ΣΧΟΛΗ ΕΠΙΣΤΗΜΩΝ ΔΙΟΙΚΗΣΗΣ ΕΠΙΧΕΙΡΗΣΕΩΝ

ΤΜΗΜΑ ΛΟΓΙΣΤΙΚΗΣ ΚΑΙ ΧΡΗΜΑΤΟΟΙΚΟΝΟΜΙΚΗΣ

Π.Μ.Σ στη Λογιστική Φορολογία και Χρηματοοικονομική Διοίκηση

(Π.Μ.Σ στην Στρατηγική Διοικητική Λογιστική και Χρηματοοικονομική Διοίκηση για Στελέχη Επιχειρήσεων)

Διπλωματική Εργασία

Χρηματοοικονομικές επιπτώσεις των κινδύνων κυβερνοχώρου και του Γενικού Κανονισμού Προστασίας Δεδομένων (GDPR) σε Λογιστικά Γραφεία & Ελεγκτικές Εταιρίες

της

ΜΑΛΛΙΑΡΙΔΟΥ ΟΛΓΑΣ

Επιβλέπων Καθηγητής: Λιβάνης Ευστράτιος

Υποβλήθηκε ως απαιτούμενο για την απόκτηση του Μεταπτυχιακού Διπλώματος στη Στρατηγική Διοικητική Λογιστική και Χρηματοοικονομική Διοίκηση

Νοέμβριος 2019

Ευχαριστίες

Μέσα στις επόμενες γραμμές θα ήθελα να εκφράσω τις ειλικρινείς μου ευχαριστίες στον επιβλέπων καθηγητή κ. Λιβάνη Ευστράτιο, Λέκτορα του τμήματος Λογιστικής και Χρηματοοικονομικής, που συνέβαλε με τη βοήθεια του στην επιτυχή ολοκλήρωση της εργασίας.

Επίσης θα ήθελα να ευχαριστήσω το εκπαιδευτικό προσωπικό του ΠΜΣ της Στρατηγική Διοικητική Λογιστική και Χρηματοοικονομική Διοίκηση για τις πλούσιες εμπειρίες που αποκόμισα.

Πάνω από όλους θα ήθελα να εκφράσω τις ευχαριστίες μου στους γονείς μου και τον Βασίλη για την ενθάρρυνση, την ηθική συμπαράσταση την υπομονή και την αγάπη που μου προσέφεραν αυτά τα χρόνια.

Περίληψη

Η εργασία αυτή είναι η μελέτη για τον οικονομικό αντίκτυπο των κινδύνων κυβερνοχώρου και τον Γενικό Κανονισμό Προστασίας Δεδομένων (GDPR) στα λογιστικά γραφεία και τις ελεγκτικές εταιρίες. Η παρούσα διπλωματική εργασία αποτελείται από τη βιβλιογραφική επισκόπηση, τα αποτελέσματα της αναζήτησης του διαδικτύου και την έρευνα. Αναλυτικότερα γίνεται αναφορά στην έννοια των κινδύνων κυβερνοχώρου, την εφαρμογή του κανονισμού προστασίας των δεδομένων και τα προβλήματα που δημιουργούνται στις επιχειρήσεις.

Ακόμη αναφέρεται στον νέο Γενικό Κανονισμό Προστασίας Δεδομένων της Ευρωπαϊκής Ένωσης, που τέθηκε σε εφαρμογή στις 25 Μαΐου 2018, ο οποίος είναι υποχρεωτικός και άμεσα εφαρμοζόμενος σε όλα τα κράτη μέλη της Ευρωπαϊκής Ένωσης. Ο νέος νόμος επιβάλλει αυστηρά πρόστιμα στις επιχειρήσεις στην περίπτωση παραβίασης των συστημάτων υποκλοπής των δεδομένων τους ή στις περιπτώσεις ¨πώλησης¨ των δεδομένων αυτών (πχ factoring), που αποτελεί μια επιπρόσθετη οικονομική επιβάρυνση. Για την μείωση του κόστους αυτού οι επιχειρήσεις θα πρέπει να λάβουν άμεσα, μέτρα ασφαλείας ώστε να εξασφαλίσουν την ομαλή λειτουργία τους.

Για όλους τους παραπάνω λόγους πραγματοποιήθηκε ποσοτική έρευνα με ερωτηματολόγιο για να καταγραφεί το κατά πόσο γνωρίζουν τα λογιστικά γραφεία και οι ελεγκτικές εταιρίες, τον κίνδυνο από τον οποίο απειλούνται τα δεδομένα που διατηρούν, τις χρηματοοικονομικές συνέπειες που θα υποστούν και τι μέτρα πρόληψης έχουν λάβει ή πρόκειται να λάβουν.

Εν κατακλείδι οι περισσότεροι είναι ενημερωμένοι για τον διαδικτυακό κίνδυνο, τις άμεσες χρηματοοικονομικές συνέπιες και τα έμμεσα κόστη που μπορεί να διατρέχουν ως λογιστικά γραφεία ή ελεγκτικές εταιρίες, έχουν λάβει μέτρα προστασίας για την διαχείριση του κινδύνου και είναι διατεθειμένοι να ενισχυθούν και άλλο με τη βοήθεια εξωτερικών παραγόντων.

Abstact

The privalization of all assects of econy and access to cyber information in real time, constantly are changing fundamentally the way the “business activity”. Within this fluid business enviroment , the enterprices attemt not only to survive but also to find other mechanisms to ensure theiw data. Catalytic role in achieving the above iw required to play the General Data Protection Requlation (GDPR), was in effect from the 25th May 2018. Through an extensive literature and emerical reseach, the purpose of this article is to assess the financial implication of cyber threat. The results highlight the active role of GDPR to the eggective management of orerational risks improvement of corporate governance principles and the safe operation of business continuity.

Περιεχόμενα

ΚΑΤΑΛΟΓΟΣ ΠΙΝΑΚΩΝ

ΚΑΤΑΛΟΓΟΣ ΔΙΑΓΡΑΜΜΑΤΩΝ

ΚΕΦΑΛΑΙΟ 1

ΕΙΣΑΓΩΓΗ

Στην εποχή που διανύουμε η τεχνολογία έχει κάνει άλματα, με άμεσα αποτελέσματα στην ψηφιοποίηση των επιχειρήσεων και τη διευκόλυνση αυτών στη διεκπεραίωση των οικονομικών, εμπορικών και παραγωγικών λειτουργιών τους.

Την ίδια στιγμή όμως αυξάνεται και ο κίνδυνος επιθέσεων υποκλοπών και απώλειας των δεδομένων από τα πληροφοριακά συστήματα των επιχειρήσεων. Γι' αυτό το λόγο οι επιχειρήσεις θα πρέπει να κατανοήσουν τον σωστό τρόπο λειτουργίας των συστημάτων αυτών, να ασφαλιστούν με κάθε δυνατό τρόπο, έτσι ώστε να επωφελούνται των νέων τεχνολογιών χωρίς να επωμίζονται τους εκάστοτε κινδύνους.

1.1 Σκοπός της Εργασίας

Σκοπός της εργασίας είναι να διερευνηθεί κατά πόσο τα λογιστικά γραφεία και οι ελεγκτικές εταιρίες γνωρίζουν τις χρηματοοικονομικές συνέπειες των κινδύνων κυβερνοχώρου, το ευαίσθητο θέμα που προκύπτει από τη λάθος χρήση προστασίας των δεδομένων και ποία είναι τα μέτρα που έχουν λάβει από τις 25 Μαΐου 2018 και μετά.

1.2 Ερευνητικά Ερωτήματα

Τα ερευνητικά ερωτήματα που τέθηκαν είναι τα εξής:

1) Εάν τα λογιστικά γραφεία και οι ελεγκτικές εταιρίες γνωρίζουν την έννοια του διαδικτυακού κινδύνου

2) Εάν γνωρίζουν τις άμεσες και έμμεσες χρηματοοικονομικές συνέπειες της παραβίασης των δεδομένων

3)Εάν έχουν λάβει μέτρα προστασίας για τη διαχείριση του διαδικτυακού κινδύνου

4)Εάν γνωρίζουν τα ασφαλιστήρια συμβόλαια ως μέτρο διαχείρισης του κινδύνου

1.3 Μεθοδολογία

Έγινε ποσοτική έρευνα με ερωτηματολόγιο το οποίο στάλθηκε με ηλεκτρονικό ταχυδρομείο σε λογιστικά γραφεία της Κύπρου που είναι εγγεγραμμένα στον Σύνδεσμο Εγκεκριμένων Λογιστών Κύπρου (ΣΕΛΚ). Ο αριθμός του δείγματος είναι 252 λογιστικά γραφεία, 50 ελεγκτικές εταιρίες και ο αριθμός των συμμετεχόντων στην έρευνα είναι 97 (ποσοστό συμμετοχής 28%)

1.4 Δομή Εργασίας

Η εργασία χωρίζεται σε δύο μέρη. Το πρώτο μέρος είναι η αναλυτική βιβλιογραφική επισκόπηση και το δεύτερο μέρος το πρακτικό κομμάτι της έρευνας.

Στο δεύτερο κεφάλαιο αναφέρεται η έννοια του κινδύνου κυβερνοχώρου, γίνεται ταξινόμηση των κινδύνων, τα κίνητρα επιθέσεων, οι κατηγορίες απειλών οι μέθοδοι επιθέσεων καθώς και γεγονότα και περιστατικά παραβιάσεων.

Στο τρίτο αναφέρεται στο θεσμικό πλαίσιο του νέου Ευρωπαϊκού Κανονισμού και τις διατάξεις αυτού όπως τις κατηγορίες των δεδομένων, και τα βασικά δικαιώματα των πολιτών καθώς και στατιστικά στοιχεία μελετών.

Στο τέταρτο αναλύονται οι πρακτικές αντιμετώπισης και εξασφάλισης ελέγχου ασφαλείας, τεχνολογικά μέσα και οι ασφάλειες- ασφαλιστήρια συμβόλαια του κυβερνοχώρου.

Στο πέμπτο και έκτο κεφάλαιο αυτό της έρευνας περιλαμβάνεται η παρουσίαση της μεθοδολογίας και η ανάλυση των αποτελεσμάτων.

Η παρούσα εργασία ολοκληρώνεται με την παράθεση των συμπερασμάτων στο έβδομο κεφάλαιο.

1.5 Συνεισφορά στη Βιβλιογραφία

Η συνεισφορά στη βιβλιογραφία έχει πολλαπλά οφέλη, καθώς γνωρίζοντας τις παραμέτρους, αναγνωρίζοντας τα προβλήματα που δημιουργούνται και αντιμετωπίζοντάς τα οι επιχειρήσεις μπορούν να αποφύγουν τις πιθανές οικονομικές συνέπειες, οι οποίες μπορεί να αποβούν καταστροφικές για τους ίδιους τους οργανισμούς.

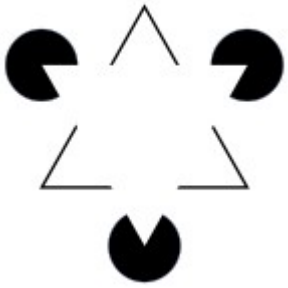
ΚΕΦΑΛΑΙΟ 2

ΒΙΒΛΙΟΓΡΑΦΙΚΗ ΕΠΙΣΚΟΠΗΣΗ

2.1 Κίνδυνοι Κυβερνοχώρου

2.1.1 Ορισμός

Ως κίνδυνο στον κυβερνοχώρο ορίζουμε τον λειτουργικό κίνδυνο των πληροφοριακών και τεχνολογικών περιουσιακών στοιχείων με συνέπεια να επηρεάζουν την εμπιστευτικότητα, τη διαθεσιμότητα ή την ακεραιότητα των πληροφοριακών συστημάτων. (Cebula and Young, 2010)



Εικόνα 1: <<Ο κυβερνοχώρος μοιάζει με το λευκό τρίγωνο της εικόνας που εμφανίζεται εικονικά, που δεν υπάρχει πουθενά, ενώ ενώνει υπολογιστές σε όλο τον κόσμο>>

2.1.2 Ταξινόμηση κινδύνων κυβερνοχώρου

Οι κίνδυνοι στον κυβερνοχώρο κατατάσσονται σε δύο κατηγορίες, οι οποίες είναι α) εσωτερικοί-ενδοεταιρικοί που αφορούν την εύρεση του προβλήματος από την ίδια την εταιρία και β) εξωτερικοί, όπου είτε ο οργανισμός μπορεί να τους προβλέψει και να προετοιμαστεί είτε όχι (π.χ. φυσικές καταστροφές)

Εσωτερικοί:

- Ακούσιες ανθρώπινες ενέργειες (Λάθος χειρισμός πληροφοριακών συστημάτων)
- Κακόβουλες ανθρώπινες ενέργειες

- Βλάβες πληροφοριακών συστημάτων

Εξωτερικοί:

- Hackers
- Πολιτικά γεγονότα χώρας
- Βλάβες πληροφοριακών συστημάτων τρίτων
- Φυσικές καταστροφές

2.2 Κίνητρα επιθέσεων

2.2.1 Οικονομικά οφέλη- Σαμποτάζ- Διαμαρτυρία

Τα κίνητρα μπορεί να ποικίλουν. Οι επιθέσεις μπορεί να έχουν σκοπό να αποσπάσουν χρήματα, να σαμποτάρουν την ομαλή λειτουργία του οργανισμού και να βλάψουν τη φήμη και την πελατεία του, ή ακόμη για να διαμαρτυρηθούν για πολιτικούς ή θρησκευτικούς λόγους. Τέλος μπορεί να γίνει για λόγους εκδίκησης ή για την απόκτηση στρατηγικού πλεονεκτήματος από ανταγωνιστή ή απλώς από περιέργεια.

2.2.2 Κατηγορίες απειλών

Μικρές και μεγάλες επιχειρήσεις δέχονται επιθέσεις λόγω του ότι δεν διαθέτουν τους πόρους, την ευαισθητοποίηση και τις γνώσεις να προφυλαχθούν από απειλές που σχετίζονται με τον κυβερνοχώρο, όπως είναι το ransomware , οι επιθέσεις τύπου social engineering η άρνηση παροχής υπηρεσιών κτλ.

- Ο Κυβερνοεκβιασμός - Ransomware είναι ένα κακόβουλο λογισμικό που ¨κλειδώνει¨ τις λειτουργίες υπολογιστών και συστημάτων, ενώ παράλληλα μπορεί να κρυπτογραφήσει δεδομένα ζητώντας λύτρα για να αποκτηθεί πάλι ο έλεγχος του υπολογιστή και να χρησιμοποιηθούν ξανά τα μολυσμένα αρχεία.
- Η κοινωνική μηχανή – Social enginnering. Οι επιθέσεις συνήθως ξεκινούν με την εξαπάτηση ατόμων, αποσπώντας πληροφορίες που επιτρέπουν στον εισβολέα να έχει πρόσβαση σε πληροφοριακά συστήματα οργανισμών. Ο μεγάλος όγκος των δεδομένων που αναρτούν μέσω στον social media, δημιουργεί πρόσφορο έδαφος σε τέτοιου είδους επιθέσεις.

- Μια επίθεση άρνησης παροχής υπηρεσιών (DDoS) μπορεί να απενεργοποιήσει της online υπηρεσίες μιας επιχείρησης για μεγάλο χρονικό διάστημα, να βλάψει τη φήμη της και να στερήσει υπάρχοντες ή μελλοντικούς πελάτες.

- Το κατασκοπευτικό λογισμικό Spyware συγκεντρώνει κρυφά πληροφορίες σχετικές με τη χρήση μέσω σύνδεσης του διαδικτύου χωρίς ο χρήστης να το γνωρίζει. Μόλις εγκατασταθεί παρακολουθεί τη δραστηριότητα του χρήστη, και μεταδίδει κρυφά τις πληροφορίες σε κάποιον τρίτο. Μπορεί να απομνημονεύσει κωδικούς πρόσβασης και λογαριασμού.

- Ένας ιός υπολογιστών Virus μπορεί να μολύνει ένα ή περισσότερα αρχεία ενός υπολογιστή και να ταξιδεύει αυτόματα από υπολογιστή σε υπολογιστή. Τρόποι μετάδοσης γίνεται με το άνοιγμα ενός μολυσμένου συνημμένου μέσω e-mail, με το άνοιγμα ενός μολυσμένου αρχείου μέσω ενός USB flash memory stick.

- Μία υβριδική απειλή το Bothnet δίνει τον έλεγχο σε κάποιον εισβολέα καθώς μπορεί να κάνει σχεδόν τα πάντα. Από τη συλλογή εμπιστευτικών δεδομένων μέχρι και την αποστολή ενοχλητικής αλληλογραφίας. Το πρώτο πράγμα που κάνει είναι να συνδέσει τον μολυσμένο υπολογιστή με άλλους, δημιουργώντας έτσι ένα μολυσμένο δίκτυο υπολογιστών (ρομποτικό δίκτυο).

- Το Trojan Horse που προέρχεται από το μυθικό «δούρειο ίππο». Υπάρχουν διάφορα είδη δούρειων ίππων, τα πιο διαδεδομένα είναι, το Backdoor Trojans που επιτρέπει την πρόσβαση την πρόσβαση σε υπολογιστή από απρόσκλητους επισκέπτες και τους δίνει τη δυνατότητα να διαχειρίζονται τον υπολογιστή από απόσταση. Οι Banking Trojans που έχουν σχεδιαστεί για να κλέψουν χρήματα από τραπεζικούς λογαριασμούς και τέλος οι Trojan downloaders που κατεβάζουν ενημερωμένες εκδόσεις των δούρειων ίππων.

- Επίσης υπάρχει μια ευρύτερη ανησυχία από όλα τα ενδιαφερόμενα μέρη για την πιθανή παραβίαση δεδομένων των παροχών υπηρεσιών νεφοϋπολογιστικής (cloud computing), δηλαδή εταιριών που παρέχουν αποθήκευση δεδομένων εκτός ιστοχώρου (offsite). Πρόκειται για μελλοντικό κίνδυνο, καθώς η νεφοϋπολογιστική γίνεται όλο και περισσότερο διαδεδομένη.

Οι κυβερνό-βανδαλισμοί προκαλούν βλάβες χωρίς οικονομικό όφελος, που μπορεί να είναι η διαγραφή αρχείων, η μετονομασία δεδομένων ή διαγραφή αυτών.

2.3. Στόχοι επιθέσεων κυβερνοχώρου

Η ιδιωτικότητα αποτελεί πλέον ένα κρίσιμο επιχειρηματικό θέμα για πολλές εταιρίες, ειδικά για αυτές που δραστηριοποιούνται σε τομείς επιβαρυμένους από πλήθος δεδομένων όπως η υγεία, η εκπαίδευση, η λιανική πώληση και οι χρηματοοικονομικές υπηρεσίες.

Ανάλογα με τα κίνητρα οι κυβερνό-εγληματίες βρίσκουν και τους στόχους-μέρη που θέλουν να δράσουν οι οποίοι μπορεί να είναι είτε δημόσιοι, είτε ιδιωτικοί οργανισμοί, είτε συγκεκριμένοι εργαζόμενοι ή στελέχη οργανισμών.

2.3.1 Αναλυτική παράθεση

Σε δημόσιους οργανισμούς σε πιο μικρές χώρες όπως είναι η Ελλάδα, είναι πιο εύκολη η πρόσβαση, καθώς τα πληροφοριακά συστήματα κατά βάση είναι πεπαλαιωμένα, με σχεδόν ανύπαρκτα μέσα προστασίας και με μη καλά επανδρωμένο και καταρτισμένο προσωπικό. Έτσι στα εθνικά δίκτυα υποδομών αυξάνεται ο κίνδυνος των παραβιάσεων. Οι εταιρίες κοινής ωφέλειας συλλέγουν μεγάλο όγκο δεδομένων των πολιτών, οικονομικών και μη.

Οι τηλεπικοινωνίες, τα μέσα κοινωνικής δικτύωσης και οι εταιρίες διαδικτυακών υπηρεσιών, είναι ένας κλάδος που προσελκύει επίδοξους κυβερνό-εγκληματίες, καθώς καθημερινά ανταλλάσσονται εκατομμύρια εταιρικές και προσωπικές πληροφορίες. Σε πολλές περιπτώσεις και οικονομικές. Λόγω του είδους αντιμετωπίζουν καινούργιους, εξελιγμένους ιούς οι οποίοι απειλούν τη λειτουργία τους, που σημαίνει και απώλεια εσόδων.

Εταιρίες λιανικής πώλησης προϊόντων και υπηρεσιών διαθέτουν πάρα πολλά προσωπικά στοιχεία και στοιχεία καρτών και λογαριασμών των πελατών τους, καθώς τα τελευταία χρόνια έχουν αυξηθεί οι ηλεκτρονικές πωλήσεις. Ακόμα οι ιστοσελίδες λιανικής πώλησης είναι ευάλωτες από τους hackers, με στόχο τα έσοδα από τις online πωλήσεις.

Επίσης επιχειρήσεις του κλάδου των ξενοδοχειακών – τουριστικών απειλούνται επειδή αποτελούν παγκόσμια βάση χρηματικών συναλλαγών, ακόμα το μεγαλύτερο μέρος των κρατήσεων και πληρωμών γίνεται διαδικτυακά. Εν τω μεταξύ οι επιχειρήσεις αυτές κινδυνεύουν όχι μόνο από οικονομικής απόψεως αλλά και ηθικής, καθώς έχουν καταγραφεί περιστατικά δημοσιοποίησης προσωπικών στιγμών, διασήμων αλλά και κοινών προσώπων. Κάτι τέτοιο βλάπτει τη φήμη των ξενοδοχείων αυτών, τη μείωση των πελατών και την απώλεια εσόδων.

Τέλος τα χρηματοπιστωτικά ιδρύματα γίνονται πολύ συχνά τόπος επιθέσεων. Λόγω της δραστηριότητας τους και του τεράστιου «φακελώματος» τα στοιχεία που μπορεί κανείς να αποσπάσει είναι τεράστια σε όγκο και υλικό. Ειδικά στις

μέρες μας που οι συναλλαγές γίνονται κατά κόρον μέσω χρωστικών – πιστωτικών καρτών, e-banking μέσω υπολογιστών, κινητών και tablets, ακόμα και με ένα τηλεφώνημα (phone banking).

2.3.2 Είδη δεδομένων

Σύνηθες στόχοι των επιθέσεων είναι η υποκλοπή προσωπικών και εταιρικών δεδομένων. Ειδικότερα, τα δεδομένα μπορεί να αφορούν οικονομικές καταστάσεις, κωδικούς πρόσβασης, τραπεζικούς λογαριασμούς, σχέδια προώθησης προϊόντων, σχέδια ανάπτυξης παροχών και υπηρεσιών, νέες συμφωνίες, νέα προϊόντα και υπηρεσίες, προσωπικά δεδομένα, περιουσιακά στοιχεία, αριθμούς καρτών, των εργαζομένων, των διοικητικών στελεχών και των πελατών.

2.4 Μέθοδοι επιθέσεων κυβερνοχώρου

Οι μέθοδοι που μπορεί να χρησιμοποιήσει ένας επίδοξος εισβολέας για την επίτευξη του στόχου του είναι η φυσική κλοπή ψηφιακού εξοπλισμού, όπως είναι ένα USB flash memory stick, η δημιουργία κακόβουλου λογισμικού-ιού, δημιουργώντας έτσι βλάβες σε μεμονωμένους υπολογιστές ή σε συστήματα πληροφοριών. Βέβαια υπάρχουν και οι περιπτώσεις όπου δημιουργούνται ακούσια σφάλματα λόγω αμέλειας ή ημιμάθειας, όπως οι παραλείψεις και τα σφάλματα των εργαζομένων, είτε λόγω μη σωστής απόδοσης, συντήρησης και λειτουργίας των πληροφοριακών συστημάτων. Τέλος υπάρχει η περίπτωση δημιουργίας προβλημάτων από μη αναμενόμενες φυσικές καταστροφές.

2.5 Περιουσιακά στοιχεία

Τα περιουσιακά στοιχεία του οργανισμού αποτελούνται από τις υποδομές των πληροφοριακών συστημάτων, δηλαδή τα υλικά (υπολογιστές, SSD, smartphones,tablets), τις πληροφορίες και τα άυλα περιουσιακά στοιχεία που περιλαμβάνονται σε αυτά και η παρουσία του οργανισμού στο διαδίκτυο μέσω των ιστοσελίδων τους. Και τα τρία αυτά μέρη είναι εξίσου σημαντικά, αλληλένδετα και απαραίτητα για τη σωστή και ομαλή λειτουργία του οργανισμού.

2.6 Επιπτώσεις κινδύνων κυβερνοχώρου

Η παραβίαση συστημάτων λόγου κυβερνό-επιθέσεων, δημιουργεί άμεσες και έμμεσες χρηματοοικονομικές και όχι μόνο επιπτώσεις. Οι παραβιάσεις συστημάτων και η διαρροή εμπιστευτικών πληροφοριών είναι ένα από τα τρία κορυφαία περιστατικά που μπορούν να επηρεάσουν τη φήμη της εταιρίας και σε συνδυασμό με την κακή εξυπηρέτηση πελατών και πολιτικής προστασίας να οδηγήσουν σε απώλεια πελατών.

Οι νομικές αγωγές που μπορεί να ακολουθήσουν, βάζουν την επιχείρηση σε έξτρα διαδικασίες και κόστη, όπως επίσης και οι λειτουργικές επιπτώσεις με την καταστροφή ή τροποποίηση πληροφοριών, διαταραχή από τη διακοπή των πληροφοριακών συστημάτων και η διακοπή των εργασιών φέρουν προσωρινές ή ολικές καταστροφές.

2.7 Τρόποι προστασίας των εταιριών

Οι πλέον κατάλληλοι τρόποι για να προστατευθούν οι εταιρίες κατά το μέγιστο δυνατό από το κυβερνο-έγλημα είναι να εξασφαλίσουν:

1. Το προσωπικό τους εκπαιδεύεται και αναγνωρίζει τα σημάδια της πειρατείας και λαμβάνει ενημέρωση για τους σχετικούς κινδύνους.
2. Έχει δημιουργηθεί μια κουλτούρα στην οποία οι εργαζόμενοι αισθάνονται αρκετά βέβαιοι και έχουν την άνεση να αναφέρουν προειδοποιητικά σημάδια ή συμβάντα.
3. Έχουν καθοριστεί και καταγραφεί τα βασικά δεδομένα των εταιριών και έχουν ληφθεί τα κατάλληλα μέτρα προστασίας τους (τόσο στα πληροφοριακά συστήματα όσο και στις επιχειρησιακές διαδικασίες).
4. Υπάρχει παρακολούθηση των πληροφοριακών συστημάτων για την ανίχνευση σχετικών απειλών σε πρώτο στάδιο.
5. Να υπάρχει έτοιμη, σχεδιασμένη δράση- απάντηση.
6. Να υπάρχει συνεργασία μεταξύ των τμημάτων για την καταπολέμηση των απειλών
7. Η κυβερνοασφάλεια (cyber insurance) είναι μια μορφή διαχείρισης απαραίτητη για κάθε οντότητα.

2.7.1 Νομοθετική αντιμετώπιση του ηλεκτρονικού εγκλήματος σε Αλλοδαπές έννομες τάξεις

Η.Π.Α.

Σε πολιτειακό επίπεδο, η Πολιτεία της Florida εξέδωσε πρώτη το 1978 νομοθέτημα με εγκλήματα σχετιζόμενα με υπολογιστές. Σε ομοσπονδιακό επίπεδο, το πρώτο νομοθετικό έργο για το ηλεκτρονικό έγκλημα ήταν ο νόμος " Computer Fraud and Abuse Act" (CFAA) που εκδόθηκε το 1984. Τροποποιήσεις δέχτηκε από τότε το 1989, 1944, 1996 και το 2001 από το νόμο USA PATRIOT Act, το 2002, και το 2008 από το νομοθέτημα Identity Theft Enforcement and Restitution Act. Οι μόνοι υπολογιστές, στη θεωρεία, που καλύπτονται από το νόμο αυτό είναι οι «προστατευόμενοι υπολογιστές». Ορίζονται σύμφωνα με το άρθρο 18 U.S.C. 1.030 (e), (2) ότι προστατευόμενος υπολογιστής είναι ο υπολογιστής αποκλειστικά για τη χρήση ενός χρηματοπιστωτικού ιδρύματος ή της κυβέρνησης των Ηνωμένων Πολιτειών, ή οποιονδήποτε υπολογιστή, όταν η συμπεριφορά που συνιστά το αδίκημα επηρεάζει τη χρήση του υπολογιστή, είτε για το χρηματοπιστωτικό ίδρυμα ή την κυβέρνηση, είτε επηρεάζουν το διαπολιτειακό ή εξωτερικό εμπόριο ή την επικοινωνία, συμπεριλαμβανομένου ενός υπολογιστή που βρίσκεται εκτός των Ηνωμένων Πολιτειών, που χρησιμοποιείται κατά τρόπο που επηρεάζει το διαπολιτειακό ή εξωτερικό εμπόριο ή την επικοινωνία των Ηνωμένων Πολιτειών. Στην πράξη οποιοσδήποτε συνηθισμένος υπολογιστής υπόκειται στη δικαιοδοσία του νόμου.

Αυστραλία

Όπως αναφέρουν οι Αυστραλοί Smith, Grabosky και Urbas, το έγκλημα στον κυβερνοχώρο το οποίο τυποποιείται στο αυστραλιανό δίκαιο στο "The Cyber Crime Act 2001" (Cth), τέθηκε σε ισχύ την 1η Οκτωβρίου 2001, με σκοπό να εκσυγχρονίσει την αντιμετώπιση των ηλεκτρονικών εγκλημάτων από την Κοινοπολιτεία, που στο παρελθόν σε μεγάλο βαθμό περιλαμβάνονταν τα εγκλήματα αυτά στο νομοθέτημα "Crime Act 1914" και να παρέχει ένα μοντέλο για τα κράτη να υιοθετήσουν. Ο νόμος "The Cyber Crime Act 2001" καλύπτει επιπρόσθετες παράνομες πράξεις όπως η μη εξουσιοδοτημένη πρόσβαση στον υπολογιστή, η τροποποίηση δεδομένων και η δυσλειτουργία των ηλεκτρονικών επικοινωνιών. Αξιοσημείωτη προσθήκη αποτελεί το γεγονός ότι καλύπτεται και η χρήση του διαδικτύου για τη διάπραξη των εν λόγω αδικημάτων.

Ηνωμένο Βασίλειο

Το βασικό νομοθέτημα του Ηνωμένου Βασιλείου για το ηλεκτρονικό έγκλημα, το οποίο εκδόθηκε το 1990 και ισχύει μέχρι και σήμερα, μετά από τροποποιήσεις, είναι ο νόμος "Computer Misuse Act 1990". Το εν λόγω νομοθέτημα βρίσκεται σε ισχύ στην Αγγλία, στην Ουαλία, την Σκοτία και τη Βόρειο Ιρλανδία. Περιλαμβάνει τρεις βασικές κατηγορίες αδικημάτων κατάχρησης ηλεκτρονικών υπολογιστών όπως αναφέρεται. Αναλυτικότερα, τυποποιείται η μη εξουσιοδοτημένη πρόσβαση στο υλικό του υπολογιστή, η μη εξουσιοδοτημένη πρόσβαση με την πρόθεση να διαπραχθεί ή να διευκολυνθεί η διάπραξη νέων αδικημάτων και τέλος ή μη εξουσιοδοτημένη τροποποίηση του υλικού του ηλεκτρονικού υπολογιστή.

Η Ευρωπαϊκή Ένωση έχει αναλάβει διάφορες νομοθετικές δράσεις που συμβάλλουν στην καταπολέμηση του εγκλήματος στον κυβερνοχώρο. Όπως αναφέρει η Ευρωπαϊκή Επιτροπή, η νομοθετική αντιμετώπιση του εγκλήματος στον κυβερνοχώρο περιλαμβάνει τις Οδηγίες 2013/40/ΕΕ, 2011/93/ΕΕ, 2009/136/ΕΚ και την απόφαση-πλαίσιο 2001/413/ΔΕΥ. Επιπλέον αξίζει να αναφερθεί η πρόσφατη εισαγωγή στον τομέα της προστασίας προσωπικών δεδομένων, του Κανονισμού (ΕΕ) 2016/679 και Οδηγίας 2016/680/ΕΕ.

2.8 Περιστατικά Παραβιάσεων

2.8.1 Γεγονότα και στατιστικά

Ο κλάδος της ασφάλειας στον κυβερνοχώρο αναπτύσσεται ραγδαία καθημερινά. Καθώς περισσότεροι ειδικοί εντάσσονται στις τάσεις, ξεκινάει περισσότερο κακόβουλο λογισμικό από ποτέ, περίπου 230.000 νέα δείγματα malware/ημέρα. Είναι σημαντικό να καθορίσουμε ποια είναι η τρέχουσα βιομηχανία ασφάλειας πληροφοριών και ασφάλειας στον κυβερνοχώρο.

1. Το 95% των διαγραφέντων εγγράφων προήλθαν από τρεις μόνο βιομηχανίες το 2016. Το Δημόσιο, το λιανικό εμπόριο και την τεχνολογία. Ο λόγος δεν οφείλεται απαραίτητα στο γεγονός ότι αυτοί οι κλάδοι είναι λιγότερο επιμελής όσον αναφορά την προστασία των αρχείων πελατών. Είναι απλώς πολύ δημοφιλείς στόχοι λόγω υψηλού επιπέδου προσωπικής ταυτοποίησης των πληροφοριών που περιέχονται στα αρχεία τους.

2. Υπάρχει μια επίθεση χάκερ κάθε 39 δευτερόλεπτα. Μια μελέτη του Clark School στο Πανεπιστήμιο του Maryland είναι μία από τις πρώτες που ποσοτικοποιεί το σχεδόν σταθερό ποσοστό επιθέσεων χακερ υπολογιστών με πρόσβαση στο Διαδίκτυο και τα μη ασφαλή ονόματα χρηστών και κωδικούς

πρόσβασης που χρησιμοποιούμε που δίνουν στους επιτιθέμενους περισσότερες πιθανότητες επιτυχίας.

3. Το 43% των επιθέσεων στον κυβερνοχώρο απευθύνονται σε μικρές επιχειρήσεις. Το 64% των εταιριών έχουν βιώσει επιθέσεις στο διαδίκτυο. Το 62% αντιμετώπισε επιθέσεις phishing & κοινωνικής μηχανής. Το 59% των εταιριών παρουσίασε κακόβουλο κώδικα και botnets και το 51% αντιμετώπισε επιθέσεις άρνησης παροχής υπηρεσιών σύμφωνα με τη cybint το Δεκέμβριο του 2018.

4. Το μέσο κόστος παραβίασης των δεδομένων το 2020 θα υπερβεί τα 150 εκατομμύρια δολάρια, καθώς συνδέονται περισσότερες επιχειρηματικές υποδομές, τα στοιχεία της Juniper Research υποδηλώνουν ότι το οικονομικό έγκλημα στον κυβερνοχώρο θα κοστίσει στις επιχειρήσεις άνω των 2 τρισεκατομμυρίων μέχρι το τέλος του 2019.

5. Από το 2013 υπάρχουν 3.809.448 αρχεία που έχουν κλαπεί από παραβιάσεις κάθε μέρα. 158.727 ανά ώρα και 2.645 ανά λεπτό και 44 κάθε δευτερόλεπτο κάθε μέρα όπως αναφέρει η Cybersecurity Ventures.

6. Περισσότερες από τις μισές ευρωπαϊκές επιχειρήσεις που συμμετείχαν στην έρευνα του Kaspersky Lab (η μελέτη κυκλοφόρησε τον Μάρτιο του 2019) δήλωσαν ότι δέχτηκαν κυβερνοεπιθέσεις τα δύο προηγούμενα χρόνια.

7. Μέχρι το 2020 θα υπάρχουν περίπου 200 δισεκατομμύρια συνδεδεμένες συσκευές, ο κίνδυνος είναι πραγματικός με την IoT και την ανάπτυξή της. Σύμφωνα με στοιχεία που καταρτίστηκαν σε πρόσφατη έκθεση της Symantec Internet Security Threat, υπάρχουν 25 συνδεδεμένες συσκευές ανά 100 κατοίκους στις ΗΠΑ.

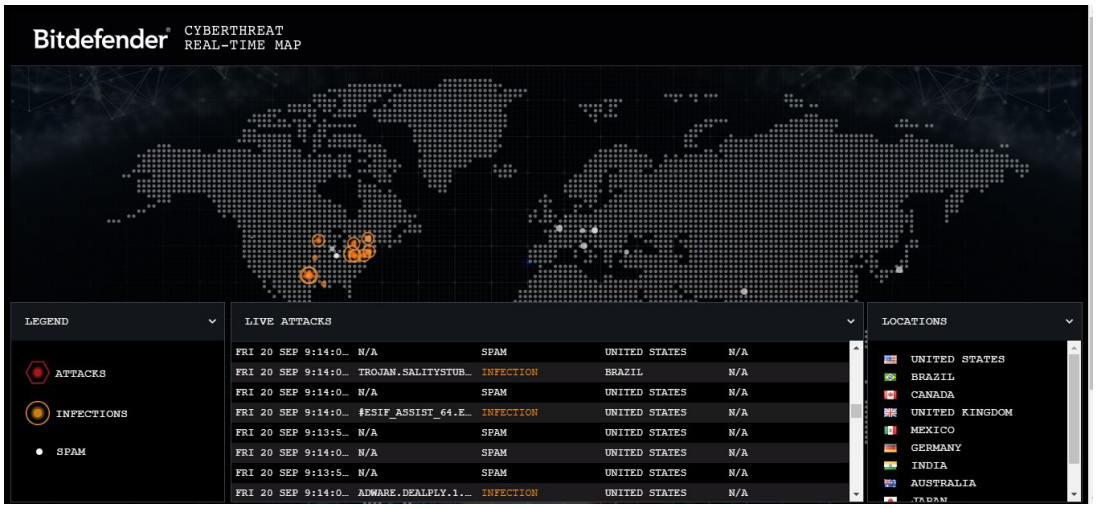
8. Το 95% των παραβιάσεων στον κυβερνοχώρο οφείλεται σε ανθρώπινο σφάλμα, καθώς οι χάκερ διεισδύουν στις εταιρίες μέσω του πιο αδύναμου συνδέσμου, ο οποίος δεν βρίσκεται σχεδόν ποτέ στο τμήμα πληροφορικής

9. Η απώλεια πληροφοριών πελατών (π.χ. ιατρικά αρχεία, οικονομικά αρχεία ή άλλες ιδιαίτερα εμπιστευτικές προσωπικές πληροφορίες) είναι ένα από τα άμεσα κόστη μιας επίθεσης στον κυβερνοχώρο. Σύμφωνα με έκθεση της IBM, το μέσο συνολικό κόστος μιας παραβίασης δεδομένων σε οργανισμό αγγίζει τα 3,92 εκατομμύρια δολάρια ενώ το μέσο κόστος ανά απώλεια ή κλοπή δεδομένων κυμαίνεται στα 150,8 δολάρια.

2.8.2 Περιστατικά σε πραγματικό χρόνο

Οι εταιρίες ασφαλείας όπως η Bitdefender και η SonicWall έχουν οπτικοποιήσει όλες τις κυβερνοεπιθέσεις μέσω διαδραστικών χαρτών. Με αυτόν τον τρόπο οι κυβερνοεπιθέσεις εμφανίζονται σε πραγματικό χρόνο.

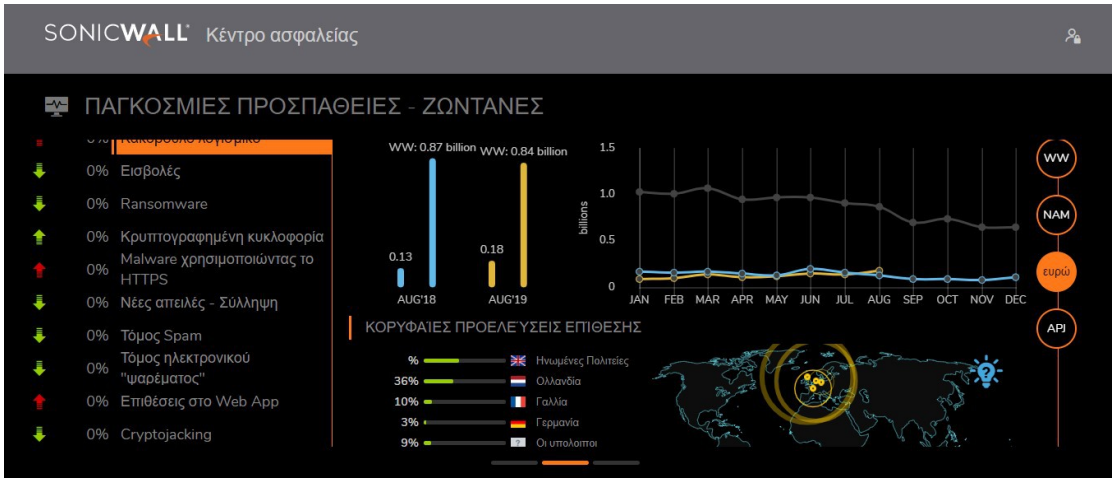
Η παρακάτω εικόνες δείχνουν τις κυβερνοεπιθέσεις που εξελίσσονται στον Παγκόσμιο χάρτη στις 20/09/2019 και ώρα 9:14 μ.μ.



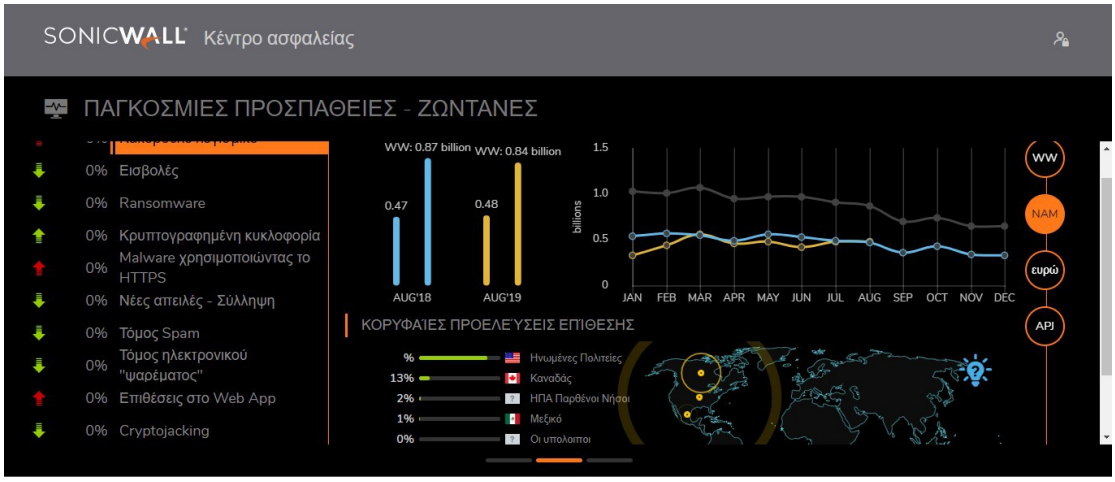
Εικόνα 2.1 Κυβερνοεπιθέσεις Παγκόσμια, **Πηγη: https://threatmap.bitdefender.com/**

Οι παρακάτω εικόνες δείχνουν τις ζωντανές προσπάθειες επίθεσης σε παγκόσμιο χάρτη, αλλά και μεμονωμένα σε Ευρώπη, Αμερική και Ασία, ενώ ταυτόχρονα απεικονίζει και τα συγκριτικά στοιχεία Αυγούστου 2018-Αυγούστου 2019.

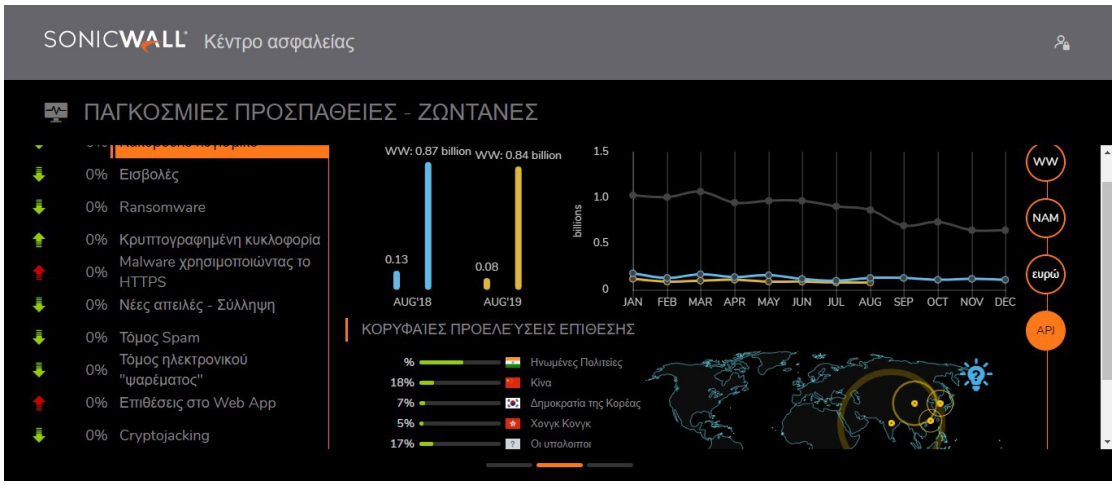
Εικόνα 2.2 Παγκόσμιος χάρτης, **Πηγή: https://securitycenter.sonicwall.com**



Εικόνα 2.3 Ευρώπη, **Πηγή: https://securitycenter.sonicwall.com**



Εικόνα 2.4 Αμερική, **Πηγή: https://securitycenter.sonicwall.com**



Εικόνα 2.5 Ασία, **Πηγή: https://securitycenter.sonicwall.com**

Η Αρχή Προστασίας Δεδομένων του Ηνωμένου Βασιλείου (ICO) ανακοίνωσε την πρόθεση της να επιβάλλει πρόστιμο ύψους 183 εκατομμύρια λιρών στην British Airways για το περιστατικό παραβίασης δεδομένων στον κυβερνοχώρο που αντμετώπθσε το 2018. Τον ίδιο μήνα η βρετανική υπηρεσία ελέγχου δεδομένων ανακοίνωσε την πρόθεση να επιβάλλει πρόστιμο 99,2 εκατομμυρίων λιρών στην Marriot International μετά από παραβίαση δεδομένων το προηγούμενο έτος, γεγονός που οδήγησε στην έκθεση προσωπικών στοιχείων περίπου 339 εκατομμυρίων πελατών.

ΚΕΦΑΛΑΙΟ 3

ΚΑΝΟΝΙΣΜΟΣ – ΘΕΣΜΙΚΟ ΠΛΑΙΣΙΟ

3.1 Γενικά

Δεδομένου των κινδύνων κυβερνοχώρου και του φόβου που επικρατεί, ο οποίος λειτουργεί ως ανασταλτικός παράγοντας για τη μέγιστη χρήση των δυνατοτήτων του διαδικτύου από πολίτες και επιχειρήσεις, θεσπίστηκαν κανόνες ασφαλείας και ορθής χρήσης των προσωπικών δεδομένων, ώστε να αποφευχθεί κάθε πιθανή κακόβουλη ενέργεια, επιβάλλοντας τις ανάλογες κυρώσεις.

Εγκρίθηκε από το κοινοβούλιο της Ευρωπαϊκής Ένωσης στις 14 Απριλίου 2016, ο Γενικός Κανονισμός για την Προστασία των Δεδομένων (General Data Protection Regulation GDPR) 2016/679,και τέθηκε σε ισχύ από τις 25 Μαΐου 2018. Ο κανονισμός είναι γενικής εφαρμογής, υποχρεωτικός σε όλα τα στοιχεία του και άμεσα εφαρμοσμένος σε όλα τα κράτη- μέλη της ΕΕ. Εξαλείφοντας την ανάγκη κατάρτισης τοπικών νομοθετικών πράξεων. Το GDPR εφαρμόζεται επίσης και σε οντότητες που είναι εγκατεστημένες εκτός ΕΕ εάν προσφέρουν αγαθά ή υπηρεσίες σε οργανισμούς ή άτομα της ΕΕ.

Ο κανονισμός αυτός περιγράφει τα δικαιώματα κάθε φυσικού προσώπου και την προστασία αυτού, έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα, καθώς και τις βασικές υποχρεώσεις των οργάνων που επεξεργάζονται τα στοιχεία αυτά.

Επειδή οι κυρώσεις που προβλέπει ο νέος κανονισμός είναι εξαιρετικά υψηλές, η μη συμμόρφωση στις νέες ρυθμίσεις εγκυμονεί τον κίνδυνο της οικονομικής καταστροφής του οργανισμού/ επιχείρησης.

Αναγκαία και επιτακτική κρίνεται η συμμόρφωση των οργανισμών αυτών με οδηγίες που δίνονται μέσω ενημερωτικών φυλλαδίων και της επίσημης ιστοσελίδας (www.dpa.gr), αλλά και η ασφάλιση των εταιριών (cyber insurance), εάν θέλουν να προστατευθούν και να διαχειριστούν αποτελεσματικά από τους παρόντες πλέον κινδύνους κυβερνοχώρου.

3.2 Δεδομένα - Ορισμός

Σύμφωνα με τον κανονισμό της ΕΕ 2016/679 (Άρθρο 4 παρ 1) της επίσημης εφημερίδας της Ευρωπαϊκής Ένωσης, για τους σκοπούς του κανονισμού νοούνται ως:

«δεδομένα προσωπικού χαρακτήρα»: κάθε πληροφορία που αφορά ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο («υποκείμενο των δεδομένων»)· το ταυτοποιήσιμο φυσικό πρόσωπο είναι εκείνο του οποίου η ταυτότητα μπορεί να εξακριβωθεί, άμεσα ή έμμεσα, ιδίως μέσω αναφοράς σε αναγνωριστικό στοιχείο ταυτότητας, όπως όνομα, σε αριθμό ταυτότητας, σε δεδομένα θέσης, σε επιγραμμικό αναγνωριστικό ταυτότητας ή σε έναν ή περισσότερους παράγοντες που προσιδιάζουν στη σωματική, φυσιολογική, γενετική, ψυχολογική, οικονομική, πολιτιστική ή κοινωνική ταυτότητα του εν λόγω φυσικού προσώπου».

3.3 Κατηγοριοποίηση δεδομένων προσωπικού χαρακτήρα

Ένα από τα βασικά ζητήματα για έναν οργανισμό, είναι να κατηγοριοποιήσει τα δεδομένα προσωπικού χαρακτήρα σε ευαίσθητα και μη. Παρατίθενται τα δεδομένα όπως έχουν εκδοθεί και χαρακτηριστεί από την Αρχή Προστασίας Δεδομένων Προσωπικού χαρακτήρα.

Πίνακας 1: Μη ευαίσθητα προσωπικά δεδομένα

ΟΜΑΔΑ Α: ΠΡΟΣΩΠΙΚΑ ΜΗ ΕΥΑΙΣΘΗΤΑ ΔΕΔΟΜΕΝΑ	
Α1. Στοιχεία αναγνώρισης	Α1.0 Προσωπικά στοιχεία
	Α1.1 Επίσημα στοιχεία Ληξιαρχείου
	Α1.2 Καταγωγή
	Α1.3 Στοιχεία Ταυτότητας (π.χ. Υπηκοότητα)
Α2. Προσωπικά χαρακτηριστικά	Α2.0 Φυσικά χαρακτηριστικά
	Α2.1 Ενδιαφέροντα, συνήθειες
	Α2.2 Μετακινήσεις – ταξίδια
	Α2.3 Στοιχεία προσωπικότητας
	Α2.4 Λοιπά στοιχεία προσωπικού χαρακτήρα

	Α3.0 Έγγαμος Βίος
Α3. Οικογενειακές συνθήκες	Α3.1 Οικογενειακή κατάσταση
	Α3.2 Κοινωνικές επαφές
	Α3.3 Λοιπά στοιχεία οικογενειακών συνθηκών
	Α4.0 Δεδομένα Ακαδημαϊκής δραστηριότητας
Α4. Εκπαίδευση	Α4.1 Τομείς ειδίκευσης & πιστοποιητικά
	Α4.2 Σπουδαστικό/ μαθητικό αρχείο
	Α4.3 Έγγραφές σε επιτροπές
	Α4.4 Επαγγελματική ειδίκευση
	Α4.5 Λοιπά στοιχεία

	Α5.0 Έσοδα, περιουσιακά στοιχεία, επενδύσεις
Α5. Οικονομική κατάσταση	Α5.1 Απολογισμός εσόδων
	Α5.2 Δάνεια, υποθήκες, πιστώσεις
	Α5.3 Επιδόματα, εργασιακά προνόμια
	Α5.4 Δεδομένα ασφάλισης, σύνταξη γήρατος
	Α5.5 Αγαθά & υπηρεσίες που προσφέρονται
	Α5.6 Αγαθά & υπηρεσίες που προσφέρει
	Α5.7 Τραπεζικοί λογαριασμοί, κάρτες
	Α5.8 Κληρονομιά
	Α5.9 Αποζημίωση
	Α5.10 Λοιπά στοιχεία οικονομικής κατάστασης

	Α6.0 Παρούσα εργασία
Α6. Εργασία	Α6.1 Δεδομένα πρόσληψης

	Α6.2 Ιστορικό εργασίας
	Α6.3 Εργασιακή συμπεριφορά
	Α6.4 Περιγραφή εργασίας
	Α6.5 Αξιολόγηση εργασίας
	Α6.6 Εκπαιδευτικό αρχείο
	Α6.7 Δεδομένα ασφαλείας
	Α6.8 Αμοιβές & κρατήσεις
	Α6.9 Εργασιακές παροχές
	Α6.10 Λοιπά στοιχεία εργασίας
	Α7.0 Δεδομένα θέσης
Α7. Δεδομένα ηλεκτρονικών πληρ	Α7.1 Δεδομένα κίνησης

Πηγή:Αρχή Προστασίας Δεδομένων Προσωπικού χαρακτήρα.

Πίνακας 2: Ευαίσθητα προσωπικά δεδομένα

ΟΜΑΔΑ Β: ΠΡΟΣΩΠΙΚΑ ΕΥΑΙΣΘΗΤΑ ΔΕΔΟΜΕΝΑ	
	Β1.0 Εθνική Καταγωγή
Β1. Φυλετική ή Εθνική προέλευση	Β1.1 Μειονότητες
	Β1.2 Φυλετική προέλευση
Β2. Πολιτικά Φρονήματα	Β2.0 Δεδομένα πολιτικών πεποιθήσεων
Β3.Θρησκευτικές πεποιθήσεις	Β.3.0 Δεδομένα θρησκευτικής πίστης
Β4.Φιλοσοφικές πεποιθήσεις	Β4.0 Δεδομένα φιλοσοφικών πεποιθήσεων
Β.5 Συνδικαλιστική δράση	Β5.0 Συνδικαλιστική δραστηριότητα

B6. Υγεία	B6.0 Φυσική κατάσταση B6.1 Πνευματική κατάσταση B6.2 Ανικανότητες & αναπηρίες B6.3 Διαιτητικές και άλλες σχετικές ανάγκες B6.4 Ιατρικό ιστορικό ασθενούς B6.5 Χορήγηση φαρμάκων B6.6 Λοιπά στοιχεία υγείας
B7. Κοινωνική πρόνοια	B7.0 Ασφάλιση B7.1 Σύνταξη
B8. Ερωτική ζωή	B8.0 Σεξουαλική ζωή
B9. Ποινικές διώξεις	B9.0 Καταγγελίες B9.1 Διώξεις B9.2 Διοικητικά μέτρα B9.3 Διοικητικές ποινές
B10. Καταδίκες	B10.0 Αποφάσεις δικαστηρίων B10.1 Ποινικό Μητρώο

Πηγή:Αρχή Προστασίας Δεδομένων Προσωπικού χαρακτήρα.

3.4 Βασικά Δικαιώματα Πολιτών

Ο κανονισμός έχει συνταχθεί άρτια, έτσι ώστε το κάθε φυσικό πρόσωπο – πολίτης μπορεί να διεκδικήσει τα δικαιώματα του. Με μία απλή αναζήτηση στο διαδίκτυο,

μπορεί να ενημερωθεί μέσω του φυλλαδίου που κυκλοφορεί, το οποίο είναι σύντομο και περιεκτικό, ή να κατεβάσει ολόκληρο το νόμο.

Τα βασικά δικαιώματα των πολιτών είναι το Δικαίωμα ενημέρωσης και πρόσβασης στα δεδομένα (Άρθρο 15 κ. 2016/679), το Δικαίωμα διόρθωσης (Άρθρο 16), το Δικαίωμα διαγραφής «δικαίωμα στη λήθη» (Άρθρο 17), το Δικαίωμα στον περιορισμό της επεξεργασίας (Άρθρο 18), Το Δικαίωμα στη φορητότητα των δεδομένων (Άρθρο 20) και το Δικαίωμα της εναντίωσης (Άρθρο 21).

3.5 Υπεύθυνοι επεξεργασίας δεδομένων

Ο νέος κανονισμός θεσπίζει επίσης, την υποχρέωση των υπεύθυνων επεξεργασίας των δεδομένων να παρέχουν διαφανείς και εύκολα προσβάσιμες πληροφορίες στα υποκείμενα όσον αφορά την επεξεργασία των δεδομένων τους. Επιπλέον ορίζει αναλυτικά τις γενικές υποχρεώσεις που έχουν οι υπεύθυνοι επεξεργασίας και εκτελούντες την επεξεργασία των δεδομένων προσωπικού χαρακτήρα για λογαριασμό αυτών. Και οι δύο, έχουν την υποχρέωση τήρησης κατάλληλων μέτρων ασφαλείας ανάλογα με τον κίνδυνο τον οποίο ενέχουν οι πράξεις επεξεργασίας δεδομένων τις οποίες εκτελούν.

Οι υπεύθυνοι επεξεργασίας σε ορισμένες περιπτώσεις, πρέπει να κοινοποιούν τα περιστατικά παραβίασης δεδομένων προσωπικού χαρακτήρα εντός 72 ωρών από την ανακάλυψη του περιστατικού παραβίασης και απώλειας προσωπικών δεδομένων στις αρμόδιες αρχές και στα υποκείμενα των δεδομένων αν η φύση των δεδομένων που χάθηκαν το απαιτεί. Επίσης, για τις εταιρίες και τις δημόσιες αρχές που εκτελούν πράξεις επεξεργασίας δεδομένων που ενέχουν και κινδύνους και το προσωπικό τους ξεπερνά τα 250 άτομα θα πρέπει να έχουν ορίσει υπεύθυνο προστασίας δεδομένων.

Για τους υπεύθυνους επεξεργασίας ή τους εκτελούντες την επεξεργασία δεδομένων οι οποίοι παραβιάζουν τους κανόνες για την προστασία των δεδομένων προβλέπονται πολύ αυστηρές κυρώσεις.

3.6 Κριτήρια επιβολής προστίμου

Βάσει του Άρθρου 83 παρ.2 κ 2016/679, οι γενικοί όροι για την επιβολή διοικητικού προστίμου, καθώς και σχετικά με το ύψος του διοικητικού προστίμου για κάθε μεμονωμένη περίπτωση, λαμβάνονται υπόψη ενδεικτικά τα ακόλουθα.

- Η φύση, η βαρύτητα και η διάρκεια της παραβίασης, λαμβάνοντας υπόψη τη φύση, την έκταση ή το σκοπό της σχετικής επεξεργασίας, καθώς και τον αριθμό

των υποκειμένων των δεδομένων που έθιξε η παραβίαση και το βαθμό ζημίας που υπέστησαν.

- Ο δόλος ή η αμέλεια που προκάλεσε την παραβίαση.
- Οποιεσδήποτε ενέργειες στις οποίες προέβη ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία για να μετριάσει τη ζημία που υπέστησαν τα υποκείμενα των δεδομένων.
- Ο βαθμός ευθύνης του υπευθύνου επεξεργασίας, λαμβάνοντας υπόψη τα τεχνικά και οργανωτικά μέτρα που εφαρμόζουν.
- Τυχόν σχετικές προηγούμενες παραβάσεις του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία.
- Ο βαθμός συνεργασίας με την αρχή ελέγχου για την επανόρθωση της παράβασης και τον περιορισμό των πιθανών δυσμενών επιπτώσεων της.
- Οι κατηγορίες δεδομένων προσωπικού χαρακτήρα που επηρεάζει η παραβίαση.
- Ο τρόπος με τον οποίο η εποπτική αρχή πληροφορήθηκε την παραβίαση, ειδικότερα αν και κατά πόσο υπεύθυνος ή ο εκτελών την επεξεργασία κοινοποίησε την παράβαση.
- Σε περίπτωση που διατάχθηκε προηγουμένως η λήψη των μέτρων που αναφέρονται κατά του εμπλεκομένου υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία σχετικά με το ίδιο αντικείμενο, η συμμόρφωση με τα εν λόγω μέτρα.
- Η τήρηση εγκεκριμένων κωδίκων δεοντολογίας ή εγκεκριμένων μηχανισμών πιστοποίησης.
- Κάθε άλλο επιβαρυντικό ή ελαφρυντικό στοιχείο που προκύπτει από τις περιστάσεις της συγκεκριμένης περίπτωσης, όπως τα οικονομικά οφέλη αποκομίστηκαν ή ζημιών που αποφεύχθηκαν, άμεσα ή έμμεσα, από την παράβαση.

Κάθε εποπτική αρχή μεριμνά ώστε η επιβολή διοικητικών προστίμων σύμφωνα με το παρών άρθρο έναντι παραβάσεων του παρόντος κανονισμού που αναφέρονται στις παραγράφους 4,5 και 6 να είναι για κάθε μεμονωμένη περίπτωση αποτελεσματική, ανάλογη και αποτρεπτική. (Άρθρο 83, παρ.1)

Αξίζει να σημειωθεί η παράγραφος 5, όπου επισύρουν διοικητικά πρόστιμα έως 20 εκατ. € ή σε περίπτωση επιχειρήσεων, έως το 4% του συνολικού παγκόσμιου ετήσιου κύκλου εργασιών του προηγούμενου οικονομικού έτους, ανάλογα με το πιο είναι υψηλότερο.

3.7 Κυρώσεις- Επιβολή διοικητικών προστίμων

Τα κράτη μέλη θεσπίζουν τους κανόνες σχετικά με τις άλλες κυρώσεις που επιβάλλονται για παραβιάσεις του παρόντος κανονισμού, ιδίως για τις παραβιάσεις που δεν αποτελούν αντικείμενο διοικητικών προστίμων δυνάμει του άρθρου 83, και λαμβάνουν όλα τα αναγκαία μέτρα για να διασφαλιστεί ότι εφαρμόζονται. Οι εν λόγω κυρώσεις είναι αποτελεσματικές, αναλογικές και αποτρεπτικές (Άρθρο 84 παρ.1

3.8 Στατιστικά στοιχεία μελετών

Σήμερα, μετά την εφαρμογή του GDPR, τα στατιστικά στοιχεία από διάφορες Ευρωπαϊκές χώρες δείχνουν ότι η πραγματικότητα δεν αφορά ένα απλό σύνολο νόμων και γενικών αρχών, αλλά την εφαρμογή τους σε πραγματικά περιστατικά παραβίασης προσωπικών δεδομένων, καταγγελίες και πρόστιμα από τις αρμόδιες Αρχές.

Μέχρι στιγμής έχουμε δει μερικά μεμονωμένα περιστατικά. Χαρακτηριστικό παράδειγμα αποτελεί περιστατικό παραβίασης που έλαβε χώρα τον περασμένο Οκτώβριο σε νοσοκομείο της Πορτογαλίας και στο οποίο επεβλήθη πρόστιμο 400.000 Ευρώ για δύο παραβιάσεις GDPR που σχετίζονται με τη μη εξουσιοδοτημένη πρόσβαση στα δεδομένα ασθενών. Εν τω μεταξύ, το Facebook ανακοίνωσε την ύπαρξη πιθανής παραβίασης στα δεδομένα 50 εκατομμυρίων χρηστών το Σεπτέμβριο της ίδιας χρονιάς.

Τα κατωτέρω διαγράμματα απεικονίζουν στατιστικές πληροφορίες που έχουν συλλεχθεί από τις Αρχές Προστασίας Δεδομένων Προσωπικού Χαρακτήρα από 8 Ευρωπαϊκές χώρες: Τη Γαλλία, τη Γερμανία, την Ιρλανδία, την Ιταλία, την Πολωνία, τη Ρουμανία, τη Σουηδία και το Ηνωμένο Βασίλειο.

Εικόνα 3.1 Συνολικός αριθμός καταγγελιών, **Πηγή: https://privacyadvocate.gr**

Ο μεγαλύτερος αριθμός καταγγελιών σημειώνεται στο Ηνωμένο Βασίλειο που αποδεικνύει ότι τα φυσικά πρόσωπα είναι γνώστες των δικαιωμάτων τους και έσπευσαν να λάβουν μέτρα.

Ο δεύτερος δείχνει το συνολικό αριθμό κοινοποιήσεων περιστατικών παραβίασης προσωπικών δεδομένων:

Εικόνα 3.2 Συνολικός αριθμός κοινοποιήσεων περιστατικών παραβίασης προσωπικών δεδομένων, **Πηγή: https://privacyadvocate.gr**

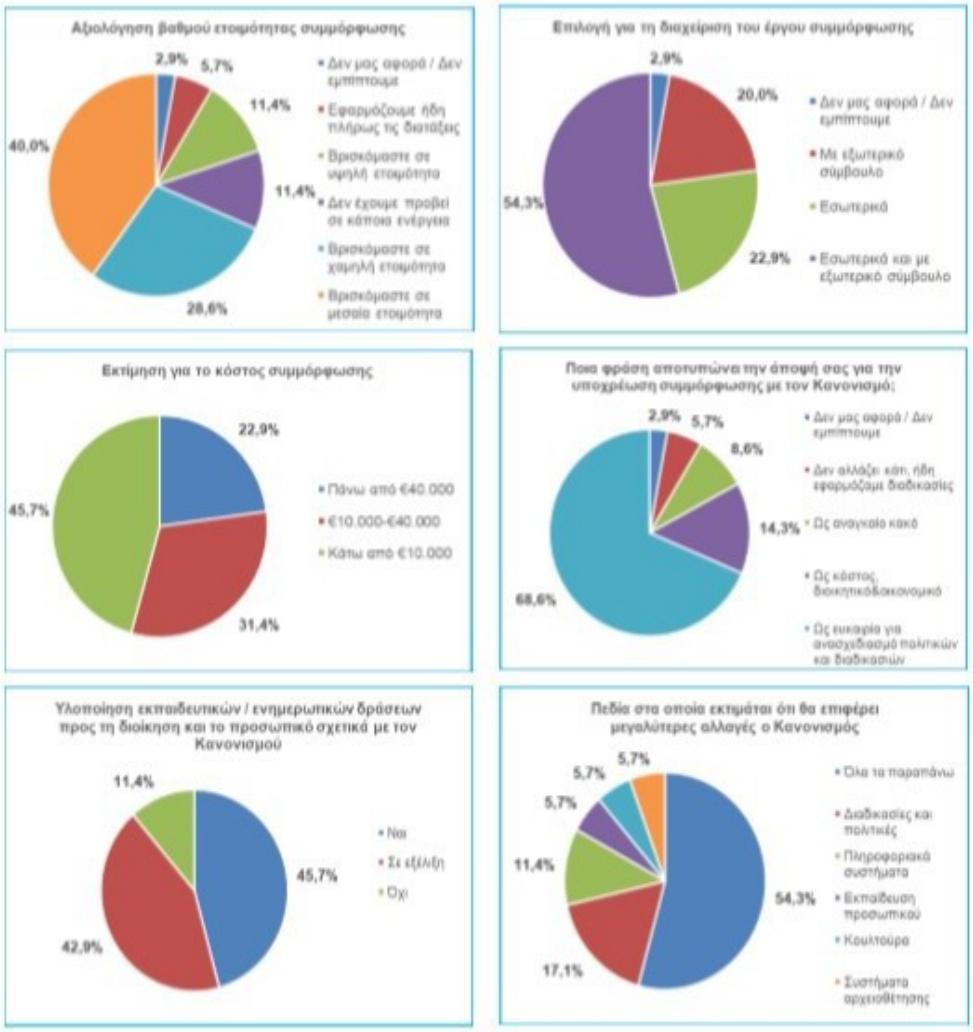
Ο συνολικός αριθμός κοινοποιήσεων παραβίασης δεδομένων υποδηλώνει ότι οι επιχειρήσεις και οι οργανισμοί αντιμετωπίζουν σοβαρά την υποχρέωση που επιβάλλει το άρθρο 33 του GDPR.

Ο τρίτος αναφέρει τον αριθμό κωδίκων δεοντολογίας:

Εικόνα 3.3 Υποβληθέντες κώδικες δεοντολογίας, **Πηγή: https://privacyadvocate.gr**

Η Γερμανία, η Πολωνία και η Ρουμανία είναι μέχρι στιγμής οι χώρες που έχουν υποβάλλει στις αρμόδιες Αρχές τα Σχέδια Κωδίκων Δεοντολογίας που έχουν καταρτιστεί.

Στην Ελλάδα, ο Σύνδεσμος επιχειρήσεων και Βιομηχανιών (ΣΕΒ) δημοσίευσε τον Οκτώβριο του 2018, έρευνα που πραγματοποιήθηκε σε δείγμα 35 επιχειρήσεων. Η διαδικασία συμμόρφωσης περιλαμβάνει πολλαπλές δράσεις σε διαφορετικά αντικείμενα και επίπεδα όπως σε: διαδικασίες και πολιτικές, πληροφοριακά συστήματα, εκπαίδευση προσωπικού εταιρική κουλτούρα και συστήματα αρχειοθέτησης.



Εικόνα 3.4 Συμμόρφωση επιχειρήσεων στον Κανονισμό και άλλα στοιχεία, **Πηγή:** ΣΕΒ

ΚΕΦΑΛΑΙΟ 4

ΔΙΑΧΕΙΡΙΣΗ ΔΙΑΔΙΚΤΥΑΚΟΥ ΚΙΝΔΥΝΟΥ

4.1 Τι είναι η διαχείριση ασφαλιστικού κινδύνου

Η διαχείριση κινδύνων αποτελεί πλέον σύγχρονη προσέγγιση για τη διασφάλιση της επιβίωσης μιας επιχείρησης ή δραστηριότητας.

Έχοντας πλέον εξελιχθεί από τις μεμονωμένες προσπάθειες <<πρόληψης ζημιών>> του (όχι πολύ μακρινού) παρελθόντος σε περίπλοκο φάσμα δραστηριοτήτων, οι οποίες αγκαλιάζουν και εμπλέκουν το σύνολο των δραστηριοτήτων, των εσωγενών και εξωγενών παραγόντων και των ενεργειών που προηγούνται, αλλά και έπονται από την επέλευση κάποιας κατάστασης, αποτελεί απαραίτητο εργαλείο, που επηρεάζει και αφορά άμεσα την εύρυθμη λειτουργία και αποδοτικότητα των επιχειρηματικών και επιχειρησιακών δραστηριοτήτων.

Θα πρέπει να σημειωθεί ότι ιστορικά υπάρχει μία άτυπη αναφορά σε εποχές διαχείρισης κινδύνων. Κατά την πρώτη/αρχική εποχή, η διαχείριση αφορούσε ουσιαστικά μόνο στους μη επιχειρηματικούς κινδύνους και η αντιμετώπιση ήταν κυρίως αμυντική, εστιαζόμενη σε παραδοσιακούς τρόπους μεταφοράς του κινδύνου.

Στη δεύτερη εποχή η προσέγγιση επεκτείνεται και σε άλλα επίπεδα, η πρόληψη αποκτά βαρύνουσα σημασία, η διαχείριση κινδύνων αρχίζει να λαμβάνει υπόψη στις εσωτερικές διαδικασίες της επιχείρησης. Εν μέρει αυτή η εξέλιξη οδηγείται και από τις ασφαλιστικές εταιρίες, οι οποίες ξεκινούν να απαιτούν χειροπιαστά και συγκεκριμένα βήματα πρόληψης των κινδύνων αλλά και από τις Αρχές (όπως πχ. Η <Ευρωπαϊκή Ένωση) οι οποίες αρχίζουν να θεωρούν τη Διαχείριση ως απαραίτητο στοιχείο του εκσυγχρονισμού της λειτουργίας των επιχειρήσεων.

Στην τρίτη εποχή, στην οποία ουσιαστικά βρίσκεται (ή πρέπει να βρίσκεται) η αγορά σήμερα, τα μέτρα ανάλυσης και πρόληψης λαμβάνουν πιο επιστημονικό και τεχνοκρατικό χαρακτήρα και η ανάλυση κινδύνων επεκτείνεται ώστε να αφορά και καθαρά επιχειρηματικούς κινδύνους. Ο παράγοντας <<κοινωνία>> έρχεται στο προσκήνιο και η διαφύλαξη της εταιρικής εικόνας της εταιρίας αποτελεί πρώτιστη προτεραιότητα. Πλέον, η ύπαρξη και ενσωμάτωση στη λειτουργία μιας επιχείρησης ενός αποτελεσματικού συστήματος διαχείρισης κινδύνων σε όλο το φάσμα των δραστηριοτήτων της επιχείρησης αποτελεί απαραίτητη προϋπόθεση και λαμβάνεται

σοβαρά υπόψη κατά την ανάλυση μιας επιχείρησης από διεθνείς χρηματοοικθονομικούς κύκλους και επενδυτές.

Το βασικό σκεπτικό της όλης προσέγγισης συνοψίζεται σε μερικά απλά ερωτήματα.

1. Τι θα μπορούσε να συμβεί;
2. Πόσο πιθανό είναι να συμβεί;
3. Πώς θα μπορούσαμε να το προβλέψουμε /αντιμετωπίσουμε;

Είναι δεδομένο ότι η απάντηση σε αυτά τα ερωτήματα είναι μια αρκετά εκτενή λίστα ενδεχομένων καταστάσεων. Είναι επίσης αυτονόητο ότι λόγω της δεδομένης έκτασης αυτής της λίστας και για να είναι πρακτική η αντιμετώπιση τους, θα πρέπει να τεθούν προτεραιότητες, να εξεταστούν όλες οι δυνατές επιλογές, να ληφθούν οι τελικές αποφάσεις με βάση επιχειρησιακά αλλά και χρηματοοικονομικά κριτήρια.

Πρωταρχικό για τη σωστή προσέγγιση του όλου θέματος είναι να υπάρχει σφαιρική επίγνωση (με την ευρεία έννοια του όρου) του κινδύνου. Οι φάσεις κατά χρονική σειρά, είναι:

1. Προσδιορισμός των κινδύνων
2. Καθορισμός προτεραιοτήτων
3. Μέτρα πρόληψης /ελαχιστοποίησης /αντιμετώπισης
4. Σχεδιασμός μέτρων διασφάλισης της επιχειρησιακής συνέχειας.

4.2 Πρακτικές εξασφάλισης ελέγχου ασφαλείας

Οι ειδικοί της Symantec δημιούργησαν μια πολύ περιεκτική λίστα επτά σημείων ελέγχου ασφαλείας στον κυβερνοχώρο που βασίζεται στις βέλτιστες πρακτικές όπως αυτές καταγράφηκαν στο πρόσφατο 2016 Internet Security Threat Report (ISTR), την ετήσια έκθεση της Symantec, η οποία παρέχει μια επισκόπηση και ανάλυση για την παγκόσμια δραστηριότητα στον τομέα των κυβερνοαπειλών.

Η παρακάτω λίστα ελέγχου έχει σκοπό να αποτελέσει έναν οδηγό για τους υπεύθυνους ασφαλείας και να βοηθήσει πριν, κατά τη διάρκεια, και μετά από μια επίθεση.

1-Επιβεβαίωση ότι όλες οι συσκευές που επιτρέπεται να είναι συνδεδεμένες σε εταιρικά δίκτυα διαθέτουν επαρκή μέτρα ασφαλείας. Κάνοντας χρήση την ενεργή παρακολούθηση και τη διαχείριση διαμόρφωσης για την διατήρηση μιας επικυρωμένης απογραφής όλων των συσκευών που είναι συνδεδεμένες με το δίκτυο

της επιχείρησης. Αυτό περιλαμβάνει serves, σταθμούς εργασίας, φορητούς υπολογιστές καθώς και απομακρυσμένες συσκευές.

2-Εφαρμογή πολιτικής αφαιρούμενου μέσου. Όπου αυτό είναι εφικτό, περιορίζοντας τις μη εξουσιοδοτημένες προς χρήση συσκευές , όπως για παράδειγμα τους εξωτερικούς φορητούς σκληρούς δίσκους αλλά και παρόμοια αφαιρούμενα μέσα. Τέτοιες συσκευές μπορεί να εισάγουν κακόβουλο λογισμικό και να διευκολύνουν τις παραβιάσεις της πνευματικής ιδιοκτησίας, είτε εκούσια είτε ακούσια. Περιορίζεται έτσι η αντιγραφή εμπιστευτικών δεδομένων σε μη κρυπτογραφημένες εξωτερικές συσκευές αποθήκευσης.

3-Συνεχή ενημέρωση & επιδιόρθωση. Οι διαδικασίες όπως update, patch και migrate από ξεπερασμένους και ανασφαλείς browser, εφαρμογές και browser plug-ins θα πρέπει να είναι μια πάγια διαδικασία που επιβάλλεται να επαναλαμβάνεται σε τακτικά χρονικά διαστήματα με ευλάβεια. Αυτό ισχύει και για τα λειτουργικά συστήματα, όχι μόνο σε όλους τους υπολογιστές αλλά και σε κινητά, ICS και συσκευές IoT.

4-Επιβολή αποτελεσματικής πολιτικής για τον κωδικό πρόσβασης. Με την επιβεβαίωση ότι όλοι οι κωδικοί πρόσβασης είναι ισχυροί και τουλάχιστον 8-10 χαρακτήρες με ένα μείγμα γραμμάτων και αριθμών, καθώς επίσης και η κοινή χρήση κωδικών πρόσβασης με άλλους θα πρέπει να απαγορεύεται.

5-Διασφάλιση με τακτική δημιουργία αντιγράφων ασφαλείας .Η δημιουργία και η διατήρηση σε τακτική βάση αντιγράφων ασφαλείας των κρίσιμων συστημάτων, καθώς και των endpoints. Σε περίπτωση έκτακτης ανάγκης ασφαλείας των δεδομένων, τα αντίγραφα ασφαλείας θα πρέπει να είναι εύκολα προσβάσιμα για την ελαχιστοποίηση της διακοπής λειτουργίας των υπηρεσιών και την παραγωγικότητα των εργαζομένων.

6-Περιορισμός στα συνημμένα του ηλεκτρονικού ταχυδρομείου. Οι mail servers πρέπει να διαμορφωθούν έτσι ώστε να μπλοκάρουν ή να απομακρύνουν μηνύματα που περιέχουν συνημμένα αρχεία που χρησιμοποιούνται συνήθως για τη διάδοση ιών, όπως .vbs, .bat, .exe, .pif και τα αρχεία .scr. Οι επιχειρήσεις θα πρέπει να διερευνούν πολιτικές για αρχεία PDF που επιτρέπεται να συμπεριληφθούν ως συνημμένα ηλεκτρονικού ταχυδρομείου. Θα πρέπει επίσης να βεβαιωθείτε ότι οι mail servers προστατεύονται επαρκώς από το λογισμικό ασφαλείας και ότι τα e-mail σαρώνονται επιμελώς.

7-Εφαρμογή διαδικασιών infection and incident response. Η χρήση των δυνατοτήτων ανίχνευσης μετά την μόλυνση από web πύλη, λύση endpoint security και firewalls για τον εντοπισμό μολυσμένων συστημάτων, η απομόνωση των μολυσμένων υπολογιστών για να αποφευχθεί ο κίνδυνος της περαιτέρω μόλυνσης στο εσωτερικό του οργανισμού, και η απαγόρευση πρόσβασης σε δικτυακές υπηρεσίες που έχουν

προσβληθεί από κακόβουλο κώδικα, μέχρι να γίνει εφαρμογή ενός patch, είναι μερικοί τρόποι αντιμετώπισης πιθανού κινδύνου.

4.2.1 Εκπαίδευση Προσωπικού

Για κάθε θέμα που αντιμετωπίζει η επιχείρηση όπως είναι οι παραβιάσεις των συστημάτων και οι απώλεια προσωπικών δεδομένων το ανθρώπινο κεφάλαιο αποτελεί ένα από τα βασικά στοιχεία της. Το ζήτημα της συμβολής συμβολής του ανθρώπινου στοιχείου στην ασφάλεια των δεδομένων είναι θεμελιώδης σημασίας.

Μια σωστή πολιτική για την προστασία των συστημάτων από τις ενέργειες κακόβουλες ή μη των εργαζομένων μιας επιχείρησης αποτελεί η εκπαίδευση ώστε να είναι κατάλληλα προετοιμασμένοι με τις απαιτητές γνώσεις για την αντιμετώπιση στις προκλήσεις των απειλών όπως για παράδειγμα η κοινωνική μηχανή.

Επίσης θα πρέπει να περιλαμβάνει και την ενημέρωση τους σχετικά με την επιχειρηματική στρατηγική αντιμετώπισης των κινδύνων του κυβερνοχώρου και τους στόχους της για την μείωση των επιπτώσεων που δημιουργούνται ώστε με αυτόν τον τρόπο η επιχείρηση να αυξήσει την ευαισθητοποίηση των εργαζομένων της για τα θέματα ασφαλείας. Έτσι επιτυγχάνεται η εναρμόνιση των εργαζομένων με την επιχειρησιακή κουλτούρα στα θέματα ασφαλείας- κινδύνων του κυβερνοχώρου.

4.2.2 Τεχνολογικά Μέσα

Ένα άλλο μέτρο στη διαχείριση του διαδικτυακού κινδύνου αποτελούν τα τεχνολογικά μέτρα, των οποίων η διάκριση γίνεται ως εξής:

- Έλεγχος πρόσβασης, όπου διασφαλίζεται η πρόσβαση στο κέντρο δεδομένων, όπως επίσης η πρόσβαση σε βασικές πηγές, όπως server rooms, μέσα, δίσκοι, CD-ROMs θα πρέπει να ασφαλίζονται χρησιμοποιώντας κατάλληλα μέτρα, επίσης οι Οργανισμοί θα πρέπει να μοντελοποιούν τις απαιτήσεις ελέγχου πρόσβασης στη γενική ευπάθεια των δεδομένων και των εφαρμογών.

- Ανίχνευση εισβολών, σε προσπάθεια εισβολής, μέσω αισθητήρων κίνησης, επαφής και αισθητήρων σε όλα τα παραμετρικά σημεία πρόσβασης στο κέντρο δεδομένων, όπως επίσης και σε κρίσιμες περιοχές.

- Συνεχή παρακολούθηση (24χ7), Οποιαδήποτε υποδομή του κέντρου δεδομένων θα πρέπει να βασίζεται δε εικοσιτετράωρη παρακολούθηση μέσω

προσωπικού φύλαξης στα κέντρα ή ακόμα και απομακρυσμένη παρακολούθηση, σε υπάρχοντα συστήματα κινδύνου και ελέγχου πρόσβασης.

- Τοίχος προστασίας (Firewall), φραγμοί συνδέσεων σε εσωτερικές πηγές από πρωτόκολλο, θήρα και διεύθυνση
- IDS, ανιχνεύει ¨την υπογραφή¨ γνωστών επιθέσεων σε επίπεδο δικτύου, σε υψηλή διακίνηση κόμβου μέσα σε δίκτυα και στην περίμετρο των δικτύων
- Antivirus, ανιχνεύει κακόβουλους κώδικες σε διαδικτυακούς κόμβους, όπως HTTP και SMTP.
- Ενδυνάμωση συστήματος, Διεργασίες, διαδικασίες και προϊόντα για την ενδυνάμωση των λειτουργικών συστημάτων και της εκμετάλλευσης των υπηρεσιών του διαδικτύου ή των ελέγχων του διακομιστή, πρέπει να πραγματοποιούνται για όλους τους βασικούς δίσκους και εσωτερικά συστήματα
- Πιστοποίηση, δηλαδή να επιτρέπεται ταυτοποίηση και διαχείριση των χρηστών του συστήματος μέσω ταυτοτήτων και κωδικών, για όλα τα βασικά συστήματα που μπορούν να χρησιμοποιηθούν σε πολλαπλές εφαρμογές, ώστε να παρέχεται η υπογραφή της επιχείρησης.
- Έλεγχος πρόσβασης, χάρτες χρηστών, ανά ταυτότητα ή ανά ρόλο, σε όλες τις βασικές εφαρμογές και
- Κρυπτογράφηση, όπου τα βασικά δεδομένα της επιχείρησης ή μη δημόσιες πληροφορίες πελατών, πρέπει να κρυπτογραφούνται (για παράδειγμα να επισκιάζονται όταν διαβιβάζονται από δημόσια δίκτυα), για όλες τις συναλλαγές συνδέσεων διαδικτύου. Επίσης, πρέπει να λαμβάνονται υπόψη για δεδομένα ασφαλείας με υψηλή ευαισθησία σε αποθήκευση.

4.2.3 ISO 31000:2009 και Αρχές του COBIT 5 GEIT

Ο Διεθνής Οργανισμός Τυποποίησης (ISO) αποτελεί σημείο αναφοράς, δεδομένου ότι τα πρότυπά του προτείνονται από πολλούς μεγάλους φορείς και εφαρμόζονται από σημαντικό πλήθος επιχειρήσεων ανά τον κόσμο. Στο πλαίσιο αυτό, ο οργανισμός διαχείρισης κινδύνων (RIMS) , προτρέπει την εφαρμογή του Διεθνούς Προτύπου Τυποποίησης 31000:2009 (το οποίο και αναθεωρήθηκε πρόσφατα το 2018), ως ένα ισχυρό και αποτελεσματικό εργαλείο για την αντιμετώπιση και διαχείριση των κινδύνων του κυβερνοχώρου. Για τις ανάγκες της παρουσίασης του προτύπου, ο Antonucci (2017), επικεντρώνεται στις πέντε βασικές αρχές του «COBIT 5 GEIT Principles», τις οποίες και συσχετίζει με τις βασικές θέσεις του ISO 31000:2009. Η αποτελεσματική εταιρική διακυβέρνηση και η διαχείριση των πληροφοριών και της

σχετικής τεχνολογίας (GEIT) αποτελεί πρωτίστως ευθύνη του διοικητικού συμβουλίου. Το COBIT 5 είναι ένα διεθνώς αποδεκτό επιχειρηματικό πλαίσιο GEIT από την ISACA, το οποίο αναπτύχθηκε από και για τους επαγγελματίες και περιλαμβάνει πληροφορίες σχετικά με την πληροφοριακή τεχνολογία και τη βιβλιογραφία περί της αποτελεσματικότερης διοίκησης. Σύμφωνα με τα όσα αναφέρει ο συγγραφέας, μπορούμε να εξάγουμε τον κάτωθι συσχετισμό μεταξύ των κατευθυντήριων γραμμών του ISO 31000:2009 και των θέσεων του COBIT 5 GEIT, ο οποίος και παρουσιάζεται στον ακόλουθο πίνακα. Στο σημείο αυτό θα πρέπει να υπογραμμιστεί ότι το Πρότυπο ISO 31000:2009 δεν αφορά συγκεκριμένα την διαχείριση των κινδύνων του κυβερνοχώρου, αλλά επισκοπεί και προτείνει ένα γενικότερο πλαίσιο διαδικασιών διαχείρισης των εταιρικών κινδύνων. Σκοπός του συγγραφέα είναι να προσπαθήσει να συσχετίσει ορισμένα κομμάτια του πλαισίου αυτού, με τις αρχές του COBIT 5, προκειμένου να παρουσιάσει μια ολοκληρωμένη πρόταση περί της αποτελεσματικής διαχείρισης των κινδύνων του κυβερνοχώρου.

Πίνακας 3: ISO 31000:2009 & COBIT 5 GEIT

COBIT 5 GEIT PRINCIPLES				
ISO31000:2009 RISK MANAGEMENT PRINCIPLES	**Ικανοποίηση των αναγκών των Ενδιαφερομένων Μερών**	**Συνολική κάλυψη του Οργανισμού**	**Εφαρμογή ενός ενιαίου πλαισίου**	**Εφαρμογή μιας ολιστικής προσέγγισης**
	Η διαχείριση των κινδύνων πρέπει να είναι διαφανής και περιεκτική.	Η διαχείριση κινδύνων δημιουργεί και προστατεύει την αξία	Η διαχείριση κινδύνων είναι συστηματική, δομημένη και έγκαιρη.	Η διαχείριση κινδύνων αποτελεί αναπόσπαστο μέρος των διαδικασιών της οργάνωσης.
	Η διαχείριση των κινδύνων είναι δυναμική, αδιάλειπτη και ανταποκρίνεται στην αλλαγή.	Η διαχείριση κινδύνων είναι προσαρμοσμένη στις ανάγκες του οργανισμού.		Η διαχείριση του κινδύνου λαμβάνει υπόψη τους ανθρώπινους και πολιτισμικούς παράγοντες.
		Η διαχείριση κινδύνων αντιμετωπίζει ρητά την αβεβαιότητα.		Η διαχείριση κινδύνων αποτελεί μέρος της διαδικασίας λήψης αποφάσεων.
				Η διαχείριση των κινδύνων βασίζεται στις καλύτερες διαθέσιμες πληροφορίες.

4.3 ENISA

Ο ENISA δημιουργήθηκε το 2004 για να εργαστεί σε ευρύ φάσμα θεμάτων σχετικά με την ασφάλεια των δικτύων και των πληροφοριών. Ο Οργανισμός υποστηρίζει την Ευρωπαϊκή Επιτροπή και τα κράτη μέλη παρέχοντας καθοδήγηση σχετικά με τις τεχνικές πτυχές της ασφάλειας των δικτύων και των πληροφοριών, συμβάλλοντας έτσι στην εύρυθμη λειτουργία της εσωτερικής αγοράς.

Ο Οργανισμός για την ασφάλεια στον Κυβερνοχώρο, ENISA, (Ευρωπαϊκός Οργανισμός για την Ασφάλεια Δικτύων & Πληροφοριών) χαρτογράφησε την ορθή πρακτική στην Ευρώπη και δημοσίευσε στο διαδίκτυο με Δελτίο τύπου, μία ενημερωμένη έκδοση των παραδοσιακών <<Κρατικών Εκθέσεων>> σχετικά με την ασφάλεια των δικτύων και πληροφοριών (NIS) των κρατών μελών και άλλων ευρωπαϊκών χωρών.

Η δημοσίευση δια πιστώνει πως οι ευρωπαϊκές χώρες διαφέρουν κατά πολύ ως προς τον βαθμό ετοιμότητας τους σχετικά με την αντιμετώπιση του κυβερνο-εγκλήματος, των δικτυακών επιθέσεων και σε ότι αφορά την ανθεκτικότητα των δικτύων. Όντας ενημερωμένη έκδοση των << Κρατικών Εκθέσεων>> περιλαμβάνει επισκόπηση και αναλυτικές, ξεχωριστές εκθέσεις για 30 ευρωπαϊκές χώρες. Το περιεχόμενο περιλαμβάνει επίσης τον καθορισμό των ενδιαφερομένων μερών και τάσεων.

Μια διαπίστωση κλειδί είναι ότι δεν διαφαίνεται κάποιο μοτίβο στις ευρωπαϊκές χώρες που περιλαμβάνονται στη μελέτη σε ότι αφορά την ύπαρξη εθνικής στρατηγικής για την Ασφάλεια Δικτύων και Πληροφοριών. Παρά ταύτα, πολλές χώρες ενισχύουν τις προσπάθειες τους και σημειώνουν πρόοδο σε αυτόν τον τομέα. Οι μηχανισμοί ανταλλαγής πληροφοριών και συνεργασίας ανάμεσα στα βασικά ενδιαφερόμενα μέρη ποικίλουν επίσης από χώρα σε χώρα. Οι επιτυχημένες πρωτοβουλίες για την ασφάλεια των δικτύων και πληροφοριών υπογραμμίζονται ως σχέδια εργασίας που μπορούν να αξιολογηθούν προς χρήση από άλλους. Οι τομείς που εξετάστηκαν περιλαμβάνουν τη διαχείριση ρίσκου και την αναφορά συμβάντων ασφαλείας, τη διαχείριση ρίσκου και τις αναδυόμενες απειλές, την ανθεκτικότητα των δικτύων, το απόρρητο και την εμπιστοσύνη, την ενίσχυση της ενημέρωσης.

Οι <<Κρατικές Εκθέσεις>> προσφέρουν μια μοναδική επισκόπηση του υφιστάμενου τοπίου Ασφαλείας Δικτύων και Πληροφοριών στα 27 κράτη μέλη της ΕΕ και στις τρεις χώρες του Ευρωπαϊκού Οικονομικού Χώρου [ΕΟΧ: Ισλανδία, Λιχτενστάιν και Νορβηγία], χωρίς να κάνει μεμονωμένες συγκρίσεις μεταξύ των κρατών, λαμβάνοντας υπ' όψη τις διαφορετικές ιστορικές καταβολές των υποδομών Ασφαλείας Δικτύων και Πληροφοριών στα κράτη αυτά. Οι εθνικές εκθέσεις περιγράφουν την εθνική στρατηγική Ασφαλείας Δικτύων και Πληροφοριών της κάθε

χώρας, το κανονιστικό πλαίσιο και τα μέτρα των κεντρικών πολιτικών, τα ενδιαφερόμενα μέρη και τη γραμμή τους, τους ρόλους και τις ευθύνες τους. Προσφέρουν μια επισκόπηση των κεντρικών δραστηριοτήτων Ασφαλείας Δικτύων και Πληροφοριών, τις αλληλεπιδράσεις των ενδιαφερομένων μερών, τους μηχανισμούς ανταλλαγής πληροφοριών, τις πλατφόρμες συνεργασίας, και τα δεδομένα, τις τάσεις και τις μελέτες περιπτώσεων ορθών πρακτικών για κάθε κράτος ξεχωριστά.

Ο εκτελεστικός διευθυντής του ENISA, καθηγητής *Udo Helmbrecht* σχολιάζοντας ανέφερε:

<<Αυτή η νέα έκδοση των <<Κρατικών Εκθέσεων>> προσφέρει μία απαραίτητη απεικόνιση του τοπίου και των υποδομών Ασφαλείας Δικτύων και Πληροφοριών για όλα τα κράτη μέλη της ΕΕ και του ΕΟΧ. Η χαρτογράφηση της κατάστασης της πληροφοριακής ασφάλειας της κάθε χώρας προσφέρει μια βασική πηγή πληροφοριών για την κοινή χρήση των ορθών πρακτικών με τους αρμόδιους για την πολιτική και τη λήψη των αποφάσεων.>>

4.3.1 Γλυκόπικρα cookies

Τα <<Γλυκόπικρα Μπισκότα>> είναι έγγραφο του Οργανισμού Enisa της ΕΕ σχετικά με τους νέους τύπους Cookies (μπισκότα) που δημιουργούν ανησυχίες σχετικά με την επιγραμμική ασφάλεια & το ιδιωτικό απόρρητο.

Τα cookies χρησιμοποιήθηκαν αρχικά για τη διευκόλυνση της επίδρασης προγραμμάτων πλοήγησης-διακομιστών. Προσφάτως, με ώθηση της διαφημιστικής βιομηχανίας, χρησιμοποιούνται για άλλους σκοπούς, π.χ τη διαχείριση της διαφήμισης, τη δημιουργία προφίλ, την ιχνηλασία, κτλ. Η δυνατότητα κατάχρησης των cookies και είναι υπαρκτή και γίνεται πράξη.

Ο νέος τύπος cookies υποστηρίζει ρη δυνατότητα αναγνώρισης χρηστών κατά τρόπο επίμονο και δεν παρέχει επαρκή διαφάνεια σχετικά με τον τρόπο χρήσης τους. Ως εκ τούτου, οι συνέπιες για την ασφάλεια και το ιδιωτικό απόρρητο δεν είναι εύκολα μετρήσιμες. Για το μετριασμό των συνεπειών για το ιδιωτικό απόρρητο, ο Οργανισμός συνιστά, μεταξύ άλλων:

- Ο σχεδιασμός των συστημάτων που χρησιμοποιούν cookies πρέπει να βασίζεται στη λογική της συναίνεσης, μετά από ενημέρωση. Η χρήση των cookies και των δεδομένων που αποθηκεύονται στα cookies πρέπει να είναι διαφανής για τους χρήστες.
- Οι χρήστες πρέπει να έχουν τη δυνατότητα να διαχειρίζονται εύκολα τα cookies και ιδιαίτερα τους τύπους cookies που σχετίζονται με τις ειδήσεις.

Επομένως, όλα τα cookies πρέπει να διαθέτουν μηχανισμούς αφαίρεσης οι οποίοι είναι εύκολα κατανοητοί και εύκολοι στη χρήση από οποιοδήποτε χρήστη.

- Η δυνατότητα αποθήκευσης cookies πέραν του ελέγχου των προγραμμάτων πλοήγησης πρέπει να περιοριστεί ή να απαγορευτεί.
- Σε περίπτωση που οι χρήστες δεν κάνουν αποδεκτή τη χρήση cookies, θα πρέπει να τους παρέχεται η δυνατότητα χρήσης άλλου διαύλου εξυπηρέτησης.

Ο *Dr. Jose Fernades*, Διευθυντής του Τμήματος Στήριξης της Ανάπτυξης και των Ακαδημαϊκών της Microsoft στην Πορτογαλία, δήλωσε ότι *<<Κάθε χρόνο όλο και περισσότερες επιχειρήσεις χρησιμοποιούν το διαδίκτυο. Η ασφάλεια και το ιδιωτικό απόρρητο είναι βασικά ζητήματα για την επιτυχία αυτής της διαδικασίας, ούτως ώστε ο τελικός χρήστης και ο επιχειρηματικός κόσμος να εμπιστεύονται πλήρως τις επιγραμμικές υπηρεσίες. Ο ENISA έχει να διαδραματίσει σπουδαίο ρόλο στο πλαίσιο αυτής της διαδικασίας και συγχαίρω τους ανθρώπους του>>*.

4.3.2 Κυβερνοζόμπι

Τα botnet είναι δίκτυα υπολογιστών που χρησιμοποιούνται χωρίς να το γνωρίζουν οι ιδιοκτήτες τους με σκοπό τη διάπραξη εγκλημάτων στο διαδίκτυο, όπως η αποστολή μηνυμάτων ανεπιθύμητης αλληλογραφίας (spam) και την αυτόματη κλοπή πολύτιμων δεδομένων, π.χ. τα στοιχεία πιστωτικών καρτών, ακόμη και για επιθέσεις στον κυβερνοχώρο με πολιτικά κίνητρα.

Ο ENISA σε διαβούλευση που διεξήγαγε με κορυφαίους εμπειρογνώμονες από όλες τις πλευρές του συμμετέχουν στην καταπολέμηση των botnet, συμπεριλαμβανομένων Παροχών Υπηρεσιών Διαδικτύου (ISP), ερευνητών σε θέματα ασφαλείας, φορέων επιβολής του νόμου, ομάδων αντιμετώπισης έκτακτων αναγκών στην πληροφορική (CERT) και εταιριών πώλησης αντιικού λογισμικού, δημοσίευσε εκτενή μελέτη σχετικά με την απειλή των botnet.

<<Ο αριθμός σχετικά με τα botnet καθορίζουν την πολιτική ατζέντα και τα εκατοντάδες εκατομμύρια ευρώ που κατευθύνονται σε επενδύσεις για την ασφάλεια. Ο αριθμός των μολυσμένων υπολογιστών και μόνο δεν αποτελεί κατάλληλο κριτήριο για την εκτίμηση του βαθμού της απειλής>> λέει ο *Dr. Giles Hogben* συντάκτης της έκθεσης.

4.3.3 Εμπιστευτικά συμβάντα εμπιστευτικών υπηρεσιών e IDAS 2018

Οι ηλεκτρονικές υπηρεσίες εμπιστοσύνης είναι μια σειρά υπηρεσιών γύρω από ψηφιακές υπογραφές, ψηφιακά πιστοποιητικά, ηλεκτρονικές σφραγίδες, χρονικές σφραγίδες κλπ, που χρησιμοποιούνται σε ηλεκτρονικές συναλλαγές για να τους εξασφαλίσουν. Το e IDAS, ένας κανονισμός της ΕΕ, είναι το πανευρωπαϊκό πλαίσιο που εξασφαλίζει τη λειτουργικότητα και την ασφάλεια αυτών των ηλεκτρονικών υπηρεσιών εμπιστοσύνης σε ολόκληρη την ΕΕ. Ένας από τους στόχους του e IDAS είναι να διασφαλίσει ότι οι ηλεκτρονικές συναλλαγές μπορούν να έχουν την ίδια νομική ισχύ με τις παραδοσιακές συναλλαγές που βασίζονται στο χαρτί. Το e IDAS είναι σημαντικό για την ευρωπαϊκή ψηφιακή αγορά, διότι επιτρέπει στις επιχειρήσεις και τους πολίτες να εργάζονται και να χρησιμοποιούν υπηρεσίες σε ολόκληρη την ΕΕ. Ο κανονισμός e IDAS εγκρίθηκε τον Ιούλιο του 2014 και τέθηκε σε ισχύ το 2016.

Σύμφωνα με την ετήσια έκθεση για τις εμπιστευτικές υπηρεσίες ασφαλείας Trust 2018, που δημοσίευσε ο ENISA στις 15/07/2019, οι κακόβουλες ενέργειες και οι αποτυχίες του συστήματος αποτελούν τις κυριότερες αιτίες των αναφερθέντων συμβάντων: Οι αστοχίες του συστήματος ανέρχονται στο 39% των συνολικών περιστατικών (σε σύγκριση με το 36% το 2017). Οι κακόβουλες ενέργειες αυξήθηκαν στο 39 % (σε σύγκριση με το 7% το 2017). Λίγα, αλλά κρίσιμες παραβιάσεις της ασφαλείας με διασυνοριακές επιπτώσεις: Περίπου το 25% των αναφερομένων περιστατικών είχε διασυνοριακό αντίκτυπο. Αν και ο λόγος είναι μικρός, η σοβαρότητα των συμβάντων ήταν υψηλή: το 75% αυτών κατατάχθηκε ως επίπεδο 4 – σοβαρό και 5 – καταστροφικό. Δημιουργία πιστοποιητικών ηλεκτρονικών υπογραφών – η πιο επηρεαζόμενη υπηρεσία: Περίπου το 50% των αναφερομένων περιστατικών επηρέασε την ειδική κατάρτιση πιστοποιημένων πιστοποιητικών για τις ηλεκτρονικές υπογραφές.

4.3.4 CyberSecurity EU

Την Πέμπτη 7 Ιουνίου 2019, τέθηκε σε ισχύ ο νόμος για την ασφάλεια στον κυβερνοχώρο της ΕΕ (CSA). Ο ENISA θα γίνει ο Οργανισμός της Ευρωπαϊκής Ένωσης για την Cybersecurity, με νέα μόνιμη εντολή.

Ο νόμος για την ασφάλεια στον κυβερνοχώρο δίνει στον ENISA ενισχυμένο ρόλο στην ασφάλεια του κυβερνοχώρου με νέα καθήκοντα. Ο Οργανισμός έχει επίσης λάθει πρόσθετους οικονομικούς και ανθρώπινους πόρους για την αντιμετώπιση αυτών των καθηκόντων.

Μια από τις μεγαλύτερες αλλαγές που επιφέρει ο εν λόγω κανονισμός της ΕΕ είναι ο ENISA θα έχει μόνιμη εντολή και θα μετονομαστεί στον Οργανισμό της Ευρωπαϊκής Ένωσης για την Cybersecurity. Επιπλέον, ο Οργανισμός καλείται εφεξής να εκτελεί τα ακόλουθα νέα καθήκοντα:

- Πιστοποίηση Cybersecurity: Ο ENISA διαδραματίζει κεντρικό ρόλο στον νέο νόμο για την ασφάλεια στον κυβερνοχώρο, δεδομένου ότι ο Οργανισμός θα διαδραματίσει βασικό ρόλο στην ανάπτυξη του πλαισίου πιστοποίησης για την ασφάλεια στον κυβερνοχώρο της ΕΕ, προετοιμάζοντας τα υποψήφια συστήματα πιστοποίησης.

- Cyber ανθεκτικότητα: θα υποστηρίζει τη δημιουργία ικανοτήτων και την ετοιμότητα σε ολόκληρη την Ένωση βοηθώντας τα θεσμικά όργανα, τους οργανισμούς, τα γραφεία και τους οργανισμούς της Ένωσης καθώς και τα κράτη μέλη και τους ενδιαφερόμενους φορείς του δημοσίου και του ιδιωτικού τομέα να αυξήσουν την προστασία του δικτύου και των συστημάτων πληροφοριών τους, την ικανότητα αντοχής και αντίδρασης και την ανάπτυξη δεξιοτήτων και ικανοτήτων στον τομέα της ασφάλειας του κυβερνοχώρου.

- Γνωστοποίηση ευπάθειας: Επιπλέον θα βοηθηθούν τα κράτη μέλη και τα θεσμικά όργανα, τους οργανισμούς, τα γραφεία και τους οργανισμούς της Ένωσης να θεσπίσουν και να εφαρμόσουν πολιτικές γνωστοποίησης ευαισθησίας σε εθελοντική βάση.

4.3.5 Ασφάλεια Προστασίας Προσωπικών Δεδομένων – GDPR

Ο γενικός κανονισμός για την προστασία των δεδομένων (GDPR) αποτέλεσε σημείο καμπής για την προστασία των προσωπικών δεδομένων στην Ευρώπη και συμπληρώνει το ισχύον νομικό πλαίσιο στον τομέα της ιδιωτικής και επαγγελματικής ζωής στις τηλεπικοινωνίες. Καθώς το νομικό τοπίο μετατοπίζεται προς τη φάση υλοποίησης του GDPR και τον συνεχιζόμενο νομοθετικό έλεγχο του σχεδίου κανονισμού για την προστασία, οι προκλήσεις που τίθενται ζητούν την κατάλληλη ανταπόκριση των υπευθύνων χάραξης πολιτικής.

Στις 13 και 14 Ιουνίου 2019, ο Οργανισμός της ΕΕ για την ασφάλεια στον κυβερνοχώρο ENISA, το Πανεπιστήμιο της Ρώμης Tor Vergata και του Πανεπιστημίου LUISS οργάνωσαν το 7ο Φόρουμ Ετήσιας Προστασίας Προσωπικών Δεδομένων 2019 στη Ρώμη, Ιταλία.

Το ετήσιο φόρουμ για την προστασία της ιδιωτικής ζωής (APF) έχει γίνει φημισμένο φόρουμ ανταλλαγής μεταξύ των υπευθύνων χάραξης πολιτικής και των εκτελεστών στον τομέα της προστασίας των δεδομένων. Τα τελευταία χρόνια η APF έχει λάβει αναγνώριση από όλους τους φορείς βιομηχανίας, συμπληρώνοντας την

αρχική της έρευνα και τον προσανατολισμό πολιτικής. Κατά την έκδοση του Κανονισμού (ΕΕ) 2019/881 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, τη; 17ης Απριλίου 2019, σχετικά με τον ENISA, ο Οργανισμός επιδιώκει να συμβάλει περαιτέρω στον τομέα της προστασίας των προσωπικών δεδομένων, στο πλαίσιο της ανανεωμένης εντολής του.

Το APF οργανώθηκε σε ένα πλαίσιο όπου τα δίκτυα ηλεκτρονικών επικοινωνιών και οι διασυνδεδεμένες ψηφιακές υπηρεσίες έχουν γίνει πανταχού παρόν, καθώς έχουν διαπεράσει κάθε πτυχή της καθημερινής ζωής. Η αυτοματοποιημένη δημιουργία προφίλ και η ηλεκτρονική επιτήρηση έχουν καταστεί εμπορεύματα.

Το σχέδιο κανονισμού για τα προσωπικά δεδομένα και τις ηλεκτρονικές επικοινωνίες αναμένεται να δώσει νέα ώθηση στον τρόπο προστασίας της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες. Προκειμένου να αντιμετωπιστεί η πρόκληση όσον αφορά τον τρόπο επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής σε ολόκληρη την ΕΕ και πέρα από αυτήν, απαιτείται η εξέταση των διαθέσιμων μεριδίων.

4.4 Ασφάλειες κυβερνοχώρου- Ασφαλιστήρια συμβόλαια

Στην ψηφιακή εποχή εντός της οποίας πλέον λειτουργούν οι επιχειρήσεις και οι επαγγελματίες είναι αναγκαία η διασφάλιση των πληροφοριακών συστημάτων που χρησιμοποιούν και των προσωπικών δεδομένων του πελατολογίου τους απέναντι σε κινδύνους παραβίασης και διαρροής αυτών, που οφείλονται σε κακόβουλα λογισμικά, ιούς και Hackers.

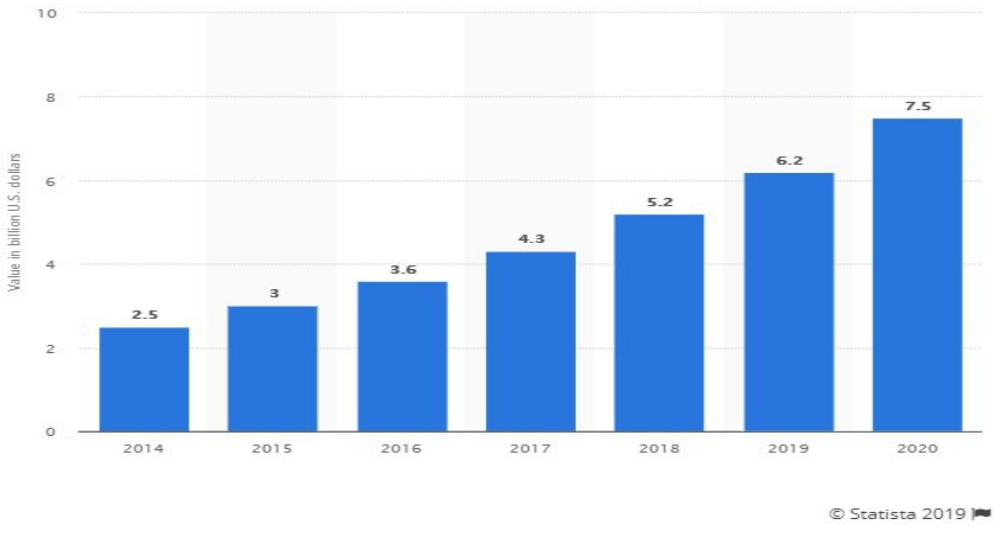
Σε περίπτωση επέλευσης ενός περιστατικού ασφαλείας με τα προγράμματα ασφάλειας κυβερνοχώρου, δίνεται η δυνατότητα να περιοριστούν οι οικονομικές επιπτώσεις στα αποτελέσματα του οργανισμού, να διατηρηθεί η εταιρική φήμη και το εταιρικό Brand, να αντιμετωπιστεί αποτελεσματικά ο κίνδυνος διαρροής των δεδομένων των πελατών του οργανισμού, παρέχοντας σωστή εξυπηρέτηση. Τα ασφαλιστήρια απευθύνονται κυρίως σε επιχειρήσεις Υπηρεσιών Υγείας, Ξενοδοχεία, ηλεκτρονικά καταστήματα (e-shops), δικηγορικές εταιρίες, λογιστικά γραφεία και ελεγκτικές εταιρίες.

Οι καλύψεις συνήθως που προσφέρονται στο ασφαλιστήριο συμβόλαιο Κυβερνοχώρου είναι οι ακόλουθες:

- Κάλυψη νομικών εξόδων, απαιτούμενων για τη διαχείριση των κανονιστικών απαιτήσεων σε περίπτωση παραβίασης δεδομένων

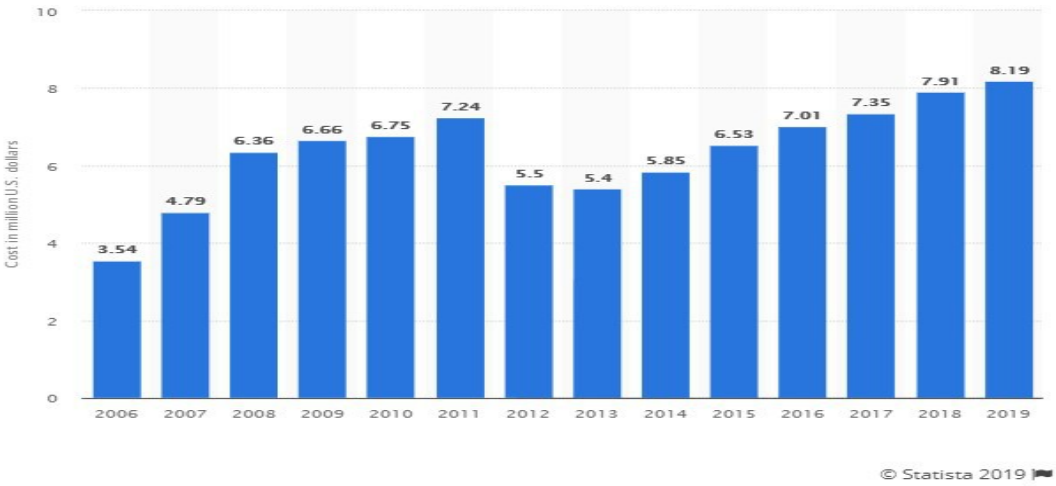
- Ενημέρωση του πελατολογίου για το περιστατικό ασφαλείας και παροχή υπηρεσίας εξυπηρέτησης πελατών
- Κάλυψη εξόδων απαιτούμενων για συμβουλευτική για τη διαχείριση κρίσεων και δημοσίων σχέσεων
- Παροχή νομικών συμβούλων και υποστήριξη στην αξιολόγηση των νομικών συνεπειών από την παραβίαση των δεδομένων
- Παροχή εξειδικευμένων ερευνητικών ασφαλείας, για τον έλεγχο της αιτίας και της έκτασης του φαινομένου παραβίασης.
- Αποζημιώσεις τρίτων ζημιωθέντων λόγω διαρροής δεδομένων
- Παροχή εξειδικευμένων διαπραγματευτών σε περίπτωση εκβιασμού αποκάλυψης πληροφοριών ή περιστατικού παραβίασης
- Πρόστιμα και κυρώσεις που ασφαλίζονται από το νόμο
- Έξοδα ανάκτησης δεδομένων που χάθηκαν λόγω περιστατικού παραβίασης της ασφάλειας του συστήματος
- Απώλεια κερδών σε περίπτωση διακοπής λειτουργίας εταιρικού δικτύου οφειλόμενη σε μη διαθεσιμότητα των πληροφοριακών συστημάτων της εταιρίας ή/και σε άρνηση παροχής υπηρεσίας αυτών λόγω παραβίασης ασφάλειας ή επίθεσης από Hackers.

Η Statista είναι μία γερμανική ηλεκτρονική πύλη που δημοσιεύει επίσημα στατιστικά στοιχεία από τον οικονομικό τομέα, που συλλέγει δεδομένα από ινστιτούτα έρευνας και γνώμης της αγοράς.



Εικόνα 4.1 Αξία των εγγεγραμμένων ασφαλίστρων στον κυβερνοχώρο παγκοσμίως από το 2014 έως το 2020 (σε δισεκατομμύρια δολάρια ΗΠΑ), **Πηγή: Statista.com**

Το 2018, τα ασφάλιστρα στον κυβερνοχώρο παγκοσμίως ανήλθαν σε 5,2 δισεκατομμύρια δολάρια ΗΠΑ και αναμένεται να αυξηθούν στα 7,5 δισεκατομμύρια δολάρια το 2020.



Εικόνα 4.2 Μέσο οργανωτικό κόστος για μια επιχείρηση στις Ηνωμένες Πολιτείες μετά από παραβίαση δεδομένων από το 2006 έως το 2019 (σε εκατομμύρια δολάρια ΗΠΑ), **Πηγή: Statista.com**

Το 2019, το μέσο κόστος για τις επιχειρήσεις που επλήγησαν από παραβίαση δεδομένων στις Ηνωμένες Πολιτείες ανήλθε σε 8,19 εκατομμύρια δολάρια, από 7,91 εκατομμύρια δολάρια το προηγούμενο έτος. Το παγκόσμιο μέσο κόστος ανά παραβίαση δεδομένων ήταν 3,92 εκατομμύρια δολάρια ΗΠΑ.

4.5 Κατηγορίες Cyber Security Insurance

4.5.1 Cyber Liability Insurance

Η ασφάλεια αστικής ευθύνης (Cyber Liability Insurance), είναι γνωστή και σαν ασφάλεια προστασίας προσωπικών δεδομένων και ιδιωτικότητας (Information Security and Privacy). Με αυτού το είδος ασφάλειας καλύπτεται η ευθύνη του ασφαλιζόμενου οργανισμού σε περίπτωση που έχουμε παραβίαση δεδομένων και δεν καλύπτει έξοδα που αφορούν το άμεσο κόστος απόκρισης από ένα περιστατικό ασφαλείας. Το συγκεκριμένο προϊόν αφορά κατά κύριο λόγο εταιρίες και

οργανισμούς οι οποίοι πουλούν υπηρεσίες και αγαθά μέσω του διαδικτύου. Ένας τέτοιου είδους οργανισμός έχεις στην κατοχή και στα συστήματα του πολύ σημαντικά και ευαίσθητα προσωπικά δεδομένα των πελατών του. Τέτοια στοιχεία μπορεί να είναι αυστηρά προσωπικά, όπως είναι η διεύθυνση κατοικίας, είτε οικονομική φύσεως, όπως είναι αριθμοί λογαριασμών τραπέζης και αριθμοί πιστωτικών καρτών, αριθμοί κοινωνικής ασφάλισης. Οι κίνδυνοι λοιπόν για έναν τέτοιο οργανισμοί είναι πολλοί και ένας τέτοιος οργανισμός θα πρέπει να έχει λάβει όλα εκείνα τα απαραίτητα μέτρα για την προστασία όλων αυτών των σημαντικών και ευαίσθητων προσωπικών δεδομένων. Ένα τέτοιου είδους λοιπόν ασφαλιστικό πακέτο καλύπτει τα εξής:

• Κλοπή ενός laptop ενός εργαζομένου (πχ από διάρρηξη του αυτοκινήτου του).

• Περίπτωση που ένα email με ευαίσθητα δεδομένα αποσταλεί σε λάθος παραλήπτη.

• Σημαντικά έγραφα να κλαπούν από τις εγκαταστάσεις του οργανισμού σε περίπτωση διάρρηξης.

• Να κλείσει επιτυχώς ένα περιστατικό ασφαλείας σε εύλογο χρονικό διάστημα.

4.5.2 Technology Errors and Omissions

Η συγκεκριμένη ασφαλιστική κατηγορία αναφέρεται αλλιώς και ως Επαγγελματική Ευθύνη (Professional Liability) ή σε συντομογραφία E&O. Είναι μία μορφή κάλυψης ευθύνης που προστατεύει τις επιχειρήσεις οι οποίες παρέχουν ή πωλούν τεχνολογικές υπηρεσίες και προϊόντα. Με τις καλύψεις της συγκεκριμένης κατηγορίας αποτρέπει τις επιχειρήσεις να φέρουν το πλήρες κόστος από μία αμέλεια που μπορεί να υποβληθεί από έναν πελάτη και τις αποζημιώσεις που θα πρέπει να δοθούν σε περίπτωση πολιτικής αγωγής. Επίσης μπορεί να καλύπτει διαφημιστικές εταιρείες οι οποίες μπορεί να δημιουργήσουν ψηφιακό περιεχόμενο το οποίοι μπορεί να βλάψει έναν οργανισμό. Παράλληλα μπορεί να καλύψει και προγραμματιστές οι οποίοι μπορεί να έχουν δημιουργήσει έναν κώδικα και να έχει κάποιο λάθος. Γενικότερα τέτοιου είδους εταιρείες θα πρέπει να σκεφτούν πολύ καλά τι μπορεί να γίνει σε περίπτωση οποιουδήποτε λάθος που μπορεί να υπάρξει στις υπηρεσίες που προσφέρουν προς τους πελάτες τους. Για παράδειγμα: • Τι θα συμβεί σε περίπτωση που ένα λάθος στο λογισμικό τους (software glitch), οδηγήσει στο να χάσει ο πελάτης τους πολύ σημαντικά δεδομένα. • Τι θα συμβεί αν μία ανεπαρκής εγκατάσταση του προγράμματος τους (flawed program installation) αποτρέψει τον τελικό τους πελάτη στο να παραλάβει μία παραγγελία του. • Τι θα συμβεί αν ένα λάθος στον κώδικα οδηγήσει τον χρήστη στο να μην μπορεί να κάνει μία κράτηση μέσω του διαδικτύου.

ΚΕΦΑΛΑΙΟ 5

ΠΑΡΟΥΣΙΑΣΗ ΜΕΘΟΔΟΛΟΓΙΑΣ

5.1. Περιγραφικά στατιστικά του Δείγματος

Στο τελευταίο μέρος της διπλωματικής εργασίας παρατίθενται τα αποτελέσματα της ποσοτικής έρευνας που πραγματοποιήθηκε με ερωτηματολόγιο. Το θέμα της έρευνας είναι η διαχείριση του διαδικτυακού κινδύνου στα λογιστικά γραφεία και στις ελεγκτικές εταιρίες.

5.1.1 Δειγματοληπτικό Πλαίσιο

Το δειγματοληπτικό πλαίσιο αφορά λογιστικά γραφεία και ελεγκτικές εταιρίες της Κύπρου. Η πηγή των στοιχείων για τον καθορισμό του δείγματος είναι ο δημοσιευμένος κατάλογος με τα αδειοδοτημένα από το ΣΕΛΚ (Σύνδεσμος Εγκεκριμένων Λογιστών Κύπρου) πρόσωπα. Στον κατάλογο αυτό αναφέρονται τα νομικά ελεγκτικά γραφεία με τα στοιχεία εγγραφής (π.χ. αριθμός μητρώου) και επικοινωνίας (διεύθυνση, τηλέφωνο, ηλεκτρονικό ταχυδρομείο). Πιο συγκεκριμένα, η κύρια δραστηριότητα του ΣΕΛΚ, όπως αναφέρεται στην επίσημη ιστοσελίδα του είναι: <<Οι κύριες δραστηριότητες του Συνδέσμου είναι η παροχή οργανωτικού σχήματος για τους επαγγελματίες λογιστές, η υποστήριξη και προαγωγή των θέσεων και συμφερόντων του λογιστικού επαγγέλματος, καθώς και η συνεχή επαγγελματική ανάπτυξη και ενημέρωση των Μελών. Ο Σύνδεσμος είναι το μοναδικό αναγνωρισμένο από το Υπουργικό Συμβούλιο σώμα λογιστών Κύπρου, και η αρμόδια αρχή για χορήγηση άδειας σε ελεγκτές. Επίσης, ο Σύνδεσμος αποτελεί αρμόδια αρχή για άσκηση άλλων δραστηριοτήτων στη βάση σχετικών νομοθεσιών ή εξουσιών που εκχωρούνται σε αυτόν από το Υπουργικό Συμβούλιο, Υπουργό ή οποιαδήποτε άλλη αρχή…>>. Περισσότερη πληροφόρηση στο www.icpac.org.cy. Τέλος, ο αριθμός των λογιστικών γραφείων που περιλαμβάνονται στον κατάλογο ανέρχεται στα 876 και των ελεγκτικών εταιριών στα 706.

5.1.2 Σχεδιασμός Ερωτηματολογίου

Όσο αναφορά στο σχεδιασμό του ερωτηματολογίου έγινε με τη χρήση φόρμας του Google Docs το οποίο ενδείκνυται για τη δημιουργία ηλεκτρονικών επαγγελματιών ερωτηματολογίων. Όσο αναφορά τη δομή του αποτελείται από 10 ερωτήσεις κλειστού τύπου. Οι μορφές των ερωτήσεων είναι διαβαθμισμένης κλίμακας (Καθόλου, Λίγο, Μέτρια, Πολύ, Πάρα πολύ) και ερωτήσεις πολλαπλής επιλογής. Χωρίζεται σε δύο μέρη. Το πρώτο περιλαμβάνει δεύτερο τις βασικές ερωτήσεις με διάρθρωση που δίνει απαντήσεις στα ερευνητικά ερωτήματα και το δεύτερο περιλαμβάνει δημογραφικές ερωτήσεις.

5.1.3 Συλλογή Δεδομένων

Η αποστολή του ερωτηματολογίου στα λογιστικά γραφεία και στις ελεγκτικές εταιρίες έγινε με το ηλεκτρονικό ταχυδρομείο. Να σημειωθεί ότι διευκρινίζονταν στους συμμετέχοντες η εμπιστευτικότητα των πληροφοριών τους και πως η έρευνα είναι ανώνυμη. Η συλλογή των δεδομένων διήρκησε περίπου δύο μήνες.

ΚΕΦΑΛΑΙΟ 6

ΠΑΡΟΥΣΙΑΣΗ ΚΑΙ ΕΡΜΗΝΕΙΑ ΑΠΟΤΕΛΕΣΜΑΤΩΝ

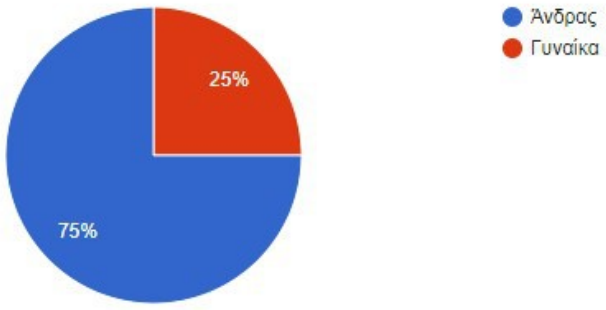
6.1 Περιγραφή Δείγματος

6.1.1 Δημογραφικά δεδομένα

Στα παρακάτω διαγράμματα 1,2,3 και 4 παρουσιάζεται η περιγραφή του δείγματος ανά φύλλο, ηλικία, ιδιότητα των ερωτηθέντων στις επιχειρήσεις και τα έτη λειτουργίας αυτών.

Φύλο

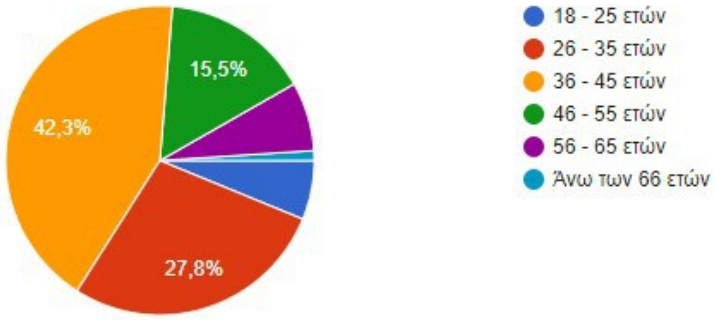
Το δείγμα αποτελείται από 96 συμμετέχοντες από τους οποίους το 75% (n=72) είναι άνδρες και το 25% (n=24) είναι γυναίκες.



Διάγραμμα 1: Περιγραφή στατιστικών δειγμάτων ανά φύλο

Ηλικία

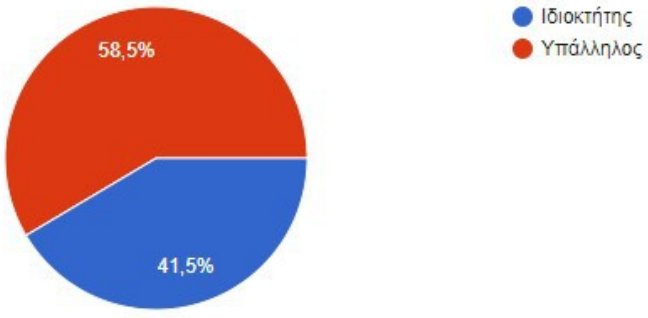
Όσο αναφορά το ηλιακό όριο των συμμετεχόντων το 6,2% (n=6) είναι ηλικίας 18-25 ετών, το 27,8% (n=27) είναι 26-35 ετών, το 42,3% (n=41) είναι 36-45 ετών, το 15,5% (n=15) είναι 46-55 ετών, το 7,2% (n=7) είναι 56-65 ετών και μόλις 1% (n=1) είναι άνω των 66 ετών.



Διάγραμμα 2: Περιγραφή στατιστικών δείγματος ανά ηλικία

Ιδιότητα στην επιχείρηση

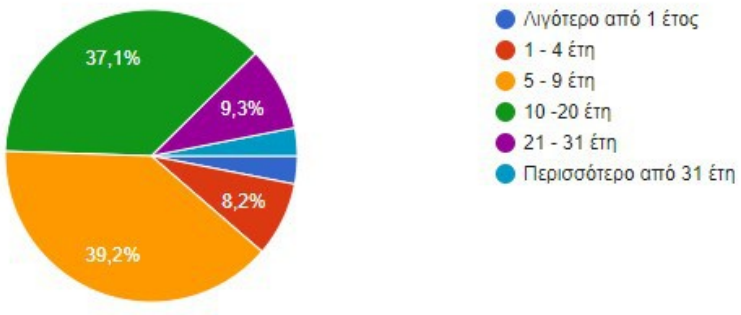
Από τους συμμετέχοντες το 58,5% (n=55) δήλωσε ότι είναι υπάλληλος σε λογιστικό γραφείο ή σε ελεγκτική εταιρία, ενώ το 41,5% (n=39) δήλωσε ότι έχει την ιδιότητα του ιδιοκτήτη.



Διάγραμμα 3: Περιγραφή στατιστικών δείγματος ανά ιδιότητα

Έτη λειτουργίας της επιχείρησης

Στο τέλος είναι το δημογραφικό που αφορά τα έτη λειτουργίας του λογιστικού γραφείο ή της ελεγκτικής εταιρίας στο οποίο το 3,1% (n=3) δήλωσε λιγότερο από ένα έτος, το 8,2% (n=8) από 1-4 έτη, το 39,2% (n=38) από 5-9 έτη, το 37,1% (n=36) από 10-20 έτη, το 9,3% (n=9) από 21-31 έτη και το 3,1% (n=3) περισσότερο από 31 έτη.



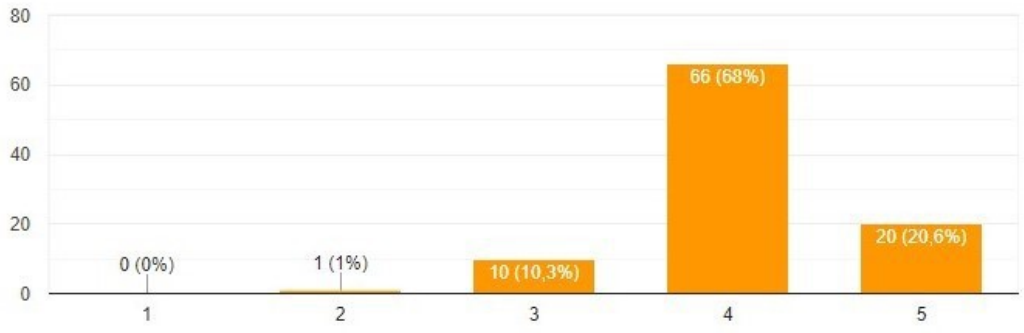
Διάγραμμα 4: Περιγραφή στατιστικών δείγματος ανά έτη λειτουργίας

6.2 Ανάλυση Εμπειρικών Αποτελεσμάτων

Στα επόμενα διαγράμματα φαίνονται τα αποτελέσματα των απαντήσεων των συμμετεχόντων στις ερωτήσεις του ερωτηματολογίου.

Ερώτηση 1

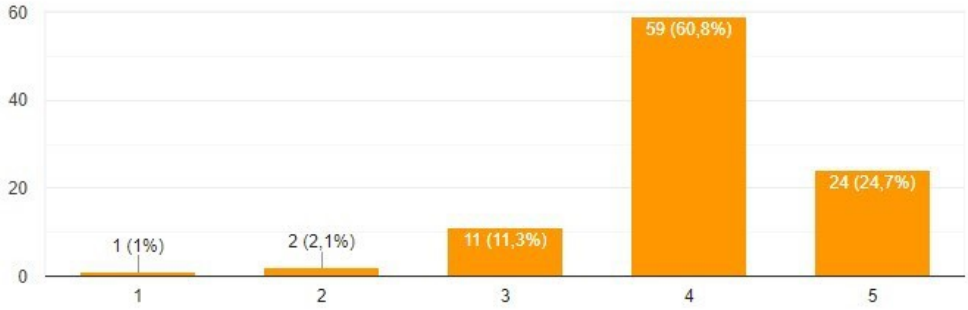
Στην πρώτη ερώτηση οι συμμετέχοντες στην έρευνα ρωτήθηκαν κατά πόσο γνωρίζουν τη έννοια του διαδικτυακού κινδύνου. Τα αποτελέσματα είναι τα εξής: το 1% (n=1) απάντησε ότι γνωρίζει λίγο, το 10,3% (n=10) απάντησαν ότι έχουν μέτρια γνώση για την έννοια του διαδικτυακού κινδύνου, το 68% (n=66) που είναι και το μεγαλύτερο ποσοστό δήλωσαν ότι γνωρίζουν την έννοια πολύ, τέλος το 20,6% (n=20) ξέρουν την έννοια πάρα πολύ καλά. Να σημειωθεί δεν υπήρχαν συμμετέχοντες που να απάντησαν καθόλου.



Διάγραμμα 5: Περιγραφή στατιστικών δείγματος Ερώτηση 1

Ερώτηση 2

Στη δεύτερη ερώτηση οι συμμετέχοντες έπρεπε να απαντήσουν σε ποιο βαθμό πιστεύουν πως τα ηλεκτρονικά τους δεδομένα (επιχειρηματικά και προσωπικά) που διατηρούν ως γραφείο μπορούν να απειλούνται από τους διαδικτυακούς κινδύνους. Οι απαντήσεις που δόθηκαν ξεκινώντας από την μικρότερη κλίμακα διαβάθμισης μέχρι την μεγαλύτερη είναι οι ακόλουθες: καθόλου το 1% (n=1), λίγο το 2,1% (n=2), σε μέτριο βαθμό 11% (n=11,3%), πολύ 60,8% (n=59) και 24,7% (n=24) πάρα πολύ.



Διάγραμμα 6: Περιγραφή στατιστικών δείγματος Ερώτηση 2

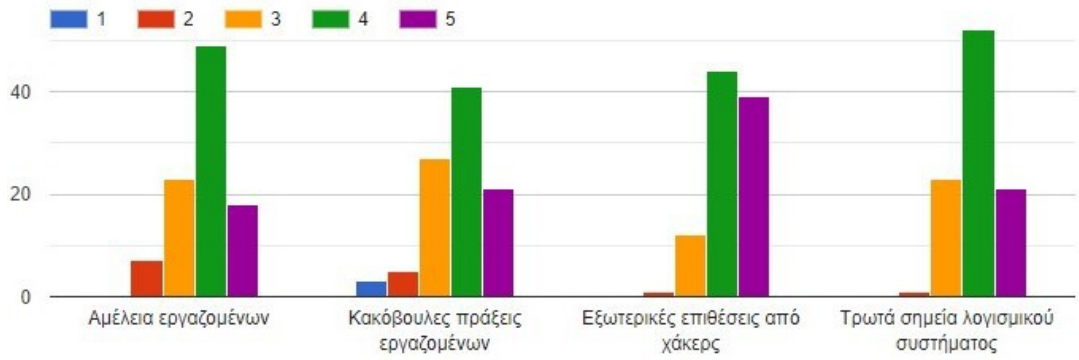
Ερώτηση 3

Στην τρίτη ερώτηση δόθηκε μια λίστα κινδύνων που απειλούν αιτίες απώλειας και διαρροής δεδομένων και ενδέχεται να διατρέχουν ως λογιστικό γραφείο ή ελεγκτική εταιρία. Οι κίνδυνοι προς αξιολόγηση είναι η αμέλεια των εργαζομένων, οι

κακόβουλες πράξεις των εργαζομένων, οι εξωτερικές επιθέσεις απ hackers, τα τρωτά σημεία του λογισμικού συστήματος. Πιο συγκεκριμένα τα αποτελέσματα έδειξαν:

Πίνακας 4: Αποτελέσματα αιτιών απώλειας και διαρροής δεδομένων

Ποσοστό (n)	**Καθόλου**	**Λίγο**	**Μέτρια**	**Πολύ**	**Πάρα πολύ**	**Σύνολο**
Αμέλεια των εργαζομένων	0% (n=0)	7,21% (n=7)	23,71% (n=23)	50,52% (n=49)	18,56% (n=18)	100% (n=97)
Κακόβουλες πράξεις των εργαζομένων	3,09% (n=3)	5,15% (n=5)	27,84% (n=27)	42,27% (n=41)	21,65% (n=21)	100% (n=97)
Εξωτερικές επιθέσεις από hackers	0% (n=0)	1,03% (n=1)	12,37% (n=12)	45,36% (n=44)	40,21% (n=39)	98,97% (n=96)
Τρωτά σημεία του λογισμικού συστήματος	0% (n=0)	1,03% (n=1)	23,71% (n=23)	53,61% (n=52)	21,65% (n=21)	100% (n=97)

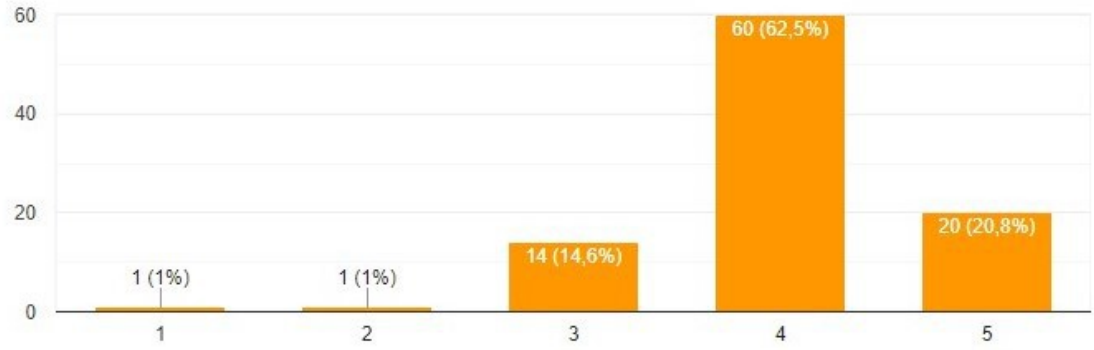


Διάγραμμα 7: Περιγραφή στατιστικών δείγματος Ερώτηση 3

Ερώτηση 4

Η τέταρτη ερώτηση κάνει μια αναφορά σε μια διάταξη του καινούργιου ευρωπαϊκού κανονισμού για την προστασία των προσωπικών δεδομένων GDPR (5419/16). Η διάταξη αυτή αφορά τις επιχειρήσεις και προβλέπει ως συνέπεια για αυτές που δεν εφαρμόζουν ή παραβιάζουν το νόμο πρόστιμο έως και το 4% του συνολικού παγκόσμιου ετήσιου κύκλου εργασιών (΄΄τζίρου΄΄) του προηγούμενου οικονομικού έτους (Άρθρο 83). Αυτό που ζητήθηκε είναι να απαντήσουν σε ποιο βαθμό είναι ενημερωμένοι. Στα αποτελέσματα βλέπουμε ότι 1% (n=1) είναι καθόλου

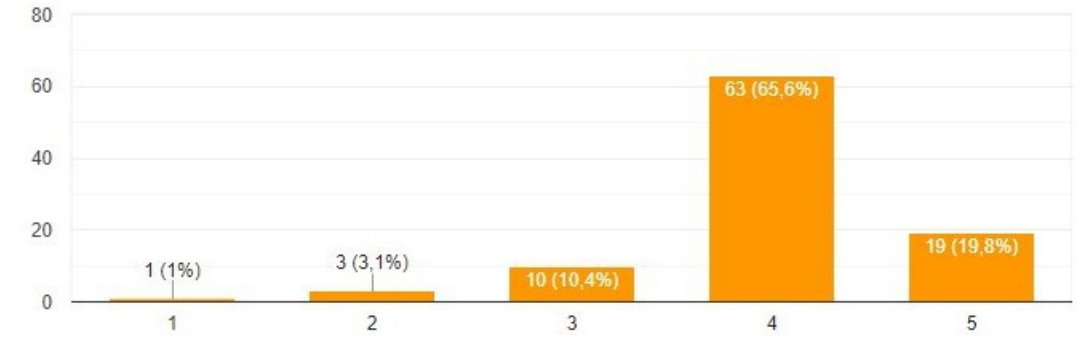
ενημερωμένοι για τη νέα αυτή διάταξη, επίσης το 1% (n=1) είναι λίγο, το 14,6% (n=14) σε μέτριο βαθμό, το 62,5% (n=60) είναι πολύ και το 20,8% (n=20) πάρα πολύ ενήμεροι.



Διάγραμμα 8: Περιγραφή στατιστικών δείγματος Ερώτηση 4

Ερώτηση 5

Στην πέμπτη ερώτηση καλούνται να απαντήσουν κατά πόσο έχουν συμμορφωθεί σύμφωνα με τις διατάξεις του νέου ευρωπαϊκού κανονισμού GDPR (5419/16). Στα αποτελέσματα βλέπουμε πάλι ότι το 1% (n=1) δεν έχει συμμορφωθεί καθόλου, το 3,1% (n=3) λίγο, το 10,04% (n=10) μέτρια, το 65,6% (n=63) πολύ και το 19,8% (n=19) έχει συμμορφωθεί πάρα πολύ.

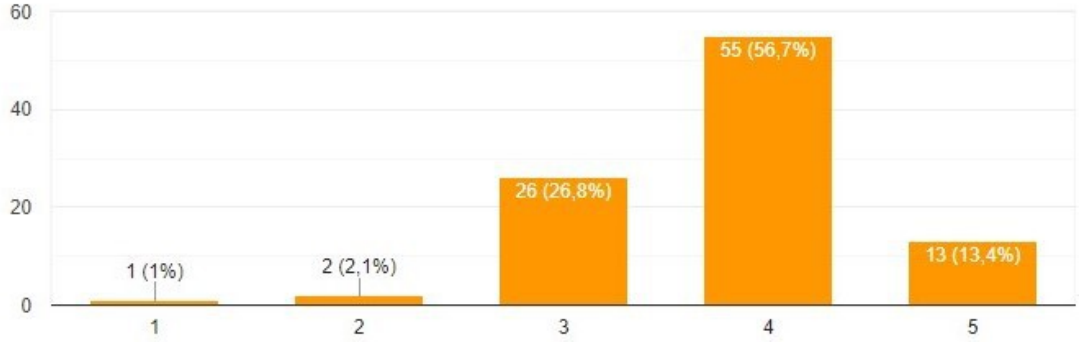


Διάγραμμα 9: Περιγραφή στατιστικών δείγματος Ερώτηση 5

Ερώτηση 6

Οι συμμετέχοντες καλούνται να αξιολογήσουν το βαθμό σύνδεσης των παραβιάσεων της ασφάλειας των πληροφοριών του γραφείου τους με χρηματοοικονομικές απώλειες. Οι απαντήσεις που δόθηκαν είναι 1% (n=1) καθόλου, λίγο είναι το 2%

(n=2), μέτρια 26,8% (n=26), πολύ που είναι το μεγαλύτερο ποσοστό το 56,7% (n=55) και το 13,4% (n=13) το αξιολόγησαν με βαθμό πάρα πολύ.



Διάγραμμα 10: Περιγραφή στατιστικών δείγματος Ερώτηση 6

Ερώτηση 7

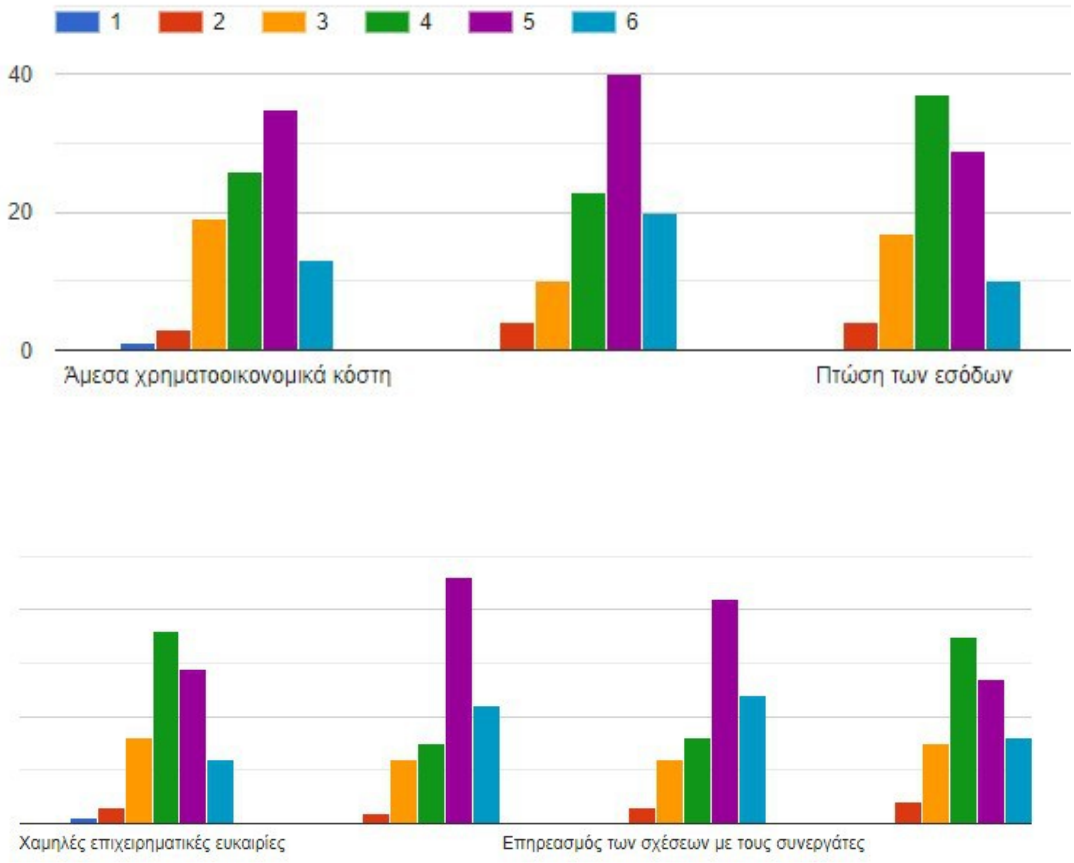
Η ερώτηση αυτή αφορά τα άμεσα και έμμεσα κόστη που θα δημιουργηθούν από την παραβίαση της ασφάλειας των πληροφοριών που διατρέχει ένα λογιστικό γραφείο ή μία ελεγκτική εταιρία και καλούνται οι συμμετέχοντες να τα αξιολογήσουν. Τα αποτελέσματα αυτής της εκτίμησης παρουσιάζονται στον παρακάτω πίνακα:

1.Άμεσα χρηματοοικονομικά κόστη, 2. Μείωση της φήμης και πελατείας του γραφείου, 3.Πτώση των εσόδων, 4. Χαμηλές επιχειρηματικές ευκαιρίες, 5. Επηρεασμός των σχέσεων με τους πελάτες, 6. Επηρεασμός των σχέσεων με τους συνεργάτες και 7. Επιχειρηματική συνέχεια.

Πίνακας 5: Αποτελέσματα σε αριθμούς και ποσοστά για τα άμεσα και έμμεσα κόστη

Ν	**Καθόλου**	**Πολύ λίγο**	**Λίγο**	**Μέτρια**	**Πολύ**	**Πάρα πολύ**	**Σύνολο**
1	1,03% (n=1)	3,09% (n=3)	19,59% (n=19)	26,80% (n=26)	36,09% (n=35)	13,40% (n=13)	100% (n=97)
2	0% (n=0)	4,12% (n=4)	10,31% (n=10)	23,71% (n=23)	41,24% (n=40)	20,62% (n=20)	100% (n=97)
3	0% (n=0)	4,12% (n=4)	17,53% (n=17)	38,14% (n=37)	29,90% (n=29)	10,31% (n=10)	100% (n=97)

4	1,03% (n=1)	3,09% (n=3)	16,49% (n=16)	37,11% (n=36)	29,90% (n=29)	12,38% (n=12)	100% (n=97)
5	0% (n=0)	2,06% (n=2)	12,37% (n=12)	15,46% (n=15)	47,43% (n=46)	22,68% (n=22)	100% (n=97)
6	0% (n=0)	3,09% (n=3)	12,37% (n=12)	16,49% (n=16)	43,31% (n=42)	24,74% (n=24)	100% (n=97)
7	0% (n=0)	4,12% (n=4)	15,46% (n=15)	36,09% (n=35)	27,84% (n=27)	16,49% (n=16)	100% (n=97)

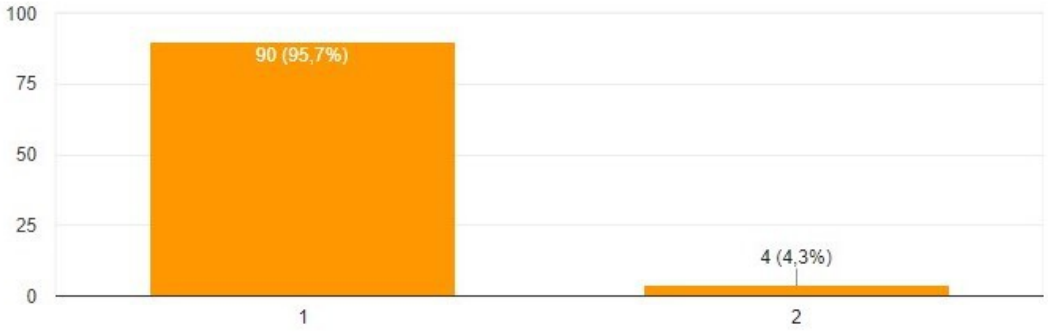


Διάγραμμα 11: Περιγραφή στατιστικών δείγματος Ερώτηση 7

Ερώτηση 8

Η ερώτηση 8 ζητάει από τους ερωτηθέντες να απαντήσουν εάν έχουν λάβει μέτρα προστασίας για τη διαχείριση του διαδικτυακού κινδύνου. Οι επιλογές στην ερώτηση

είναι <<ΝΑΙ>> και <<ΟΧΙ>> . Η επιλογή <<ΝΑΙ>> έλαβε το 90,7% (n=90) ενώ η απάντηση <<ΟΧΙ>> μόνο 4,3% (n=4) στους συνολικά 94 που απάντησαν.



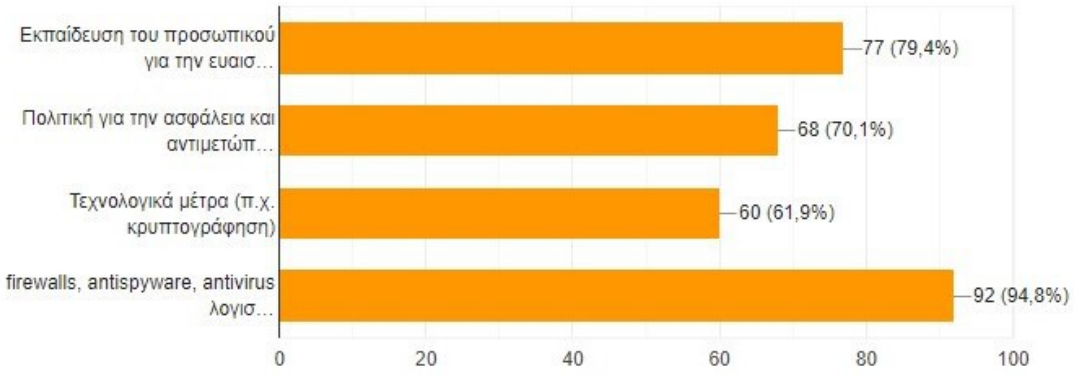
Διάγραμμα 12: Περιγραφή στατιστικών δείγματος Ερώτηση 8

Ερώτηση 9

Η ερώτηση 9 είχε προτεινόμενες κατηγορίες μέτρων που χρησιμοποιούν οι συμμετέχοντες για την πρόληψη και τον μετριασμό του διαδικτυακού κινδύνου. Οι επιλογές ήταν:

1. Εκπαίδευση του προσωπικού για την ευαισθητοποίηση σε θέματα ασφαλείας
2. Πολιτική για την ασφάλεια και την αντιμετώπιση των περιστατικών
3. Τεχνολογικά μέτρα (π.χ. κρυπτογράφηση)
4. Firewalls, antispyware, antivirus λογισμικά

και οι απαντήσεις ήταν οι εξής: για το πρώτο το ποσοστό είναι 79,4% (n= 77), το δεύτερο μέτρο έχει ποσοστό 70,1% (n=68), το τρίτο 61,9% (n=60) το τελευταίο 94,8% (n=92).



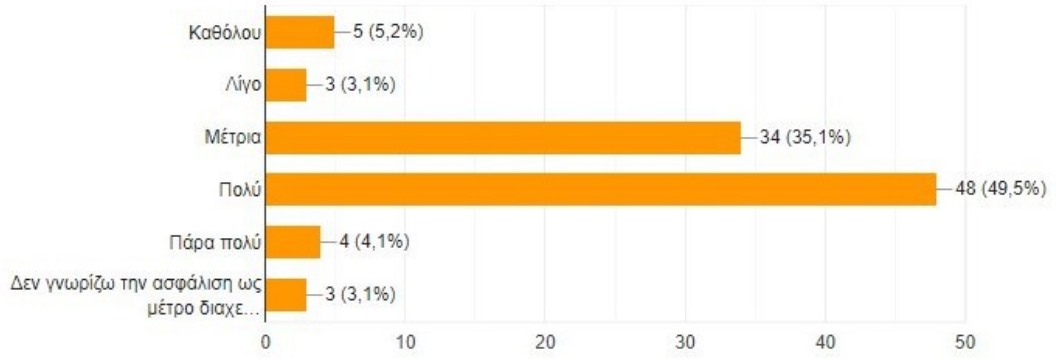
Διάγραμμα 13: Περιγραφή στατιστικών δείγματος Ερώτηση 9

Ερώτηση 10

Η τελευταία ερώτηση ζητούσε να βαθμολογήσουν κατά πόσο είναι διατεθειμένοι να προβούν σε ασφαλιστήριο συμβόλαιο με κάποια ασφαλιστική για να καλύψουν τις χρηματοοικονομικές τους επιπτώσεις και για να κάνουν χρήση των διαφόρων υπηρεσιών που παρέχουν. Οι 97 συμμετέχοντες απάντησαν:

Πίνακας 5: Απαντήσεις συμμετεχόντων στην ερώτηση 10

Ποσοστό (N)	**Καθόλου**	**Λίγο**	**Μέτρια**	**Πολύ**	**Πάρα πολύ**	**Δεν γνωρίζω την ασφάλιση ως μέτρο διαχείρισης του διαδικτυακού κινδύνου**
100% (97)	5,2% (5)	3,1% (3)	35,1% (34)	49,5% (48)	4,1% (4)	3,1% (3)



Διάγραμμα 14: Περιγραφή στατιστικών δείγματος Ερώτηση 10

ΚΕΦΑΛΙΑΟ 7

ΣΥΜΠΕΡΑΣΜΑΤΑ ΠΡΟΤΑΣΕΙΣ ΓΙΑ ΠΕΡΑΙΤΕΡΩ ΕΡΕΥΝΑ

7.1 Συμπεράσματα

Το ερωτηματολόγιο ακολουθεί μια νοητή σειρά ερευνητικών ερωτημάτων και με βάση τις απαντήσεις προκύπτουν τα εξής συμπεράσματα:

Οι συμμετέχοντες έχουν πολύ καλή ενημέρωση της έννοιας του διαδικτυακού κινδύνου, γνωρίζοντας ποιες είναι οι πιο συχνές απειλές, και γι' αυτό πιστεύουν ότι υπάρχει μεγάλη πιθανότητα τα ηλεκτρονικά τους δεδομένα που διατηρούν, να υποκλαπούν από κάποια επίθεση στα συστήματα των γραφείων ή των εταιριών τους. Ένα χρόνο μετά και αφού τέθηκε σε ισχύ ο νέος Ευρωπαϊκός Κανονισμός GDPR που αφορά την προστασία των προσωπικών δεδομένων, μόνο ένα μικρό ποσοστό δεν γνωρίζει και δεν συμμορφώνεται με τις διατάξεις αυτού.

Η πλειοψηφία μάλιστα είναι αυτοί που γνωρίζουν ότι η παραβίαση της ασφαλείας των πληροφοριών τους συνδέεται με τα άμεσα και έμμεσα χρηματοοικονομικά κόστη από την απώλεια προσωπικών δεδομένων. Μια τέτοια απειλή, μπορεί να είναι καταστροφική και να επηρεάσει την πτώση των εσόδων, τις σχέσεις με τους πελάτες αλλά και τους συνεργάτες, να ελαττώσει τις επειρηματικές ευκαιρίες, μέχρι και την επιχειρηματική συνέχεια.

Γι' αυτούς τους λόγους έχουν λάβει μέτρα προστασίας για τη διαχείριση του διαδικτυακού κινδύνου εκπαιδεύοντας το προσωπικό τους, καθώς υπάρχει ο κίνδυνος της αμέλειας ή φοβούμενοι τις κακόβουλες πράξεις των εργαζομένων τους, αλλάζοντας την πολιτική αντιμετώπιση επειδή μπορεί να υπάρχουν τρωτά σημεία στα λογισμικά συστήματα και ενισχύοντας τους αμυντικούς μηχανισμούς όπως firewalls, antivirus κτλ. για να αποφύγουν εξωτερικές επιθέσεις από χάκερς.

Τέλος αξίζει να σημειωθεί ότι ελάχιστοι είναι εκείνοι που δεν γνωρίζουν ή δεν είναι διατεθειμένοι να προχωρήσουν σε κάποιο ασφαλιστήριο συμβόλαιο. Οι περισσότεροι θέλουν πολύ, ενώ λίγο λιγότεροι είναι αυτοί που είναι επιφυλακτικοί και κλείνουν προς την απάντηση μέτρια, ίσως γιατί στην Ελλάδα και την Κύπρο δεν υπάρχουν πολλά κρούσματα ή ακόμα επειδή τα ασφαλιστήρια συμβόλαια είναι μία νέα μορφή αντιμετώπισης των κινδύνων και δεν υπάρχουν πολλές επιλογές που να ταιριάζουν στις ανάγκες του κάθε γραφείου.

7.2 Περιορισμοί Έρευνας

Οι περιορισμοί της Έρευνας είναι:

1. Ότι απευθυνθήκαμε αποκλειστικά σε λογιστικά γραφεία και ελεγκτικές εταιρίες της Κύπρου και μόνο σε αυτά που αναφέρονται στο μητρώο του ΣΕΛΚ
2. Ότι το ερωτηματολόγιο στάλθηκε σε 252 λογιστικά γραφεία, 50 ελεγκτικές εταιρίες και από αυτά απάντησαν τα 97.

7.3 Προτάσεις για περαιτέρω έρευνα

Η συμβολή των αποτελεσμάτων της έρευνας αυτής μπορεί να αποτελέσει κίνητρο για περαιτέρω στατιστική έρευνα, ακόμη μπορεί να γίνει μια συγκριτική ανάλυση με τις Εισηγμένες επιχειρήσεις στο ΧΑΑ.

ΒΙΒΛΙΟΓΡΑΦΙΑ

Βιβλία

Βαλχόπουλος Κωνσταντίνος, (2007), ηλεκτρονικό έγλημα: μορφές, πρόληψη, αντιμετώπιση, Νομική Βιβλιοθήκη, σελ. 129.

Λάζος Γρηγόρης (2001), Πληροφορική & Έκλημα, Νομική Βιβλιοθήκη, σελ.62.

Cebula, JJ and Young, LR (2010) Μια ταξινόμηση των λειτουργικών κινδύνων ασφάλειας Cyber. Τεχνική Σημείωση CMU / SEI-2010-TN-028, Ινστιτούτο Τεχνολογίας Λογισμικού, Πανεπιστήμιο Carnegie Mellon.

Schjoberg Stein (2008), The History of Global Harmonization on Cybercrime Legislation- The Road to Geneva.

Smith Russell G., Grabosky Peter N. and Urbas Gregor F. (2004) Cyber Criminals on Trial, Cambridge University Press, σελ 186.

Επιστημονικά άρθρα και μελέτες

Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, ενημερωτικό φυλλάδιο /asfaleia_sto_diadiktio_2016/asfaleia_2018/neos_kanonismos.pdf.

Νίκος Γεωργόπουλος cyRM,MBA by cyberinsurancegrecce (2016): Μικρές & Μεσαίες επιχειρήσεις και οι κίνδυνοι του Κυβερνοχώρου, https://www.cyberinsurancegreece.com/news/mikres-mesaies-epicheiriseis-kai-oi-kindynoi-toy-kyvernochoroy-toy-nikoy-georgopoyloy-cyrm-mba/, last accessed: 11 October 2016.

Νίκος Γεωργόπουλος, MBA,cyRM, Cyber Risks Advisor Cromar coverholder at Lloy's , It security, Issue T4403/04.2016.

Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης, L119/82 4 Μάιου 2016 , (Νομοθετικές πράξεις), ΚΑΝΟΝΙΣΜΟΣ (ΕΕ) 2016/679 ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για

την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων).

Σύνδεσμος Επιχειρήσεων και Βιομηχανιών (ΣΕΒ) Ο νέος Γενικός Κανονισμός για την Προστασία Δεδομένων (GDPR) Εφαρμογή και προκλήσεις για τις επιχειρήσεις στην εποχή της ψηφιοποίησης, Οκτώβριος 2018.

Υπουργείο Δικαιοσύνης, Διαδικτυακός τόπος διαβουλεύσεων, Νόμος για την Προστασία Δεδομένων Προσωπικού Χαρακτήρα σε εφαρμογή του Κανονισμού (ΕΕ) 2016/679, (2018), http://www.opengov.gr/ministryofjustice/?p=9331.

Accountancy Greece ΙΕΣΟΕΛ , τεύχος 27, Ασφάλεια στον Κυβερνοχώρο by BDO Netherlands, Απρίλιος/Μάϊος/Ιούνιος 2017.

AON plc Public limited company «Prepare for the expected: Safeguarding value in the era of cyber risk», Nextdeal newsroom, 12/9/2019 https://www.nextdeal.gr/asfalistikes-eidiseis/idiotiki-asfalisi/108471/aon.

Devon Milkovich, Γεγονότα και Στατιστικά Ασφαλούς Cyber Security Cybint, 3 Δεκεμβρίου 2018, https://www.cybintsolutions.com/cyber-security-facts-stats.

Enisa (European Network and Information Security Agency),Ασφάλεια και προστασία προσωπικών δεδομένων, Δελτίο τύπου, 13 Ιουνίου 2019, https://www.enisa.europa.eu/news/enisa-news/security-and-privacy.

Enisa (European Network and Information Security Agency), EU cybersecurity act enters into force, Δελτίο τύπου, 26 Ιουνίου 2019.

Enisa (European Network and Information Security Agency), ενημερωμένη έκδοση των παραδοσιακών του «Κρατικών Εκθέσεων» σχετικά με την ασφάλεια των δικτύων και των πληροφοριών (NIS) των κρατών μελών και άλλων ευρωπαϊκών χωρών, Ετήσια έκθεση, 15 Ιουλίου 2019.

Indernational Journal of Computer Sience and I ndernational Security (IJCSIS) Vol 17, No 5, May 2019.

International Journal of Network Security, Vol 21, No.1, PP166-17, Jan.2019 (DOI:106633/iJNS.201901 21(1).21).

Internet Security Threat Report (ISTR) Volume 24, February 2019.

Journal of Advances in Mathematics and Computer Science 31(2): 1-99,2019 article no.JAMCS, 47754.

Journal of Physical Sciences, Vol.24,2019, 133-141.

Market Insights from the world of Lloyd's, Market magazine, (2012): Πως πρέπει να αντιμετωπίσει η αγορά τον κίνδυνο στον κυβερνοχώρο, https:// insuranceworld.gr/13522/archive.

Ηλεκτρονικές πηγές

http://bb-insurance.gr

https://cybersecuritymonth.eu

https://www.datalossdb.gr

https://www.dpa.gr

https://etl.enisa.europa.eu/

http://www.enisa.europa.eu/act/it/pat

https://ec.europa.eu/dgs/home-affairs/what-we-do/policies/organized-crime-and-human-traggicking/cybercrime/index_en.htm

https://www.interasco.gr

htpps://www.isaca.org/pages/default.aspx

htpps://www.iso.org/home.html

https://legislation.gov.uk

https://www.lloyds.com/riskindex

https://www.niriis.gr/gdpr/katigories-prosopikon-dedomenon/

http://www.opengov.gr

https://privacyadvocate.gr

htpps://www.rims.org/Pages/Default.aspx

https://securitycenter.sonicwall.com

https://threatmap.bitdefender.com

https://en.wikipedia.org/wiki/Computer_Fraud_and_Abuse_Act#Protecterd_computer

ΠΑΡΑΡΤΗΜΑ

ΜΟΡΦΗ ΕΡΩΤΗΜΑΤΟΛΟΓΙΟΥ

Ερώτηση 1

Κατά πόσο γνωρίζετε την έννοια του διαδικτυακού κινδύνου;

(1) Καθόλου (2) Λίγο (3) Μέτρια (4) Πολύ (5) Πάρα πολύ

Ερώτηση 2

Σε ποιο βαθμό πιστεύετε ότι τα ηλεκτρονικά δεδομένα (επιχειρηματικά και προσωπικά) που διατηρείτε ως γραφείο μπορούν να απειλούνται από τους διαδικτυακούς κινδύνους;

(1) Καθόλου (2) Λίγο (3) Μέτρια (4) Πολύ (5) Πάρα πολύ

Ερώτηση 3

Αξιολογείστε τους παρακάτω κινδύνους, που αποτελούν αιτίες απώλειας και διαρροής δεδομένων και μπορεί να διατρέχετε ως λογιστικό γραφείο-ελεγκτική εταιρία.

1.Αμέλεια εργαζομένων

2.Κακόβουλες πράξεις εργαζομένων

3.Εξωτερικές επιθέσεις από χάκερς

4.Τρωτά σημεία λογισμικού συστήματος

Ερώτηση 4

Κατά πόσο είστε ενημερωμένοι για τον νέο Ευρωπαϊκό Κανονισμό GDPR (5419/16), που αφορά την προστασία προσωπικών δεδομένων;

(1) Καθόλου (2) Λίγο (3) Μέτρια (4) Πολύ (5) Πάρα πολύ

Ερώτηση 5

Ερώτηση 5: Κατά πόσο έχετε συμμορφωθεί με τις διατάξεις του νέο Ευρωπαϊκού Κανονισμού GDPR (5419/16), που αφορά την προστασία προσωπικών δεδομένων;

(1) Καθόλου (2) Λίγο (3) Μέτρια (4) Πολύ (5) Πάρα πολύ

Ερώτηση 6: Σε ποιο βαθμό θεωρείτε ότι η παραβίαση της ασφάλειας των πληροφοριών του γραφείου σας συνδέεται με χρηματοοικονομικές απώλειες;

(1) Καθόλου (2) Λίγο (3) Μέτρια (4) Πολύ (5) Πάρα πολύ

Ερώτηση 7

Αξιολογείστε τα παρακάτω κόστη που μπορεί να διατρέχετε ως λογιστικό γραφείο.

1.Άμεσα χρηματοοικονομικά κόστη

2.Μείωση της φήμης και την αξιοπιστίας του γραφείου

3.Πτώση των εσόδων

4.Χαμηλές επιχειρηματικές ευκαιρίες

5.Επηρεασμός των σχέσεων με τους πελάτες

6.Επηρεασμός των σχέσεων με τους συνεργάτες

7.Επιχειρηματική συνέχεια

Ερώτηση 8

Έχετε λάβει μέτρα προστασίας για την διαχείριση του διαδικτυακού κινδύνου;

(1) Ναι (2) Όχι

Ερώτηση 9

Επιλέξτε ποια από τα παρακάτω μέτρα χρησιμοποιείτε για την πρόληψη και μετριασμό του διαδικτυακού δικτύου;

(1) Εκπαίδευση του προσωπικού για ευαισθητοποίηση σε θέματα ασφαλείας

(2) Πολιτική για την ασφάλεια και αντιμετώπιση των περιστατικών

(3) Τεχνολογικά μέτρα π.χ. κρυπτογράφηση

(4) firewalls, antispyware, antivirus λογισμικά

Ερώτηση 10

Σε ποιό βαθμό είστε διατεθειμένοι να προβείτε σε ασφαλιστήριο συμβόλαιο με κάποια ασφαλιστική για να καλύψετε τις χρηματοοικονομικές σας επιπτώσεις και για να κάνετε χρήση των διαφόρων υπηρεσιών που παρέχουν;

(1)Καθόλου (2)Λίγο (3)Μέτρια (4)Πολύ (5) Πάρα πολύ

(6) Δεν γνωρίζω την ασφάλιση ως μέτρο διαχείρισης του διαδικτυακού κινδύνου