Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μεταπτυχιακό Πρόγραμμα Σπουδών

Ασφάλεια Υπολογιστών και Δικτύων

Μεταπτυχιακή Διατριβή

Ετοιμότητα για την Ασφάλεια στον Κυβερνοχώρο στις Μικρές και Μεσαίες Επιχειρήσεις στη Κυπρο

Αντώνιος Κουτρώτσιος

Επιβλέπων Καθηγητής
Αδαμαντίνη Περατικού

Δεκέμβριος 2019

Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μεταπτυχιακό Πρόγραμμα Σπουδών

Ασφάλεια Υπολογιστών και Δικτύων

Μεταπτυχιακή Διατριβή

Ετοιμότητα για την Ασφάλεια στον Κυβερνοχώρο στις Μικρές και Μεσαίες Επιχειρήσεις στη Κυπρο

Αντώνιος Κουτρώτσιος

Επιβλέπων Καθηγητής
Αδαμαντίνη Περατικού

Η παρούσα μεταπτυχιακή διατριβή υποβλήθηκε
προς μερική εκπλήρωση των απαιτήσεων για απόκτηση
μεταπτυχιακού τίτλου σπουδών

στην Ασφάλεια Υπολογιστών και Δικτύων

από τη Σχολή Θετικών και Εφαρμοσμένων Επιστημών
του Ανοικτού Πανεπιστημίου Κύπρου.

Δεκέμβριος 2019

Περίληψη

Σκοπός της παρούσας διατριβής είναι να μελετήσει την ετοιμότητα για την ασφάλεια στον κυβερνοχώρο των μικρών και μεσαίων επιχειρήσεων στην Κυπρο. Αρχικά γίνεται λόγος για τις αρχές της ασφάλειας πληροφοριών, οι οποίες αποτελούν μέρος της ασφάλειας μιας επιχείρησης, καθώς και τι θεωρείται μικρομεσαία επιχείρηση σύμφωνα με την Ευρωπαϊκή Ένωση. Στην συνέχεια παρουσιάζονται οι δέκα κορυφαίες απειλές που δέχονται οι μικρομεσαίες επιχειρήσεις στον κυβερνοχώρο τη σήμερον ημέρα, όπως επίσης και νέες τεχνολογίες που χρησιμοποιούνται από τις επιχειρήσεις, όπως το cloud computing και BYOD, οι οποίες εισάγουν νέες απειλές.

Εν συνεχεία, στην παρούσα διατριβή γίνεται λόγος και για την διαχείριση της ασφάλειας πληροφοριών, όπως είναι έλεγχοι διαχείρισης ασφάλειας πληροφοριών, οι οποίοι αποτελούνται από τρία πεδία, την διοικητική, την τεχνική και την φυσική ασφάλεια. Όλες οι επιχειρήσεις πρέπει να κατανοήσουν τους κινδύνους που σχετίζονται με την ασφάλεια τους αλλά και να συμμορφώνονται με τις άμεσες ή έμμεσες απαιτήσεις της. Για τον λόγο αυτό, μελετήθηκε η διακυβέρνηση, η διαχείριση κίνδυνου, όπως και η συμμόρφωση των επιχειρήσεων. Επίσης, γίνεται λόγος για το τι είναι πλαίσια, μοντέλα και πρότυπα που μπορούν ακολουθήσουν ή να αποκτήσουν οι επιχειρήσεις, καθώς και τα συστήματα διαχείρισης ασφάλειας, τα οποία έχουν ως ρόλο να προστατεύουν τα κρίσιμα πληροφοριακά περιουσιακά στοιχεία και δεδομένα της επιχείρησης από απειλές των αρχών της ασφάλειας πληροφοριών. Στη συνέχεια, γίνεται αναφορά στο General Data Protection Regulation (GDPR), το οποίο αποτελεί τον νέο σκληρό νομό της Ευρωπαϊκής Ένωσης σε σχέση με την ιδιωτικότητα και την ασφάλεια.

Τέλος, αναφέρεται η μεθοδολογία που ακολουθήθηκε για την έρευνα, την συλλογή δεδομένων, παρουσιάζονται τα αποτελέσματα του ερωτηματολογίου που συντάχθηκε και συμπληρώθηκε με σκοπό την ερευνά της ετοιμότητας της ασφάλειας των μικρομεσαίων επιχειρήσεων της Κύπρου στον κυβερνοχώρο, καθώς επίσης συντάχθηκε ένας οδηγός για την προετοιμασία των μικρομεσαίων επιχειρήσεων στον κυβερνοχώρο.

Summary

The main objective of this dissertation is to study cybersecurity preparedness for small and medium businesses in Cyprus. Firstly, are mentioned the three principles of security, which are part of business security, as well as what is considered a small and medium sized business according to the European Union. Following are the top ten threats that small to medium sized businesses face today, as well as new technologies used by businesses, such as cloud computing and BYOD, that introduce new threats.

This dissertation deals with information security management, such as information security controls, which fall under three domains, administrative, technical and physical. All businesses must understand the risks associated with their security but also comply with direct and indirect requirements. For this reason, in this dissertation we study the governance, risk management and compliance, along with frameworks, models and standards that can be followed or acquired by businesses. Also, we study security management systems, which have the role of protecting critical business information and data from threats to security principles. Following is the reference to the General Data Protection Regulation (GDPR), which is the European Union's new law on privacy and security.

Finally, are presented the methodology followed for the survey, data collection, the results of the questionnaire that completed with the main objective of investigating the cybersecurity preparedness of small to medium sized businesses in Cyprus, also a guide was written for preparing the small and medium businesses in cyberspace.

Ευχαριστίες

Θα ήθελα να ευχαριστώ την οικογένεια μου για την αμέριστη συμπαράσταση και υποστήριξη. Επίσης, θα ήθελα να ευχαριστώ την επιβλέπουσα καθηγήτρια Αδαμαντίνη Περατικού για την πολύτιμη βοήθεια της. Τέλος, πρέπει να ευχαριστήσω όλους όσους συνέβαλαν στην σωστή συμπλήρωση του ερωτηματολογίου.

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

Ευρετήριο Εικόνων και Πινάκων

Εικόνες

Πίνακες

ΚΕΦΑΛΑΙΟ 1
Εισαγωγή

Την σημερινή εποχή όπου όλα περιστρέφονται γύρο από το διαδίκτυο, η ασφάλεια των υπολογιστών και δικτύων έχει πρωταγωνιστικό ρολό. Οι επιχειρήσεις πλέον χρησιμοποιούν ολοένα και περισσότερο το διαδίκτυο, έτσι η ανάγκη για την ασφάλεια τους αυξάνεται. Παρόλο που ορισμένες παγκοσμίου φάσματος επιχειρήσεις διαθέτουν τις απαραίτητες ικανότητες και πόρους για την ανάπτυξη και τη διατήρηση της παρουσίας τους στο κυβερνοχώρο, καθώς και την εξασφάλιση της ασφάλειας των επιχειρησιακών δεδομένων, υπάρχουν πολλές μικρομεσαίες επιχειρήσεις που είτε ευσυνείδητα είτε ασυνείδητα παραμελούν την κρισιμότητα της ασφάλειας στο κυβερνοχώρο.

Η έννοια της χρήσης του διαδικτύου στην επιχειρησιακή τεχνολογία είναι σχετικά νέα και ανεξερεύνητη επικράτεια στη Κύπρο. Υπάρχουν πολλά θετικά από τη χρήση του διαδικτύου σε επιχειρήσεις, υπάρχουν όμως και πιθανοί κίνδυνοι που μπορεί να αντιμετωπίσουν. Οι κίνδυνοι αυτοί μπορεί να είναι καταστροφικοί για την επιχείρηση αν δεν ληφθούν κατάλληλα μέτρα ασφάλειας.

Ο σκοπός αυτής της διατριβής είναι να ερευνήσει την ετοιμότητα των μικρομεσαίων επιχειρήσεων στην Κυπρο στον κυβερνοχώρο. Η ασφάλεια στον κυβερνοχώρο είναι ζωτικής σημασίας καθώς διακυβεύονται σημαντικά δεδομένα σε περίπτωση μιας επίθεσης.

Οι μικρομεσαίες επιχειρήσεις παγκοσμίως, συχνά πιστεύουν ότι δύσκολα μπορούν να πέσουν θύμα επιθέσεων στον κυβερνοχώρο λόγω του μεγέθους τους. Στο παρελθόν, η στάση αυτή μπορεί να ήταν βιώσιμη για τις επιχειρήσεις λόγω της μικρής διείσδυσης του διαδικτύου στον κόσμο. Ωστόσο, την σημερινή εποχή είναι κατανοητό ότι μια μικρή ή μεσαία

επιχείρηση είναι ελκυστικός στόχος λόγω του ότι ο επιτιθέμενος περιμένει ότι μια επιχείρηση με μικρή χρηματοδότηση δεν θα έχει επενδύσει στην ασφάλεια της. Οι επιπτώσεις μιας κυβερνοεπίθεσης μπορεί να είναι τρομακτικές για μια επιχείρηση, όπως ακόμα και τους πελάτες της, καθώς μπορεί να διαρρεύσουν ευαίσθητα προσωπικά δεδομένα τους.

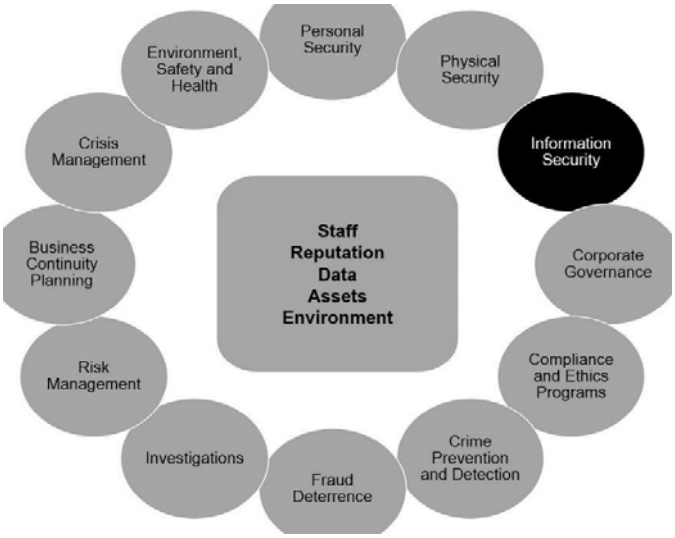
Τέλος, οι μικρομεσαίες επιχειρήσεις θα πρέπει να ευθυγραμμιστούν με διεθνείς κανόνες και οδηγίες ασφάλειας ώστε να αποκτήσουν μεγαλύτερη ασφάλεια στον κυβερνοχώρο.

ΚΕΦΑΛΑΙΟ 2
Κυβερνοασφάλεια για Μικρές και Μεσαίες Επιχειρήσεις

Όλες οι επιχειρήσεις χρησιμοποιούν πληροφορίες - π.χ. πληροφορίες για τους εργαζόμενους τους, φορολογικές πληροφορίες, πληροφορίες πελατών κ.α. Οι πληροφορίες είναι ζωτικής σημασίας για την λειτουργία μιας επιχείρησης. Αν οι πληροφορίες αυτές παραβιαστούν ή αλλοιωθούν με κάποιο τρόπο, η επιχείρηση ίσως να μην μπορεί να λειτουργήσει άλλο. Η προστασία αυτών των πληροφοριών που η επιχείρηση δημιουργεί, χρησιμοποιεί και αποθηκεύει ονομάζεται Ασφάλεια Πληροφοριών.

2.1 Η Ασφαλεια Πληροφοριων ειναι Μερος της Ασφαλειας της Επιχειρησης

Η ασφάλεια πληροφοριών αποτελεί μέρος της ασφάλειας μιας επιχείρηση όπως βλέπουμε στην παρακάτω Εικόνα 1. Ο σκοπός της επιχειρησιακής ασφάλειας είναι η διαχείριση της ασφάλειας, η ομαλή λειτουργία και η προστασία της επιχείρησης. Τα τμήματα που πρέπει να ληφθούν υπόψη μπορεί να διαφέρουν μεταξύ των επιχειρήσεων αλλά η διακυβέρνηση της ασφάλειας στο σύνολο της αποτελεί σημαντική πτυχή της επιχειρησιακής διαχείρισης, καθώς προστατεύει το προσωπικό, την φήμη, τα δεδομένα, τα περιουσιακά στοιχεία και το περιβάλλον που λειτουργεί η επιχείρηση.



Εικόνα 1 Τμήματα της ασφάλειας επιχειρήσεων

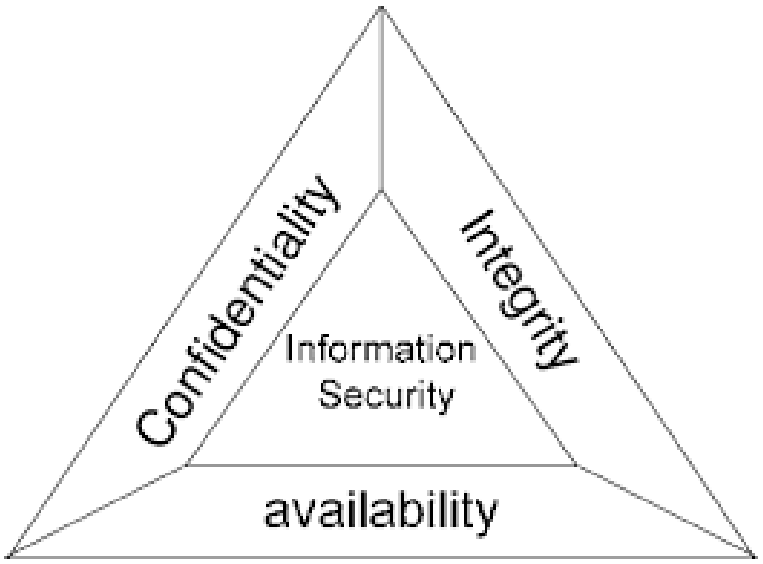
Ο ρόλος της ασφάλειας πληροφοριών είναι να διατηρεί όλα τα δεδομένα και τα συστήματα ασφαλή από παράγοντες που θα προσπαθήσουν να τα εκμεταλλευτούν ή να κάνουν κακή χρήση τους, όπως επίσης να τα προστατεύσει και από φυσικές καταστροφές.

Η ασφάλεια πληροφοριών πρέπει να λαμβάνει υπόψη ένα ευρύ φάσμα πιθανών κινδύνων και να παρέχει όλα τα μέσα για την προστασία και την ασφάλεια ενάντια των κινδύνων αυτών. Τη σήμερον ημέρα, οι κίνδυνοι δεν αφορούν αποκλειστικά φυσικά πράγματα όπως τα δίκτυα ή τα υπολογιστικά συστήματα αλλά και την πνευματική ιδιοκτησία, όπως είναι τα δεδομένα και ο πηγαίος κώδικας.

2.2 Αρχες της Ασφαλειας Πληροφοριων

Η ασφάλεια πληροφοριών στηρίζεται σε τρεις βασικές απαιτήσεις, οι οποίες αναφέρονται ως το τρίγωνο C.I.A (Confidentiality, Integrity, Availability)[1]. Το τρίγωνο αυτό θεωρείται

κοινή γνώση και είναι απαραίτητο για την ανάπτυξη πολιτικής ασφάλειας. Αποτελείται από τρία μέρη που σε κάθε ασφαλές σύστημα θα πρέπει να διασφαλίζεται η ύπαρξη τους. Εάν κάποιο τμήμα τους τρίγωνου παραβιαστεί, ίσως υπάρξουν σοβαρές συνέπειες, παρότι από πολλούς ειδικούς ασφάλειας θεωρείται πλέον ότι είναι μια περιορισμένη άποψη της ασφάλειας αλλά συνεχίζει να αποτελεί ένα καλό σημείο εκκίνησης.



Εικόνα 2 Η τριάδα CIA [42]

2.2.1 Εμπιστευτικοτητα (Confidentiality)

Η εμπιστευτικότητα έχει να κανει με την προστασία της ιδιωτικότητας των πληροφοριών και πολλές φορές εφαρμόζεται σε πολλά επίπεδα μιας διαδικασίας. Η εμπιστευτικότητα παραβιάζεται όταν κάποιος υποκλέπτει πληροφορίες οι οποίες δεν προορίζονται για αυτόν. Τέτοιες παραβιάσεις μπορούν να συμβούν όταν κάποιος βλέπει κάποιον άλλο να πληκτρολογεί τον κωδικό του ή κάποιος κλέβει ένα λάπτοπ. Μπορεί επίσης να περιλαμβάνει αθέλητες παραβιάσεις, όπως όταν ένα μήνυμα ηλεκτρονικού ταχυδρομείου αποστέλλεται σε λάθος παραλήπτη [1].

Η διαχείριση της εμπιστευτικότητας είναι συνήθως έργο του Συστήματος Διαχείρισης Ασφάλειας των Πληροφοριών (ISMS). Οι εργασίες του συστήματος αυτού συνήθως

περιλαμβάνουν την διαχείριση των δικαιωμάτων αρχείων, έλεγχο πρόσβασης και κρυπτογράφηση αρχείων.

2.2.2 Ακεραιοτητα (Integrity)

Η ακεραιότητα αφορά την διαχείριση των δεδομένων προστατεύοντας τα από το να αλλαχτούν χωρίς άδεια. Αυτό συνεπάγεται ότι τα δεδομένα πρέπει να προστατεύονται ακόμα και από εγκεκριμένες αλλά μη επιθυμητές αλλαγές ή διαγραφές. Ένα καλό σύστημα διαχείρισης πληροφοριών θα πρέπει να είναι ικανό να περιορίζει την πρόσβαση και τις ενέργειες μη εξουσιοδοτημένων χρηστών και να διαθέτει την ικανότητα να αντιστρέφει τις ανεπιθύμητες ενέργειες από τους εξουσιοδοτημένους χρήστες [1].

Συνήθεις λύσεις τεχνικού επιπέδου σε ζητήματα ακεραιότητας περιλαμβάνουν περιορισμένα δικαιώματα αρχείων, σημαίες μόνο ανάγνωσης για αρχεία, συστήματα ελέγχου εκδόσεων και αντιγράφων ασφαλείας. Μια τυπική επίθεση στην ακεραιότητα είναι η υποκλοπή ενός αρχείου, η πραγματοποίηση αλλαγών σε αυτό και στην συνέχεια η επαναπροώθηση του στον δέκτη για τον οποίον προοριζόταν.

2.2.3 Διαθεσιμοτητα (Availability)

Η διαθεσιμότητα αφορά τη δυνατότητα πρόσβασης στα δεδομένα όταν χρειάζεται. Ο στόχος της ασφαλείας πληροφοριών είναι να εξασφαλιστεί η πρόσβαση σε δεδομένα που βρίσκονται ακόμα και σε συστήματα που έχουν προβλήματα. Αυτό σημαίνει ότι οι πελάτες μπορούν να έχουν πρόσβαση σε μια ιστοσελίδα ακόμα και όταν αυτή δέχεται επίθεση άρνησης εξυπηρέτησης (DoS attack). Μπορεί επίσης να σημαίνει ότι οι εργαζόμενοι σε μια επιχείρηση έχουν πρόσβαση στα δεδομένα ακόμα και όταν υπάρχει διακοπή ρεύματος [1].

2.3 ΜΙΚΡΟΜΕΣΑΙΕΣ ΕΠΙΧΕΙΡΗΣΕΙΣ

Δεν υπάρχει ακριβής ορισμός στο τι είναι μικρομεσαία επιχείρηση. Η Ευρωπαϊκή Επιτροπή, η οποία είναι θεσμικό όργανο της Ευρωπαϊκής Ένωσης με απώτερο σκοπό την προστασία των κοινοτικών συμφερόντων των κρατών μελών της Ένωσης, ανέπτυξε μερικά κριτήρια στα οποία μπορεί να οριστεί μια μικρομεσαία επιχείρηση. Τα κριτήρια αυτά είναι ο αριθμός υπάλληλων, ο κύκλος εργασιών (τζίρος) και ο ισολογισμός μιας επιχείρησης.

Σύμφωνα λοιπόν με την Ευρωπαϊκή Επιτροπή, μικρομεσαία επιχείρηση θεωρείται η επιχείρηση που απασχολεί λιγότερους από 250 υπαλλήλους, έχει κύκλο εργασιών έως 50 εκατομμύρια ευρώ και ο ισολογισμός της επιχείρησης δεν ξεπερνάει τα 43 εκατομμύρια ευρώ. Όπως βλέπουμε στον παρακάτω πίνακα, η Ευρωπαϊκή Επιτροπή κατηγοριοποιεί τις μικρομεσαίες επιχειρήσεις σε τρεις υποκατηγορίες [2].

Πίνακας 1 Κατηγορίες μικρομεσαίων επιχειρήσεων

Κατηγορίες Επιχείρησης	**Υπάλληλοι**	**Κύκλος Εργασιών**	**Ισολογισμός**
Μεσαίες	< 250	≤ € 50 εκ	≤ € 43 εκ
Μικρές	< 50	≤ € 10 εκ	≤ € 10 εκ
Πολύ μικρές	< 10	≤ € 2 εκ	≤ € 2 εκ

2.4 ΜΙΚΡΟΜΕΣΑΙΕΣ ΕΠΙΧΕΙΡΗΣΕΙΣ ΚΑΙ ΑΣΦΑΛΕΙΑ

Για να καθορίσουμε μέτρα ασφάλειας πληροφοριών , πρώτα πρέπει να καθορίσουμε τι μπορεί να επηρεαστεί από τις απειλές ασφάλειας. Όροι όπως περιουσιακό στοιχείο (asset), απειλή (threat) και ευπάθεια (vulnerability) χρησιμοποιούνται συχνά σε μελέτες ασφάλειας

της πληροφορικής. Ο παρακάτω πίνακας περιγράφει αυτές τις εννοείς γύρω από την ασφάλεια για καλύτερη κατανόηση.

Πίνακας 2 Περιγραφή Περιουσιακού Στοιχείου, Ευπάθειας και Απειλής

Λέξεις Κλειδιά	**Περιγραφή**
Περιουσιακό Στοιχείο	Σύμφωνα με το ISO 27005 [3], περιουσιακό στοιχείο θεωρείται οτιδήποτε έχει αξία ή σημασία για μια επιχείρηση. Τα περιουσιακά στοιχεία μπορεί να είναι διάφορων ειδών. Μπορεί να είναι κτίρια, ηλεκτρονικοί υπολογιστές, κώδικας, βάσεις δεδομένων, εργαλεία ανάπτυξης εφαρμογών, πνευματική ιδιοκτησία. Ακόμα και η φήμη θεωρείται πολύτιμο περιουσιακό στοιχείο για μια επιχείρηση [4].
Ευπάθεια	Ευπάθεια ορίζεται ως μια αδυναμία σε ένα περιουσιακό στοιχείο, η οποία μπορεί να δώσει την ευκαιρία να την εκμεταλλευτεί και να υποστεί κάποια ζημιά από μια απειλή[3].
Απειλή	Μια απειλή μπορεί να είναι μια πιθανή αιτία η οποία μπορεί να μετατραπεί σε ένα ανεπιθύμητο περιστατικό που προκαλεί βλάβη σε μια επιχείρηση [4].

2.5 Απειλες Ασφαλειας

Οι μικρομεσαίες επιχειρήσεις αντιμετωπίζουν εσωτερικές και εξωτερικές απειλές όπως και οι μεγαλύτερες επιχειρήσεις. Δυστυχώς, οι περισσότερες μικρομεσαίες επιχειρήσεις δυσκολεύονται στο να συμβαδίσουν με τις τεχνολογικές εξελίξεις για πολλούς και διάφορους λόγους, το οποίο σημαίνει ότι μένουν πίσω και στον τομέα της ασφάλειας, καθώς όσο εξελίσσεται η τεχνολογία, εξελίσσονται και οι απειλές στον τομέα της ασφάλειας λόγω του ότι είναι άρρηκτα συνδεδεμένες [5]. Συνήθως οι μικρομεσαίες επιχειρήσεις έχουν ένα βασικό επίπεδο ασφάλειας, το οποίο συνήθως σημαίνει ότι χρησιμοποιούν ένα anti-virus πρόγραμμα και firewall.

Όπως προαναφέρθηκε το τοπίο στην ασφάλεια εξελίσσεται συνεχώς και θα πρέπει να αρχίσουν όλες οι μικρομεσαίες επιχειρήσεις να λαμβάνουν σοβαρότερα μέτρα ασφαλείας. Για παράδειγμα, zero day ιοί, οπού ήταν προηγούμενος άγνωστοι καθώς δεν είχαν antivirus signature, αυξήθηκαν από μερικές χιλιάδες που ήταν την προηγουμένη δεκαετία σε εκατοντάδες χιλιάδες. Ο αριθμός των επιθέσεων συνεχίζει να αυξάνεται με εκθετικό ρυθμό. Βέβαια μπορεί να αυξάνεται ο αριθμός των επιθέσεων, ωστόσο οι πραγματικοί τύποι απειλών παραμένουν στα ίδια επίπεδα.

Οι διαδικτυακές απειλές περιλαμβάνουν spam, phishing, ιούς, rootkits και διάφορα είδη malware. Η διαφορά σήμερα με το παρελθόν είναι η αλλαγή στην φιλοσοφία των επιθέσεων και στον αριθμό συσκευών και υπηρεσιών που επηρεάζονται. Τα malwares συγκεκριμένα έχουν γίνει ένα πολύ σοβαρό πρόβλημα για τις επιχειρήσεις, καθώς επηρεάζουν πολλαπλές συσκευές. Δεν έχουν αλλάξει μόνο οι επιθέσεις τη σήμερον ημέρα αλλά και αυτοί που είναι πίσω από αυτές τις επιθέσεις. Στο παρελθόν ένας hacker συνήθως κυνηγούσε την αναγνώριση αλλά πλέον αυτό έχει αλλάξει. Σήμερα, οι κυβερνοεγκληματίες στοχεύουν σε οικονομικά οφέλη και είναι περισσότερο οργανωμένοι. Το επίπεδο οργάνωσης τους προκαλεί μεγάλη ανησυχία καθώς για να μπορέσουν να έχουν τέτοιο επίπεδο οργάνωσης σημαίνει ότι έχουν πολλούς πόρους.

Σύμφωνα με την έρευνα του US State of Cybercrime [6], οι μικρομεσαίες επιχειρήσεις άθελα τους αυξάνουν τις απειλές, οι οποίες αυξάνουν τις ευπάθειες, απλά υιοθετώντας διαφορετικά πληροφοριακά συστήματα. Οι πιο συνηθισμένες τάσεις στις ευπάθειες είναι η αυξανομένη χρήση των κινητών συσκευών, η αποθήκευση δεδομένων στο cloud, η ψηφιοποιήση ευαίσθητων δεδομένων, η κοινωνική συνεργασία, η μετάβαση σε τεχνολογίες έξυπνων δικτύων και η υιοθέτηση ενναλακτικών λύσεων για την κινητικότητα των υπάλληλων μιας επιχείρησης.

Η εταιρία WatchGuard έχει παρουσιάσει μια λίστα με απειλές ασφαλείας οι οποίες πιστεύει ότι είναι οι πιο επικίνδυνες για τις μικρομεσαίες επιχειρήσεις στις Ηνωμένες Πολιτείες Αμερικής [7]. Η εταιρία αυτή παρέχει επαγγελματική καθοδήγηση και υποστήριξη σε ένα μεγάλο αριθμό πελατών από τους οποίους οι περισσότεροι είναι μικρομεσαίες επιχειρήσεις. Η WatchGuard παρακολουθεί καθημερινός για καινούργιες απειλές ασφαλείας, με ιδιαίτερη έμφαση σε προβλήματα που επηρεάζουν τις μικρομεσαίες επιχειρήσεις, αυτό κανει την έρευνα της εταιρίας πολύτιμη, καθώς δεν υπάρχουν πολλές έρευνες που να επικεντρώνονται στην καταγραφή των απειλών στις μικρομεσαίες επιχειρήσεις. Βέβαια, υπάρχει και η έρευνα «The Verizon Data Breach Investigations Reports 2019» [9] η οποία αναλύει πάνω από 2000 επιβεβαιωμένες παραβιάσεις δεδομένων και δείχνει παρόμοιες απειλές με την έρευνα της WatchGuard. Ωστόσο, η έρευνα της Verizon για τις παραβιάσεις δεδομένων δεν βασίζεται σε απειλές που υπάρχουν μόνο στις μικρομεσαίες επιχειρήσεις καθώς η έρευνα βασίζεται σε πάνω από 50 διεθνείς οργανισμούς κυβερνοασφάλειας, έτσι το δείγμα είναι περιορισμένο και όχι τυχαίο όπως την έρευνα της WatchGuard. Επίσης η έρευνα της WatchGuard περιγράφει και μέτρα προστασίας από αυτές τις απειλές που περιγράφει η έρευνα της. Οι απειλές ασφαλείας της έρευνας περιγράφονται παρακάτω.

2.5.1 Αυτοματη Εκμεταλλευση μιας Γνωστης Ευπαθειας

Οι συγκεκριμένες επιθέσεις είναι μη στοχευμένες, διότι οι επιθέσεις αυτές προσπαθούν να διακυβευθεί το λειτουργικό σύστημα σε έναν ηλεκτρονικό υπολογιστή μέσο οποιασδήποτε

γνωστής ευπάθειας. Οι πιο πολλές αυτόματες επιθέσεις προσπαθούν να εκμεταλλευτούν ευπάθειες του λειτουργικού συστήματος Windows. Συνήθως αυτές οι επιθέσεις πραγματοποιούνται όταν δεν έχουν γίνει εγκατάσταση όλες οι απαραίτητες ενημερώσεις του λειτουργικού συστήματος. Πολλές φορές οι μικρές και μεσαίες επιχειρήσεις παραμελούν την άμεση εγκατάσταση των ενημερώσεων, είτε λόγο του μικρού αριθμού υπάλληλων στην μηχανογράφηση είτε γιατί έχουν άγνοια. Οπότε το κύριο περιουσιακό στοιχείο που θα διακυβευθεί είναι το λειτουργικό σύστημα των ηλεκτρονικών υπολογιστών της επιχείρησης [15].

Για να αποφευχθούν οι συγκεκριμένες επιθέσεις, οι μικρομεσαίες επιχειρήσεις συνίσταται να χρησιμοποιούν ειδικό λογισμικό το οποίο θα σαρώνει το δίκτυο και θα αναγνωρίζει τις ενημερώσεις που λείπουν από τα λειτουργικά συστήματα των υπολογιστών και θα διανέμει τις απαραίτητες ενημερώσεις μέσο μιας κεντρικής κονσόλας ώστε όλο το δίκτυο της επιχειρήσεις να είναι ενημερωμένο. Επίσης θα μπορούσαν οι επιχειρήσεις να εκπαιδεύσουν τους υπαλλήλους της ώστε να είναι σε θέση να ενημερώνουν τα λειτουργικά συστήματα οι ίδιοι [7].

2.5.2 Κακόβουλα HTML Email

Αυτός ο τύπος επίθεσης καταφθάνει ως ένα μήνυμα ηλεκτρονικού ταχυδρομείου HTML που συνδέεται με έναν κακόβουλο ιστότοπο που κρύβει πολλές παγίδες. Όταν ο χρήστης πατήσει πάνω στον σύνδεσμο, είτε ηθελημένα είτε άθελα του, ξεκινάει μια διαδικασία αυτόματης λήψης και εκτέλεσης ενός exploit από τον συγκεκριμένο ιστότοπο [10].

Το κύριο περιουσιακό στοιχείο της επιχείρησης που πλήττεται είναι: οι ηλεκτρονικοί υπολογιστές, κινητά τηλέφωνα και γενικά οποία συσκευή μπορεί να λάβει και να ανοίξει τα κακόβουλα μηνύματα ηλεκτρονικού ταχυδρομείου. Για να αποφύγει να λαμβάνει τέτοιου είδους μηνύματα ηλεκτρονικού ταχυδρομείου, η επιχείρηση θα πρέπει να εφαρμόσει ένα επιθετικό φιλτράρισμα ανεπιθύμητων μηνυμάτων, ώστε να μην εμφανίζονται στα

εισερχόμενα μηνύματα των χρηστών. Επίσης είναι αναγκαία και η ευαισθητοποίηση των εργαζομένων γύρω από την ασφάλεια του ηλεκτρονικού ταχυδρομείου μέσω περιοδικής εκπαίδευσης τους, ώστε να είναι σε θέση να ξεχωρίσουν ένα ανεπιθύμητο μήνυμα ηλεκτρονικού ταχυδρομείου [7].

2.5.3 Απερισκεπτη Περιηγηση του Διαδικτυου απο τους Υπαλληλους

Οι υπάλληλοι της επιχείρησης ενδέχεται να χρησιμοποιούν τις ηλεκτρονικές συσκευές που ανήκουν στην επιχείρηση για να περιηγηθούν στο διαδίκτυο σε ιστοσελίδες που δεν σχετίζονται με την εργασία τους. Η απερίσκεπτη περιήγηση του διαδικτύου μπορεί να επηρεάσει το δίκτυο της επιχείρησης με trojans, bot clients, spyware και με διάφορα είδη malware. Οι ιστοσελίδες που διαδίδουν τα περισσότερα malware είναι: ιστοσελίδες διάσημων προσώπων, ιστοσελίδες με διάφορα παιχνίδια και ιστοσελίδες ερωτικού περιεχομένου. Επίσης, οι ιστοσελίδες κοινωνικής δικτύωσης αποτελούν στόχο των malwares και αυτό κάνει τις συγκεκριμένες σελίδες επικίνδυνες για τα περιουσιακά στοιχεία της επιχείρησης [7].

Τα κύρια περιουσιακά στοιχεία της επιχείρησης που μπορεί να επηρεαστούν είναι: οι ηλεκτρονικοί υπολογιστές, κινητά τηλεφωνά, tablets και το δίκτυο όλης της επιχείρησης. Για να αποφευχθούν όλα αυτά, θα πρέπει οι υπάλληλοι της επιχείρησης να είναι ενημερωμένοι ώστε να μην επισκέπτονται ιστοσελίδες που δεν σχετίζονται με την εργασία τους. Επίσης, οι υπάλληλοι θα πρέπει να είναι ενήμεροι ότι όλες οι περιήγησης στο διαδίκτυο καταγράφονται και παρακολουθούνται ώστε να μην επισκέπτονται ανήθικες ιστοσελίδες κατά την διάρκεια της εργασίας τους, όπως επίσης είναι καλό είναι να εφαρμοστεί «Πολιτική Αποδεκτής Χρήσης» στο διαδίκτυο. Τέλος, μπορεί εφαρμοστεί φιλτράρισμα του διαδικτύου που αποτρέπει την επίσκεψη σε ιστοσελίδες που δεν σχετίζονται με την εργασία, εφαρμόζοντας την «Πολιτική Αποδεκτής Χρήσης» του διαδικτύου στους υπαλλήλους [11].

2.5.4 Επιθεση σε Web Server

Μια από τις πιο κοινές επιθέσεις είναι η επίθεση σε μια ιστοσελίδα. Οι πιο πολλές μικρομεσαίες επιχειρήσεις έχουν μια ιστοσελίδα ώστε να μπορούν να επικοινωνήσουν με τους πελάτες τους. Οι ιστοσελίδες μπορεί να έχουν αρκετές ευπάθειες εάν έχουν έναν κακογραμμένο κώδικα, καθώς αυτό μπορεί να οδηγήσει σε αρκετά κενά ασφαλείας που μπορούν να εκμεταλλευτούν οι κυβερνοεγκληματίες [7].

Τα κύρια περιουσιακά στοιχεία της επιχείρησης που πλήττονται είναι η ιστοσελίδα της επιχείρησης και οι servers. Ο καλύτερος τρόπος να αποφευχθεί αυτή η επίθεση είναι να γίνεται έλεγχος όλου του κώδικα της ιστοσελίδας για τυχόν κενά ασφαλείας και η διόρθωση τους. Επίσης η χρήση ενός firewall το οποίο θα φιλτράρει την κίνηση προς τον server είναι μια καλή λύση για να αποφευχθούν οι επίθεσης σε web server [12].

2.5.5 Απωλεια Δεδομενων απο Φορητες Συσκευες

Αυτό το είδος απειλής συμβαίνει όταν μια φορητή συσκευή της επιχείρησης κλαπεί ή χαθεί. Ευαίσθητα δεδομένα μπορεί να είναι αποθηκευμένα σε μια συσκευή όπως laptop, κινητό τηλέφωνο ή tablet και να διαρρεύσουν, κάτι που αποτελεί πραγματική απειλή για μια επιχείρηση. Οι φορητές συσκευές όπως τα κινητά τηλεφωνά και τα laptops, λόγω της μεγάλης τους αξίας και της ευκολίας να κλαπούν, αποτελούν στόχο για τους επιτήδειους. Για παράδειγμα, υπολογίζεται ότι πάνω από 70 εκατομμύρια κινητά τηλέφωνα κλέβονται ή χάνονται κάθε χρόνο [13]. Αυτό το μεγάλο νούμερο κλεμμένων συσκευών δείχνει την σοβαρότητα της απώλειας δεδομένων από φορητές συσκευές. Τα περιουσιακά στοιχεία της επιχείρησης που πλήττονται είναι οι φορητές συσκευές αλλά κυρίως τα δεδομένα που είναι αποθηκευμένα σε αυτές.

Για την αποφύγουν αυτή την απειλή οι επιχειρήσεις θα πρέπει να κρυπτογραφούν όλα τα δεδομένα στις φορητές συσκευές που έχουν στην κατοχή τους και να είναι υποχρεωτική η

χρήση κωδικού για την πρόσβαση στα δεδομένα. Θα πρέπει να υπάρχει μια πολίτικη στις επιχειρήσεις, ώστε όλες οι φορητές συσκευές που τους ανήκουν να χρησιμοποιούν τα παραπάνω χαρακτηριστικά. Η χρήση λογισμικών όπως το BitLocker, Workspace One, Mobile Iron κ.α. οπού κρυπτογραφούν και επιτρέπουν στις επιχειρήσεις να διαγράψουν όλα τα δεδομένα από τις φορητές συσκευές σε περίπτωση που κλαπούν ή χαθούν πρέπει να είναι υποχρεωτική[7].

2.5.6 Απερισκεπτη Χρηση Wi-Fi Hotspots

Επιτήδειοι μπορεί να στήσουν ένα Wi-Fi access point και να αφήσουν την πρόσβαση σε αυτό δωρεάν ή ελεύθερη ώστε να προσελκύσουν θύματα. Εάν τα θύματα έχουν πρόσβαση στο διαδίκτυο χρησιμοποιώντας το συγκεκριμένο Wi-Fi access point επιτρέπουν στον επιτήδειο να παρακολουθεί όλη την κίνηση των θυμάτων στο διαδίκτυο, παίρνοντας πολύτιμες πληροφορίες, όπως τους κωδικούς πρόσβασης τους σε ιστοσελίδες που σχετίζονται με την εργασία τους και όχι μόνο [7].

Το κύριο περιουσιακό στοιχείο που πλήττεται είναι ευαίσθητα δεδομένα της επιχείρησης. Για να αποφύγουν οι υπάλληλοι την απερίσκεπτη χρήση Wi-Fi hotspot, θα πρέπει να είναι ενημερωμένοι ώστε να διαλέγουν πάντα κρυπτογραφημένη σύνδεση αλλά και να χρησιμοποιούν VPN (Virtual Private Network). Επίσης, καλό θα ήταν να αποφεύγουν γενικά να ενώνουν τις συσκευές τους με άγνωστα Wi-Fi hotspots.

2.5.7 Απερισκεπτη Χρηση Δικτυων Ξενοδοχειων και Καταστηματων

Τα ξενοδοχεία πολλές φορές προσφέρουν δωρεάν πρόσβαση στο διαδίκτυο μέσο του Wi-Fi δικτύου τους, το οποίο μπορεί να μολύνει τις συσκευές που είναι ενωμένες με αυτό με ιούς, spyware, worms και malware. Τα laptops που δεν έχουν ενημερωμένο firewall, anti-virus,

anti-malware κ.α. μπορούν να μολυνθούν πολύ εύκολα από τέτοιου είδους δίκτυα. Αργότερα, όταν ο υπάλληλος ενώσει την μολυσμένη συσκευή του στο δίκτυο της επιχείρησης, μπορεί να μολύνει όλο το δίκτυο αυτής [14].

Τα περιουσιακά στοιχεία της επιχείρησης που μπορεί να επηρεαστούν από αυτή την απειλή είναι όλο το δίκτυο της αλλά και η συσκευή του υπάλληλου που ενώθηκε στο δίκτυο. Για να αποφύγουν οι επιχειρήσεις την παραπάνω απειλή θα πρέπει όλες οι συσκευές που της ανήκουν, όπως laptops, κινητά τηλέφωνα, tablets κ.α. να έχουν ενημερωμένα προγράμματα ασφαλείας, όπως anti-virus, anti-malware, anti-spyware και firewall. Επίσης, θα ήταν καλό να υπάρχει μια πολιτική οπού να απαγορεύει στους υπαλλήλους της επιχείρησης να απενεργοποιούν τα παραπάνω προγράμματα στις συσκευές τους [7].

2.5.8 Οι Κακες Ρυθμισεις Οδηγουν σε Ευπαθειες

Οι ρυθμίσεις ασφαλείας σε όλα τα πληροφοριακά συστήματα είναι ρυθμισμένες στο να λειτουργούν με τις προεπιλεγμένες ρυθμίσεις. Οι χρήστες καλούνται να αλλάξουν τις προεπιλεγμένες ρυθμίσεις, αν θέλουν ουσιαστικά να είναι τα συστήματα τους ασφαλή. Αυτό συμβαίνει διότι, οι προεπιλεγμένοι κωδικοί σε όλα τα συστήματα μπορούν να βρεθούν πολύ εύκολα στο διαδίκτυο και έτσι ένας επιτήδειος μπορεί εύκολα να έχει πρόσβαση στο δίκτυο της επιχείρησης [7].

Σύμφωνα με την ερευνά «Verizon's Data Breach Report 2018», από τις 1799 παραβιάσεις συστημάτων που ερεύνησε, οι 66 οφείλονται σε κακές ρυθμίσεις συστημάτων [8]. Το περιουσιακό στοιχείο της επιχείρησης που μπορεί να επηρεαστεί από αυτή την απειλή είναι ολόκληρο το δίκτυο της. Για να αποφευχθεί αυτή η απειλή θα πρέπει να αλλάζονται οι προεπιλεγμένοι κωδικοί στα συστήματα ανά τακτά χρονικά διαστήματα.

2.5.9 Έλλειψη Σχεδιου Έκτακτης Αναγκης

Πολλές μικρομεσαίες επιχειρήσεις δεν έχουν σχέδιο έκτακτης ανάγκης, το οποίο συνεπάγεται ότι σε περίπτωση έκτακτης ανάγκης δεν έχουν μια σωστή εναλλακτική λύση στο να επαναφέρουν τα δεδομένα και τα συστήματα τους με ευκολία. Το κύριο περιουσιακό στοιχείο που πλήττεται από την έλλειψη σχεδίου έκτακτης ανάγκης είναι όλη η υποδομή των πληροφοριακών συστημάτων της επιχείρησης. Ο τρόπος για να αποφευχθεί αυτή η απειλή είναι δημιουργία ενός σχεδίου έκτακτης ανάγκης [7].

2.5.10 Επιθεσεις εκ των Έσω

Στις μικρομεσαίες επιχειρήσεις οι επιθέσεις εκ των έσω δεν είναι τόσο συχνές όσο στις μεγάλες, αυτό συμβαίνει διότι οι μικρομεσαίες επιχειρήσεις έχουν λιγότερους υπαλλήλους. Παράνομες πρακτικές που σχετίζονται με την ασφάλεια είναι πολύ εύκολο να καταγράφουν, εντοπιστούν και να διορθωθούν στο μικρότερο δίκτυο μιας μικρομεσαίας επιχείρησης απ' ότι σε ένα τεράστιο δίκτυο με πολλούς χρήστες. Από την άλλη πλευρά, λόγω των λιγότερων υπαλλήλων, οι μικρομεσαίες επιχειρήσεις βασίζουν όλο τον έλεγχο των περιουσιακών στοιχείων τους σε ένα μόνο άτομο. Αυτό το άτομο αποκτά αμέσως την ικανότητα να βλάψει την επιχείρηση εκ των έσω [16].

Οι επιθέσεις εκ των έσω έχουν μεγάλο εύρος, καθώς μπορεί να γίνει εξαγωγή ή χειραγώγηση δεδομένων, καταστροφή περιουσιακών στοιχείων, χρήση μη εξουσιοδοτημένων λογισμικών τα οποία μπορεί να περιλαμβάνουν κακόβουλα λογισμικά κ.α. Το κύριο περιουσιακό στοιχείο που μπορεί να πληγεί με τις επιθέσεις εκ των έσω είναι όλη η υποδομή της επιχείρησης. Για την αποφυγή της παραπάνω επίθεσης, θα πρέπει οι μικρομεσαίες επιχειρήσεις πριν προσλάβουν κάποιον υπάλληλο, να διενεργούν έναν έλεγχο του ιστορικό του. Επίσης, δεν θα πρέπει να δίνεται όλος ο έλεγχος των περιουσιακών στοιχείων της επιχείρησης σε ένα μόνο άτομο [7].

2.6 Συζητηση περι Απειλων

Από τις απειλές κατά της ασφάλειας και τα πιθανά μετρά πρόληψης που αναφέρονται παραπάνω μπορεί να ειπωθεί ότι, οι περισσότερες από τις απειλές προκύπτουν από την εισαγωγή νέων τεχνολογιών και την απρόσεκτη χρήση τους. Βέβαια, πρέπει να θεωρηθεί δεδομένο και ότι οι περισσότερες απειλές ασφαλείας υπάρχουν λόγω του ανθρώπινου παράγοντα. Ο παρακάτω Πίνακας 3 απαριθμεί όλες τις επιθέσεις που είναι η μεγαλύτερη απειλή για τις μικρομεσαίες επιχειρήσεις στις Ηνωμένες Πολιτείες Αμερική, σύμφωνα με την έρευνα της WatchGuard [7] που συζητήθηκε παραπάνω.

Επίσης, μπορεί να ειπωθεί από την παραπάνω συζήτηση ότι οι περισσότερες απειλές κατά της ασφάλειας, μπορούν να αποφευχθούν με την επιβολή διάφορων πολιτικών για τον έλεγχο της συμπεριφοράς των υπάλληλων της επιχείρησης. Αυτό εγείρει το ερώτημα εάν οι μικρομεσαίες επιχειρήσεις πρέπει να κάνουν παραπάνω πράγματα για να είναι προστατευμένες στον κυβερνοχώρο. Η απάντηση είναι απλά «ναι». Όλες οι μικρομεσαίες επιχειρήσεις πρέπει να δώσουν έμφαση στο γεγονός ότι μπορεί να πέσουν θύματα εγκληματιών στον κυβερνοχώρο.

Πίνακας 3 Οι κορυφαίες απειλές ασφαλείας των μικρομεσαίων επιχειρήσεων

Αρ.	**Επίθεση**	**Περιουσιακό Στοιχείο**	**Μέτρα Πρόληψης**
1	Αυτόματη εκμετάλλευση μιας γνωστής ευπάθειας	Λειτουργικό Σύστημα Η/Υ	• Χρήση λογισμικού διαχείρισης ενημερώσεων • Εκπαίδευση υπαλλήλων • Εφαρμογή πολιτική πρόληψης

2	Κακόβουλα HTML Email	Συσκευές που λαμβάνουν email	• Εφαρμογή Spam Filter • Ευαισθητοποίηση των υπαλλήλων • Εφαρμογή πολιτική πρόληψης
3	Απερίσκεπτη περιήγηση του διαδικτύου από τους υπάλληλους	Η/Υ, κινητά τηλέφωνα, laptops κ.α.	• Φιλτράρισμα και απαγόρευση ιστοσελίδων • Χρήση Firewall
4	Επίθεση σε Web Server	Ιστοσελίδα και server	• Έλεγχος του κώδικα της ιστοσελίδας • Χρήση Firewall
5	Απώλεια δεδομένων από φορητές συσκευές	Φορητές συσκευές και δεδομένα	• Κρυπτογράφηση δεδομένων στις συσκευές • Χρήση λογισμικών διαχείρισης συσκευών
6	Απερίσκεπτη χρήση Wi-Fi Hotspots	Δεδομένα της επιχείρησης	• Χρήση κρυπτογραφημένων συνδέσεων Wi-Fi • Χρήση VPN
7	Απερίσκεπτη χρήση δικτυών ξενοδοχείων και καταστημάτων	Συσκευές των υπαλλήλων	• Χρήση ενημερωμένων λογισμικών ασφαλείας • Χρήση Firewall
8	Οι κακές ρυθμίσεις οδηγούν σε ευπάθειες	Όλο το δίκτυο της επιχείρησης	• Αλλαγή προεπιλεγμένων κωδίκων και όνομα χρήστη • Εφαρμογή πολιτική πρόληψης

9	Έλλειψη σχεδίου έκτακτης ανάγκης	Ολόκληρη η υποδομή της επιχείρησης	• Ανάπτυξη πολιτικής σύμφωνα με τις ανάγκες της επιχείρησης • Εφαρμογή πολιτικής πρόληψης
10	Επιθέσεις εκ των έσω	Ολόκληρη η υποδομή της επιχείρησης	• Έλεγχος του ιστορικού των υπαλλήλων • Δεν πρέπει να έχει τον έλεγχο όλων των συστημάτων ένα μόνο άτομο • Εφαρμογή πολιτικής πρόληψης

2.7 ΝΕΕΣ ΤΕΧΝΟΛΟΓΙΕΣ, ΝΕΕΣ ΑΠΕΙΛΕΣ

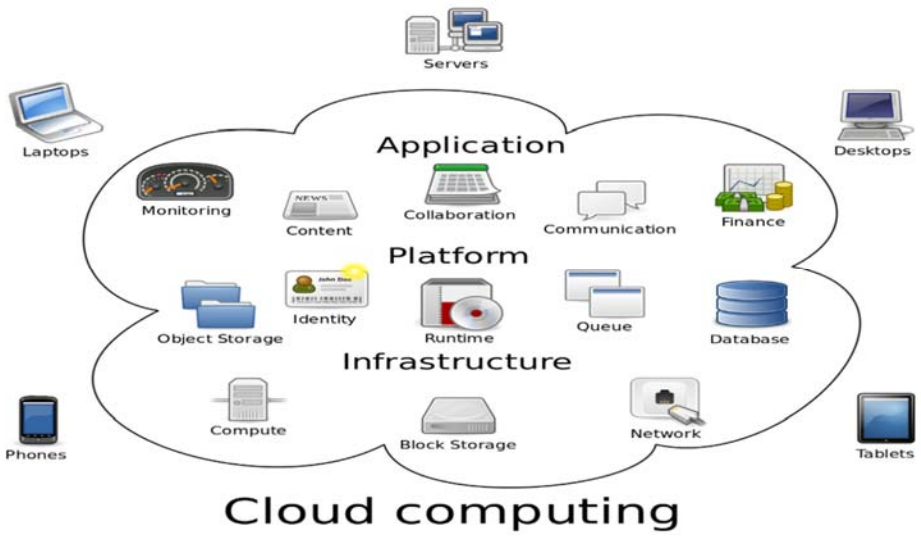
Καινοτόμες νέες τεχνολογίες που παρέχουν υποστήριξη και επιτάχυνση της ανάπτυξης των επιχειρήσεων εισάγονται σχεδόν καθημερινά στην αγορά. Το να παραμείνουν ενημερωμένες οι μικρομεσαίες επιχείρησης με τις τεχνολογίες τους σήμερα είναι ένας καθημερινός αγώνας. Γενικά όμως, είναι εύκολο να ακολουθήσουν τις γραμμές που άλλες επιχειρήσεις τείνουν να ακολουθούν, το οποίο είναι γνωστό ως «ακολουθώντας την τεχνολογική τάση». Οι τάσεις στην πληροφορική υποδεικνύουν την παγκόσμια ζήτηση για προϊόντα και υπηρεσίες πληροφορικής τα οποία χρησιμοποιούνται από τις περισσότερες επιχειρήσεις.

Εξετάζοντας το γεγονός ότι οι περισσότερες απειλές ασφαλείας σε μικρομεσαίες επιχειρήσεις σχετίζονται με τις νέες τεχνολογίες και τον ανθρώπινο παράγοντα, η έρευνα αυτή θα ασχοληθεί και με δυο τεχνολογικές τάσεις της εποχής μας, οι οποίες φαίνεται να αποτελούν σημαντικές απειλές ασφαλείας στις μικρομεσαίες επιχειρήσεις. Σε αυτό το πλαίσιο, θα συζητηθούν οι ανερχόμενες τεχνολογίες Cloud Computing και BYOD (Bring Your Own Device), οι οποίες έχουν συγκεντρώσει τα βλέμματα πάνω τους, καθώς βοηθάν τις μικρομεσαίες επιχειρήσεις να μειώσουν το κόστος της τεχνολογικής υποδομής τους.

2.7.1 Cloud Computing

Η πρόσφατη ανάπτυξη του cloud computing έχει αρχίσει να αλλάζει τις υποδομές πληροφορικής πολλών επιχειρήσεων. Αντί για αποθήκευση δεδομένων, προγραμμάτων ή επεξεργαστική ισχύ σε έναν ηλεκτρονικό υπολογιστή της επιχείρησης, το cloud computing αποθηκεύει δεδομένα και προγράμματα σε απομακρυσμένους servers και παρέχει πρόσβαση σε αυτά μέσω του διαδικτύου. Επιπλέον, η τεχνολογία που χρησιμοποιούν οι τελικοί χρήστες δεν ανήκει σε αυτούς αλλά όλος ο εξοπλισμός και το λογισμικό ανήκει στην επιχείρηση η οποία παρέχει την υπηρεσία. Η επιχείρηση που της παρέχετε το cloud computing πρέπει να πληρώσει μόνο για τις υπηρεσίες, οπού το κόστος είναι κατά πολύ μικρότερο από το να της ανήκε ολόκληρη η υποδομή που θα παρείχε τις ίδιες υπηρεσίες.

Το cloud computing λύνει το πρόβλημα του χαμηλού προϋπολογισμού που έχουν οι μικρομεσαίες επιχειρήσεις για την τεχνολογική υποδομή τους. Μερικά παραδείγματα cloud computing είναι το Google Drive, webmail, Dropbox κ.α. Οι πιο γνωστές εταιρίες παροχής cloud computing είναι η Google, Amazon και Microsoft, οι οποίες έχουν φτιάξει τεράστιες υποδομές για να υποστηρίξουν τις υπηρεσίες τους [19].



Εικόνα 3 Cloud Computing [43]

Τα πλεονεκτήματα του μοντέλου cloud computing είναι αρκετά. Ο πελάτης μπορεί να τροποποιήσει τις υπολογιστικές δυνατότητες, όπως την αποθήκευση μέσω δικτύου χωρίς να χρειάζεται να επικοινωνήσει με την εταιρία που παρέχει την υπηρεσία. Επίσης, ο πελάτης μπορεί να χρησιμοποιήσει την υπηρεσία μέσω του διαδικτύου και να έχει πρόσβαση σε αυτήν από οποιαδήποτε συσκευή θέλει, όπως το κινητό τηλέφωνο και laptop. Από την πλευρά της εταιρίας παροχής του cloud computing, η «συγκέντρωση πόρων» είναι εφικτή όπου ο αποθηκευτικός χώρος στο cloud και η υπολογιστική ισχύ μπορούν να διαμοιραστούν σε διαφορετικούς πελάτες, κατόπιν ζήτησης. Η χρήση πόρων του cloud μπορεί να ελεγχθεί και να καταγραφεί από τον παροχέα αλλά και από τον πελάτη για λόγους διαφάνειας [18].

Παρόλο που η τεχνολογία cloud computing έχει πολλά πλεονεκτήματα, οι απειλές ασφαλείας που σχετίζονται με την τεχνολογία αυτή είναι αρκετές. Οι μικρομεσαίες επιχειρήσεις που ενδιαφέρονται να αποκτήσουν τα πλεονεκτήματα του cloud computing θα πρέπει να βελτιώσουν τα σχέδια διαχείρισης κινδύνου τους. Η ανάθεση όλων των δεδομένων στο cloud εισάγει κινδύνους όπως η κλοπή πνευματικής ιδιοκτησίας, κρίσιμα εμπιστευτικά δεδομένα κ.α. Σε περίπτωση που ο παροχέας υπηρεσιών cloud καταχραστεί τα δεδομένα του πελάτη της μπορεί να αποκαλύψει μυστικά σχέδια κάποιου πελάτη ή ακόμα και της ιδίας της μικρομεσαίας επιχείρησης. Επίσης, μπορεί να οδηγήσει σε κακή χρήση ιδιωτικών δεδομένων. Για παράδειγμα, αν τα δεδομένα ενός πελάτη μιας μικρομεσαίας επιχείρησης είναι αποθηκευμένη στο cloud και παραβιαστεί, μπορεί να οδηγήσει σε αποκάλυψη ιδιωτικών πληροφοριών και στην χειρότερη περίπτωση πλήρη κλοπή της ταυτότητας του[20] [21] [22].

Επομένως, ενώ η αποθήκευση δεδομένων στο cloud βοηθάει την μικρομεσαία επιχείρηση στο να μειώσει το κόστος των συστημάτων πληροφορικής και κάνει την αποθήκευση και διαμοιρασμό των δεδομένων πιο εύκολο, εισάγει επίσης περισσότερες ευπάθειες στην ασφαλείας της επιχείρησης [23].

Οι μικρομεσαίες επιχειρήσεις για να είναι πιο προστατευμένες όταν χρησιμοποιούν cloud computing υπηρεσίες, θα πρέπει να είναι πολύ προσεκτικές στο ποιος έχει πρόσβαση στα αποθηκευμένα δεδομένα στο cloud. Επίσης, θα μπορούσαν να κρυπτογραφούν όλα τα δεδομένα πριν τα αποθηκεύσουν στο cloud.

2.7.2 BYOD (Bring Your Own Device)

Την σημερινή εποχή, η εύκολη πρόσβαση στο διαδίκτυο μέσω δικτυών 3/4G και η μεγάλη διαθεσιμότητα συσκευών όπως έξυπνα κινητά τηλεφωνά, tablets, laptops κ.α. εισήγαγε μια ξαφνική αύξηση στην χρήση των φορητών συσκευών. Μέρος αυτής της νέας τεχνολογικής τάσης είναι το BYOD (Bring Your Own Device), το οποίο σημαίνει ότι οι υπάλληλοι της επιχείρησης μπορούν να χρησιμοποιούν τις δικές τους συσκευές κατά την διάρκεια του χρόνου εργασίας τους. Ο πιο πρόσφατος όρος BYOT (Bring Your Own Technology) αντικαθιστά σιγά σιγά τον όρο BYOD (Bring Your Own Device), το οποίο συνήθως περιλαμβάνει συσκευές αλλά και λογισμικό.

Εικόνα 4 Bring your own device [44]

Η χρήση του BYOD είναι σύνηθες σε πολλές μεγάλες επιχειρήσεις και λιγότερο σε μικρομεσαίες. Σύμφωνα με την έρευνα της Cisco [24], η οποία πραγματοποιήθηκε στις Ηνωμένες Πολιτείες Αμερικής και συμμετείχαν πάνω από 900 επιχειρήσεις, το 89% των ερωτηθέντων απάντησε ότι το τμήμα τεχνολογίας της επιχείρησης επιτρέπει στους υπαλλήλους να χρησιμοποιούν τις συσκευές τους στο εργασιακό περιβάλλον ως ένα βαθμό. Επίσης, στην παραπάνω έρευνα υπολογίζεται ότι ο μέσος υπάλληλος με τεχνολογικό υπόβαθρο χρησιμοποιεί 2,3 με 2,8 ενωμένες συσκευές με το δίκτυο της επιχείρησης κατά την διάρκεια της εργασίας του και αυτό το νούμερο αναμένεται να αυξηθεί τα επόμενα χρόνια. Μια έρευνα της Ευρωπαϊκής Επιτροπής ισχυρίζεται ότι και στην Ευρώπη αρχίζει να αυξάνεται ο αριθμός των επιχειρήσεων που υιοθετούν την τεχνολογία BYOD.

Ωστόσο, υπάρχουν ακόμα αρκετοί προβληματισμοί γύρω από τα προβλήματα ασφάλειας που μπορεί να εισάγει η χρήση του BYOD, καθώς οι υπάλληλοι συνδέουν τις προσωπικές τους συσκευές με περιουσιακά στοιχεία της επιχείρησης. Η κύρια απειλή στην τεχνολογία BYOD είναι ο υπάλληλος, δηλαδή η επίθεση εκ των έσω [25]. Υπάρχουν μελέτες που επικεντρώνονται στις επιθέσεις εκ των έσω, οι οποίες αποτελούν σοβαρές απειλές για την ασφάλεια της επιχείρησης. Σύμφωνα με έρευνα του FBI η οποία πραγματοποιήθηκε αναμεσά σε 616 επαγγελματίες ασφάλειας υπολογιστών, ποσοστό 64% των ερωτηθέντων ανέφεραν ότι ορισμένες απώλειες που σχετίζονται με την ασφάλεια υπολογιστών έχουν προκύψει λόγω ενεργειών που πραγματοποιήθηκαν εκ των έσω [26]. Για παράδειγμα, ένας χρήστης μπορεί να προκαλέσει μια απειλή ασφαλείας απλά ανοίγοντας ένα μήνυμα ηλεκτρονικού ταχυδρομείου, του οποίου η επισύναψη περιέχει κάποιον ιό.

Η έρευνα Norton Report που πραγματοποιήθηκε ανάμεσα σε πάνω από 13000 ενήλικους και 24 χώρες, ισχυρίζεται ότι [27]:

- 49% χρησιμοποιούν τις προσωπικές συσκευές τους σε δραστηριότητες που σχετίζονται με την εργασία τους
- Σχεδόν οι μισοί δεν χρησιμοποιούν βασικά μέτρα ασφαλείας, όπως κωδικοί ασφαλείας και προγράμματα ασφαλείας
- 27% έχουν χάσει την συσκευή τους ή έχει κλαπεί

Οι χρήστες των φορητών συσκευών πολλές φορές συνδέουν τις συσκευές τους σε δίκτυα ή άλλες συσκευές οι οποίες δεν είναι ασφαλή, το οποίο συνεπάγεται ότι η συσκευή τους μπορεί να μολυνθεί με κάποιον ιό, malware ή άλλο κακόβουλο λογισμικό. Έτσι, όταν ο χρήστης ενώσει την συσκευή του με το δίκτυο της επιχείρησης μπορεί να ανοίξει τον δρόμο σε αυτό το κακόβουλο λογισμικό να μεταπηδήσει από την συσκευή του χρήστη σε όλο το δίκτυο της επιχείρησης. Αυτό μας δείχνει πόσο εύκολα μπορεί μόνο μια συσκευή να επηρεάσει όλη την υποδομή πληροφορικής της επιχείρησης.

Αντίθετα, πολλές ευαίσθητες πληροφορίες μπορεί να είναι αποθηκευμένες στις προσωπικές συσκευές. Οι πληροφορίες αυτές μπορεί να είναι σε μορφή ηλεκτρονικού ταχυδρομείου και να περιέχουν δεδομένα ενός πελάτη, όπως και δεδομένα της επιχείρησης. Έτσι, έστω και μια

τυχαία φορητή συσκευή να κλαπεί ή χαθεί, μπορεί να διαρρεύσουν πληροφορίες οι οποίες θεωρούνται ευαίσθητες για την επιχείρηση [28].

Ο καλύτερος τρόπος για να διευθετηθούν οι απειλές του BYOD είναι μέσω πολιτικών που μπορεί να εφαρμόσει η επιχείρηση. Μερικές τέτοιες πολιτικές είναι: ο καθορισμός των φορητών συσκευών που επιτρέπονται, ο καθορισμός των υπηρεσιών όπως εφαρμογές που επιτρέπονται να γίνονται χρήση σε μια συσκευή BYOD κ.α. Η επιχείρηση θα πρέπει να αποφασίσει σε ποιο βαθμό θα επιτρέψει να γίνεται χρήση του BYOD από τους υπαλλήλους. Επίσης, η χρήση λογισμικού διαχείρισης συσκευών MDM (Mobile Device Management) μπορεί να βοηθήσει τις επιχειρήσεις να μειώσουν τις απειλές που σχετίζονται με το BYOD.

Βέβαια, εκτός από προβλήματα γύρω από την ασφάλεια που εισάγει το BYOD έχει και πολλά προτερήματα. Η αλλαγή προς την υιοθέτηση του BYOD φέρνει νέες ευκαιρίες για τις επιχειρήσεις. Τα δυο κύρια χαρακτηρίστηκα που εισάγει το BYOD είναι η αύξηση της παραγωγικότητας των υπαλλήλων και η μείωση του κόστους. Επίσης, οι υπάλληλοι μπορεί να νοιώθουν πιο οικεία να χρησιμοποιούν συσκευές που τους ανήκουν για την δουλειά τους. Τέλος, με την χρήση του BYOD οι υπάλληλοι επωμίζονται το κόστος αγοράς και συντήρησης των συσκευών, έτσι μειώνονται κατά πολύ τα έξοδα της επιχείρησης.

2.8 Συζητηση περι BYOD και Cloud Computing

Οι απειλές ασφαλείας που εισάγονται με τις τεχνολογίες BYOD και Cloud Computing φαίνεται να είναι πολύ σοβαρές, παρόλα αυτά είναι εύκολο να αντιμετωπιστούν μέσω εφαρμογής διαφόρων πολιτικών από τις επιχειρήσεις στους υπαλλήλους που χρησιμοποιούν αυτές τις τεχνολογίες. Για παράδειγμα, όλες οι απειλές ασφαλείας του BYOD βασίζονται αποκλειστικά στην δραστηριότητα της φορητής συσκευής του υπάλληλου. Έτσι, εφαρμόζοντας τις πολιτικές στο πως πρέπει να χρησιμοποιούνται οι προσωπικές συσκευές με ευαίσθητα δεδομένα λύνουμε το πρόβλημα. Εκτός αυτού, όλες οι απειλές ασφαλείας του Cloud Computing υπάρχουν λόγω του ότι ευαίσθητα δεδομένα μπορεί να διαρρεύσουν. Εάν

εφαρμοστούν μερικές κοινές πρακτικές στο πως μπορούμε να αποθηκεύσουμε δεδομένα στο cloud με ασφαλή τρόπο, τότε η απειλή μπορεί να μετριαστεί. Ο παρακάτω πίνακας 4 περιγράφει με ακρίβεια το Cloud Computing και BYOD.

Οι δέκα μεγαλύτερες απειλές που μελετήσαμε, μαζί με τις τεχνολογικές τάσεις του BYOD και Cloud Computing μας δείχνουν το πόσο ευάλωτες είναι οι μικρομεσαίες επιχειρήσεις στον κυβερνοχώρο. Επιχειρήσεις κάθε μεγέθους θα πρέπει να είναι προετοιμασμένες για να ανταπεξέλθουν στις απειλές ασφαλείας του σήμερα αλλά και του μέλλοντος.

Πίνακας 4 Cloud Computing και BYOD με μια ματιά

Κατηγορία	**Cloud Computing**	**BYOD**
Ορισμός	Το Cloud Computing αποθηκεύει δεδομένα και προγράμματα σε έναν απομακρυσμένο server. Παρέχει πρόσβαση μέσω διαδικτύου. Ο πελάτης δεν χρειάζεται να αποθηκεύει δεδομένα, προγράμματα ή επεξεργαστική ισχύ στον δικό του Η/Υ	BYOD (Bring Your Own Device) σημαίνει ότι ο υπάλληλος μπορεί να χρησιμοποιήσει την προσωπική του συσκευή κατά την διάρκεια εργασίας
Πλεονεκτήματα	Προσφέρει όλες τις λειτουργίες των σύγχρονων υπηρεσιών τεχνολογίας της πληροφορικής και μειώνει το κόστος.	Αυξάνει τη παραγωγικότητα των υπαλλήλων και μειώνει το κόστος
Μειονεκτήματα	Η αποθήκευση δεδομένων στο Cloud εισάγει ρίσκα όπως κλοπή πνευματικής ιδιοκτησίας κ.α. Επίσης ο	Οι προσωπικές φορητές συσκευές οπού χρησιμοποιούνται στην εργασία μπορεί να κλαπούν ή

	παροχέας της υπηρεσίας μπορεί να καταχραστεί ευαίσθητα δεδομένα.	χαθούν. Οι συσκευές αυτές μπορεί να έχουν μολυνθεί και να επηρεάσουν όλο το δίκτυο της επιχείρησης.
Τρόποι Αντιμετώπισης	Εφαρμογή πολιτικών διασφάλισης της χρήσης cloud. Έλεγχος στο ποιος έχει πρόσβαση στα αποθηκευμένα δεδομένα και κρυπτογράφηση των δεδομένων πριν την αποθήκευση.	Εφαρμογή πολιτικών που διευκρινίζουν τις επιτρεπόμενες συσκευές και υπηρεσίες που μπορούν να χρησιμοποιήσουν οι υπάλληλοι. Επίσης ένα λογισμικό διαχείρισης των συσκευών που επιτρέπονται.

ΚΕΦΑΛΑΙΟ 3
Διαχείριση της Ασφάλειας Πληροφοριών

Όλες οι επιχειρήσεις μπορούν να μετριάσουν τις απειλές που δέχονται χρησιμοποιώντας διάφορους τρόπους ώστε να διαχειριστούν την ασφάλεια τους. Οι έλεγχοι διαχείρισης της ασφαλείας πληροφοριών έχουν τρία πεδία ορισμού: την διοικητική, φυσική και τεχνική (λογική). Αυτοί οι έλεγχοι διαχείρισης ασφάλειας πληροφοριών περιγράφονται παρακάτω.

3.1 Διοικητικη Ασφαλεια

Η διοικητική ασφάλεια ουσιαστικά καθορίζει τον τρόπο λειτουργίας και διαχείρισης της ασφάλειας πληροφοριών της επιχείρησης. Επίσης, περιλαμβάνει τις πολίτικες, τις διαδικασίες, τα πρότυπα αλλά και τις κατευθυντήριες γραμμές που ενημερώνουν τους ανθρώπους της επιχείρησης σχετικά με τον τρόπο λειτουργίας της σε καθημερινή βάση. Τέλος, ορίζει τις ευθύνες, τα καθήκοντα και αποτελεί την βάση για άλλους τρόπους διαχείρισης της ασφάλειας πληροφοριών.

Τα είδη διοικητικής ασφάλειας διαφέρουν ανάλογα με την ανάγκη και τους πόρους της επιχείρησης. Είναι επίσης σημαντικό να μετρηθεί πόσο συμμορφωμένη είναι η επιχείρηση. Εάν δεν τηρούνται οι πολίτικες και οι διαδικασίες, έστω και μια καλή πολιτική ασφαλείας μπορεί να έχει πολύ μικρό αντίκτυπο. Ως εκ τούτου, είναι ζωτικής σημασίας οι πολίτικες ασφαλείας να επιβάλλονται και να παρακολουθούνται με τους κατάλληλους πόρους [1].

3.2 Τεχνικη Ασφαλεια

Η τεχνική ασφάλεια είναι ίσως ο πιο γνωστός έλεγχος διαχείρισης της ασφάλειας πληροφοριών. Η ασφάλεια αυτή περιλαμβάνει πράγματα που αντιμετωπίζουν πολλοί άνθρωποι καθημερινά, όπως τα firewalls, κρυπτογράφηση, κωδικοί ασφαλείας, συστήματα ανίχνευσης εισβολής κ.α. Ο στόχος της τεχνικής ασφάλειας είναι η πρόληψη της μη εξουσιοδοτημένης πρόσβασης σε δίκτυα και συστήματα της επιχείρησης. Αυτό σημαίνει ότι οι επίδοξοι εισβολείς δεν είναι σε θέση να έχουν πρόσβαση στα δίκτυα και τα συστήματα της επιχείρησης [1].

Η τεχνική ασφάλεια μπορεί να διαχωριστεί σε τρεις κατηγορίες:

- Προληπτικός έλεγχος
- Έλεγχος ασύρματης πρόσβασης
- Ασφάλεια απομακρυσμένης πρόσβασης

Ο προληπτικός έλεγχος περιλαμβάνει λογισμικό ελέγχου πρόσβασης, λογισμικό προστασίας από κακόβουλα λογισμικά, κωδικούς ασφαλείας, βιομετρικά στοιχεία κ.α. Ο έλεγχος ασύρματης πρόσβασης επικεντρώνεται στον περιορισμό της πρόσβασης σε ασύρματα δίκτυα και στην κρυπτογράφηση και παρακολούθηση της κυκλοφορίας στο δίκτυο. Τέλος, η ασφάλεια απομακρυσμένης πρόσβασης αφορά την παροχή εξωτερικής πρόσβασης σε δίκτυα και συστήματα, προστατεύοντας τα από κακόβουλη χρήση.

3.3 Φυσικη Ασφαλεια

Η φυσική ασφάλεια αφορά γενικά την προστασία του περιβάλλοντος της επιχείρησης, δηλαδή την προστασία της υποδομής πληροφορικής, όπως ηλεκτρονικούς υπολογιστές και servers, από μη εξουσιοδοτημένη φυσική πρόσβαση και από άλλους κινδύνους. Χωρίς καλή φυσική ασφάλεια, τα άλλα είδη ασφαλείας μπορεί να γίνουν ευάλωτα, είτε να μην έχουν

πλέον νόημα. Η φυσική ασφάλεια περιλαμβάνει βασικά μέτρα ασφαλείας όπως, φράκτες, κλειδαριές, πόρτες, φρουρούς ασφαλείας και κάμερες. Μια ακόμη πτυχή της φυσικής ασφαλείας είναι η κατανομή των καθηκόντων και ρόλων, ώστε να διασφαλιστεί ότι η ασφάλεια δεν εξαρτάται από ένα μόνο άτομο [1].

Διαχωρίζεται σε τρία μέρη η φυσική ασφάλεια, στην αποτρεπτική, προληπτική και ανιχνευτική. Η αποτρεπτική εστιάζει στην αποθάρρυνση των ανθρώπων από την παραβίαση των ελέγχων ασφαλείας, όπως είναι οι επιγραφές και οι προειδοποιήσεις. Από την άλλη πλευρά, η ανιχνευτική εστιάζει στην ανίχνευση και την αναφορά των παραβιάσεων. Τα μέτρα ανίχνευσης περιλαμβάνουν συστήματα όπως κάμερες και ανιχνευτές καπνού. Η προληπτική μπορεί να περιλαμβάνει οτιδήποτε, από απλές κλειδαριές έως ψηλούς φράκτες που εμποδίζουν την μη εξουσιοδοτημένη πρόσβαση σε ορισμένες περιοχές.

3.4 Διακυβερνηση, Διαχειριση Κινδυνου και Συμμορφωση

Όλες οι επιχειρήσεις πρέπει να κατανοήσουν τους κινδύνους που σχετίζονται με την ασφάλεια, επίσης πρέπει να συμμορφώνονται με τις άμεσες ή έμμεσες απαιτήσεις της. Ο όρος που χρησιμοποιείται για να περιγράψει το παραπάνω είναι η συμμόρφωση. Με άλλα λόγια, οι επιχειρήσεις πρέπει να συμμορφώνονται ή να προσαρμόζονται όπως απαιτείται ή ζητείται από τρίτους, όπως κάποιον άμεσο συνεργάτη ή κυβέρνηση. Η συμμόρφωση είναι στενά συνδεδεμένη με τη διαχείριση κινδύνου και την διακυβέρνηση. Οι απαιτήσεις της συμμόρφωσης μπορούν να βοηθήσουν την διαχείριση κινδύνου στο να αναγνωρίσει τους ελέγχους ασφαλείας που χρειάζονται και σε ποιο βαθμό [29].

Η διακυβέρνηση, η διαχείριση κινδύνου και η συμμόρφωση είναι ένας γενικός όρος που χρησιμοποιείται για να μπορέσει να περιγράψει μια διαδικασία που βοηθάει τις επιχειρήσεις να εφαρμόζουν πολίτικες και ελέγχους ώστε να αντιμετωπίζει ζητήματα συμμόρφωσης

όπως επίσης και να συλλέγει πληροφορίες για την επιχείρηση. Ο στόχος του παραπάνω τρίπτυχου είναι να συμβάλει στην αποτελεσματικότερη διαχείριση μιας επιχείρησης. Για την ασφάλεια πληροφοριών αυτό σημαίνει ότι η διαχείριση των κίνδυνων και η συμμόρφωση απαιτούν την εφαρμογή ελέγχων ασφαλείας, ενώ μια σωστή διακυβέρνηση εξασφαλίζει ότι οι κίνδυνοι διαχειρίζονται με σωστό τρόπο, υποστηρίζοντας τους επιχειρησιακούς και επιχειρηματικούς στόχους της επιχείρησης [30].

Εικόνα 5 Διακυβέρνηση, Διαχείριση κινδύνου και Συμμόρφωση [45]

Οι απαιτήσεις της συμμόρφωσης μπορεί να προέρχονται από διάφορες πηγές και να είναι είτε εσωτερικές, είτε εξωτερικές. Επίσης, οι απαιτήσεις μπορεί να είναι υποχρεωτικές ή προαιρετικές. Οι εσωτερικές απαιτήσεις μπορεί για παράδειγμα να είναι το πως η επιχείρηση καταφέρνει να συμμορφωθεί με τις πολιτικές ασφάλειας πληροφοριών. Οι εξωτερικές απαιτήσεις μπορεί να σχετίζονται με επιχειρηματικές πρακτικές, κανονισμούς, νόμους, πρότυπα ή άλλες πρακτικές που απαιτούνται από μια επιχείρηση ώστε να συμμορφωθεί. Οι υποχρεωτικές απαιτήσεις είναι αυτές που πρέπει η επιχείρηση να πληροί, ενώ οι

προαιρετικές απαιτήσεις μπορεί να υιοθετηθούν αν η αξιολόγηση τους κριθεί λογική ή κατάλληλη για την επιχείρηση.

Οι πελάτες και οι συνεργάτες της επιχείρησης ενδέχεται να έχουν απαιτήσεις ασφαλείας που πρέπει να τηρούνται πριν αρχίσουν την συνεργασία τους. Για παράδειγμα, ένας προμηθευτής μπορεί να απαιτήσει ένα ορισμένο επίπεδο ασφαλείας πριν επιτρέψει την σύνδεση με τα πληροφοριακά του συστήματα. Χαρακτηριστικό παράδειγμα είναι η βιομηχανία καρτών πληρωμής που έχει αναπτύξει τα δικά της πρότυπα ασφαλείας. Όλες οι επιχειρήσεις που θέλουν να λαμβάνουν πληρωμές με κάρτες πληρωμής πρέπει να συμμορφώνονται με το πρότυπο ασφαλείας δεδομένων Payment Card Industry Data Security Standard (PCI DSS) [29].

3.5 Πλαισια, Μοντελα και Προτυπα

Το νομοθετικά πλαίσια συνήθως αποτελούν την βάση για την ανάπτυξη πολικών ασφάλειας πληροφοριών. Παράλληλα, πολλά πλαίσια, μοντέλα και πρότυπα έχουν αναπτυχθεί ώστε βοηθούν στην οργάνωση των αναγκών της ασφάλειας πληροφοριών των επιχειρήσεων. Δεν είναι όλα τα μοντέλα κατάλληλα για όλες τις επιχειρήσεις, μερικά έχουν αναπτυχθεί για συγκεκριμένους σκοπούς. Βέβαια, υπάρχουν αρκετά μοντέλα που είναι κατάλληλα για τις μικρομεσαίες επιχειρήσεις.

Οι επιχειρήσεις μπορούν να αποκτήσουν προτυποποιήσεις που θα βοηθήσουν στο να αξιολογήσουν το επίπεδο της ασφάλειας πληροφοριών τους. Τα πρότυπα αυτά μπορούν να εφαρμοστούν σε προϊόντα, συστήματα, υπηρεσίες, ακόμα και στο προσωπικό των επιχειρήσεων. Οι επιχειρήσεις που θέλουν να αποκτήσουν προτυποποιήσεις θα πρέπει να εξετάσουν πόσο γνωστές είναι αλλά και κατά πόσο θα επωφεληθούν από αυτές. Η εφαρμογή ενός πρότυπου ασφαλείας μπορεί να δημιουργήσει μια εικόνα αξιοπιστίας αλλά θα πρέπει να ληφθεί υπόψιν ότι απόκτηση και η συντήρηση τους είναι πολύ δαπανηρή για την επιχείρηση.

Πολλές μικρομεσαίες επιχειρήσεις πρέπει να εκτιμήσουν το κόστος της απόκτησης ενός πρότυπου ασφαλείας σε σχέση με το πιθανό κέρδος που θα έχουν από αυτή, λόγω του χαμηλότερου προϋπολογισμού που έχουν σε σχέση με τις μεγαλύτερες επιχειρήσεις. Εντούτοις, η προτυποποίηση των επιχειρήσεων, σε ορισμένες περιπτώσεις, είναι υποχρεωτική. Ένα πολύ γνωστό πρότυπο ασφαλείας είναι το ISO/IEC 27000/27001 το οποίο θα μελετηθεί παρακάτω.

3.6 Συστηματα Διαχειρισης Ασφαλειας Πληροφοριων

Ο ρόλος των συστημάτων διαχείρισης ασφάλειας πληροφοριών είναι να προστατεύει κρίσιμα πληροφοριακά περιουσιακά στοιχεία και δεδομένα από απειλές των αρχών της ασφάλειας πληροφοριών, δηλαδή την διαθεσιμότητα, ακεραιότητα και εμπιστευτικότητα [30]. Τα συστήματα διαχείρισης ασφάλειας πληροφοριών φέρνουν τους ελέγχους ασφάλειας πληροφοριών κάτω από το ίδιο σύστημα διαχείρισης. Ο διεθνής οργανισμός ασφαλείας (International Security Organization) και η διεθνή ηλεκτροτεχνική επιτροπή (International Electrotechnical Commission) αποτελούν πλαίσια αναφοράς για την εφαρμογή προτύπων για τον κυβερνοχώρο.

3.6.1 ISO/IEC 27001

Το ISO/IEC 27001 είναι το πιο γνωστό πρότυπο, το οποίο παρέχει τις απαιτήσεις ασφαλείας σε ένα σύστημα διαχείρισης ασφάλειας πληροφοριών. Ο διεθνής οργανισμός ασφαλείας (ISO) περιγράφει ένα σύστημα διαχείρισης ασφάλειας πληροφοριών, ως μια συστηματική προσέγγιση διαχείρισης ευαίσθητων επιχειρησιακών δεδομένων ώστε αυτά να παραμείνουν ασφαλή [31]. Περιλαμβάνει ανθρώπους, διαδικασίες και συστήματα πληροφορικής με την εφαρμογή της διαδικασίας διαχείρισης κινδύνου. Ουσιαστικά το

συγκεκριμένο πρότυπο περιγράφει τον τρόπο με τον οποίο μια επιχείρηση πρέπει να θέσει τους στόχους της στην ασφάλεια και να καθορίσει τους κινδύνους που απειλούν αυτούς τους στόχους. Η επιχείρηση μπορεί να ανταποκριθεί στους κινδύνους που έχουν καθοριστεί, με ένα σχέδιο αντιμετώπισης κινδύνου. Ένα σημαντικό μέρος αυτού του σχεδίου είναι η επιλογή των κατάλληλων ελέγχων ασφαλείας.

Το πρότυπο ISO/IEC 27001 περιλαμβάνει μια λίστα ελέγχων για κάθε στόχο ασφαλείας που έχει θέσει η επιχείρηση, αν και δεν είναι υποχρεωτική η εφαρμογή όλων αυτών των ελέγχων, καθώς μπορούν να χρησιμοποιηθούν και άλλοι έλεγχοι ασφαλείας. Επίσης, το συγκεκριμένο πρότυπο μαζί με αλλά πρότυπα της οικογένειας 27000, παρέχουν ένα πλαίσιο για ελέγχους της ασφάλειας της επιχείρησης από τρίτους. Όπως αναφέρθηκε και προηγούμενος, το ISO 27001 είναι ένα σύστημα διαχείρισης και ακολουθεί τον κύκλο Σχεδίασε, Πράξε, Έλεγξε, Δράσε (Plan Do Check Act) [32].

Εικόνα 6 Κύκλος PDCA [47]

Πίνακας 5 Ο κύκλος PDCA με μια ματιά

Σχεδίασε (Καθόρισε το σύστημα διαχείρισης κινδύνου)	Καθόρισε τις πολιτικές, τους στόχους, τις διαδικασίες σχετικά με την διαχείριση κινδύνου και βελτίωσε την ασφάλεια πληροφοριών ώστε να είναι εναρμονισμένη με τους στόχους και τις πολιτικές της επιχείρησης.

Πράξε (Εφάρμοσε και λειτούργησε το σύστημα διαχείρισης κινδύνου)	Εφάρμοσε και λειτούργησε τις πολιτικές, τους ελέγχους, και τις διαδικασίες του συστήματος διαχείρισης κινδύνου.
Έλεγξε (παρακολούθησε και έλεγξε το σύστημα διαχείρισης κινδύνου)	Αξιολόγησε και οπού χρειάζεται, μέτρησε την επίδοση των πολιτικών, των στόχων και την πρακτική εμπειρία του συστήματος διαχείρισης κινδύνου και ανέφερε τα αποτελέσματα για επανέλεγχο.
Δράσε (διατήρησε και βελτίωσε το σύστημα διαχείρισης κινδύνου)	Λάβε προληπτικές και διορθωτικές ενέργειες, βάση των αποτελεσμάτων του εσωτερικού ελέγχου του συστήματος διαχείρισης κινδύνου, προκειμένου να επιτευχθεί η συνεχής βελτίωση του.

Η οικογένεια του προτύπου ISO 27000 μεγαλώνει συνέχεια τα τελευταία χρονιά, καθώς πλέον περιλαμβάνει πάνω από 40 νέα πρότυπα. Η παρακάτω λίστα παρέχει επιπλέον πληροφορίες για τα πιο σημαντικά πρότυπα της οικογένειας ISO 27000.

Πίνακας 6 Τα σημαντικότερα πρότυπα της οικογένειας ISO 27000 [33]

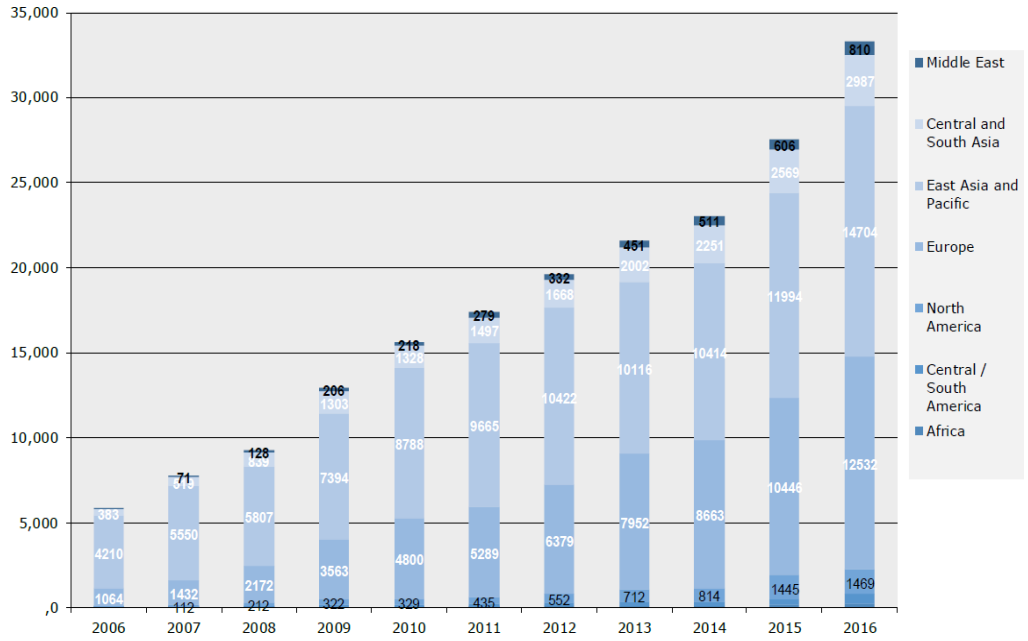
Αριθμός ISO/IEC	Στόχος
ISO/IEC 27002	Παρέχει κατευθυντήριες γραμμές και γενικές αρχές για την δημιουργία, την εφαρμογή και την διατήρηση συστημάτων διαχειρίσεις ασφάλειας πληροφοριών.

ISO/IEC 27003	Οδηγός εφαρμογής του ISO 27001
ISO/IEC 27004	Οδηγός για την παρακολούθηση, μέτρηση, ανάλυση και αξιολόγηση ενός συστήματος διαχείρισης ασφάλειας πληροφοριών
ISO/IEC 27005	Παρέχει κατευθυντήριες γραμμές για την διαχείριση κινδύνου ασφάλειας πληροφοριών
ISO/IEC 27011	Προσθέτει απαιτήσεις, οδηγίες και ελέγχους συγκεκριμένα για επιχειρήσεις τηλεπικοινωνίας
ISO/IEC 27017	Προσθέτει απαιτήσεις, οδηγίες και ελέγχους συγκεκριμένα για υπηρεσίες cloud
ISO/IEC 27018	Προσθέτει απαιτήσεις, οδηγίες και ελέγχους συγκεκριμένα για δημόσιες υπηρεσίες cloud
ISO/IEC 27019	Προσθέτει απαιτήσεις, οδηγίες και ελέγχους συγκεκριμένα για την βιομηχανία ηλεκτρικής ενέργειας
ISO/IEC 27032	Προσθέτει απαιτήσεις, οδηγίες, και ελέγχους για την βελτίωση της κυβερνοασφάλειας
ISO/IEC 27033	Προσθέτει απαιτήσεις, οδηγίες και ελέγχους για την ασφάλεια δικτύου
ISO/IEC 27034	Προσθέτει απαιτήσεις, οδηγίες και ελέγχους για την ασφάλεια προγραμμάτων
ISO/IEC 27035	Προσθέτει απαιτήσεις, οδηγίες και ελέγχους για διαχείρισης συμβάντων
ISO/IEC 27036	Προσθέτει απαιτήσεις, οδηγίες και ελέγχους για διαχείριση προμηθευτών

Κατά την δημιουργία ενός συστήματος διαχείρισης κινδύνου που μπορεί να πιστοποιηθεί με το ISO 27001, μια επιχείρηση θα πρέπει να αναπτύξει και να τεκμηριώσει τις απαραίτητες διαδικασίες και ελέγχους ISO 27001. Αυτές οι διαδικασίες και οι έλεγχοι θα πρέπει στην συνέχεια να εφαρμοστούν σύμφωνα με αυτά τα τεκμήρια. Οι τακτικοί έλεγχοι, οι έλεγχοι διαχείρισης αυτών των τεκμηρίων και η εφαρμογή τους είναι μέρος των απαιτήσεων του ISO 27001, το οποίο επίσης απαιτεί το σύστημα διαχείρισης κινδύνου να μην είναι απλά συμμορφωμένο αλλά να είναι και συνέχεια ενημερωμένο. Όλες οι περιπτώσεις μη συμμόρφωσης που διαπιστωθήκαν κατά την διάρκεια του εσωτερικού ελέγχου πρέπει να μετριαστούν με διορθωτικές και προληπτικές ενέργειες. Με άλλα λόγια, όχι μόνο πρέπει να διορθωθούν τα σφάλματα, αλλά πρέπει να παρθούν μετρά για να αποφευχθούν τα συγκεκριμένα σφάλματα στο μέλλον.

Μόλις ολοκληρωθούν τα παραπάνω, η διαδικασία της προτυποποίησης μπορεί να ξεκινήσει. Η διαδικασία αυτή χωρίζεται σε δυο στάδια: Στον έλεγχο Στάδιο 1 και στον έλεγχο Στάδιο 2. Στον έλεγχο Στάδιο 1, ο ελεγκτής ελέγχει κατά πόσο η τεκμηρίωση της επιχείρησης είναι συμμορφωμένη με το πρότυπο ISO 27001. Κατά τον έλεγχο Στάδιο 2, ο ελεγκτής ελέγχει το αν όλες οι δραστηριότητες της επιχείρησης είναι συμμορφωμένες με το πρότυπο ISO 27001 αλλά και τις τεκμηρίωσης που έχουν γίνει προηγούμενος. Οποιαδήποτε μη συμμόρφωση που διαπιστώνει ο ελεγκτής που αποτρέπει την προτυποποίηση, πρέπει να διορθωθεί εντός συγκεκριμένης χρονικής περιόδου. Το πρότυπο ISO 27001 έχει ισχύ για τρία χρονιά, τα οποία όταν παρέλθουν θα πρέπει να επαναληφθεί ο έλεγχος Στάδιο 1 και Στάδιο 2 ώστε να ανανεωθεί [34].

Ο διεθνής οργανισμός ασφαλείας (ISO) εκδίδει τακτικά το «ISO Survey of Certifications», το οποίο δείχνει τον αριθμό των εγκύρων πιστοποιητικών στα πρότυπα διαχείρισης συστημάτων παγκοσμίως. Η τελευταία έκδοση αυτής της έρευνας είναι από το 2016 και παρουσιάζει την ιδιαίτερα μεγάλη αύξηση του ISO 27001 με 21%, το νούμερο των πιστοποιήσεων έχει φτάσει στις 33,290 παγκοσμίως. Από αυτόν τον αριθμό, οι 12,532 έχουν εκδοθεί στην Ευρώπη, δηλαδή σχεδόν το 37% όπως μπορούμε να δούμε στην παρακάτω εικόνα.



Εικόνα 7 Αριθμός πιστοποιήσεων ISO 27001 [34]

Η έρευνα καταδεικνύει επίσης ότι οι επιχειρήσεις με πρότυπο ISO 27001 προέρχονται από όλους τους τομείς της οικονομίας. Τέλος, η έρευνα καθιστά σαφές ότι το ISO 27001 είναι πρότυπο για την ασφάλεια πληροφοριών με την μεγαλύτερη άνοδο [34].

Βέβαια, η εφαρμογή του προτύπου ISO 27001 στις μικρομεσαίες επιχειρήσεις με μικρό αριθμό υπάλληλων είναι δύσκολη λόγω της πολυπλοκότητας εφαρμογής σε μειωμένο πεδίο. Παρόλα αυτά, είναι δυνατό να εφαρμοστούν μερικές καλές πρακτικές ελέγχου ασφαλείας, όπως αυτές που παρουσιάζονται στο ISO 27032.

3.6.2 ISO/IEC 27032

Το ISO/IEC 27032 είναι ένα διεθνές πρότυπο που επικεντρώνεται ρητά στην ασφάλεια στον κυβερνοχώρο. Παρόλο που οι έλεγχοι ασφαλείας που συνίστανται στο συγκεκριμένο πρότυπο δεν είναι τόσο ακριβείς ή περιγραφικοί όσο με εκείνους που παρέχονται στο ISO

27001, αναγνωρίζει τους φορείς οπού βασίζονται οι επιθέσεις στον κυβερνοχώρο, συμπεριλαμβανομένων αυτών που προέρχονται εκτός κυβερνοχώρου. Επιπλέον, περιλαμβάνει κατευθυντήριες γραμμές για την προστασία των πληροφοριών πέρα από τα σύνορα της επιχείρησης, όπως με πελάτες, συνεργάτες κ.α. [35].

Οι έλεγχοι ασφαλείας στον κυβερνοχώρο που προσδιορίζονται στο πρότυπο ISO 27032 θα πρέπει να αποτελούν σημείο αναφοράς για την ασφάλεια των επιχειρήσεων στον κυβερνοχώρο. Επίσης καλύπτει βασικές πρακτικές ασφαλείας [36]:

- Επισκόπηση της ασφαλείας στον κυβερνοχώρο
- Εξηγεί την σχέση της ασφαλείας στον κυβερνοχώρο με άλλα είδη ασφαλείας
- Παρέχει καθοδήγηση και ελέγχους για την αντιμετώπιση κοινών κίνδυνων ασφαλείας στον κυβερνοχώρο
- Παρέχει πλαίσιο που επιτρέπει στους ενδιαφερομένους φορείς να συνεργαστούν για την επίλυση ζητημάτων ασφαλείας στον κυβερνοχώρο
- Ορισμός των ενδιαφερομένων φορέων και περιγραφή των ρόλων τους στην ασφάλεια στον κυβερνοχώρο.

3.7 General Data Protection Regulation (GDPR)

Το General Data Protection Regulation (GDPR) είναι ο πιο σκληρός νόμος στον κόσμο σε σχέση με την ιδιωτικότητα και την ασφάλεια. Αν και έχει συνταχθεί και εγκριθεί από την Ευρωπαϊκή Ένωση, επιβάλλει τους κανονισμούς του σε οργανισμούς και επιχειρήσεις σε όλον τον κόσμο, εφόσον στοχεύουν ή συγκεντρώνουν δεδομένα σχετικά με κατοίκους της Ευρωπαϊκής Ένωσης. Ο κανονισμός αυτός τέθηκε σε ισχύ στις 25 Μάιου 2018. Το GDPR θα επιβάλει σκληρά πρόστιμα σε όσους παραβιάζουν τα πρότυπα προστασίας της ιδιωτικής ζωής και ασφάλειας, με κυρώσεις που μπορεί να φτάσουν τα δεκάδες εκατομμύρια ευρώ [37].

Με τον νέο αυτό κανονισμό, η Ευρώπη σηματοδοτεί την αυστηρή στάση της όσον αφορά την ιδιωτικότητα και την ασφάλεια των δεδομένων, σε μια εποχή που οι περισσότεροι άνθρωποι εμπιστεύονται τα προσωπικά τους δεδομένα σε υπηρεσίες cloud και οι παραβιάσεις είναι ένα καθημερινό φαινόμενο. Το GDPR είναι μεγάλο, αρκετά εκτεταμένο και ελαφρύ όσον αφορά τις ιδιαιτερότητες, καθιστώντας έτσι την συμμόρφωση μαζί του μια ιδιαίτερα δύσκολη διαδικασία, ιδιαίτερα για τις μικρομεσαίες επιχειρήσεις.

Σύμφωνα με το GDPR, εάν μια επιχείρηση ή οργανισμός διαχειρίζεται δεδομένα, πρέπει να κάνουν τα παρακάτω σύμφωνα με το Άρθρο 5.1-2 [41]:

- **Νομιμότητα, δικαιοσύνη, διαφάνεια** – Η επεξεργασία των δεδομένων πρέπει να είναι νόμιμη, δίκαιη και διαφανής για το υποκείμενο των δεδομένων.
- **Περιορισμός στόχου** - Τα δεδομένα πρέπει να επεξεργάζονται για νόμιμους σκοπούς που καθορίζονται ρητά στο υποκείμενο των δεδομένων όταν αυτά συλλέγονται.
- **Ελαχιστοποίηση δεδομένων** – Πρέπει να συλλέγονται και να διαχειρίζονται μόνο τα δεδομένα που είναι απαραίτητα για τους σκοπούς που έχουν καθοριστεί.
- **Ακρίβεια** – Πρέπει να διατηρούνται τα προσωπικά δεδομένα ακριβή και ενημερωμένα.
- **Περιορισμός αποθήκευσης** – Μπορούν να παραμείνουν αποθηκευμένα προσωπικά δεδομένα προσωπικής ταυτοποίησης για όσο χρονικό διάστημα είναι απαραίτητο από τον καθορισμένο σκοπό.
- **Ακεραιότητα και εμπιστευτικότητα** – Η επεξεργασία των δεδομένων πρέπει να γίνεται με τέτοιο τρόπο ώστε να εξασφαλίζεται η κατάλληλη ασφάλεια, ακεραιότητα και εμπιστευτικότητα (π.χ. χρήση κρυπτογράφησης)
- **Λογοδοσία** – Ο υπεύθυνος επεξεργασίας δεδομένων είναι υπεύθυνος για να καταδείξει την συμμόρφωση με το GDPR με όλες τις άλλες αρχές.

3.7.1 GDPR ΣΤΙΣ ΜΙΚΡΟΜΕΣΑΙΕΣ ΕΠΙΧΕΙΡΗΣΕΙΣ

Οι μικρομεσαίες επιχειρήσεις στην Ευρωπαϊκή Ένωση πρέπει να συμμορφωθούν με το GDRP, καθώς η εφαρμογή του δεν εξαρτάται από το μέγεθος της επιχείρησης αλλά από την φύση των δραστηριοτήτων της. Δραστηριότητες που παρουσιάζουν μεγάλο κίνδυνο για τα δικαιώματα και τις ελευθερίες των ατόμων, ανεξάρτητα αν εκτελούνται από μικρομεσαίες επιχειρήσεις ή από μεγάλη επιχείρηση, προκαλούν την εφαρμογή αυστηρότερων κανόνων [38].

Παρόλα αυτά, ορισμένες υποχρεώσεις του κανονισμού μπορεί να μην ισχύουν για όλες τις μικρομεσαίες επιχειρήσεις. Για παράδειγμα, οι επιχειρήσεις με λιγότερους από 250 υπάλληλους δεν χρειάζεται να τηρούν αρχεία για τις δραστηριότητες επεξεργασίας των δεδομένων τους πάρα μόνο αν η επεξεργασία προσωπικών δεδομένων είναι συχνή δραστηριότητα της επιχείρησης, αποτελεί απειλή για τα δικαιώματα και την ελευθέρια των ατόμων και τέλος κατέχει ευαίσθητα δεδομένα. Ομοίως, οι μικρομεσαίες επιχειρήσεις για να ορίσουν έναν υπεύθυνο προστασίας δεδομένων θα πρέπει να ισχύουν τα παραπάνω.

Το GDPR αποτελεί έναν σύνθετο κανονισμό και πολλές μικρομεσαίες επιχειρήσεις δυσκολεύονται στην κατανόηση του και την συμμόρφωση τους με αυτό. Παρακάτω υπάρχει ένας οδηγός με πέντε προτάσεις που μπορούν να ακολουθήσουν οι μικρομεσαίες επιχειρήσεις για να αποδείξουν την συμμόρφωση τους [39].

1. **Έλεγχος** – Είναι η διαδικασία της διεξοδικής χαρτογράφησης των προσωπικών δεδομένων που χρησιμοποιούνται σε μια επιχείρηση. Είναι το κλειδί για ολόκληρο το πρόγραμμα συμμόρφωσης με το GDPR και το πρώτο βήμα που πρέπει γίνει. Περιλαμβάνει τον έλεγχο τους είδους των προσωπικών δεδομένων που κατέχει η επιχείρηση και πως αυτά αποθηκεύονται. Θα πρέπει να καθοριστεί αν τα προσωπικά δεδομένα είναι δικαιολογημένα και νόμιμα στην κατοχή της επιχείρησης. Αφού πραγματοποιηθεί αυτό, θα πρέπει να είναι σε θέση να κρίνουν αν τα δεδομένα που κατέχει η επιχείρηση είναι επαρκώς προστατευμένα. Επίσης, η επιχείρηση θα πρέπει να έχει σοβαρά

μετρά ασφαλείας για την προστασία των προσωπικών δεδομένων ώστε να αποφευχθεί η μη εξουσιοδοτημένη χρήση τους.

2. **Ανάλυση** – Ο έλεγχος χαρτογράφησης δεδομένων είναι μια σημαντική άσκηση, η οποία είναι πιθανό να χρειαστεί αρκετό χρόνο για να πραγματοποιηθεί, εάν γίνει σωστά. Τα αποτελέσματα του ελέγχου χαρτογράφησης δεδομένων θα επισημάνουν αδυνάμους τομείς και μη συμμόρφωσης στο ισχύον καθεστώς προστασίας δεδομένων. Η ομάδα που έχει αναλάβει την συμμόρφωση με το GDPR πρέπει στην συνέχεια να αναλάβει την ανάπτυξη ενός σχεδίου για την αντιμετώπιση όλων των κίνδυνων που εντοπίζονται από τον έλεγχο χαρτογράφησης δεδομένων, ξεκινώντας από τα υψηλού κίνδυνου ευρήματα. Συνίσταται η ομάδα αυτή να αποτελείται από άτομα από όλη την επιχείρηση, έτσι ώστε κάθε άτομο να μπορεί να εξετάσει ποια προσωπικά δεδομένα επεξεργάζονται οι αντίστοιχες υπηρεσίες τους.

3. **Καθαρισμός** – Μια από τις βασικές ενέργειες που πρέπει να πραγματοποιηθούν στο πλαίσιο του προγράμματος συμμόρφωσης με το GDPR είναι να καθαριστούν τα προσωπικά δεδομένα που διατηρούνται στα συστήματα της επιχείρησης. Για παράδειγμα, τα προσωπικά δεδομένα υπαλλήλων που έχουν αποχωρήσει από την επιχείρηση μπορούν να διαγράφουν ή προσωπικά δεδομένα πελατών τα οποία δεν έχουν χρησιμότητα πλέον.

4. **Προστασία** – Η προστασία είναι ίσως το πιο σημαντικό στάδιο αυτού του οδηγού. Μια από τις θεμελιώδεις αρχές που διέπουν το GDPR είναι ότι τα προσωπικά δεδομένα πρέπει να διατηρούνται ασφαλή, ιδίως την ψηφιακή εποχή που διανύουμε, οπού οι επιθέσεις σε δεδομένα συμβαίνουν συνεχώς. Το GDPR απαιτεί από κάθε οντότητα που επεξεργάζεται δεδομένα προσωπικού χαρακτήρα να διαθέτει ισχυρά και επαρκή συστήματα ασφαλείας για την προστασία των προσωπικών δεδομένων, τα οποία να είναι ανάλογα της αξίας των δεδομένων που προστατεύουν. Είναι σημαντικό οι επιχειρήσεις να μπορούν να αποδείξουν ότι όλα τα συστήματα και οι διαδικασίες ασφαλείας

έχουν εκτιμηθεί και είναι επαρκείς, καθώς είναι μια συνεχής υποχρέωση των επιχειρήσεων προς το GDPR και θα πρέπει να επανεξετάζεται σε τακτά χρονικά διαστήματα. Εάν η επιχείρηση απαλλάσσεται από τον διορισμό ενός υπευθύνου προστασίας δεδομένων, θα πρέπει να έχει έστω ένα άτομο στην επιχείρηση που θα αναλαμβάνει την συμμόρφωση με το GDPR.

5. **Συνεχής συμμόρφωση** – Για να είναι επιτυχής η συμμόρφωση, οι αρχές του GDPR πρέπει να ενσωματωθούν στην επιχείρηση και να αντιπροσωπεύουν τους συνήθεις τρόπους λειτουργίας της. Θα πρέπει να οδηγήσουν στην αλλαγή κουλτούρας, για το καλύτερο, στο πως η επιχείρηση διαχειρίζεται τα προσωπικά δεδομένα. Θα πρέπει να γίνονται τακτικοί έλεγχοι στις διαδικασίες ασφαλείας των δεδομένων, καθώς και τα προηγούμενα τέσσερα βήματα. Πρέπει να διατηρούνται πλήρη στοιχεία σχετικά με την συμμόρφωση της επιχείρησης με το GDPR, ώστε να είναι εύκολο να απαντηθούν ερωτήσεις σχετικά με την ασφάλεια δεδομένων, την συμμόρφωση με το GDPR και ελέγχους για τυχόν παραβιάσεις ασφαλείας.

Η έρευνα «GDPR Small Business Survey» [40] που πραγματοποιήθηκε το 2019 και συμμετείχαν 716 μικρές επιχειρήσεις από την Ισπανία, Γαλλία, Ιρλανδία και Ηνωμένο Βασίλειο, ώστε να κατανοήσουμε πως οι επιχειρήσεις αντιμετωπίζουν τις νέες απαιτήσεις του GDPR, έδειξε ότι υπάρχει μεγάλη προθυμία από τις επιχειρήσεις να συμμορφωθούν με τον νέο κανονισμό και έχουν ξοδέψει μεγάλα χρηματικά ποσά σε συμβούλους και σε νέα πληροφοριακά συστήματα για να το πέτυχουν αυτό. Επίσης, οι πιο πολλές επιχειρήσεις πιστεύουν ότι το GDPR δεν θα επιβραδύνει την ανάπτυξη των επιχειρήσεων. Τέλος, παραπάνω από τις μισές επιχειρήσεις πιστεύουν ότι έχουν συμμορφωθεί πλήρως με το GDPR, ενώ 36% πιστεύει ότι σχεδόν έχουν συμμορφωθεί.

ΚΕΦΑΛΑΙΟ 4
Μεθοδολογία και Συλλογή Δεδομένων

Σε αυτό το κεφάλαιο θα αναλυθεί η μεθοδολογία που ακολουθήθηκε για την συλλογή απαντήσεων των ερευνητικών ερωτημάτων. Στην παρακάτω εικόνα φαίνεται η ερευνητική διαδικασία που ακολουθήθηκε.

Εικόνα 8 Ερευνητική διαδικασία

Η ερευνητική διαδικασία χωρίστηκε σε επτά φάσεις με σκοπό την καταδείξει την ετοιμότητα της ασφάλειας των μικρομεσαίων επιχειρήσεων στον κυβερνοχώρο.

4.1 Ερευνητικος Σκοπος

Ο ερευνητικός σκοπός είναι η κατανόηση της τρέχουσας κατάστασης αλλά και των μελλοντικών τάσεων της ασφάλειας πληροφοριών στις μικρομεσαίες επιχειρήσεις στην Κυπρο. Για μεγαλύτερη κατανόηση του θέματος πραγματοποιήθηκε μελέτη διαφόρων πηγών που αφορούν την ασφάλεια πληροφοριών, τον κυβερνοχώρο και διαφόρων προτύπων και πλαισίων που αφορούν την κυβερνοασφάλεια. Η φάση αυτή της έρευνας μπορεί να χαρακτηριστεί και ως διερευνητική. Επίσης, κατά την διάρκεια της φάσης αυτής λήφθηκαν υπόψη και διατυπώθηκαν πιθανά ερευνητικά ερωτήματα.

4.2 Ερευνητικος Σχεδιασμος

Ο ερευνητικός σχεδιασμός συντάχθηκε τον Απρίλιο του 2019 και βασίστηκε στην περιγραφή του σχεδίου και τα πορίσματα της διερευνητικής φάσης. Το περίγραμμα του σχεδίου ήταν ο ερευνητικός σκοπός και οι απαιτήσεις αυτού, γιατί η έρευνα αυτή είναι απαραίτητη, ποιες ερευνητικές μέθοδοι πρόκειται να χρησιμοποιηθούν και γιατί. Ο σχεδιασμός περιλάμβανε επίσης ένα πρώιμο χρονοδιάγραμμα της έρευνας, τον προϋπολογισμό, διάφορες άλλες οικονομικές εκτιμήσεις καθώς και τις αρχές δεοντολογίας της έρευνας.

4.2.1 Ερευνητικες Μεθοδοι

Ο αρχικός σχεδιασμός περιλάμβανε δυο έρευνες. Η μια έρευνα θα διεξαγόταν μέσω συνεντεύξεων ατόμων που είναι υπεύθυνα για την ασφάλεια πληροφοριών μικρομεσαίων επιχειρήσεων και η δεύτερη θα πραγματοποιούνταν μέσω ενός διαδικτυακού

ερωτηματολογίου. Μετά από περαιτέρω εξέταση, αποφασίστηκε από κοινού με την επιβλέπουσα καθηγήτρια να πραγματοποιηθεί μόνο η έρευνα μέσω διαδικτυακού ερωτηματολογίου λόγω της φύσης της έρευνας. Η ασφάλεια πληροφοριών αποτελεί δύσκολο θέμα προς συζήτηση και θα ήταν πρακτικά αδύνατο να βρεθούν πρόθυμες επιχειρήσεις να απαντήσουν μέσω συνεντεύξεων. Επίσης, το διαδικτυακό ερωτηματολόγιο είναι ευκολότερο να συμπληρωθεί από τους ερωτηθέντες, καθώς μπορούν να το συμπληρώσουν την ώρα και την ημέρα που επιθυμούν αυτοί.

4.2.2 Ερευνητικο Δειγμα

Οι ερωτηθέντες της έρευνας διαλέχθηκαν από μικρομεσαίες επιχειρήσεις που δραστηριοποιούνται στην Κυπρο. Η σύσταση της Ευρωπαϊκής Επιτροπής σχετικά με τον ορισμό των μικρομεσαίων επιχειρήσεων χρησιμοποιήθηκε στην παρούσα έρευνα. Λόγω του μικρού μεγέθους της Κύπρου θεωρήθηκε ότι ένα δείγμα πάνω από 25 απαντήσεων θα ήταν κατάλληλο για να μπορέσει η έρευνα να θεωρηθεί έγκυρη και να έχει σωστά αποτελέσματα.

4.2.3 Χρονοδιαγραμμα και Προϋπολογισμος

Το αρχικό χρονοδιάγραμμα του ερευνητικού σχεδίου ήταν να διεξαχθεί το διαδικτυακό ερωτηματολόγιο τον Ιούνιο, Ιούλιο και Αύγουστο του 2019. Το χρονοδιάγραμμα αυτό τροποποιήθηκε καθώς αποφασίστηκε να διεξαχθεί το διαδικτυακό ερωτηματολόγιο τον Σεπτέμβριο και Οκτώβριο του ίδιου έτους, λόγω του ότι το καλοκαίρι πολλοί εργαζόμενοι των επιχειρήσεων απουσιάζουν λόγω των καλοκαιρινών διακοπών και δεν θα ήταν σε θέση να απαντήσουν. Δεν υπήρξε θέμα προϋπολογισμού καθώς το ερωτηματολόγιο που χρησιμοποιήθηκε ήταν το Forms της εταιρίας Google, το οποίο διατίθεται δωρεάν.

4.2.4 Αρχες Δεοντολογιας

Το κομμάτι των αρχών δεοντολογίας σε μια ερευνά καθορίζει τις αρχές που καθορίστηκαν κατά την διεξαγωγή της έρευνας, της ανάλυσης και της υποβολής της. Το διαδικτυακό ερωτηματολόγιο της έρευνας δημιουργήθηκε και εκτελέστηκε βάση του νόμου 125(I)/2018 της Κυπριακής Δημοκρατίας [46] που αφορά την προστασία των προσωπικών δεδομένων. Όλα τα προσωπικά δεδομένα που συλλέχθηκαν ήταν ανώνυμα, όπως επίσης όλα τα προσωπικά δεδομένα που συλλέχθηκαν δεν χρησιμοποιήθηκαν για οποιοδήποτε άλλο σκοπό. Τέλος, στο διαδικτυακό ερωτηματολόγιο, οι ερωτηθέντες ρωτήθηκαν αν επιβεβαιώνουν ότι διάβασαν και κατάλαβαν το έντυπο συγκατάθεσης που υπήρχε στην πρώτη σελίδα τους ερωτηματολογίου, καθώς και αν συμφωνούν με αυτό.

4.3 Ερωτηθεντες, Ερωτηματολογιο και Χρονοδιαγραμμα

Το διαδικτυακό ερωτηματολόγιο σχεδιάστηκε και εκτελέστηκε μέσω της εφαρμογής Forms της Google, η οποία διατίθεται δωρεάν. Η ερωτήσεις που έγιναν για την έρευνα μπορούν να βρεθούν στο Παράρτημα Α. Το ερωτηματολόγιο δημιουργήθηκε στην ελληνική γλώσσα αλλά χρησιμοποιήθηκαν αρκετές αγγλικές ορολογίες ώστε να είναι πιο εύκολο για τους ερωτηθέντες να κατανοήσουν τις ερωτήσεις, καθώς στον χώρο της πληροφορικής σπάνια χρησιμοποιούνται ορολογίες στα ελληνικά.

Ο σχεδιασμός του ερωτηματολογίου επικεντρώθηκε στο να γίνουν οι ερωτήσεις εύκολα κατανοητές και στο να μπορεί να απαντηθεί το ερωτηματολόγιο σε 5 με 10 λεπτά. Ήταν πολύ σημαντικό το να είναι άνετοι οι ερωτηθέντες να απαντήσουν στις ερωτήσεις αλλά και να μην χρειαστεί πολύς χρόνος γι' αυτό. Μόλις το ερωτηματολόγιο δοκιμάστηκε και εγκρίθηκε, γράφτηκε ένα χρονοδιάγραμμα. Η αποστολή του ερωτηματολογίου έγινε τμηματικά ώστε να αποφευχθεί η ανεπιθύμητη αλληλογραφία.

Ο στόχος του ερωτηματολογίου ήταν να βρεθούν άτομα που λαμβάνουν τις αποφάσεις σχετικά με την ασφάλεια πληροφοριών των επιχειρήσεων. Οι επαφές έλαβαν προτεραιότητα λαμβάνοντας υπόψη τον ρόλο τους στην επιχείρηση. Πολλές μικρές επιχειρήσεις δεν έχουν στο δυναμικό τους κάποιο άτομο που ασχολείται με τα πληροφοριακά συστήματα, γι' αυτόν τον λόγο δόθηκε προτεραιότητα και στους ιδιοκτήτες των επιχειρήσεων.

4.4 Συλλογη Δεδομενων

Η συλλογή δεδομένων πραγματοποιήθηκε κατά την διάρκεια του Σεπτεμβρίου και Οκτωβρίου του έτους 2019. Στόχος ήταν να ληφθούν τουλάχιστον 25 απαντήσεις καθώς θεωρείται το ελάχιστο για τέτοιου είδους έρευνα εν συγκρίσει με την χώρα που διεξάγεται. Το ερωτηματολόγιο εστάλη μέσω ηλεκτρονικού ταχυδρομείου και η συλλογή δεδομένων περιλάμβανε την παρακολούθηση της ποιότητας των απαντήσεων και τυχόν προβλημάτων που θα μπορούσαν να προκύψουν. Τέλος, κανένας από τους ερωτηθέντες δεν θέλησε να αποσύρει την συγκατάθεση του για την συμμετοχή στο ερωτηματολόγιο, όπως είχαν δικαίωμα να κάνουν.

4.5 Επεξεργασια Δεδομενων και Αναλυση

Τα δεδομένα που συλλέχθηκαν, επεξεργάστηκαν με την χρήση του Microsoft Excel, Google Sheets και IBM SPSS Statistics. Η ανάλυση των δεδομένων έγινε πρωτίστως με ποσοτικές μεθόδους αλλά έγινε επίσης ποιοτική ανάλυση για τις ανοικτού τύπου ερωτήσεις.

ΚΕΦΑΛΑΙΟ 5
Αποτελέσματα

Το συγκεκριμένο κεφάλαιο θα χωριστεί σε τέσσερα μέρη. Στο πρώτο μέρος θα εξεταστούν τα δεδομένα της έρευνας σχετικά με τους ερωτηθέντες. Στο δεύτερο μέρος θα εξεταστεί η τωρινή κατάσταση της ασφάλειας πληροφοριών των επιχειρήσεων, στο τρίτο μέρος θα δούμε μελλοντικά σχέδια ανάπτυξης και επένδυσης στην ασφάλεια και τέλος αναπτύχθηκε ένας οδηγός για την προετοιμασία των μικρομεσαίων επιχειρήσεων βάση των αποτελεσμάτων του ερωτηματολογίου.

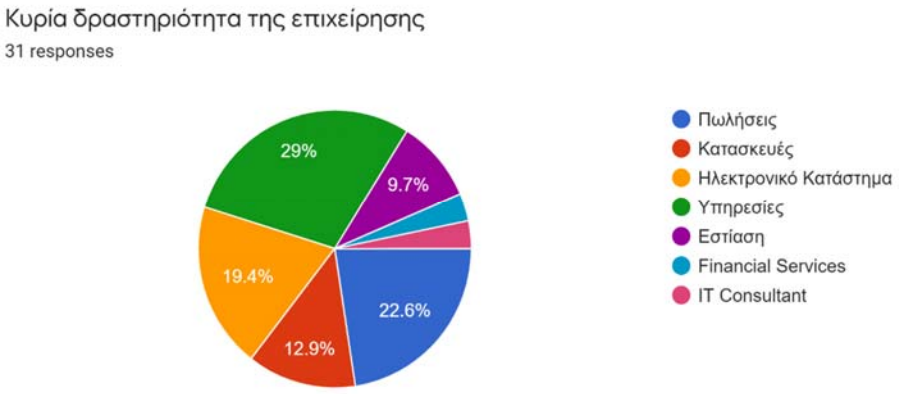
5.1 Δεδομενα της Έρευνας Σχετικα με τους Ερωτηθεντες

Το ερωτηματολόγιο στάλθηκε σε πάνω από 60 επιχειρήσεις και απαντήθηκε από 31, αυτό μας δίνει ποσοστό ανταπόκρισης περίπου 50%. Από τους 31 ερωτηθέντες, οι 12 απάντησαν ότι είναι ιδιοκτήτες της επιχείρησης, 17 απάντησαν ότι ανήκουν στο τμήμα IT της επιχείρησης και τέλος ένα άτομο απάντησε ότι είναι λογιστής και ένα τεχνικός υπεύθυνος της επιχείρησης.

Το 71% των ερωτηθέντων δήλωσε ότι είναι υπεύθυνοι για την ασφάλεια πληροφοριών της επιχείρησης, το 22,6% ότι δεν είναι, ενώ υπήρχαν δύο άτομα που δεν μπόρεσαν να απαντήσουν στην ερώτηση.

Το επίπεδο μόρφωσης των ερωτηθέντων μπορεί να θεωρηθεί αρκετά υψηλό καθώς το 58,1% έχει πανεπιστημιακή μόρφωση, το 32,3% κατέχει μεταπτυχιακό τίτλο, ενώ μόλις το 6,5% των ερωτηθέντων έχει δευτεροβάθμια εκπαίδευση.

Οι επιχειρήσεις που έλαβαν μέρος στο ερωτηματολόγιο είναι από ένα ευρύ φάσμα της οικονομίας. Το 29% των απαντήσεων ανήκουν σε μικρομεσαίες επιχειρήσεις που παρέχουν υπηρεσίες, 22,6% σε μικρομεσαίες επιχειρήσεις λιανικής πώλησης, 19,4% ανήκουν σε ηλεκτρονικά καταστήματα, 12,9% σε επιχειρήσεις του κατασκευαστικού κλάδου, 9,7% σε επιχειρήσεις εστίασης, ενώ είχαμε και απαντήσεις από μια επιχείρηση που παρέχει αποκλειστικά υπηρεσίες IT και μια επιχείρηση που παρέχει υπηρεσίες οικονομικής φύσεως.

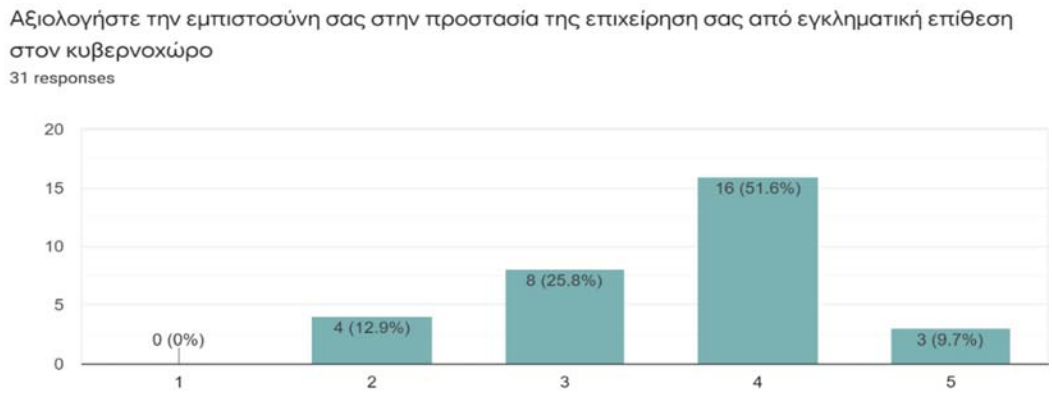


Εικόνα 9 Διάγραμμα επιχειρήσεων που έλαβαν μέρος στην έρευνα.

5.2 Ασφαλεια Πληροφοριων των Μικρομεσαιων Επιχειρησεων

Οι μικρομεσαίες επιχειρήσεις της Κύπρου έδειξαν ότι έχουν μεγάλη εμπιστοσύνη στην ασφάλεια πληροφοριών τους. Οι ερωτηθέντες κλήθηκαν να αξιολογήσουν την εμπιστοσύνη τους στην προστασία της επιχείρησης που εργάζονται από μια εγκληματική επίθεση στον

κυβερνοχώρο. Όπως διαπιστώνουμε από την παρακάτω Εικόνα 10, το 9,7% έχει πολύ εμπιστοσύνη, ενώ το 51,6% εμπιστεύεται αρκετά την προστασία της επιχείρησης. Το 25,8 δήλωσε ότι απλά εμπιστεύονται την προστασία, ενώ μόλις το 12,8 δείχνει να έχει μικρή εμπιστοσύνη στην προστασία της επιχείρησης από εγκληματική επίθεση στον κυβερνοχώρο.



Εικόνα 10 Εμπιστοσύνη στην προστασία της επιχείρησης από κυβερνοεπίθεση

Αν υποθέσουμε ότι η μέση τιμή εμπιστοσύνης για την προστασία των επιχειρήσεων από μια εγκληματική επίθεση στον κυβερνοχώρο είναι κοντά στις 3 μονάδες, θα εξετάσουμε αν η εμπιστοσύνη είναι σημαντικά διαφορετική. Όπως μπορούμε να δούμε στην παρακάτω Εικόνα 11, η μέση τιμή εμπιστοσύνης είναι 3,58 (±0,85) μονάδες.

One-Sample Statistics

	N	Mean	Std. Deviation	Std. Error Mean
Αξιολογήστε την εμπιστοσύνη σας στην προστασία της επιχείρηση σας από εγκληματική επίθεση στον κυβερνοχώρο	31	3.58	.848	.152

Εικόνα 11 One-Sample Statistics

Το p<a, άρα απορρίπτουμε την μηδενική υπόθεση ότι ο μέσος ορός του δείγματος είναι ίσος με 3. Συμπεραίνουμε ότι η μέση εμπιστοσύνη του δείγματος είναι σημαντικά διαφορετική από τη μέση εμπιστοσύνη των επιχειρήσεων, το οποίο συνεπάγεται ότι οι επιχειρήσεις στην Κυπρο έχουν μεγάλη εμπιστοσύνη στην ασφάλεια πληροφοριών τους.

One-Sample Test

	Test Value = 3					
					95% Confidence Interval of the Difference	
	t	df	Sig. (2-tailed)	Mean Difference	Lower	Upper
Αξιολογήστε την εμπιστοσύνη σας στην προστασία της επιχείρηση σας από εγκληματική επίθεση στον κυβερνοχώρο	3.815	30	.001	.581	.27	.89

Εικόνα 12 One-Sample Test

5.2.1 Έλεγχοι Διαχειρισης Ασφαλειας Πληροφοριων

Συνεχίζοντας στους ελέγχους διαχείρισης ασφάλειας πληροφοριών και πιο συγκεκριμένα στα τρία επίπεδα τα οποία είναι: η Διοικητική, Φυσική και Τεχνική ασφάλεια, παρατηρούμε πάλι ότι οι μικρομεσαίες επιχειρήσεις στην Κυπρο θεωρούν ότι βρίσκονται σε καλό επίπεδο.

Στην διοικητική ασφάλεια το 16,1% θεωρεί ότι είναι σε πολύ καλό επίπεδο και το 45,2% ότι είναι αρκετά καλό. Το 22,6% πιστεύει ότι είναι ούτε καλό αλλά ούτε κακό το επίπεδο της διοικητής τους ασφάλειας. Το 9,7% πιστεύει ότι δεν είναι αρκετά καλό και μόνο το 6,5% πιστεύει ότι δεν είναι καθόλου καλό. Η διοικητική ασφάλεια αποτελεί δύσκολο κομμάτι για τις μικρομεσαίες επιχειρήσεις και προκαλούν μεγάλη έκπληξη τα αποτελέσματα της.

Το φυσικό επίπεδο ασφάλειας για τις μικρομεσαίες επιχειρήσεις θεωρείται ίσως το πιο εύκολο καθώς δεν χρειάζεται να ξοδέψουν πολλά χρήματα, όπως επίσης και γνώση για να διασφαλιστεί ένα καλό φυσικό επίπεδο ασφάλειας. Αυτό φαίνεται και στα αποτελέσματα

καθώς το 22,6% θεωρεί ότι επιχείρηση τους έχει ένα πολύ καλό επίπεδο φυσικής ασφάλειας, το 41,9% θεωρεί ότι έχει ένα αρκετά καλό επίπεδο, ενώ το 25,8% θεωρεί ότι έχει ούτε καλό αλλά ούτε κακό επίπεδο. Μόνο τρεις επιχειρήσεις θεωρούν ότι έχουν κακό φυσικό επίπεδο ασφάλειας.

Η τεχνική ασφάλεια αποτελεί τον πιο γνωστό έλεγχο διαχείρισης της ασφάλειας πληροφοριών. Οι μικρομεσαίες επιχειρήσεις ίσως να δυσκολεύονται να έχουν ένα καλό επίπεδο τεχνικής ασφάλειας καθώς έχει πολλές παραμέτρους. Αυτό φαίνεται και από τα αποτελέσματα, καθώς σύμφωνα με τους ερωτηθέντες μόλις το 9,7% θεωρεί ότι είναι σε πολύ καλό επίπεδο. Το 48,4% δήλωσε ότι έχουν αρκετά καλή τεχνική ασφάλεια και το 19,4% ότι είναι ούτε καλή αλλά ούτε κακή. Το 19,4% δήλωσε ότι δεν είναι αρκετά καλή και το 3,2% ότι είναι κακή.

5.2.2 Προσφατες Αλλαγες, Ελλειψεις και Πολιτικες Ασφαλειας

Οι μικρομεσαίες επιχειρήσεις της Κύπρου φαίνεται να επενδύουν σε νέες τεχνολογίες που έχουν να κάνουν με τα πληροφοριακά συστήματα τους, καθώς το 32,3% απάντησε ότι έχουν γίνει σημαντικές αλλαγές σε αυτά τους τελευταίους δώδεκα μήνες. Το 51,6% απάντησε ότι έχουν γίνει μικρές αλλαγές, ενώ μόλις το 12,9% απάντησε ότι δεν έχουν γίνει καθόλου αλλαγές.

Σύμφωνα με τους ερωτηθέντες, οι τεχνολογίες που χρησιμοποιούνται πιο πολύ στην επιχείρηση που εργάζονται για σκοπούς ασφάλειας τους τελευταίους δώδεκα μήνες φαίνεται να είναι τα Anti-virus/Anti-malware προγράμματα με ποσοστό 87,1%, καθώς και εργαλεία Anti-spam/Anti-Phishing με ποσοστό 80,6%, το οποίο είναι λογικό, λόγω του μικρού κόστους τους σε σχέση με άλλες τεχνολογίες ασφαλείας. Ακολουθούν τα Virtual Private Networks (VPN) με ποσοστό 64,5% και τα Firewalls με ποσοστό 58,1%. Τα VPN και τα Firewalls αποτελούν πολύ καλές λύσεις για την ασφάλεια των μικρομεσαίων επιχειρήσεων καθώς παρέχουν υψηλή ασφάλεια με σχετικά μικρό κόστος. Ένα

μειονεκτήματα τους είναι ότι χρειάζεται γνώση για να μπορέσουν να στηθούν σωστά ώστε να προσφέρουν την μέγιστη ασφάλεια.

Πολλές μικρομεσαίες επιχειρήσεις χρησιμοποιούν κρυπτογράφηση των δεδομένων τους αλλά και κρυπτογραφημένη σύνδεση, όπως μπορούμε να δούμε στην παρακάτω Εικόνα 11. Επίσης πολλές μικρομεσαίες επιχειρήσεις έχουν UPS (Uninterrupted Power Supply) με ποσοστό 48,4%, κατέχουν νόμιμα λογισμικά και χρησιμοποιούν Access Control με ποσοστό 35,5%. Όπως είναι φυσιολογικό ελάχιστες μικρομεσαίες επιχειρήσεις έχουν IDS (Intrusion Detection Systems) κυρίως λόγω του αυξημένου κόστους. Τέλος, μόλις 5 μικρομεσαίες επιχειρήσεις χρησιμοποιούν φυσικούς τρόπους αποτροπής κλοπής, όπως οι κλειδαριές Kensington.

Εικόνα 13 Τεχνολογίες που χρησιμοποιούνται για σκοπούς ασφαλείας.

Εν συνεχεία, οι ερωτηθέντες κλήθηκαν να απαντήσουν στην ερώτηση ποιες πολιτικές ασφαλείας υπάρχουν στην επιχείρηση που εργάζονται. Εδώ το μεγαλύτερο ποσοστό (67,7%) έλαβε ο έλεγχος για πειρατικό λογισμικό και η διατήρηση αντιγράφων ασφάλειας. Οι μικρομεσαίες επιχειρήσεις προσπαθούν να εκπαιδεύσουν τους υπάλληλους τους σε διαδικασίες ασφαλείας σύμφωνα με τα αποτελέσματα (61,3%). Αξιόλογο είναι και το ποσοστό (32,3%) των μικρομεσαίων επιχειρήσεων που έχουν μέτρα ασφαλείας Cloud Computing και μέτρα ασφαλείας για την χρήση προσωπικών συσκευών στην εργασία.

Δυστυχώς, είναι λίγες οι επιχειρήσεις που χρησιμοποιούν επίσημα/τεκμηριωμένα πρότυπα ασφαλείας, όπως επίσης και Business Continuity Plan, καθώς μόνο οχτώ επιχειρήσεις έχουν αυτές τις πολίτικες ασφαλείας. Επίσης, οι μικρομεσαίες επιχειρήσεις δεν πραγματοποιούν περιοδικές αξιολογήσεις ευπαθειών/κίνδυνων καθώς μόνο το 38,7% πραγματοποιεί. Αυτό μπορεί να οφείλεται, όπως θα δούμε παρακάτω, στο ότι δεν υπάρχει η σωστή ενημέρωση γύρω από την κυβερνοασφάλεια αλλά και στο ότι μόνο το 19,4% έχει προσλάβει εξωτερική εταιρία που θα καθοδηγήσει τις επιχειρήσεις στο είναι πιο ασφαλείς στον κυβερνοχώρο.

Οι μικρομεσαίες επιχειρήσεις που έλαβαν μέρος στην ερευνά κλήθηκαν να απαντήσουν για τις ελλείψεις που πιθανόν να έχουν σε επίπεδο ασφαλείας. Όπως είναι λογικό οι περισσότερες απάντησαν ότι δεν υπάρχει καθοδήγηση με ποσοστό 64,5%, όπως μπορούμε να δούμε στην παρακάτω Εικόνα 12. Μεγάλο ποσοστό (58,1%) έλαβε η ανεπαρκής χρηματοδότηση, το ότι δεν υπάρχει επαρκής γνώση γύρω από την ασφάλεια (45,2%) αλλά και ότι οι οδηγίες δεν ακολουθούνται (41,9%).

Τέλος, μερικές επιχειρήσεις απάντησαν ότι δεν έχει πραγματοποιηθεί αξιολόγηση κινδύνου (25,8%), ενώ το 19,4% ότι δεν υπάρχουν κατάλληλες τεχνικές λύσεις. Τα αποτελέσματα θεωρούνται φυσιολογικά για μικρομεσαίες επιχειρήσεις, καθώς το κύριο πρόβλημα τους είναι ο μικρός προϋπολογισμός που διαθέτουν, όπως και η έλλειψη καθοδήγησης σε θέματα που αφορούν την ασφάλεια στον κυβερνοχώρο.

Εικόνα 14 Ελλείψεις σε επίπεδο ασφάλειας

5.2.3 Κυβερνοεπιθεσεις και Κυβερνοασφαλεια

Οι ερωτηθέντες κλήθηκαν να απαντήσουν σε ερωτήσεις που αφορούν την κυβερνοασφάλεια και τις κυβερνοεπιθέσεις που πιθανόν να έχουν δεχτεί. Σύμφωνα λοιπόν με τις απαντήσεις που δοθήκαν, η συντριπτική πλειοψηφία των μικρομεσαίων επιχειρήσεων που έλαβαν μέρος στην ερευνά έχουν δεχτεί κάποιο είδος κυβερνοεπίθεσης, όπως μπορούμε να δούμε στην παρακάτω Εικόνα 13.

Εικόνα 15 Κυβερνοεπιθέσεις σε μικρομεσαίες επιχειρήσεις

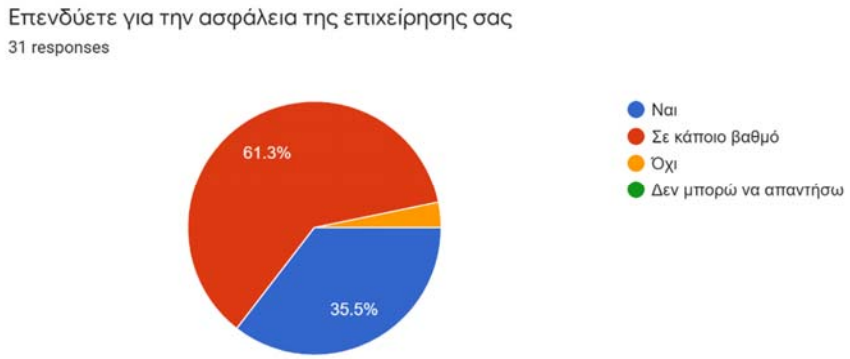
Πιο συγκεκριμένα, το 80,6% των μικρομεσαίων επιχειρήσεων έλαβε μήνυμα ηλεκτρονικού ταχυδρομείου Spam/Phishing, ενώ το 61,3% είχε κάποια μόλυνση με Virus/Malware. Το 19,4% έπεσε θύμα επίθεσης Denial of Service, Web site defacement και Degradation of network. Πέντε επιχειρήσεις δήλωσαν ότι είχαν κάποια απώλεια δεδομένων, ενώ μόλις μια επιχείρηση δήλωσε ότι έπεσε θύμα hacking.

Ζητήθηκε από τους ερωτηθέντες να απαντήσουν στο αν η επιχείρηση τους έχει αναφέρει οποιοδήποτε περιστατικό σε οργανισμούς όπως αστυνομία, ειδική εταιρία ασφάλειας υπολογιστών ή σε κάποιο προμηθευτή ηλεκτρονικών υπολογιστών. Δυστυχώς, σύμφωνα με τα αποτελέσματα, οι μικρομεσαίες επιχειρήσεις δεν αναφέρουν περιστατικά εγκλήματος στον κυβερνοχώρο σε τρίτους, όπως μπορούμε να δούμε στην παρακάτω Εικόνα 14.

Εικόνα 16 Αναφορά περιστατικών εγκλήματος στον κυβερνοχώρο

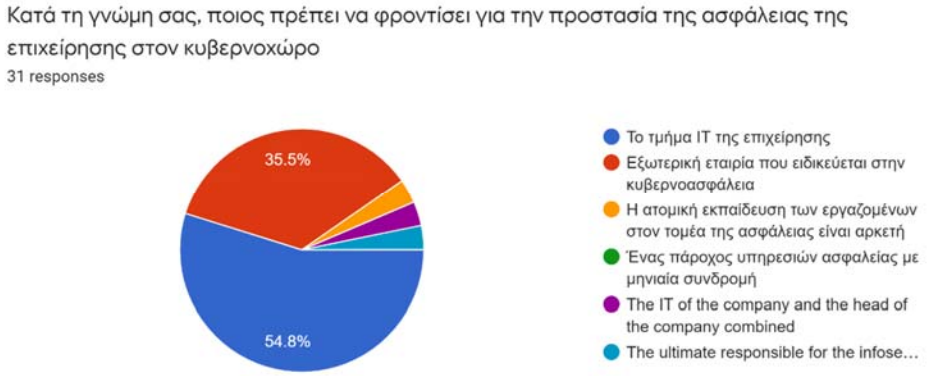
Εάν οι μικρομεσαίες επιχειρήσεις ανέφεραν τα περιστατικά που σχετίζονται με την ασφάλειας τους, θα ήταν ευκολότερο να έχουν καλύτερη εικόνα οι εταιρίες που ασχολούνται με την κυβερνοασφάλεια, ακόμα και οι κυβερνητικές υπηρεσίες θα ήταν πιο ενημέρωνες σε περιπτώσεις που έχουν να κάνουν με κυβερνοεπιθέσεις.

Οι μικρομεσαίες επιχειρήσεις στην Κυπρο φαίνεται να επενδύουν στην ασφάλεια πληροφοριών τους σύμφωνα με τις απαντήσεις που λήφθηκαν και αυτό δημιουργεί καλούς οιωνούς για την ασφάλεια των μικρομεσαίων επιχειρήσεων. Όπως μπορούμε να δούμε στην παρακάτω Εικόνα 15, το 35,5% επενδύει στην ασφάλεια πληροφοριών, ενώ το 61,3% επενδύει σε κάποιο βαθμό σε αυτήν. Μόνο μια επιχείρηση απάντησε ότι δεν επενδύει καθόλου, κάτι που μας οδηγεί στο παραπάνω συμπέρασμα.



Εικόνα 17 Επένδυση στην ασφάλεια

Στην ερώτηση ποιος πρέπει να φροντίσει για την προστασία της ασφάλειας της επιχείρησης στον κυβερνοχώρο, το μεγαλύτερο ποσοστό (54,8%) απάντησε ότι πρέπει να φροντίζει το τμήμα IT της επιχείρησης. Το 35,5% έχει προσλάβει εξωτερική εταιρεία που ειδικεύεται στην κυβερνοασφάλεια, μια επιχείρηση πιστεύει ότι η ατομική εκπαίδευση των εργαζομένων στον τομέα της ασφάλειας είναι αρκετή, ενώ μια επιχείρηση πιστεύει ότι για την ασφάλεια πρέπει να φροντίσει το τμήμα IT της επιχείρησης μαζί με τον ιδιοκτήτη. Τέλος, μια επιχείρηση αναφέρει ότι η ασφάλεια πληροφοριών είναι ευθύνη του ιδιοκτήτη και ότι η ασφάλεια είναι ευθύνη όλων των εργαζομένων. Η τελευταία ανοιχτή απάντηση που δόθηκε θεωρείται και η πιο σωστή, αν και ισχύει περισσότερο σε μεγάλες επιχειρήσεις και όχι τόσο στις μικρομεσαίες.



Εικόνα 18 Ποιος πρέπει να φροντίσει για την προστασία της ασφάλειας

Πολλές μικρομεσαίες επιχειρήσεις δεν διαθέτουν τμήμα IT (Information Technology), για πολλούς και διαφόρους λόγους. Π.χ. διαθέτουν μικρό προϋπολογισμό ή έχουν προσλάβει κάποιον εξωτερικό συνεργάτη για να ασχολείται με τα τεχνολογικά θέματα της επιχείρησης. Στην ερώτηση αν χρησιμοποιούν μια ή περισσότερες εταίρες ασφάλειας IT, οι ερωτηθέντες απάντησαν με ποσοστό 54,8% ότι δεν χρησιμοποιούν, ενώ προκαλεί ενδιαφέρον το ότι το 25,8% σκοπεύει να προσλάβει. Μόνο το 19,4% των ερωτηθέντων απάντησε ότι χρησιμοποιούν, κάτι που δηλώνει ότι ενδιαφέρονται για την ασφάλεια τους στον κυβερνοχώρο.

Εικόνα 19 Επιχειρήσεις που χρησιμοποιούν εταιρίες ασφάλειας IT

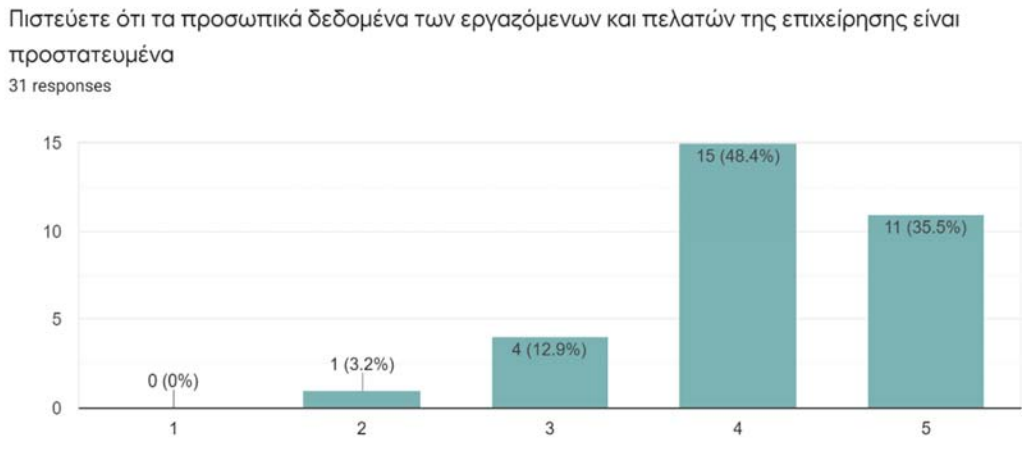
5.2.4 Σχεδιο Έκτακτης Ανάγκης, Προσωπικα Δεδομενα και GDPR

Οι ερωτηθέντες κλήθηκαν να απαντήσουν στο αν η επιχείρηση που εργάζονται διαθέτει σχέδιο έκτακτης ανάγκης σε περίπτωση εγκληματικής ενέργειας στον κυβερνοχώρο. Όπως είναι λογικό το μεγαλύτερο ποσοστό (58,1%) δεν διαθέτει σχέδιο έκτακτης ανάγκης. Παρόλα αυτά είναι ενθαρρυντικό ότι το 35,5% των ερωτηθέντων απάντησε ότι διαθέτει. Το 6,5% των ερωτηθέντων δεν γνώριζε αν διαθέτουν οι επιχειρήσεις που εργάζονται σχέδιο έκτακτης ανάγκης.

Ο σκοπός του σχεδίου έκτακτης ανάγκης είναι να προστατέψει την επιχείρηση και την λειτουργία της σε περίπτωση που πέσει θύμα εγκληματικής ενέργειας στον κυβερνοχώρο. Αποτελεί σημαντικό παράγοντα στο να συνεχίσει η επιχείρηση την λειτουργία της σε περίπτωση επίθεσης, γι' αυτό προτείνεται από πολλούς ειδικούς στην ασφάλειας πληροφοριών να έχουν όλες οι επιχειρήσεις ανεξαρτήτου μεγέθους.

Ένα ακόμα σημαντικό ζήτημα που ταλανίζει τις μικρομεσαίες επιχειρήσεις είναι το ζήτημα των προσωπικών δεδομένων, ειδικά μετά την εφαρμογή του General Data Protection Regulation (GDPR), γι' αυτό θεωρήθηκε σωστό να υπάρχει ερώτηση στο ερωτηματολόγιο για τα προσωπικά δεδομένα όπως και για το GDPR, ώστε να ερευνηθεί και αυτό το μέρος της ασφάλειας πληροφοριών.

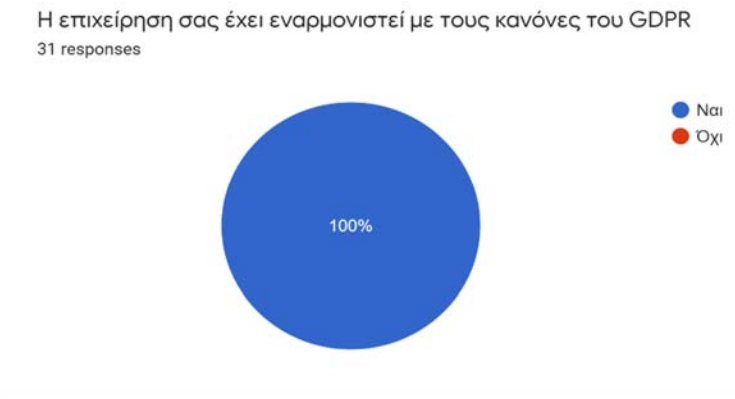
Οι ερωτηθέντες κλήθηκαν να απαντήσουν αν πιστεύουν ότι τα προσωπικά δεδομένα των εργαζομένων αλλά και των πελατών της επιχείρησης που εργάζονται είναι προστατευμένα. Όπως θα δούμε στην παρακάτω Εικόνα 18 οι μικρομεσαίες επιχειρήσεις στην Κυπρο δείχνουν εμπιστοσύνη στην προστασία των προσωπικών δεδομένων που κατέχουν. Μόνο μια επιχείρηση πιστεύει ότι δεν είναι αρκετά προστατευμένα τα προσωπικά δεδομένα που κατέχει.



Εικόνα 20 Εμπιστοσύνη στην προστασία των προσωπικών δεδομένων

Όπως αναφέρθηκε παραπάνω, το General Data Protection Regulation (GDPR) είναι ένας νέος νομός που επέβαλε η Ευρωπαϊκή Ένωση σε σχέση με την ιδιωτικότητα και την ασφάλεια, ο οποίος τέθηκε σε ισχύ στις 25 Μάιου 2018 [37]. Οι μικρομεσαίες επιχειρήσεις κλήθηκαν να απαντήσουν στο αν γνωρίζουν τι είναι το GDPR αλλά και αν έχουν εναρμονιστεί με αυτό.

Τα αποτελέσματα είναι παραπάνω από ενθαρρυντικά, καθώς το 96,8% απάντησε ότι γνωρίζει τι είναι GDPR και το απολυτό 100% έχει εναρμονιστεί με τον κανονισμό αυτόν. Τα αποτελέσματα είναι λογικά καθώς όσοι παραβιάζουν τα πρότυπα προστασίας της ιδιωτικής ζωής και ασφάλειας που θέτει ο συγκεκριμένος κανονισμός μπορεί να τους επιφέρουν σκληρές κυρώσεις και πρόστιμα, που μπορεί να φτάσουν σε δεκάδες εκατομμύρια ευρώ.



Εικόνα 21 Επιχειρήσεις που έχουν εναρμονιστεί με το GDPR

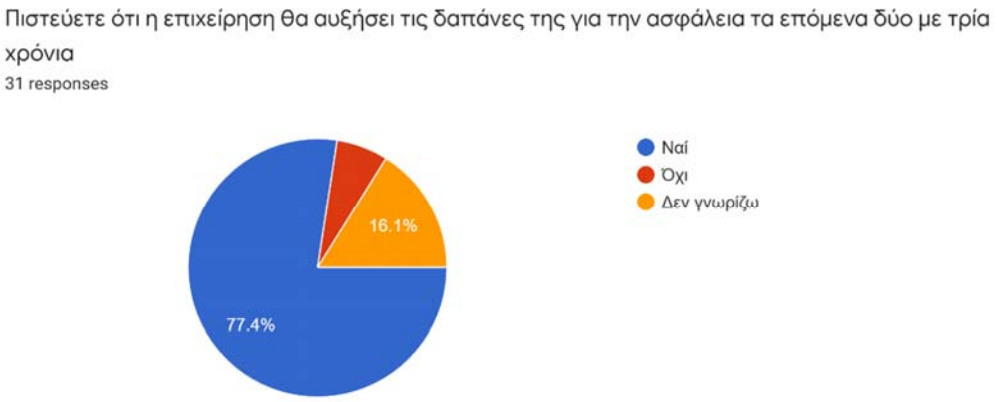
5.3 Μελλοντικά Σχεδια Αναπτυξης και Επενδυσης στην Ασφαλεια Πληροφοριων

Οι μικρομεσαίες επιχειρήσεις στην Κυπρο φαίνεται ότι έχουν σκοπό να αναπτύξουν ή να επενδύσουν στις ανάγκες της ασφάλειας πληροφοριών που έχουν. Σύμφωνα με τις απαντήσεις που έδωσαν, το 35,5% έχει σκοπό να επενδύσει μέσα στους επομένους δώδεκα μήνες στις ανάγκες της ασφάλειας πληροφοριών. Το 38,7% απάντησε ότι πιθανόν να

επενδύσει σε αυτές αλλά όχι σύντομα, ενώ το 19,4% ότι υπάρχει πιθανότητα να επενδύσει στους επομένους δώδεκα μήνες. Το 6,5% απάντησε ότι θα επενδύσει στην ασφάλεια πληροφοριών αλλά όχι σύντομα όπως μπορούμε να δούμε στην παρακάτω Εικόνα. Έκπληξη προκαλεί ότι καμία μικρομεσαία επιχείρηση δεν απάντησε ότι δεν έχει σκοπό να επενδύσει στις ανάγκες της ασφάλειας πληροφοριών επειδή βρίσκεται σε καλό επίπεδο, όπως επίσης καμία επιχείρηση δεν απάντησε όχι λόγω του ότι δεν χρειάζεται.

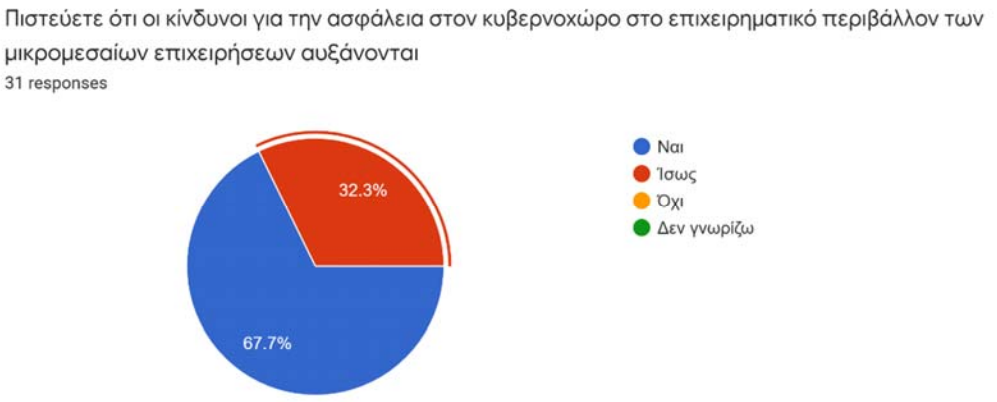
Εικόνα 22 Ανάπτυξη ή επένδυση στις ανάγκες ασφάλειας πληροφοριών

Στην ερώτηση αν πιστεύουν ότι η επιχείρηση που εργάζονται θα αυξήσει τις δαπάνες της για την ασφάλεια πληροφοριών τα επόμενα δυο με τρία χρονιά το μεγαλύτερο ποσοστό των ερωτηθέντων (77,4%) απάντησε ναι, ενώ μόλις το 6,5% απάντησε όχι. Αυτό μας δείχνει ότι οι μικρομεσαίες επιχειρήσεις της Κύπρου πιστεύουν ότι η ασφάλεια πληροφοριών διαδραματίζει σημαντικό ρόλο στην σωστή και καλή λειτουργία της επιχείρησης και γι' αυτό είναι διατεθειμένες να αυξήσουν τον προϋπολογισμό τους για την προστασία τους. Το 16,1% των ερωτηθέντων απάντησε ότι δεν γνωρίζει αν η επιχείρηση αυξήσει τις δαπάνες της για την ασφάλεια πληροφοριών τα επόμενα δυο με τρία χρονιά.



Εικόνα 23 Αύξηση των δαπανών για την ασφάλεια πληροφοριών

Τέλος, στην γενική ερώτηση αν πιστεύουν ότι οι κίνδυνοι για την ασφάλεια στον κυβερνοχώρο στο επιχειρηματικό περιβάλλον των μικρομεσαίων επιχειρήσεων αυξάνονται, οι ερωτηθέντες απάντησαν ναι με 67,7%, το 32,3% απάντησε ίσως, ενώ κανένας δεν απάντησε όχι. Αυτό δηλώνει ότι μικρομεσαίες επιχειρήσεις στην Κυπρο αρχίζουν να αντιλαμβάνονται τους κίνδυνους που υπάρχουν σε σχέση με την ασφάλεια τους στον κυβερνοχώρο και ότι οι κίνδυνοι αυτοί αυξάνονται κάθε μέρα.



Εικόνα 24 Αύξηση κίνδυνων για την ασφάλεια

5.4 Οδηγος για την Προετοιμασια των Μικρομεσαιων Επιχειρησεων στον Κυβερνοχωρο

Βάση των αποτελεσμάτων του ερωτηματολογίου, αναπτύχθηκε ένας οδηγός για την προετοιμασία των μικρομεσαίων επιχειρήσεων στον κυβερνοχώρο. Όπως αναφέρθηκε προηγουμένως, οι μικρομεσαίες επιχειρήσεις αντιμετωπίζουν καθημερινά νέους κινδύνους στον κυβερνοχώρο, γι' αυτό αποφασίστηκε να δημιουργηθεί ένας οδηγός που μπορούν να ακολουθήσουν όλες οι επιχειρήσεις για να είναι προετοιμασμένες και καλύτερα οργανωμένες στον κυβερνοχώρο. Θα πρέπει να τονιστεί ότι οι μικρομεσαίες επιχειρήσεις που θα ακολουθήσουν τον οδηγό δεν αποκτούν αυτομάτως ασφάλεια στον κυβερνοχώρο, αλλά αποκτούν την αρχική γνώση, οργάνωση και προετοιμασία για την ασφάλεια στον κυβερνοχώρο. Παρακάτω ακολουθούν τα δέκα βήματα του οδηγού:

1. **Διακυβέρνηση και διαχείριση κινδύνων –** Η κυβερνοασφάλεια δεν αποτελεί μόνο ευθύνη του IT, αλλά πρόκειται για μια πολύπλευρη πρόκληση που απαιτεί προσέγγιση όλης της επιχείρησης για την διαχείριση της. Οι επιχειρήσεις πρέπει να καθιερώσουν και να διατηρούν ένα κατάλληλο πλαίσιο διακυβέρνησης και διαχείρισης κινδύνων για τον εντοπισμό και την αντιμετώπιση των προκλήσεων της κυβερνοασφάλειας.

2. **Επιχειρησιακή πολιτική ασφαλείας και κώδικας δεοντολογίας –** Οι επιχειρήσεις πρέπει να δημιουργήσουν και να εφαρμόζουν διαδικασίες κατά την πρόσληψη αλλά και την απόλυση ή παραίτηση των υπαλλήλων, να περιγράψουν τους ρόλους και τις αρμοδιότητες ασφαλείας, να αναπτύξουν και να διανείμουν ένα κώδικα συμπεριφοράς χρήσης πληροφοριακών συστημάτων, καθώς και να σχεδιάζονται και να εκτελούνται έλεγχοι ασφαλείας σε τακτά χρονικά διαστήματα.

3. **Ενημέρωση και κατάρτιση των υπαλλήλων στον κυβερνοχώρο** – Οι υπάλληλοι της επιχείρησης πρέπει να εγγράφουν στον κώδικα δεοντολογίας. Πρέπει να τους υπενθυμίζεται η σημασία της ασφαλούς συμπεριφοράς στον

κυβερνοχώρο, όπως επίσης να τους υπενθυμίζεται ότι τα δεδομένα και οι πληροφορίες πρέπει να αντιμετωπίζονται ως ευαίσθητα και να σέβονται τους κανόνες απορρήτου. Οι υπάλληλοι πρέπει να μπορούν να αναγνωρίζουν ένα phishing μήνυμα ηλεκτρονικού ταχυδρομείου και πως να το διαχειριστούν. Επίσης πρέπει να εκπαιδεύονται ανά τακτά χρονικά διαστήματα πάνω στην κυβερνοασφάλεια.

4. **Φυσική ασφάλεια** – Η φυσική ασφάλεια των περιουσιακών στοιχείων πληροφορικής της επιχείρησης είναι η πρώτη γραμμή άμυνας της κυβερνοασφάλειας. Η κλοπή ενός υπολογιστή ή κινητού τηλεφώνου μπορεί να έχει την ίδια επίδραση στην επιχείρηση όπως μια κυβερνοεπίθεση. Ως αποτέλεσμα, οι δικλείδες ασφαλείας όπως οι κωδικοί πρόσβασης, πρέπει να συμπληρώνονται και από άλλα μέτρα ασφαλείας όπως κλειδαριές υπολογιστών ή UPS (Uninterruptible Power Supply) σε περίπτωση διακοπής ρεύματος. Επίσης, καλό είναι να ακολουθείτε η πολιτική «καθαρού γραφείου»

5. **Αξιολόγηση απειλών και ευπαθειών** – Οι εγκληματίες στον κυβερνοχώρο συνεχίζουν να εκμεταλλεύονται βασικές ευπάθειες ασφαλείας, όπως μη ενημερωμένα λειτουργικά συστήματα, αδύναμοι κωδικοί ασφάλειας κ.α. Οι επιχειρήσεις που δεν ελέγχουν ανά τακτά χρονικά διαστήματα για ευπάθειες και δεν παίρνουν μέτρα για να διορθώσουν τις αδυναμίες των συστημάτων τους, αντιμετωπίζουν αυξημένο κίνδυνο να παραβιαστούν τα συστήματα τους. Για να προστατέψουν οι επιχειρήσεις τα περιουσιακά τους στοιχεία από την αυξανόμενη απειλή των κυβερνοεπιθέσεων, που έχουν ως στόχο τις ευπάθειες των συστημάτων, θα πρέπει να συμπεριλάβουν αξιολογήσεις απειλών και ευπαθειών ώστε να μπορούν να αναγνωρίσουν τις ευπάθειες των πληροφοριακών τους συστημάτων. Τα αποτελέσματα των αξιολογήσεων βοηθούν τις επιχειρήσεις στην κατανόηση των κινδύνων που συνδέονται με τον κυβερνοχώρο.

6. **Ασφάλεια δικτύων** – Η συνεχής σύνδεση των επιχειρήσεων με το διαδίκτυο τις εκθέτει μόνιμα σε ένα εχθρικό περιβάλλον με απειλές που εξελίσσονται

συνεχώς. Επιπλέον, οι εργαζόμενοι στις επιχειρήσεις μπορεί εσκεμμένα ή ακούσια να βλάψουν το δίκτυο των επιχειρήσεων λόγω των ενεργειών τους. Η ασφάλεια δικτύων αναφέρεται σε κάθε δραστηριότητα που σχεδιάστηκε για την προστασία της εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας τους δικτύου αλλά και όλων των περιουσιακών στοιχείων που συνδέονται σε αυτό. Για την προστασία του δικτύου τους, οι επιχειρήσεις καλό είναι να έχουν στην διάθεση τους συσκευές προστασίας από απειλές του διαδικτύου, όπως είναι τα firewalls, τα οποία παρέχουν πολύ-επίπεδη προστασία και μειώνουν δραματικά των αριθμό των επιτυχημένων επιθέσεων που σχετίζονται με το διαδίκτυο στο εσωτερικό δίκτυο των επιχειρήσεων. Επίσης πρέπει να διασφαλιστεί ο απομακρυσμένος έλεγχος σε συστήματα των επιχειρήσεων και όλες οι συνδέσεις στο δίκτυο τους πρέπει να είναι ασφαλείς και κρυπτογραφημένες.

7. **Προστασία πληροφοριακών συστημάτων** – Όπως η ασφάλεια δικτύων, έτσι και η προστασία των πληροφοριακών συστημάτων είναι εξίσου σημαντική. Οι επιχειρήσεις θα πρέπει να εφαρμόσουν διαδικασίες δημιουργίας αντιγράφων ασφαλείας και ανάκτησης και να πραγματοποιούν τις διαδικασίες αυτές τακτικά. Θα πρέπει να αναπτύξουν λύσεις κατά κακόβουλων λογισμικών που θα παρακολουθούν συνέχεια τους servers, υπολογιστές, φορητές συσκευές κ.α. όπως anti-virus, anti-spyware και προσωπικά firewalls. Επίσης θα πρέπει να εφαρμόσουν πολίτικες για τον έλεγχο πρόσβασης σε αφαιρούμενα μέσα όπως τις συσκευές USB. Οι επιχειρήσεις που θέλουν να εφαρμόσουν το BYOD (Bring Your Own Device) θα πρέπει να πάρουν μετρά και να εφαρμόσουν ελέγχους.

8. **Διαχείριση λογαριασμού χρήστη και έλεγχος πρόσβασης** – Οι έλεγχοι πρόσβασης καθορίζουν το πως οι εργαζόμενοι της επιχείρησης διαβάζουν ένα μήνυμα ηλεκτρονικού ταχυδρομείου, έχουν πρόσβαση σε ένα έγγραφο ή πως συνδέονται σε άλλους πόρους του δικτύου της επιχείρησης. Οι σωστά εφαρμοσμένοι έλεγχοι πρόσβασης βοηθούν στην προστασία της πνευματικής ιδιοκτησίας και ευαίσθητων δεδομένων από την μη εξουσιοδοτημένη χρήση, τροποποίηση και αποκάλυψη. Οι επιχειρήσεις θα πρέπει να εφαρμόσουν μια

διαδικασία διαχείρισης λογαριασμών και να έχουν ένα κεντρικό σύστημα διαχείρισης λογαριασμών όπως είναι το Microsoft Active Directory.

9. **Διαχείριση περιουσιακών στοιχείων** – Ο έλεγχος και η διαχείριση των υπολογιστικών συστημάτων και του λογισμικού διαδραματίζει σημαντικό ρολό στην ασφάλεια της επιχείρησης. Είναι πολύ σημαντικό να εντοπίζονται και να διαχειρίζονται όλα τα συστήματα ηλεκτρονικών υπολογιστών, έτσι ώστε μόνο τα εξουσιοδοτημένα συστήματα να έχουν πρόσβαση στο δίκτυο της επιχείρησης. Είναι σημαντικό επίσης να διασφαλιστεί ότι μόνο εξουσιοδοτημένο λογισμικό είναι εγκαταστημένο και ότι εμποδίζεται η εκτέλεση μη εξουσιοδοτημένου λογισμικού. Οι επιχειρήσεις θα πρέπει να διατηρούν και να ενημερώνουν μια καταγραφή των περιουσιακών στοιχείων τους, καθώς επίσης να δημιουργήσουν και να ενημερώνουν έναν ακριβή χάρτη με όλα τα δίκτυα τους και των διασυνδέσεων τους.

10. **Επιχειρησιακή συνέχεια και σχέδιο διαχείρισης συμβάντων** – Ο σχεδιασμός και η προετοιμασία για ένα περιστατικό στον κυβερνοχώρο είναι μια από τις μεγαλύτερες προκλήσεις που αντιμετωπίζει οποιαδήποτε επιχείρηση. Όταν συμβεί ένα περιστατικό στον κυβερνοχώρο πρέπει να λάβουμε δράσει για να μετριαστεί οποιαδήποτε απειλή για την εμπιστευτικότητα, την ακεραιότητα και την διαθεσιμότητα των περιουσιακών στοιχείων των επιχειρήσεων όσο το δυνατό γρηγορότερα. Οι επιχειρήσεις πρέπει να δημιουργήσουν ένα σχέδιο διαχείρισης συμβάντων στον κυβερνοχώρο, όπως επίσης πρέπει να σχεδιάσουν ένα σχέδιο επιχειρησιακής συνέχειας ώστε να μπορούν να συνεχίσουν την λειτουργία τους.

ΚΕΦΑΛΑΙΟ 6
Επίλογος

6.1 ΣΥΝΟΨΗ

Το τοπίο στην ασφάλεια πληροφοριών συνεχώς αλλάζει με την εισαγωγή του cloud computing, φορητών συσκευών, κοινωνικών δικτύων, είτε ακόμα και νέων νομοθεσιών, έτσι δημιουργούνται νέες ανάγκες για την ασφάλεια των επιχειρήσεων. Οι επιθέσεις από κακόβουλους στις επιχειρήσεις γίνονται πλέον πιο οργανωμένα, γι' αυτό οι απαιτήσεις για καλύτερη ασφάλεια στον κυβερνοχώρο αυξάνονται ακόμα και στις μικρότερες επιχειρήσεις. Οι μικρομεσαίες επιχειρήσεις φαίνεται να μένουν πίσω σε σχέση με τις μεγαλύτερες σε θέματα ασφαλείας παρότι έχουν να αντιμετωπίσουν τις ίδιες απειλές.

Η παρούσα διατριβή εστίασε στην ετοιμότητα της ασφάλειας πληροφοριών στον κυβερνοχώρο των μικρών και μεσαίων επιχειρήσεων στη Κυπρο. Αρχικά γίνεται λόγος για τις αρχές της ασφάλειας πληροφοριών οι οποίες αποτελούν μέρος της ασφάλειας μιας επιχείρησης, καθώς και τι θεωρείται μικρομεσαία επιχείρηση σύμφωνα με την Ευρωπαϊκή Ένωση. Στην συνέχεια παρουσιάζονται οι δέκα κορυφαίες απειλές που δέχονται οι μικρομεσαίες επιχειρήσεις στον κυβερνοχώρο σήμερα, όπως επίσης και νέες τεχνολογίες που χρησιμοποιούνται από τις επιχειρήσεις, όπως το cloud computing και BYOD, οι οποίες εισάγουν νέες απειλές.

Στην παρούσα διατριβή γίνεται λόγος και για την διαχείριση της ασφάλειας πληροφοριών, όπως είναι έλεγχοι διαχείρισης ασφάλειας πληροφοριών, οι οποίοι αποτελούνται από τρία πεδία, την διοικητική, την τεχνική και την φυσική ασφάλεια. Επίσης όλες οι επιχειρήσεις πρέπει να κατανοήσουν τους κινδύνους που σχετίζονται με την ασφάλεια τους αλλά και να

συμμορφώνονται με τις άμεσες ή έμμεσες απαιτήσεις της. Για τον λόγο αυτό μελετήθηκε η διακυβέρνηση, η διαχείριση κίνδυνου, όπως και η συμμόρφωση των επιχειρήσεων. Επίσης γίνεται λόγος για το τι είναι πλαίσια, μοντέλα και πρότυπα που μπορούν ακολουλουθησουν ή να αποκτήσουν οι επιχειρήσεις, καθώς και τα συστήματα διαχείρισης ασφάλειας, τα οποία έχουν ως ρόλο να προστατεύουν τα κρίσιμα πληροφοριακά περιουσιακά στοιχεία και δεδομένα της επιχείρησης από απειλές των αρχών της ασφάλειας πληροφοριών. Στην συνέχεια γίνεται αναφορά στο General Data Protection Regulation (GDPR), το οποίο αποτελεί τον νέο σκληρό νομό της Ευρωπαϊκής Ένωσης σε σχέση με την ιδιωτικότητα και την ασφάλεια.

Τέλος, αναφέρεται η μεθοδολογία που ακολουθήθηκε για την έρευνα, την συλλογή δεδομένων και παρουσιάζονται τα αποτελέσματα του ερωτηματολογίου που συντάχθηκε και συμπληρώθηκε με σκοπό την ερευνά της ετοιμότητας της ασφάλειας των μικρομεσαίων επιχειρήσεων της Κύπρου στον κυβερνοχώρο, καθώς και ένας οδηγός για την προετοιμασία των μικρομεσαίων επιχειρήσεων στον κυβερνοχώρο.

6.2 Συμπερασματα και Μελλοντικη Έρευνα

Σύμφωνα με τις απαντήσεις που δοθήκαν στο ερωτηματολόγιο που συμπληρώθηκε από τους ερωτηθέντες που εργάζονται ή είναι ιδιοκτήτες μικρομεσαίων επιχειρήσεων στην Κυπρο, μπορούμε να συμπεράνουμε ότι έχουν μεγάλη εμπιστοσύνη στην ασφάλειας τους, παρόλο που το μεγαλύτερο ποσοστό δήλωσε ότι έχουν δεχτεί κάποιο είδος κυβερνοεπίθεσης τους τελευταίους δώδεκα μήνες.

Οι μικρομεσαίες επιχειρήσεις στην Κυπρο δείχνουν να επενδύουν σε νέες τεχνολογίες που έχουν να κάνουν με τα πληροφοριακά τους συστήματα, αν και σύμφωνα με το ερωτηματολόγιο, χρησιμοποιούν βασικές τεχνολογίες για την ασφάλεια τους. Επίσης, οι μικρομεσαίες επιχειρήσεις που χρησιμοποιούν επίσημα/τεκμηριωμένα πρότυπα ασφαλείας, όπως επίσης και Business Continuity Plan είναι λίγες και δηλώνουν ως μεγαλύτερο

πρόβλημα τους την έλλειψη καθοδήγησης ώστε να μπορέσουν να ενισχύσουν την ασφάλεια τους αλλά και την ανεπαρκή χρηματοδότηση.

Πρέπει να επισημανθεί ότι οι μικρομεσαίες επιχειρήσεις στην Κυπρο δεν αναφέρουν περιστατικά εγκλήματος στον κυβερνοχώρο σε τρίτους κάτι που αποτελεί πρόβλημα, καθώς αν ανέφεραν περιστατικά που σχετίζονται με την ασφάλειας τους, θα ήταν ευκολότερο να έχουν καλύτερη εικόνα οι εταιρίες που ασχολούνται με την κυβερνοασφάλεια, ακόμα και οι κυβερνητικές υπηρεσίες θα ήταν πιο ενημέρωνες σε περιπτώσεις που έχουν να κάνουν με κυβερνοεπιθέσεις.

Οι μικρομεσαίες επιχειρήσεις στην Κυπρο φαίνεται να επενδύουν στην ασφάλεια πληροφοριών τους, σύμφωνα με τις απαντήσεις που λήφθηκαν και αυτό δημιουργεί καλούς οιωνούς για την ασφάλεια των μικρομεσαίων επιχειρήσεων, καθώς όταν μια επιχείρηση έχει ενημερωμένα συστήματα ασφάλειας είναι πιο εύκολο να αποτραπεί μια κυβερνοεπίθεση. Παρόλα αυτά, το μεγαλύτερο ποσοστό των επιχειρήσεων δεν διαθέτει σχέδιο έκτακτης ανάγκης σε περίπτωση εγκληματικής ενέργειας.

Ένα ακόμα σημαντικό ζήτημα που ταλανίζει τις μικρομεσαίες επιχειρήσεις είναι το ζήτημα των προσωπικών δεδομένων, ειδικά μετά την εφαρμογή του General Data Protection Regulation (GDPR). Οι μικρομεσαίες επιχειρήσεις της Κύπρου δείχνουν εμπιστοσύνη στην προστασία των προσωπικών δεδομένων που κατέχουν, όπως επίσης έχουν εναρμονιστεί πλήρως με το GDPR.

Οι μικρομεσαίες επιχειρήσεις στην Κυπρο φαίνεται ότι έχουν σκοπό να αναπτύξουν ή να επενδύσουν στις ανάγκες της ασφάλειας πληροφοριών που έχουν, σύμφωνα πάντα με το ερωτηματολόγιο. Επίσης, είναι έτοιμες να αυξήσουν τις δαπάνες τους για την ασφάλεια τους, καθώς πιστεύουν ότι οι κίνδυνοι για την ασφάλεια στον κυβερνοχώρο στο επιχειρηματικό περιβάλλον των μικρομεσαίων επιχειρήσεων αυξάνονται.

Τα αποτελέσματα της έρευνας θα προωθηθούν σε όλες τις μικρομεσαίες επιχειρήσεις που έλαβαν μέρος στην έρευνα, ώστε να αντιληφθούν τις αδυναμίες τους και να διορθώσουν τα «κακώς κείμενα» της ασφάλειας τους.

Μια μελλοντική έρευνα σχετικά με το θέμα, θα μπορούσε να επωφεληθεί από υψηλότερο ποσοστό ανταπόκρισης. Ο ιδανικός αριθμός απαντήσεων θα ήταν περίπου στις εκατό. Παρόλα αυτά, το μέγεθος τους δείγματος της ερευνάς θεωρείται ικανοποιητικό κρίνοντας από τον πληθυσμό της χωρά διεξαγωγής του ερωτηματολογίου. Επίσης, θα μπορούσαν να διεξαχθούν συνεντεύξεις μέσω συνάντησης ή τηλεφωνικά, αν και οι συνεντεύξεις για θέματα ασφαλείας είναι δύσκολο να πραγματοποιηθούν, λόγω του ότι λίγοι θα δεχτούν να μιλήσουν για την ασφάλεια των επιχειρήσεων τους. Τέλος, μια έρευνα για την ασφάλεια πληροφοριών των start-up επιχειρήσεων αποτελεί μια ενδιαφέρουσα πρόταση.

ΒΙΒΛΙΟΓΡΑΦΙΑ

[1] J. Andress and S. Winterfeld, *The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice: Second Edition*. 2014.

[2] "What is an SME? | Internal Market, Industry, Entrepreneurship and SMEs." [Online]. Available: https://ec.europa.eu/growth/smes/business-friendly-environment/sme-definition_en. [Accessed: 17-Nov-2019].

[3] "ISO/IEC 27005 risk management standard." [Online]. Available: https://www.iso27001security.com/html/27005.html. [Accessed: 17-Nov-2019].

[4] "ISO/IEC 27001 certification standard." [Online]. Available: https://www.iso27001security.com/html/27001.html. [Accessed: 17-Nov-2019].

[5] GFI Software, "SECURITY THREATS : A GUIDE FOR SMALL Security threats : A guide for SMEs What does an SME need ?," 2010.

[6] SEI, "State of Cybercrime Survey 2013," *CERT Present.*, p. 20, 2013.

[7] P. Scott, "Top 10 Threats to SME Data Security," *WatchGuard*, pp. 1–3, 2008.

[8] V. Business, "2018 Data breach investigations report," *Trends*, pp. 1–62, 2018.

[9] "Verizon: 2019 Data Breach Investigations Report," *Comput. Fraud Secur.*, vol. 2019, no. 6, p. 4, 2019.

[10] G. M. J, M. M. Mohideen, M. Shahira, and B. N. Assistant, "E-Mail Phishing -An open threat to everyone," *Int. J. Sci. Res. Publ.*, vol. 4, no. 1, pp. 2250–3153, 2014.

[11] R. Khan, "Network Threats, Attacks and Security Measures: a Review," *Int. J. Adv. Res. Comput. Sci.*, vol. 8, no. 8, pp. 116–120, 2017.

[12] T. Government, H. Kong, S. Administrative, and R. The, “Web Attacks and Countermeasures,” no. February, 2008.

[13] “Mobile Device Security: Startling Statistics on Data Loss and Data Breaches | The ChannelPro Network.” [Online]. Available: https://www.channelpronetwork.com/article/mobile-device-security-startling-statistics-data-loss-and-data-breaches. [Accessed: 17-Nov-2019].

[14] “Is Hotel Wi-Fi Safe? Staying Secure on Public Wi-Fi | Norton.” [Online]. Available: https://us.norton.com/internetsecurity-privacy-stay-safe-on-public-wi-fi-when-you-travel.html. [Accessed: 18-Nov-2019].

[15] T. N. Brooks, “Survey of automated vulnerability detection and exploit generation techniques in cyber reasoning systems,” *Adv. Intell. Syst. Comput.*, vol. 857, pp. 1083–1102, 2019.

[16] H. Industry, “Industry Survey Insider Attacks,” 2017.

[17] F. M. Groom, “The Basics of Cloud Computing,” in *Enterprise Cloud Computing for Non-Engineers*, 2018, pp. 1–42.

[18] L. Badger, T. Grance, R. Patt-Corner, and J. Voas, “Cloud Computing Synopsis and Recommendations Recommendations of the National Institute of Standards and Technology.”

[19] A. Ahmad, S. Jafar, M. Alizadeh, and S. Karamizadeh, “Associated Risks of Cloud Computing for SMEs,” *Open Int. J. Informatics*, vol. 1, pp. 37–45, 2012.

[20] E. Alsolami, “Security threats and legal issues related to Cloud based solutions,” *156 IJCSNS Int. J. Comput. Sci. Netw. Secur.*, vol. 18, no. 5, pp. 156–163, 2018.

[21] K. A. Ahmat, “Emerging Cloud Computing Security Threats,” no. 1, pp. 1–4, 2012.

[22] T.-S. Chou, “SECURITY THREATS ON CLOUD COMPUTING VULNERABILITIES,” *Int. J. Comput. Sci. Inf. Technol.*, vol. 5, no. 3, 2013.

[23] A. Rot, “Selected issues of IT risk management in the cloud computing model. Theory and practice,” in *IMCIC 2017 - 8th International Multi-Conference on Complexity, Informatics and Cybernetics, Proceedings*, 2017, vol. 2017-March, pp. 89–94.

[24] J. Bradley, J. Loucks, J. Macaulay, R. Medcalf, and L. Buckalew, “BYOD: A Global Perspective Harnessing Employee-Led Innovation Executive Summary,” pp. 1–21, 2012.

[25] D. T. Monitor, “Bring your own device : a major security concern Bring your own device : a major security concern,” no. May, 2017.

[26] Gordon A., Lawrence L., P. Martin Lucyshyn William, and Richardson R., “Eleventh Annual Computer Crime and Security Survey,” 2006.

[27] Symantec, “2013 Norton Report,” p. 28, 2013.

[28] P. Ruggiero and J. Foote, “Cyber Threats to Mobile Phones,” *Us-Cert*, pp. 1–6, 2011.

[29] M. Weiss and M. G. Solomon, *Auditing IT Infrastructures for Compliance*. 2015.

[30] N. King and A. Khan, *Governance, Risk, and Compliance Handbook for Oracle Applications*. 2012.

[31] “ISO - ISO/IEC 27001 Information security management.” [Online]. Available: https://www.iso.org/isoiec-27001-information-security.html. [Accessed: 19-Nov-2019].

[32] C. Pelnekar, “Planning for and Implementing ISO 27001,” *ISACA J.*, vol. 4, p. 8, 2011.

[33] “About The ISO27K Standards.” [Online]. Available:

https://www.iso27001security.com/html/iso27000.html. [Accessed: 19-Nov-2019].

[34] "D3.1 - SMEs Cyber Security threats digest and analysis | FORTIKA." [Online]. Available: https://fortika-project.eu/content/d31-smes-cyber-security-threats-digest-and-analysis. [Accessed: 19-Nov-2019].

[35] ISO, "ISO/IEC 27032:2012 Information Technology — Security Techniques — Guidelines for Cybersecurity," *ISO.org [Online]*, 2012. [Online]. Available: https://www.iso.org/standard/44375.html. [Accessed: 19-Nov-2019].

[36] "ISO/IEC 27032 cybersecurity guideline." [Online]. Available: https://www.iso27001security.com/html/27032.html. [Accessed: 19-Nov-2019].

[37] "What is GDPR, the EU's new data protection law? - GDPR.eu." [Online]. Available: https://gdpr.eu/what-is-gdpr/. [Accessed: 19-Nov-2019].

[38] "Do the rules apply to SMEs? | European Commission." [Online]. Available: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/application-regulation/do-rules-apply-smes_en. [Accessed: 19-Nov-2019].

[39] "A five-step guide to GDPR for SME's - PrivSec Report." [Online]. Available: https://gdpr.report/news/2018/04/16/a-five-step-guide-to-gdpr-for-smes/. [Accessed: 19-Nov-2019].

[40] "GDPR Small Business Survey." [Online]. Available: https://gdpr.eu/wp-content/uploads/2019/05/2019-GDPR.EU-Small-Business-Survey.pdf. [Accessed: 19-Nov-2019].

[41] P. Voigt and A. Bussche, *The EU General Data Protection Regulation (GDPR): A Practical Guide*. 2017.

[42] M. Ko, K. M. Osei-Bryson, and C. Dorantes, "Investigating the impact of publicly

announced information security breaches on three performance indicators of the breached firms," *Inf. Resour. Manag. J.*, vol. 22, no. 2, pp. 1–21, 2009.

[43] "Cloud computing - Wikipedia." [Online]. Available: https://en.wikipedia.org/wiki/Cloud_computing. [Accessed: 19-Nov-2019].

[44] "Bring Your Own Device (BYOD) | Redeemer Lutheran College." [Online]. Available: https://www.redeemer.com.au/learning/vision/byod. [Accessed: 19-Nov-2019].

[45] "Importance of GRC in ERP | allthatsaidisred." [Online]. Available: https://allthatsaidisred.wordpress.com/2011/12/26/importance-of-grc-in-erp/. [Accessed: 19-Nov-2019].

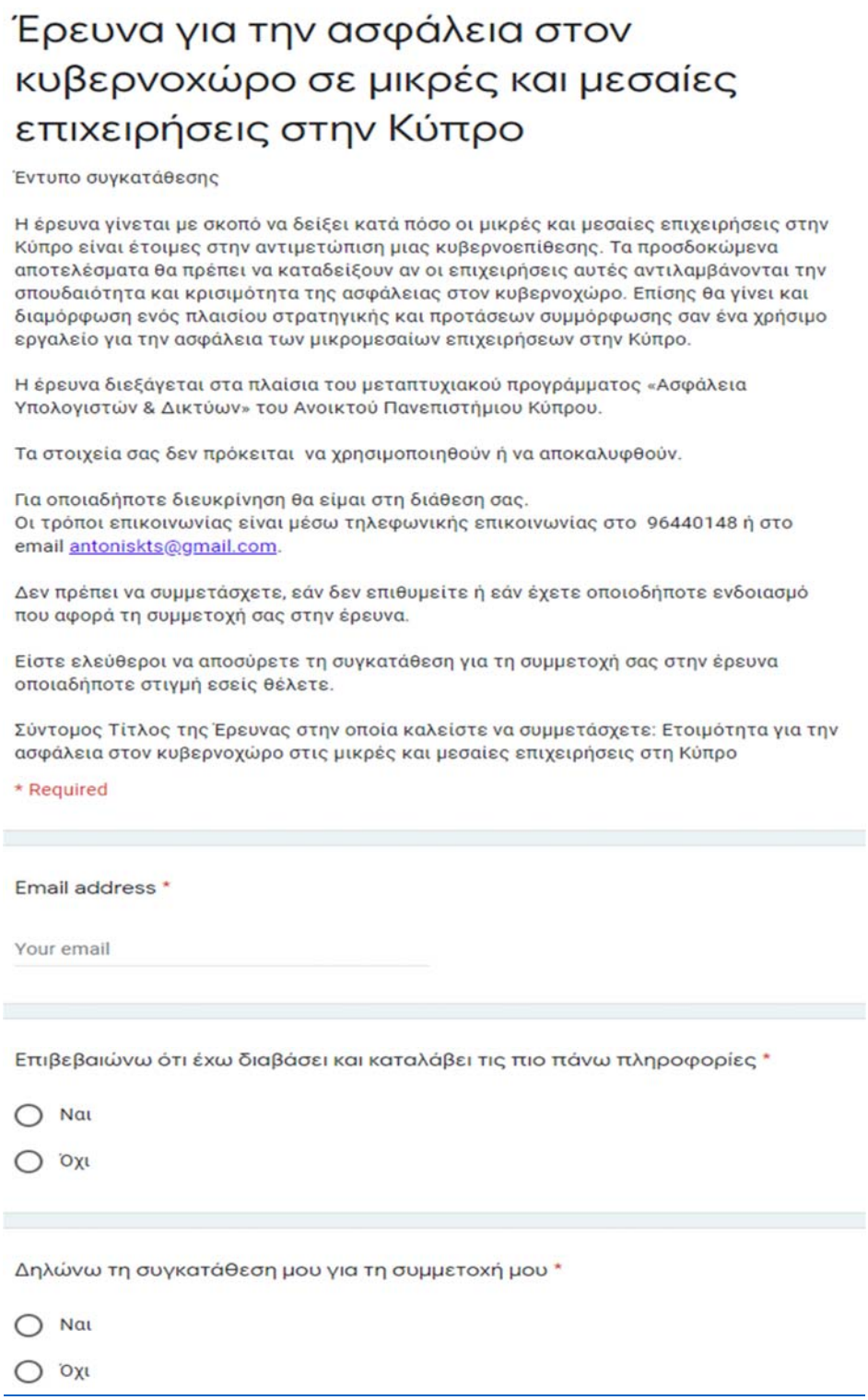
[46] "ΕΠΙΣΗΜΗ ΕΦΗΜΕΡΙΔΑ ΤΗΣ ΚΥΠΡΙΑΚΗΣ ΔΗΜΟΚΡΑΤΙΑΣ ΠΑΡΑΡΤΗΜΑ ΠΡΩΤΟ ΝΟΜΟΘΕΣΙΑ-ΜΕΡΟΣ I," 2018. [Online]. Available: http://www.cylaw.org/nomoi/arith/2018_1_125.pdf. [Accessed: 19-Nov-2019].

[47] R. Moen and C. Norman, "Evolution of the PDCA Cycle," *Society*, pp. 1–11, 2009.

ΠΑΡΑΡΤΗΜΑ Α
Ερωτηματολόγιο

Η πλήρης έκδοση του ερωτηματολογίου βρίσκεται στις παρακάτω εικόνες, καθώς και διαδικτυακά στον παρακάτω σύνδεσμο με την μορφή Google Forms:

https://docs.google.com/forms/d/1Ugnw3b0-qCEJpyUFkantiLZP6p1dJPAvEMQNtBq06IY



Έρευνα για την ασφάλεια στον κυβερνοχώρο σε μικρές και μεσαίες επιχειρήσεις στην Κύπρο

Έντυπο συγκατάθεσης

Η έρευνα γίνεται με σκοπό να δείξει κατά πόσο οι μικρές και μεσαίες επιχειρήσεις στην Κύπρο είναι έτοιμες στην αντιμετώπιση μιας κυβερνοεπίθεσης. Τα προσδοκώμενα αποτελέσματα θα πρέπει να καταδείξουν αν οι επιχειρήσεις αυτές αντιλαμβάνονται την σπουδαιότητα και κρισιμότητα της ασφάλειας στον κυβερνοχώρο. Επίσης θα γίνει και διαμόρφωση ενός πλαισίου στρατηγικής και προτάσεων συμμόρφωσης σαν ένα χρήσιμο εργαλείο για την ασφάλεια των μικρομεσαίων επιχειρήσεων στην Κύπρο.

Η έρευνα διεξάγεται στα πλαίσια του μεταπτυχιακού προγράμματος «Ασφάλεια Υπολογιστών & Δικτύων» του Ανοικτού Πανεπιστήμιου Κύπρου.

Τα στοιχεία σας δεν πρόκειται να χρησιμοποιηθούν ή να αποκαλυφθούν.

Για οποιαδήποτε διευκρίνηση θα είμαι στη διάθεση σας.
Οι τρόποι επικοινωνίας είναι μέσω τηλεφωνικής επικοινωνίας στο 96440148 ή στο email antoniskts@gmail.com.

Δεν πρέπει να συμμετάσχετε, εάν δεν επιθυμείτε ή εάν έχετε οποιοδήποτε ενδοιασμό που αφορά τη συμμετοχή σας στην έρευνα.

Είστε ελεύθεροι να αποσύρετε τη συγκατάθεση για τη συμμετοχή σας στην έρευνα οποιαδήποτε στιγμή εσείς θέλετε.

Σύντομος Τίτλος της Έρευνας στην οποία καλείστε να συμμετάσχετε: Ετοιμότητα για την ασφάλεια στον κυβερνοχώρο στις μικρές και μεσαίες επιχειρήσεις στη Κύπρο

* Required

Email address *

Your email

Επιβεβαιώνω ότι έχω διαβάσει και καταλάβει τις πιο πάνω πληροφορίες *

- ◯ Ναι
- ◯ Όχι

Δηλώνω τη συγκατάθεση μου για τη συμμετοχή μου *

- ◯ Ναι
- ◯ Όχι

Εικόνα 25 Έντυπο συγκατάθεσης

Ποια είναι η θέση/ρόλος σας στην επιχείρηση *

- ◯ Ιδιοκτήτης
- ◯ IT (Information Technology)
- ◯ Other:

Είστε ο υπεύθυνος για την ασφάλεια της επιχείρησης *

- ◯ Ναι
- ◯ Όχι
- ◯ Δεν μπορώ να απαντήσω

Ποιο είναι το επίπεδο μόρφωσης σας *

- ◯ Λύκειο
- ◯ Πανεπιστήμιο
- ◯ Μεταπτυχιακό
- ◯ Διδακτορικό
- ◯ Other:

Κυρία δραστηριότητα της επιχείρησης *

- ◯ Πωλήσεις
- ◯ Κατασκευές
- ◯ Ηλεκτρονικό Κατάστημα
- ◯ Υπηρεσίες
- ◯ Εστίαση
- ◯ Other:

Εικόνα 26 Ερωτήσεις 1 έως 4

Επενδύετε για την ασφάλεια της επιχείρησης σας *

- ◯ Ναι
- ◯ Σε κάποιο βαθμό
- ◯ Όχι
- ◯ Δεν μπορώ να απαντήσω

Πως αξιολογείται τις αλλαγές των πληροφοριακών συστημάτων στην επιχείρηση τους τελευταίους 12 μήνες *

- ◯ Σημαντικές αλλαγές
- ◯ Μικρές αλλαγές
- ◯ Καθόλου αλλαγές
- ◯ Δεν μπορώ να απαντήσω

Αν η επιχείρηση σας είχε ελλείψεις σε επίπεδο ασφάλειας, ποιες θα περιμένατε να είναι *

- ☐ Δεν υπάρχει επαρκής γνώση γύρω από την ασφάλεια στην επιχείρηση
- ☐ Η ασφάλεια δεν αποτελεί πρόβλημα
- ☐ Έλλειψη κατάλληλων τεχνικών λύσεων
- ☐ Έλλειψη καθοδήγησης
- ☐ Οι οδηγίες δεν ακολουθούνται
- ☐ Ελλειψη προσωπικού
- ☐ Ανεπαρκής χρηματοδότηση
- ☐ Δεν έχει πραγματοποιηθεί αξιολόγηση κινδύνου

Πώς θα αξιολογούσατε το επίπεδο διοικητικής ασφάλειας του οργανισμού σας *

- ◯ Πολύ καλό
- ◯ Αρκετά καλό
- ◯ Ούτε καλό αλλά ούτε κακό
- ◯ Όχι αρκετά καλό
- ◯ Καθόλου καλό
- ◯ Δεν μπορώ να απαντήσω

Εικόνα 27 Ερωτήσεις 5 έως 8

Πώς θα αξιολογούσατε το φυσικό επίπεδο ασφάλειας του οργανισμού σας *

- ◯ Πολύ καλό
- ◯ Αρκετά καλό
- ◯ Ούτε καλό αλλά ούτε κακό
- ◯ Όχι αρκετά καλό
- ◯ Καθόλου καλό
- ◯ Δεν μπορώ να απαντήσω

Πώς θα αξιολογούσατε το τεχνικό επίπεδο ασφάλειας του οργανισμού σας *

- ◯ Πολύ καλό
- ◯ Αρκετά καλό
- ◯ Ούτε καλό αλλά ούτε κακό
- ◯ Όχι αρκετά καλό
- ◯ Καθόλου καλό
- ◯ Δεν μπορώ να απαντήσω

Έχετε σκοπό να αναπτύξετε ή να επενδύσετε στις ανάγκες της ασφάλειας πληροφοριών της επιχείρησης *

- ◯ Ναι, αλλά όχι σύντομα
- ◯ Ναι, μέσα στους επόμενους 12 μήνες
- ◯ Πιθανόν, αλλά όχι σύντομα
- ◯ Πιθανόν, μέσα στους επόμενους 12 μήνες
- ◯ Όχι, είναι σε κάλο επίπεδο
- ◯ Όχι, δεν χρειάζεται
- ◯ Δεν μπορώ να απαντήσω

Εικόνα 28 Ερωτήσεις 9 έως 11

Ποιες από τις παρακάτω πολιτικές ασφάλειας υπάρχουν στην επιχείρηση *

- [ ] Business continuity plan
- [ ] Πρόσληψη εξωτερικής εταιρείας για την ασφάλεια των υπολογιστών
- [ ] Περιοδική αξιολόγηση ευπαθειών / κινδύνων
- [ ] Επίσημα / τεκμηριωμένα πρότυπα ασφάλειας υπολογιστών
- [ ] Εκπαίδευση του προσωπικού σε διαδικασίες ασφαλείας
- [ ] Διατήρηση αντιγράφων ασφαλείας
- [ ] Έλεγχος για πειρατικό λογισμικό
- [ ] Μέτρα ασφάλειας cloud computing
- [ ] Μέτρα ασφαλείας για τη χρήση προσωπικών συσκευών στην εργασία
- [ ] Δεν γνωρίζω
- [ ] Other:

Τους τελευταίους 12 μήνες, ποιες από τις ακόλουθες τεχνολογίες χρησιμοποιούνται στην επιχείρηση σας για σκοπούς ασφάλειας *

- [ ] Anti-virus/-malware protection
- [ ] Firewalls
- [ ] Anti-spam/-phishing tools
- [ ] Virtual Private Networks (VPN)
- [ ] Encrypted login/sessions (SSL/HTTPS)
- [ ] Intrusion detection systems
- [ ] Encrypted files
- [ ] Use of legal software
- [ ] Access control
- [ ] Uninterrupted power supply (UPS) for servers
- [ ] Physical theft prevention (Kensington locks)
- [ ] Offsite backups
- [ ] Δεν γνωρίζω
- [ ] Other:

Εικόνα 29 Ερωτήσεις 12 έως 13

Τους τελευταίους 12 μήνες, ποια από τα παρακάτω συμβάντα που σχετίζονται με την ασφάλεια πληροφορικής έχει αντιμετωπίσει μέχρι στιγμής η επιχείρηση σας *

- [ ] Virus/malware attack/infection
- [ ] Spam/phishing
- [ ] Hacker intrusion
- [ ] Unauthorized access of sensitive data/system by outsider
- [ ] Data loss
- [ ] Theft of electronic device
- [ ] Computer facilitated financial fraud
- [ ] Denial of service attack
- [ ] Unauthorised privileged access
- [ ] Degradation of network
- [ ] System penetration
- [ ] Web site defacement
- [ ] Theft of customer information
- [ ] Κανένα από τα παραπάνω

Τους τελευταίους 12 μήνες, πόσες φόρες πιστεύετε ότι υπήρξε κάποιο συμβάν στην επιχείρηση που αφορούσε την ασφάλεια της *

- ◯ Κανένα
- ◯ 1 εώς 5
- ◯ 6 εως 10
- ◯ 11 ή παραπάνω
- ◯ Other:

Έχει αναφέρει η επιχείρηση σας οποιαδήποτε περιστατικά εγκλήματος στον κυβερνοχώρο σε κάποιον από τους ακόλουθους οργανισμούς; *

- [ ] Αστυνομία
- [ ] Computer supplier
- [ ] Ειδική εταιρεία ασφάλειας υπολογιστών
- [ ] Κανέναν
- [ ] Other:

Εικόνα 30 Ερωτήσεις 14 έως 16

Αξιολογήστε την εμπιστοσύνη σας στην προστασία της επιχείρηση σας από εγκληματική επίθεση στον κυβερνοχώρο *

	1	2	3	4	5	
Καθόλου	○	○	○	○	○	Πολύ προστατευμένη

Η επιχείρηση σας διαθέτει σχέδιο έκτακτης ανάγκης σε περίπτωση εγκληματικής ενέργειας στον κυβερνοχώρο *

- ○ Ναί
- ○ Όχι
- ○ Δεν γνωρίζω
- ○ Other:

Πιστεύετε ότι η επιχείρηση θα αυξήσει τις δαπάνες της για την ασφάλεια τα επόμενα δύο με τρία χρόνια *

- ○ Ναί
- ○ Όχι
- ○ Δεν γνωρίζω
- ○ Other:

Χρησιμοποιεί η επιχείρηση σας μία ή περισσότερες εταιρίες ασφάλειας IT *

- ○ Ναι
- ○ Όχι
- ○ Σκοπεύομαι να προσλάβουμε
- ○ Other:

Πιστεύετε ότι οι κίνδυνοι για την ασφάλεια στον κυβερνοχώρο στο επιχειρηματικό περιβάλλον των μικρομεσαίων επιχειρήσεων αυξάνονται *

- ○ Ναι
- ○ Ίσως
- ○ Όχι
- ○ Δεν γνωρίζω
- ○ Other:

Εικόνα 31 Ερωτήσεις 17 έως 21

Κατά τη γνώμη σας, ποιος πρέπει να φροντίσει για την προστασία της ασφάλειας της επιχείρησης στον κυβερνοχώρο *

- ◯ Το τμήμα IT της επιχείρησης
- ◯ Εξωτερική εταιρία που ειδικεύεται στην κυβερνοασφάλεια
- ◯ Η ατομική εκπαίδευση των εργαζομένων στον τομέα της ασφάλειας είναι αρκετή
- ◯ Ένας πάροχος υπηρεσιών ασφαλείας με μηνιαία συνδρομή
- ◯ Other: _____

Πιστεύετε ότι τα προσωπικά δεδομένα των εργαζόμενων και πελατών της επιχείρησης είναι προστατευμένα *

	1	2	3	4	5	
Καθόλου προστατευμένα	◯	◯	◯	◯	◯	Αρκετά προστατευμένα

Γνωρίζετε τι είναι το GDPR (General Data Protection Regulation) *

- ◯ Ναι
- ◯ Όχι
- ◯ Other: _____

Η επιχείρηση σας έχει εναρμονιστεί με τους κανόνες του GDPR *

- ◯ Ναι
- ◯ Όχι
- ◯ Other: _____

Εικόνα 32 Ερωτήσεις 22 έως 25