα δεδομένα ή πληροφοριακά συστήματα.

Οι στόχοι του GDPR είναι:

1. Η καθιέρωση κανόνων για την προστασία και επεξεργασία των προσωπικών δεδομένων.

2. Προστασία των δικαιωμάτων και ανεξαρτησίας των ατόμων που έχουν να κάνουν με τα προσωπικά τους δεδομένα.

3. Η ασφαλή διακίνηση των προσωπικών δεδομένων εντός της Ευρωπαϊκής Ένωσης (άρθρο 1 GDPR). [07]

Το 1995 η Ευρωπαϊκή Ένωση επικύρωσε την οδηγία 95/46/ΕΚ όπου βασίζεται σε επτά αρχές που είναι: όταν τα προσωπικά δεδομένα χρησιμοποιούνται πρέπει να γίνεται γνωστοποίηση, συμφωνία με το άτομο στο οποίο ανήκουν τα δεδομένα, μεταφορά

δεδομένων μετά από μια συγκεκριμένη χρονική στιγμή, διασφάλιση και γνησιότητα των δεδομένων, προσβασιμότητα και εφαρμογές (applications).

2.1.2 GDPR στις επιχειρήσεις

Οι πληροφορίες (δεδομένα) σε μία επιχείρηση είναι το άλφα και το ωμέγα. Πρέπει να γνωρίζει η κάθε επιχείρηση ποίες πληροφορίες κρατάει, ποιος τις κρατάει και αν είναι ασφαλές ή όχι. Η κακή χρήση των φυσικών και ψηφιακών πληροφοριών (έλλειψη συμμόρφωσης) έχει μεγάλες πιθανότητες όπως έχει διατυπωθεί προηγουμένως να κατευθύνει την επιχείρηση σε μεγάλες οικονομικές απώλειες καθώς και σε κακή φήμη.
Η υλοποίηση διαδικασιών οι οποίες επιφέρουν μηδαμινή ασφάλεια στις πληροφορίες ενδέχεται να φέρει δημοσιοποίηση σε τίτλους εφημερίδων, ανεπιθύμητο δημόσιο έλεγχο και σε κακές σχέσεις με τους πελάτες. Οι επιχειρήσεις πρέπει να εναρμονίζονται με τις τελευταίες οδηγίες συμμόρφωσης όμως οι κλοπές των πληροφοριών και των ταινιών που γίνονται (backups) έχουν δημιουργήσει μεγάλο πρόβλημα. Έτσι καλούνται να δώσουν μεγαλύτερη βαρύτητα στα φυσικά και ψηφιακά δεδομένα τα οποία πρέπει να βρεθούν σωστοί τρόποι οργάνωσης, υποστήριξης και αποθήκευσης. Σε αντίθετη περίπτωση τα στελέχη ενδέχεται να δεχτούν κυρώσεις που μπορεί να οδηγήσουν και σε φυλάκιση. [23]

Προσωπικά δεδομένα είναι πληροφορίες οι οποίες μπορούν να αναγνωρίσουν άμεσα ή έμμεσα ένα πρόσωπο. Στα προσωπικά δεδομένα συμπεριλαμβάνονται οι διευθύνσεις IP (Internet Protocol) και cookies. [26] Πλέον τα προσωπικά δεδομένα δεν αφορούν εξολοκλήρου στους κλάδους των τραπεζών ή ιατρών αλλά αφορά όνομα ατόμου, διεύθυνση IP ή ηλεκτρονικού ταχυδρομείου, ιατρικά δεδομένα, στοιχεία τραπεζικού λογαριασμού, φωτογραφία, μηνύματα σε σελίδες δικτύου που δημοσιεύονται κ.α.

Η ψευδονοποίηση (pseudonymisation) είναι μια διαδικασία αναγνώρισης πληροφοριών για τα προσωπικά δεδομένα και χρησιμοποιείται για να προστατεύσει την ιδιωτική ζωή των ανθρώπων. Επίσης παρέχει την δυνατότητα στις επιχειρήσεις να ελαχιστοποιήσουν τους κινδύνους που έχουν άμεσα σχέση με την επεξεργασία και παραβίαση των δεδομένων. Κατά τη διάρκεια της διαδικασίας ψευδονοποίησης τα δεδομένα υποβάλλονται σε επεξεργασία και διαφυλάσσονται ξεχωριστά από κάθε πληροφορία με τρόπο που να μην καταλήξει στα χέρια ενός άλλου ατόμου που δεν πρέπει.

Για την επεξεργασία των δεδομένων των μεμονωμένων προσώπων απαιτείται η συγκατάθεση και η ενημέρωσή τους. Οι ίδιοι έχουν το δικαίωμα πρόσβασης στα δεδομένα όπως και το δικαίωμα να αρνηθούν για την επεξεργασία τους. Επίσης ένα άλλο δικαίωμα είναι το δικαίωμα να ξεχαστούν (right to be forgotten), δηλαδή να αφαιρεθούν δεδομένα που δεν τους ενδιαφέρουν πια ή που δεν είναι πλήρεις. Αυτό έχει σαν αποτέλεσμα οι επιχειρήσεις να πρέπει να γνωρίζουν για τα δεδομένα που διαθέτουν καθώς και το πού βρίσκονται. [26]

Όπου δεν υπάρχουν ικανοποιητικά επίπεδα ασφάλειας δεν επιτρέπονται οι μεταβιβάσεις δεδομένων εκτός και αν δώσει το δικαίωμα η εποπτική αρχή. Πλέον τα προσωπικά δεδομένα δεν αφορούν εξολοκλήρου τους κλάδους των τραπεζών ή των ιατρών, αλλά αφορούν το όνομα του ατόμου, τη διεύθυνση IP ή ηλεκτρονικού ταχυδρομείου, τα ιατρικά δεδομένα, τα στοιχεία τραπεζικού λογαριασμού, τις φωτογραφίες, μηνύματα σε σελίδες δικτύου που δημοσιεύονται κ.ά.

2.1.3 Κρυπτογράφηση και GDPR

Η κατάλληλη μέθοδος για την προστασία των δεδομένων είναι η κρυπτογράφηση (cryptography) μαζί με την ψευδονοποίηση (pseudonymisation). Όταν εφαρμοστεί η μέθοδος αυτή οι επιχειρήσεις που θα υποστούν παραβίαση δεδομένων δεν υποχρεώνονται να ενημερώσουν τα άτομα αυτά στα οποία ανήκουν, αφού έχουν κρυπτογραφηθεί σωστά.
Η κρυπτογράφηση εφαρμόζεται στα ευαίσθητα δεδομένα όταν αποθηκευτούν ή αντιγραφούν. Για τα κρυπτογραφημένα δεδομένα που έχουν δημιουργηθεί αντίγραφα για σκοπούς ασφάλειας γίνεται μια ανάλυση αξίας / κέρδους. [23] Σκοπός της κρυπτογράφησης είναι η προστασία των δεδομένων που μεταφέρονται και αποθηκεύονται όπου τα δεδομένα αυτά εμφανίζονται σε δομημένη καθώς και σε μη δομημένη μορφή τα οποία βρίσκονται σε βάσεις δεδομένων ή αρχείων, σε ηλεκτρονικά μηνύματα κ.α. Τα κρυπτογραφικά κλειδιά των δεδομένων που αποθηκεύονται στα τελικά σημεία (endpoints) και στο σύννεφο (cloud) πρέπει να διατηρούνται στις επιχειρήσεις που είναι ο άμεσα αρμόδιος για τη συλλογή ή επεξεργασία δεδομένων ώστε να προστατευτούν από τη μη εξουσιοδότηση άλλων ατόμων.

Η μέθοδος της κρυπτογράφησης δεν είναι αρκετή για την προστασία των δεδομένων και για αυτόν τον λόγο χρειάζεται επιπρόσθετους ελέγχους πρόσβασης όταν αποκρυπτογραφούνται τα δεδομένα από άτομα τα οποία δεν έχουν δικαιώματα πρόσβασης όπως επίσης και για τον έλεγχο των ικανοτήτων που πρέπει να έχει ο κάθε χρήστης με τα δεδομένα. Αυτοί οι έλεγχοι πρέπει να συνδέονται σε βάσεις δεδομένων όπως για παράδειγμα το Active Directory που διευκολύνει τον προσδιορισμό δικαιωμάτων και όταν παρουσιάζεται μια αλλαγή θα γίνεται ενημέρωση.

Ο έλεγχος ταυτότητας χρησιμοποιείται για να διαπιστώσουμε ότι τα δεδομένα μεταχειρίζονται από τους σωστούς ανθρώπους και τα δικαιώματα πρόσβασης που διακατέχονται στα δεδομένα δεν θα μπορούν να δοθούν κάπου αλλού. Οι έλεγχοι αυτοί καθώς και τα συστήματα ασφαλείας πρέπει να παρακολουθούνται συνεχώς έχοντας υπόψη τους κινδύνους που μπορεί να υπάρξουν όσον αφορά την αποθήκευση, επεξεργασία ακόμη και την απώλεια ή την καταστροφή των δεδομένων. Για καλύτερη ασφάλεια γίνεται ενσωμάτωση με τα συστήματα πληροφοριών και με τα συστήματα που διευθύνουν τα περιστατικά τα οποία θα έχουν πιο ξεκάθαρη εικόνα για το τι συμβαίνει στο διαδίκτυο. [26]

Ο κανονισμός του 99 λέει ότι το GDPR ισχύει για όλες τις επιχειρήσεις που δραστηριοποιούνται στην Ευρώπη ανεξάρτητα με το που βρίσκονται. Έτσι για κάθε επιχείρηση που η ηλεκτρονική της παρουσία είναι διαθέσιμη στους Ευρωπαίους πολίτες για να την χρησιμοποιήσουν, αν πουλάει στην Ευρώπη ή δίνει πρόσβαση σε ηλεκτρονικές υπηρεσίες τότε πρέπει να συμμορφωθούν με το GDPR αλλιώς θα πρέπει να υποστεί προστίματα.

Το GDPR έχει επιδιώξεις που μπορούν να γίνουν διαμέσου της χρήσης των πιστοποιητικών SSL. Το άρθρο 32 του κανονισμού (Ασφάλεια) που λέει ότι σύμφωνα με την κατάσταση της τεχνολογίας, το κόστος υλοποίησης και η φύση, το πεδίο εφαρμογής, πλαίσιο και σκοποί επεξεργασίας, κίνδυνοι των δικαιωμάτων και ελευθεριών των φυσικών προσώπων, ο ελεγκτής και ο υπεύθυνος επεξεργασίας θα πρέπει να υλοποιήσουν κατάλληλα τεχνικά και οργανωτικά μέτρα για την διασφάλιση του κινδύνου ανάλογα με την περίπτωση:

1. Ψευδονοποίηση και κρυπτογράφηση των προσωπικών δεδομένων.

2. Η δυνατότητα να επιτυγχάνεται η συνεχής εμπιστευτικότητα, ακεραιότητα, διαθεσιμότητα και ανθεκτικότητα των συστημάτων και υπηρεσιών επεξεργασίας.

Το GDPR με αυτές τις εκφράσεις θέλει να δηλώσει ότι οι τροποποιημένες πληροφορίες επιβάλλεται να διασφαλίζονται με κατάλληλα τεχνικά και οργανωτικά μέτρα, κρυπτογράφηση των προσωπικών δεδομένων και της δυνατότητας να υπάρχει ατέλειωτη διαφύλαξη της εμπιστευτικότητας των συστημάτων και υπηρεσιών. Τα ψηφιακά πιστοποιητικά (όπως και το TLS/SSL) και η κρυπτογράφηση χρειάζονται για όλες τις εμπιστευτικές επικοινωνίες σε όλο το διαδίκτυο που βρίσκεται ελεύθερο.

Ο κανονισμός επηρεάζει σχεδόν όλα τα προσωπικά δεδομένα συμπεριλαμβανομένου των προσωπικών προσωπικής ταυτοποίησης (personal identifiable information), προσωπικές πληροφορίες για την υγεία (personal health information), των πληροφοριών για την χρήση του διαδικτύου και ενός συνόλου προσωπικών χαρακτηριστικών όπως η φυλή, σεξουαλικός προσανατολισμός και οι πολιτικές απόψεις.

Εάν οι ιστοσελίδες εφαρμόζουν το πρωτόκολλο HTTPS και χρησιμοποιούν πιστοποιητικά για να πιστοποιήσουν την ταυτότητα (εξακρίβωση της ταυτότητας) και στην κρυπτογράφηση επικοινωνιών μεταξύ εσωτερικών συστημάτων τότε πληρούνται οι απαιτήσεις του GDPR για την ασφάλεια των δεδομένων. Αν σε περίπτωση που δεν γίνεται αυτό είναι καλά να εφαρμοστεί γιατί μόνο θετικά αποτελέσματα μπορεί να έχει όπως διασφάλιση των πελατών, προστασία της ίδιας της επιχείρησης και η εμπιστοσύνη στον ιστότοπο θα αυξηθεί. [14]

2.1.4 Επιρροή στις επιχειρήσεις

Η κάθε επιχείρηση πρέπει να έχει ένα υπεύθυνο προστασίας δεδομένων ο οποίος θα εκτελεί σοβαρές δραστηριότητες επεξεργασίας δεδομένων και όπου χρειάζεται θα αξιολογηθούν οι συνέπειες των δεδομένων κάθε φορά που έχουν προκύψει κίνδυνοι παραβίασης των δικαιωμάτων και ελευθερίας των ανθρώπων. Οι αξιολογήσεις περιέχουν μέτρα προστασίας και μηχανισμούς ώστε να αποφθεχθούν οι τυχόν κίνδυνοι για τη διασφάλιση της συμμόρφωσης. [26] Επίσης στην αξιολόγηση κινδύνου πρέπει να υπάρχουν διαδικασίες, πολιτικές, όπου απαιτείται να γνωρίζεται ανά πάσα στιγμή που βρίσκονται αποθηκευμένα τα δεδομένα και να γίνεται εντοπισμός ευπαθειών για την ασφάλεια της επιχείρησης. Οι ευθύνες πρέπει να μοιράζονται σε όλη την επιχείρηση και να μη στηρίζονται σε ένα μικρό τμήμα. Επιπρόσθετο κόστος προστασίας χρειάζονται τα αρχεία και οι βάσεις των δεδομένων που είναι ευαίσθητα. [23]

Με την νέα προσθήκη της νέας θυρίδας (one stop shop*) οι υπεύθυνοι επεξεργασίας δεδομένων και οι επεξεργαστές θα διευκολυνθούν καθώς δεν θα χρειάζεται να ενημερώνουν την αρχή προστασίας δεδομένων σε όλα τα κράτη μέλη της Ευρωπαϊκής

---

*One stop shop: κάθε πολίτης και κάθε επιχείρηση θα μπορούν να συναλλάσσονται με μία μόνο Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ).

Ένωσης αλλά αρκεί μόνο το κράτος μέλος που εδρεύει ο υπεύθυνος επεξεργασίας δεδομένων ή ο επεξεργαστής ή όπου διεκπεραιώνεται το μεγαλύτερο στάδιο επεξεργασίας. [26]

Το GDPR επιδιώκει στην ενδυνάμωση και αρμονία του ιδιωτικού απορρήτου καθώς και στην χορήγηση ενός σταθερού πεδίου δράσης στις επιχειρήσεις που δραστηριοποιούνται στην Ευρώπη. Επίσης το GDPR μπορεί να διασφαλίσει όλα τα δεδομένα για την ταυτοποίηση ενός ατόμου όπως το όνομα και το επίθετο, ο τόπος διαμονής, η ημερομηνία γέννησης, ο αριθμός ταυτότητας, η διεύθυνση ηλεκτρονικού ταχυδρομείου (email), το πρωτόκολλο διαδικτύου (Internet Protocol) κ.ά. [16]

Με την εφαρμογή της νομοθεσίας GDPR, οι επιχειρήσεις που ασχολούνται με τη συγκέντρωση δεδομένων, θα χρειάζονται τη συγκατάθεση των πελατών τους. Οι πελάτες έχουν το νόμιμο δικαίωμα να ενημερώνονται όσο αφορά τις λεπτομέρειες που αποθηκεύονται για αυτούς και να αποσύρουν τη συγκατάθεσή τους για διατήρηση των προσωπικών τους δεδομένων στις επιχειρήσεις. Επίσης οι επιχειρήσεις επιβάλλεται να έχουν διαδικασίες ενημέρωσης των ατόμων, όταν παραβιάζονται τα δεδομένα τους και στη συνέχεια αυτοί έχουν το δικαίωμα να το αναφέρουν στον Επίτροπο Προστασίας Δεδομένων. [16]

2.2 HTTPS

Με το πέρας του χρόνου η ανθρωπότητα βρίσκεται περιτριγυρισμένη γύρω από πληροφορίες στις οποίες οι επιχειρήσεις και κάποιοι χρήστες επιβάλλεται να στηρίζονται στην προστασία και στο απόρρητο. Η ανάγκη για προστασία οδήγησε 6 μήνες από την ανάπτυξη του browser Mosaic το 1994 στη δημιουργία του SSL, Version 1.0 για την προσθήκη επιπλέον επιπέδου προστασίας στο HTTP. Με την πάροδο του χρόνου αναγνωρίστηκαν διάφορες ευπάθειες του SSL, που οδήγησαν στην συνεχή ανάπτυξη διαφόρων Version και πρωτοκόλλων. [32]

Το HTTPS (Hypertext Transfer Protocol Secure) είναι ένα πρωτόκολλο ασφάλειας (κρυπτογραφικό) στο διαδίκτυο που έχει τη δυνατότητα να διαβιβάζει προσωπικές πληροφορίες, οι οποίες είναι άκρως απόρρητες και προσφέρει ασφαλείς υπηρεσίες, όταν γίνονται συναλλαγές WWW (World Wide Web), από μία σύνδεση σε μία άλλη (εξασφαλίζει την πρόσβαση στο διαδίκτυο δηλαδή είναι ένα πρωτόκολλο επικοινωνίας HTTP μέσω μη ασφαλών δικτύων με την βοήθεια SSL/TLS). Το πρωτόκολλο αυτό έχει σαν βασικό μέλημα τους μηχανισμούς διαχείρισης κλειδιών, των πολιτικών ασφάλειας και κρυπτογραφικών αλγορίθμων, την επικοινωνία μεταξύ πελατών και εξυπηρετών/διακομιστών (server). Επίσης παρέχει κρυπτογράφηση, αυθεντικοποίηση και υπογραφή. Οι πληροφορίες κρυπτογραφούνται κατάλληλα σε μια σελίδα Web για να μην παραβιαστούν από μη εξουσιοδοτημένους χρήστες. Υλοποιείται στο επίπεδο της εφαρμογής (Application Layer) και το HTTP μαζί με το SSL (Secure Socket Layer) πρωτόκολλο συνθέτουν το HTTPS. Η αυθεντικότητα και η εμπιστευτικότητα είναι δύο πράγματα που διαβεβαιώνουν το HTTPS. Στην πραγματικότητα κάθε φορά που ο πελάτης θέλει να επικοινωνήσει με τον διακομιστή ιστού χρησιμοποιώντας το HTTPS θα πρέπει :

1. να μην μπορούν να αποκτηθούν δεδομένα HTTPS από κακόβουλο κεντρικό υπολογιστή στο δίκτυο.

2. να έχει ο διακομιστής τη σωστή ταυτότητα που προνοεί το πιστοποιητικό και

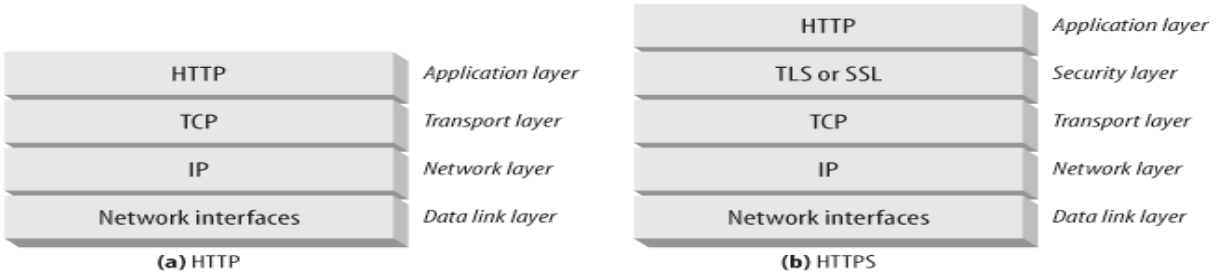
3. να μην υπάρχει η δυνατότητα σε κανένα κακόβουλο κεντρικό υπολογιστή μέσα στο διαδίκτυο να μπορέσει να μιμηθεί έναν πιστοποιημένο χρήστη με σκοπό να εισέλθει στον διακομιστή. Αυτά τα χαρακτηριστικά πρέπει να έχουν τόσο το πρόγραμμα περιήγησης όσο και ο διακομιστής για να είναι αξιόπιστοι.

Η ασφάλεια του HTTPS στηρίζεται εκτός από τα πρωτόκολλα TLS/SSL και σε μια σχέση εμπιστοσύνης η οποία είναι πολύπλοκη. Αυτή η σχέση εμπιστοσύνης γίνεται κατανοητή μέσα από ένα απλό παράδειγμα στο οποίο ένας χρήστης χρησιμοποιεί HTTPS για να αποκτήσει πρόσβαση σε έναν ιστότοπο ενός διακομιστή. Στο συγκεκριμένο παράδειγμα ο χρήστης θα πρέπει να έχει εμπιστοσύνη στο πρόγραμμα περιήγησης, το οποίο πρέπει να είναι ενημερωμένο στις πιο πρόσφατες ενημερώσεις, για να μην υπάρξουν θέματα ευπαθειών στην ασφάλεια, στον διακομιστή με τον οποίο το πρόγραμμα περιήγησης ανταλλάσσει πληροφορίες και στο πιστοποιητικό που το φανερώνει ο διακομιστής στον πελάτη. Επίσης πρέπει να εμπιστεύεται την Αρχή Πιστοποίησης τρίτου μέρους (certification authority) που επιβεβαιώνει ότι το πιστοποιητικό ανήκει πράγματι στον συγκεκριμένο διακομιστή/υποσύνολο διαδικτύου με διευθύνσεις (domain), δύναμη των κλειδιών, λειτουργία hash [hash function: παίρνει ως είσοδο αντικείμενα (objects) και εξάγει συμβολοσειρές ή αριθμούς] και κρυπτογραφικούς αλγόριθμους που χρησιμοποιούνται για την τοποθέτηση και μεταβίβαση των δεδομένων. [20]

Το πρωτόκολλο HTTPS δίνει το δικαίωμα σε ένα πρόγραμμα περιήγησης να ελέγξει κατά πόσο ένας διακομιστής Web είναι πραγματικός ή όχι και προσφέρει ένα ασφαλισμένο κανάλι, το οποίο είναι κρυπτογραφημένο ώστε να προστατευτούν τα δεδομένα που μεταβιβάζονται. Στην πραγματικότητα η ιστοσελίδα είναι μια συγκέντρωση δεδομένων διαφορετικών τμημάτων μεταξύ τους, όπως είναι ο κώδικας HTML, τα Cascading Style Sheets (CSS) τα οποία δίνουν μια αναφορά για το τι περιέχει η σελίδα, οι εικόνες ή διάφορα άλλα ενσωματωμένα μέσα κ.ά. Όλα αυτά τα δεδομένα μετακινούνται από τον διακομιστή Web και καταλήγουν στο πρόγραμμα περιήγησης διαμέσου των συνδέσεων TCP που είναι ανεξάρτητες μεταξύ τους. Όταν έχει ήδη ανοίξει η ιστοσελίδα, πατώντας σε κάποιο σύνδεσμο μέσα σε αυτήν ενεργοποιείται μια νέα ανταλλαγή δεδομένων μεταξύ του προγράμματος περιήγησης και του διακομιστή Web. Ο φυλλομετρητής (browser) έχει την ικανότητα να καθορίζει ποιο πρωτόκολλο θα συμπεριληφθεί για να γίνει η πραγματοποίηση της επικοινωνίας ανάλογα με τη διεύθυνση URL που θα επιλεγεί. Ένα πιστοποιητικό το οποίο είναι εγκεκριμένο προσφέρει μια σύνδεση TLS, παρέχει κρυπτογραφία του πρωτοκόλλου HTTPS για να διασφαλίσει το περιεχόμενο της ιστοσελίδας από την ύπαρξη παράνομης επεξεργασίας προσφέροντας στο πρόγραμμα περιήγησης αξιοπιστία ώστε να αποκτά αυτά που πραγματικά διαβίβασε ο διακομιστής. Μία σελίδα επιλέγει το πρωτόκολλο HTTPS ως το κατάλληλο πρωτόκολλο για να ψάξει τις αναγκαίες CSSs, εικόνες και στην συνέχεια δίνει το δικαίωμα στο πρωτόκολλο HTTPS να εκτελέσει μια υποβολή φόρμας που περιέχει δεδομένα. [21]

Με τη βοήθεια του HTTPS τα δεδομένα που μεταβιβάζονται από έναν πελάτη σε έναν διακομιστή ή το αντίθετο μετακινούνται διαμέσου μιας σύνδεσης, η οποία είναι κρυπτογραφημένη από ένα σημείο σε ένα άλλο χρησιμοποιώντας πιστοποιητικά TLS /SSL (Secure Sockets Layer) από ασφαλή φορέα (Αρχή Πιστοποίησης). Το πρωτόκολλο

SSL έχει σκοπό την επαλήθευση της ταυτότητας των διακομιστών (έλεγχος ταυτότητας από το ένα σημείο στο άλλο) και την εξακρίβωση ότι ο διακομιστής έχει την ικανότητα να αποκρυπτογραφήσει και να διαβάσει ορθά τις πληροφορίες (κρυπτογράφηση και ακεραιότητα των μηνυμάτων) που διαβίβασε ο πελάτης και αντίστροφα. [24] Σε πρακτικές εφαρμογές στο πρωτόκολλο SSL υπάρχουν αδυναμίες στις οποίες μπορεί να προκύψει επίθεση man-in-the-middle και έτσι προκύπτει κίνδυνος ασφάλειας σε συνδέσεις HTTPS. Η ζήτηση του HTTPS αυξάνεται συνεχώς λόγω του ότι έχει αυξηθεί και η αξία των πληροφοριών. Το HTTPS έχει τη δυνατότητα να διασφαλίζει τις μεταφορές χρημάτων και τις απόρρητες πληροφορίες από τη μία πλευρά στην άλλη (χρησιμοποιείται για ευαίσθητες επικοινωνίες) και χρησιμοποιείται κυρίως σε τμήματα που είναι αναγκαία η επαλήθευση ταυτότητας, για παράδειγμα η ηλεκτρονική τραπεζική (internet banking: υπηρεσίες που προσφέρουν οι τράπεζες μέσω διαδικτύου), οι υπηρεσίες και αγορές στην κοινωνική δικτύωση (συναλλαγές μέσω διαδικτύου). Οι επιχειρήσεις πλέον έχοντας στο μυαλό τους τις αυξημένες υποκλοπές, τις επιθέσεις (man-in the-middle) και τον χειρισμό που γίνεται στην κίνηση δικτύου, εφαρμόζουν το HTTPS για να διασφαλίσουν τις συνδέσεις που κάνουν από το ένα σημείο στο άλλο. [20] Οι διαφορές μεταξύ του πρωτόκολλου HTTP και HTTPS φαίνονται στο πιο κάτω σχήμα:



Σχήμα 2.1: Πρωτόκολλα δικτύου HTTP και HTTPS

Ένα αίτημα HTTPS μπορεί να ξεκινήσει με δύο τρόπους:

1. Συνήθειες των χρηστών: ένας χρήστης όταν εισέλθει σε ένα ιστότοπο HTTPS μέσα στο πρόγραμμα περιήγησης και πληκτρολογεί την διεύθυνση URL χωρίς να προσθέσει το https στην αρχή της γραμμής διεύθυνσης για παράδειγμα πληκτρολογεί την διεύθυνση hostname (π.χ www.google.com). Σε αυτήν την περίπτωση που δεν υφίσταται η διεύθυνση πρωτοκόλλου στην διεύθυνση URL τότε το πρόγραμμα περιήγησης εφαρμόζει το πρωτόκολλο HTTP για να συνδεθεί στον ιστότοπο. Όταν ο πελάτης πραγματοποιήσει μια σύνδεση HTTP και ο διακομιστής είναι ιστότοπος HTTPS τότε θα στείλει μήνυμα πίσω ανακατεύθυνσης HTTP. Στο πακέτο αυτό περιλαμβάνεται η κανονική διεύθυνση HTTPS που πρέπει να είναι στην πραγματικότητα δηλαδή https://hostname. Ο πελάτης παίρνει πίσω αυτό το πακέτο και το πρόγραμμα περιήγησης ξεκινάει μια καινούργια σύνδεση HTTPS.

2. Εφαρμογή στην πράξη: για την σύνδεση HTTP υπάρχει κάποιο κουμπί στην σελίδα για να ενεργοποιηθούν οι συνδέσεις HTTPS. Ένα απλό παράδειγμα για

την κατανόηση είναι όταν γίνεται προσπάθεια πρόσβασης σε ένα λογαριασμό ηλεκτρονικού ταχυδρομείου και επιλεγεί το κουμπί υποβολής το οποίο μεταδίδει το αναγνωριστικό (ID) και τον κωδικό πρόσβασης ενός χρήστη. Στην ουσία όταν γίνει αυτό ο πελάτης αρχίζει τις συνδέσεις HTTPS για να διασφαλίσει τα προσωπικά του δεδομένα.

Στην πρώτη περίπτωση οι χρήστες δεν καταλαβαίνουν την ουσιαστική διαφορά μεταξύ touhttp και https στην διεύθυνση URL. Στην δεύτερη περίπτωση που λαμβάνονται υπόψη τα γενικά έξοδα που συντελούν στην χειραψία SSL, οι σημαντικότερες πληροφορίες είναι αυτές που κρυπτογραφούνται και όχι όλες σε μια σύνδεση. Συνολικά οι ιστότοποι δεν συνηθίζουν κατά την διάρκεια μιας διαδικασίας να χρησιμοποιούν σύνδεση HTTPS για τον λόγο ότι είναι αργή από δύο μέχρι και εκατό φορές από την σύνδεση HTTP. Άρα στη υποβολή των έμπιστων προσωπικών πληροφοριών χρησιμοποιείται η σύνδεση HTTPS και οι άλλες υπηρεσίες χρησιμοποιούν την σύνδεση HTTP. Με αυτόν τον τρόπο η παράδοση του HTTPS URL βρίσκεται εγκατεστημένη μέσα στο μήνυμα HTTP παρά το γεγονός ότι το πρωτόκολλο HTTP είναι ανασφαλές προκαλώντας ευπάθειες στην ασφάλεια. [02]

Έχοντας στο μυαλό ότι το διαδίκτυο έχει εξαπλωθεί σε κάθε γωνιά του κόσμου οι πελάτες έχουν αρκετούς τρόπους και λόγους να αγοράσουν τα προϊόντα τους διαμέσου του διαδικτύου το λεγόμενο ηλεκτρονικό εμπόριο. Τα προϊόντα αυτά βρίσκονται σε ιστότοπους όπου οι πελάτες καλούνται να δώσουν κάποια προσωπικά δεδομένα για να δημιουργήσουν λογαριασμό ώστε να τα αγοράσουν. Έτσι καλείται επιτακτική ανάγκη αυτά τα δεδομένα να διασφαλιστούν σωστά και να μην πέσουν σε χέρια άλλων που θα τα εκμεταλλευτούν. [03]

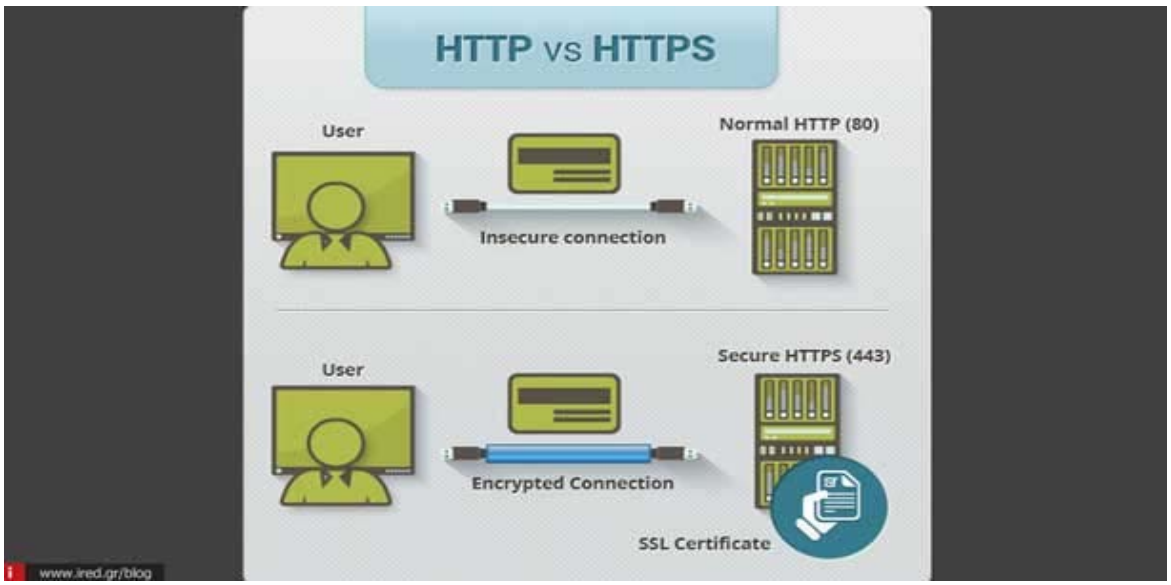
Το πρωτόκολλο HTTPS δίνει την δυνατότητα ασφάλειας και προστασίας των προσωπικών δεδομένων στο διαδίκτυο ώστε να μην μπορούν να τα υποκλέψουν. Έχοντας αυτό το προτέρημα να παρέχει ένα ασφαλές και αξιόπιστο κανάλι επικοινωνίας, το πρωτόκολλο αυτό χρησιμοποιείται στους ιστότοπους του ηλεκτρονικού εμπορίου. Όμως παρουσιάζει και ένα μειονέκτημα που αφορά τη μη εξουσιοδοτημένη πρόσβαση με την τεχνική του ενδιάμεσου ανθρώπου με SSL (Man-in-the-Middle). Αυτό οδηγεί στο συμπέρασμα ότι τα προσωπικά δεδομένα των πελατών είναι δυνατό να ανακτηθούν και να τύχουν εκμετάλλευσης [03]

Εικόνα 2.1: Πώς παρουσιάζεται το πρωτόκολλο HTTPS στο URL των ιστοσελίδων

2.2.1 Η ανάπτυξη του HTTPS

Το HTTPS δεν υπήρχε στις πρώτες μέρες του διαδικτύου. Αρχικά αναπτύχθηκε το πρωτόκολλο HTTP το 1965 και στην συνέχεια το πρωτόκολλο HTTPS από την κοινοπραξία CommerceNet την χρονική περίοδο 1994. Όπως φαίνεται για πολύ καιρό δεν το χρησιμοποιούσαν όμως στο σημερινό διαδίκτυο είναι αναγκαίο. Με την επέκταση του ηλεκτρονικού ταχυδρομείου διαμέσου των πανεπιστημίων, παρουσιάστηκε να είναι απαραίτητο για την διασφάλιση των καναλιών επικοινωνίας. Το διαδίκτυο εξακολούθησε να παρουσιάζει δείγματα εξέλιξης και με την εμφάνιση του ηλεκτρονικού εμπορίου οι τράπεζες άρχισαν να εφαρμόζουν το ασφαλές αυτό πρωτόκολλο στις μεθόδους πληρωμής των ηλεκτρονικών καταστημάτων. Όσο περνούν τα χρόνια το πρωτόκολλο HTTPS χρησιμοποιείτε ολοένα και περισσότερο.

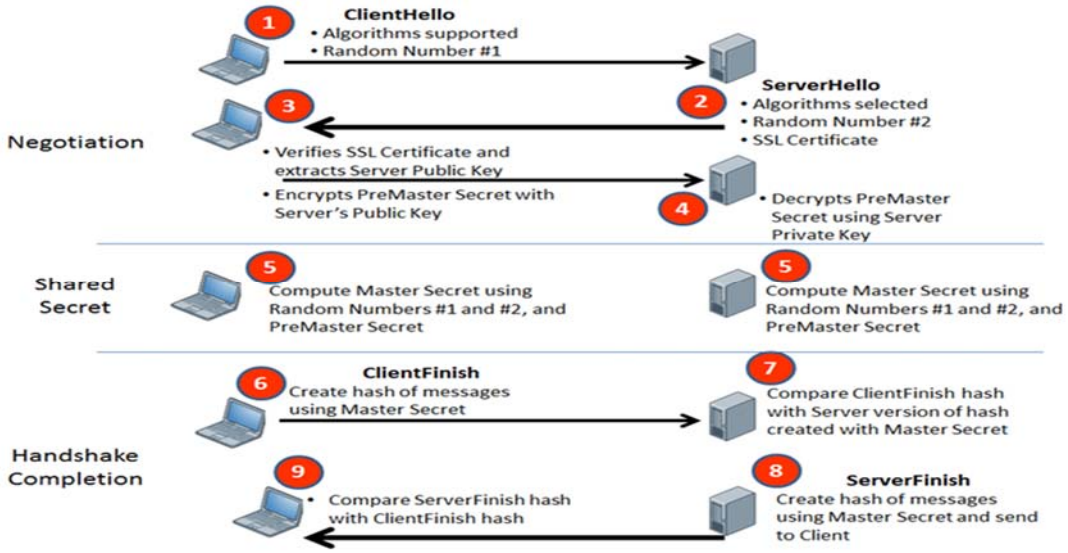
Στην σημερινή εποχή, η μορφή του πρωτοκόλλου διατυπώνει μια επέκταση του HTTP που έχει την ικανότητα να χρησιμοποιηθεί για να υποστηρίξει υπηρεσίες ασφάλειας από ένα σημείο σε ένα άλλο σε συναλλαγές WWW. Το HTTPS είναι ένα πρωτόκολλο που συνδυάζει το απλό πρωτόκολλο HTTP και τις ικανότητες που δίνει το πρωτόκολλο SSL. Το HTTPS στην αρχή εφάρμοζε το πρωτόκολλο SSL για να προστατεύσει την διάδοση δεδομένων. Το SSL όταν πρωτοεμφανίστηκε το χρησιμοποιούσαν στους ιστότοπους ηλεκτρονικού ταχυδρομείου, ηλεκτρονικού εμπορίου και σε portal πληρωμών. Έτσι ο σκοπός της δημιουργίας του SSL είναι να μην μπορεί να υλοποιηθεί σε ιστοσελίδες που δεν έχουν ασφάλεια ώστε να εξαπατήσει τους επισκέπτες και διαμέσου του πρόγραμμα περιήγησης να μεταφέρει κακόβουλο λογισμικό. Πλέον το SSL έχει αντικατασταθεί από το TLS το οποίο διασφαλίζει αρκετά καλύτερα το επίπεδο ασφάλειας προστασίας της ιδιωτικής ζωής. Το TLS διατίθεται στην νέα έκδοση 1.3. [12]



Εικόνα 2.2: Η σημασία των δύο πρωτοκόλλων HTTP και HTTPS

2.2.2 Κλειδί συνόδου https (session key)

Όταν γίνει μια καινούργια σύνδεση HTTPS ο πελάτης (περιηγητής) και ο διακομιστής επιβάλλεται να εκπληρώσουν μια συμφωνία/χειραψία (handshake) TLS/SSL που στην ουσία είναι οι λεπτομέρειες της περιόδου σύνδεσης μαζί με το TLS/SSL και των κρυπτογραφικών αλγόριθμων. Η επιδίωξη της συμφωνίας είναι να διασφαλιστεί ότι ο πελάτης και ο διακομιστής επικοινωνούν μεταξύ τους. [24] Τη στιγμή της διαδικασίας συμφωνίας ο διακομιστής εμφανίζει ένα ψηφιακό πιστοποιητικό X.509 που σκοπό έχει να φανερώσει την ταυτότητα του διακομιστή στον πελάτη. Στο συγκεκριμένο πιστοποιητικό παρουσιάζονται πληροφορίες όσον αφορά την ταυτότητα του διακομιστή (π.χ website domain name), την περίοδο ισχύος, το δημόσιο κλειδί και υπογράφεται από μια τρίτη οντότητα Αρχής Πιστοποίησης με ένα πιστοποιητικό ρίζας (R: root certificate).Έχοντας στην κατοχή αυτό το πιστοποιητικό, ο πελάτης μπορεί να εξετάσει αν η ταυτότητα είναι πράγματι η ίδια με αυτή του διακομιστή προορισμού, αν το πιστοποιητικό έχει λήξει και αν η ψηφιακή υπογραφή της αρχής προστασίας είναι έγκυρη. Στην περίπτωση που η εγκυρότητα είναι επιτυχής υπολογίζεται το κλειδί συνόδου και ανοίγει το κρυπτογραφημένο κανάλι επικοινωνίας μεταξύ των δύο άκρων. [20]



Σχήμα 2: Διάγραμμα χειραψίας/συμφωνίας SSL

Η επικοινωνία πραγματοποιείται την στιγμή που ένας πελάτης αποστέλλει ένα αίτημα στον διακομιστή προσδιορίζοντας μια URL διεύθυνση με πρωτόκολλο HTTPS χρησιμοποιώντας την θύρα 443. Ο διακομιστής ιστού (web server) ο οποίος είναι ο άμεσα υπεύθυνος για την υπηρεσία HTTPS ανταποκρίνεται στον πελάτη στέλλοντας ένα πιστοποιητικό. Στην συνέχεια το πρόγραμμα περιήγησης ιστού γνωστοποιεί το δημόσιο κλειδί του διακομιστή ιστού ο οποίος τοποθετεί και το πιστοποιητικό. Η χρησιμότητα του κλειδιού είναι να κωδικοποιήσει τις πληροφορίες που αποστέλλει ο πελάτης στον διακομιστή ιστού. Σε τεχνικής φύσεως η πρώτη πληροφορία που αποστέλλει ο πελάτης στον διακομιστή ιστού λέγεται κλειδί περιόδους σύνδεσης (session key) το οποίο θα χρησιμοποιηθεί από ένα σημείο και μετά για τη μεταφορά δεδομένων μεταξύ πελάτη και διακομιστή ιστού. Επομένως ο διακομιστής ιστού θα χρησιμοποιήσει το δικό του ιδιωτικό κλειδί για να μπορέσει να αποκωδικοποιήσει τις πληροφορίες (session key) που διαβιβάζει ο πελάτης. Σαν επακόλουθο αυτού που προκύπτει είναι ότι μόνο ο διακομιστής ιστού ή ο πελάτης κατανοεί το κλειδί σύνδεσης (session key) και έτσι η ακόλουθη μετάδοση είναι πλέον διασφαλισμένη. [03]

Κεφάλαιο 3
Μεθοδολογία

Η μεταπτυχιακή διατριβή διαχωρίζεται σε δύο ερευνητικές φάσεις. Στην πρώτη φάση της έρευνας θα χρησιμοποιηθεί ένας συνδυασμός ερευνητικών σχεδιασμών της ποιοτικής και ποσοτικής προσέγγισης. Αυτές οι δύο προσεγγίσεις λέγονται μικτές μέθοδοι στις οποίες συλλέγουν ποσοτικά (quantitative: αριθμητικά δεδομένα) αλλά και ποιοτικά (qualitative: κείμενο ή εικόνα) δεδομένα. Ο συνδυασμός των δύο μεθόδων δίνει μια πιο ξεκάθαρη εικόνα για την καλύτερη κατανόηση στο ερευνητικό πρόβλημα. Η συγκεκριμένη μέθοδος είναι μια διαδικασία ώστε να μαζευτούν, να συγκεντρωθούν, να αναλυθούν και να γίνει ένας συνδυασμός των δύο μεθόδων σε μια μόνο μελέτη ή σε μια σειρά μελετών πολλών φάσεων.

Η ποσοτική έρευνα εστιάζει περισσότερο στο να καθοριστεί η έκταση του προβλήματος, ζητήματος ή φαινομένου ενώ η ποιοτική έρευνα προσπαθεί να δώσει έμφαση στην διερεύνηση του προβλήματος, θέματος ή φαινομένου. Η ποσοτική έρευνα αναφέρεται στη συστηματική διερεύνηση φαινομένων με στατιστικές μεθόδους και αριθμητικά δεδομένα. Χρησιμοποιείται συνήθως αντιπροσωπευτικό δείγμα παρατηρήσεων επιδιώκοντας τα αποτελέσματα να γενικευτούν στον ευρύτερο πληθυσμό. Η συλλογή δεδομένων μπορεί να κατορθωθεί με ερωτηματολόγια, κλίμακες κλπ. Είναι μια μέθοδος που συγκεντρώνει αξιόπιστα και έγκυρα στοιχεία που οδηγούν σε γενικεύσιμα συμπεράσματα. [31]

Τα χαρακτηριστικά της ποσοτικής έρευνας εξηγούνται πιο κάτω μέσα από τα στάδια στη διαδικασία της έρευνας:

1. Ο προσδιορισμός του ερευνητικού προβλήματος είναι επικεντρωμένος στην περιγραφή και στην εξήγηση.

2. Η ανασκόπηση της βιβλιογραφίας παίζει σημαντικό ρόλο, χρειάζεται αιτιολόγηση για το ερευνητικό πρόβλημα και συγκεκριμένη αναφορά στην ανάγκη για τη μελέτη.

3. Ο προσδιορισμός του σκοπού είναι συγκεκριμένος, δομημένος και τα δεδομένα είναι μετρήσιμα καθώς και παρατηρήσιμα.

4. Η συγκέντρωση των δεδομένων γίνεται με προκαθορισμένα εργαλεία, περιέχει αριθμητικά (αριθμοποιημένα) δεδομένα και μεγάλο αριθμών ατόμων.

5. Η ανάλυση και ερμηνεία των δεδομένων γίνεται με στατιστική ανάλυση, με περιγραφή τάσεων /σύγκριση ομάδων ή σχέσεις ανάμεσα σε μεταβλητές και σύγκριση των αποτελεσμάτων με προβλέψεις όπως και με προηγούμενες μελέτες.

6. Η αναφορά και αξιολόγηση της έρευνας είναι τυποποιημένη, καθορισμένη, αντικειμενική και αμερόληπτη. [31]

Οι ερευνητικοί σχεδιασμοί είναι διαδικασίες που συμπεριλαμβάνονται στα τελευταία τρία στάδια της διαδικασίας - έρευνας που είναι η συγκέντρωση δεδομένων, η ανάλυση δεδομένων και συγγραφή αναφοράς. Στα είδη των ερευνητικών σχεδιασμών είναι οι πειραματικοί (experimental) και συσχετικοί (correlational) σχεδιασμοί όπου σε κάποιο βαθμό εφαρμόζονται στην παρούσα μεταπτυχιακή μελέτη. Οι πειραματικοί σχεδιασμοί είναι διαδικασίες ποσοτικής έρευνας και αξιολογείται δίνοντας σε μια ομάδα ένα σύνολο δραστηριοτήτων. Οι συσχετικοί σχεδιασμοί περιλαμβάνουν και αυτοί διαδικασίες ποσοτικής έρευνας στις οποίες οι μελετητές υπολογίζουν το βαθμό της συσχέτισης (ή σχέσης) ανάμεσα σε δύο ή πιο πολλές μεταβλητές. Επίσης εφαρμόζεται η στατιστική διαδικασία της συσχετικής ανάλυσης και ο βαθμός συσχέτισης, αντικατοπτρίζεται ως αριθμός που παρουσιάζει αν οι δύο μεταβλητές σχετίζονται μεταξύ τους.

Η δειγματοληπτική έρευνα (survey research) είναι ένας από τους πιο γνωστούς ερευνητικούς σχεδιασμούς ποσοτικής έρευνας, στην οποία με την χρησιμοποίηση των ερωτηματολογίων (survey instrument) συγκεντρώνει ποσοτικά δεδομένα. Στην έρευνα αυτή συμμετέχει ένα δείγμα ή ολόκληρος ο πληθυσμός των ανθρώπων, η ανάλυση των δεδομένων υλοποιείται με στατιστικές τεχνικές και απεικονίζει συνήθως τις στάσεις, απόψεις, συμπεριφορές ή τα γνωρίσματα του πληθυσμού.

Πιο συγκεκριμένα θα διεκπεραιωθεί μια σειρά από ηλεκτρονικά ερωτηματολόγια στον επιχειρηματικό κόσμο της Κύπρου, με σκοπό τη συλλογή δεδομένων. Οι συνεντεύξεις και τα

ερωτηματολόγια είναι δύο κύρια εργαλεία για τη συγκέντρωση δεδομένων στην δειγματοληπτική έρευνα. Στην παρούσα μεταπτυχιακή μελέτη θα εφαρμοστούν ερωτηματολόγια διαδικτύου. Στο ερωτηματολόγιο οι συμμετέχοντες που θα πάρουν μέρος θα πρέπει να το συμπληρώσουν και στην συνέχεια θα το επιστρέψουν πίσω στον ερευνητή. Οι συμμετέχοντες στην διαδικασία αυτή έχουν τη δυνατότητα να απαντήσουν στις ερωτήσεις στις οποίες υπάρχουν επιλογές και δίνουν κάποια απαραίτητα προσωπικά ή δημογραφικά στοιχεία που θα ζητηθούν. Οι κύριοι τύποι ερωτηματολογίων είναι οι εξής: υπάρχουν τα είδη των ταχυδρομημένων και διαδικτύων. [31]

Στην δεύτερη φάση της έρευνας θα χρησιμοποιηθεί η βιβλιογραφία καθώς και η ιστοσελίδα Alexa (https://www.alexa.com) για να εντοπιστούν οι πιο δημοφιλείς ιστοσελίδες στην Κύπρο. Μετά θα εφαρμοστούν μέσω του λειτουργικού συστήματος Kali Linux οι εντολές sslscan και openssl για την εξεύρεση πληροφοριών, κυρίως πιστοποιητικών για τους ιστότοπους. Μέσω μεθοδολογιών και συγκεκριμένα ερωτηματολογίων διαδικτύου θα σχηματιστούν κάποια χρήσιμα αποτελέσματα τα οποία θα μας δείξουν κατά πόσο οι επιχειρήσεις στην Κύπρο είναι προετοιμασμένες στο θέμα ασφάλειας προστασίας των προσωπικών δεδομένων.

3.1 Μέγεθος Δείγματος

Η μελέτη γίνεται στη Κύπρο για την ικανοποίηση των ερευνητικών ερωτημάτων, λόγο γεωγραφικής θέσης και στο ότι βολεύει τον ερευνητή.

3.1.1 Μέγεθος Δείγματος ερωτηματολογίων

Ο πληθυσμός στόχος για τη συλλογή δεδομένων μέσω ερωτηματολογίου είναι οι εργαζόμενοι μικρομεσαίων επιχειρήσεων στη Κύπρο. Το τελικό δείγμα της έρευνας ήταν δείγμα ευχέρειας 55 επιχειρήσεων. Το δείγμα αυτό χρησιμοποιήθηκε για να διαπιστωθεί κατά πόσο ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων (GDPR) έχει ευαισθητοποιήσει τον επιχειρηματικό κόσμο στη Κύπρο για να συμμορφωθεί με τους κανονισμούς και έχει λάβει τα κατάλληλα μέτρα για την προστασία των προσωπικών δεδομένων. Επίσης εξακριβώνεται σε ποιες ιστοσελίδες των επιχειρήσεων γίνεται η χρησιμοποίηση του πρωτοκόλλου HTTPS.

3.1.2 Μέγεθος Δείγματος ιστοσελίδων

Στην παρούσα έρευνα η επιλογή του μεγέθους του δείγματος όπου θα εκτελεστούν οι εντολές sslscan και openssl για εντοπισμό και αξιολόγηση του πιστοποιητικού (certificate) έγινε με βάση τις top-50 ιστοσελίδες από άποψης επισκεψιμότητας όπως καθορίστηκε από την ιστοσελίδα Alexa.com. Το δείγμα των ιστοσελίδων είναι από κυπριακές ιστοσελίδες και είναι συνολικά 44.

Κεφάλαιο 4
Συλλογή Δεδομένων

Σε αυτό το κεφάλαιο περιγράφεται ο τρόπος με τον οποίο έχει γίνει η συλλογή δεδομένων. Όπως αναφέρθηκε και πιο πάνω η συλλογή δεδομένων χωρίζεται σε 2 στάδια. Στο πρώτο στάδιο θα αξιολογηθεί η χρήση του HTTPS σε κυπριακές ιστοσελίδες με την εφαρμογή των εντολών sslscan και openssl. Στην συνέχεια, στο δεύτερο στάδιο αναφέρονται τα ευρήματα που έχει επιφέρει η υλοποίηση του ερωτηματολογίου [ΒΛΕΠΕ ΠΑΡΑΡΤΗΜΑ Α.1] από 55 συμμετέχοντες που έχουν εκπροσωπήσει την επιχείρηση που εργάζονται.

Για την καλύτερη κατανόηση των πεδίων του πρωτοκόλλου HTTPS που θα εκτελεστούν με τις εντολές sslscan και openssl θα χρησιμοποιηθούν τα RFC που διαδίδονται από το IETF. Το IETF (Internet Engineering Task Force) είναι μια τεράστια ομάδα σχεδιαστών δικτύων, χειριστών, πωλητών και ερευνητών παγκόσμιας εμβέλειας και ασχολούνται με την εξέλιξη της αρχιτεκτονικής και την ομαλή λειτουργία όσον αφορά το διαδίκτυο. Επίσης είναι ο πιο διακεκριμένος οργανισμός προτύπων διαδικτύου, ο οποίος δημιουργεί ανοικτά πρότυπα διαμέσου ανοικτών διαδικασιών. Βρίσκεται δωρεάν στον ευρύ κοινό και είναι διατεθειμένη στην ιστοσελίδα https://tools.ietf.org. Η αποστολή και οι αρχές του IETF είναι να βελτιώσει το διαδίκτυο με την παραγωγή υψηλής ποιότητας, σχετικών τεχνικών εγγράφων που επιδρούν στον τρόπο με τον οποίο οι άνθρωποι σχεδιάζουν, εκμεταλλεύονται και διευθύνουν το διαδίκτυο. [17]

RFC 5280: Πιστοποιητικό X.509 έκδοσης 3: οι χρήστες που έχουν στην κατοχή τους δημοσία κλειδιά επιδιώκουν να είναι σίγουροι και ασφαλείς ότι το ιδιωτικό κλειδί ανήκει στο πραγματικό πρόσωπο ή σύστημα με το οποίο θα χρησιμοποιηθεί ένας μηχανισμός κρυπτογράφησης ή ψηφιακής υπογραφής. Η ασφάλεια αυτή εκπληρώνεται με την χρήση πιστοποιητικών δημοσίου κλειδιού και η δέσμευση για την ψηφιακή υπογραφή του κάθε πιστοποιητικού επικυρώνεται με την ύπαρξη μιας αξιόπιστης Αρχής Πιστοποίησης (CA: Certification Authority). Το πιστοποιητικό έχει περιορισμένη διάρκεια ζωής η οποία αναγράφεται στα περιεχόμενα της. Λόγω του ότι η υπογραφή και η επικαιρότητα ενός πιστοποιητικού μπορούν να ελεγχτούν ανεξάρτητα από έναν

πελάτη που χρησιμοποιεί πιστοποιητικό, τα πιστοποιητικά μπορούν να διανεμηθούν μέσω μη αξιόπιστων συστημάτων επικοινωνίας και διακομιστών.

Το ITU-T X.509 ή ISO/IEC 9594-8 δημοσιεύτηκε για πρώτη φορά το 1988 και προσδιορίζει μια τυποποιημένη μορφή πιστοποιητικού (X.509). Η μορφή πιστοποιητικού στο πρότυπο 1988 ονομάζεται έκδοση 1(v1). Όταν το X.500 αναθεωρήθηκε το 1993, προστέθηκαν ακόμη δύο πεδία που ήταν αποτέλεσμα της μορφής έκδοσης 2 (v2). Φαίνεται όμως οι εκδόσεις 1 και 2 ήταν ανεπαρκές για τον λόγο ότι χρειαζόταν περισσότερα πεδία για την διακίνηση των πληροφοριών. Έτσι αναπτύχθηκε από την ISO/IEC, ITU-U και ANSI X9 η έκδοση 3 (v3) X.509 η οποία είναι μια επέκταση του v2 προσθέτοντας πρόγνωση για πρόσθετα πεδία επέκτασης. Στην έκδοση v3 έχουν αναπτύξει τυποποιημένες επεκτάσεις για χρήση στο πεδίο επεκτάσεων οι οποίες είναι πολύ ευρείες όσον αφορά την εφαρμογή τους. Για να αναπτυχθούν οι υλοποιήσεις συστημάτων X.509 για χρήση στο διαδίκτυο απαιτούνται να καθοριστεί ένα προφίλ για χρήση των επεκτάσεων X.509 v3 προσαρμοσμένων για το διαδίκτυο. [17]

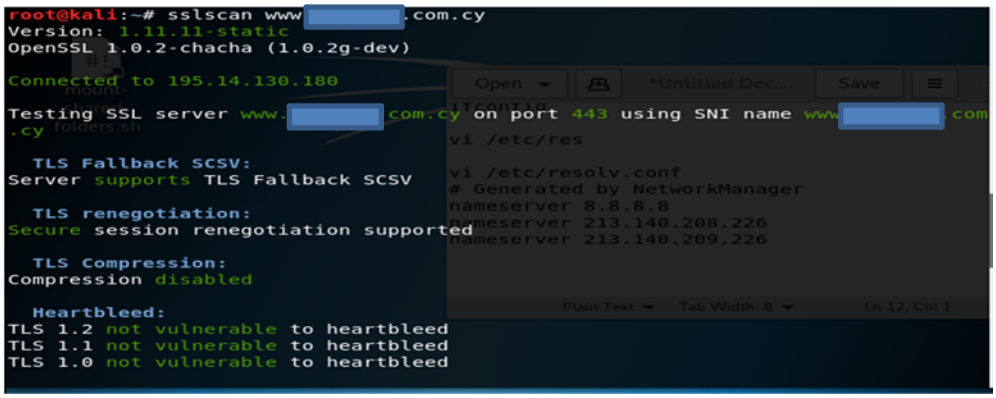
Όπως αναφέρθηκε και στο προηγούμενο κεφάλαιο θα χρησιμοποιηθεί ο ιστότοπος Alexa για να βρεθούν οι πιο δημοφιλές, από άποψης επισκεψιμότητας ιστοσελίδες της Κύπρου. Ο ιστότοπος (website) Alexa [ΒΛΕΠΕ ΠΑΡΑΤΗΜΑ Γ.1] βρίσκεται στην ιστοσελίδα https://www.alexa.com όπου ασχολείται με την αναλυτική διορατικότητα και αναπτύσσει υπηρεσίες ανάλυσης ιστού. Παρέχει πλούσια και σημαντικά εργαλεία ανάλυσης που αποσκοπούν στην απόκτηση γρήγορων αλλά και εύκολων πληροφοριών. Για αυτό έχει επιλεγεί στην παρούσα μεταπτυχιακή διατριβή και έχει χρησιμοποιηθεί για την εξεύρεση των πιο δημοφιλών ιστοσελίδων στην Κύπρο. Μέσα στην ιστοσελίδα Alexa έχει επιλέγει το σημείο που ονομάζεται top sites στην Κύπρο. [06]

Ακολούθως χρησιμοποιείτε το HTTrack για την τοπική αποθήκευση των ιστοσελίδων για περαιτέρω διερεύνηση. Το HTTrack είναι δωρεάν και ανοικτού κώδικα πρόγραμμα καθώς και εύκολο στην χρήση πρόγραμμα περιήγησης που βρίσκεται εκτός δικτύου (offline). Έχει την δυνατότητα να μεταφέρει τις ιστοσελίδες WWW (World Wide Web) από το διαδίκτυο σε ένα κατάλογο που βρίσκεται πάνω στον υπολογιστή δίνοντας την ευχέρεια να αποκτηθούν όλοι οι κατάλογοι, HTML, εικόνες και διάφορα άλλα αρχεία από τον διακομιστή στον υπολογιστή. Επίσης έχει την ικανότητα να οργανώνει την δομή σύνδεσης που είχε αρχικά ο ιστότοπος. Αυτό μπορεί να γίνει όταν ανοίξει μια σελίδα που αντικατοπτρίζεται μέσα στον πρόγραμμα περιήγησης που είναι εκτός δικτύου και θα υπάρξει δυνατότητα περιήγησης στον ιστότοπο σαν να βρίσκεται σε απευθείας σύνδεση. [15]

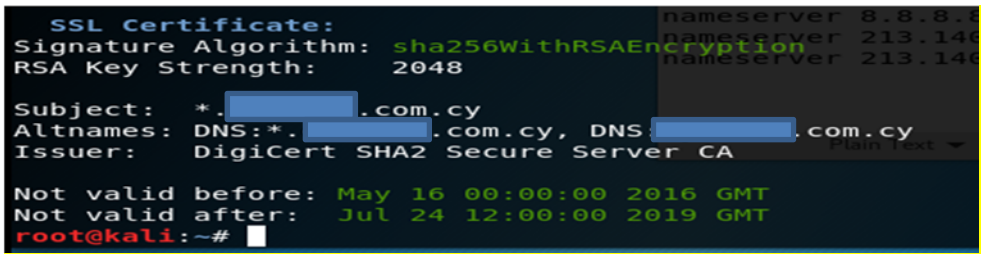
4.1 Ευρήματα κατά την εκτέλεση των εντολών sslscan και openssl

Διαμέσου του λειτουργικού συστήματος Kali Linux έχουν εκτελεστεί οι πιο κάτω εντολές για τον εντοπισμό πληροφοριών: sslscan hostname / openssl s_client -connect the.host.name:443 / openssl s_client -connect the.host.name:443 | openssl x509 -pubkey –noout. Το SSLScan είναι ένα ολοκληρωμένο εργαλείο το οποίο εκτελεί εντολές στο Kali Linux και χρησιμοποιείται για την αξιολόγηση της ασφάλειας SSL/TLS σε μια απομακρυσμένη υπηρεσία ιστού. Η εντολή sslsscan είναι ένα αποτελεσματικό πρόγραμμα στην C το οποίο δίνει το δικαίωμα να εντοπιστούν εκδόσεις SSL και κρυπτογραφικές σουίτες (cipher suites) συμπεριλαμβανομένου του ελεγκτή έκδοσης TLS. Επίσης εκτελεί ελέγχους για ευπάθειες όπως Heartbleed και POODLE.

Η εντολή για το SSL scan είναι: sslscan hostname (hostname: αντιπροσωπεύει την ιστοσελίδα). Πιο κάτω παρουσιάζεται ένα παράδειγμα ενός ιστότοπο [ΒΛΕΠΕ ΠΑΡΑΡΤΗΜΑ Β.1]:



Εικόνα 4.1: Αποτελέσματα κατά την διάρκεια εκτέλεσης της εντολής sslscan στον ιστότοπο

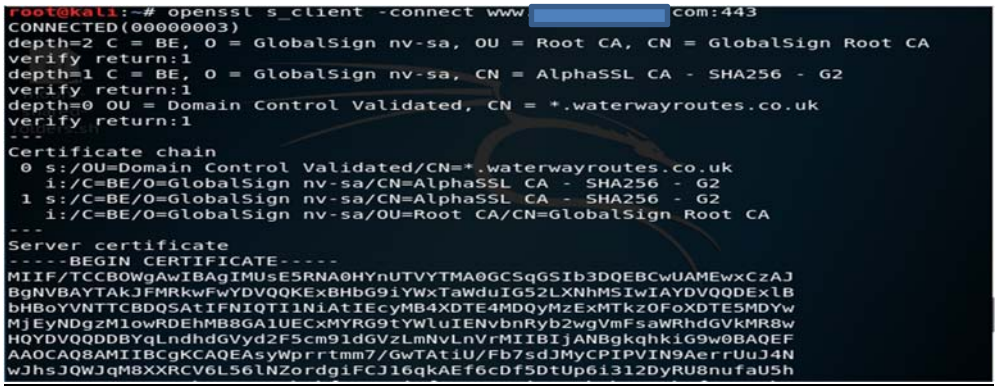


Εικόνα 4.2: Αποτελέσματα κατά την διάρκεια εκτέλεσης της εντολής sslscan στον ιστότοπο

Η εντολή openssl χρησιμοποιείται για την ασφαλή σύνδεση στον διακομιστή και στη δυνατότητα του πλήρους ελέγχου στο επίπεδο SSL/TLS. Για την σύνδεση με τον διακομιστή χρειάζεται η εντολή: openssl s_client -connect the.host.name:443.
Επεξήγηση της προηγούμενης εντολής: the.host.name: αντιπροσωπεύει τον ιστότοπο (website)

443 : αντιπροσωπεύει την θύρα (port).

Παρακάτω φαίνονται κάποιες πληροφορίες για το πιστοποιητικό του διακομιστή με το παράδειγμα του ιστότοπου (στην πρώτη γραμμή υπάρχει ο ιστότοπος και στην δεύτερη πληροφορίες για τον εκδότη). [ΒΛΕΠΕ ΠΑΡΑΡΤΗΜΑ Β.2]

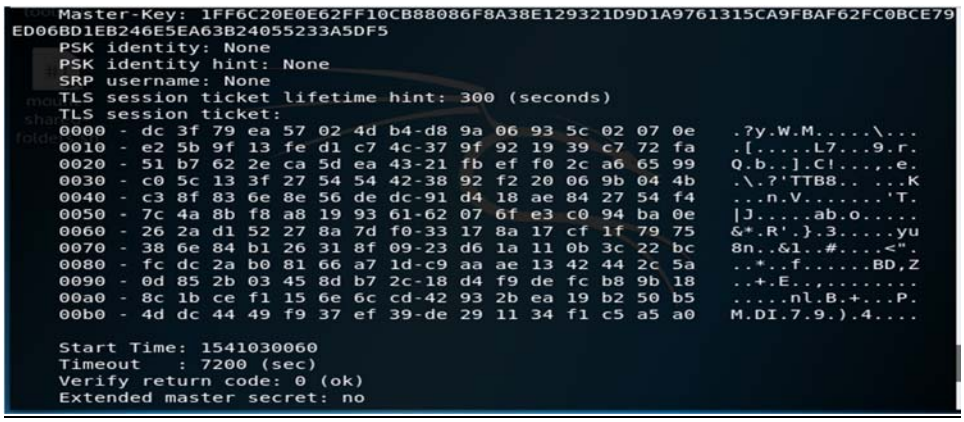


Εικόνα 4.3: Αποτελέσματα κατά την διάρκεια εκτέλεσης της εντολής openssl στον ιστότοπο

Εικόνα 4.4: Αποτελέσματα κατά την διάρκεια εκτέλεσης της εντολής openssl στον ιστότοπο

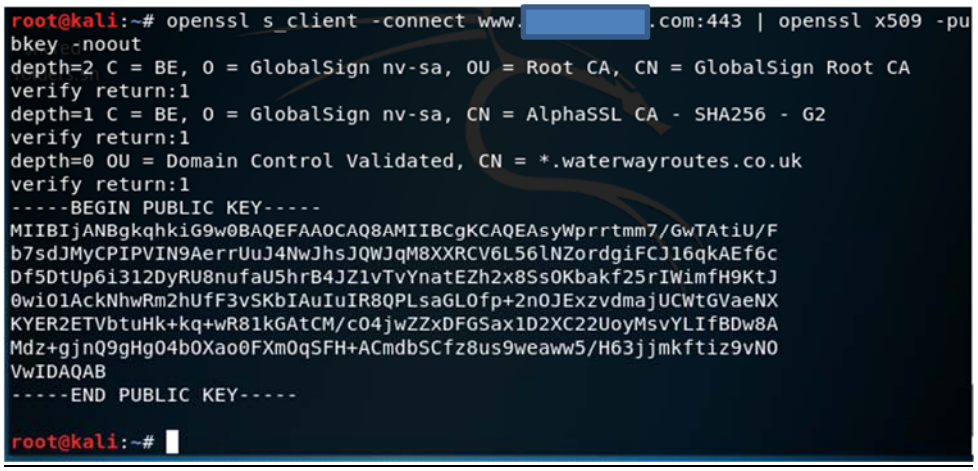
Πληροφορίες για την σύνδεση TLS (σημαντικά στοιχεία είναι η έκδοση πρωτοκόλλου TLS, η χρησιμοποίηση του cipher suite, οι εκδόσεις session ID και TLS session ticket).

Εικόνα 4.5: Αποτελέσματα κατά την διάρκεια εκτέλεσης της εντολής openssl στον ιστότοπο



Εικόνα 4.6: Αποτελέσματα κατά την διάρκεια εκτέλεσης της εντολής openssl στον ιστότοπο

Η πιο κάτω εντολή ελέγχει και επιβεβαιώνει τα πιστοποιητικά SSL και public key η οποία είναι: openssl s_client -connect the.host.name:443 | openssl x509 -pubkey –noout



Εικόνα 4.7: Αποτελέσματα κατά την διάρκεια εκτέλεσης της εντολής openssl στον ιστότοπο

4.2 Ερμηνεία των εντολών sslscan και openssl

Με την εκτέλεση των προηγούμενων εντολών στους ιστότοπους των επιχειρήσεων που επιλέχθηκαν έχουν καταγραφεί σημαντικές πληροφορίες και αποθηκευτεί σε ένα αρχείο στο πρόγραμμα excel. Η ερμηνεία των πληροφοριών παρουσιάζεται πιο κάτω

4.2.1 Αλγόριθμος υπογραφής (Signature algorithm)

Το πεδίο αλγόριθμου υπογραφής περιέχει το αναγνωριστικό για τον κρυπτογραφικό αλγόριθμο που χρησιμοποιείται από την Αρχή Πιστοποίησης για να υπογράψει αυτό το πιστοποιητικό. Το αναγνωριστικό αλγορίθμου χρησιμοποιείται για την αναγνώριση ενός κρυπτογραφικού

αλγορίθμου[10]. Ο αλγόριθμος υπογραφής αναφέρεται στην υπογραφή του πιστοποιητικού που έχει δημιουργήσει ο εκδότης. Αυτή η υπογραφή αποδεικνύει ότι ο εκδότης του πιστοποιητικού είναι ο πραγματικός από την στιγμή που η υπογραφή μπορεί να αποδειχθεί από το δημόσιο κλειδί του πιστοποιητικού που έχει στην κατοχή ο εκδότης. Στην παρούσα περίπτωση (εικόνα 4.2) οι αλγόριθμοι υπογραφής που χρησιμοποιούνται είναι: sha1/256/512WithRSAEncryption. Αυτό σημαίνει ότι ο εκδότης έχει το δημόσιο κλειδί RSA μέσα στο πιστοποιητικό του και το hash χρησιμοποιείται για την υπογραφή του φύλλου πιστοποιητικού από τον εκδότη που είναι το sha1/256/512. Το ecda-with-SHA256 είναι η ελλειπτική καμπύλη αλγόριθμου ψηφιακής υπογραφής (DSA) σε συνδυασμό με τον ασφαλές αλγόριθμο κατακερματισμού (hash) 256 (SHA256). Στην κρυπτογραφία ο αλγόριθμος ψηφιακής υπογραφής ελλειπτικής καμπύλης (ECDSA) προσφέρει μια παραλλαγή του αλγόριθμού ψηφιακής υπογραφής (DSA) που χρησιμοποιεί κρυπτογράφηση ελλειπτικής καμπύλης. Η συνάρτηση κατακερματισμού (hash) είναι οποιαδήποτε λειτουργία που μπορεί να χρησιμοποιηθεί για την χαρτογράφηση αυθαίρετου μεγέθους δεδομένα σε δεδομένα σταθερού μήκους. Οι τιμές που επιστρέφονται από μια συνάρτηση κατακερματισμού ονομάζονται τιμές hash. Το SHA (Secure hash algorithm) είναι ένας κρυπτογραφικός αλγόριθμος κατακερματισμού που χρησιμοποιείται για τον προσδιορισμό της ακεραιότητας ενός συγκεκριμένου τεμαχίου δεδομένων. Ο διάδοχος του SHA-1 είναι το SHA-2 με το SHA-1 να είναι ένα hash 160-bit ενώ το SHA-2 έχει διάφορα μήκη όπως το 256/512bit. Ο αλγόριθμος SHA-1 λόγω τις αδυναμίες που παρουσίασε (δεν είναι ασφαλισμένο) οδήγησε σε νέο πρότυπο το SHA-2. Στον πιο κάτω πίνακα φαίνονται οι διάφοροι αλγόριθμοι υπογραφής που έχουν εντοπιστεί και σε πόσους ιστότοπους έχουν εντοπιστεί:

Signature algorithm	sha1WithRSA Encryption	ecdsa-with-SHA256	sha256WithRSA Encryption	sha512WithRSA Encryption	Δεν εντοπίστηκαν
Ποσότητα ιστότοπων	4 (δεν είναι ασφαλισμένο)	5	24	1	10

Πίνακας 4.1: αλγόριθμος υπογραφής (signature algorithm)

4.2.2 Μέγεθος /Ισχύς κλειδιού RSA (RSA Key Strength)

Είναι το μέγεθος του κλειδιού για μια ισχυρή κρυπτογραφία χρησιμοποιώντας κρυπτογράφηση δημοσίων κλειδιών αντί για απλούς κωδικούς πρόσβασης. Αυτό αναφέρεται ως αυθεντικοποίηση του πιστοποιητικού όμως τα πιστοποιητικά είναι ένας τρόπος για να

χρησιμοποιηθεί η τεχνολογία των δημοσίων κλειδιών. Τα δεδομένα για να παραμείνουν εμπιστευτικά πρέπει τουλάχιστον να χρησιμοποιηθεί κλειδί με 2048-bits. Όμως για να διατηρηθούν για τις επόμενες δεκαετίες το RSA προτείνει μεγαλύτερο μέγεθος κλειδιού από το 2048 bits. Στον πίνακα 4.2 παρουσιάζονται τα μεγέθη των κλειδιών και σε πόσους ιστότοπους έχουν εμφανιστεί:

RSA Key Strength	2048	4096	Δεν εντοπίστηκαν
Ποσότητα ιστότοπων	28	1	15

Πίνακας 4.2: μέγεθος κλειδιού RSA

4.2.3 Εκδότης (Issuer)

Το πεδίο (τομέας) εκδότη καθορίζει την οντότητα που έχει υπογράψει και εκδώσει το πιστοποιητικό. Πρέπει να περιέχει ένα κενό διακεκριμένο όνομα (DN: Distinguished Name) και ορίζεται ως το όνομα τύπου X.501. Το όνομα περιγράφει ένα ιεραρχικό όνομα που αποτελείται από χαρακτηριστικά όπως όνομα χώρας και αντίστοιχες τιμές όπως Κύπρος. Ωστόσο πρέπει να είναι προετοιμασμένες για να λάβουν πιστοποιητικά με ονόματα εκδοτών που περιέχουν το σύνολο τύπων χαρακτηριστικών η οποία συνιστάται την υποστήριξη για πρόσθετους τύπους χαρακτηριστικών. Τα τυπικά σύνολα χαρακτηριστικών έχουν προσδιοριστεί από το X.500 (X.520) και οι εφαρμογές αυτές πρέπει να είναι έτοιμες σε αυτούς τους τύπους χαρακτηριστικών σε ονόματα εκδότη και υποκειμένου (το πεδίο θέματος προσδιορίζει την οντότητα που σχετίζεται με το δημόσιο κλειδί που είναι αποθηκευμένο στο πεδίο του δημόσιου κλειδιού του θέματος) : χώρα, οργάνωση, οργανική μονάδα, διακεκριμένος προσδιοριστής ονομασίας (distinguished name qualifier), όνομα κράτους ή επαρχίας (state or province name), συνηθισμένο όνομα (common name) και σειριακός αριθμός (serial number). Οι χρήστες των πιστοποιητικών πρέπει να είναι έτοιμοι να επεξεργαστούν τα πεδία διακριτικού ονόματος και εκδότη για την εκτέλεση αλυσιδωτών ονομασιών για επικύρωση διαδρομής πιστοποίησης. Η αλυσιδοποίηση ονόματος (name chaining) γίνεται σύμφωνα με το διακριτικό όνομα του εκδότη και του αντικειμένου σε ένα πιστοποιητικό της Αρχής Πιστοποίησης. Εάν τα ονόματα στο πεδίο του εκδότη και του θέματος σε ένα πιστοποιητικό ταιριάζουν σύμφωνα με τους κανόνες τότε το πιστοποιητικό εκδίδεται αυτόματα. [17]

Πιο κάτω αναφέρονται και εξηγούνται οι εκδότες πιστοποιητικών που έχουν εντοπιστεί στις 44 ιστοσελίδες όταν εκτελέστηκαν οι εντολές sslscan στο λειτουργικό σύστημα Kali Linux:
Thawte: είναι ένα ασφαλές, πιστοποιημένο πρωτόκολλο SSL όπως και μια αξιόπιστη, δημοφιλής Αρχή Πιστοποίησης (CA: Certificate Authority) για το πιστοποιητικό X.509 όπως είναι η Symantec, GeoTrust, RapidSSL και Comodo. Ιδρύθηκε το 1995 στην Νότια Αφρική, είναι θυγατρική της εταιρείας Symantec Group και ανήκει στην DigiCert Inc. Είναι η τρίτη μεγαλύτερη δημόσια Αρχή Πιστοποίησης στο διαδίκτυο με ποσοστό αγοράς 25% και προμηθεύει προϊόντα που έχουν να κάνουν με τα πιστοποιητικά δημοσίου κλειδιού. [29]

Comodo (μετονομάστηκε σε Sectigo): είναι μια επιχείρηση η οποία ιδρύθηκε το 1998, στο Ηνωμένο Βασίλειο, με έδρα το Clifton, New Jersey στις Ηνωμένες Πολιτείες. Δραστηριοποιείται στον τομέα της ασφάλειας στον κυβερνοχώρο και των ψηφιακών πιστοποιητικών το οποίο για ένα διάστημα ήταν ένας από τους μεγαλύτερους εκδότες πιστοποιητικών SSL. Έχει μερίδιο αγοράς πάνω από το 48% και παρέχει προϊόντα κρυπτογράφησης παγκόσμιας κλάσης (πιστοποιητικά SSL). [04]

cPanel, Inc. : είναι μια ιδιωτική επιχείρηση που ιδρύθηκε το 1997 και εδρεύει στο Χιούστον του Τέξας. Λειτουργεί ως θυγατρική του WebPros Holdco B.V και παρέχει λογισμικό φιλοξενίας ιστοσελίδων, cPanel και WHM (Webhost Manager) για να γίνονται αυτόματα οι λειτουργίες που είναι δύσκολες στους διακομιστές φιλοξενίας ιστού (web hosting servers) στις Ηνωμένες Πολιτείες. Το λογισμικό χωρίζεται σε δύο τμήματα διεπαφών. Το ένα τμήμα είναι το cPanel το οποίο είναι γραφικό ενός πίνακα ελέγχου μέσω διαδικτύου για τους ιδιοκτήτες ιστότοπων που έχει την δυνατότητα να μπορεί να γίνεται η χρήση λογαριασμών ιστότοπου και φιλοξενίας. Το άλλο τμήμα είναι το WHM το οποίο προσφέρει στους παρόχους φιλοξενίας ένα γραφικό περιβάλλον για να μπορούν να χρησιμοποιήσουν κάθε λογαριασμό σε ένα διακομοστή, στην διαμόρφωση υπηρεσιών και πακέτα ανάπτυξης κ.ά. Η επιχείρηση βοηθά ιδιοκτήτες που διαθέτουν ιστότοπους, παρόχους φιλοξενίας, κέντρα δεδομένων, διαχειριστές συστημάτων και προγραμματιστές. [08]

DigiCert Inc: Η DigiCert είναι μια ιδιωτική Αμερικάνικη Αρχή Πιστοποίησης που ιδρύθηκε το 2003 και εδρεύει στην Lehi, Utah στις Ηνωμένες Πολιτείες. Είναι μια αρχή έκδοσης πιστοποιητικών (CA) που βασίζεται στα πιστοποιητικά X.509 SSL και επαληθεύει την αυθεντικότητα των ασφαλών ιστότοπων για λογαριασμό ενός προγράμματος περιήγησης ιστού. Παρέχει υποδομές δημοσίου κλειδιού και συνήθως γίνονται πωλήσεις σε πιστοποιητικά

SSL για επικύρωση οργάνωσης (OV: organization validation) και εκτεταμένη επικύρωση (EV: extended validation). [09]

Let's Encrypt: είναι μια ελεύθερη, αυτοματοποιημένη και ανοικτή αρχή έκδοσης πιστοποιητικών (CA), που ιδρύθηκε το 2014 και εδρεύει στο Σαν Φρανσίσκο στις Ηνωμένες Πολιτείες Αμερικής. Η υπηρεσία αυτή παρέχεται από την Ομάδα Έρευνας για την Ασφάλεια στο Διαδίκτυο (ISRG: Internet Security Research Group) και προμηθεύει πιστοποιητικά X.509 με σκοπό την ασφαλή κρυπτογράφηση στο επίπεδο μεταφοράς (TLS: Transport Layer Protocol) χωρίς χρέωση. Το πιστοποιητικό αυτό έχει διάρκεια 90 μέρες και η διαδικασία είναι αυτοματοποιημένη στο θέμα της δημιουργίας, επικύρωσης, υπογραφή, εγκατάσταση και ανανέωση πιστοποιητικών. Αυτό κάνει πιο εύκολη την ρύθμιση της κρυπτογράφησης HTTPS, για την απόκτηση και εγκατάσταση των πιστοποιητικών. [19]

RapidSSL: Ιδρύθηκε το 1999 στις Ηνωμένες Πολιτείες και λειτουργεί από την GeoTrust Inc. Παρέχει ψηφιακά πιστοποιητικά δημοσίου κλειδιού και είναι μια Αρχή Πιστοποίησης επιτρέπει την κρυπτογράφηση SSL για την ασφάλεια του ιστότοπου. Ειδικεύονται στην γρήγορη έκδοση χαμηλού κόστους και δωρεάν πιστοποιητικών SSL. Η επωνυμία GeoTrust αγοράστηκε από τη Symantec και Verisign αλλά συμφώνησε να πωλήσει την επιχείρηση πιστοποιητικών (μαζί με την GeoTrust) στην επιχείρηση Thoma Bravo LLC. [01-11]

Terena (Trans-European Research and Education Networking Association): Ιδρύθηκε το 1986 και εδρεύει στο Άμστερνταμ της Ολλανδίας. Ήταν μια μη κερδοσκοπική ένωση ευρωπαϊκών εθνικών δικτύων έρευνας και εκπαίδευσης (NRENs: nation research and education networks). Ο σκοπός της ήταν η προβολή και ανάπτυξη μιας υψηλής ποιότητας διεθνούς υποδομής πληροφοριών και τηλεπικοινωνιών για καλύτερα αποτελέσματα στον τομέα της έρευνας και της εκπαίδευσης. Αρχικά το 1986 ονομαζόταν Réseaux Associés pour la Recherche européenne (RARE) και στη συνέχεια το 1994 άλλαξε το όνομά της σε TERENA. Αργότερα το 2015 μετονομάστηκε GÉANT. [28]

Starfield Technologies: Ιδρύθηκε το 2004 στις Ηνωμένες Πολιτείες και ανήκει στο GoDaddy. Είναι μια επιχειρηματική οντότητα που σχετίζεται με το GoDaddy η οποία είναι Αμερικανικής προέλευσης επιχείρηση και οι αρμοδιότητες της σχετίζονται με την καταχώρηση τομέα στο διαδίκτυο (internet domain registrar) και φιλοξενίας ιστοσελίδων (web hosting). Επίσης ασχολείται και στον τομέα των πωλήσεων η οποία προωθεί λογισμικά και υπηρεσίες σε

διαδικτυακές επιχειρήσεις . Η Starfield δραστηριοποιείται στην έρευνα και των υπηρεσιών του GoDaddy διαμέσου του διαδικτύου, δημιουργεί τεχνολογίες και εργαλεία υποστήριξης της επιχείρησης καθώς και των πελατών της. [25]

Πιο κάτω παρουσιάζονται δύο πίνακες με τις ονομασίες των εκδοτών που έχουν εντοπιστεί και αναφέρεται σε πόσους ιστότοπους έχουν βρεθεί, πότε ιδρύθηκαν, πού εδρεύουν και τις υπηρεσίες που παρέχουν.

Issuer	COMODO RSA Domain Validation Secure Server CA & COMODO ECC Domain Validation Secure Server CA 2	cPanel, Inc.	Cronus & Parallels Panel & Ιστοσελίδα ενός οργανισμού	DigiCert SHA2 Extended Validation Server CA & DigiCert SHA2 Secure Server CA	Thawte EV RSA CA 2018 & Thawte TLS RSA CA G1
Ποσότητα ιστότοπων	4 (COMODO RSA) 5 (COMODO ECC)	2	Cronus & Parallels Panel (έχουν τερματιστεί) Ιστοσελίδα ενός οργανισμού (έχει υπογράψει η ίδια επιχείρηση το πιστοποιητικό self-signed)	1 (Digicert SHA2 Extended) 5 (Digicert SHA2 Secure)	1 (Thawte EV) 1 (Thawte TLS)
Πότε Ιδρύθηκε	1998 στο Ηνωμένο Βασίλειο	1997		2003	1995
Έδρα	Clifton, New Jersey στις Ηνωμένες Πολιτείες	Χιούστον, Τέξας		Lehi, Utah Ηνωμένες Πολιτείες	Νότια Αφρική
Υπηρεσίες	Εκδίδει SSL και άλλα ψηφιακά πιστοποιητικά	Παρέχει λογισμικό φιλοξενίας ιστοσελίδεων, cPanel, WebHost Manager, βοηθά ιδιοκτήτες που διαθέτουν ιστότοπους, παρόχους φιλοξενίας, κέντρα δεδομένων, διαχειριστές συστημάτων και προγραμματιστές		Ασφάλεια στο διαδίκτυο και υποδομή δημοσίου κλειδιού	Πιστοποιητικά δημοσίου κλειδιού

Πίνακας 43: Εκδότες

Issuer	Let's Encrypt Authority X3	RapidSSL RSA CA 2018	Starfield Secure Certification Authority & Starfield Secure Certificate Authority – G2	Σε κάποιες ιστοσελίδες δεν εντοπίστηκαν οι εκδότες τους	TERENA SSL CA 3 & TERENA SSL High Assurance CA 3
Ποσότητα ιστότοπων που έχουν τον συγκεκριμένο εκδότη	4	1	1 (Starfield Secure Certificate Authority) 2 (Starfield Secure Certificate Authority – G2)	10	2 (TERENA SSL CA 3) 3 (TERENA SSL High Assurance CA 3)
Πότε Ιδρύθηκε	18 Νοεμβρίου, 2014	1999	2004		1986
Έδρα	Σαν Φρανσίσκο, Καλιφόρνια, Ηνωμένες Πολιτείες	Ηνωμένες Πολιτείες	Ηνωμένες Πολιτείες		Άμστερνταμ, Ολλανδίας
Υπηρεσίες	Παρέχει πιστοποιητικά X.509 για ασφαλή κρυπτογράφηση στο επίπεδο μεταφοράς (TLS)	Ψηφιακά πιστοποιητικά δημοσίου κλειδιού	Έρευνα και των υπηρεσιών του GoDaddy μέσω διαδικτύου, αναπτύσσοντας τεχνολογίες και εργαλεία υποστήριξης της επιχείρησης και των πελατών της		προβολή και ανάπτυξη μιας υψηλής ποιότητας διεθνούς υποδομής πληροφοριών και τηλεπικοινωνιών

Πίνακας 4.4: Εκδότες

4.2.4 Χρονική Περίοδος που βρίσκονται σε ισχύ τα πιστοποιητικά (Not valid before / after)

Στον πιο κάτω πίνακα παρουσιάζονται τα αποτελέσματα για τα πιστοποιητικά τα οποία είναι έγκυρα και μη. Σε μερικές περιπτώσεις όπως φαίνεται δεν εντοπίστηκαν.

Not valid before/after	Έγκυρα	Άκυρα	Δεν εντοπίστηκαν
Ποσότητα ιστότοπων	31	3	10

Πίνακας 4.5: Πιστοποιητικά έγκυρα, άκυρα και κάποια δεν εντοπίζονται

4.2.5 Παρατηρήσεις που έγιναν μετά την εκτέλεση των εντολών sslscan και openssl

Πιο κάτω θα αναφερθούν οι παρατηρήσεις (observations) κατά την διάρκεια εκτέλεσης της εντολής του sslscan και στην εξεύρεση του δημοσίου κλειδιού (discovery public key) που εκτελέστηκε με την εντολή openssl. Όλα αυτά θα αναλυθούν στο κεφάλαιο 5: Αποτελέσματα.
Παρατηρήσεις που σχηματίστηκαν μετά την ολοκλήρωση της εντολής sslscan: η εκτέλεση του sslscan έγινε με την εντολή sslscan <hostname>

1. Session renegotiation not supported

2. Server does not support TLS Fallback SCSV

3. Could not open a connection to host <hostname> (212.31.118.26) on port 443

Παρατηρήσεις που σχηματίστηκαν μετά την ολοκλήρωση της εντολής openssl: η εξεύρεση των δημοσίων κλειδιών έγινε με τις δύο πιο κάτω εντολές: openssl s_client -connect the.host.name:443 και openssl s_client -connect the.host.name:443 | openssl x509 -pubkey –noout

1. Verification error: unable to verify the first certificate/unable to get local issuer certificate

2. No peer certificate available

3. Secure renegotiation is not supported

4. Unable to load certificate/Expecting: trusted certificate

5. Verification error: self-signed certificate

6. Verification error: certificate has expired

4.3 Συλλογή δεδομένων από το ερωτηματολόγιο

Σε αυτήν την μεταπτυχιακή διατριβή χρησιμοποιήθηκε το ερωτηματολόγιο με την μέθοδο της ποσοτικής έρευνας σε διάφορες επιχειρήσεις. Οι λόγοι επιλογής του ερωτηματολογίου καθορίστηκαν πιο πάνω στο κεφάλαιο 3 Μεθοδολογία. Το συνηθέστερο μέσο συλλογής δεδομένων στις ποσοτικές ερευνητικές προσεγγίσεις είναι το ερωτηματολόγιο το οποίο στη συνέχεια θα αναλυθεί μέσα από τη στατιστική επεξεργασία των δεδομένων. Στο ερωτηματολόγιο έχουν τοποθετηθεί συγκεκριμένα σύντομα ερωτήματα και τα δεδομένα που θα συγκεντρωθούν από τους συμμετέχοντες μπορούν να εκφραστούν ποσοτικά. Η ανάλυση των αριθμών θα γίνει με τη χρησιμοποίηση της στατιστικής (η έρευνα διεξάγεται με αντικειμενικό τρόπο). Έχουν πάρει μέρος άντρες και γυναίκες ηλικίας 18 μέχρι 60 χρονών και από όλα τα είδη επιχειρήσεων. Περιλαμβάνει κλειστές ερωτήσεις που συνοδεύονται από προκαθορισμένες απαντήσεις και όχι διατύπωσης στάσεων και απόψεων, γιατί απαιτείται περισσότερος χρόνος και σκέψη για να απαντηθούν. [ΒΛΕΠΕ ΠΑΡΑΡΤΗΜΑ Α.1]

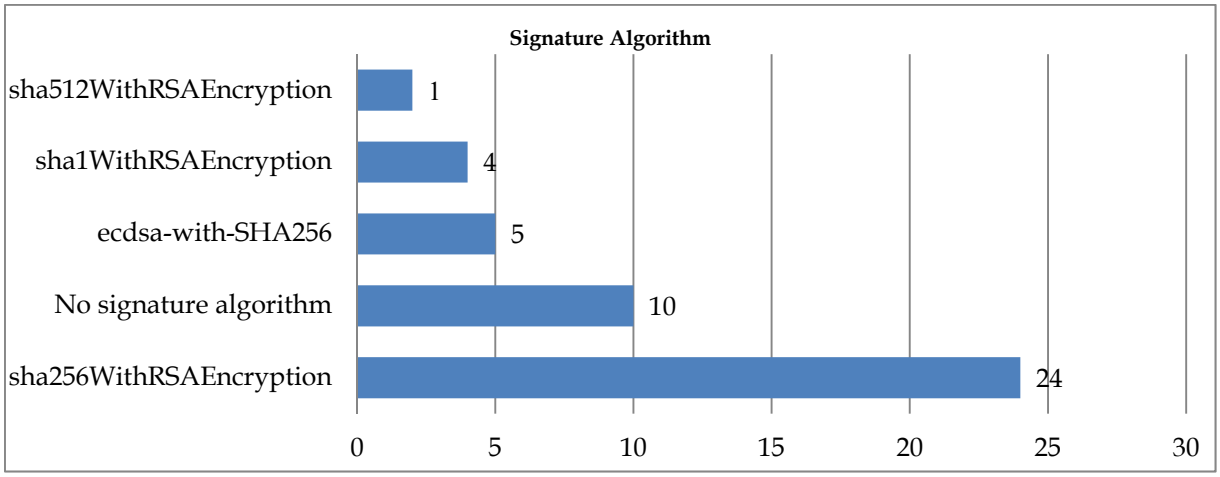
Κεφάλαιο 5
Αποτελέσματα

Για την εξεύρεση χρήσιμων πληροφοριών ώστε να βγουν σημαντικά αποτελέσματα έχουν πραγματοποιηθεί μια σειρά από εντολές στο λειτουργικό σύστημα Kali Linux και το ερωτηματολόγιο. Οι εντολές που έχουν χρησιμοποιηθεί όπως έχει αναφερθεί προηγουμένως είναι το sslscan και το opensslscan στους ιστότοπους των επιχειρήσεων με σκοπό να διαπιστωθεί κατά πόσο τηρούνται οι ανάλογες ασφάλειες. Το ερωτηματολόγιο πραγματοποιήθηκε σε ένα αριθμό ανθρώπων με ερωτήσεις επιλογών στο θέμα την νομοθεσίας του GDPR, τρόπους προστασίας των προσωπικών δεδομένων (περισσότερο τεχνικά χαρακτηριστικά) και για το πρωτόκολλο HTTPS.

5.1 Αποτελέσματα κατά την διαδικασία των εντολών sslscan και openssl

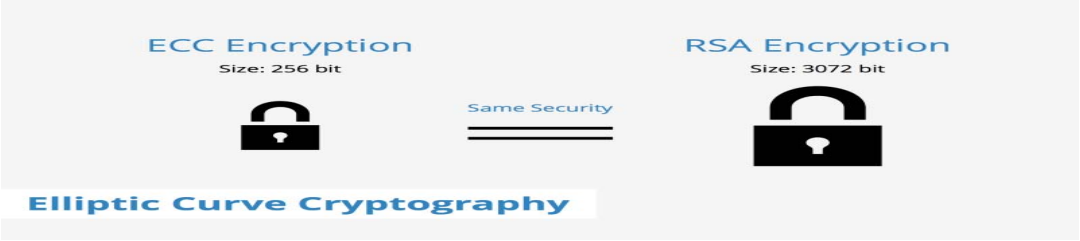
Μετά την ολοκλήρωση των διαδικασιών εφαρμογής των εντολών έχουν αναλυθεί και βγει κατάλληλα συμπεράσματα τα οποία θα αναφερθούν πιο κάτω κατά κατηγορία.

5.1.1 Αλγόριθμος υπογραφής (Signature algorithm)



Σχήμα 5.1: Αλγόριθμος υπογραφής

Τα αποτελέσματα που προκύπτουν από τον πίνακα 5.1 είναι ότι 24 από τις 44 ιστοσελίδες χρησιμοποιούν τον αλγόριθμο υπογραφής sha256WithRSAEncryption (είναι ο πιο δημοφιλής). Ο αλγόριθμος 256RSA είναι 10 φορές πιο ακριβός για να δημιουργηθεί μια υπογραφή από το ecdsa-with-SHA256 που το χρησιμοποιούν μόνο 5 ιστοσελίδες. Επίσης με τη χρησιμοποίηση του ECDSA μπορεί να υπάρξει ακριβώς το ίδιο επίπεδο ασφάλειας με το 256RSA αλλά με μικρότερο αριθμό κλειδιών. Τα μικρότερα κλειδιά είναι πολύ καλύτερα από τα μεγάλα λόγω του ότι οι αλγόριθμοι είναι γρηγορότεροι στη δημιουργία υπογραφών (εκτελώντας υπολογιστικές πράξεις με τα μικρότερα κλειδιά παρουσιάζουν και μικρότερους αριθμούς). Τα μικρότερα δημόσια κλειδιά έχουν ως αποτέλεσμα μικρότερα πιστοποιητικά και έτσι η ζήτηση των δεδομένων θα είναι μικρότερη όταν εκτελεστεί μια κανονική διαδικασία για να δημιουργηθεί μια σύνδεση TLS. Αυτό θα έχει ως επακόλουθο ταχύτερες συνδέσεις και ταχύτερους χρόνους φόρτωσης στους ιστότοπους. Έτσι στους διακομιστές στους οποίους χρησιμοποιείται το πιστοποιητικό ECDSA μειώνεται το κόστος λειτουργίας του ιδιωτικού κλειδιού κατά 9,5 φορές εξοικονομώντας πολλούς κύκλους CPU [10]. Όμως το ECDSA είναι πιο αργό από το RSA στην επαλήθευση της υπογραφής όπως και τα πιστοποιητικά RSA είναι παλιά, δοκιμασμένης τεχνολογίας πράγμα σημαντικό από πλευράς ασφάλειας. Ένας ακόμη λόγος που οι ιστότοποι υστερούν να υλοποιήσουν καινούργιους αλγόριθμους όπως είναι το ECDSA είναι ότι επιθυμούν να διατηρήσουν υποστήριξη για προγράμματα περιήγησης παλαιού τύπου. Ο αλγόριθμος RSA έχει την ικανότητα να χρησιμοποιηθεί για κρυπτογράφηση και ψηφιακή υπογραφή, ενώ το ECDSA μπορεί να χρησιμοποιηθεί μόνο για υπογραφή. Για το σπάσιμο του κλειδιού RSA χρειάζεται ο παράγοντας (factor) δύο μεγάλων αριθμών. Στην περίπτωση ECDSA για το σπάσιμο κλειδιού απαιτείται να βρεθεί ο διακριτικός λογάριθμος (discrete logarithm) μεταξύ δύο σημείων στην ελλειπτική καμπύλη (elliptic curve), το οποίο δεν έχει πραγματοποιηθεί ακόμη. Η κρυπτογραφία ελλειπτικής καμπύλης είναι μια εναλλακτική προσέγγιση στην κρυπτογραφία δημοσίου κλειδιού έναντι του προτύπου RSA, ίσως επειδή το ECDSA δεν είναι μια τεχνολογία δοκιμασμένη όσο το RSA και το γεγονός ότι υπάρχουν κάποια ερωτήματα στο θέμα της συμβατότητας (αν μπορεί να χρησιμοποιηθεί σε λειτουργικά συστήματα και στα τρέχων προγράμματα περιήγησης). [22]



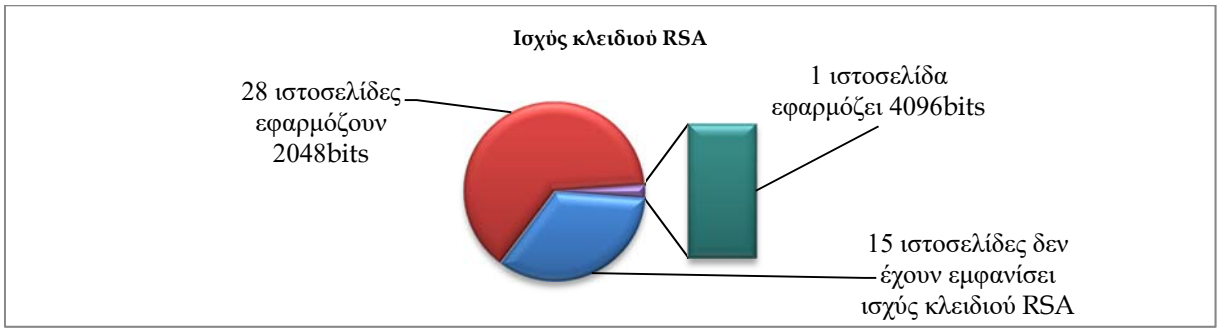
Εικόνα 5.1: Κρυπτογραφία ελλειπτικής καμπύλης

Υπάρχει μια ιστοσελίδα που εντοπίστηκε η οποία χρησιμοποιεί 256RSA 4096 bit. Στην περίπτωση αυτή το 4096 δεν είναι ασφαλέστερο από το 2048 bit που κανονικά θα έπρεπε και η αιτία είναι ότι η Αρχή Πιστοποίησης (CA) δεν παρέχει 4096 bit RSA Keychain. Επίσης έχοντας δυο φορές μεγαλύτερο αριθμό για το ιδιωτικό κλειδί του RSA, αυτό που τελικά επιτυγχάνεται είναι να μειωθεί περίπου 6 με 7 φορές η απόδοση της χειραψίας (handshake) TLS. Οπότε στο θέμα ασφάλεια η επιλογή του ECDSA φαντάζει πολύ καλύτερη. [22]

Ο αλγόριθμος υπογραφής sha512WithRSAEncryption είναι το ίδιο ασφαλές όπως και το sha256WithRSAEncryption το οποίο χρησιμοποιείται μόνο από μια ιστοσελίδα (δεν παράγονται συγκρούσεις ούτε στο ένα αλλά ούτε στο άλλο οπότε η ασφάλεια είναι η ίδια). Ο λόγος που το 256RSA είναι δημοφιλέστερο είναι ότι είναι πιο μικρό, χρειάζεται μικρότερο εύρος ζώνης για απόδοση και μετάδοση. Επίσης έχει πιο λίγη μνήμη και σε αρκετές περιπτώσεις λιγότερη ισχύ επεξεργασίας για υπολογισμό (υπάρχει και το ενδεχόμενο κάποιες φορές να είναι πιο αποδοτικό και ταχύτερο το 512RSA). Το 512RSA είναι πιο ανθεκτικό σε σύγκρουση (το 512RSA απαιτεί αντίσταση 256 bit ενώ το 256RSA 128 bit) αλλά έχει προβλήματα συμβατότητας. Με όλα αυτά που αναφέρθηκαν είναι και ένα λόγος να μην είναι η πρώτη επιλογή αφού ακούγονται περισσότερο τα μειονεκτήματα παρά τα πλεονεκτήματα. Έτσι προκύπτει να είναι μια διεθνής επιλογή το 256RSA για τις ιστοσελίδες. [13]

Το SHA-1 εντοπίστηκε σε τρείς ιστοσελίδες το οποίο θεωρείται πλέον ανασφαλές λόγω του μεγέθους και της κατασκευής του που ήταν εφικτό να προκαλέσει σύγκρουση (collision*). Σε κάποιες ιστοσελίδες (συνολικά 10) δεν εντοπίστηκε αλγόριθμος υπογραφής για τον λόγο ότι δεν χρησιμοποιείται το πρωτόκολλο HTTPS.

5.1.2 RSA Key Strength (Ισχύς κλειδιού RSA)



Σχήμα 5.2: Ισχύς κλειδιού RSA

*σύγκρουση (collision): όταν δύο κόμβοι επιλέξουν ταυτόχρονα να αποστείλουν ένα πλαίσιο, τότε τα δύο σήματα θα εμφανιστούν μαζί στο μέσο μετάδοσης με αποτέλεσμα να μην μπορεί να αποκωδικοποιηθεί από τους παραλήπτες.

Τα αποτελέσματα που προκύπτουν από την ισχύς (μέγεθος) κλειδιού RSA είναι ότι οι περισσότερες ιστοσελίδες, συνολικά 29 από τις 44 εφαρμόζουν μέγεθος κλειδιού 2048bit το οποίο είναι ασφαλές. Αυτό σημαίνει ότι τα δεδομένα μπορούν να παραμείνουν εμπιστευτικά με αυτό το μέγεθος κλειδιού στην χρονική αυτή περίοδο αλλά το RSA για τις επόμενες δεκαετίες προτείνει το 4096bits. Το μέγεθος κλειδιού με 4096bits εφαρμόζεται μόλις σε μια μόνο ιστοσελίδα που θα ήταν καλό και οι υπόλοιπες ιστοσελίδες να το πράξουν αν θέλουν να κρατήσουν την ασφάλεια σε υψηλά επίπεδα. Θεωρητικά τα κλειδιά RSA με 2048bits θα είναι καλά μέχρι το 2030.

Στον πιο κάτω πίνακα σύμφωνα με την ειδική έκδοση NIST υπάρχουν τα μεγέθη κλειδιών RSA με την αξία ασφάλειας δηλαδή πόση δουλειά χρειάζεται για να τα σπάσει ένας κρυπτογραφικός αλγόριθμος. Όσο πιο μεγάλος είναι ο αριθμός τόσο πιο μεγάλο κόπο χρειάζεται για να σπάσει.

Security Strength	RSA key length
<= 80	1024
112	2048
128	3072
192	7680
256	15360

Πίνακας 5.1: Ισχύς ασφάλειας των μεγεθών κλειδιών RSA

Πιο κάτω παρουσιάζεται η περίοδος κατά την οποία κάθε δύναμη ασφαλείας θεωρείται αποδεκτή.

Security Strength	Through 2030	2031 and beyond
< 112	Disallowed	Disallowed
112	Acceptable	Disallowed
128	Acceptable	Acceptable
192	Acceptable	Acceptable
256	Acceptable	Acceptable

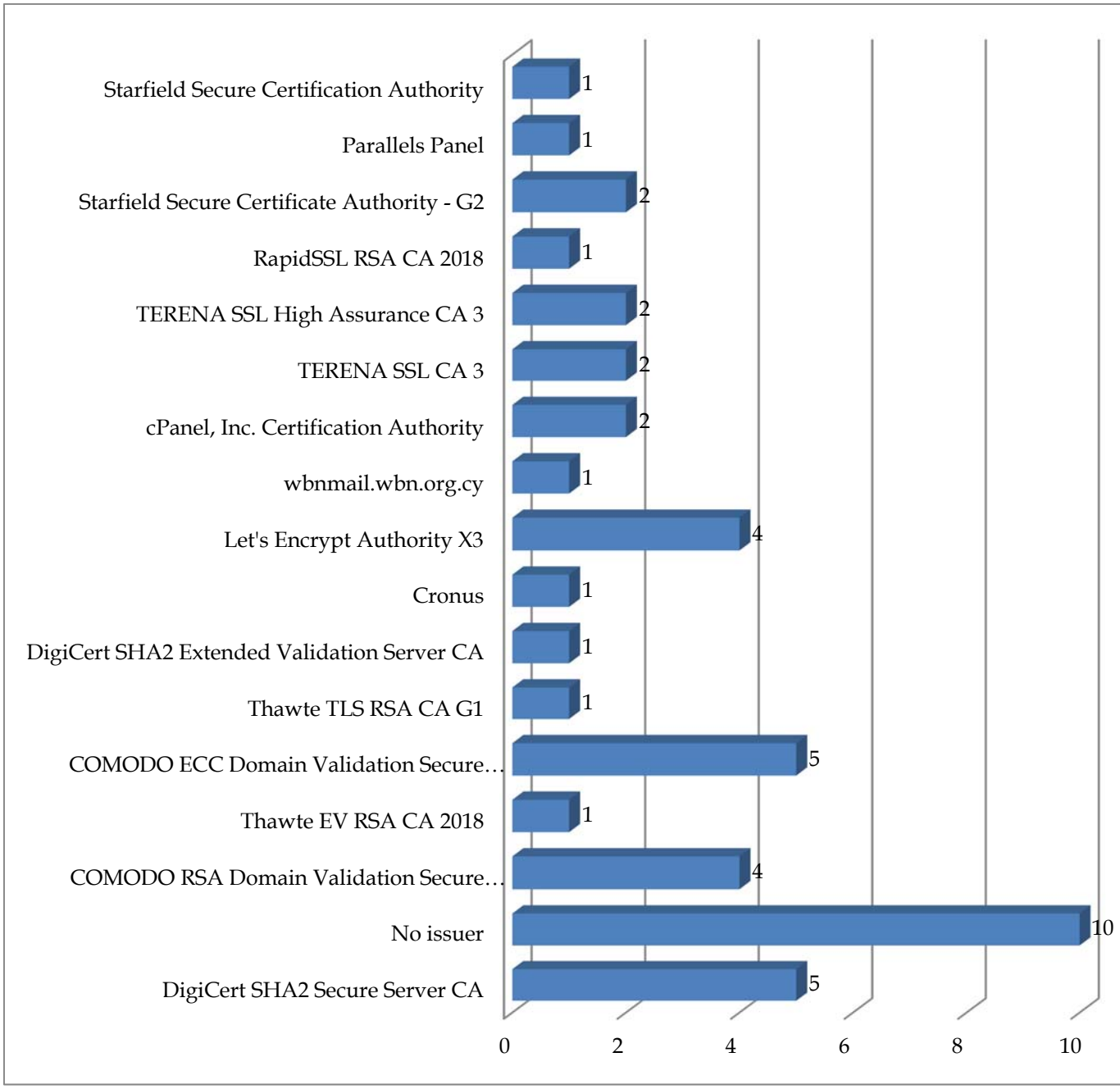
Πίνακας 5.2: Περίοδος δύναμης ασφαλείας

Οπότε σύμφωνα με το NIST, το μέγεθος 2048-bit με αξία 112 είναι αποδεκτό μέχρι το 2030 αλλά δεν είναι ακόμη σίγουρο ότι είναι ασφαλές για τον λόγο ότι οι εγκληματίες στον κυβερνοχώρο βρίσκονται πάντα ένα βήμα πιο μπροστά. Τα κλειδιά 4096 έχουν πιο μεγάλα keys από το 2048 άρα χρειάζονται περισσότερο χρόνο να παραχθούν και υπολογιστικούς πόρους (CPU) για κρυπτογράφηση και αποκρυπτογράφηση. Άρα ενδέχεται σε ένα διακομιστή μεταφορών

αρχείων να επηρεάσει την απόδοση του. Βέβαια η χρησιμοποίηση των κλειδιών αυτών είναι αισθητή μόνο σε μια μικρή στιγμή κατά την μεταφορά αρχείων. Κατά πόσο θα επηρεαστεί η απόδοση με την χρησιμοποίηση του 4096bit θα εξαρτηθεί με βάση το CPU του διακομιστή, ο αριθμός ταυτόχρονων μεταφορών αρχείων, το εύρος ζώνης δικτύου κ.ά. [30]

Σε κάποιες ιστοσελίδες δεν έχουν εμφανίσει μετά από την εκτέλεση των εντολών τι ακριβώς μέγεθος κλειδιού χρησιμοποιούν που ίσως σε κάποιες περιπτώσεις κάποια συστήματα των διακομιστών ιστοσελίδων να μην το επιτρέπουν και σε κάποιες άλλες περιπτώσεις λόγω της απουσίας του πρωτοκόλλου HTTPS.

5.1.3 Εκδότες



Σχήμα 5.3: Εκδότες

Τα αποτελέσματα που προκύπτουν από το σχήμα 5.3 είναι:
Οι ιστοσελίδες που δεν χρησιμοποιούν εκδότη (issuer) είναι 10 στο σύνολο και αυτό επιδεικνύει ότι δεν χρησιμοποιούν κάποιο πιστοποιητικό άρα ούτε το πρωτόκολλο HTTPS για την ασφάλεια τους. Αυτές οι ιστοσελίδες είναι κυρίως ενημερωτικές αλλά και κάποιες ιστοσελίδες αφορούν την κυβέρνηση. Από την στιγμή που δεν υπάρχει η ύπαρξη του πρωτοκόλλου αυτό έχει ως επακόλουθο να μην υπάρχει ισχύς (μέγεθος) κλειδιού RSA όπως και η μη χρησιμοποίηση του αλγόριθμου υπογραφής.

Ο εκδότης με την ονομασία Comodo έχει εντοπιστεί σε 9 ιστοσελίδες με δύο διαφορετικές εκδόσεις το Comodo ECC και το Comodo RSA. Η έκδοση Comodo ECC χρησιμοποιείται σε 5 ιστοσελίδες οι οποίες είναι κυρίως ιστοσελίδες που αναφέρονται σε αθλητικά. Αυτές οι ιστοσελίδες χρησιμοποιούν αλγόριθμο υπογραφής ecdsa-with-SHA256 αλλά δεν εντοπίζεται σε καμία ιστοσελίδα το μέγεθος του κλειδιού RSA.. Όσον αφορά την έκδοση Comodo RSA, έχουν εντοπιστεί 4 ιστοσελίδες που το εφαρμόζουν και είναι κυρίως κυβερνητικοί οργανισμοί. Οι ιστοσελίδες αυτές χρησιμοποιούν αλγόριθμο υπογραφής sha256 με κρυπτογράφηση RSA και μέγεθος κλειδιού RSA 2048bits (σε αντίθεση με την έκδοση Comodo ECC που δεν περιλαμβάνει μέγεθος κλειδιού). Γενικά φαίνεται ο εκδότης COMODO να προτιμείται αφού το έχουν εφαρμόσει 9 ιστοσελίδες και είναι ο δημοφιλέστερος εκδότης σε σχέση με τις υπόλοιπες 44 ιστοσελίδες που έχουν ερευνηθεί. Ο λόγος που είναι δημοφιλής είναι ότι παρέχει πιστοποιητικά SSL χαμηλού κόστους και αξιόπιστα για τους ιστότοπους. Επίσης είναι ένας από τους μεγαλύτερους εκδότες πιστοποιητικών SSL με ποσοστά αγοράς πάνω από το 48% (πρώτη παγκοσμίως Αρχή Πιστοποίησης). Προσφέρει δωρεάν πιστοποιητικά SSL με διάρκεια 90 ημερών και κρυπτογράφηση 256bit. Έχει χαμηλότερες τιμές για τα πιστοποιητικά ενιαίου τομέα SSL και πιστοποιητικά EV (Extended Validation). [04-05]

Η Digicert έχει παρουσιαστεί σε συνολικά 6 ιστοσελίδες με 2 εκδόσεις. Η μία είναι η DigiCert SHA2 Secure Server CA (εντοπίστηκε σε 5 ιστοσελίδες) και η άλλη είναι η DigiCert SHA2 Extended Validation Server CA (εντοπίστηκε σε 1 ιστοσελίδα). Δηλαδή εντοπίστηκε σε ιστοσελίδες ημικρατικών οργανισμών και τις κυβέρνησης. Είναι η δεύτερη σε επιλογή Αρχή Πιστοποίησης (είναι δεύτερη παγκοσμίως Αρχή Πιστοποίησης με ποσοστά αγοράς στο 25%) για τον λόγο ότι είναι αξιόπιστη, βοηθάει στην επιλογή του καταλληλότερου πιστοποιητικού SSL με πολλούς τύπους αρχείων βοήθειας και τεκμηρίωσης. Επίσης έχει την δυνατότητα να παρέχει ποιοτικές τακτικές για την ασφάλεια της επιχείρησης και της ιστοσελίδας από βίαιες επιθέσεις

δυνάμεων χρησιμοποιώντας κρυπτογράφηση 256-bit μαζί με πιστοποιητικά ρίζας (root) 2048-bit. [05-09]

Η Thawte έχει εντοπιστεί σε δύο μόνο ιστοσελίδες και σε δύο εκδόσεις. Η μία είναι η Thawte EV RSA CA 2018 και η άλλη είναι Thawte TLS RSA CA G1. Χρησιμοποιήθηκε σε μία τράπεζα και σε μια διαδικτυακή πύλη. Αν και ανήκει στην Digicert Inc και είναι τρίτη μεγαλύτερη δημόσια Αρχή Πιστοποίησης εντούτοις δεν είναι μέσα στις επιλογές των επιχειρήσεων. Ίσως επειδή αρμόζει σε επιχειρήσεις που θα ήθελαν πολύ περισσότερες επιλογές πιστοποιητικών SSL. Η Thawte προμηθεύει έναν βασικό τομέα που προσφέρεται ως δωρεάν SAN και εγκρίνει κωδικούς πιστοποιημένων πιστοποιητικών για εφαρμογές desktop της Apple. [05-29]

Η Let's Encrypt παρουσιάστηκε σε 4 ιστοσελίδες με μία έκδοση την Let's Encrypt Authority X3. Χρησιμοποιήθηκε κυρίως από κολλέγια και πανεπιστήμια. Δεν είναι μέσα στις δημοφιλέστερες Αρχές Πιστοποίησης όπως είναι η Digicert και Comodo. Είναι μια ελεύθερη, αυτοματοποιημένη και ανοιχτή αρχή πιστοποιητικού που προσφέρει δωρεάν πιστοποιητικό SSL για 90 μέρες και στη συνέχεια πρέπει να ανανεωθεί. Αυτή η αρχή εξαρτάται από το είδος επιχείρησης που, θα εφαρμοστεί γιατί παρέχει μόνο επικυρωμένο πιστοποιητικό SSL, που δεν αποτελεί ιδανική λύση για μεγάλες ιστοσελίδες ή για ιστότοπους ηλεκτρονικού εμπορίου. Άρα εξασφαλίζει μόνο τον βασικό ιστότοπο και αν η ιστοσελίδα περιέχει ηλεκτρονική συναλλαγή, τότε δεν επαρκεί η προστασία στον ιστότοπο. Επίσης το πιστοποιητικό αυτό δεν προσφέρει καμία εγγύηση σε περίπτωση κατάχρησης ή βάσης δεδομένων. [19]

Το cPanel χρησιμοποιείται σε δύο ιστοσελίδες και σε μία έκδοση η οποία είναι η cPanel, Inc. Certification Authority. Έχει χρησιμοποιηθεί στις ιστοσελίδες κολλεγίων. Παρόλο που έχει περισσότερα πλεονεκτήματα παρά μειονεκτήματα δεν χρησιμοποιείται και αυτό φαίνεται από τη διαπίστωση ότι μόνο 2 επιχειρήσεις από τις 44 το έχουν επιλέξει και το έχουν εφαρμόσει. Ο λόγος είναι ότι είναι σχετικά ακριβό, αλλά αν αγοραστεί από Reseller ή VPS hosting provider είναι αρκετά πιο φθηνό. Κάποια από τα πλεονεκτήματα του είναι η εξαιρετική συμβατότητα, η ευκολία στη χρήση και στην εγκατάσταση, είναι εύκολα φορητό, η διαχείριση φιλοξενίας κ.ά. όσον αφορά τα μειονεκτήματα έχει περιορισμένο μέγεθος, ευπάθεια cPanelto, κόστος στην άδεια , έλλειψη επαγγελματικής εμφάνισης κ.ά. [08]

Το RapidSSL χρησιμοποιείται σε μόλις μία ιστοσελίδα με την έκδοση RapidSSL RSA CA 2018. Αν και είναι φτηνό και απλό εντούτοις δεν χρησιμοποιείται. Ο λόγος είναι ότι δεν προσφέρει τα

χαρακτηριστικά, την υποστήριξη που έχουν οι άλλες πιο αξιόπιστες Αρχές Πιστοποίησης και στο ότι είναι περισσότερο σε μικρό μεσαίες ιστοσελίδες ηλεκτρονικού εμπορίου για επικυρώσεις τομέα (domain validation). [01-11]

Η Terena (GÉANT) εντοπίστηκε σε 4 ιστοσελίδες των επιχειρήσεων από τις 44 με δύο διαφορετικές εκδόσεις. Η μία ονομάζεται TERENA SSL CA 3 (εντοπίστηκε σε 2 ιστοσελίδες) και η άλλη ονομάζεται TERENA SSL High Assurance CA 3 (εντοπίστηκε σε 2 ιστοσελίδες). Η εφαρμογή του έγινε ως επί των πλείστων σε πανεπιστήμια. Δεν είναι από τις μεγαλύτερες αξιόπιστες Αρχές Πιστοποίησης αλλά διαπιστώνεται ότι το έχουν επιλέξει πανεπιστήμια για τον λόγο ότι μπορούν να αποκτήσουν πιστοποιητικά διακομιστή σε χαμηλότερο κόστος διαμέσου των εθνικών δικτύων έρευνας και εκπαίδευσης. Η διευθέτηση αυτή έγινε εφικτή με την συμφωνία μεταξύ της Terena και της GlobalSign (θυγατρική της Cybertrust). [27-28]

Η Αρχή Πιστοποίησης Starfield έχει χρησιμοποιηθεί σε 3 ιστοσελίδες με δύο διαφορετικές εκδόσεις. Η μία λέγετε Starfield Secure Certification Authority (βρέθηκε σε μια ιστοσελίδα) και η Starfield Secure Certificate Authority - G2 (βρέθηκε σε δύο ιστοσελίδες). Επιλέχτηκε να υλοποιηθεί περισσότερο σε οργανισμούς. Αν το συγκρίνουμε με την Αρχή Πιστοποίησης Comodo που είναι κατηγορίας 1 τότε η Starfield είναι κατηγορίας 5 με παγκόσμιο σύνολο αγορών να φτάνει το 228%. Η Starfield αν και είναι φτηνές επώνυμες πιστοποιήσεις της GoDaddy, χρησιμοποιείται σε μόλις τρεις ιστοσελίδες από τις 44 που έχουν εξεταστεί. [25]

Γενικά σχόλια για τους εκδότες των ιστοσελίδων που ερευνήθηκαν: Συνολικά δύο ιστοσελίδες παρουσίασαν πιστοποιητικά τα οποία έχουν τερματιστεί και οι εκδότες τους είναι Cronus και Parallels Panel. Επίσης άλλες τέσσερις ιστοσελίδες έχουν εκδοθεί και υπογραφτεί από Αρχή Πιστοποίησης (CA) εντός της επιχείρησης τους (self-signed). Οι Αρχές Πιστοποίησης που προσφέρουν δωρεάν πιστοποιητικά τα οποία χρειάζονται ανανέωση σε κάποιο διάστημα είναι τα ακόλουθα: Comodo (Sectigo), RappidSSL, Thawte, Terena (GÉANT- μη κερδοσκοπική ένωση) και Let's Encrypt.

5.1.4 Αποτελέσματα που διεξήχθηκαν μετά την εκτέλεση των εντολών sslscan και openssl

Τα αποτελέσματα που σχηματίστηκαν μετά την ολοκλήρωση της εντολής sslscan είναι τα παρακάτω:

Session renegotiation not supported: η επίθεση που σχετίζεται με τα χαρακτηριστικά του πρωτοκόλλου SSL/TLS ονομάζεται επαναδιαπραγμάτευση περιόδου σύνδεσης (session renegotiation). Η ανακάλυψη της ευπάθειας θα μπορούσε να χρησιμοποιηθεί για χειρισμό δεδομένων που λαμβάνονται από ένα πελάτη ή διακομιστή. Ένα απλό παράδειγμα είναι το εξής: ένας διακομιστής θεωρείται ευάλωτος όταν έχει ρυθμιστεί να επιτρέπει την επαναδιαπραγμάτευση περιόδου σύνδεσης αλλά δεν χρησιμοποιεί ακόμη ενημερωμένο λογισμικό. Ένας τρόπος για την προστασία από αυτήν την επίθεση είναι να απενεργοποιηθεί η επαναδιαπραγμάτευση περιόδου σύνδεσης πάνω στον διακομιστή. Άρα όταν υπάρχει η ένδειξη <session renegotiation not supported> σημαίνει ότι δεν υποστηρίζεται η επαναδιαπραγμάτευση της περιόδου σύνδεσης για να προστατευτεί από αυτήν την ευπάθεια που πιθανόν να επιφέρει επίθεση.

Server does not support TLS Fallback SCSV: είναι μια τιμή σουίτας TLS Signaling Cipher Suite (SCSV) το οποίο εφαρμόζεται όταν θα πρέπει να γίνει προστασία από επιθέσεις με σκοπό να εκμεταλλευτεί τις υποβαθμίσεις πρωτοκόλλου. Αυτό γίνεται στην πράξη όταν χρησιμοποιείται μια μικρότερη έκδοση πρωτοκόλλου και γίνει προσπάθεια εφαρμογής μιας πιο υψηλής έκδοσης πρωτοκόλλου. Για παράδειγμα όταν κάποιος προσπαθήσει να κάνει μια επίθεση θα προσπαθήσει να διακόψει την διαπραγμάτευση ενός ανωτέρου πρωτοκόλλου π.χ TLS 1.2 ή 1.1 με σκοπό να ξαναπροσπαθήσει με πιο χαμηλού επιπέδου πρωτόκολλο όπως είναι το TLS 1.0 ή SSLv3. Αν τότε γίνει αυτό ο επιτιθέμενος θα εκμεταλλευτεί τα ελαττώματα που έχουν τα πρωτόκολλα αυτά και θα εκτελέσει άλλες επιθέσεις.

Could not open a connection to host <hostname> (212.31.118.26) on port 443 (Η παρατήρηση εμφανίστηκε εκεί που δεν υπήρχε signature algorithm, RSA key strength, issuer): Είναι φυσιολογικό να εμφανίζεται αυτό από την στιγμή που δεν υπάρχει το πρωτόκολλο HTTPS. Ένας σύνδεσμος (URL) που αρχίζει με το πρόθεμα https δηλώνει ότι θα χρησιμοποιηθεί κανονικά το πρωτόκολλο HTTP αλλά η σύνδεση θα γίνει σε διαφορετική πόρτα δηλαδή στην πόρτα 443 αντί 80, οπότε και τα δεδομένα θα μεταφέρονται κρυπτογραφημένα.

Τα αποτελέσματα που σχηματίστηκαν μετά την ολοκλήρωση της εντολής openssl είναι τα εξής: unable to load certificate / expecting: trusted certificate (Το σφάλμα εμφανίστηκε εκεί που δεν υπήρχε signature algorithm, RSA key strength, issuer): Δε μπορεί να γίνει εφικτή η φόρτωση του πιστοποιητικού αφού δεν υπάρχει πιστοποιητικό στη συγκεκριμένη ιστοσελίδα.

Verification error: unable to verify the first certificate/unable to get local issuer certificate: Τα πιστοποιητικά που υπάρχουν στον διακομιστή (server) είναι ελλιπής και δεν είναι αναμενόμενα από τον χρήστη (client).

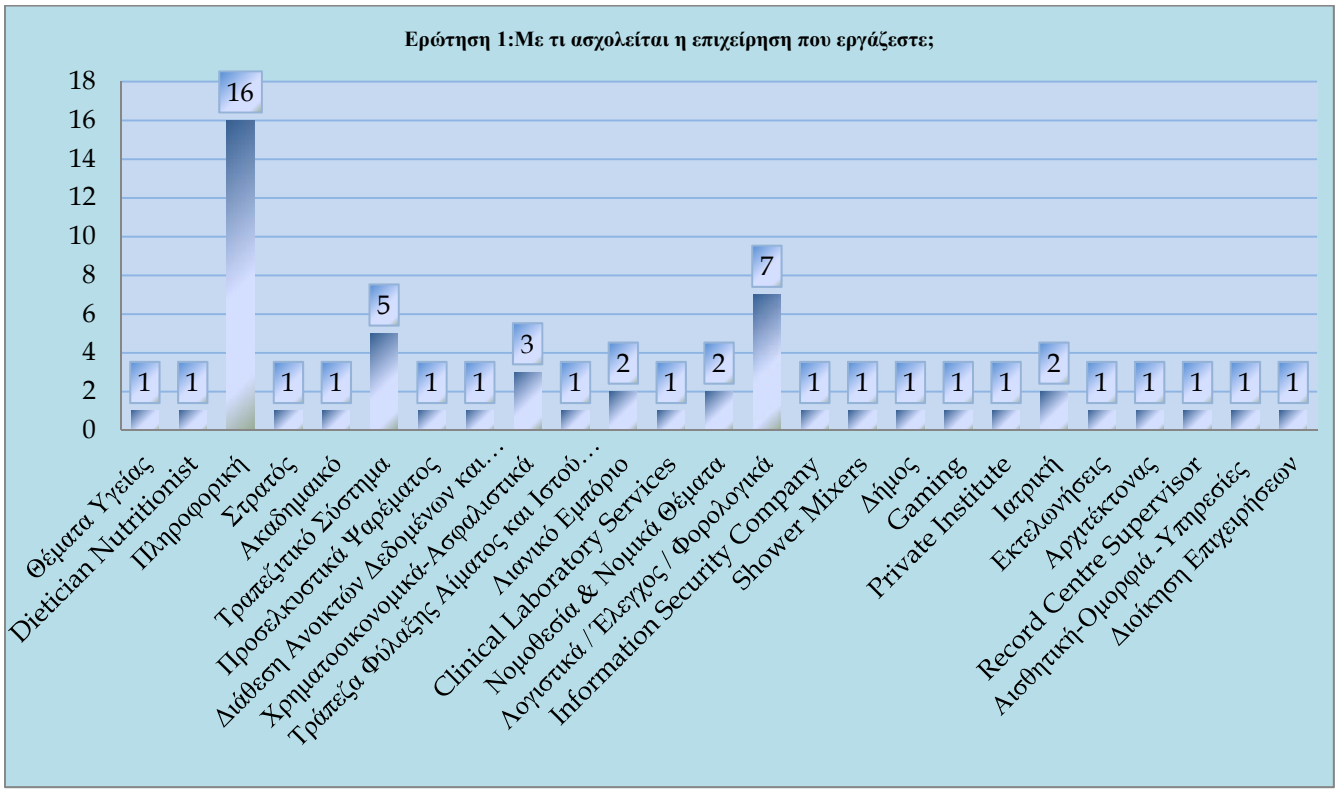
No peer certificate available / Secure Renegotiation is not supported: το συμπέρασμα που έγινε είναι όταν εκτελείτε η εντολή του openssl και δείξει ότι υπάρχει η ένδειξη αυτή <secure renegotiation is not supported> τότε παρουσιάζεται το σφάλμα <unable to load certificate/expecting: trusted certificate>. Ενώ όταν υπάρχει η ένδειξη <secure renegotiation is supported> τότε δεν παρουσιάζεται κάποιο πρόβλημα.

Verification error: self-signed certificate: προειδοποίηση ότι το πιστοποιητικό που εκδόθηκε και υπογράφτηκε από Αρχή Πιστοποίησης (AC) είναι εντός της επιχείρησης.
Verification error: certificate has expired: το πιστοποιητικό της ιστοσελίδας έχει τερματιστεί.

5.2 Ερωτηματολόγιο

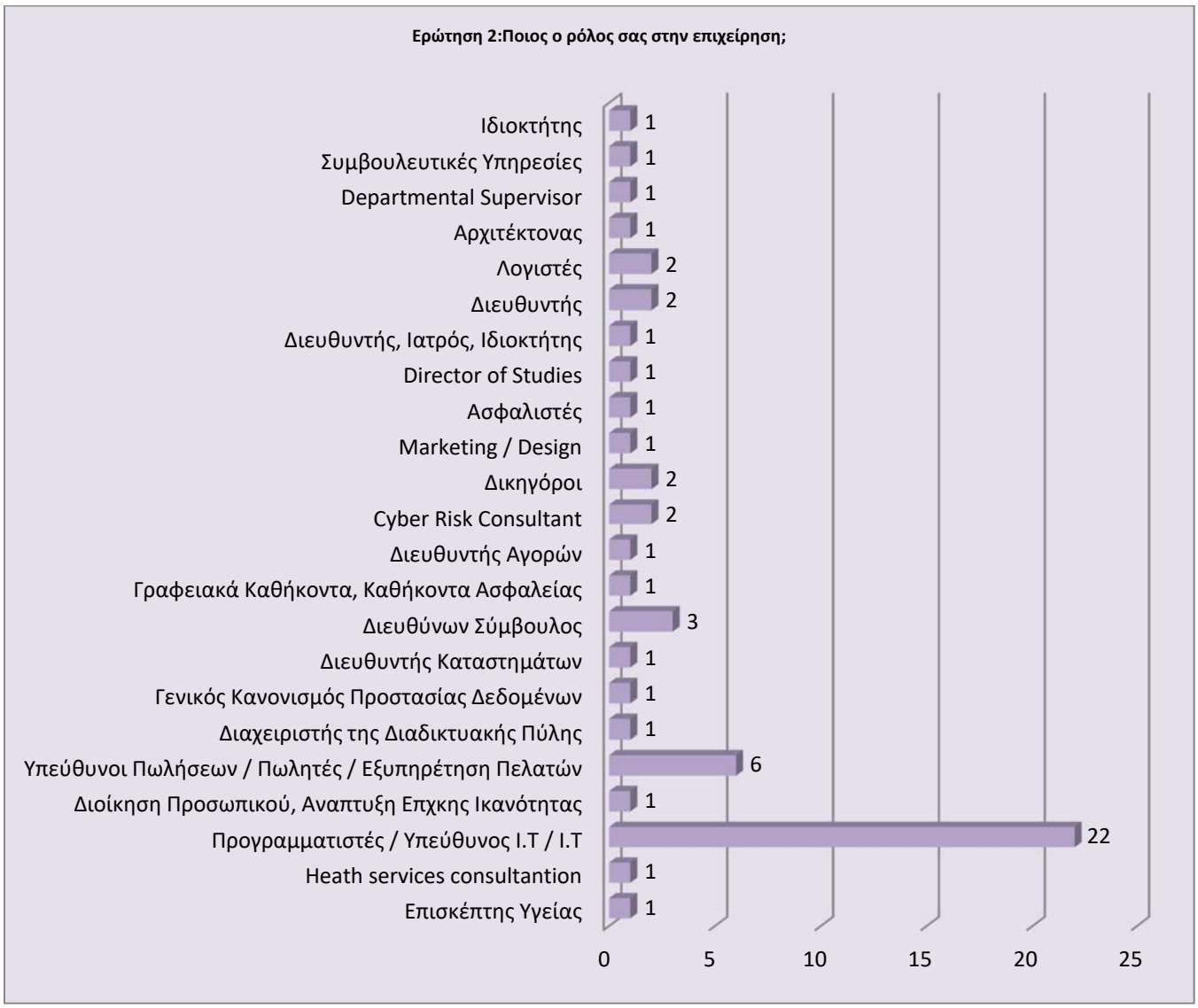
Το ερωτηματολόγιο υλοποιήθηκε σε 55 συμμετέχοντες οι οποίοι εκπροσωπούσαν τις επιχειρήσεις που εργάζονται. Οι ερωτήσεις ήταν κλειστού τύπου δηλαδή υπήρχε η επιλογή απαντήσεων και αφορούσαν γενικά τα προσωπικά δεδομένα και την προστασία τους, τον Γενικό Κανονισμό Προστασίας Προσωπικών Δεδομένων (GDPR) και το πρωτόκολλο HTTPS. Σκοπός του ερωτηματολογίου είναι να παρθούν συμπεράσματα κατά πόσο οι επιχειρήσεις στην Κύπρο έχουν συμμορφωθεί σωστά με τον κανονισμό του GDPR και έχουν δημιουργηθεί οι κατάλληλες διαδικασίες και μέτρα αντιμετώπισης της προστασίας των προσωπικών δεδομένων. Επίσης διερευνήθηκε αν χρησιμοποιείται το πρωτόκολλο HTTPS στις ιστοσελίδες των επιχειρήσεων.

Δημογραφικά στοιχεία συμμετεχόντων και επιχειρήσεων



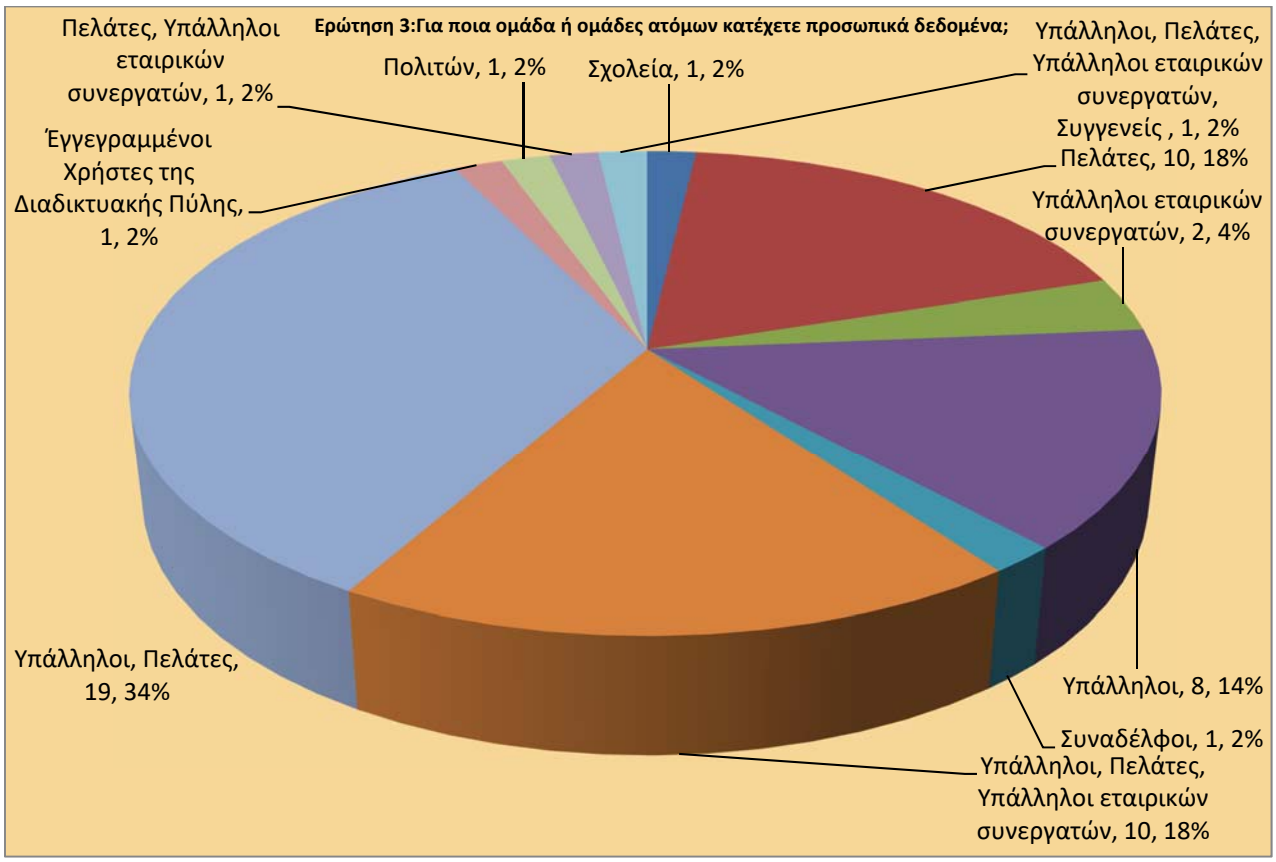
Σχήμα 5.4: Είδη επιχειρήσεων

Στο ερωτηματολόγιο της μεταπτυχιακής διατριβής έχει καταστεί δυνατό να ληφθούν απαντήσεις από πολλών ειδών επιχειρήσεις που ασχολούνται με τη μάθηση (private institute), τη διοίκηση επιχειρήσεων, τη νομική, την ιατρική, τις εκτελωνίσεις, τις υπηρεσίες αισθητικής/ομορφιάς κ.ά. Μεγάλη συμμετοχή στο ερωτηματολόγιο υπήρξε από επιχειρήσεις στον τομέα της πληροφορικής (συνολικά 16 συμμετέχοντες). Ακολουθεί ο τομέας που έχει να κάνει με λογιστικά/έλεγχο/φορολογικά (συνολικά 7) και στη συνέχεια ο τομέας του τραπεζικού συστήματος (συνολικά 5). Στον χρηματοοικονομικό-ασφαλιστικό τομέα έλαβαν μέρος 3 συμμετέχοντες, στον τομέα του λιανικού εμπορίου/ νομοθεσίας και νομικών θεμάτων / ιατρικής υπήρξαν 2 συμμετέχοντες, ενώ οι άλλοι τομείς έλαβαν μέρος με μία συμμετοχή. Συνολικά το ερωτηματολόγιο συμπληρώθηκε από 55 συμμετέχοντες.



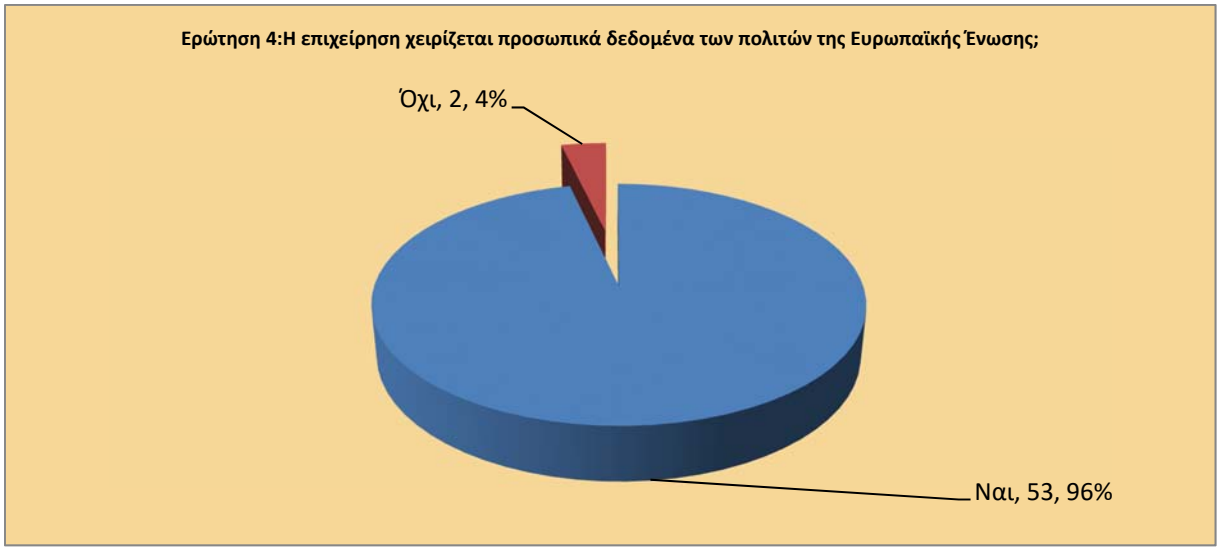
Σχήμα 5.5: Αρμοδιότητες στις επιχειρήσεις

Μετά από την συλλογή των ερωτηματολογίων και όπως φαίνεται στο σχήμα 5.5 υπάρχει ένας μεγάλος αριθμός συμμετεχόντων (συνολικά 22) που ανήκουν στους προγραμματιστές/Υπεύθυνος I.T/I.T αφού είναι φυσιολογικό από την στιγμή που συνολικά 16 ανήκουν στον τομέα της πληροφορικής (παρουσιάζεται στο σχήμα 5.4), 5 συμμετέχοντες στο τραπεζικό σύστημα και σε άλλου είδος επιχείρησης που μπορεί να έχουν τα καθήκοντα των προγραμματιστών / υπεύθυνοι I.T / I.T . Στην αρμοδιότητα των υπεύθυνων πωλήσεων / πωλητές / εξυπηρέτηση πελατών υπήρξαν συνολικά 6 συμμετέχοντες και 3 είχαν τον ρόλο του διευθύνων σύμβουλου. Στις ευθύνες του λογιστή / διευθυντή / δικηγόρου / cyber risk consultant είναι συνολικά 8, δύο στην κάθε ειδικότητα και ακολουθούν οι υπόλοιπες με ένα συμμετέχοντα.



Σχήμα 5.6: Ομάδες προσωπικών δεδομένων

Οι επιχειρήσεις έχουν στην κατοχή τους προσωπικά δεδομένα που αφορούν κυρίως στις πλείστες περιπτώσεις υπαλλήλων (συναδέλφων) και πελατών ενώ σε μικρό βαθμό έχουν να κάνουν με δεδομένα υπαλλήλων εταιρικών συνεργατών, εγγεγραμμένοι χρήστες διαδικτυακής πύλης, πολιτών, μαθητών στα σχολεία και συγγενείς. Όλοι οι συμμετέχοντες γνωρίζουν ακριβώς ποιες ομάδες προσωπικών δεδομένων υπάρχουν στις επιχειρήσεις που απασχολούνται.



Σχήμα 5.7: Δεδομένα πολιτών που κατοικούν στην Ευρωπαϊκή Ένωση

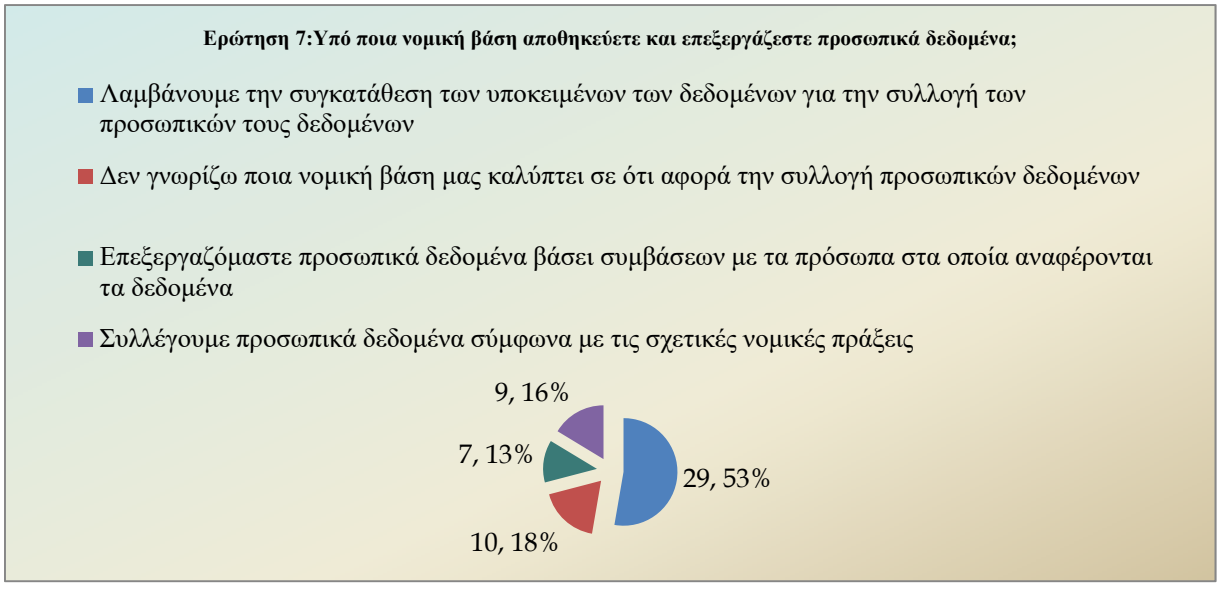
Ένα μεγάλο ποσοστό των επιχειρήσεων (96%) χρησιμοποιούν δεδομένα από ανθρώπους που κατοικούν στην Ευρώπη. Από τους 55 συμμετέχοντες μόλις 2 απάντησαν ότι στην επιχείρηση που εργάζονται χειρίζονται δεδομένα από ανθρώπους εκτός Ευρωπαϊκής Ένωσης.

Ερώτηση 5: Εάν ναι, τι είδους προσωπικά δεδομένα χειρίζεται η επιχείρηση;

Οι περισσότεροι συμμετέχοντες (11 συνολικά) επέλεξαν τον συνδιασμό δεδομένων: αριθμός ταυτότητας/διαβατηρίου-οικονομικές πληροφορίες-τραπεζικοί λογαριασμοί και 8 συμμετέχοντες δήλωσαν τον προηγούμενο συνδιασμό με επιπρόσθετα τα δεδομένα με το αναγνωριστικά στο διαδίκτυο. Την επιλογή αναγνωριστικό στο διαδίκτυο-αριθμός ταυτότητας/διαβατήριο έθεσαν 5 συμμετέχοντες, 4 συμμετέχοντες ανάφεραν μόνο τα δεδομένα με αριθμό ταυτότητας/διαβατηρίου και 3 συμμετέχοντες δήλωσαν και αυτοί μόνο για τις πληροφορίες δεδομένων στην υγεία. Τέσσερις ομάδες από 2 συμμετέχοντες (συνολικά 8 συμμετέχοντες) δήλωσαν τους εξής συνδιασμούς κάθε φορά: αριθμός ταυτότητας/διαβατηρίου-πληροφορίες για την υγεία, αναγνωριστικό στο διαδίκτυο, οικονομικές πληροφορίες και αναγνωριστικά στο διαδίκτυο-αριθμός ταυτότητας/διαβατηρίου-οικονομικές πληροφορίες-πληροφορίες για την υγεία-τραπεζικοί λογαριασμοί. Οι υπόλοιποι 16 συμμετέχοντες διάλεξαν διαφορετικές επιλογές όπως μόνο διεύθυνση-τηλέφωνα, τραπεζικοί λογαριασμοί, ονοματεπώνυμο-τηλέφωνο-διεύθυνση ηλεκτρονικού ταχυδρομείου. Το συμπέρασμα που προκύπτει είναι ότι υπάρχουν αρκετοί συνδιασμοί δεδομέων που μπορουν να επιλεγούν. Το σημαντικό όμως είναι ότι τα πιο γνωστά είδη δεδομέων που χειρίζονται οι επιχειρήσεις είναι ότι έχει να κάνει με τον αριθμό ταυτότητας / διαβατηρίου, ονοματεπώνυμο / τηλέφωνα / διεύθυνση / ημερομηνία γέννησης / ηλεκτρονική διεύθυνση (email), οικονομικές πληροφορίες, τραπεζικοί λογαριασμοί και αναγνωριστικά στο διαδίκτυο (διεύθυνση IP, RFID, cookie συστήματος κ.ά). Σε πιο λίγο βαθμό οι επιχειρήσεις χειρίζονται δεδομένα που αφορούν πληροφορίες με την υγεία, τίτλους ιδιοκτησίας και θρησκευτικές απόψεις. Οι συμμετέχοντες είναι ενήμεροι για τα είδη των προσωπικών δεδομένων που χειρίζονται στις επιχειρήσεις που εργοδοτούνται.

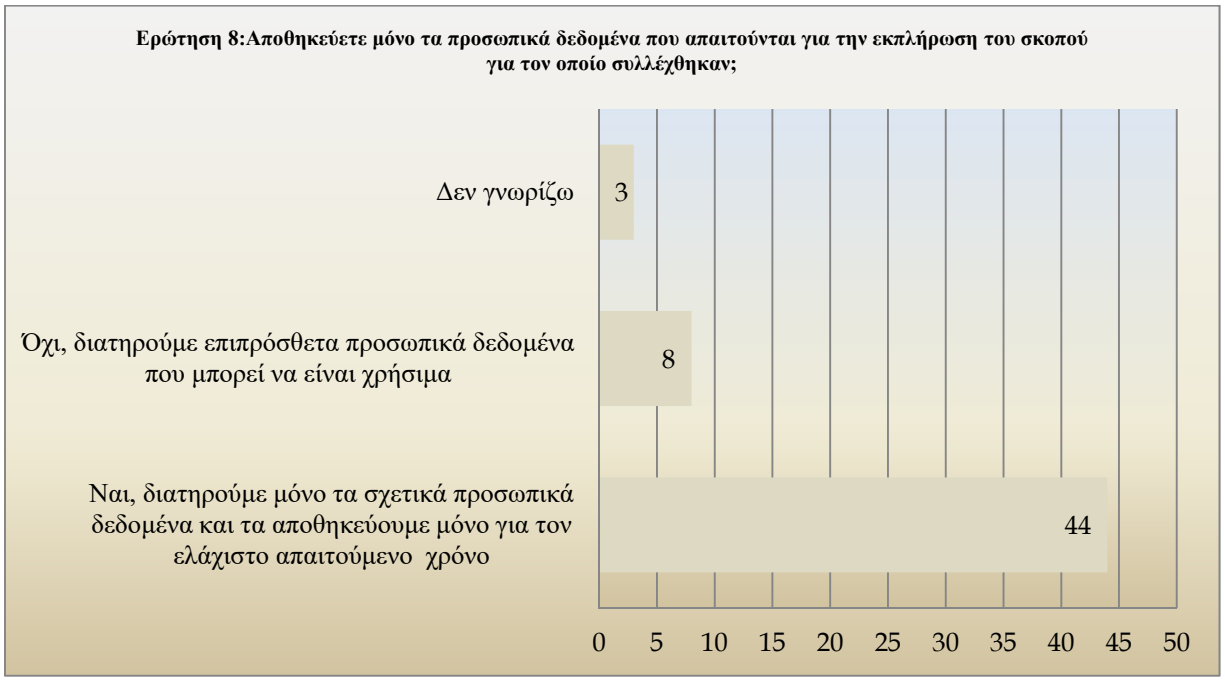
Σχήμα 5.8: Διαδικασίες αποθήκευσης προσωπικών δεδομένων

Ένα ποσοστό των συμμετεχόντων που αγγίζει το 96% γνωρίζουν για τις διαδικασίες αποθήκευσης προσωπικών δεδομένων που ακολουθούνται στις επιχειρήσεις που εργάζονται και μόνο δύο (4%) δεν γνωρίζουν. Τα δύο είδη αποθήκευσης προσωπικών δεδομένων είναι η έντυπη σε μορφή υπηρεσιακούς φακέλους και σε ηλεκτρονική μορφή στο μηχανογραφικό σύστημα. Πλέον με την πάροδο του χρόνου οι επιχειρήσεις προσπαθούν να αποθηκεύσουν εξολοκλήρου τα δεδομένα τους σε ηλεκτρονική μορφή αλλά στην σημερινή εποχή οι περισσότερες επιχειρήσεις έχουν και τα δύο είδη αποθήκευσης. Βέβαια υπάρχουν και επιχειρήσεις που έχουν μείνει μόνο σε έντυπη μορφή για τα προσωπικά τους δεδομένα οι οποίες είναι λίγες.



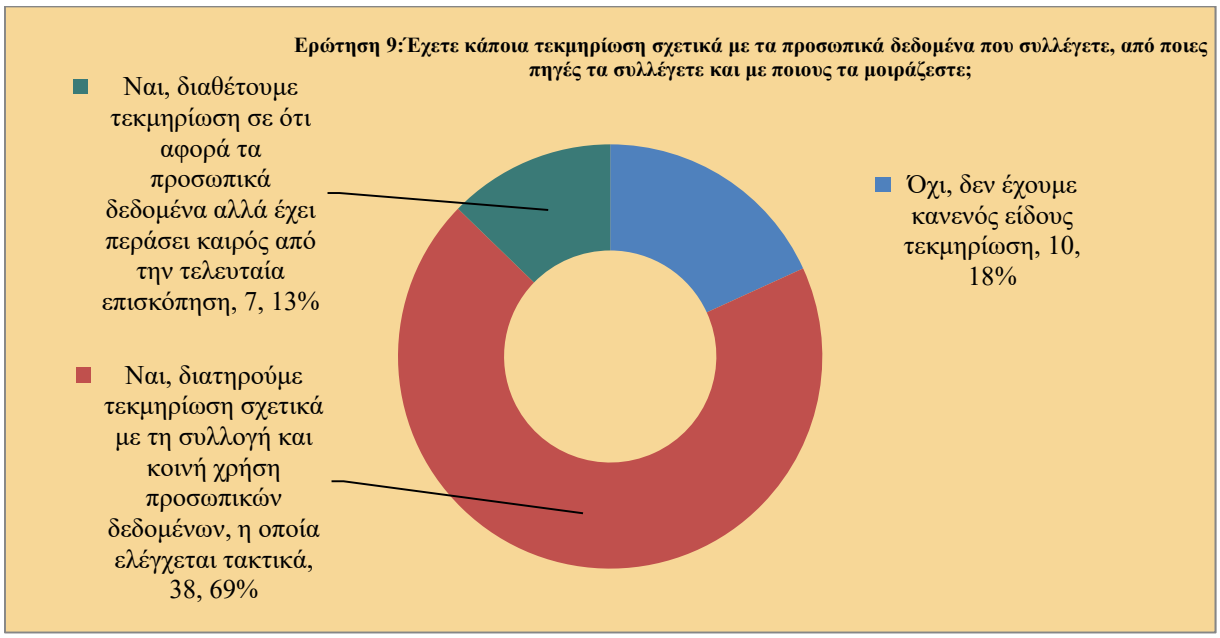
Σχήμα 5.9: Νομική βάση αποθήκευσης και επεξεργασίας δεδομένων

Οι παραπάνω συμμετέχοντες γνωρίζουν για τη νομική βάση αποθήκευσης και επεξεργασίας των προσωπικών δεδομένων και σχετικά λίγοι (συνολικά μόνο 10) δε τη γνωρίζουν. Η συγκεκριμένη ερώτηση απευθύνεται περισσότερο σε άτομα που εμπλέκονται στην διαχείριση και επεξεργασία δεδομένων όπως είναι οι δικηγόροι, λογιστές, άτομα που εργάζονται στο τραπεζικό σύστημα, υπεύθυνοι επεξεργασίας δεδομένων (DPO) κ.ά. Συνολικά 29 συμμετέχοντες, περισσότερο από τους μισούς απάντησαν ότι η συλλογή των προσωπικών δεδομένων γίνεται με την συγκατάθεση των ατόμων που ανήκουν αυτά τα δεδομένα ενώ συνολικά 9 συμμετέχοντες απάντησαν ότι η συλλογή των δεδομένων γίνεται με βάση σχετικές νομικές πράξεις. Οι υπόλοιποι 7 συμμετέχοντες ανάφεραν ότι τα προσωπικά δεδομένα επεξεργάζονται βάσει συμβάσεων με τα άτομα τα οποία ανήκουν τα δεδομένα.



Σχήμα 5.10: Αποθήκευση αναγκαίων ή επιπρόσθετων προσωπικών δεδομένων για τον σκοπό που έχουν συλλεχθεί και για τον απαιτούμενο χρόνο

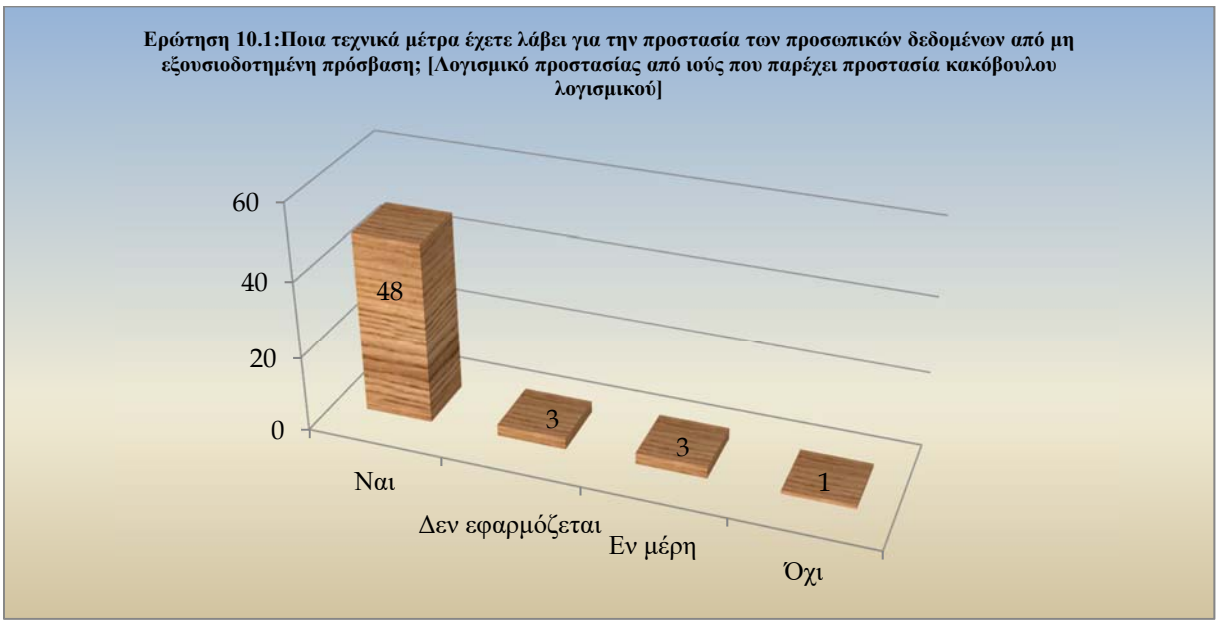
Οι πιο πολλές επιχειρήσεις (συνολικά 44) αποθηκεύουν τα προσωπικά τους δεδομένα τα οποία θα χρειαστούν και όχι περισσότερα από αυτά καθώς και το διάστημα που τα έχουν ανάγκη. Πιο λίγες επιχειρήσεις, (συνολικά 8) διατηρούν επιπρόσθετα προσωπικά δεδομένα από αυτά που είναι αναγκαία ενώ 3 από τους συμμετέχοντες δεν γνωρίζουν ποια απαιτούμενα προσωπικά δεδομένα αποθηκεύονται. Ίσως κάποιοι οι οποίοι δεν έχουν άμεση σχέση με τα προσωπικά δεδομένα των πελατών να μην γνωρίζουν τις διαδικασίες που ακολουθούνται για το τι ακριβώς πρέπει να γίνεται.



Σχήμα 5.11: Τεκμηρίωση/έλεγχος για την συλλογή και κοινή χρήση των προσωπικών δεδομένων

Ο σωστός τρόπος που πρέπει να εφαρμόζεται για τη συλλογή και κοινή χρήση των προσωπικών δεδομένων είναι να διατηρείται η απαραίτητη τεκμηρίωση και να ελέγχεται τακτικά. Αυτό γίνεται σε μεγάλο ποσοστό στις περισσότερες επιχειρήσεις το οποίο αγγίζει το 69% (38 από τους 55 συμμετέχοντες) ενώ το 18% (10 συμμετέχοντες) δήλωσαν ότι στις επιχειρήσεις που εργάζονται δεν εφαρμόζουν καμία τεκμηρίωση. Όταν δεν υπάρχει κάποια τεκμηρίωση για τη συλλογή των προσωπικών δεδομένων, μπορεί να προκληθούν προβλήματα και δεν θα υπάρχουν τα αποδεικτικά στοιχεία που θα τα επιβεβαιώνουν. Μια μικρή μερίδα επιχειρήσεων διαθέτουν τεκμηρίωση για τα προσωπικά δεδομένα αλλά δεν γίνεται τακτικός έλεγχος και αυτό μπορεί να επιφέρει κινδύνους όταν σε κάποιες περιπτώσεις δεν γίνει σωστά (ελλιπής) η τεκμηρίωση ή αυτή η τεκμηρίωση απουσιάζει για κάποιο λόγο.

Ερώτηση 10.1 μέχρι 10.10: Με γνώμονα το GDPR είναι αναγκαίο, γνωρίζοντας τη φύση, το πεδίο υλοποίησης, το πλαίσιο και τις επιδιώξεις της επεξεργασίας καθώς και τις απώλειες που μπορούν να εντοπιστούν στα δικαιώματα κα τις ελευθερίες φυσικών προσώπων, να συμμορφωθούν ανάλογα τεχνικά και οργανωτικά μέτρα για να προφυλαχθούν ώστε να μπορεί να αποδεικτή ότι η επεξεργασία γίνεται όπως προβλέπει ο κανονισμός. Τα μέτρα αυτά διερευνώνται σε τακτική βάση και όταν υπάρξουν προβλήματα διορθώνονται.



Σχήμα 5.12: Τεχνικά μέτρα προστασίας χρησιμοποιώντας το λογισμικό προστασίας από ιούς που παρέχει προστασία από κακόβουλο λογισμικό

Ένα λογισμικό προστασίας πρέπει να παρέχει μια γενική προστασία έναντι των ιών και κάθε είδους κακόβουλου λογισμικού. Επίσης ανίχνευση του συστήματος και εντοπισμός spyware, adware κ.ά. Άρα είναι πολύ σημαντικό να υπάρχει ένα λογισμικό που να προστατεύει από κακόβουλο λογισμικό και από ότι διαπιστώνεται στο σχήμα 5.12 υλοποιείται σε πολύ μεγάλο ποσοστό. Από τους 55 συμμετέχοντες, οι 48 ανάφεραν ότι αυτό εφαρμόζεται ενώ μόλις 4 συμμετέχοντες εξέφρασαν ότι αυτό δεν γίνεται (δεν εφαρμόζεται). Ένας πολύ μικρός αριθμός συμμετεχόντων που είναι συνολικά 3 δήλωσαν ότι αυτό παρουσιάζεται σε κάποιες περιπτώσεις (εν μέρη).

Ερώτηση 10.2: Ποια τεχνικά μέτρα έχετε λάβει για την προστασία των προσωπικών δεδομένων από μη εξουσιοδοτημένη πρόσβαση; [Λογισμικό προστασίας από ιούς που παρέχει προστασία ηλεκτρονικού ταχυδρομείου και προγράμματος περιήγησης στον ιστό]

Οι περισσότεροι ιοί μεταδίδονται μέσω του διαδικτύου, των μηνυμάτων ηλεκτρονικού ταχυδρομείου ή μέσω κακοπροαίρετων τοποθεσιών στο διαδίκτυο. Οπόταν είναι πολύ σημαντικό να υπάρχει ένα λογισμικό από ιούς ώστε να διασφαλίζει τις κινήσεις στο διαδίκτυο που γίνονται μέσω του προγράμματος περιήγησης και των μηνυμάτων που λαμβάνονται από το ηλεκτρονικό ταχυδρομείο. Ένα μεγάλο ποσοστό στις επιχειρήσεις που αγγίζει το 85% (47 από τους 55 συμμετέχοντες) εφαρμόζουν λογισμικό προστασίας από ιούς ενώ αντίθετα μόλις 5 επιχειρήσεις (10%) δήλωσαν ότι δεν εφαρμόζουν κάποιο λογισμικό. Ένα πολύ μικρό ποσοστό

που φτάνει στο 5% (3 συμμετέχοντες) ανάφεραν ότι εφαρμόζεται σε κάποιες περιπτώσεις (εν μέρη).

Ερώτηση 10.3: Ποια τεχνικά μέτρα έχετε λάβει για την προστασία των προσωπικών δεδομένων από μη εξουσιοδοτημένη πρόσβαση; [Το εταιρικό μας δίκτυο προστατεύεται από τοίχο προστασίας (firewall)]

Το firewall (τοίχος προστασίας) είναι ένα δυνατό εργαλείο σε μια επιχείρηση το οποίο δρα ως φράκτης μεταξύ στο Internet και στο εσωτερικό δίκτυο ή υπολογιστή και σταματάει διάφορους κινδύνους και επιθέσεις, συμπεριλαμβανομένων και ορισμένων ιών (virus). Άρα είναι πολύτιμο για την ασφάλεια μιας επιχείρησης που θέλει να προστατεύσει τα προσωπικά της δεδομένα από μη εξουσιοδοτημένους. Οι επιχειρήσεις το χρησιμοποιούν αρκετά και αυτό φαίνεται ότι από τις 55 επιχειρήσεις το χρησιμοποιούν οι 46 (84%) και μόνο 7 δήλωσαν ότι δεν το εφαρμόζουν ή όχι δεν υπάρχει (12%). Μόνο 2 επιχειρήσεις (4%) ανάφεραν ότι εφαρμόζεται σε κάποιες περιπτώσεις (εν μέρη).

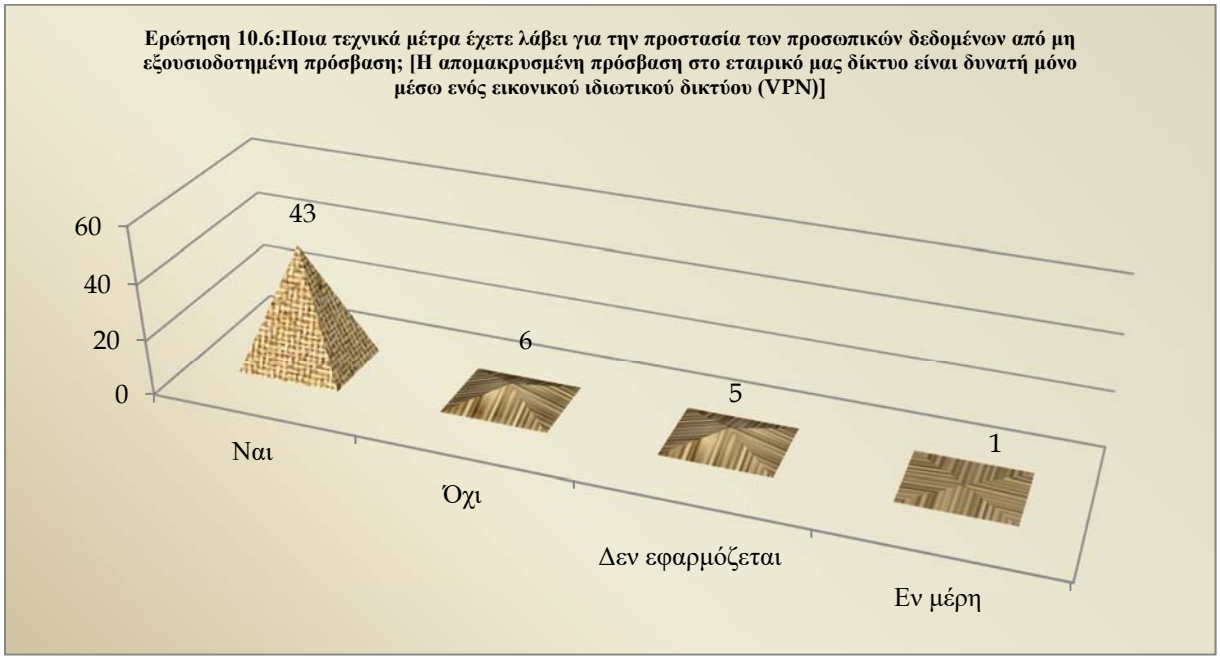
Ερώτηση 10.4: Ποια τεχνικά μέτρα έχετε λάβει για την προστασία των προσωπικών δεδομένων από μη εξουσιοδοτημένη πρόσβαση; [Τακτικό backup των προσωπικών δεδομένων εφαρμόζεται αυτόματα]

Η πραγματοποίηση τακτικών backup των προσωπικών δεδομένων που εφαρμόζεται αυτόματα μεγιστοποιούν τα επίπεδα ασφαλείας και συνεισφέρουν στον τελικό στόχο που είναι η προστασία και η ασφάλεια των δεδομένων που αποθηκεύονται στους διακομιστές (server). Οι επιχειρήσεις πλέον το εφαρμόζουν και αυτό δείχνει ότι το 93% (51 συμμετέχοντες) απάντησαν θετικά (ΝΑΙ) ενώ μόλις 3 επιχειρήσεις (5%) ανάφεραν ότι δεν εφαρμόζεται. Το 2% (1 συμμετέχοντας) δηλαδή μια επιχείρηση δήλωσε ότι η διαδικασία αυτή εφαρμόζεται εν μέρη (σε κάποια σημεία).

Ερώτηση 10.5: Ποια τεχνικά μέτρα έχετε λάβει για την προστασία των προσωπικών δεδομένων από μη εξουσιοδοτημένη πρόσβαση; [Το εταιρικό μας Wi-Fi προστατεύεται με κωδικό πρόσβασης]

Είναι σημαντικό να καθιερωθούν ενέργειες και διαδικασίες συμμόρφωσης όπως είναι η προστασία με κωδικό πρόσβασης στο επιχειρηματικό δίκτυο Wi-Fi ώστε να αποκλειστούν

φορητές συσκευές για να μειωθεί ο κίνδυνος παραβίασης των δεδομένων. Η προστασία με κωδικό πρόσβασης στο Wi-Fi μιας επιχείρησης έχει καθιερωθεί αφού το 95% (52 συμμετέχοντες) έχει δηλώσει ΝΑΙ ενώ μόλις το 5% (3 συμμετέχοντες) έχουν αναφέρει ότι δεν εφαρμόζεται.

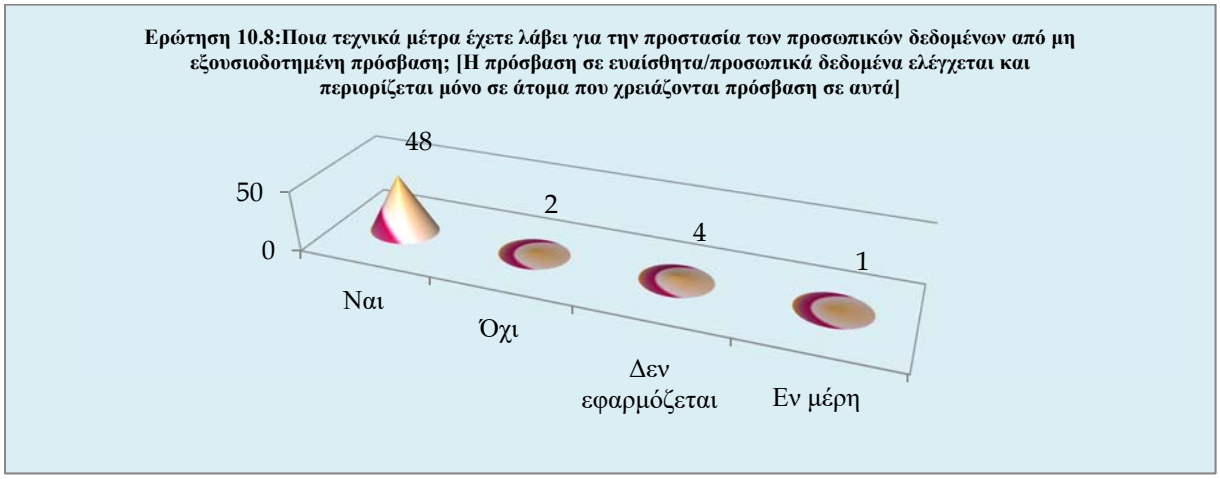


Σχήμα 5.13: Η απομακρυσμένη πρόσβαση στις επιχειρήσεις γίνεται μόνο μέσου εικονικού ιδιωτικού δικτύου (VPN: Virtual Private Network)

Το εικονικό ιδιωτικό δίκτυο (VPN) είναι ένα δίκτυο το οποίο συγκροτείται από εικονική υποδομή και λειτουργεί διαδικτυακά απαρτίζοντας το ίδιο επίπεδο ασφαλείας όπως και με κάθε ιδιωτικό δίκτυο. Οι λόγοι της χρησιμοποίησης των VPN είναι ότι χρησιμοποιούνται ως μια εναλλακτική λύση της κατασκευής των WAN (Wide Area Network) που υποκαθιστά ή επαυξάνουν τα υφιστάμενα ιδιωτικά δίκτυα τα οποία προσαρμόζουν μισθωμένες γραμμές οι οποίες ανήκουν στην επιχείρηση. Οπότε τα πλεονεκτήματα είναι αρκετά και αυτό φαίνεται και από το σχήμα 5.13 όπου χρησιμοποιείται σε υψηλό βαθμό με σύνολο 43 συμμετεχόντων από τους 55 να το κάνουν στην πράξη στις επιχειρήσεις που ασχολούνται. Σχετικά μικρός αριθμός συμμετεχόντων που αναλογούν στους 11 συμμετέχοντες ανάφεραν ότι δεν γίνεται υλοποιήσιμο αυτό ενώ μόλις 1 συμμετέχοντας υποστήριξε ότι αυτό συμβαίνει σε μερικές περιπτώσεις (εν μέρη).

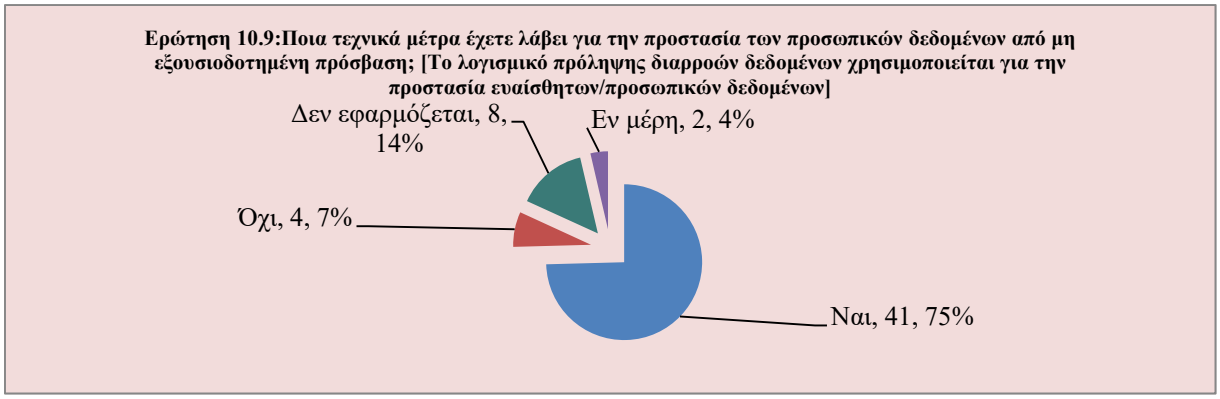
Σχήμα 5.14: Η σύνδεση χρηστών με προνομιακά δικαιώματα γίνεται μόνο από εξειδικευμένες συσκευές και οι λογαριασμοί τους δεν χρησιμοποιούνται καθημερινά. Επίσης η πρόσβαση περιορίζεται μόνο σε εξουσιοδοτημένα άτομα.

Ο προσδιορισμός και η χρήση των προνομιακών δικαιωμάτων προσπέλασης (σύνολο δικαιωμάτων ή χαρακτηριστικών σε ένα σύστημα τα οποία επιτρέπουν την παράκαμψη των μηχανισμών ελέγχου στο σύστημα) θα πρέπει να είναι ελεγχόμενα και περιορισμένα. Όταν στο σύστημα πραγματοποιηθεί ακατάλληλη η χρησιμοποίηση των προνομιακών δικαιωμάτων τότε υπάρχει μεγάλος κίνδυνος να παρουσιαστεί εισβολή από πρόσωπα που δεν είναι αποδεχτά. Συνεπάγεται ότι πρέπει να τηρείται αυστηρά και από ότι δείχνει το σχήμα 5.14 γίνεται και στην πραγματικότητα με ποσοστό που αγγίζει το 78% των επιχειρήσεων (43 συμμετέχοντες από τους 55). Η χρήση των προνομιακών δικαιωμάτων εφαρμόζεται σε μερικά περιστατικά (εν μέρη) όπως ανάφεραν 4 συμμετέχοντες (7%) ενώ οι υπόλοιποι 8 συμμετέχοντες (15%) δήλωσαν ότι δεν υφίσταται κάτι τέτοιο στην επιχείρηση.



Σχήμα 5.15: Εφαρμογή ελέγχου και περιορισμού μόνο στα άτομα που χρειάζονται πρόσβαση στα ευαίσθητα/προσωπικά δεδομένα

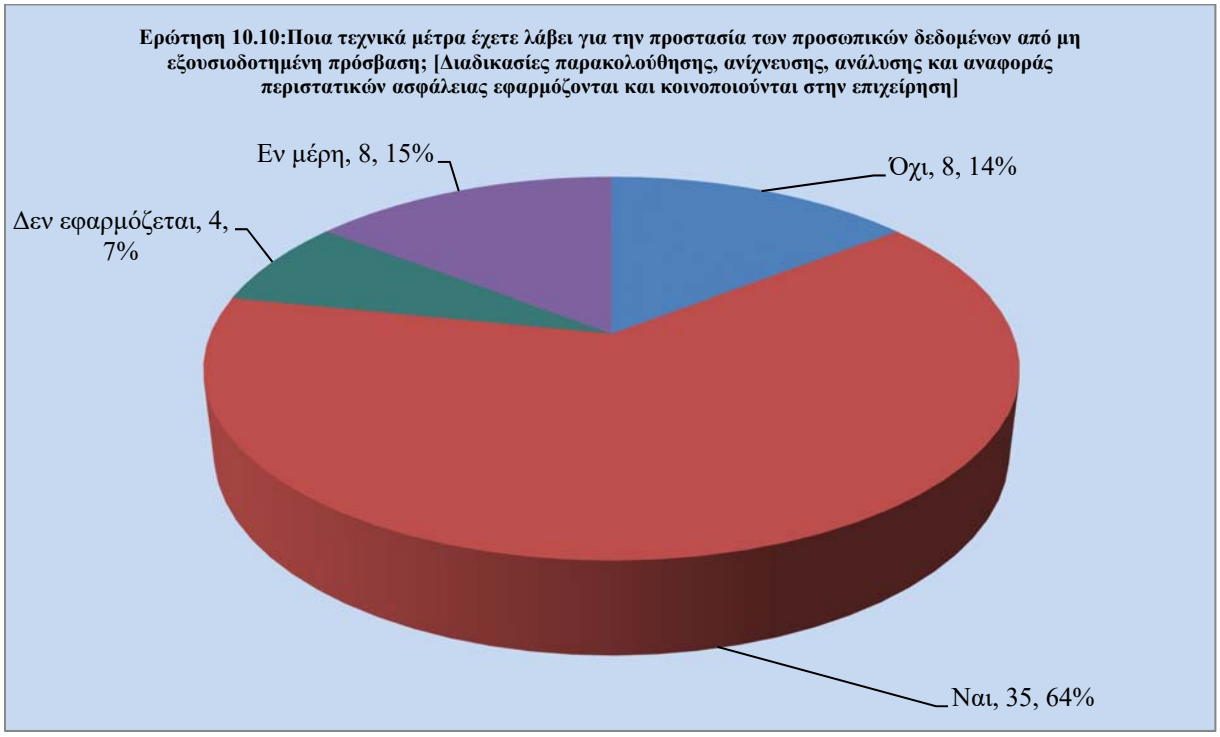
Η πρόσβαση στα προσωπικά/ευαίσθητα δεδομένα πρέπει να ελέγχεται και να περιορίζεται μόνο στα επιτρεπόμενα άτομα τα οποία έχουν εξουσιοδότηση για να πάρουν τις απαραίτητες πληροφορίες που χρειάζονται. Είναι σημαντικό να υπάρχουν αυτές οι διαδικασίες γιατί οποιοσδήποτε που έχει αποθηκευμένα ευαίσθητα/προσωπικά δεδομένα σε μια επιχείρηση μπορεί να ζητήσει ανά πάσα στιγμή πληροφορίες για το πώς χρησιμοποιήθηκαν ή χρησιμοποιούνται τα δεδομένα του. Έτσι θα γίνεται πιο αντιληπτό και ελεγχόμενο για το τι συμβαίνει πραγματικά με την διαχείριση των δεδομένων. Στο σχήμα 5.15 δίνει το μήνυμα ότι γίνεται και στην πράξη αυτό, με τους 48 συμμετέχοντες να δηλώνουν ότι γίνεται έλεγχος και περιορισμός στην πρόσβαση δεδομένων ενώ μόλις 6 συμμετέχοντες ανάφεραν ότι δεν τηρείται το ενδεχόμενο αυτό. Μόλις ένας συμμετέχοντας είπε ότι αυτή η διαδικασία εφαρμόζεται σε μερικές περιπτώσεις (εν μέρη).



Σχήμα 5.16: Λογισμικό πρόσληψης διαρροών εφαρμόζεται για την προστασία των ευαίσθητων/προσωπικών δεδομένων

Μια από τις σημαντικές πηγές διαρροών δεδομένων που προέρχεται από μέσα σε μια επιχείρηση είναι τα τερματικά της (ηλεκτρονική ή ηλεκτρομηχανική συσκευή). Τα εργαλεία και το λογισμικό πρόληψης διαρροών δεδομένων (DLP: data loss prevention) έχουν την ικανότητα να δίνουν μια πλήρη εικόνα για τις δραστηριότητες των τερματικών μιας επιχείρησης. Επιπρόσθετα μπορούν να χρησιμοποιηθούν για να φιλτράρουν και να προστατεύουν την ανταλλαγή δεδομένων στο εσωτερικό ενός επιχειρηματικού δικτύου. Αυτό το κάνει να είναι πολύτιμο για οποιαδήποτε επιχείρηση για να μπορεί να προστατεύσει τα προσωπικά/ευαίσθητα δεδομένα της και να αποτρέψει την διαρροή τους εκτός των επιθυμητών προορισμών. Στο σχήμα 5.16 δείχνει ότι σε μεγάλο ποσοστό των επιχειρήσεων που φτάνει στο 75% (41 συμμετέχοντες) έχουν εφαρμόσει αυτό το λογισμικό για να παρθούν τα κατάλληλα μέτρα προστασίας των δεδομένων. Μόλις 4%

των επιχειρήσεων (2 συμμετέχοντες) δήλωσαν ότι αυτό το μέτρο γίνεται σε κάποιες περιπτώσεις (εν μέρη) ενώ με ποσοστό 21% των επιχειρήσεων (12 συμμετέχοντες) ανάφεραν ότι το μέτρο αυτό δεν εφαρμόζεται καθόλου. Το ποσοστό του 21% είναι κάπως ψηλό όπου είναι σημείο για να αναφερθεί και θα πρέπει να δώσει το μήνυμα ότι οι επιχειρήσεις θα πρέπει να το εφαρμόσουν γιατί είναι πολύ βοηθητικό λογισμικό στον εντοπισμό και την πρόληψη των παρεμβάσεων από κακόβουλους.

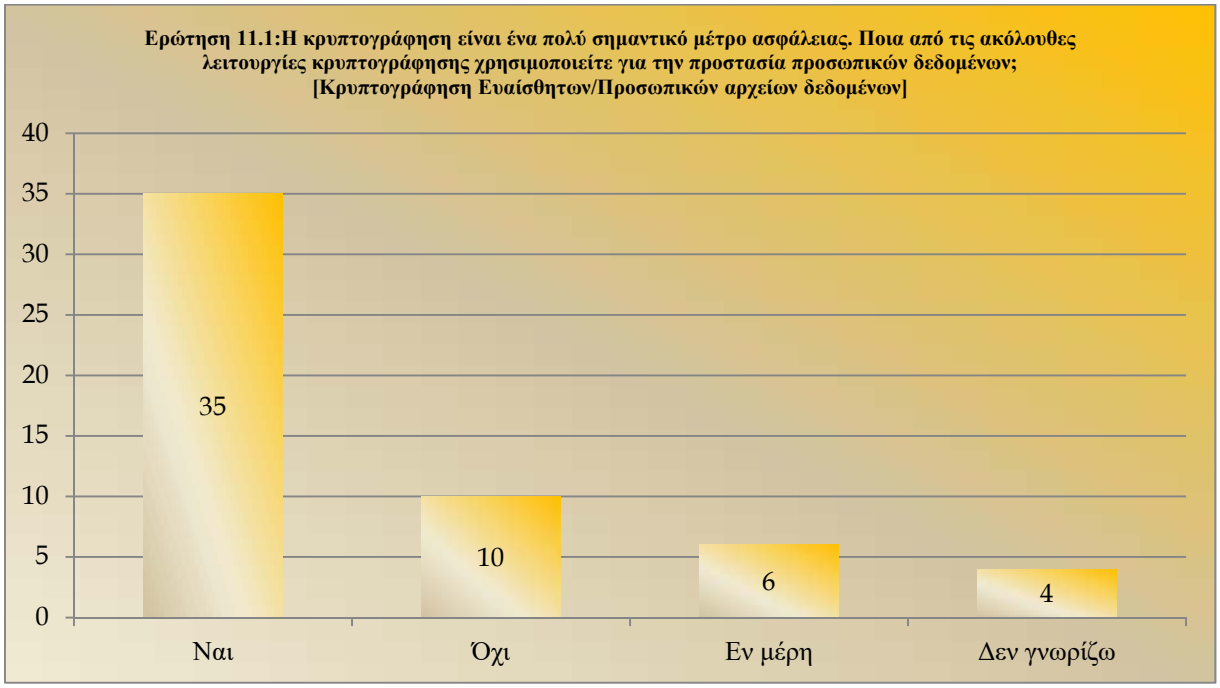


Σχήμα 5.17: Στις επιχειρήσεις εφαρμόζονται και κοινωνικοποιούνται οι διαδικασίες παρακολούθησης, ανίχνευσης, ανάλυσης και αναφοράς περιστατικών ασφαλείας

Οι διαδικασίες παρακολούθησης, ανίχνευσης, ανάλυσης και αναφοράς περιστατικών ασφάλειας εφαρμόζονται και κοινοποιούνται στην επιχείρηση με σκοπό την έγκαιρη αναγνώριση, εντοπισμό, διερεύνηση και αντιμετώπιση περιστατικών παραβίασης της ασφάλειας. Επίσης βοηθούν στον περιορισμό της έκτασης των ζημιών και καταστροφών όπως και στην ελαχιστοποίηση των επιπτώσεων που επιφέρουν στην λειτουργία της επιχείρησης. Αυτό δείχνει ότι είναι απαραίτητη μια τέτοια διαδικασία, η οποία πρέπει να εφαρμόζεται με συνέπεια και φαίνεται ότι σχετικά γίνεται σε ένα ικανοποιητικό βαθμό που αγγίζει το 64% (35 συμμετέχοντες), ενώ το 21% (12 συμμετέχοντες) δήλωσαν ότι δεν εφαρμόζεται. Το 21% είναι ένα ποσοστό που πρέπει να προβληματίσει γιατί φανερώνει ότι τα προσωπικά δεδομένα μένουν εκτεθειμένα σε τρίτους και μπορεί να παραβιαστούν. Οι υπόλοιποι 8 συμμετέχοντες (15%)

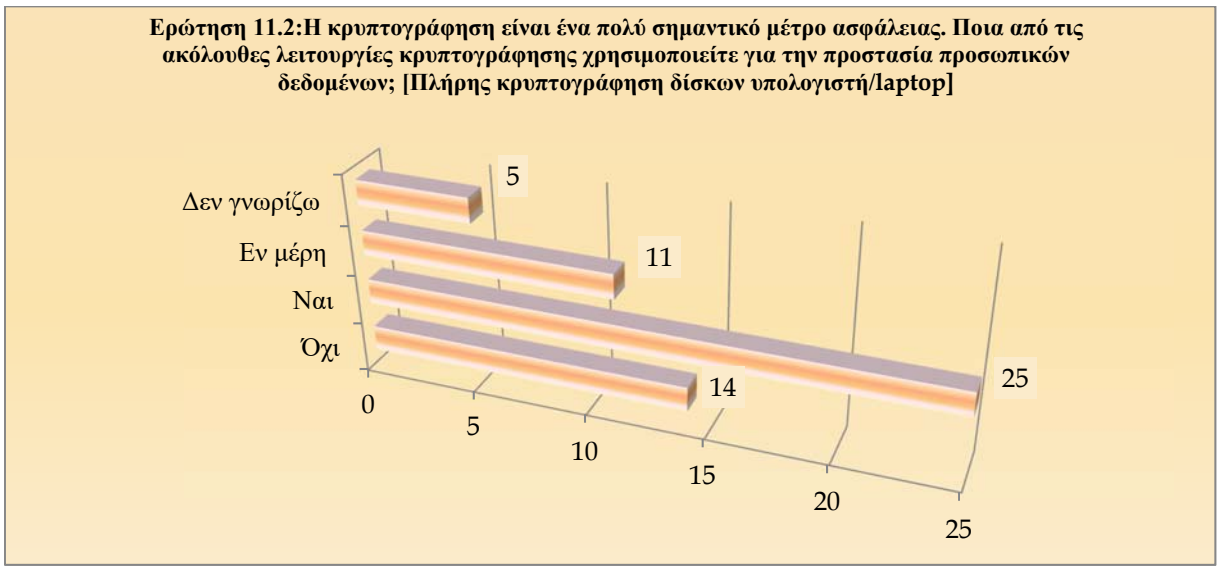
εκφράστηκαν ότι αυτή η διαδικασία δεν γίνεται εξολοκλήρου (εν μέρη) που και αυτό περικλείει κινδύνους στην ασφάλεια των προσωπικών δεδομένων.

Ερώτηση 11.1 μέχρι 11.5: Το GDPR προτείνει την κρυπτογράφηση η οποία πληροί της προϋποθέσεις για την υλοποίηση των τεχνικών μέτρων για την εκπλήρωση της συμμόρφωσης με ορισμένες από τις υποχρεώσεις του. Είναι αναγκαίο πάντα να γίνεται εξέταση ότι η κρυπτογράφηση εφαρμόζεται τόσο στα δεδομένα που μεταφέρονται (διαμέσου του διαδικτύου) όπως και για τα δεδομένα που είναι ακίνητα (αποθηκευμένα σε διάφορα μέσα).



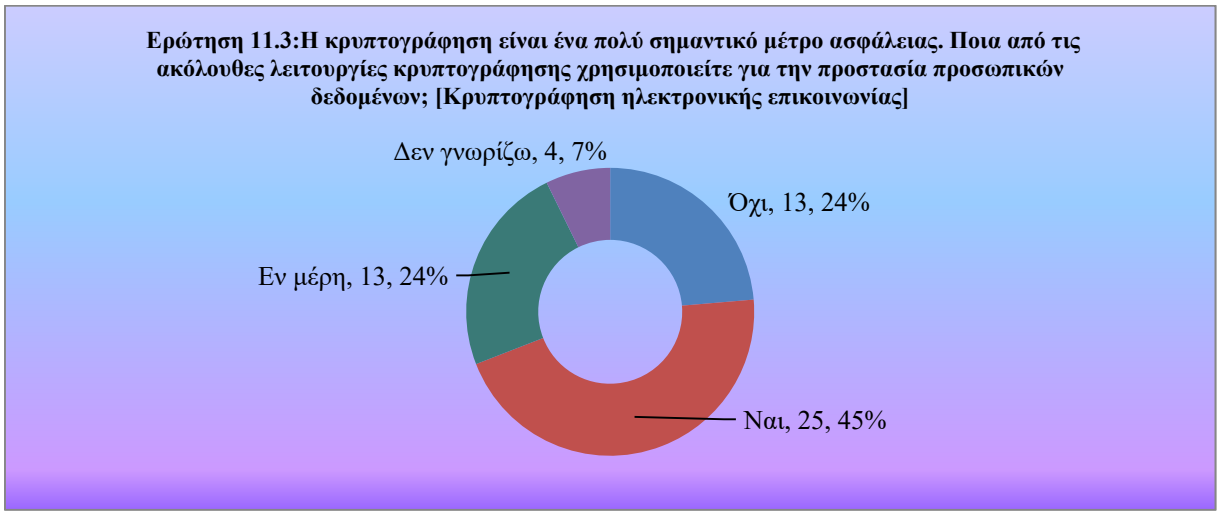
Σχήμα 5.18: Κρυπτογράφηση ευαίσθητων/προσωπικών αρχείων δεδομένων

Η κρυπτογράφηση εξασφαλίζει το απόρρητο των προσωπικών δεδομένων και έτσι γίνεται μια αναγκαία διαδικασία για να μην μπορούν να αναγνωριστούν όταν κλαπούν. Πλέον οι επιχειρήσεις έχουν βάλει την διαδικασία κρυπτογράφησης (έχουν ευαισθητοποιηθεί) στα μέτρα προστασίας των προσωπικών δεδομένων και αυτό είναι ένα καλό σημάδι αφού θεωρούνται σημαντικά. Από τους 55 συμμετέχοντες οι 35 έχουν αναφέρει ότι σαφώς πραγματοποιείται η κρυπτογράφηση των ευαίσθητων/προσωπικών αρχείων δεδομένων και 10 συμμετέχοντες απάντησαν ότι δεν γίνεται καμία κρυπτογράφηση. Συνολικά 6 συμμετέχοντες ανάφεραν ότι η κρυπτογράφηση γίνεται εν μέρη δηλαδή σε κάποια άλλα προσωπικά δεδομένα θεωρούν ότι δεν χρειάζεται να γίνει και 4 συμμετέχοντες δήλωσαν ότι δεν γνωρίζουν. Η κρυπτογράφηση γίνεται συνήθως στο τμήμα της τεχνολογίας/υπολογιστών και δικτύων, οπόταν κάποιοι ίσως να μην γνωρίζουν την διαδικασία αυτήν αφού δεν ανήκουν στον τμήμα αυτό.



Σχήμα 5.19: Η κρυπτογράφηση δίσκων του υπολογιστή/laptop εφαρμόζεται πλήρης

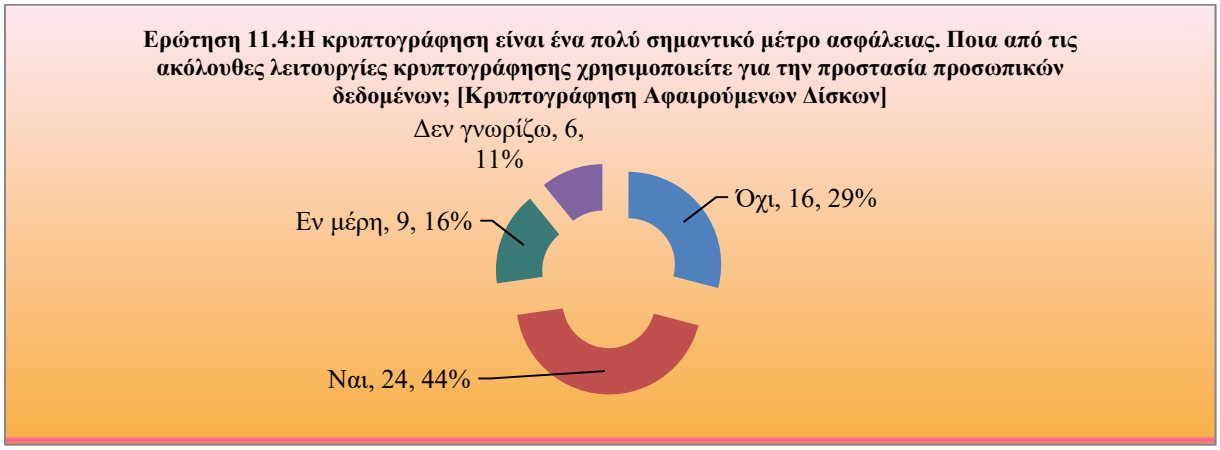
Φαίνεται στις επιχειρήσεις η πλήρης κρυπτογράφηση δίσκων υπολογιστών και laptop, υλοποιείται σε κάποιο βαθμό γιατί μόλις λίγο πιο κάτω από τους μισούς έχουν απαντήσει ότι γίνεται πραγματικά (25 από τους 55 συμμετέχοντες). Σχετικά υψηλό ποσοστό (14 συμμετέχοντες) δήλωσαν ότι δεν γίνεται καθόλου κρυπτογράφηση και αυτό είναι ένα θέμα που προβληματίζει γιατί η φύλαξη των δεδομένων θα έπρεπε να είναι το Α και το Ω. Κάποιοι από τους συμμετέχοντες (συνολικά 11) αποκάλυψαν ότι η κρυπτογράφηση δεν εφαρμόζεται σε όλες τις λειτουργίες δηλαδή εν μέρη ενώ 5 συμμετέχοντες ανάφεραν ότι δεν είναι ενήμεροι αν εφαρμόζεται αυτή η συγκεκριμένη λειτουργία της κρυπτογράφησης.



Σχήμα 5.20: Κρυπτογράφηση ηλεκτρονικής επικοινωνίας (email)

Η ηλεκτρονική επικοινωνία είναι από τους βασικούς τρόπους επικοινωνίας και η ασφάλεια της είναι σημαντική. Οι κίνδυνοι παραβίασης του προσωπικού απορρήτου είναι πολλοί για αυτό

απαιτείται η κρυπτογράφηση. Μόλις το 45% (25 συμμετέχοντες) εφαρμόζουν την κρυπτογράφηση, ενώ 13 συμμετέχοντες δεν την υλοποιούν καθόλου. Σε μερικές περιπτώσεις χρησιμοποιείται (δηλαδή εν μέρη, 13 συμμετέχοντες) και μόλις 4 συμμετέχοντες δήλωσαν ότι δεν ξέρουν αν πραγματοποιείται η κρυπτογράφηση στην ηλεκτρονική επικοινωνία.



Σχήμα 5.21: Κρυπτογράφηση αφαιρούμενων δίσκων

Η κρυπτογράφηση των αφαιρούμενων δίσκων γίνεται αναγκαία διαδικασία, γιατί έτσι προφυλάσσονται τα προσωπικά δεδομένα αν υπάρξει κλοπής του δίσκου. Από τη στιγμή που δεν είναι μέσα στον υπολογιστή φαντάζει και πιο εύκολο αν γίνει στόχος κλοπής. Οπότε αν γίνει σωστή κρυπτογράφηση δεν θα μπορούν εύκολα να ανακτηθούν τα προσωπικά δεδομένα. Όχι ψηλό ποσοστό, μόλις 44% (συνολικά 24 συμμετέχοντες) δήλωσαν ότι υλοποιείται η κρυπτογράφηση, ενώ προβληματίζει το γεγονός ότι 16 από τους συμμετέχοντες ανάφεραν ότι δεν υφίσταται κάτι τέτοιο. Η εν μέρη κρυπτογράφηση παρουσιάστηκε από 9 συμμετέχοντες, πράγμα που προβληματίζει και συνολικά 6 συμμετέχοντες απάντησαν ότι δεν γνωρίζουν αν γίνεται η συγκεκριμένη κρυπτογράφηση.

Σχήμα 5.22: Κρυπτογράφηση φακέλου δικτύου/cloud

Ο καταλληλότερος τρόπος για ασφαλή διατήρηση πολύτιμων πληροφοριών είναι σε κρυπτογραφικούς φακέλους οι οποίοι θα αποθηκεύονται σε φυσικά μέσα αλλά και σε περιβάλλον cloud*. Έτσι θα προστατεύονται τα προσωπικά δεδομένα των χρηστών από τις απειλές. Άρα είναι πολύ σημαντικό να γίνεται η κρυπτογράφηση φακέλου δικτύου/cloud. Όμως στο σχήμα 5.22 φαίνεται καθαρά ότι δεν εφαρμόζεται σε μεγάλο ποσοστό αφού μόλις 27 συμμετέχοντες είπαν ότι γίνεται σε πράξη και 14 συμμετέχοντες (σχετικά μεγάλος αριθμός) δήλωσαν ότι δεν συμβαίνει η συγκεκριμένη κρυπτογράφηση. Έχουν αναφέρει 9 συμμετέχοντες ότι η κρυπτογράφηση εφαρμόζεται ως ένα σημείο (εν μέρη) και μόλις 5 συμμετέχοντες διατύπωσαν άποψη ότι δεν γνωρίζουν.

Ερώτηση 12.1 μέχρι 12.6: Η δεξιότητα των υποκειμένων των δεδομένων να διεκδικήσουν τα δικαιώματα τους είναι απαραίτητο στοιχείο για την επεξεργασία των προσωπικών δεδομένων.

Όταν δεν έχουν πραγματοποιηθεί οι ανάλογες ενέργειες μετά από αίτηση του υποκειμένου των δεδομένων, είναι αναγκαίο να πληροφορήσουν άμεσα για την αιτία που δεν έχει διεκπεραιωθεί, ενώ ενδέχεται να υποβληθεί καταγγελία σε εποπτική αρχή, επιδιώκοντας να ανασταλεί η εφαρμογή της επεξεργασίας προσωπικών δεδομένων.

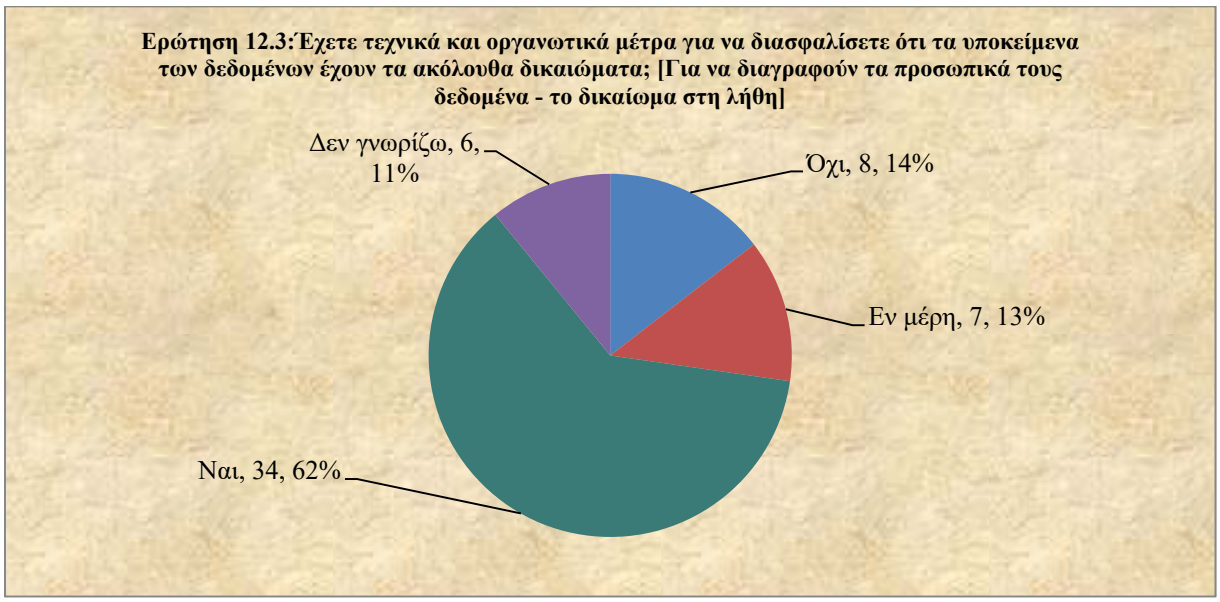
Σχήμα 5.23: Δικαίωμα υποκειμένων για απόκτηση πρόσβασης στα επεξεργασμένα προσωπικά τους δεδομένα

* περιβάλλον cloud: περιγράφει μια επιχείρηση ή έναν άτομο που χρησιμοποιεί μια εφαρμογή που βασίζεται στο διαδίκτυο για κάθε εργασία παρά την εγκατάσταση λογισμικού ή την αποθήκευση δεδομένων σε έναν υπολογιστή.

Τα υποκείμενα (άνθρωποι) των δεδομένων έχουν το δικαίωμα να ζητήσουν πρόσβαση στα προσωπικά τους δεδομένα, να ρωτήσουν πως χρησιμοποιούνται αυτά και από ποιόν επεξεργάζονται μετά την συλλογή τους. Αυτό υφίσταται σε ένα καλό ποσοστό που φτάνει το 67% (37 συμμετέχοντες) ενώ μόλις το 15% (8 συμμετέχοντες) δήλωσαν ότι δεν μπορεί να διασφαλιστεί το δικαίωμα αυτό. Έχουν αναφέρει 7 συμμετέχοντες (13%) ότι αυτό παρουσιάζεται όχι στον απόλυτο βαθμό (εν μέρη) και 3 συμμετέχοντες (5%) εκφράστηκαν ότι δεν γνωρίζουν αν τηρείται το δικαίωμα αυτό.

Σχήμα 5.24: Δικαίωμα υποκειμένων για να αποκατασταθούν οι ανακρίβειες των προσωπικών τους δεδομένων

Ένα από τα δικαιώματα των υποκείμενων που έχουν σχέση με τα δεδομένα είναι η απαίτηση να επαναφερθούν οι ανακρίβειες των προσωπικών τους δεδομένων δηλαδή αν έχει εξακριβωθεί ότι τα στοιχεία δεν είναι πλήρης ή λανθασμένα τότε μπορεί να ζητηθεί η ενημέρωση τους (διορθώσεις οποιεσδήποτε ανακρίβειες στα προσωπικά δεδομένα). Ένα ψηλό ποσοστό από τους συμμετέχοντες που φτάνει στο 69% (38 συμμετέχοντες) ανάφεραν ότι μπορούν να διασφαλίσουν το δικαίωμα αυτό ενώ 7 συμμετέχοντες (13%) δήλωσαν ότι αυτό δεν μπορεί να γίνει (όχι). Έχουν εκφράσει 6 συμμετέχοντες (11%) ότι το σε κάποιο βαθμό (εν μέρη) πραγματοποιείται το δικαίωμα αυτό και 4 συμμετέχοντες (7%) γνωστοποίησαν ότι δεν γνωρίζουν κατά πόσο εφαρμόζεται.

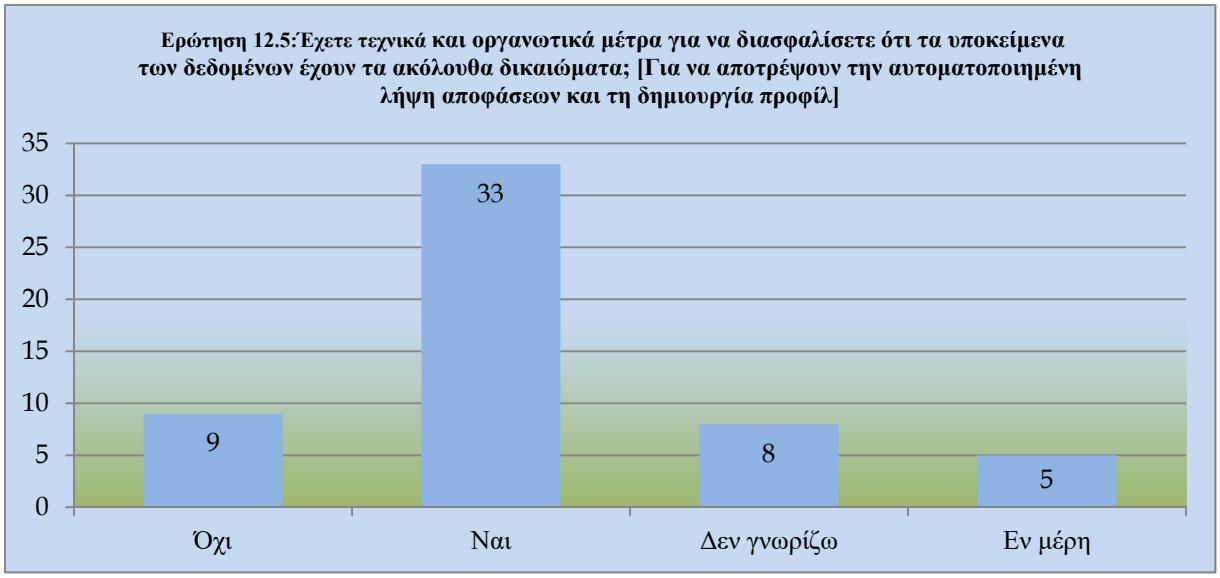


Σχήμα 5.25: Δικαίωμα υποκειμένων να διαγράψουν τα προσωπικά τους δεδομένα-το δικαίωμα στη λήθη

Το δικαίωμα στη λήθη είναι ένα δικαίωμα σύμφωνα το οποίο είναι δυνατόν κάποιο άτομο να αποσύρει την συγκατάθεση που έχει παραχωρήσει για χρήση των προσωπικών του δεδομένων σε μια επιχείρηση καθώς ενδέχεται να ζητήσει ακόμη και την διαγραφή τους. Τα δικαίωμα αυτό διασφαλίζεται σε ένα καλό ποσοστό από τις επιχειρήσεις που αγγίζει το 62% (34 συμμετέχοντες από τους 55), ενώ 8 συμμετέχοντες (14%) ανάφεραν ότι αδυνατεί να διασφαλιστεί το δικαίωμα αυτό. «Εν μέρη» δήλωσαν 7 συμμετέχοντες (13%) και 6 συμμετέχοντες (11%) απάντησαν ότι δεν γνωρίζουν κάτι για το δικαίωμα αυτό.

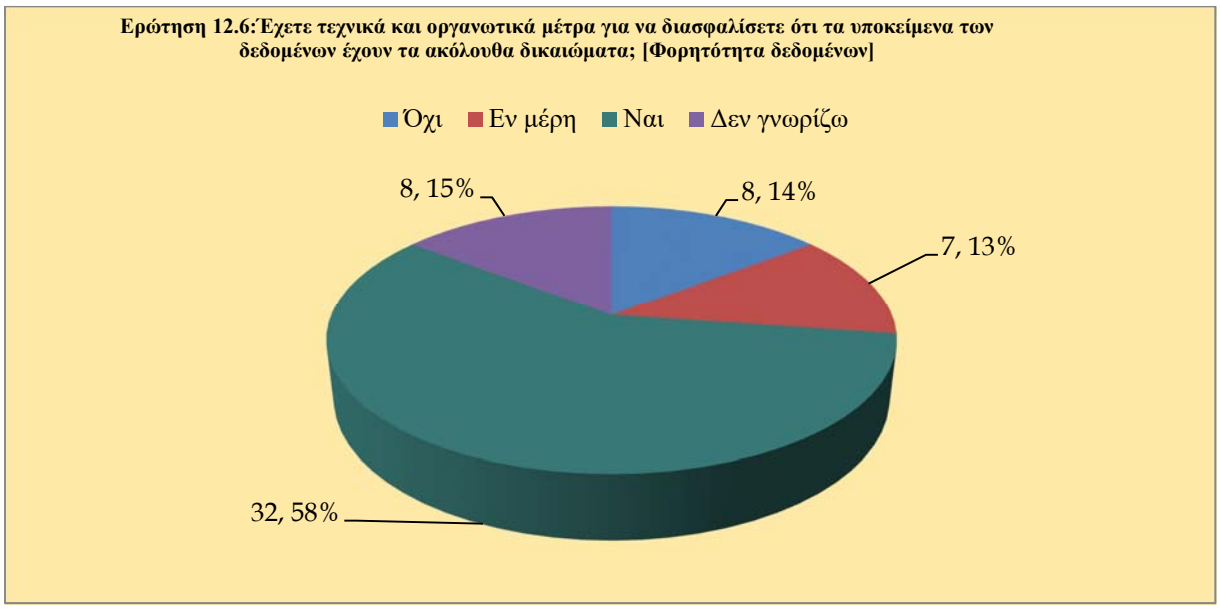
Σχήμα 5.26: Δικαίωμα υποκειμένων να αποτρέψουν τις άμεσες προωθητικές ενέργειες

Για την αποτροπή των άμεσων προωθητικών ενεργειών, τα υποκείμενα των δεδομένων έχουν το δικαίωμα να ζητήσουν από μια επιχείρηση να μην επεξεργάζεται τα προσωπικά δεδομένα που έχουν αποθηκευτεί για αυτούς. Οι πληροφορίες θα μείνουν αποθηκευμένες, όμως η επιχείρηση δεν θα έχει την ικανότητα να τις εκμεταλλευτεί. Στο σχήμα 5.26, φαίνεται ότι οι περισσότερες επιχειρήσεις διασφαλίζουν το δικαίωμα αυτό στα υποκείμενα των δεδομένων με 35 συμμετέχοντες (63%) να λένε ναι ενώ 7 συμμετέχοντες (13%) δήλωσαν κάτι τέτοιο δεν υφίσταται (όχι). Σε κάποιο βαθμό (εν μέρη) ανάφεραν 6 συμμετέχοντες (11%) και 7 συμμετέχοντες (13%) γνωστοποίησαν ότι δεν γνωρίζουν.



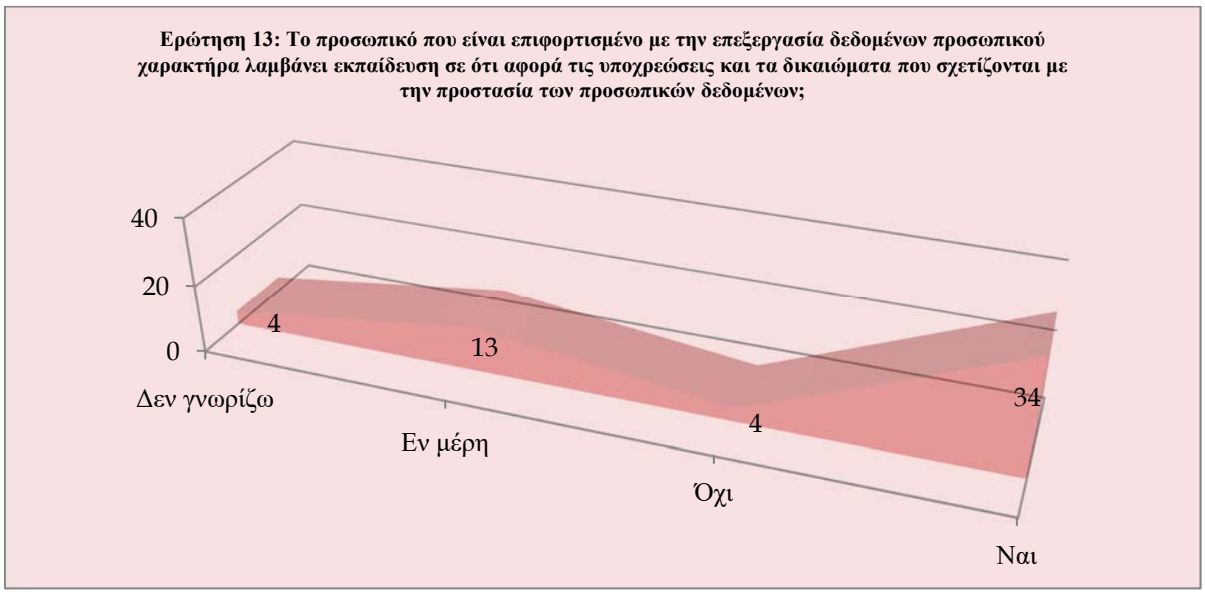
Σχήμα 5.27: Δικαίωμα υποκειμένων να αποτρέψουν την αυτοματοποιημένη λήψη αποφάσεων και τη δημιουργία προφίλ

Η εξέλιξη στην τεχνολογία και οι δυνατότητες της ανάλυσης μαζικών δεδομένων, της τεχνητής νοημοσύνης, και της νοημοσύνης των μηχανών (machine learning) έχουν διευκολύνει την δημιουργία προφίλ καθώς και τη λήψη αυτοματοποιημένων αποφάσεων. Το γεγονός αυτό δημιουργεί σοβαρές απειλές στα δικαιώματα και τις ελευθερίες των ανθρώπων και είναι ένας επιπρόσθετος λόγος για να πραγματοποιηθούν κατάλληλες εγγυήσεις. Λίγο πιο πάνω από τους μισούς συμμετέχοντες, 33 συμμετέχοντες (60%) ανάφεραν ότι διασφαλίζουν το δικαίωμα αυτό στα υποκείμενα των δεδομένων ενώ 9 συμμετέχοντες (16%) δήλωσαν όχι. Συνολικά 5 συμμετέχοντες (9%) εκφράστηκαν ότι αυτό το δικαίωμα γίνεται σε κάποιο βαθμό (εν μέρη) και 8 συμμετέχοντες (15%) αποκάλυψαν ότι δεν γνωρίζουν αν το δικαίωμα αυτό εφαρμόζεται.



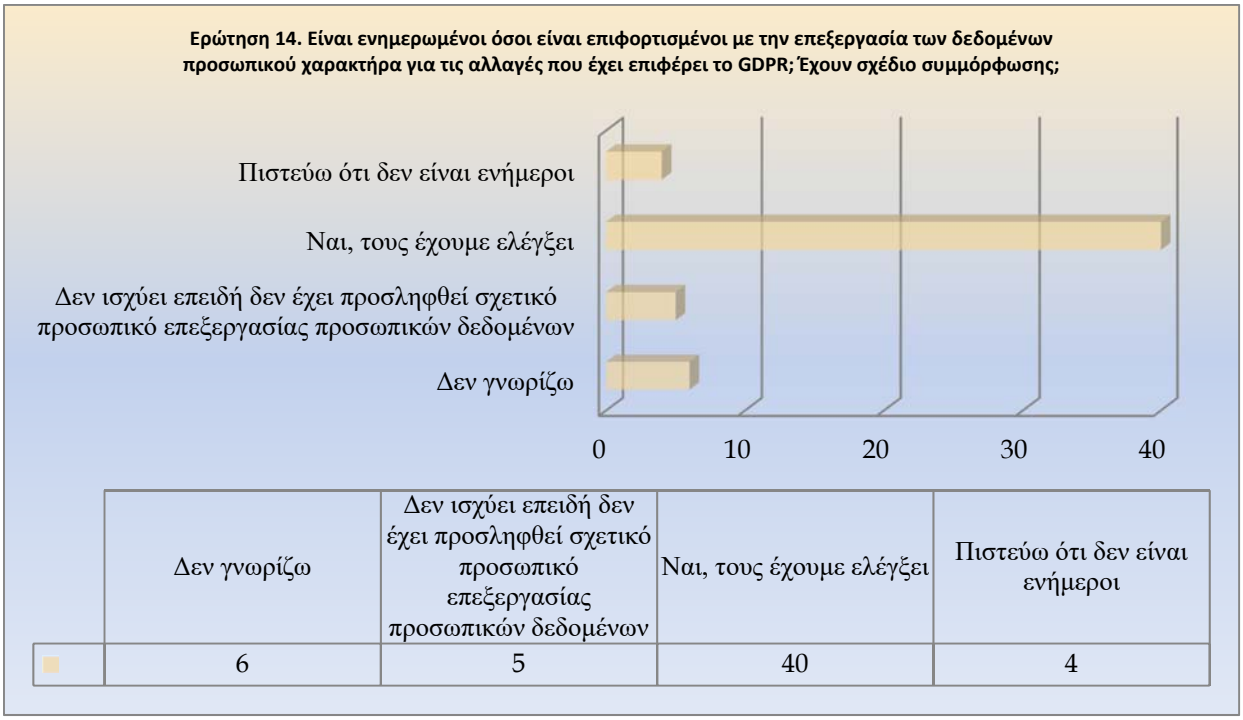
Σχήμα 5.28: Δικαίωμα υποκειμένων στην φορητότητα δεδομένων

Η φορητότητα των δεδομένων είναι ένα δικαίωμα που μπορεί οποιοδήποτε να μεταφέρει τα δεδομένα του όποτε το επιθυμεί από ένα πάροχο σε έναν άλλο. Στις επιχειρήσεις έχουν λάβει σοβαρά υπόψη τα δικαιώματα των υποκειμένων των δεδομένων όπως είναι η φορητότητα, με 32 συμμετέχοντες (58%) να δηλώνουν ναι ενώ 8 συμμετέχοντες (14%) ανάφεραν ότι δε διασφαλίζουν το δικαίωμα αυτό (όχι). Συνολικά 8 συμμετέχοντες (15%) αποκάλυψαν ότι δε γνωρίζουν αν παρέχεται αυτό το δικαίωμα και οι υπόλοιποι 7 συμμετέχοντες (13%) εξέφρασαν ότι αυτό το δικαίωμα υλοποιείται σε κάποιο βαθμό (εν μέρη).



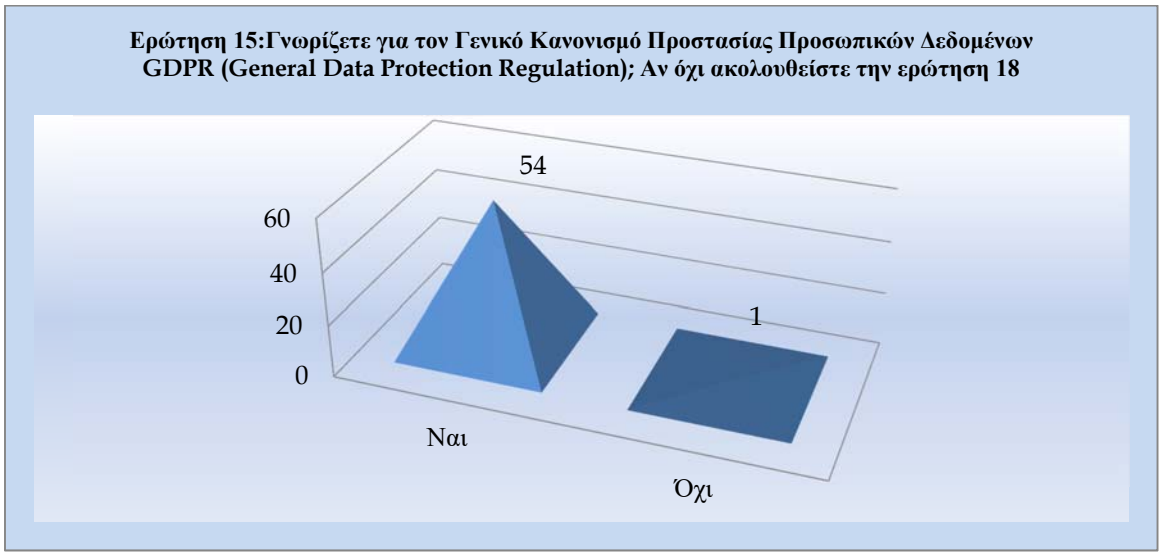
Σχήμα 5.29: Το προσωπικό που επεξεργάζεται τα προσωπικά δεδομένα λαμβάνει εκπαίδευση για τα δικαιώματα και υποχρεώσεις που αφορούν την προστασία προσωπικών δεδομένων

Το GDPR απαιτεί κατάρτιση του προσωπικού που εμπλέκεται σε εργασίες επεξεργασίας δεδομένων προσωπικού χαρακτήρα. Οι επιχειρήσεις απ' ότι φαίνεται κρατούν ενήμερο το προσωπικό που σχετίζονται με την επεξεργασία δεδομένων προσωπικού χαρακτήρα (34 συμμετέχοντες), ενώ 4 συμμετέχοντες δήλωσαν ότι δεν παρέχεται καθόλου εκπαίδευση στο προσωπικό που εμπλέκεται. Συνολικά 13 συμμετέχοντες αποκάλυψαν ότι γίνεται εν μέρη η εκπαίδευση δηλαδή όχι εξ' ολοκλήρου (σε μερικά σημεία) και άλλοι 4 συμμετέχοντες δήλωσαν ότι δεν γνωρίζουν αν παρέχεται η κατάλληλη εκπαίδευση στο προσωπικό επεξεργασίας δεδομένων προσωπικού χαρακτήρα.



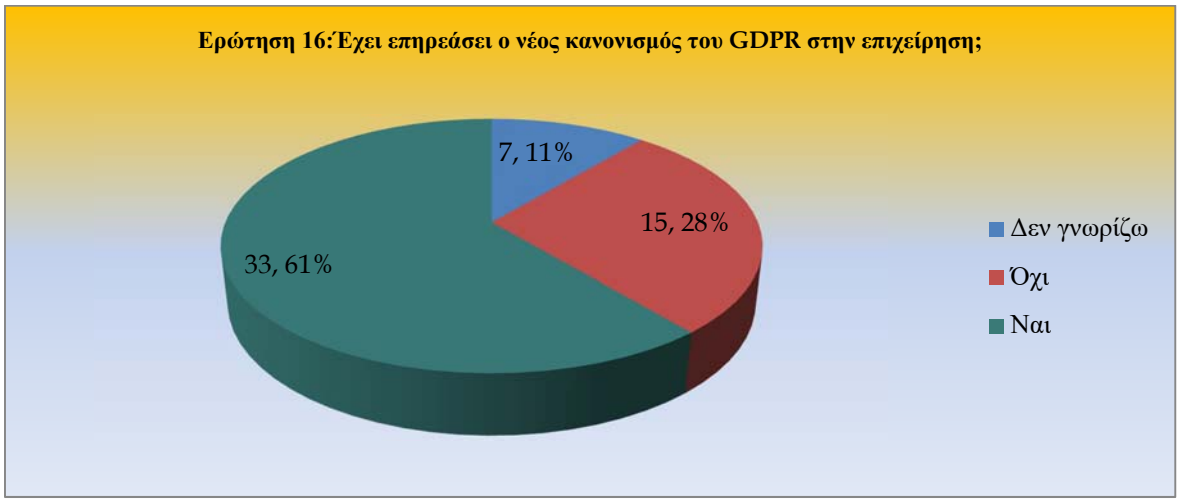
Σχήμα 5.30: Κατά πόσον ενημερώνονται οι άμεσα εμπλεκόμενοι που επεξεργάζονται τα προσωπικά δεδομένα για τις αλλαγές του GDPR και αν υπάρχει σχέδιο συμμόρφωσης;

Η επεξεργασία προσωπικών δεδομένων σε μία επιχείρηση μπορεί να είναι περίπλοκη διαδικασία που στις περισσότερες περιπτώσεις περιλαμβάνει την ανταλλαγή δεδομένων με όσους έχουν επιφορτιστεί με τη διαδικασία αυτή (όταν δηλαδή τα δεδομένα μεταφέρονται σε τρίτους). Είναι σημαντικό τα άτομα αυτά να είναι ενήμεροι, να γνωρίζουν τα καθήκοντα και ευθύνες τους. Ένας μεγάλος αριθμός των επιχειρήσεων μέσω των συμμετεχόντων (συνολικά 40) δηλώνουν ότι το προσωπικό είναι ενήμεροι για τις αλλαγές που έχει επιφέρει το GDPR ενώ ένας μικρός αριθμός των συμμετεχόντων (συνολικά 5) ανάφεραν ότι δεν είναι ενήμεροι για τον λόγο ότι δεν έχει προσληφθεί προσωπικό για την επεξεργασία προσωπικών δεδομένων. Άλλη μια μικρή μερίδα των συμμετεχόντων (4 συμμετέχοντες) πιστεύουν ότι δεν είναι ενήμεροι και οι υπόλοιποι 6 συμμετέχοντες δεν γνωρίζουν καθόλου τι γίνεται.



Σχήμα 5.31: Γνωρίζετε για τον Γενικό Κανονισμό Προστασίας Προσωπικών Δεδομένων (GDPR);

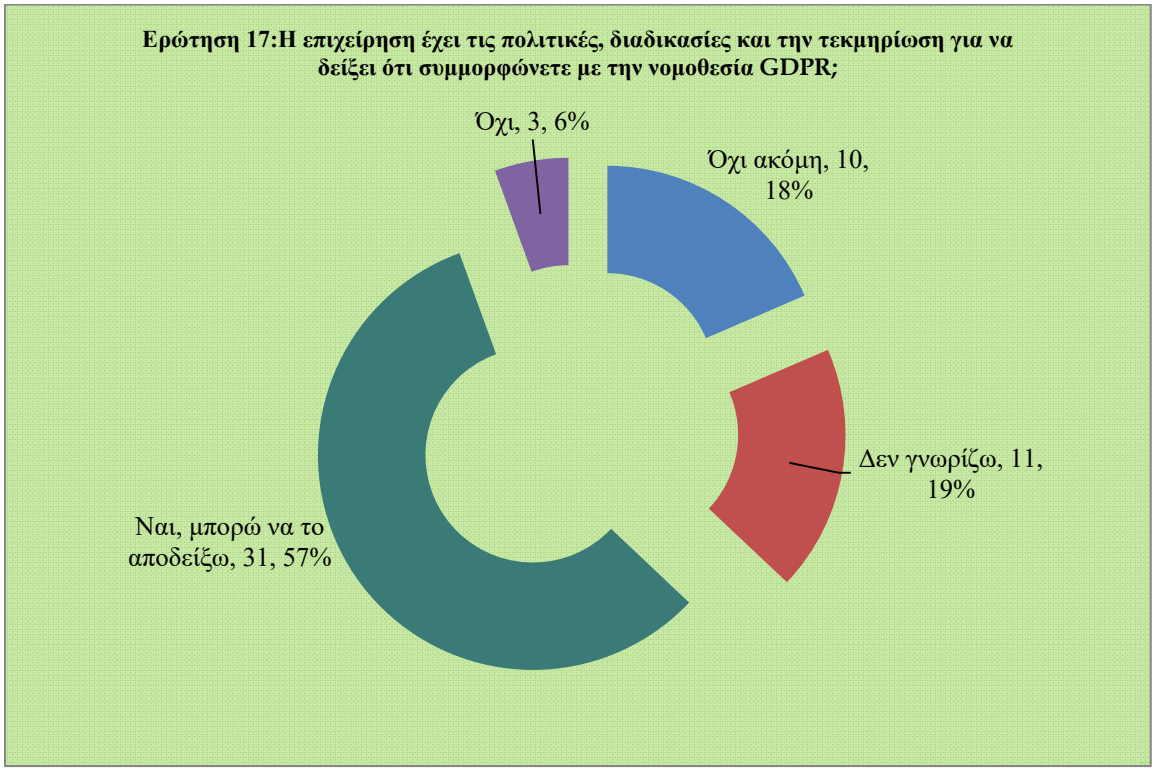
Οι πρωτοτυπίες που εισάγει ο κανονισμός επιδιώκουν να προκαλέσουν ένα ομοιόμορφο, συνεκτικός και αυστηρότερο πλαίσιο προστασίας των προσωπικών δεδομένων προσωπικού. Έτσι οι επιχειρήσεις προτρέπονται να μεταρρυθμίσουν τις δομές τους και να παρθούν τα αναγκαία μέτρα για τη συμμόρφωση. Από ότι παρουσιάζεται στο σχήμα 5.31, από τους 55 συμμετέχοντες που έχουν ερωτηθεί στην συγκεκριμένη ερώτηση φαίνεται, καθαρά ότι οι ερωτηθέντες γνωρίζουν για τον κανονισμό του GDPR (συνολικά 54) και αυτό είναι θετικό, ενώ μόνο ένας δεν γνωρίζει τίποτα για τον κανονισμό του GDPR.



Σχήμα 5.32: Ο νέος κανονισμός του GDPR έχει επηρεάσει τις επιχειρήσεις;

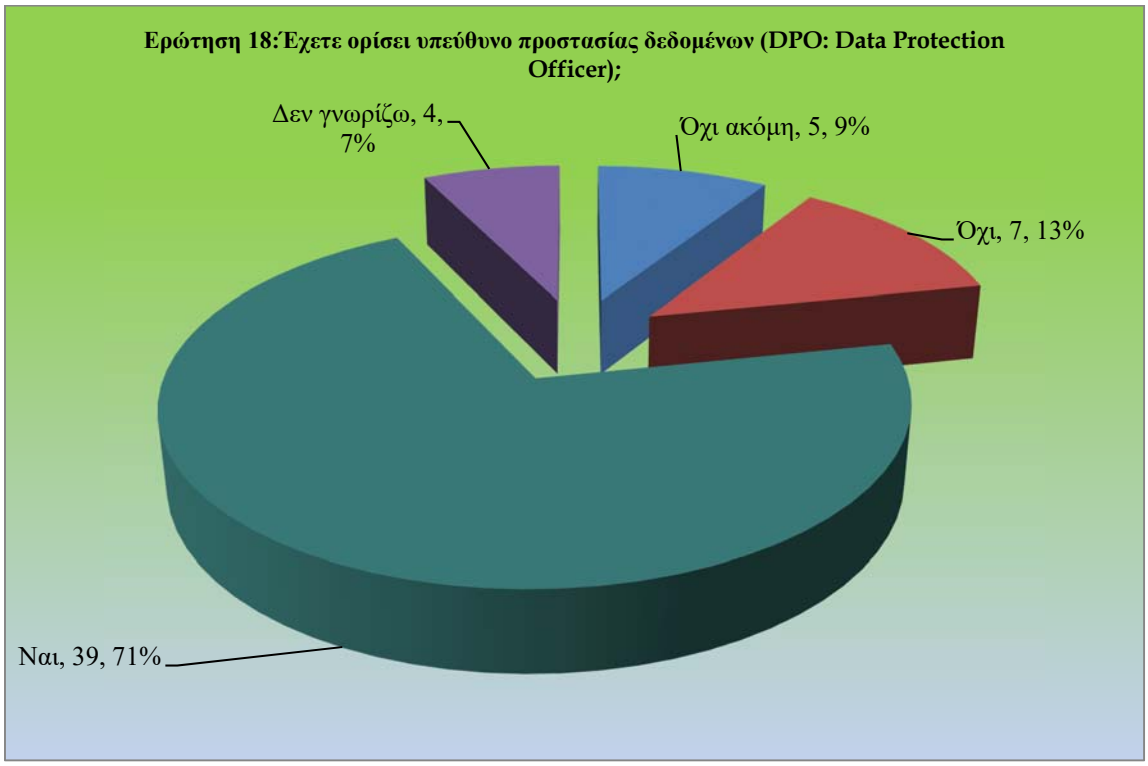
Γενικά οι επιχειρήσεις έχουν επηρεαστεί σε ψηλό βαθμό (61%) λόγω του ότι με τον κανονισμό του GDPR οι επιχειρήσεις θα πρέπει να προσαρμοστούν στα δεδομένα που ορίζει, αφού θα

πρέπει να διαθέτουν τις κατάλληλες διαδικασίες και τεχνολογία για να μπορούν να αξιολογούν το μέγεθος παραβίασης που μπορεί να προκληθεί. Όλα αυτά χρειάζονται αρκετό χρονικό διάστημα για να υλοποιηθούν και σίγουρα κοστίζουν π.χ. πρέπει να υπάρχει συμβατότητα συστημάτων, να πάρουν συμβουλές από ειδικούς (π.χ. δικηγόρους), να προσλάβουν προσωπικό (υπεύθυνο επεξεργασίας δεδομένων). Ένα μέρος των συμμετεχόντων (15 στο σύνολο) ανέφεραν ότι δεν έχουν επηρεαστεί οι επιχειρήσεις που εργάζονται, ενώ 7 συμμετέχοντες δεν έχουν γνώμη για το αν έχουν επηρεαστεί πράγματι οι επιχειρήσεις.



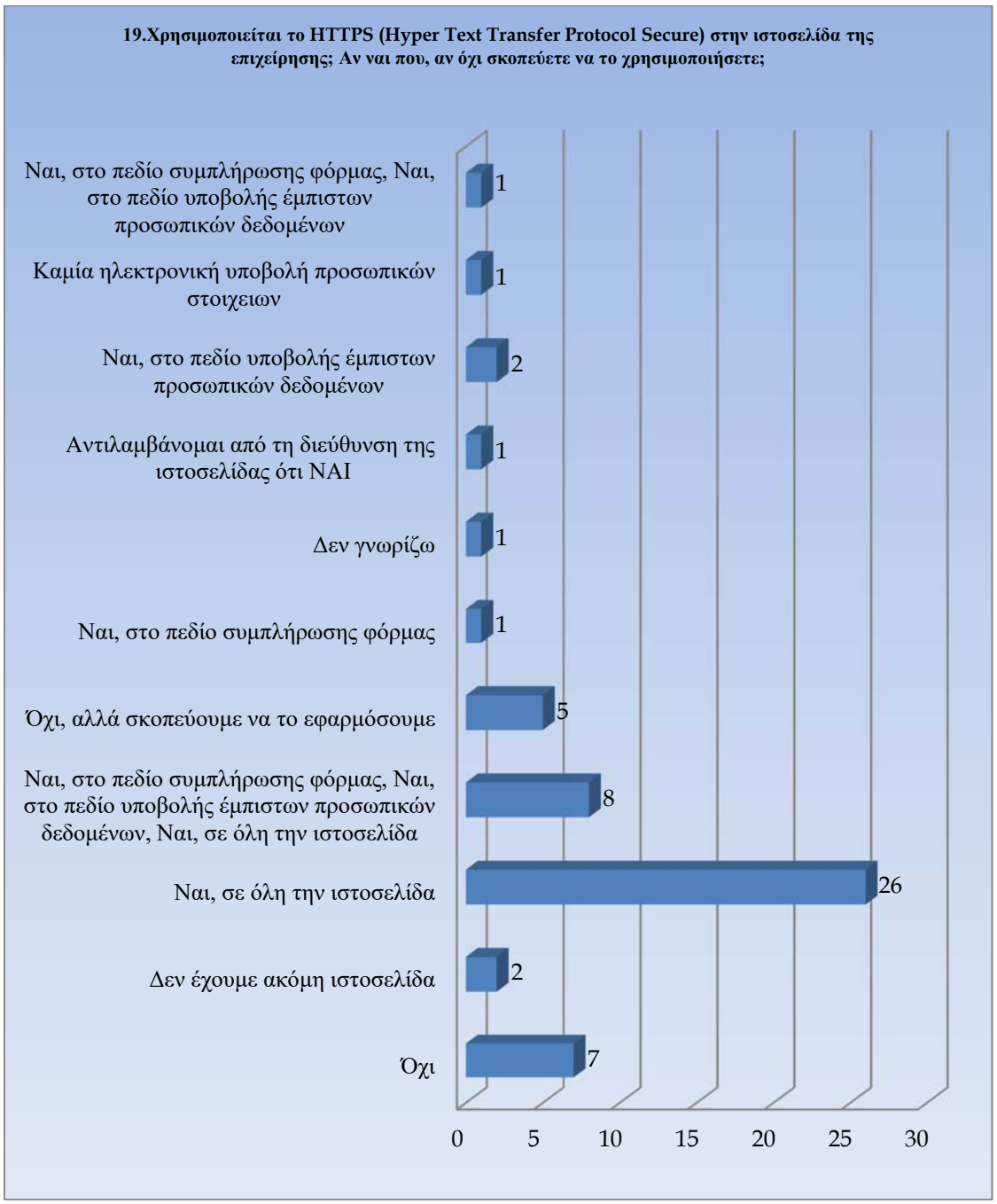
Σχήμα 5.33: Κατά πόσο στις επιχειρήσεις υπάρχουν οι πολιτικές, διαδικασίες και τεκμηρίωση για να επιβεβαιώσουν ότι συμμορφώνονται με την νομοθεσία GDPR;

Θα πρέπει να γίνεται καταγραφή για όλα τα προσωπικά δεδομένα που υπάρχουν, από πού προήλθαν, και με ποιόν τα μοιράζονται. Ο κανονισμός απαιτεί να τηρείται ένα αρχείο με όλες τις πράξεις επεξεργασίας των προσωπικών δεδομένων που εφαρμόζεται. Αυτό θα βοηθήσει στη συμμόρφωση. Με την αρχή της λογοδοσίας, κανονισμός σύμφωνα με την οποία όλες οι επιχειρήσεις θα πρέπει να είναι ικανές να αποδείξουν με ποιους τρόπους συμμορφώνονται στις αρχές προστασίας δεδομένων, π.χ υλοποιώντας αποτελεσματικές πολιτικές και διαδικασίες. Έτσι από τους 31 συμμετέχοντες ανάφεραν ότι μπορούν να αποδείξουν ότι συμμορφώνονται οι επιχειρήσεις που εργάζονται, ενώ 11 συμμετέχοντες δήλωσαν ότι δεν γνωρίζουν. Συνολικά 10 συμμετέχοντες είπαν ότι δεν είναι ακόμη ικανοί να το αποδείξουν και μόλις 3 συμμετέχοντες αποκάλυψαν ότι δεν υπάρχει τίποτα που να δείχνει ότι η επιχείρηση συμμορφώνεται.



Σχήμα 5.34: Έχει οριστεί υπεύθυνος προστασίας δεδομένων (DPO);

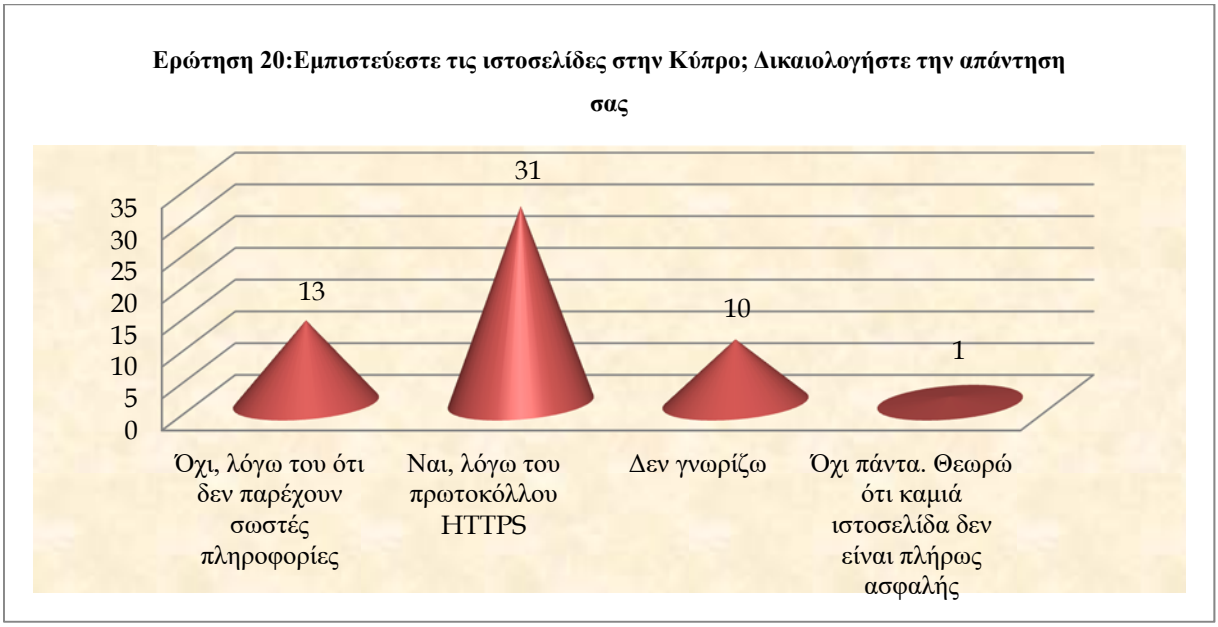
Ο ορισμός του υπεύθυνου προστασίας δεδομένων (DPO) είναι ένα σημαντικό εργαλείο στα χέρια κάθε επιχειρήσεις, μιας και αυτός μπορεί να συνδράμει στη λογοδοσία, την συνεννόηση με την εποπτική Αρχή και στη σύσκεψη με αυτήν όταν αυτό είναι αναγκαίο. Επίσης αποτελεί εχέγγυο για την σωστή εφαρμογή του κανονισμού το οποίο μπορεί να οδηγήσει σε ένα ανταγωνιστικό πλεονέκτημα αφού αυτός είναι και ο κατάλληλος για την συμμόρφωση σε μια επιχείρηση. Άρα διορίζοντας ένα υπεύθυνο προστασίας δεδομένων οι επιχειρήσεις αποκτούν σημαντικά κέρδη και οφέλη. Οι περισσότερες επιχειρήσεις έχουν ορίσει υπεύθυνο προστασίας δεδομένων (συνολικά 39), ενώ άλλες 5 επιχειρήσεις το σκέφτονται ακόμη (όχι ακόμη). Συνολικά 7 συμμετέχοντες δήλωσαν ότι δεν έχουν ορίσει καθόλου υπεύθυνο και άλλοι 4 συμμετέχοντες ανάφεραν ότι δε γνωρίζουν κατά πόσο έχει οριστεί ή όχι.



Σχήμα 5.35: Γίνεται η χρησιμοποίηση του πρωτοκόλλου HTTPS στις ιστοσελίδες των επιχειρήσεων; Αν ναι που, και αν όχι σκέφτεστε να το χρησιμοποιήσετε;

Ένας σύνδεσμος (URL) που αρχίζει με το πρόθεμα HTTPS δηλώνει ότι τα δεδομένα που μεταβιβάζονται μεταξύ μιας ιστοσελίδας και τελικού χρήστη είναι κρυπτογραφημένα. Το σύστημα αυτό έγινε για να υλοποιείται σε ιστοσελίδες όπου χρειάζεται αυθεντικοποίηση χρηστών και κρυπτογραφημένη επικοινωνία. Στην σημερινή εποχή χρησιμοποιείται παγκόσμια στο διαδίκτυο όπου απαιτείται αυξημένη ασφάλεια λόγω του ότι μεταφέρονται ευαίσθητες πληροφορίες (π.χ κωδικοί πρόσβασης, αριθμοί πιστωτικών καρτών κ.ά.), και κυρίως σε διαδικτυακά καταστήματα (online shops). Οποιαδήποτε ιστοσελίδα δε χρησιμοποιεί το

πρωτόκολλο HTTPS θεωρείται ως μη ασφαλής, οπόταν είναι επιτακτική ανάγκη να εφαρμοστεί. Στις επιχειρήσεις από ότι φαίνεται το χρησιμοποιούν σε ολόκληρη την ιστοσελίδα, αφού 26 συμμετέχοντες απάντησαν ναι, 8 συμμετέχοντες δήλωσαν ότι χρησιμοποιείται σε όλη την ιστοσελίδα-στο πεδίο συμπλήρωσης φόρμας-στο πεδίο υποβολής έμπιστων προσωπικών δεδομένων, ενώ 7 συμμετέχοντες ανέφεραν ότι δε χρησιμοποιείται καθόλου. Συνολικά 5 συμμετέχοντες δήλωσαν ότι δεν το χρησιμοποιούν αλλά είναι στα άμεσα τους σχέδια, 2 συμμετέχοντες είπαν ότι εφαρμόζεται στο πεδίο υποβολής έμπιστων προσωπικών δεδομένων, ενώ μόλις 2 συμμετέχοντες αποκάλυψαν ότι δεν έχουν ακόμη ιστοσελίδα. Οι υπόλοιποι 5 συμμετέχοντες εκφράστηκαν με διαφορετικές επιλογές όπως φαίνεται στο σχήμα 5.35.



Σχήμα 5.36: Έχετε εμπιστοσύνη τις ιστοσελίδες στην Κύπρο; Δικαιολογήστε την απάντηση σας.

Οι περισσότεροι χρήστες δεν εμπιστεύονται τις ιστοσελίδες που επισκέπτονται λόγω του ότι υπάρχουν ανακρίβειες και λάθη, μεγάλος χρόνος φόρτωσης, προηγούμενες παραβιάσεις ασφάλειας, έλλειψη πιστοποιητικά ασφάλειας (SSL) κ.ά. Γενικά οι ιστοσελίδες δεν προσφέρουν ασφάλεια, αλλά με την εφαρμογή του πρωτοκόλλου HTTPS τα δεδομένα αλλάζουν. Οι περισσότεροι συμμετέχοντες ανάφεραν ότι εμπιστεύονται τις ιστοσελίδες λόγω του HTTPS ενώ 13 συμμετέχοντες δήλωσαν ότι δεν τις εμπιστεύονται λόγω του ότι δεν προσφέρουν αξιόπιστες πληροφορίες. Ένα μερίδιο συμμετεχόντων (συνολικά 10 συμμετέχοντες) αποκάλυψαν ότι δε γνωρίζουν αν πράγματι πρέπει να τις εμπιστεύονται και ένας συμμετέχοντας εξέφρασε ότι σε καμία ιστοσελίδα δεν είναι πλήρως ασφαλής.

5.3 Τελικά συμπεράσματα

Σύμφωνα με την εκτέλεση των εντολών sslscan και openssl έχουν εξαχθεί τα πιο κάτω τελικά συμπεράσματα: Στον αλγόριθμο υπογραφής χρησιμοποιείται περισσότερο το 256RSAEncryption για τον λόγο ότι είναι μια δοκιμασμένη τεχνολογία και το κάνει να είναι πιο ασφαλές σε σχέση με το ECDA-with-SHA256 το οποίο δεν έχει εξεταστεί αρκετά. Στην ισχύς (μέγεθος) κλειδιού φαίνεται να χρησιμοποιείται σε μεγάλο βαθμό το 2048bits το οποίο για την ώρα είναι ασφαλές αλλά θα ήταν καλό στο άμεσο μέλλον να εφαρμοστεί το 4096bits για καλύτερη προστασία. Έχουν εντοπιστεί 10 διαφορετικές Αρχές Πιστοποίησης από τις 44 ιστοσελίδες που έχουν ερευνηθεί οι οποίες οι πιο δημοφιλέστερες είναι η Comodo και ακολουθεί η Digicert, Terena, Let's Encrypt. Μέσα από τις Αρχές Πιστοποίησης διαπιστώνεται ότι μερικές από αυτές προσφέρουν και δωρεάν πιστοποιητικά όπως είναι η Comodo, RapidSSL, Thawte, Terena (GÉANT) και Let's Encrypt. Αξίζει να σημειωθεί ότι 10 ιστοσελίδες δεν έχουν εφαρμόσει το πρωτόκολλο HTTPS που αυτό δείχνει εκτός από ότι δεν εφαρμόζεται η κατάλληλη προστασία και κρυπτογράφηση, δεν περιέχουν αλγόριθμο υπογραφής, μέγεθος κλειδιού και εκδότη πιστοποίησης πιστοποιητικού (Αρχή Πιστοποίησης). Επίσης δύο ιστοσελίδες έχουν παρουσιάσει πιστοποιητικό όπου έχει περάσει η ημερομηνία λήξεως και σε συνολικά τέσσερις ιστοσελίδες έχει υλοποιηθεί ο αλγόριθμος υπογραφής SHA1 το οποίο είναι ανασφαλές.

Με την εφαρμογή του ερωτηματολογίου, τα τελικά συμπεράσματα που δημιουργούνται είναι τα εξής: χρησιμοποιούνται ως επί των πλείστων δεδομένα για υπαλλήλους και πελάτες της Ευρωπαϊκής Ένωσης. Στην σύγχρονη εποχή πλέον τα δεδομένα στις επιχειρήσεις αποθηκεύονται ηλεκτρονικά αλλά υπάρχουν ακόμη δεδομένα που βρίσκονται σε έντυπη μορφή. Η αποθήκευση των δεδομένων στις πλείστες φορές των περιστάσεων γίνεται για αυτά που είναι αναγκαία και για το διάστημα που απαιτείται. Σύμφωνα με το GDPR εφαρμόζονται σε πολύ καλό βαθμό τα τεχνικά και οργανωτικά μέτρα για να διασφαλιστούν τα προσωπικά δεδομένα όπως είναι τα λογισμικά προστασίας, τοίχος προστασίας (firewall), τακτικά backup, κωδικό πρόσβασης στο Wi-Fi, VPN κ.ά. Όμως σε κάποια σημεία χρειάζεται βελτίωση όπως είναι το λογισμικό πρόσληψης διαρροών δεδομένων και οι διαδικασίες περιστατικών ασφάλειας. Διαπιστώνεται σχεδόν σε όλες τις διαδικασίες κρυπτογράφησης ότι δεν εφαρμόζεται σε μεγάλα επίπεδα το οποίο είναι ένα θέμα που πρέπει να βελτιωθεί. Για τα δικαιώματα των υποκειμένων των δεδομένων παρουσιάζεται μια ικανοποιητική διασφάλιση και δεν υπάρχουν αρκετές επιχειρήσεις που δεν το εφαρμόζουν καθόλου. Όμως υπάρχει ένας σημαντικός αριθμός των επιχειρήσεων που δεν υλοποιεί πλήρης τα δικαιώματα και κάποιες που δεν είναι ενήμερες. Στο

ζήτημα των ενημερώσεων για αυτούς που εμπλέκονται στην επεξεργασία δεδομένων βρίσκεται σε καλό επίπεδο αλλά χρειάζεται περισσότερη πρόοδο. Ο κανονισμός του GDPR είναι γνωστός σε όλες τις επιχειρήσεις που έγινε στην έρευνα με μια μόνο εξαίρεση και αυτό αφήνει πολλές υποσχέσεις. Όμως οι επιχειρήσεις έχουν επηρεαστεί από τον κανονισμό για τον λόγο ότι θα πρέπει να προσαρμοστούν στα γεγονότα που καθορίζει και αυτό προϋποθέτει χρόνο και χρήμα. Όσον αφορά τις διαδικασίες τεκμηρίωσης για την συμμόρφωση βρίσκεται σε ένα στάδιο που πρέπει να εξελιχθεί γιατί φαίνεται ότι δεν το τηρούν όλες οι επιχειρήσεις σε αντίθεση με τον ορισμό του υπεύθυνου προστασίας δεδομένων όπου τηρείται σε πολύ καλό βαθμό. Στην χρησιμοποίηση του πρωτοκόλλου HTTPS διαπιστώνεται να υλοποιείται σε αρκετά ψηλό βαθμό και στις πλείστες περιπτώσεις γίνεται σε ολόκληρη την ιστοσελίδα όπου φανερώνει ότι οι επιχειρήσεις αναζητούν την ακέραια ασφάλεια στις ιστοσελίδες τους. Για την εμπιστοσύνη των ιστοσελίδων δείχνει ότι ένα σχετικά μεγάλο μερίδιο των επιχειρήσεων σε σύγκριση με τις άλλες επιλογές δίνουν ψήφο εμπιστοσύνης στο πρωτόκολλο HTTPS που είναι μια ένδειξη ότι προσδίδει προστασία και ασφάλεια.

Κεφάλαιο 6
Επίλογος

Η προστασία και ασφάλεια των προσωπικών δεδομένων στις επιχειρήσεις είναι το άλφα και το ωμέγα για την υλοποίηση και συμμόρφωση με τον Γενικό Κανονισμό Προστασίας Δεδομένων (GDPR). Οι επιχειρήσεις έχουν επηρεαστεί σε κάποιο βαθμό από την εφαρμογή του κανονισμού, όμως τα ωφελήματα που θα επωμιστούν είναι πολλά. Ο κανονισμός επέβαλλε στις επιχειρήσεις να διασφαλίσουν τα δικαιώματα των υποκειμένων, ορθός προγραμματισμός, έρευνα, αξιολόγηση και λήψη κατάλληλων μέτρων προστασίας των προσωπικών δεδομένων. Με την εφαρμογή των τεχνικών και οργανωτικών μέτρων (κρυπτογράφηση) διευκολύνει την διαχείριση (να γνωρίζεται που είναι αποθηκευμένα τα δεδομένα) και ασφάλεια των προσωπικών δεδομένων σε βαθμό ώστε να διατηρούνται ασφαλή, ιδιωτικά και ακέραια. Η χρησιμοποίηση του πρωτοκόλλου HTTPS με πιστοποιημένα πιστοποιητικά από Αρχή Πιστοποίησης προσδίδει προστασία, κρυπτογράφηση και εμπιστοσύνη στις ιστοσελίδες των επιχειρήσεων στη Κύπρο με εφαρμογή στις συναλλαγές, μεταφορές δεδομένων, κωδικούς πρόσβασης κ.ά. Το πρωτόκολλο HTTPS υλοποιείται σε αρκετά ψηλό βαθμό το οποίο είναι πολύ περισσότερο από αναγκαίο στην σύγχρονη εποχή με τις αρκετές ηλεκτρονικές συναλλαγές και τους μεγάλους όγκους δεδομένων στο διαδίκτυο που διεκπεραιώνονται καθημερινά. Στις επιχειρήσεις που εξετάστηκαν, όσον αφορά κάποια σημεία που υπάρχουν στη νομοθεσία περί προστασίας προσωπικών δεδομένων (GDPR) δεν εφαρμόζονται πλήρες.

Μετά την εφαρμογή των εντολών και του ερωτηματολογίου αυτό που είναι σημαντικό είναι ότι πρέπει να εφαρμόζεται σωστά το πρωτόκολλο HTTPS, στο οποίο το πιστοποιητικό SSL πρέπει να έχει τις κατάλληλες προδιαγραφές όπως να είναι έγκυρο, υπογραμμένο από Αρχή Πιστοποίησης, αλγόριθμο υπογραφής ο οποίος να είναι ασφαλές όπως και το μέγεθος κλειδιού RSA.

Στην συγκεκριμένη μεταπτυχιακή διατριβή θα μπορούσε στο μέλλον να δημιουργηθεί ένα πρόγραμμα (π.χ τύπου script) που να συγκεντρώνει τα λεπτομερή δεδομένα από τους ιστότοπους των επιχειρήσεων της Κύπρου με την βοήθεια του sslscan και να τα αποθηκεύει σε μια βάση δεδομένων για καλύτερη και πιο εύκολη ανάλυση δεδομένων. Επίσης με την

χρησιμοποίηση του openssl θα κατόρθωνε εκτός από την συλλογή δεδομένων να ανοίγει καινούργιες πόρτες (ports).

Η αποκάλυψη των προσωπικών δεδομένων είναι ένα ενδεχόμενο που μπορεί να πραγματοποιηθεί όμως αυτό που μπορεί να αναφερθεί με σιγουριά είναι ότι έχουν γίνει βήματα ανόδου από τις επιχειρήσεις για την μείωση αυτών των περιπτώσεων και στο ότι υπάρχει ένα πολύ καλό επίπεδο ασφάλειας για την προστασία των προσωπικών δεδομένων.

Το διαδίκτυο είναι ένας ατελείωτος ωκεανός με πληθώρα ροή πληροφοριών καθώς και ένα μέσο απόλυτης ελευθερίας για να εκφράζονται και να επικοινωνούν οι άνθρωποι. Συνέβαλε στην ανάπτυξη της τεχνολογίας και του ηλεκτρονικού εμπορίου. Υπάρχουν ωστόσο οι εγκληματίες στον κυβερνοχώρο οι οποίοι κάνουν κατάχρηση των υπηρεσιών του διαδίκτυο που οδήγησαν στην εμφάνιση των παραβιάσεων των προσωπικών και ευαίσθητων δεδομένων για πολλαπλά οφέλη εις βάρος άλλον. Στην σημερινή εποχή η τεχνολογία με τις τεράστιες ικανότητες της προσφέρει ασφάλεια και δεν θα υφίσταται κίνδυνοι ώστε να εμφανίζεται έλλειψη προστασίας προσωπικών δεδομένων των ανθρώπων. Η χρησιμοποίηση του πρωτοκόλλου HTTPS είναι αναμφισβήτητα απαραίτητη για την διασφάλιση της ιστοσελίδας μιας επιχείρησης αλλά και στην διακίνηση προσωπικών δεδομένων σε αυτήν όπως αριθμοί λογαριασμών και πιστωτικές κάρτες, κωδικοί πρόσβασης, ονοματεπώνυμα, ταυτότητες κ.ά.

Στο άμεσο μέλλον θα ήταν απαραίτητο να υπάρχει η δημιουργία κατευθυντήριων γραμμών για την προστασία των προσωπικών δεδομένων των ανθρώπων μέσα σε ένα κόσμο χωρίς σύνορα που λέγεται διαδίκτυο. Τα περισσότερα κράτη στον κόσμο δεν έχουν συγκεκριμένη νομοθεσία προστασίας των προσωπικών δεδομένων οπότε είναι αναγκαίο να εφαρμοστούν Διεθνή Πρότυπα για την προστασία της ιδιωτικότητας και των προσωπικών δεδομένων. Η ανάπτυξη της τεχνολογίας σε συνδυασμό με τις απειλές που παραμονεύουν για την ιδιωτικότητα του ανθρώπου επιβάλλεται να ρυθμιστεί το νομοθετικό πλαίσιο ενώ οι προκλήσεις στο μέλλον θα είναι τεράστιες για όλους. Θα πρέπει οι νομοθέτες να δουν πολύ πιο ζεστά τις διαδικασίες επικύρωσης νόμων και νομοθεσιών έτσι να υπάρξουν άμεσα υλοποιήσιμες και να βρίσκονται ενημερωμένες με την τεχνολογία που βελτιώνεται ακατάπαυστα.

Έτσι είναι αναγκαία η θέσπιση προτύπων προστασίας της ιδιωτικής ζωής τα οποία χρειάζονται και αναμένουν οι χρήστες και στον τομέα του διαδικτύου που διαρκώς αλλάζει. Στο προσεχές μέλλον αυτό που θα πρέπει να προβληματίσει και να επιλυθεί είναι ο μεγάλος όγκος

πληροφοριών στο διαδίκτυο που υπάρχει και η καθιέρωση διεθνών προτύπων για την διασφάλιση των προσωπικών δεδομένων.

Βιβλιογραφία:

Διαδίκτυο:

[01] - About Rapid SSL. (n.d.). Retrieved November 18, 2018, from https://www.rapidssl.com/about/

[02] - Cheng, K., Gao, M., & Guo, R. (2010). Analysis and Research on HTTPS Hijacking Attacks. In *2010 Second International Conference on Networks Security, Wireless Communications and Trusted Computing* (Vol. 2, pp. 223–226). https://doi.org/10.1109/NSWCTC.2010.187

[03] - Chomsiri, T. (2007). HTTPS Hacking Protection. In *21st International Conference on Advanced Information Networking and Applications Workshops (AINAW'07)* (Vol. 1, pp. 590–594). https://doi.org/10.1109/AINAW.2007.200

[04] - Comodo Group - Wikipedia. (n.d.). Retrieved November 17, 2018, from https://en.wikipedia.org/wiki/Comodo_Group

[05] - Comodo vs Thawte vs Entrust vs DigiCert: SSL Certificates. (n.d.). Retrieved November 19, 2018, from https://sslcertifications.knoji.com/comodo-vs-thawte-vs-entrust-vs-digicert-ssl-certificates/

[06] - Cooper, K. (n.d.). Keyword Research, Competitor Analysis, & Website Ranking | Alexa. Retrieved November 29, 2018, from https://www.alexa.com/

[07] - Cornock, M. (2018). General Data Protection Regulation (GDPR) and implications for research. *Maturitas*, *111*, A1–A2. https://doi.org/10.1016/j.maturitas.2018.01.017

[08] - cPanel, Inc.: Private Company Information - Bloomberg. (n.d.). Retrieved November 17, 2018, from

https://www.bloomberg.com/research/stocks/private/snapshot.asp?privcapid=133674569

[09] - DigiCert - Wikipedia. (n.d.). Retrieved November 18, 2018, from https://en.wikipedia.org/wiki/DigiCert

[10] - ECDSA: The digital signature algorithm of a better internet. (2014, March 10). Retrieved November 7, 2018, from https://blog.cloudflare.com/ecdsa-the-digital-signature-algorithm-of-a-better-internet/

[11] - GeoTrust. (2018). In *Wikipedia*. Retrieved from https://en.wikipedia.org/w/index.php?title=GeoTrust&oldid=859873241

[12] - Giorgos. (2018, April 20). HTTP και HTTPS: Τι πρέπει να ξέρω για τα πρωτόκολλα μεταφοράς. Retrieved November 24, 2018, from https://iguru.gr/2018/04/20/https-http/

[13] - hash - Why would I choose SHA-256 over SHA-512 for a SSL/TLS certificate? (n.d.). Retrieved November 16, 2018, from https://security.stackexchange.com/questions/165559/why-would-i-choose-sha-256-over-sha-512-for-a-ssl-tls-certificate

[14] - How Does SSL Fit into GDPR? - Blog - GeoCerts.com. (n.d.). Retrieved November 24, 2018, from https://www.geocerts.com/blog/how-does-ssl-fit-into-gdpr

[15] - HTTrack. (2018). In *Wikipedia*. Retrieved from https://en.wikipedia.org/w/index.php?title=HTTrack&oldid=851309875

[16] - Hyland, J. (2017). Data Protection in EU Businesses: an Introduction to GDPR. *DBS Business Review*, *1*, 146–148. https://doi.org/10.22375/dbsbr.v1.12

[17] - IETF Tools. (n.d.). Retrieved October 13, 2018, from https://tools.ietf.org/

[18] - Krystlik, J. (2017). With GDPR, preparation is everything. *Computer Fraud & Security*, *2017*(6), 5–8. https://doi.org/10.1016/S1361-3723(17)30050-7

[19] - Let's Encrypt - Wikipedia. (n.d.). Retrieved November 18, 2018, from https://en.wikipedia.org/wiki/Let%27s_Encrypt

[20] - Ouvrier, G., Laterman, M., Arlitt, M., & Carlsson, N. (2017). Characterizing the HTTPS Trust Landscape: A Passive View from the Edge. *IEEE Communications Magazine*, *55*(7), 36–42. https://doi.org/10.1109/MCOM.2017.1600981

[21] - Prandini, M., Ramilli, M., Cerroni, W., & Callegati, F. (2010). Splitting the HTTPS Stream to Attack Secure Web Connections. *IEEE Security Privacy*, *8*(6), 80–84. https://doi.org/10.1109/MSP.2010.190

[22] - Samoshkin, A. (2018, January 5). RSA and ECDSA hybrid Nginx setup with LetsEncrypt certificates. Retrieved November 16, 2018, from https://hackernoon.com/rsa-and-ecdsa-hybrid-nginx-setup-with-letsencrypt-certificates-ee422695d7d3

[23] - Sanderson, R. (2011). A secure data protection strategy. *Network Security*, *2011*(3), 10–12. https://doi.org/10.1016/S1353-4858(11)70025-3

[24] - Stanivuk, I., Bjelić, V., Samardžić, T., & Simić, Đ. (2017). Expanding lua interface to support HTTP/HTTPS protocol. In *2017 13th International Conference on Advanced Technologies, Systems and Services in Telecommunications (TELSIKS)* (pp. 407–410). https://doi.org/10.1109/TELSKS.2017.8246311 https://ieeexplore.ieee.org/document/8246311?figureId=fig5#fig5

[25] - Starfield Technologies. (2018). In *Wikipedia*. Retrieved from https://en.wikipedia.org/w/index.php?title=Starfield_Technologies&oldid=858849373

[26] - Tankard, C. (2016). What the GDPR means for businesses. *Network Security*, *2016*(6), 5–8. https://doi.org/10.1016/S1353-4858(16)30056-3

[27] - TERENA> News> Low-cost Server Certificates Available via TERENA. (n.d.). Retrieved November 19, 2018, from https://www.terena.org/news/fullstory.php?news_id=1509

[28] - TERENA. (2018). In *Wikipedia*. Retrieved from https://en.wikipedia.org/w/index.php?title=TERENA&oldid=829743616

[29] - Thawte - Wikipedia. (n.d.). Retrieved November 17, 2018, from https://en.wikipedia.org/wiki/Thawte

[30] - Villanueva, J. C. (n.d.). Should We Start Using 4096 bit RSA keys? Retrieved November 16, 2018, from https://www.jscape.com/blog/should-i-start-using-4096-bit-rsa-keys

Βιβλία:

[31] -Κεφάλαιο 1 & 2 του βιβλίου:
"Creswell, J. W. (2011). Η έρευνα στην εκπαίδευση: σχεδιασμός, διεξαγωγή και αξιολόγηση της ποσοτικής και ποιοτικής έρευνας. "
Ελληνική έκδοση του βιβλίου:
"Creswell, J. W. (2008). Educational research: planning, conducting and evaluating quantitative and qualitative research (3rd ed.). "

[32] - Oppliger, R. (2009). SSL and TLS: Theory and Practice. Artech House. https://books.google.com.cy/books/about/SSL_and_TLS.html?id=dR2G0oPufe0C&redir_esc=y

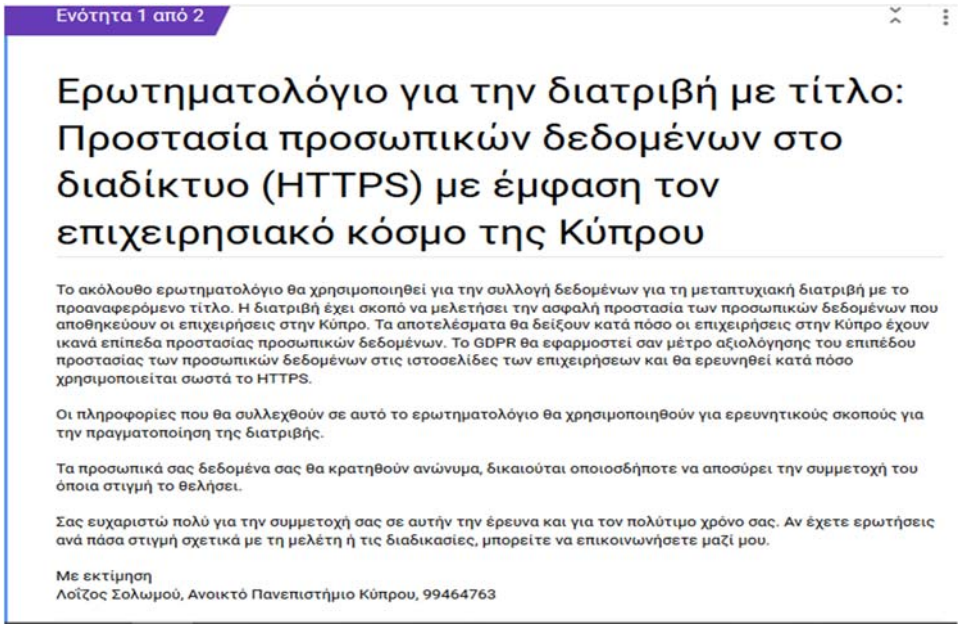
Άρθρα:

[31] - "Olsen, W. K. (2004). Triangulation in Social Research: Qualitative and Quantitative Methods Can Really Be Mixed."

Πίνακας Παραρτημάτων

Παράρτημα Α
Ερωτηματολόγιο

Α.1 Ερωτήσεις ερωτηματολογίου όπως έχουν διατυπωθεί στους συμμετέχοντες



Ενότητα 1 από 2

Ερωτηματολόγιο για την διατριβή με τίτλο: Προστασία προσωπικών δεδομένων στο διαδίκτυο (HTTPS) με έμφαση τον επιχειρησιακό κόσμο της Κύπρου

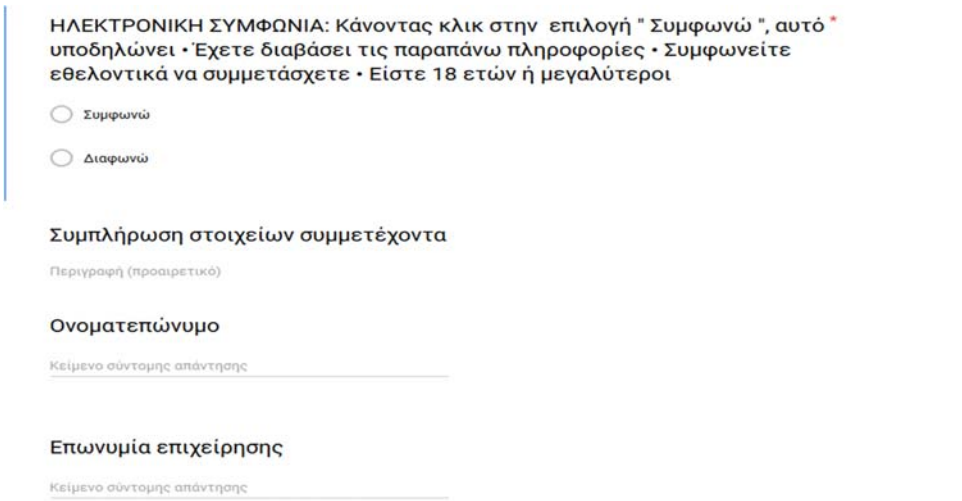
Το ακόλουθο ερωτηματολόγιο θα χρησιμοποιηθεί για την συλλογή δεδομένων για τη μεταπτυχιακή διατριβή με το προαναφερόμενο τίτλο. Η διατριβή έχει σκοπό να μελετήσει την ασφαλή προστασία των προσωπικών δεδομένων που αποθηκεύουν οι επιχειρήσεις στην Κύπρο. Τα αποτελέσματα θα δείξουν κατά πόσο οι επιχειρήσεις στην Κύπρο έχουν ικανά επίπεδα προστασίας προσωπικών δεδομένων. Το GDPR θα εφαρμοστεί σαν μέτρο αξιολόγησης του επιπέδου προστασίας των προσωπικών δεδομένων στις ιστοσελίδες των επιχειρήσεων και θα ερευνηθεί κατά πόσο χρησιμοποιείται σωστά το HTTPS.

Οι πληροφορίες που θα συλλεχθούν σε αυτό το ερωτηματολόγιο θα χρησιμοποιηθούν για ερευνητικούς σκοπούς για την πραγματοποίηση της διατριβής.

Τα προσωπικά σας δεδομένα σας θα κρατηθούν ανώνυμα, δικαιούται οποιοσδήποτε να αποσύρει την συμμετοχή του όποια στιγμή το θελήσει.

Σας ευχαριστώ πολύ για την συμμετοχή σας σε αυτήν την έρευνα και για τον πολύτιμο χρόνο σας. Αν έχετε ερωτήσεις ανά πάσα στιγμή σχετικά με τη μελέτη ή τις διαδικασίες, μπορείτε να επικοινωνήσετε μαζί μου.

Με εκτίμηση
Λοΐζος Σολωμού, Ανοικτό Πανεπιστήμιο Κύπρου, 99464763



ΗΛΕΚΤΡΟΝΙΚΗ ΣΥΜΦΩΝΙΑ: Κάνοντας κλικ στην επιλογή " Συμφωνώ ", αυτό υποδηλώνει • Έχετε διαβάσει τις παραπάνω πληροφορίες • Συμφωνείτε εθελοντικά να συμμετάσχετε • Είστε 18 ετών ή μεγαλύτεροι *

- Συμφωνώ
- Διαφωνώ

Συμπλήρωση στοιχείων συμμετέχοντα

Περιγραφή (προαιρετικό)

Ονοματεπώνυμο

Κείμενο σύντομης απάντησης

Επωνυμία επιχείρησης

Κείμενο σύντομης απάντησης

Διεύθυνση ηλεκτρονικού ταχυδρομείου (email), δεν θα συμπεριληφθεί στην διατριβή αλλά για σκοπούς της έρευνας *

Κείμενο σύντομης απάντησης

Τηλέφωνο επικοινωνίας

Κείμενο σύντομης απάντησης

Ιστοσελίδα (website)

Κείμενο σύντομης απάντησης

Ενότητα 2 από 2

Ερωτήσεις

Περιγραφή (προαιρετικό)

1. Με τι ασχολείται η επιχείρηση που εργάζεστε; *

- ◯ Διοίκηση Επιχειρήσεων
- ◯ Λογιστικά / Έλεγχος / Φορολογικά
- ◯ Νομοθεσία & Νομικά Θέματα
- ◯ Πληροφορική
- ◯ Τραπεζιτικό σύστημα
- ◯ Χρηματοοικονομικά-Ασφαλιστικά
- ◯ Άλλο...

2. Ποιος ο ρόλος σας στην επιχείρηση; *

- ◯ Ασφαλιστές
- ◯ Γραμματέας
- ◯ Διευθύνων Σύμβουλος
- ◯ Δικηγόροι
- ◯ Λογιστές
- ◯ Προγραμματιστές / Υπεύθυνος I.T / I.T
- ◯ Υπεύθυνοι Πωλήσεων / Πωλητές / Εξυπηρέτηση Πελατών
- ◯ Άλλο...

3. Για ποια ομάδα ή ομάδες ατόμων κατέχετε προσωπικά δεδομένα; *

- ☐ Υπάλληλοι
- ☐ Πελάτες
- ☐ Υπάλληλοι εταιρικών συνεργατών
- ☐ Άλλο...

4. Η επιχείρηση χειρίζεται προσωπικά δεδομένα των πολιτών της Ευρωπαϊκής Ένωσης;

- ◯ Ναι
- ◯ Όχι

5. Εάν ναι, τι είδους προσωπικά δεδομένα χειρίζεται η επιχείρηση;

- ☐ Αναγνωριστικά στο διαδίκτυο (διεύθυνση IP, RFID, cookie συστήματος κ.λ.π)
- ☐ Αριθμός ταυτότητας / διαβατηρίου
- ☐ Θρησκευτικές απόψεις
- ☐ Οικονομικές πληροφορίες
- ☐ Πληροφορίες για την υγεία
- ☐ Τραπεζικοί λογαριασμοί
- ☐ Άλλο...

6. Υπάρχουν κάποιες διαδικασίες που αποθηκεύονται τα προσωπικά δεδομένα και αν ναι πως και που;

- ◯ Ναι, σε έντυπη μορφή στους υπηρεσιακούς φακέλους
- ◯ Ναι, σε ηλεκτρονική μορφή στο μηχανογραφικό σύστημα
- ◯ Ναι, σε έντυπη και ηλεκτρονική μορφή
- ◯ Όχι
- ◯ Δεν γνωρίζω

7. Υπό ποια νομική βάση αποθηκεύετε και επεξεργάζεστε προσωπικά δεδομένα; *

- ◯ Επεξεργαζόμαστε προσωπικά δεδομένα βάσει συμβάσεων με τα πρόσωπα στα οποία αναφέρονται τα δεδομένα
- ◯ Συλλέγουμε προσωπικά δεδομένα σύμφωνα με τις σχετικές νομικές πράξεις
- ◯ Λαμβάνουμε την συγκατάθεση των υποκειμένων των δεδομένων για την συλλογή των προσωπικών τους δεδομένων
- ◯ Δεν γνωρίζω ποια νομική βάση μας καλύπτει σε ότι αφορά την συλλογή προσωπικών δεδομένων

8. Αποθηκεύετε μόνο τα προσωπικά δεδομένα που απαιτούνται για την εκπλήρωση του σκοπού για τον οποίο συλλέχθηκαν; *

- ◯ Ναι, διατηρούμε μόνο τα σχετικά προσωπικά δεδομένα και τα αποθηκεύουμε μόνο για τον ελάχιστο απαιτούμενο χρόνο
- ◯ Όχι, διατηρούμε επιπρόσθετα προσωπικά δεδομένα που μπορεί να είναι χρήσιμα
- ◯ Δεν γνωρίζω

9. Έχετε κάποια τεκμηρίωση σχετικά με τα προσωπικά δεδομένα που συλλέγετε, από ποιες πηγές τα συλλέγετε και με ποιους τα μοιράζεστε; *

- ◯ Ναι, διατηρούμε τεκμηρίωση σχετικά με τη συλλογή και κοινή χρήση προσωπικών δεδομένων, η οποία ελέγχεται τακτικά
- ◯ Ναι, διαθέτουμε τεκμηρίωση σε ότι αφορά τα προσωπικά δεδομένα αλλά έχει περάσει καιρός από την τελευταία επισκόπηση
- ◯ Όχι, δεν έχουμε κανενός είδους τεκμηρίωση

10. Ποια τεχνικά μέτρα έχετε λάβει για την προστασία των προσωπικών δεδομένων από μη εξουσιοδοτημένη πρόσβαση; *

	Ναι	Όχι	Εν μέρη	Δεν εφαρμόζεται
Λογισμικό προστασίας από ιούς που παρέχει προστασία κακόβουλου λογισμικού	◯	◯	◯	◯
Λογισμικό προστασίας από ιούς που παρέχει προστασία ηλεκτρονικού ταχυδρομείου και προγράμματος περιήγησης στον ιστό	◯	◯	◯	◯
Το εταιρικό μας δίκτυο προστατεύεται από firewall	◯	◯	◯	◯
Τακτικό backup των προσωπικών δεδομένων εφαρμόζεται αυτόματα	◯	◯	◯	◯
Το εταιρικό μας Wi-Fi προστατεύεται με κωδικό πρόσβασης	◯	◯	◯	◯

Η απομακρυσμένη πρόσβαση στο εταιρικό μας δίκτυο είναι δυνατή μόνο μέσω ενός εικονικού ιδιωτικού δικτύου (VPN)	○	○	○	○
Οι λογαριασμοί με προνομιακά δικαιώματα δεν χρησιμοποιούνται για καθημερινές εργασίες. Η σύνδεση με χρήστες με προνομιακά δικαιώματα είναι δυνατή μόνο από εξειδικευμένες συσκευές και η πρόσβαση περιορίζεται μόνο σε εξουσιοδοτημένα άτομα	○	○	○	○
Η πρόσβαση σε ευαίσθητα/προσωπικά δεδομένα ελέγχεται και περιορίζεται μόνο σε άτομα που χρειάζονται πρόσβαση σε αυτά	○	○	○	○
Το λογισμικό πρόληψης διαρροών δεδομένων χρησιμοποιείται για την προστασία ευαίσθητων/προσωπικών δεδομένων	○	○	○	○
Διαδικασίες παρακολούθησης, ανίχνευσης, ανάλυσης και αναφοράς περιστατικών ασφάλειας εφαρμόζονται και κοινοποιούνται στην επιχείρηση	○	○	○	○

11. Η κρυπτογράφηση είναι ένα πολύ σημαντικό μέτρο ασφάλειας. Ποια από τις ακόλουθες λειτουργίες κρυπτογράφησης χρησιμοποιείτε για την προστασία προσωπικών δεδομένων; *

	Ναι	Όχι	Εν μέρη	Δεν γνωρίζω
Κρυπτογράφηση Ευαίσθητων/Προσωπικών αρχείων δεδομένων	○	○	○	○
Πλήρης κρυπτογράφηση δίσκων υπολογιστή/laptop	○	○	○	○
Κρυπτογράφηση ηλεκτρονικής επικοινωνίας	○	○	○	○
Κρυπτογράφηση Αφαιρούμενων Δίσκων	○	○	○	○
Κρυπτογράφηση φακέλου δικτύου/cloud	○	○	○	○

12. Έχετε τεχνικά και οργανωτικά μέτρα για να διασφαλίσετε ότι τα υποκείμενα των δεδομένων έχουν τα ακόλουθα δικαιώματα; *

	Ναι	Όχι	Εν μέρη	Δεν γνωρίζω
Για να αποκτήσουν πρόσβαση στα επεξεργασμένα προσωπικά τους δεδομένα	○	○	○	○
Προκειμένου να αποκατασταθούν οι ανακρίβειες των προσωπικών τους δεδομένων	○	○	○	○
Για να διαγραφούν τα προσωπικά τους δεδομένα - το δικαίωμα στη λήθη	○	○	○	○
Για να αποτρέψουν τις άμεσες προωθητικές ενέργειες	○	○	○	○
Για να αποτρέψουν την αυτοματοποιημένη λήψη αποφάσεων και τη δημιουργία προφίλ	○	○	○	○
Φορητότητα δεδομένων	○	○	○	○

13. Το προσωπικό που είναι επιφορτισμένο με την επεξεργασία δεδομένων προσωπικού χαρακτήρα λαμβάνει εκπαίδευση σε ότι αφορά τις υποχρεώσεις και τα δικαιώματα που σχετίζονται με την προστασία των προσωπικών δεδομένων; *

- ○ Ναι
- ○ Όχι
- ○ Εν μέρη
- ○ Δεν γνωρίζω

14. Είναι ενημερωμένοι όσοι είναι επιφορτισμένοι με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα για τις αλλαγές που έχει επιφέρει το GDPR; Έχουν σχέδιο συμμόρφωσης; *

- ○ Ναι, τους έχουμε ελέγξει
- ○ Πιστεύω ότι δεν είναι ενήμεροι
- ○ Δεν ισχύει επειδή δεν έχει προσληφθεί σχετικό προσωπικό επεξεργασίας προσωπικών δεδομένων
- ○ Δεν γνωρίζω

15. Γνωρίζετε για τον Γενικό Κανονισμό Προστασίας Προσωπικών Δεδομένων GDPR (General Data Protection Regulation); Αν όχι ακολουθείστε την ερώτηση 18 και κάτω. *

- ○ Ναι
- ○ Όχι

16. Έχει επηρεάσει ο νέος κανονισμός του GDPR στην επιχείρηση;

- ○ Ναι
- ○ Όχι
- ○ Δεν γνωρίζω

17. Η επιχείρηση έχει τις πολιτικές, διαδικασίες και την τεκμηρίωση για να δείξει ότι συμμορφώνετε με την νομοθεσία GDPR;

- ○ Ναι, μπορώ να το αποδείξω
- ○ Όχι ακόμη
- ○ Όχι
- ○ Δεν γνωρίζω

18. Έχετε ορίσει υπεύθυνο προστασίας δεδομένων (DPO: Data Protection Officer); *

- ○ Ναι
- ○ Όχι ακόμη
- ○ Όχι
- ○ Δεν γνωρίζω

19. Χρησιμοποιείται το HTTPS (Hyper Text Transfer Protocol Secure) στην ιστοσελίδα της επιχείρησης; Αν ναι που, αν όχι σκοπεύετε να το χρησιμοποιήσετε; *

- [ ] Ναι, στο πεδίο συμπλήρωσης φόρμας
- [ ] Ναι, στο πεδίο υποβολής έμπιστων προσωπικών δεδομένων
- [ ] Ναι, σε όλη την ιστοσελίδα
- [ ] Όχι, αλλά σκοπεύουμε να το εφαρμόσουμε
- [ ] Όχι
- [ ] Άλλο...

20. Εμπιστεύεστε τις ιστοσελίδες στην Κύπρο; Δικαιολογήστε την απάντηση σας. *

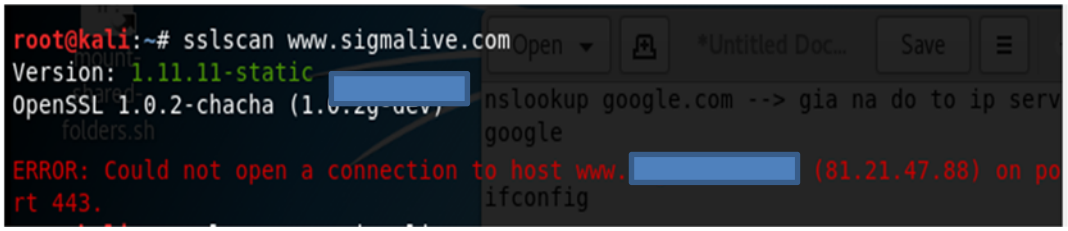
- ( ) Ναι, λόγω του πρωτοκόλλου HTTPS
- ( ) Όχι, λόγω του ότι δεν παρέχουν σωστές πληροφορίες
- ( ) Δεν γνωρίζω
- ( ) Άλλο...

Παράρτημα Β

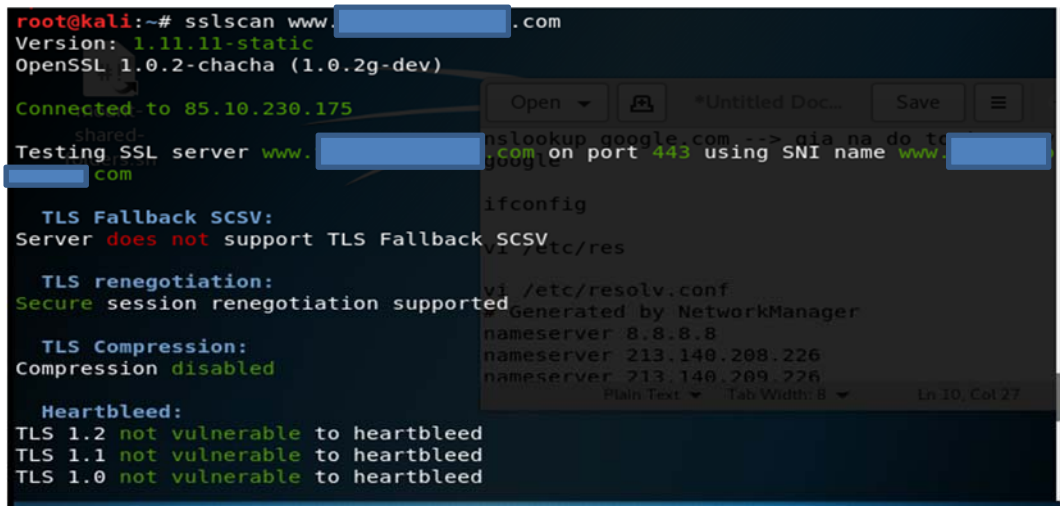
Εντολές sslscan και openssl

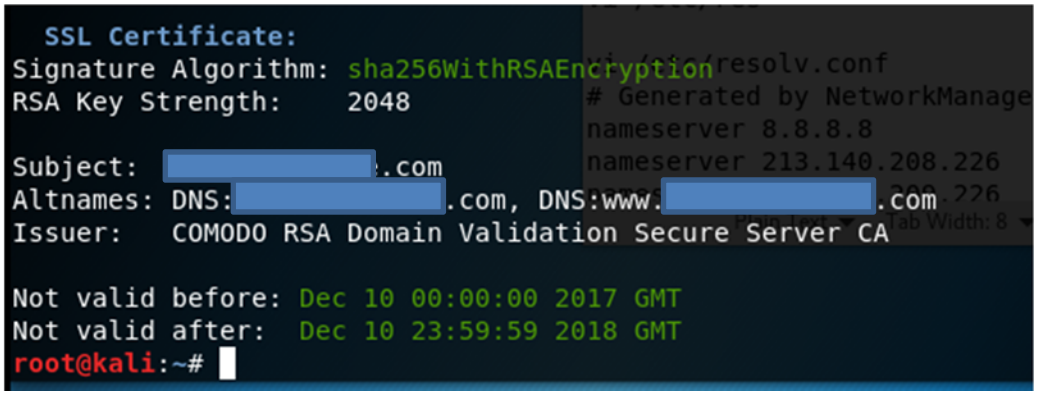
Β.1 Παραδείγματα των αποτελεσμάτων sslscan

Η ιστοσελίδα πιο κάτω δεν υλοποιεί το πρωτόκολλο HTTPS με αποτέλεσμα να μην μπορεί να συνδεθεί στην πόρτα (port) 443 που χρησιμοποιεί το πρωτόκολλο HTTPS αντί την πόρτα 80 που χρησιμοποιεί το πρωτόκολλο HTTP.

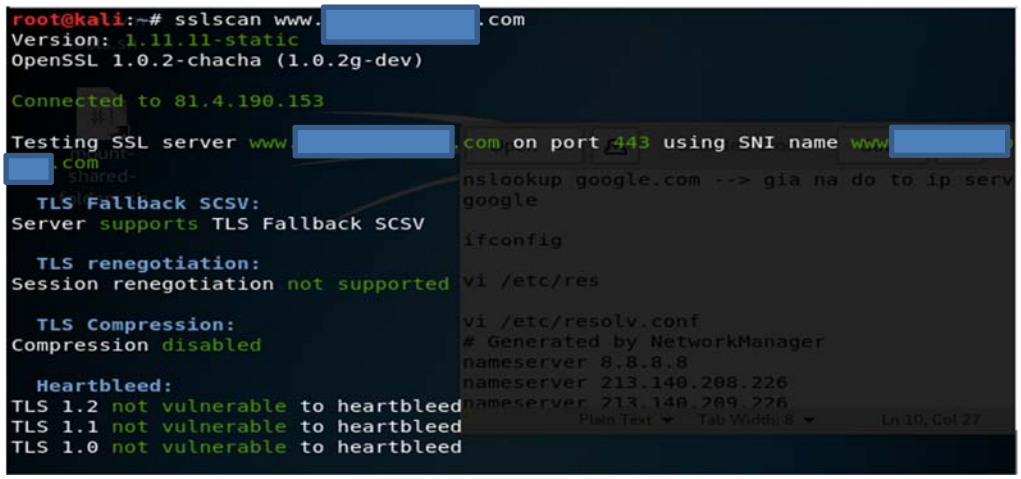


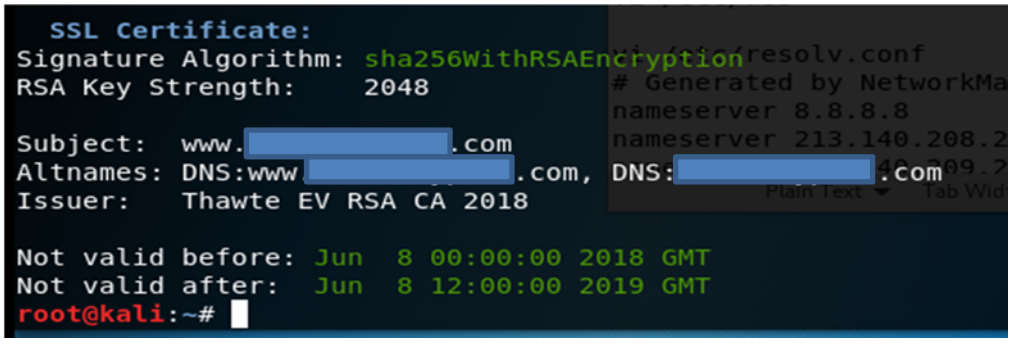
Στην ιστοσελίδα παρακάτω εμφανίζεται η ένδειξη: server does not support TLS Fallback SCSV. Αυτό σημαίνει ότι έχει απενεργοποιηθεί το TLS Fallback SCSV για να μην γίνουν επιθέσεις οι οποίες εκμεταλλεύονται τις υποβαθμίσεις πρωτοκόλλων. Επίσης υποδείχνει σε ένα πελάτη ότι γίνεται εις γνώση του μια προσπάθεια σύνδεσης SSL/TLS σε μια χαμηλότερη έκδοση πρωτοκόλλου από ότι υποστηρίζεται.



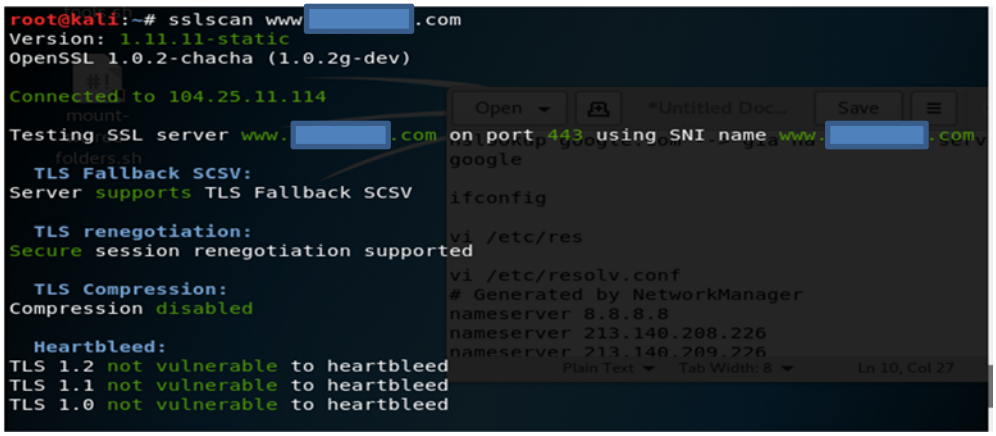


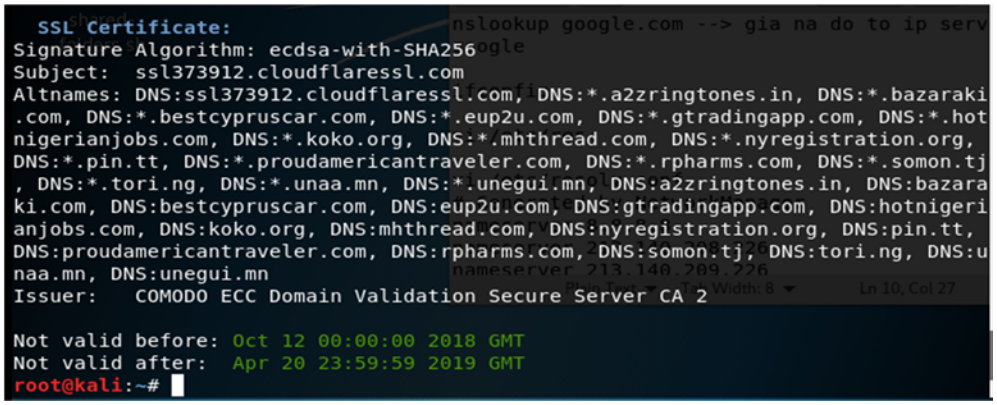
Η ένδειξη session renegotiation not support που παρουσιάζεται πιο κάτω σημαίνει ότι δεν υποστηρίζεται η επαναδιαπραγμάτευση της περιόδου σύνδεσης η οποία σχετίζεται με τις επιθέσεις των χαρακτηριστικών του πρωτοκόλλου SSL/TLS.



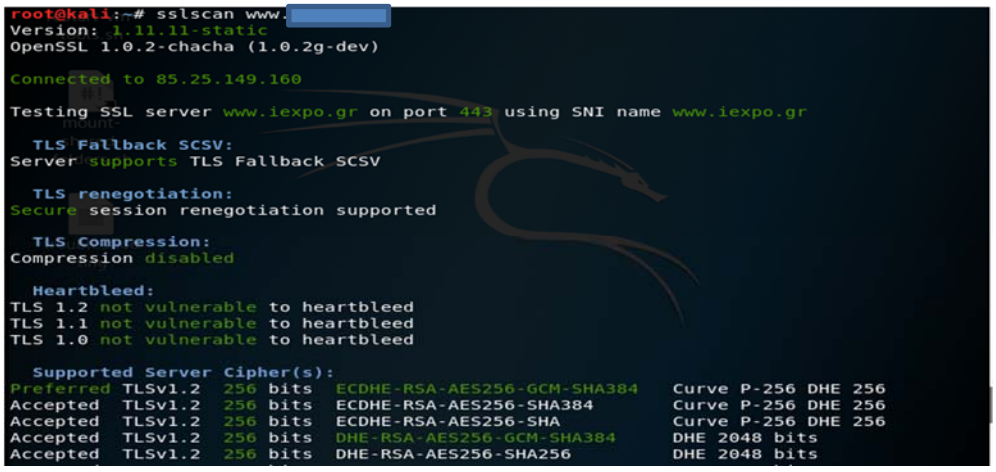


Στο παράδειγμα αυτό γίνεται η εφαρμογή της εντολής sslscan σε μια ιστοσελίδα η οποία εφαρμόζει το πρωτόκολλο HTTPS, με το πιστοποιητικό να είναι ενεργοποιημένο σωστά και να πληροί τις κατάλληλες προϋποθέσεις.





Στην πιο κάτω περίπτωση της ιστοσελίδας έχει εκτελεστεί η εντολή sslscan όπου τα αποτελέσματα έδειξαν ότι δεν υπάρχει ασφάλεια στον αλγόριθμο υπογραφής (Sha1WithRsaEncryption) και το πιστοποιητικό που χρησιμοποιεί ο εκδότης Cronus έχει περάσει την ημερομηνία λήξεως. Επίσης για τα πρωτόκολλα SSLv2 και SSLv3 θα πρέπει να απενεργοποιηθούν γιατί δεν παρέχουν ασφάλεια και να ενεργοποιηθεί το πρωτόκολλο TLS.



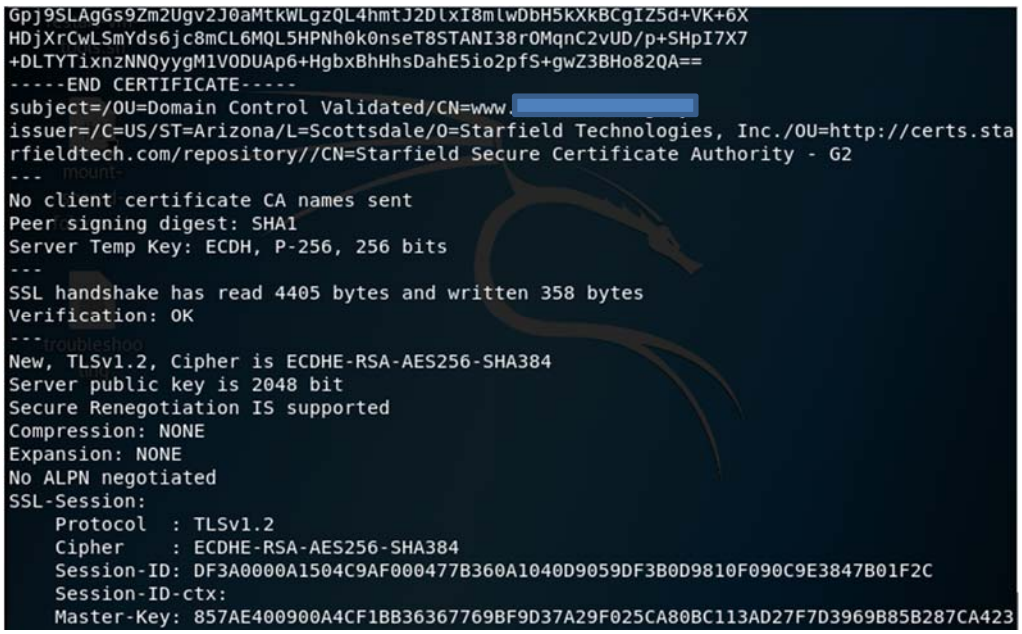
```
Accepted  TLSv1.0  112 bits  DES-CBC3-SHA
Preferred SSLv3    256 bits  ECDHE-RSA-AES256-SHA          Curve P-256 DHE 256
Accepted  SSLv3    256 bits  DHE-RSA-AES256-SHA            DHE 2048 bits
Accepted  SSLv3    256 bits  DHE-RSA-CAMELLIA256-SHA       DHE 2048 bits
Accepted  SSLv3    256 bits  AES256-SHA
Accepted  SSLv3    256 bits  CAMELLIA256-SHA
Accepted  SSLv3    128 bits  ECDHE-RSA-AES128-SHA          Curve P-256 DHE 256
Accepted  SSLv3    128 bits  DHE-RSA-AES128-SHA            DHE 2048 bits
Accepted  SSLv3    128 bits  DHE-RSA-SEED-SHA              DHE 2048 bits
Accepted  SSLv3    128 bits  DHE-RSA-CAMELLIA128-SHA       DHE 2048 bits
Accepted  SSLv3    128 bits  AES128-SHA
Accepted  SSLv3    128 bits  SEED-SHA
Accepted  SSLv3    128 bits  CAMELLIA128-SHA
Accepted  SSLv3    128 bits  ECDHE-RSA-RC4-SHA             Curve P-256 DHE 256
Accepted  SSLv3    128 bits  RC4-SHA
Accepted  SSLv3    112 bits  ECDHE-RSA-DES-CBC3-SHA        Curve P-256 DHE 256
Accepted  SSLv3    112 bits  EDH-RSA-DES-CBC3-SHA          DHE 2048 bits
Accepted  SSLv3    112 bits  DES-CBC3-SHA

  SSL Certificate:
Signature Algorithm: sha1WithRSAEncryption
RSA Key Strength:    2048

Subject:  Cronus
Issuer:   Cronus

Not valid before: Oct 25 09:09:18 2013 GMT
Not valid after:  Oct 25 09:09:18 2014 GMT
root@kali:~#
```

B.2 Παραδείγματα των αποτελεσμάτων openssl

Χρησιμοποίηση των εντολών openssl σε ιστοσελίδα που υποστηρίζει το πρωτόκολλο HTTPS για τον εντοπισμό κυρίως του δημοσίου κλειδιού (public key).

```
root@kali:~# openssl s_client -connect www.[redacted]:443
CONNECTED(00000003)
depth=2 C = US, ST = Arizona, L = Scottsdale, O = "Starfield Technologies, Inc.", CN =
Starfield Root Certificate Authority - G2
verify return:1
depth=1 C = US, ST = Arizona, L = Scottsdale, O = "Starfield Technologies, Inc.", OU =
http://certs.starfieldtech.com/repository/, CN = Starfield Secure Certificate Authority
 - G2
verify return:1
depth=0 OU = Domain Control Validated, CN = www.[redacted]
verify return:1
---
Certificate chain
 0 s:/OU=Domain Control Validated/CN=www[redacted]
   i:/C=US/ST=Arizona/L=Scottsdale/O=Starfield Technologies, Inc./OU=http://certs.starf
ieldtech.com/repository//CN=Starfield Secure Certificate Authority - G2
 1 s:/C=US/ST=Arizona/L=Scottsdale/O=Starfield Technologies, Inc./OU=http://certs.starf
ieldtech.com/repository//CN=Starfield Secure Certificate Authority - G2
   i:/C=US/ST=Arizona/L=Scottsdale/O=Starfield Technologies, Inc./CN=Starfield Root Cer
tificate Authority - G2
 2 s:/C=US/ST=Arizona/L=Scottsdale/O=Starfield Technologies, Inc./CN=Starfield Root Cer
tificate Authority - G2
   i:/C=US/O=Starfield Technologies, Inc./OU=Starfield Class 2 Certification Authority
---
```

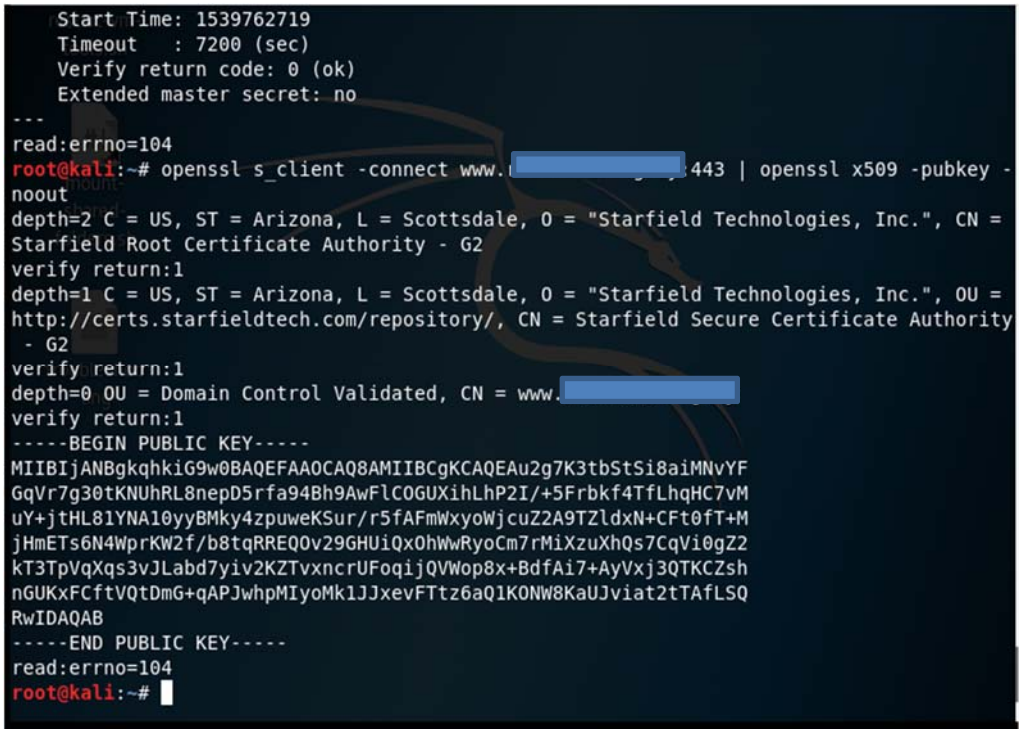
```
Server certificate
-----BEGIN CERTIFICATE-----
MIIFZzCCBE+gAwIBAgIJAObbGsZsDlOOMA0GCSqGSIb3DQEBCwUAMIHGMQswCQYD
VQQGEwJVUzEQMA4GA1UECBMHQXJpem9uYTETMBEGA1UEBxMKU2NvdHRzZGFsZTEl
MCMGA1UEChMcU3RhcmZpZWxkIFRlY2hub2xvZ2llcywgSW5jLjEzMDEGA1UECxMq
aHR0cDovL2NlcnRzLnN0YXJmaWVsZHRlY2guY29tL3JlcG9zaXRvcnkvMTQwMgYD
VQQDEytTdGFyZmllbGQgU2VjdXJlIENlcnRpZmljYXRlIEF1dGhvcml0eSAtIEcy
MB4XDTE4MDIxNDA5MDMwMFoXDTE5MDQxMjA3NDEzOFowQTEhMB8GA1UECxMYRG9t
YWluIENvbnRyb2wgVmFsaWRhdGVkMRwwGgYDVQQDExN3d3cucmVkY3Jvc3Mub3Jn
LmN5MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAu2g7K3tbStSi8aiM
NvYFGqVr7g30tKNUhRL8nepD5rfa94Bh9AwFlCOGUXihLhP2I/+5FrbkF4TfLhqH
C7vMuY+jtHL81YNA10yyBMky4zpuweKSur/r5fAFmWxyoWjcuZ2A9TZldxN+CFt0
fT+MjHmETs6N4WprKW2f/b8tqRREQOv29GHUiQxOhWwRyoCm7rMiXzuXhQs7CqVi
0gZ2kT3TpVqXqs3vJLabd7yiv2KZTvxncrUFoqijQVWop8x+BdfAi7+AyVxj3QTK
CZshnGUKxFCftVQtDmG+qAPJwhpMIyoMk1JJxevFTtz6aQ1KONW8KaUJv1at2tTA
fLSQRwIDAQABo4IB2jCCAdYwDAYDVR0TAQH/BAIwADAdBgNVHSUEFjAUBggrBgEF
BQcDAQYIKwYBBQUHAwIwDgYDVR0PAQH/BAQDAgWgMDwGA1UdHwQ1MDMwMaAvoC2G
K2h0dHA6Ly9jcmwuc3RhcmZpZWxkdGVjaC5jb20vc2ZpZzJzMS04NC5jcmwwYwYD
VR0gBFwwWjBOBgtghkgBhv1uAQcXATA/MD0GCCsGAQUFBwIBFjFodHRwOi8vY2Vy
dGlmaWNhdGVzLnN0YXJmaWVsZHRlY2guY29tL3JlcG9zaXRvcnkvMAgGBmeBDAEC
ATCBggYIKwYBBQUHAQEEdjB0MCoGCCsGAQUFBzABhh5odHRwOi8vb2NzcC5zdGFy
ZmllbGR0ZWNoLmNvbS8wRgYIKwYBBQUHMAKGOmh0dHA6Ly9jZXJ0aWZpY2F0ZXMu
c3RhcmZpZWxkdGVjaC5jb20vcmVwb3NpdG9yeS9zZmlnMi5jcnQwHwYDVR0jBBgw
FoAUJUWBaFAmOD07LSy+zWrZtj2zZmMwLwYDVR0RBCgwJoITd3d3LnJlZGNyb3Nz
Lm9yZy5jeYIPcmVkY3Jvc3Mub3JnLmN5MB0GA1UdDgQWBBROooQ9CDMHt5I1py/d
QQ2/AmuqHTANBgkqhkiG9w0BAQsFAAOCAQEAzW5nV8kUfBgp8d2C/rt7R8AC7GKT
rkK7+sp6bqxu0Uq3uVQVUthHhoNXOE/F9hNyHruFfw6mMllTINt+6AMfptNw/ic8i
/PQUDTRqifeFEoLxjS3tjq5jmafNTlgjQ5d26l7I9TImFeRbQItg4aIOCCVlgPFp
```


Gpj9SLAgGs9Zm2Ugv2J0aMtkWLgzQL4hmtJ2DlxI8mlwDbH5kXkBCgIZ5d+VK+6X
HDjXrCwLSmYds6jc8mCL6MQL5HPNh0k0nseT8STANI38rOMqnC2vUD/p+SHpI7X7
+DLTYTixnzNNQyygM1VODUAp6+HgbxBhHhsDahE5io2pfS+gwZ3BHo82QA==
-----END CERTIFICATE-----
subject=/OU=Domain Control Validated/CN=www.[redacted]
issuer=/C=US/ST=Arizona/L=Scottsdale/O=Starfield Technologies, Inc./OU=http://certs.sta
rfieldtech.com/repository//CN=Starfield Secure Certificate Authority - G2

No client certificate CA names sent
Peer signing digest: SHA1
Server Temp Key: ECDH, P-256, 256 bits

SSL handshake has read 4405 bytes and written 358 bytes
Verification: OK

New, TLSv1.2, Cipher is ECDHE-RSA-AES256-SHA384
Server public key is 2048 bit
Secure Renegotiation IS supported
Compression: NONE
Expansion: NONE
No ALPN negotiated
SSL-Session:
    Protocol : TLSv1.2
    Cipher   : ECDHE-RSA-AES256-SHA384
    Session-ID: DF3A0000A1504C9AF000477B360A1040D9059DF3B0D9810F090C9E3847B01F2C
    Session-ID-ctx:
    Master-Key: 857AE400900A4CF1BB36367769BF9D37A29F025CA80BC113AD27F7D3969B85B287CA423


    Start Time: 1539762719
    Timeout   : 7200 (sec)
    Verify return code: 0 (ok)
    Extended master secret: no
---
read:errno=104
root@kali:~# openssl s_client -connect www.[redacted]:443 | openssl x509 -pubkey -
noout
depth=2 C = US, ST = Arizona, L = Scottsdale, O = "Starfield Technologies, Inc.", CN =
Starfield Root Certificate Authority - G2
verify return:1
depth=1 C = US, ST = Arizona, L = Scottsdale, O = "Starfield Technologies, Inc.", OU =
http://certs.starfieldtech.com/repository/, CN = Starfield Secure Certificate Authority
 - G2
verify return:1
depth=0 OU = Domain Control Validated, CN = www.[redacted]
verify return:1
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAu2g7K3tbStSi8aiMNvYF
GqVr7g30tKNUhRL8nepD5rfa94Bh9AwFlCOGUXihLhP2I/+5Frbkf4TfLhqHC7vM
uY+jtHL81YNA10yyBMky4zpuweKSur/r5fAFmWxyoWjcuZ2A9TZldxN+CFt0fT+M
jHmETs6N4WprKW2f/b8tqRREQOv29GHUiQxOhWwRyoCm7rMiXzuXhQs7CqVi0gZ2
kT3TpVqXqs3vJLabd7yiv2KZTvxncrUFoqijQVWop8x+BdfAi7+AyVxj3QTKCZsh
nGUKxFCftVQtDmG+qAPJwhpMIyoMk1JJxevFTtz6aQ1KONW8KaUJviat2tTAfLSQ
RwIDAQAB
-----END PUBLIC KEY-----
read:errno=104
root@kali:~#

Μετά την εφαρμογή των εντολών openssl παρουσιάζεται το σφάλμα: unable to load certificate/expecting: trusted certificate. Οι ιστοσελίδες αυτές δεν χρησιμοποιούν το πρωτόκολλο HTTPS με αποτέλεσμα να μην γίνεται κατορθωτή η φόρτωση του πιστοποιητικού.

```
root@kali:~# openssl s_client -connect www[redacted].com:443
140306162155712:error:0200206F:system library:connect:Connection refused:../crypto/bio/
b_sock2.c:108:
140306162155712:error:2008A067:BIO routines:BIO_connect:connect error:../crypto/bio/b_s
ock2.c:109:
connect:errno=111
root@kali:~# openssl s_client -connect www.[redacted]443 | openssl x509 -pubkey -no
out
140447431004352:error:0200206F:system library:connect:Connection refused:../crypto/bio/
b_sock2.c:108:
140447431004352:error:2008A067:BIO routines:BIO_connect:connect error:../crypto/bio/b_s
ock2.c:109:
connect:errno=111
unable to load certificate
140088634417344:error:0906D06C:PEM routines:PEM_read_bio:no start line:../crypto/pem/pe
m_lib.c:691:Expecting: TRUSTED CERTIFICATE
root@kali:~#
```

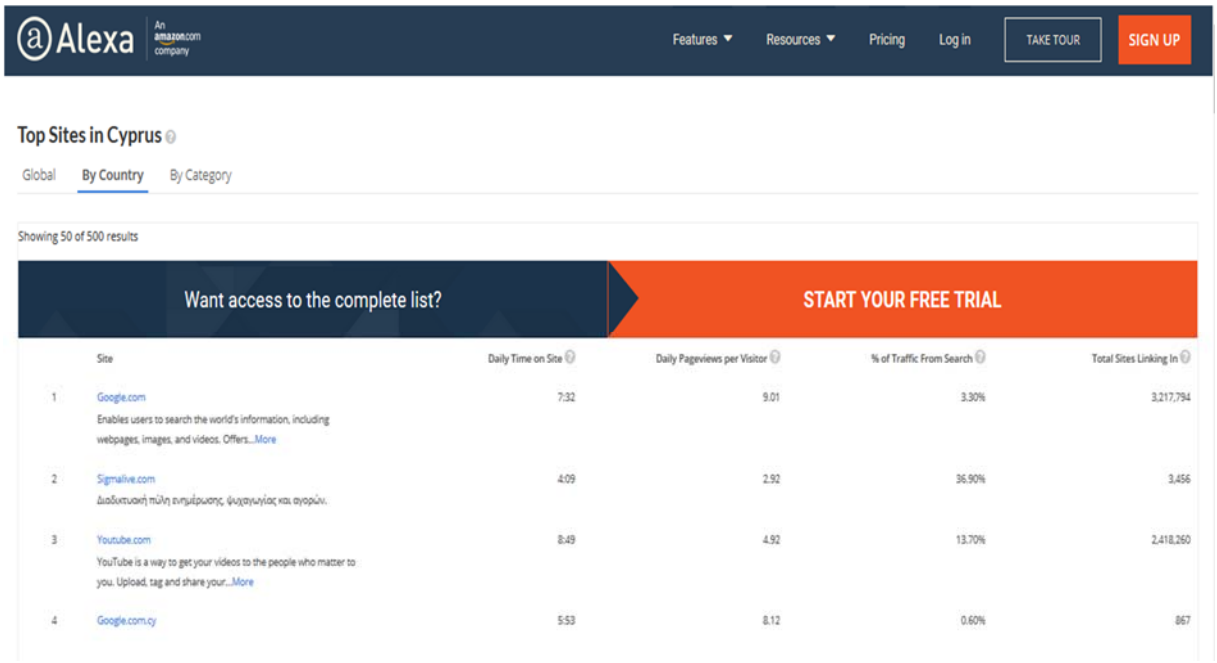
```
root@kali:~# openssl s_client -connect www[redacted]com:443
CONNECTED(00000003)
write:errno=104
---
no peer certificate available
---
No client certificate CA names sent
---
SSL handshake has read 0 bytes and written 176 bytes
Verification: OK
---
New, (NONE), Cipher is (NONE)
Secure Renegotiation IS NOT supported
Compression: NONE
Expansion: NONE
No ALPN negotiated
SSL-Session:
    Protocol  : TLSv1.2
    Cipher    : 0000
    Session-ID:
    Session-ID-ctx:
    Master-Key:
    PSK identity: None
    PSK identity hint: None
    SRP username: None
    Start Time: 1539890496
    Timeout   : 7200 (sec)
    Verify return code: 0 (ok)
    Extended master secret: no
```

```
root@kali:~# openssl s_client -connect www[redacted].com:443 | openssl x509 -pubkey
 -noout
write:errno=104
unable to load certificate
140159433941184:error:0906D06C:PEM routines:PEM_read_bio:no start line:../crypto/pem/pe
m_lib.c:691:Expecting: TRUSTED CERTIFICATE
root@kali:~#
```

Παράρτημα Γ

Ο ιστότοπος Alexa

Γ.1 Οι κορυφαίες ιστοσελίδες στην Κύπρο σύμφωνα με τον ιστότοπο Alexa:



5	Philenews.com Η επίσημη ιστοσελίδα της μεγαλύτερης σε κυκλοφορία εφημερίδα της Κύπρου. Σας ενημερώνουμε για ό...More	5:08	3.77	26.20%	2,429
6	Tothemaonline.com ΤΟ ΠΛΗΡΕΣΤΕΡΟ ΕΙΔΗΣΕΟΓΡΑΦΙΚΟ PORTAL ΤΗΣ ΚΥΠΡΟΥ. Αποκαλυπτικό άμεσο και τολμηρό.	4:00	2.70	19.00%	514
7	Facebook.com A social utility that connects people, to keep up with friends, upload photos, share links and ...More	9:49	3.92	7.40%	6,415,532
8	Politis.com.cy Η ηλεκτρονική έκδοση της ημερήσιας πρωινής εφημερίδος «ΠΟΛΙΤΗΣ». Περιλαμβάνει τα τελευταία πολι...More	3:46	2.41	36.90%	1,123
9	Vk.com Социальная сеть как средство для коммуникации и поиска людей. Международный сервис, созданный р...More	10:03	4.51	4.70%	378,829
10	Yandex.ru Поиск информации в интернете с учетом русской морфологии, возможность регионального уточнения. ...More	6:27	3.33	0.80%	262,228
11	Wikipedia.org A free encyclopedia built collaboratively using wiki software. (Creative Commons Attribution-Sh...More	4:05	3.07	60.00%	1,715,394
12	Live.com Search engine from Microsoft.	4:01	3.67	12.30%	50,940
13	Instagram.com	5:58	3.56	10.60%	1,778,460
14	Yahoo.com A major internet portal and service provider offering search results, customizable content, cha...More	3:54	3.38	7.50%	612,450
15	Bankofcyprus.com Includes a joint stock bank and an insurance company.	5:26	3.72	12.20%	369
16	Diaforetiko.gr Παράξενες ειδήσεις απο μια διαφορετική ματιά!	3:17	1.96	12.90%	1,346
17	Bazaraki.com Bazaraki.com: Selling is believing... / About Us The Ultimate in Cyprus Classified Ads ... After...More	11:14	9.14	18.10%	72
18	Mail.ru Портал Mail.Ru (проект Mail.Ru Group) – самый популярный сайт рунета (30,452 млн. пользователей...More	5:16	3.50	2.30%	255,343
19	Ebay.com International person to person auction site, with products sorted into categories.	9:14	6.88	19.30%	147,109
20	Tilestwra.com Τα καλύτερα θέματα, ειδήσεις, βίντεο και φωτογραφίες από όλο τον κόσμο.	3:33	1.88	11.80%	2,134
21	Lifo.gr LIFO.gr - Ειδήσεις, Άνθρωποι, Διασκέδαση, Urban Culture & Αθήνα με πρωτοποριακό πάντα τρόπο.	9:52	4.64	18.50%	5,850
22	Google.ru Русскоязычная версия поискового сервера.	5:10	7.55	0.60%	33,620
23	Aliexpress.com Launched in April 2010, AliExpress (www.aliexpress.com) is a global retail marketplace targeted...More	12:30	11.38	9.90%	36,701
24	Pentapostagma.gr Ειδήσεις από Ελλάδα και Κύπρο. Στο Πενταπόσταγμα θα μάθεις ότι, οι άλλοι σου κρύβουν..	9:16	4.30	14.60%	3,741
25	Blogspot.com	3:13	2.41	44.80%	18,146
26	Amazon.com Amazon.com seeks to be Earth's most customer-centric company, where customers can find and disc...More	7:56	8.08	22.60%	719,570
27	Pornhub.com Please contact dice[/at/]pornhub[/dot/]com for any inquiries.	8:36	3.29	27.40%	10,161

28	Parimatch.com.cy	1:58	1.20	1.10%	14
29	Moec.gov.cy Features programs, news and list of the associated authorities.	4:03	3.57	37.90%	694
30	Ebay.co.uk Person to person online auction site where you can buy or sell new and used items.	10:04	8.07	21.90%	32,543
31	Amazon.co.uk Online retailer of books, movies, music and games along with electronics, toys, apparel, sports...More	5:60	6.81	25.70%	108,790
32	Stoiximan.com.cy	1:33	1.20	3.60%	22
33	Booking.com Worldwide accommodation reservations.	8:54	4.70	20.70%	63,510
34	Zougla.gr Ειδησεογραφία από την Ελλάδα και τον κόσμο. Όλα τα νέα γύρω από την Πολιτική, Οικονομία, Υγεία,...More	6:41	3.51	15.00%	7,311
35	Google.gr Η μεγαλύτερη μηχανή αναζήτησης παγκόσμια στα ελληνικά.	6:35	10.14	0.80%	6,385
36	Bongacams.com Live Webcam Sex Shows For Free Without Registration! Join largest Adult Sex Cams community and ...More	4:12	1.86	10.20%	151,932
37	Kerkida.net sports news -europe -milan -liverpool -ajax -tennis -football -cyprus -greece -athens-formula -...More	6:05	5.73	7.90%	173
38	Vice.com Vice.com is the world beyond the front page, in all its absurdity: opinion, human interest, ent...More	2:22	1.36	26.90%	107,684
39	Xhamster.com xHamster is a community of open-minded people. Our site contains adult videos, photos, dating, ...More	12:16	9.72	22.60%	6,644
40	Enallaktikidirasi.com	4:06	2.85	20.80%	1,683
41	Twitter.com Social networking and microblogging service utilising instant messaging, SMS or a web interface.	6:01	2.92	9.80%	4,897,007
42	Altsantiri.gr Αληθινές ειδήσεις - Ενημέρωση με άποψη και σάτιρα! Βρείτε ειδήσεις για Ελλάδα, Πολιτική, Παραπο...More	4:47	3.03	18.10%	1,637
43	Imdb.com Features plot summaries, reviews, cast lists, and theatre schedules.	3:31	3.99	50.40%	285,674
44	Cytanet.com.cy Presents company's network, services, support contacts, downloads and search. Games and cafes a...More	3:54	1.80	9.70%	299
45	Office.com Online business resource with industry-specific news and analysis, tools and access to relevant...More	3:20	2.17	13.40%	9,258
46	Livejournal.com LiveJournal is a rich, community media platform that willfully blurs the lines between journali...More	5:19	2.96	10.70%	40,352
47	Jccsmart.com JCCSmart is a registered trademark of JCC PAYMENT SYSTEMS LTD. jccsmart.com is an online market...More	7:01	6.40	25.30%	65
48	Cyta.com.cy Provides mobile, fixed and internet services for residential and business customers. Publishers...More	3:30	3.00	31.10%	178
49	In.gr Δικτυακή πύλη με θεματικό κατάλογο, νέα, υπηρεσίες e-mail, διασκέδαση, πολιτιστικά, καιρό, μηχα...More	6:53	3.18	15.40%	9,751
50	Ladbible.com	2:35	1.36	12.00%	4,520

Παράρτημα Δ
Απαιτήσεις του GDPR στις Επιχειρήσεις

Δ.1 Βασικές αρχές νομιμότητας του GDPR:

Διεθνείς Μεταφορές Δεδομένων και Ασπίδα Προστασίας Προσωπικών Δεδομένων: Το GDPR δεν επιτρέπει στις επιχειρήσεις να μετακινούν τα προσωπικά δεδομένα εκτός Ευρωπαϊκής Ένωσης όμως με την συμφωνία Ασπίδα Προστασίας Προσωπικών Δεδομένων ΕΕ-ΗΠΑ παρέχει το δικαίωμα στις Ευρωπαϊκές επιχειρήσεις να κρατούν στην κατοχή τους δεδομένα στο νέφος (cloud) που βρίσκονται στις ΗΠΑ.

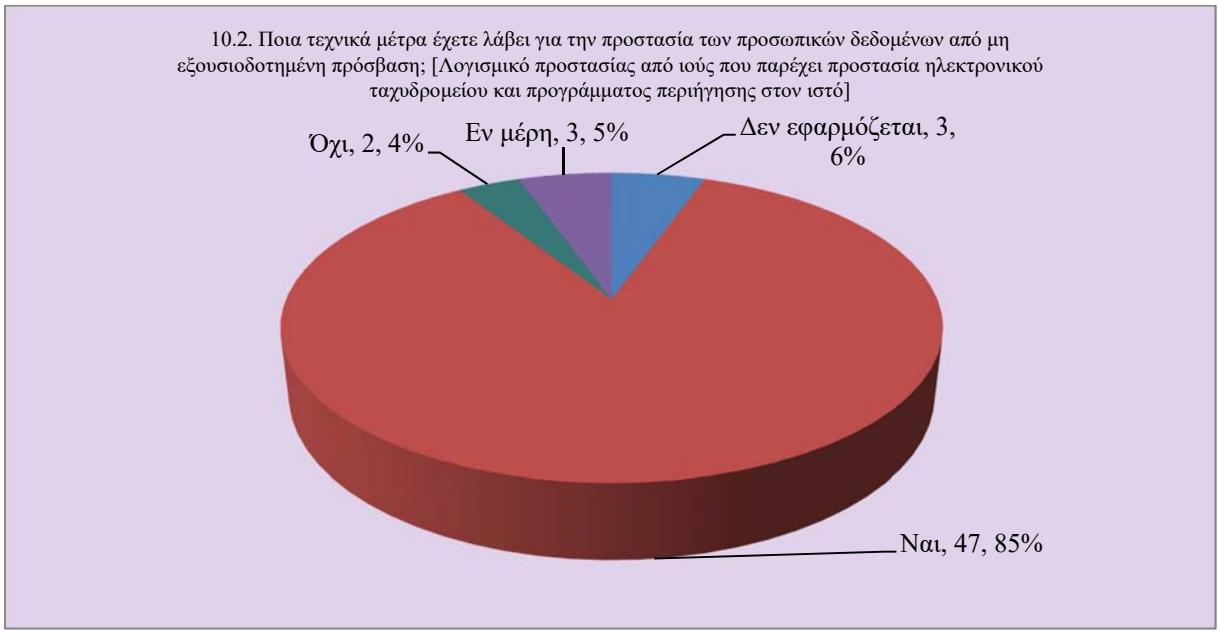
Θέματα Αιτήσεων Πρόσβασης: Το GDPR δίνει το δικαίωμα στους πελάτες να έχουν πρόσβαση στα προσωπικά τους δεδομένα για να μπορούν να τα διαγράψουν ή διορθώσουν. Μετά από κάποιες έρευνες που έγιναν στις επιχειρήσεις έδειξαν ότι είναι ανέτοιμες σε θέματα αιτημάτων πρόσβασης και έτσι καλούνται να διερευνηθούν κάποια σημεία τα οποία χρειάζονται βελτίωση όπως τον τρόπο που θα υποβάλλουν τα αιτήματα τους (ηλεκτρονικά, τηλεφωνικά, κλπ.), ο χρόνος που χρειάζεται για να υλοποιηθεί ένα αίτημα κ.α.

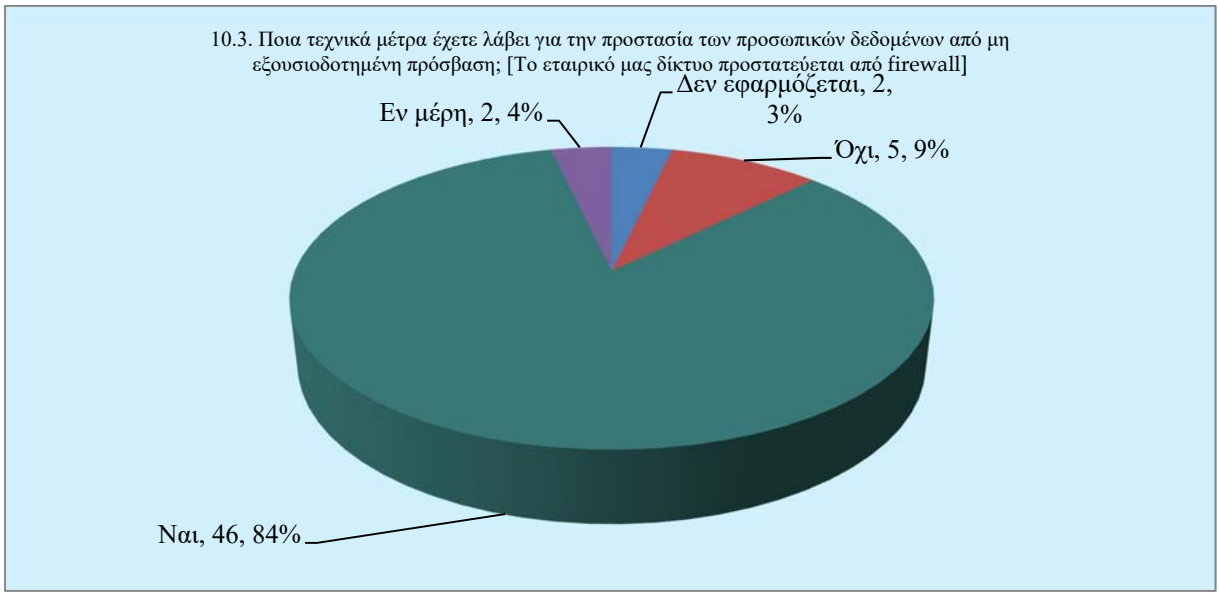
Συλλογή Δεδομένων: Στην διαδικασία συλλογής δεδομένων οι επιχειρήσεις είναι υποχρεωμένες να ειδοποιήσουν τους πελάτες που έχουν άμεσα σχέση με τα δεδομένα για την ταυτότητα της επιχείρησης, για τον σκοπό που τα χρειάζονται, γιατί τα θέλουν και πως θα τα χρησιμοποιήσουν. Επίσης η συμφωνία αποδοχής που έχει γίνει μεταξύ του πελάτη πρέπει να υφίσταται σε ένα αρχείο για σκοπούς επιβεβαίωσης.

Διατήρηση Δεδομένων: Οι επιχειρήσεις πλέον δεν θα μπορούν να έχουν στην κατοχή τους μόνιμα τα προσωπικά δεδομένα των πελατών τους και για αυτόν τον λόγο θα πρέπει να γνωρίζουν το διάστημα στο οποίο θα τα έχουν και πως θα τα εξαλείψουν.

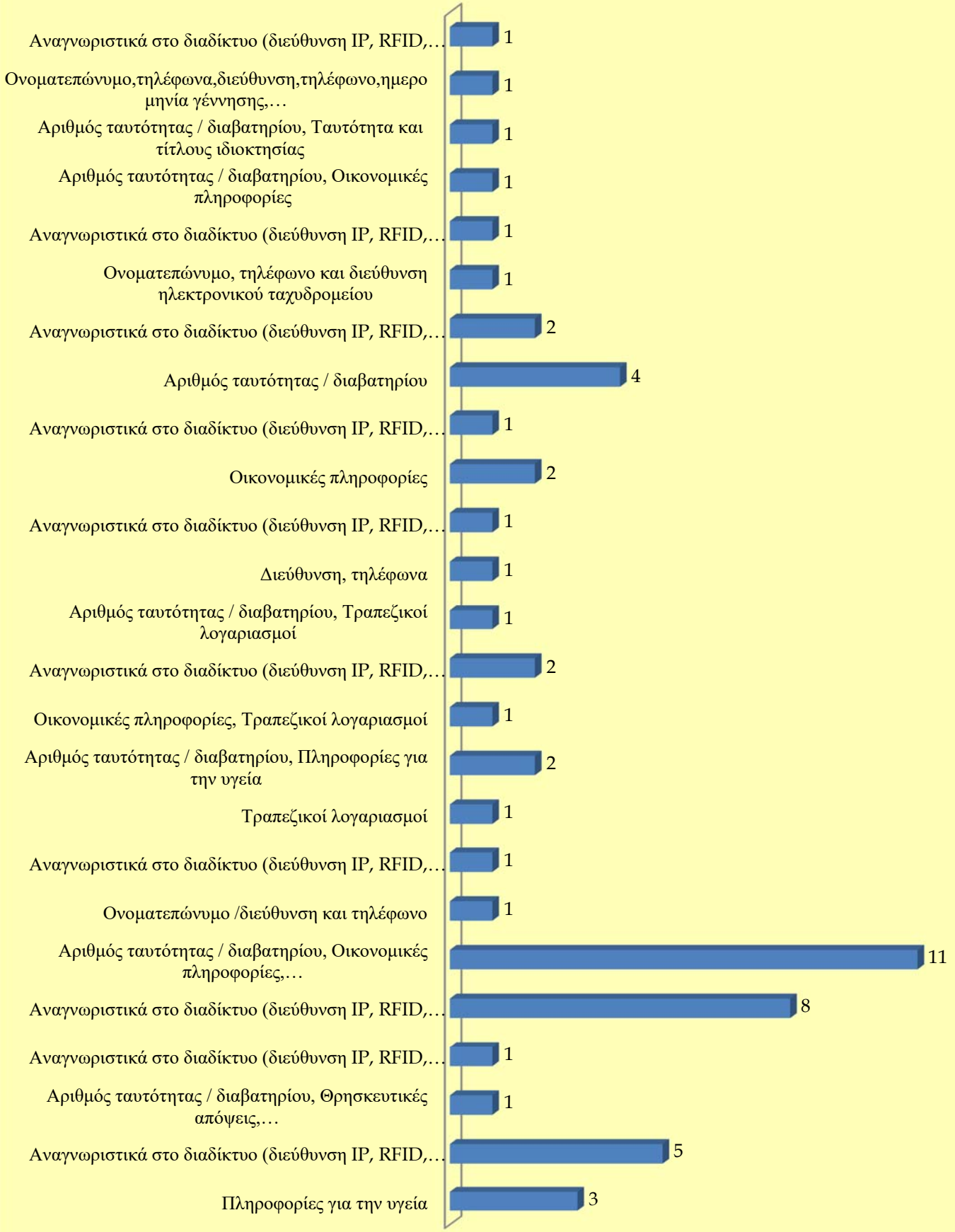
Παράρτημα Ε
Σχήματα ερωτήσεων ερωτηματολογίου

Ε.1 Σχήματα Ερωτηματολογίου

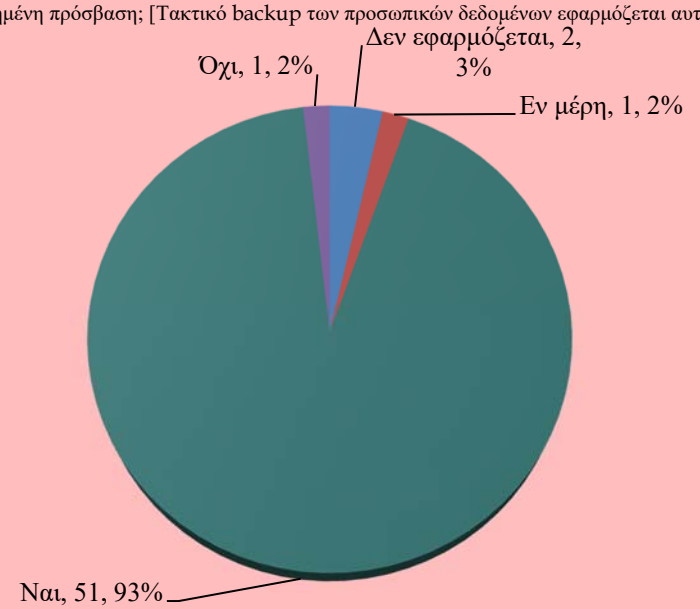




5. Εάν ναι, τι είδους προσωπικά δεδομένα χειρίζεται η επιχείρηση;



10.4. Ποια τεχνικά μέτρα έχετε λάβει για την προστασία των προσωπικών δεδομένων από μη εξουσιοδοτημένη πρόσβαση; [Τακτικό backup των προσωπικών δεδομένων εφαρμόζεται αυτόματα]



10.5.Ποια τεχνικά μέτρα έχετε λάβει για την προστασία των προσωπικών δεδομένων από μη εξουσιοδοτημένη πρόσβαση; [Το εταιρικό μας Wi-Fi προστατεύεται με κωδικό πρόσβασης]