ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΗΛΕΚΤΡΟΝΙΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
ΕΥΦΥΕΙΣ ΤΕΧΝΟΛΟΓΙΕΣ ΔΙΑΔΙΚΤΥΟΥ – WEBINTELLIGENCE

Βέλτιστες Πρακτικές Κυβερνοασφάλειας για Μικρομεσαίους Οργανισμούς: Ανάπτυξη Εργαλείου Αξιολόγησης του Επιπέδου Κυβερνοασφάλειας.

ΜΕΤΑΠΤΥΧΙΑΚΗ ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

της

ΣΤΑΜΑΤΙΑΣ ΔΑΛΚΙΤΣΗΣ

Επιβλέπων : Χρήστος Ηλιούδης
Καθηγητής ΔΙ.ΠΑ.Ε.

Θεσσαλονίκη, Σεπτέμβριος 2023

Η σελίδα αυτή είναι σκόπιμα λευκή.

ΔΙΕΘΝΕΣ ΠΑΝΕΠΙΣΤΗΜΙΟ ΤΗΣ ΕΛΛΑΔΟΣ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΗΛΕΚΤΡΟΝΙΚΩΝ ΣΥΣΤΗΜΑΤΩΝ
ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
ΕΥΦΥΕΙΣ ΤΕΧΝΟΛΟΓΙΕΣ ΔΙΑΔΙΚΤΥΟΥ – WEB INTELLIGENCE

Βέλτιστες Πρακτικές Κυβερνοασφάλειας για Μικρομεσαίους Οργανισμούς: Ανάπτυξη Εργαλείου Αξιολόγησης του Επιπέδου Κυβερνοασφάλειας.

ΜΕΤΑΠΤΥΧΙΑΚΗ ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

της

ΣΤΑΜΑΤΙΑΣ ΔΑΛΚΙΤΣΗΣ

Επιβλέπων: Χρήστος Ηλιούδης
Καθηγητής ΔΙ.ΠΑ.Ε.

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή στις Choose a date.

(Υπογραφή)	*(Υπογραφή)*	*(Υπογραφή)*
.....	.....	.....
Όνομα Επώνυμο Choose an item. ΔΙ.ΠΑ.Ε.	Όνομα Επώνυμο Choose an item. ΔΙ.ΠΑ.Ε.	Όνομα Επώνυμο Choose an item. ΔΙ.ΠΑ.Ε.

Θεσσαλονίκη, Σεπτέμβριος 2023

(Υπογραφή)

Δαλκίτση Σταματία

Μηχανικός Πληροφορικής και Τεχνολογίας Υπολογιστών

Περίληψη

Η κυβερνοασφάλεια είναι ένα από τα σημαντικότερα αντικείμενα μελέτης παγκοσμίως. Η ευρεία και αυξανόμενη χρήση του διαδικτύου, η τεχνητή νοημοσύνη, το διαδίκτυο των πραγμάτων, τα big data, ο ψηφιακός μετασχηματισμός και το νέο εργασιακό μοντέλο λειτουργίας με εργασία από το σπίτι ή υβριδική εργασία, με πολλαπλές συσκευές και τοποθεσίες, καθώς επίσης και η έλλειψη μέτρων κυβερνοασφάλειας έχουν οδηγήσει στην ραγδαία αύξηση των κυβερνοεπιθέσεων και του κυβερνοεγκλήματος.

Βάσει του σημαντικού ρόλου που διαδραματίζουν οι μικρομεσαίες επιχειρήσεις (ΜμΕ) και οργανισμοί στην οικονομία της Ελλάδας και της Ε.Ε. επιβάλλεται να εφαρμόσουν επαρκώς στρατηγικές κυβερνοασφάλειας. Τα διαθέσιμα πλαίσια κυβερνοασφάλειας λόγω της πολυπλοκότητας τους είναι δύσκολο να εφαρμοστούν σε ΜμΕ. Έτσι, είναι αναγκαία μια προσέγγιση επικεντρωμένη στις ΜμΕ.

Η παρούσα διπλωματική μελετάει εις βάθος τα παγκόσμια πλαίσια, πρότυπα και βέλτιστες πρακτικές της κυβερνοασφάλειας και αναπτύσσει ένα πλαίσιο κυβερνοασφάλειας προσαρμοσμένο στις ΜμΕ. Το πλαίσιο αυτό στοχεύει να βοηθήσεις τις ΜμΕ στην αξιολόγηση της κυβερνοασφάλεια τους. Λαμβάνει υπόψη του τις οδηγίες NIS και NIS2, καθώς επίσης και την Εθνική Στρατηγική Κυβερνοασφάλειας. Επιπλέον, βάσει του πλαισίου διεξάγεται έρευνα στις ΜμΕ και παρουσιάζονται τα αποτελέσματα της. Το πλαίσιο αξιολογείται από Ειδικούς στην κυβερνοασφάλεια τόσο του ιδιωτικού και δημοσίου τομέα όσο και από την ακαδημαϊκή και επιστημονική κοινότητα.

Λέξεις Κλειδιά:<< ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ, ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΩΝ, ΑΞΙΟΛΟΓΗΣΗ ΚΙΝΔΥΝΟΥ ΚΥΒΕΡΝΟΑΣΦΆΛΕΙΑΣ, ΠΛΑΙΣΙΟ STAM>>

Η σελίδα αυτή είναι σκόπιμα λευκή.

Abstract

Cybersecurity is one of the most important subjects of study worldwide. The wide and growing use of the internet, the artificial intelligence, the internet of things, the big data, the digital transformation, and the new model of remote or hybrid working, with multiple devices and locations, as well as the lack of cybersecurity measures have led to a rapid increase in cyber-attacks and cyber-crime.

Based on the important role that small and medium-sized businesses (SMBs) and organizations take part in the economy of Greece and the EU, it is imperative that they adequately implement cybersecurity strategies. The available cybersecurity frameworks due to their complexity are difficult to implement in SMBs. A SMB-focused approach is necessary.

This thesis, studies in depth the global cybersecurity frameworks, standards and best practices. Also, it develops a cybersecurity framework adapted to SMBs. This framework aims to help the SMBs with their cybersecurity's assessment. This considers the NIS and NIS2 directives, as well as the National Cyber Security Strategy. In addition, a survey of SMBs is carried out based on the framework and the results of this survey are presented. The framework is evaluated by cybersecurity experts from both private and public sector and the academic and scientific community.

Keywords:<< CYBER SECURITY, INFORMATION SECURITY, CYBER SECURITY RISK ASSESSMENT, NIS, STAM FRAMEWORK>>

Η σελίδα αυτή είναι σκόπιμα λευκή.

Περιεχόμενα

1. Εισαγωγή 10
   1.1. Επισκόπηση 10
   1.2. Ερευνητικό Πρόβλημα 10
   1.3. Μεθοδολογία 11
   1.4. Προσδοκώμενα Αποτελέσματα 12
   1.5. Δομή διπλωματικής 13
2. Κυβερνοασφάλεια 14
   2.1. Ορισμός κυβερνοασφάλειας 14
   2.2. Έννοιες στην κυβερνοασφάλεια 15
   2.3. Απειλές στην ασφάλεια 16
   2.4. Η κατάσταση στην κυβερνοασφάλεια σήμερα 20
   2.5. Η κυβερνοασφάλειας στις ΜμΕ 23
   2.6. Προβλήματα που αντιμετωπίζουν οι ΜμΕ 24
3. Βέλτιστες Πρακτικές 26
   3.1. Πρότυπα και πλαίσια 26
   3.2. Διεθνή Πρότυπα Ασφάλειας Πληροφοριών 26
   3.3. NIST Cybersecurity Framework 28
   3.4. CIS Controls 29
4. Νόμοι, Κανονισμοί & Οδηγίες 32
   4.1. Γενικός Κανονισμός για την Προστασία των Δεδομένων (GDPR) 32
   4.2. Οδηγία NIS 33
   4.3. Οδηγία NIS2 33
   4.4. Εθνικό σχέδιο δράσης για την κυβερνοασφάλεια 34
5. Πλαίσιο STAM - Security Technology and Management 37
   5.1. Βέλτιστες πρακτικές κυβερνοασφάλειας 37
   5.2. Διοίκηση και διαχείριση κυβερνοασφάλειας 38
   5.3. Καταγραφή και έλεγχος περιουσιακών στοιχείων 39
   5.4. Καταγραφή και έλεγχος λογισμικού 40
   5.5. Ασφαλής διαμόρφωση υλικού και λογισμικού 41
   5.6. Προστασία Δεδομένων 42
   5.7. Διαχείριση λογαριασμών 44
   5.8. Διαχείριση ελέγχου πρόσβασης 45

5.9. Διαχείριση αρχείων καταγραφής ... 46
5.10. Διαχείριση παρόχων υπηρεσιών ... 48
5.11. Διαχείριση δικτυακής υποδομής ... 49
5.12. Προστασία ηλεκτρονικού ταχυδρομείου και προγραμμάτων περιήγησης ... 50
5.13. Προστασία από κακόβουλο λογισμικό ... 51
5.14. Ασφάλεια εφαρμογών λογισμικού ... 52
5.15. Παρακολούθηση και άμυνα του δικτύου ... 54
5.16. Εκπαίδευση και ενημέρωση για την ασφάλεια ... 55
5.17. Αντίγραφα ασφαλείας & ανάκτηση δεδομένων ... 56
5.18. Διαχείριση αντιμετώπισης περιστατικών ... 57
5.19. Δοκιμές διείσδυσης ... 59
5.20. Συνεχής διαχείριση ευπαθειών ... 60
5.21. Φυσική ασφάλεια ... 61
6. Υλοποίηση & Αξιολόγηση του Πλαισίου STAM ... 63
6.1. Περιγραφή ... 63
6.2. Βαθμολογία & Επικινδυνότητα ... 64
6.3. Διερεύνηση για την εφαρμογή σε ΜμΕ ... 69
6.4. Σχεδιασμός & Υλοποίηση έρευνας και αξιολόγησης του πλαισίου STAM ... 70
6.4.1. Είσοδος του χρήστη & προφίλ χρήστη ... 71
6.4.2. Περιβάλλον ερωτημάτων & απαντήσεις ... 73
6.4.3. Αξιολόγηση εργαλείου από τον χρήστη ... 75
6.4.4. Εισαγωγή και οδηγίες για τη συμμετοχή στην έρευνα ... 76
6.4.5. Αξιολόγηση εργαλείου από Ειδικούς Ασφαλείας (CyberSecurity Experts) ... 78
6.5. Αποτελέσματα εργαλείου ... 79
6.6. Αποτελέσματα αξιολόγησης εργαλείου από Ειδικούς στην ασφάλεια ... 89
7. Επίλογος ... 96
7.1. Σύνοψη και συμπεράσματα ... 96
7.2. Αποτελέσματα ... 96
7.3. Μελλοντικές επεκτάσεις ... 98
8. Αναφορές ... 99

1. Εισαγωγή

1.1. Επισκόπηση

Οι μικρομεσαίοι οργανισμοί και επιχειρήσεις (ΜμΕ) στην Ευρώπη είναι 100 εκατομμύρια και αντιπροσωπεύουν το 99% όλων των επιχειρήσεων στην Ε.Ε. Σήμερα, τα δυο τρίτα των θέσεων εργασίας είναι σε ΜμΕ. Σύμφωνα με το άρθρο της Ευρωπαϊκής Επιτροπής (Commission, 2020) αντιπροσωπεύουν περισσότερο από το μισό του ΑΕΠ της Ε.Ε., αποτελούν βασικό πυλώνα της οικονομίας της και διαδραματίζουν βασικό ρόλο σε κάθε τομέα της οικονομίας. Επιπλέον, είναι απαραίτητες για την ανταγωνιστικότητα και την ευημερία της Ευρώπης και για την οικονομική και τεχνολογική κυριαρχία. Ο ορισμός των ΜμΕ διαφέρει σημαντικά μεταξύ των περιοχών παγκοσμίως. Σύμφωνα με την Eurostat, ΜμΕ ορίζονται αυτές που απασχολούν λιγότερα από 250 άτομα και έχουν ετήσιο κύκλο εργασιών έως 50 εκατομμύρια ευρώ ή συνολικό ισολογισμό όχι μεγαλύτερο από 43 εκατομμυρίων ευρώ.

Τα τελευταία χρόνια οι κυβερνοεπιθέσεις εναντίον τέτοιων επιχειρήσεων έχουν αυξηθεί δραματικά. Σε αυτήν την αύξηση έχει συμβάλει η πανδημία Covid-19, καθώς οι επιχειρήσεις από ένα μοντέλο στατικό έχουν περάσει σε ένα νέο μοντέλο λειτουργίας με απομακρυσμένη (remote) εργασία από το σπίτι (remote) ή υβριδική (hybrid), με πολλαπλές συσκευές και πολλές τοποθεσίες. Αυτή η κατάσταση, σε συνδυασμό με τον ψηφιακό μετασχηματισμό των ΜμΕ, τους συνεχώς αυξανόμενους καινοτόμους κυβερνοεγκληματίες και την έλλειψη μέτρων κυβερνοασφάλειας έχουν οδηγήσει παγκοσμίως σε ραγδαία αύξηση του κυβερνοεγκλήματος.

Βάσει του σημαντικού ρόλου που διαδραματίζουν οι ΜμΕ στην οικονομία, επιβάλλεται να εφαρμόσουν επαρκώς στρατηγικές κυβερνοασφάλειας και πρακτικές προστασίας συστημάτων, δικτύων και προγραμμάτων από τις ψηφιακές επιθέσεις. Η πρόοδος των τεχνολογιών μπορεί να έχει δημιουργήσει καινοτόμες δραστηριότητες, αλλά ταυτόχρονα έχει ενθαρρύνει τη δημιουργία τρωτών σημείων. Οι ΜμΕ χωρίς μέτρα κυβερνοασφάλειας δίνουν χώρο στους κυβερνοεγκληματίες με αποτέλεσμα να αποκτούν πρόσβαση σε συσκευές, δίκτυα, πόρους, προσωπικά δεδομένα, οικονομικά στοιχεία και άλλα. Οι επιθέσεις στον κυβερνοχώρο στοχεύουν συνήθως στην μη εξουσιοδοτημένη πρόσβαση, στην αλλαγή ή στην καταστροφή ευαίσθητων πληροφοριών, στην διακοπή της επιχειρηματικής δραστηριότητας, στον εκβιασμό μέσω ransomware και άλλα. Οι υψηλοί δείκτες του εγκλήματος παγκοσμίως στον κυβερνοχώρο και η απουσία δράσεων πρόληψης στις ΜμΕ, καθιστούν αυτή τη μελέτη ένα εργαλείο επιχειρηματικής κυβερνοασφάλειας. Οι ΜμΕ πρέπει να είναι προετοιμασμένες για τα κυβερνοεγκλήματα, καθώς και να επιδιώκουν να μειώσουν τους κινδύνους εφαρμόζοντας αποτελεσματικά μέτρα, κανονισμούς και πλαίσια που σχετίζονται με την κυβερνοασφάλεια. Η ανάπτυξη και η εφαρμογή αποτελεσματικών μέτρων κυβερνοασφάλειας αποτελεί σημαντική πρόκληση για τις ΜμΕ, καθώς οι κυβερνοεπιθέσεις μπορούν να έχουν σοβαρές συνέπειες τόσο οικονομικές όσο και στη φήμη τους.

1.2. Ερευνητικό Πρόβλημα

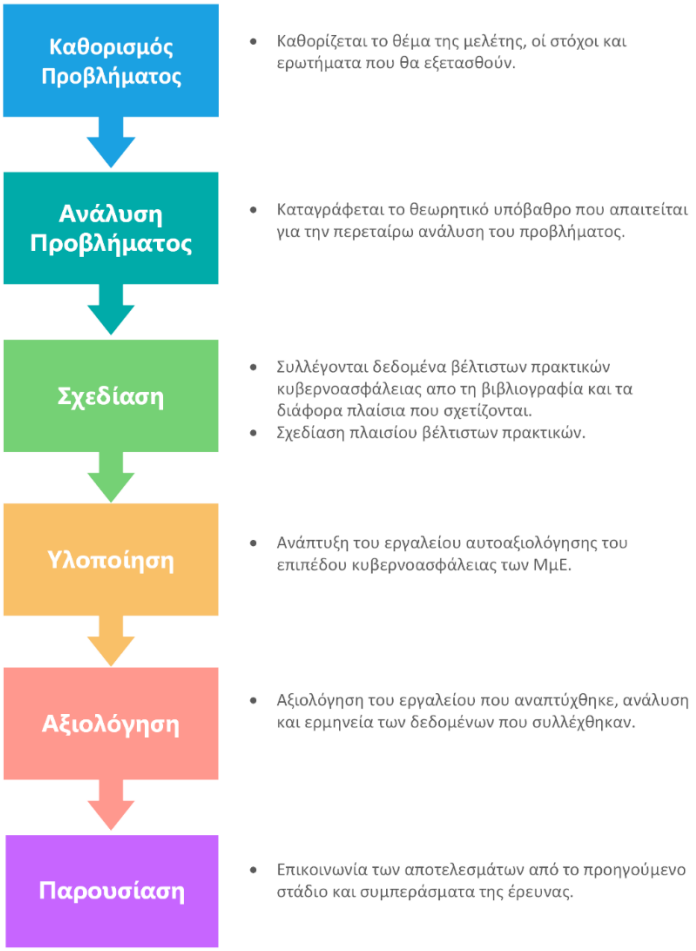
Η κυβερνοασφάλεια, η ασφάλεια των πληροφοριακών συστημάτων και η ασφάλεια της πληροφορίας αποτελούν έναν πολύπλοκο συνδυασμό μέτρων προφύλαξης, δηλαδή τεχνικών λύσεων, οργάνωσης και διαδικασιών, πολιτικών ασφαλείας, εκπαίδευσης, κατάρτισης και ενημέρωσης του ανθρώπινου δυναμικού και τακτικών ελέγχων όλων αυτών. Υπάρχουν πολλοί κανονισμοί και πλαίσια που εφαρμόζονται για την κυβερνοασφάλεια σε διάφορα επίπεδα, όπως σε επιχειρήσεις, οργανισμούς, κράτη

και διεθνείς οργανισμούς. Δυστυχώς, όλα τα παραπάνω δεν μπορούν να υλοποιηθούν στην πράξη σε κάθε επιχείρηση ή οργανισμό και ιδιαίτερα σε μικρές επιχειρήσεις.

Η μελέτη αυτή διερευνά τις παγκόσμιες κατευθυντήριες γραμμές, τα πλαίσια και τους κανονισμούς για την κυβερνοασφάλεια και επικεντρώνεται στην κυβερνοασφάλεια των μικρομεσαίων επιχειρήσεων και οργανισμών. Πραγματοποιείται εκτεταμένη έρευνα για την ανάπτυξη ενός πλαισίου βέλτιστων πρακτικών αυτοπροστασίας και ευαισθητοποίησης σε θέματα ασφάλειας των ΜμΕ. Τέλος, γίνεται προσπάθεια αξιολόγησης του πλαισίου για το αν αυτό μπορεί να συνεισφέρει στις ΜμΕ σχετικά με την λήψη στρατηγικών αποφάσεων για την κυβερνοασφάλειας, καθώς και αν συμβάλει στον σχεδιασμό και την ενδυνάμωση των μηχανισμών ασφαλείας.

1.3. Μεθοδολογία

Η μεθοδολογία αυτής της μελέτης περιλαμβάνει τον καθορισμό του προβλήματος και τα ερευνητικά ερωτήματα που θα εξετασθούν. Πραγματοποιείται μια συστηματική ανασκόπηση της βιβλιογραφίας για την κατανόηση της περιοχής της έρευνας ώστε να βρεθούν ανάλογες μελέτες και να καθοριστεί η θεωρητική βάση της μελέτης. Ακολουθεί η ανάλυση του προβλήματος, η σχεδίαση, η υλοποίηση, η αξιολόγηση και η παρουσίαση. Η μεθοδολογία παρουσιάζεται στην Εικόνα 1.



Εικόνα 1: Μεθοδολογία έρευνας.

1.4. Προσδοκώμενα Αποτελέσματα

Τα προσδοκώμενα αποτελέσματα αυτής της μελέτης είναι να επιτευχθούν οι στόχοι της και να απαντηθούν τα ερωτήματα τους. Η μελέτη έχει θεωρητικούς στόχους (Θ.Σ.), ερευνητικούς στόχους (Ε.Σ) και πρακτικούς στόχους (Π.Σ). Αναλυτικά:

1ος θεωρητικός στόχος: Βιβλιογραφική επισκόπηση της κυβερνοασφάλειας στις μικρομεσαίες επιχειρήσεις (ΜμΕ) και οργανισμούς.

Ερωτήματα:

1. Ποια είναι η έννοια της Κυβερνοασφάλειας;
2. Ποια είναι η σημερινή κατάσταση της κυβερνοασφάλειας στις ΜμΕ;

2ος θεωρητικός στόχος: Βιβλιογραφική επισκόπηση των προκλήσεων ασφάλειας που αντιμετωπίζουν οι μικρομεσαίες επιχειρήσεις (ΜμΕ) και οι οργανισμοί.

Ερωτήματα:

1. Ποιες είναι οι κυβερνοαπειλές που πρέπει να αντιμετωπίσουν οι ΜμΕ;
2. Με ποιόν τρόπο επηρεάζεται η ασφάλεια της επιχείρησης;
3. Ποιοι κανονισμοί και πλαίσια εφαρμόζονται για την κυβερνοασφάλειας στις ΜμΕ;

1ος ερευνητικός στόχος: Ανάπτυξη ενός πλαισίου βέλτιστων πρακτικών αυτοπροστασίας και ευαισθητοποίησης σε θέματα ασφάλειας των ΜμΕ.

Ερωτήματα:

1. Ποιοι είναι τα σημεία ελέγχου της ασφάλειας σε μια ΜμΕ;
2. Ποιες είναι οι βέλτιστες πρακτικές ασφάλειας για μια ΜμΕ;

Πρακτικός στόχος: Σχεδίαση και υλοποίηση ενός εργαλείου αξιολόγησης του επιπέδου κυβερνοασφάλειας των ΜμΕ σύμφωνα με το πλαίσιο που αναπτύχθηκε.

Ερωτήματα:

1. Έχει η ΜμΕ τεκμηριωμένη πολιτική και διαδικασίες σχετικά με την κυβερνοασφάλεια;
2. Ακολουθεί η ΜμΕ τις κατευθυντήριες γραμμές σύμφωνα με παγκόσμια πλαίσια για την ασφάλεια;

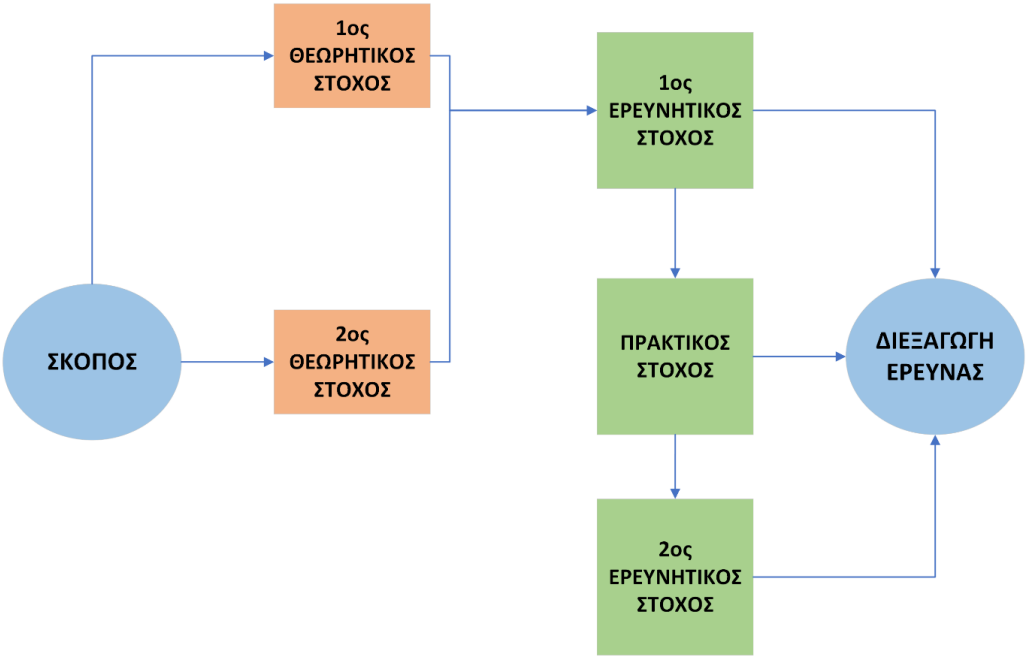
2ος ερευνητικός στόχος: Αξιολόγηση του εργαλείου αξιολόγησης τους επιπέδου κυβερνοασφάλειας των ΜμΕ.

Ερωτήματα:

1. Μπορεί να βοηθήσει ένα εργαλείο αυτοαξιολόγησης του επιπέδου κυβερνοασφάλειας μια ΜμΕ;
2. Είναι ικανοποιητική την ποιότητα των ζητημάτων που τέθηκαν;

Η μελέτη αυτή μπορεί να συνεισφέρει στην επιστημονική κοινότητα και να διαμορφώσει αυτό το γνωστικό αντικείμενο λόγω του ότι προσπαθεί να αναδείξει τη σχέση της θεωρίας και των εμπειρικών δεδομένων. Στο Διάγραμμα 1 παρουσιάζεται τη σύνδεση μεταξύ των θεωρητικών, των πρακτικών και των ερευνητικών στόχων.

Διάγραμμα 1: Σχέσεις των στόχων την μελέτης.



1.5. Δομή διπλωματικής

Αυτή η διπλωματική εργασία αποτελείται από τρία μέρη. Το πρώτο μέρος καλύπτει την βιβλιογραφική και θεωρητική πλευρά του θέματος και αποτελείται από το κεφάλαιο 2,3 και 4. Παρουσιάζει την κατάσταση της κυβερνοασφάλειας και συγκεκριμένα στις ΜμΕ. Επίσης, διεξάγει έρευνα σχετικά με τα πρότυπα, πλαίσια και τους κανονισμούς που σχετίζονται με το θέμα.

Στο δεύτερο μέρος της εργασίας, βάσει του θεωρητικού υπόβαθρου, αναπτύσσεται το πλαίσιο των βέλτιστων πρακτικών αυτοπροστασίας και ευαισθητοποίησης στα θέματα ασφάλειας των ΜμΕ. Το μέρος αυτό αποτελείται από το κεφάλαιο 5, το οποίο αποτελεί και τον βασικό πυλώνα της διπλωματικής εργασίας.

Το τελευταίο μέρος της εργασίας αποτελείται από το 6ο κεφάλαιο και περιλαμβάνει τη σχεδίαση του εργαλείου για την έρευνα στις ΜμΕ σχετικά με την αξιολόγησης της κυβερνοασφάλειας τους. Η υλοποίηση βασίζεται στο πλαίσιο που αναπτύχθηκε στο προηγούμενο στάδιο. Επιπλέον, το μέρος αυτό περιλαμβάνει τα αποτελέσματα της έρευνας καθώς και την αξιολόγηση του από Ειδικούς της ασφάλειας.

Η εργασία ολοκληρώνεται με τα αποτελέσματα και τα συμπεράσματα στο κεφάλαιο 7, καθώς επίσης συμπεριλαμβάνει και προτάσεις για μελλοντική επέκταση της έρευνας.

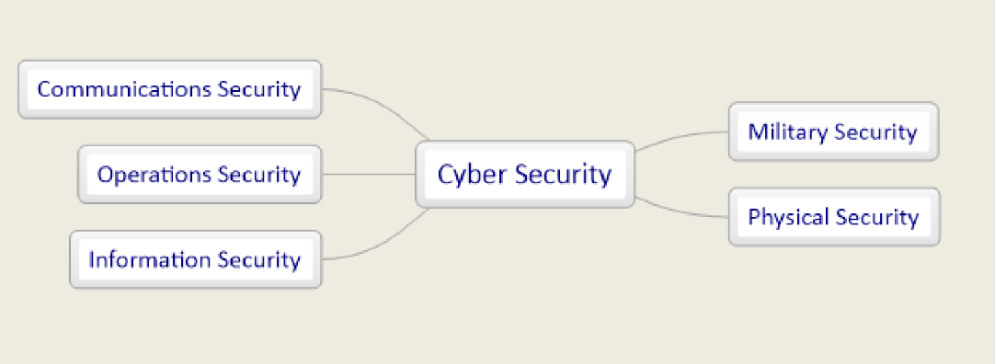
2. Κυβερνοασφάλεια

2.1. Ορισμός κυβερνοασφάλειας

Η ασφάλεια στον κυβερνοχώρο είναι ένας πολύ σύνθετος όρος που περνάει μέσα από πολυδιάστατα αιτήματα και απαντήσεις. Σήμερα, η «Κυβερνοασφάλεια – Cyber Security» εμφανίζεται ως ένας ευρέως χρησιμοποιούμενος όρος, ενώ φαίνεται να υπάρχει μικρή κατανόηση του τι πραγματικά συνεπάγεται ο όρος αυτός. Στην κοινή γλώσσα, η «κυβερνοασφάλεια» ορίζεται από το Αγγλικό Λεξικό της Οξφόρδης ως «η κατάσταση της προστασίας από την εγκληματική ή μη εξουσιοδοτημένη χρήση ηλεκτρονικών δεδομένων ή τα μέτρα που λαμβάνονται για να επιτευχθεί αυτό». Το έγγραφο (ENISA, 2015) αναφέρει ότι σύμφωνα με αυτή την ερμηνεία, καλύπτεται μόνο η μη εξουσιοδοτημένη και εγκληματική κατάχρηση πληροφοριών. (Patel, Suthar, & Parekh, 2021)

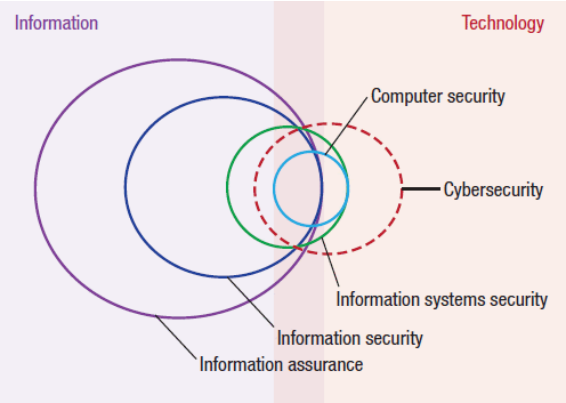
Γενικά, διάφορες παραλλαγές ορισμών αποδίδονται στον όρο από την παγκόσμια κοινότητα της επιστήμης των υπολογιστών. Επιπλέον, (ENISA, 2015) η διάδοση του όρου «κυβερνοασφάλεια» στα μέσα μαζικής ενημέρωσης αποτελεί μια φράση που αγγίζει τα πάντα, δηλαδή, οτιδήποτε μπορεί να διαταράξει τους υπολογιστές αποδίδεται ως απειλή για την «κυβερνοασφάλεια». Από την άλλη πλευρά στρατιωτικά περιβάλλοντα προσεγγίζουν τον όρο «κυβερνοασφάλεια» από μια ακόμη ευρύτερη και πολύ πιο στρατηγική προοπτική, χρησιμοποιώντας τον όρο σε σχέση με τους όρους «κυβερνοάμυνα» και «κυβερνοπόλεμος».

Ενδιαφέρον παρουσιάζει η έρευνα (Schatz, Bashroush, & Wall, 2017) η οποία μελετά την υπάρχουσα βιβλιογραφία για να προσδιορίσει τους κύριους ορισμούς που παρέχονται για τον όρο «κυβερνοασφάλεια» από έγκυρες πηγές και διεξάγει διάφορες τεχνικές λεξιλογικής και σημασιολογικής ανάλυσης ώστε να κατανοηθεί καλύτερα το εύρος και το πλαίσιο αυτών των ορισμών, μαζί με τη συνάφειά τους. Ωστόσο, στην κοινότητα των Προτύπων, ο ορισμός είναι σημαντικά ευρύτερος για να περιλαμβάνει προστασία έναντι ποικίλων κινδύνων για οργανισμούς και δεδομένα, ειδικά όταν η κυβερνοασφάλεια» θεωρείται συνώνυμο του «Information Security - Ασφάλεια πληροφοριών». Στο έγγραφο (ENISA, 2015), παρουσιάζονται οι διαφορετικοί τομείς εντός του όρου «Κυβερνοασφάλεια», δηλαδή ασφάλεια των επικοινωνιών, των λειτουργιών, των πληροφοριών, φυσική ασφάλεια και δημόσια/εθνική ασφάλεια, όπως απεικονίζεται στην Εικόνα 2.



Εικόνα 2: Διαφορετικοί τομείς της Κυβερνοασφάλειας (ENISA, 2015).

Οι πολλοί όροι που σχετίζονται με την ασφάλεια των υπολογιστών και έχουν χρησιμοποιηθεί τα τελευταία 50 χρόνια έχουν προκαλέσει σύγχυση ακόμη και στους επαγγελματίες της πληροφορικής. Η Εικόνα 3 είναι ένα πλασματικό διάγραμμα που απεικονίζει τη σχετική έμφαση και το εύρος σε σχέση με την πληροφορία έναντι της τεχνολογίας.



Εικόνα 3: Όροι που ισχύουν στην ασφάλειας των υπολογιστών με έμφαση στην τεχνολογία ή τις πληροφορίες και το εύρος. (Paulsen, 2016)

Τέλος, αξίζει να σημειωθεί ότι μπορεί η «κυβερνοασφάλεια» να μην έχει ευρέως αποδεκτό ορισμό, αλλά υπάρχει συναίνεση ότι εκτείνεται πέρα από τους υπολογιστές και περιλαμβάνει οποιοδήποτε ηλεκτρονικό σύστημα βασίζεται σε επικοινωνίες, όπως δορυφόρους ή αισθητήρες, καθώς και τα δεδομένα που αποθηκεύονται ή μεταδίδονται από αυτά τα συστήματα. Κάποιοι ορισμοί αποκλείουν προσεκτικά πληροφορίες που δεν αποθηκεύονται ή δεν μεταδίδονται από τέτοιες συσκευές, όπως για παράδειγμα, πληροφορίες που βασίζονται σε χαρτί ώστε να αποφευχθεί η σύγχυση με την ασφάλεια των πληροφοριών. (Paulsen, 2016)

2.2. Έννοιες στην κυβερνοασφάλεια

Η κυβερνοασφάλεια, η ασφάλεια των πληροφοριακών συστημάτων και η ασφάλεια των πληροφοριών συχνά συγχέονται μεταξύ τους, παρόλα αυτά συσχετίζονται με τους κοινούς στόχους τους, όπως η διασφάλιση της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας. Αυτοί είναι οι τρεις βασικοί πυλώνες της ασφάλειας, οι οποίοι και σχετίζονται μεταξύ τους και είναι γνωστοί ως η τριάδα της CIA. Θεωρείται ότι είναι οι κύριοι πυλώνες της ασφάλειας και πως οποιοσδήποτε προστατεύει ένα σύστημα πληροφοριών πρέπει να τους κατανοεί.

Εικόνα 4: Τριάδα της CIA.

Η τριάδα της CIA αντιπροσωπεύει τους τρεις πυλώνες της ασφάλειας των πληροφοριών, σύμφωνα με τους (Μαυρίδης, 2015) (Cawthra, et al., 2020) (Patel, Suthar, & Parekh, 2021) ως εξής:

> **Εμπιστευτικότητα (Confidentiality):** διατήρηση εγκεκριμένων περιορισμών στην πρόσβαση και την αποκάλυψη πληροφοριών. Αφορά την προστασία της πληροφορίας από μη εξουσιοδοτημένη αποκάλυψη (ανάγνωση) της. Στόχος της είναι να εξασφαλιστεί ότι οι ευαίσθητες πληροφορίες, όπως τα προσωπικά δεδομένα πελατών/υπαλλήλων, τα εμπιστευτικά δεδομένα επιχειρήσεων και άλλα ευαίσθητα δεδομένα, δεν θα διαρρεύσουν σε μη εξουσιοδοτημένα άτομα

ή οντότητες. Για τη διατήρηση της εμπιστευτικότητας, χρησιμοποιούνται μέτρα ασφαλείας όπως η κρυπτογράφηση, η διαχείριση πρόσβασης και άλλα.

Ακεραιότητα (Integrity): προστασία από αθέμιτη τροποποίηση ή καταστροφή πληροφοριών και διασφάλιση της μη άρνησης και της αυθεντικότητας των πληροφοριών. Η ακεραιότητα εξασφαλίζει ότι οι πληροφορίες δεν έχουν τροποποιηθεί από μη εξουσιοδοτημένους χρήστες ή αλλοιωθεί από τυχόν αποτυχίες του συστήματος. Ένας μηχανισμός ασφάλειας που χρησιμοποιείται για την διασφάλιση της ακεραιότητας είναι η ψηφιακή υπογραφή.

Διαθεσιμότητα (Availability): εξασφάλιση έγκαιρης και αξιόπιστης πρόσβασης στις πληροφορίες και στη χρήση τους. Διαφυλάσσει την εξουσιοδοτημένη πρόσβαση της πληροφορίας, χωρίς εμπόδια ή καθυστέρηση. Πιο συγκεκριμένα, η διαθεσιμότητα αφορά το ότι ένα πληροφοριακό σύστημα ή μια υπηρεσία είναι λειτουργικά διαθέσιμα κατά τη διάρκεια χρήσης τους από τους εξουσιοδοτημένους χρήστες, δηλαδή μπορούν να χρησιμοποιούνται και να εξυπηρετούνται τα αιτήματα των χρηστών όταν απαιτούνται. Αυτό σημαίνει ότι το σύστημα πρέπει να είναι προσβάσιμο και να λειτουργεί όπως προβλέπεται, χωρίς να υπάρχουν διακοπές ή αποτυχίες ή καθυστερήσεις που επηρεάζουν την παροχή των υπηρεσιών στους χρήστες.

Επιπλέον, πρέπει να αναφερθεί ότι η ασφάλεια συσχετίζεται με την επιτυχημένη ανάπτυξη και υλοποίηση μηχανισμών ασφάλειας, όπως:

Αυθεντικοποίηση (Authentication): ή αλλιώς επαλήθευση της ταυτότητας, είναι η διαδικασία επιβεβαίωσης της ταυτότητας μιας οντότητα στο σύστημα. Ο στόχος της αυθεντικοποίησης είναι να διασφαλιστεί ότι ο χρήστης ή το σύστημα που ζητά πρόσβαση είναι όντως αυτό που υποστηρίζει ότι είναι. Με την αυθεντικοποίηση, επιτυγχάνεται η διασφάλιση ότι ο χρήστης ή το σύστημα που ζητά πρόσβαση είναι ορθός, αλλά δεν διασφαλίζεται η δικαιοδοσία ή η εξουσιοδότηση του συγκεκριμένου χρήστη ή συστήματος να έχει πρόσβαση σε συγκεκριμένο πόρο. Για τη διασφάλιση της δικαιοδοσίας ή εξουσιοδότησης χρειάζεται η χρήση ενός συστήματος εξουσιοδότησης (Authorization), το οποίο ελέγχει τα δικαιώματα πρόσβασης του χρήστη ή του συστήματος σε συγκεκριμένους πόρους ή λειτουργίες.

Εξουσιοδότηση (Authorization): είναι η διαδικασία λήψης απόφασης για την αποδοχή ή την απόρριψη ενός αιτήματος πρόσβασης αυθεντικοποιημένων οντοτήτων στο σύστημα. Η εξουσιοδότηση συνήθως βασίζεται σε αναγνωριστικά στοιχεία, όπως το όνομα χρήστη και ο κωδικός πρόσβασης, που επιβεβαιώνουν την ταυτότητα του χρήστη και το δικαίωμά του να έχει πρόσβαση στο συγκεκριμένο πόρο ή στα συγκεκριμένα δεδομένα.

Μη αποποίηση (Non-Repudiation): είναι η διαδικασία της αδυναμίας άρνησης της ευθύνης για μιας ενέργεια στο σύστημα. Για παράδειγμα, σε ένα περιβάλλον ηλεκτρονικής επικοινωνίας, η αδυναμία αποποίησης σημαίνει ότι ένας αποστολέας δεν μπορεί να αρνηθεί την αποστολή ενός μηνύματος και ότι ο παραλήπτης μπορεί να αποδείξει ότι το μήνυμα προέρχεται από τον συγκεκριμένο αποστολέα. Αυτό επιτυγχάνεται με τη χρήση ψηφιακών υπογραφών και άλλων μηχανισμών πιστοποίησης ταυτότητας.

2.3. Απειλές στην ασφάλεια

Οι επιθέσεις που έχουν παρατηρηθεί στην ΕΕ έχουν διάφορους στόχους. Με βάση τα στοιχεία της λίστα απειλών ENISA και το έγγραφο (ΥΨΔ_ΕΑΚ, 2020) της Εθνικής Αρχής Κυβερνοασφάλειας 2020-2025, στα top threats του 2017 και 2018 είναι το κακόβουλο λογισμικό (malware) στην 1η θέση και οι επιθέσεις από το διαδίκτυο στη 2η θέση.

Top Threats 2017	Assessed Trends 2017	Top Threats 2018	Assessed Trends 2018	Change in ranking
1. Malware	▶	1. Malware	▶	▶
2. Web Bassed Attacks	▲	2. Web Bassed Attacks	▲	▶
3. Web Application Attacks	▲	3. Web Application Attacks	▶	▶
4. Phishing	▲	4. Phishing	▲	▶
5. Spam	▲	5. Denail of Service	▲	▲
6. Denial of Service	▲	6. Spam	▶	▼
7. Ransomware	▲	7. Botnets	▲	▲
8. Botnets	▲	8. Data Breaches	▲	▲
9. Insider threat	▶	9. Insider threat	▼	▶
10. Physical manipulation / damage / theft / loss	▶	10. Physical manipulation / damage / theft / loss	▶	▶
11. Data Breaches	▲	11. Information Leakage	▲	▲
12. Identity Theft	▲	12. Identity Theft	▲	▶
13. Information Leakage	▲	13. Cryptojacking	▲	NEW
14. Exploit Kits	▼	14. Ransomware	▼	▼
15. Cyber Espionage	▲	15. Cyber Espionage	▼	▶

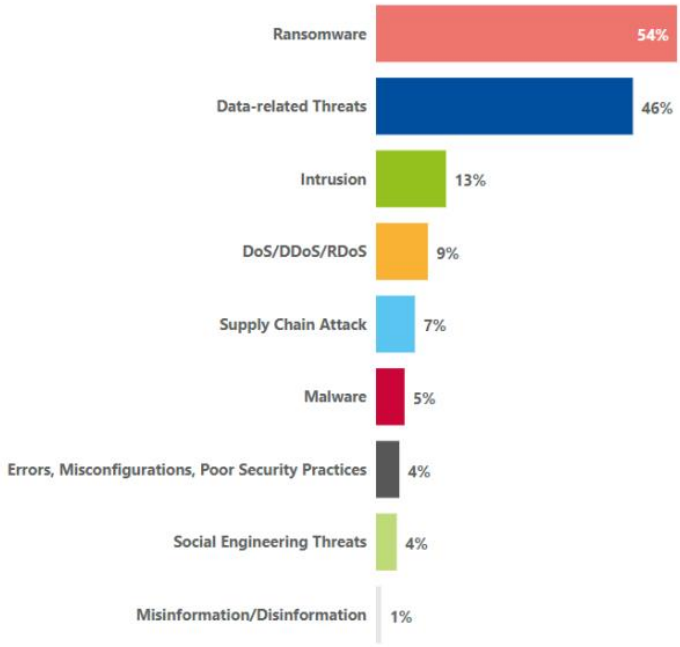
Legend: Trends: ▼ Declining ▶ Stable ▲ Increasing - Ranking: ▲ Going up ▶ Same ▼ Going down

Εικόνα 5: ENISA - 15 Top Cyberthreats and Trends. Αναφορά του 2018. (ΥΨΔ_ΕΑΚ, 2020)

Το τοπίο της κυβερνοασφάλειας αλλάζει συνεχώς και φαίνεται ότι είναι διαφορετικό από ότι πριν την πανδημία COVID-19. Τα τελευταία δύο χρόνια, εμφανίζονται νέοι τύποι απειλών για την ασφάλεια. Το 61% των οργανισμών αντιμετώπισε άλμα 25% ή περισσότερο στις κυβερνοαπειλές ή τις ειδοποιήσεις (alerts) από την έναρξη του COVID-19. Οι σύγχρονες επιθέσεις είναι πιθανόν να έχουν πολλαπλά στάδια που εκθέτουν τις εταιρείες σε διαφορετικούς κινδύνους. Όπως για παράδειγμα, μια επίθεση ransomware μπορεί να κλειδώσει τους χρήστες έξω από το εταιρικό δίκτυο, ενώ ταυτόχρονα εκμεταλλεύεται ευαίσθητα δεδομένα για να τα πουλήσει στο σκοτεινό διαδίκτυο (darkweb).

Το 2020, σύμφωνα με (ENISA_3, 2020), στο top threats, στην 1η θέση παραμένει το Malware, στη 2η θέση το Web-based attack και στην 3η θέση έχει ανέλθει το Phishing. Επιπλέον, σύμφωνα με (ENISA_2, 2023), παρατηρήθηκαν οι ακόλουθοι τύποι απειλών (Διάγραμμα 2) που στοχεύουν την ευρωπαϊκή υγεία. Τα περιστατικά που καταγράφηκαν, κατηγοριοποιήθηκαν σε περισσότερες από μια κατηγορίες απειλών, δηλαδή, μια επίθεση μπορεί να περιλαμβάνει αρχικά μια επίθεση Phishing και στη συνέχεια να ακολουθεί Ransomware. Για τον λόγο αυτό στο Διάγραμμα 5 τα ποσοστά υπερβαίνουν το 100%.

Διάγραμμα 2: Απειλές στον τομέα της υγείας (Ιανουάριος 2021 έως Μάρτιος 2023). (ENISA_2, 2023)



Παράλληλα, από τις πρόσφατες έρευνες και αναφορές της Cisco, υπάρχουν αξιόλογα δεδομένα. Σύμφωνα με (Whitaker, 2023) και (Cisco, 2022), τα δεδομένα για τις τάσεις απειλών στον κυβερνοχώρο από το 2021 έδειξαν (Εικόνα 7) ότι:

- Το 86% των οργανισμών βίωσαν phishing.
- Το 69% των οργανισμών βίωσε unsolicited cryptomining.
- Το 50% των οργανισμών βίωσε ransomware.
- Το 48% των οργανισμών αντιμετώπισε κακόβουλο λογισμικό κλοπής πληροφοριών (information-stealing malware).

Εικόνα 6: Τα δεδομένα του 2021 για τις τάσεις απειλών στον κυβερνοχώρο. (Cisco, 2022)

Οι ανησυχίες σχετικά με το ransomware έχουν αυξηθεί μαζικά. Σύμφωνα με την έρευνα της ESG και την αναφορά της HPE (Bertrand & Keane, 2022) το 82% των οργανισμών ανησυχούν σήμερα περισσότερο για το ransomware από ό,τι πριν από δύο χρόνια. Η πρόσφατη έρευνα δείχνει ότι ένα ανησυχητικό 63% των οργανισμών έχουν γίνει αποδέκτες απόπειρας επιθέσεων ransomware κατά τους τελευταίους 12 μήνες, ενώ το 36% αντιμετωπίζει συνεχείς απόπειρες σε μηνιαία βάση ή ακόμη πιο συχνά. Είναι ανησυχητικό ότι σχεδόν οι μισοί (48%) από τους ερωτηθέντες ανέφεραν ότι έπεσαν θύματα μιας επιτυχημένης επίθεσης ransomware.

Η έκθεση (CheckPoint, 2023) για την ασφάλεια στον κυβερνοχώρο κάνει μια αναδρομή σε ένα ταραχώδες 2022, το οποίο είδε τις κυβερνοεπιθέσεις να φτάνουν στο υψηλότερο επίπεδο όλων των εποχών ως απάντηση στον ρωσο-ουκρανικό πόλεμο. Οι παγκόσμιες κυβερνοεπιθέσεις αυξήθηκαν κατά 38% το 2022 σε σύγκριση με το 2021. Αξίζει να σημειωθεί ότι το «Cloud: Third Party Threat - Απειλή από τρίτους» είχε σημαντική αύξηση του αριθμού των επιθέσεων σε δίκτυα που βασίζονται στο νέφος ανά οργανισμό, ο οποίος εκτοξεύτηκε κατά 48% το 2022 σε σύγκριση με το 2021, υποδεικνύοντας μια ανησυχητική μετατόπιση.

Παράλληλα, με βάση την έκθεση (Sophos, 2023), δύο πράγματα ξεχωρίζουν: α) η συνεχής μείωση των εμποδίων εισόδου για επίδοξων κυβερνοεγκληματιών και β) η εμπορευματοποίηση των εργαλείων και τακτικών hacking που γίνονται πιο γρήγορα διαθέσιμα στην ευρύτερη εγκληματική κοινότητα. Επιπλέον, σύμφωνα με τους ισχυρισμούς (Heinrihs, Julija, & Andrejs, 2020), περίπου το 60% όλων των περιστατικών ασφάλειας πληροφοριών σε οργανισμούς προέρχονται από κακή χρήση των εργαζομένων.

Από τις τρέχουσες τάσεις, διαπιστώνεται ότι τα επόμενα χρόνια θα συνεχίσουμε να βλέπουμε μια ποικιλία απειλών για την ασφάλεια στον κυβερνοχώρο. Σύμφωνα με τις παγκόσμιες έρευνες, οι βασικότερες απειλές είναι:

Ransomware attacks - Επιθέσεις ransomware: Το Ransomware είναι ένας τύπος κακόβουλου λογισμικού που κρυπτογραφεί τα αρχεία και απαιτεί από το θύμα και κάτοχο των αρχείων πληρωμή σε αντάλλαγμα με το κλειδί αποκρυπτογράφησης.

Phishing attacks - Επιθέσεις ηλεκτρονικού "ψαρέματος": Το phishing είναι μια τεχνική κοινωνικής μηχανικής (social engineering) που χρησιμοποιείται από εγκληματίες του κυβερνοχώρου για να εξαπατήσουν τους ανθρώπους ώστε να τους αποκαλύψουν ευαίσθητες πληροφορίες ή να κατεβάσουν ή εγκαταστήσουν κακόβουλο λογισμικό.

Insider threats - Απειλές εκ των έσω: Οι απειλές εκ των έσω συμβαίνουν όταν εργαζόμενοι ή άλλοι εσωτερικοί χρήστες θέτουν σε κίνδυνο την ασφάλεια ενός οργανισμού εκούσια ή ακούσια. Αυτό μπορεί να περιλαμβάνει κλοπή ευαίσθητων δεδομένων, εγκατάσταση κακόβουλου λογισμικού ή άλλες κακόβουλες ενέργειες.

Supply chain attacks - Επιθέσεις στην αλυσίδα εφοδιασμού: Οι επιθέσεις στην εφοδιαστική αλυσίδα περιλαμβάνουν την παραβίαση ενός προμηθευτή ή τρίτου προμηθευτή προκειμένου να αποκτήσουν πρόσβαση στα συστήματα ή τα δεδομένα του οργανισμού που είναι στόχος.

Zero-day exploits - Εκμεταλλεύσεις μηδενικής ημέρας: Οι εκμεταλλεύσεις μηδενικής ημέρας είναι ευπάθειες σε λογισμικό ή υλικό που δεν είναι ακόμη γνωστές στον κατασκευαστή και για τις οποίες δεν υπάρχει διαθέσιμη επιδιόρθωση ή ενημέρωση. Οι επιτιθέμενοι μπορούν να χρησιμοποιήσουν τα zero-day exploits για να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση σε συστήματα ή δεδομένα.

Η έκθεση του 2020 από τη Verizon έδειξε ότι οι επιθέσεις είναι εκτεταμένες σε κάθε οργανισμό, ανεξάρτητα από το μέγεθος, τη βιομηχανία ή τον τομέα. Ωστόσο, σημειώνεται ότι παγκοσμίως, οι πάροχοι υπηρεσιών υγειονομικής περίθαλψης και οι επιχειρήσεις που σχετίζονται με τη χρηματοδότηση είναι οι πιο στοχευμένοι. Οι εκθέσεις του ακαδημαϊκού χώρου (Alladean, Sebastian, & Polychronis, 2022) αποκαλύπτουν ότι οι πιο συνηθισμένοι τύποι κυβερνοεπιθέσεων που αντιμετωπίζουν οι μικρομεσαίες επιχειρήσεις περιλαμβάνουν: κοινωνική μηχανική (π.χ. phishing), πειρατεία (π.χ. κλεμμένα διαπιστευτήρια, κλοπή δεδομένων), κακόβουλο λογισμικό (π.χ. ransomware), κακή χρήση (π.χ. κακόβουλο μυστικό), επιθέσεις που βασίζονται στον ιστό και επιθέσεις στην αλυσίδα εφοδιασμού ηλεκτρονικού εμπορίου.

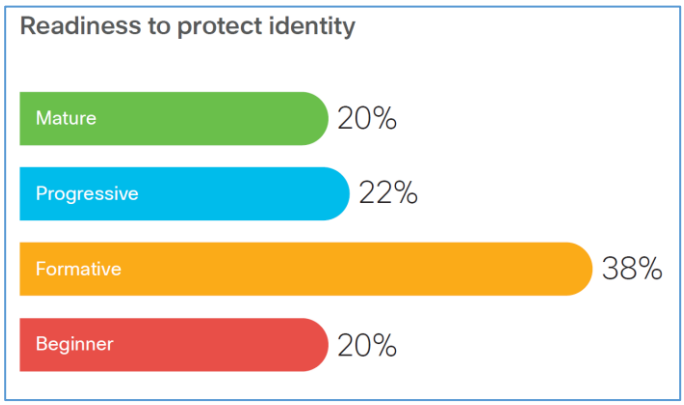
2.4. Η κατάσταση στην κυβερνοασφάλεια σήμερα

Η πανδημία COVID-19, σύμφωνα με την έκθεση IDB και OAS, επέτρεψε την επέκταση των τεχνολογιών πληροφοριών, της συνδεσιμότητας και της ασφάλειας στον κυβερνοχώρο παγκοσμίως. Ενώ σε παγκόσμιο επίπεδο, αντιμετωπίζεται μια πανδημία, το έγκλημα στον κυβερνοχώρο αυξήθηκε εκθετικά, επηρεάζοντας την ανάπτυξη των λειτουργιών των κρατικών υπηρεσιών και εταιρειών. Στην επίσημη ετήσια έκθεση για το έγκλημα στον κυβερνοχώρο της Cybercurity Ventures υποστηρίζεται ότι το έγκλημα στον κυβερνοχώρο είναι η μεγαλύτερη απειλή για όλους τους οργανισμούς παγκοσμίως. Υπολογίζεται ότι το 43% των παραβιάσεων δεδομένων συνέβη μέσω διαδικτυακών εφαρμογών και το 70% των επιθέσεων αυτών έγιναν από άτομα εκτός οργανώσεων και συγχρώνω το 86% υποκινήθηκαν από την οικονομική κρίση. Η μελέτη State of Cyber Risk in Latin America in Times of COVID-19, αναφέρει ότι το 21% θεωρεί ότι η κοινωνική μηχανική όπως το phishing είναι η κυβερνοεπίθεση που έχει αυξηθεί περισσότερο, ενώ το 20% υποστηρίζει ότι είναι το κακόβουλο λογισμικό. (Liset, και συν., 2022)

Η εταιρεία IBM και το Ponemon Institute (Megat, Zuraini, & Mohd, 2022), στην παγκόσμια μελέτη Cyber Resilient Organization, τόνισαν ότι το 77% των ερωτηθέντων περισσότερων από 3600 επαγγελματιών ασφάλειας και πληροφορικής από όλο τον κόσμο δεν έχουν σχέδιο αντιμετώπισης περιστατικών ασφάλειας στον κυβερνοχώρο και δεν είναι έτοιμοι να ανταποκριθούν κατάλληλα σε περιστατικά ασφάλειας στον κυβερνοχώρο.

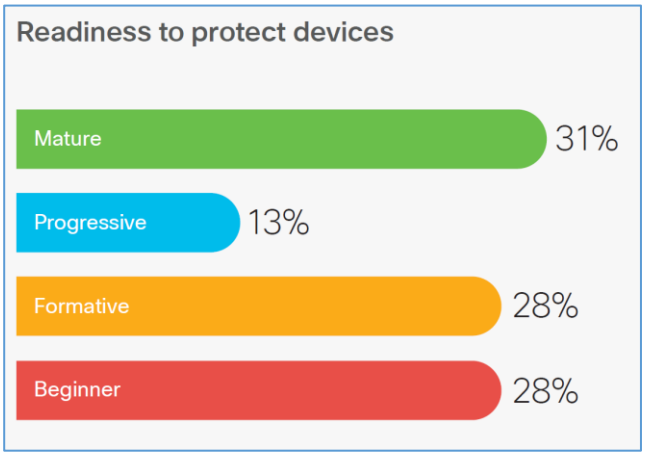
Η πρόσφατη έρευνα (Cisco-Secure, 2023), που πραγματοποιήθηκε μεταξύ Αυγούστου και Σεπτεμβρίου 2022, σχετικά με τον δείκτης ετοιμότητας για την κυβερνοασφάλεια, προέρχεται από 6.700 ηγέτες στον τομέα της κυβερνοασφάλειας του ιδιωτικού τομέα και οι οργανισμοί αυτοί καλύπτουν 27 περιοχές παγκοσμίως. Η έρευνα βασίστηκε σε πέντε πυλώνες: Ταυτότητα (identity), Συσκευές (devices), Δίκτυο (network), Φόρτος εργασίας Εφαρμογών (application workloads) και Δεδομένα (data). Μέσα από αυτούς τους πυλώνες, εξετάστηκαν 19 διαφορετικές λύσεις που απαιτούνται για την αντιμετώπισή τους. Ζητήθηκε από τους ερωτηθέντες να υποδείξουν ποιες από αυτές είχαν αναπτύξει, το στάδιο της ανάπτυξης και εάν αυτές οι λύσεις δεν είχαν ήδη αναπτυχθεί, τότε ποιοι προϋπολογισμοί είχαν εγκριθεί και το προβλεπόμενο χρονοδιάγραμμα ανάπτυξης. Οι ερωτηθέντες προέρχονται από 18 κλάδους: κατασκευής, εκπαίδευσης, αρχιτεκτονικής, χρηματοπιστωτικές υπηρεσίες, επικοινωνίες, υπηρεσίες φροντίδας υγείας, ακίνητων, τεχνολογίας, μεταφορών και άλλους.

Δεδομένου ότι η διαχείριση ταυτότητας κατατάσσεται από τους ερωτηθέντες ως ο υπ' αριθμόν ένα κίνδυνος, το 95% έχει εφαρμόσει κάποιο είδος λύσης διαχείρισης ταυτότητας. Ωστόσο, είναι ανησυχητικό το γεγονός ότι για όσους δεν έχουν ακόμη αναπτύξει λύσεις ταυτότητας, περισσότερα από τα δύο τρίτα (69%) δήλωσαν ότι δεν έχουν πρόθεση να το κάνουν. Παρά τη σαφή απειλή που παρουσιάζει η διαχείριση ταυτότητας, οι περισσότεροι από τους ερωτηθέντες βρίσκονται στο στάδιο Διαμόρφωσης (38%). (Cisco-Secure, 2023)



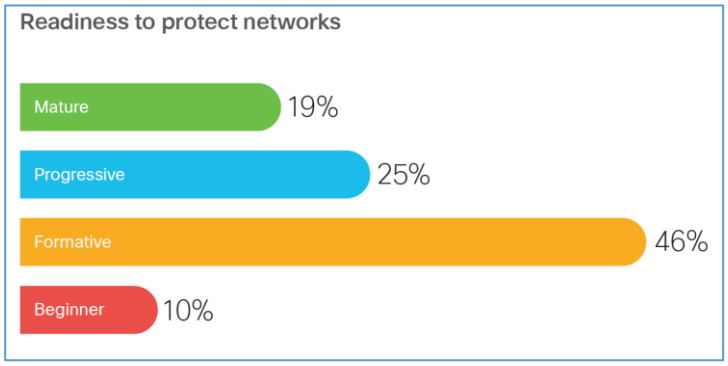
Εικόνα 7: Ετοιμότητα για προστασία της ταυτότητας. (Cisco-Secure, 2023)

Για τους ερωτηθέντες, η προστασία των συσκευών κατατάσσεται στην τρίτη θέση από τις πέντε της λίστα, πίσω από τη διαχείριση ταυτότητας και το ίδιο το δίκτυο. Επίσης, κατατάσσεται στην τρίτη θέση της λίστα τους για δυσκολία. Σχεδόν τα τρία τέταρτα (73%) των ερωτηθέντων επέλεξαν να χρησιμοποιήσουν βελτιωμένες λύσεις προστασίας από ιούς ως τη βασική τους λύση για την προστασία των συσκευών.



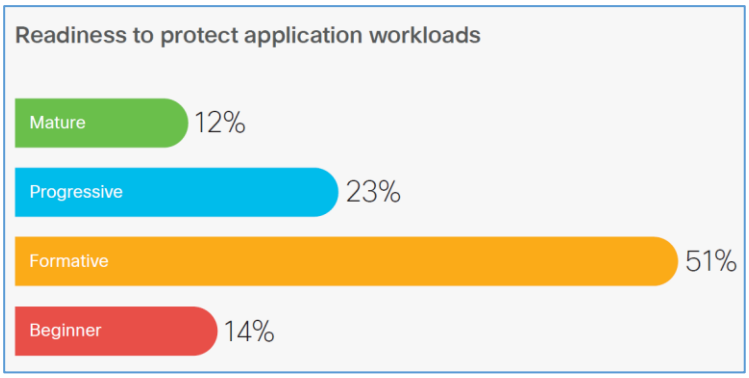
Εικόνα 8: Ετοιμότητα για προστασία συσκευών. (Cisco-Secure, 2023)

Μεταξύ των εταιρειών που εξακολουθούν να αναπτύσσουν λύσεις ασφάλειας δικτύου, οι μισές (50%) δήλωσαν ότι σχεδιάζουν να τις αναπτύξουν μέσα στους επόμενους 12 μήνες. Ανεξάρτητα από το πού βρίσκονται οι εταιρείες στην ανάπτυξή τους και ποια τεχνολογία χρησιμοποιούν, οι εταιρείες αξιολογούν την προστασία του δικτύου ως τη νούμερο δύο προτεραιότητά τους, το 56% βρίσκονται είτε στη διαμόρφωση είτε στη κατηγορία αρχάριων και μόλις 19% κάθεται στην κατηγορία ωρίμανσης.



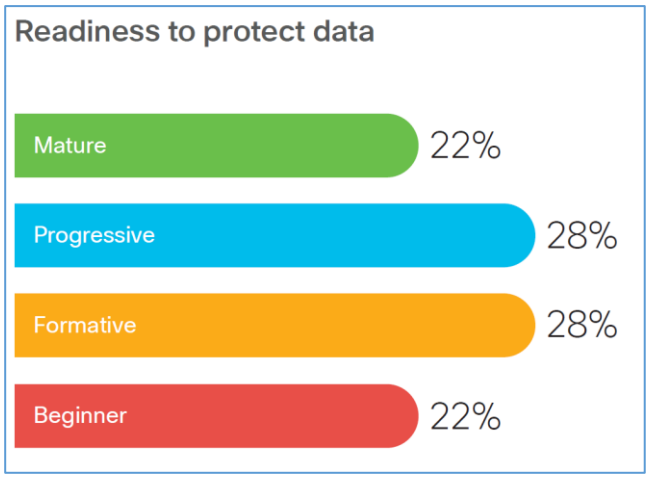
Εικόνα 9: Ετοιμότητα για προστασία των δικτύων. (Cisco-Secure, 2023)

Από την έρευνα προέκυψε ότι το 97% έχει αναπτύξει κάποιο είδος λύσης για την προστασία του φόρτου εργασίας των εφαρμογών. Το 66% επέλεξε να χρησιμοποιήσει ένα τείχος προστασίας λογισμικού κεντρικού υπολογιστή, αλλά η προστασία τελικού σημείου ήταν σε δεύτερη μοίρα με το 64% των οργανισμών να το επέλεξαν για να προστατευθούν. Λιγότερο δημοφιλή είναι τα εργαλεία προστασίας με επίκεντρο την εφαρμογή και το λογισμικό πρόληψης απώλειας δεδομένων (Data Loss Prevention – DLP).



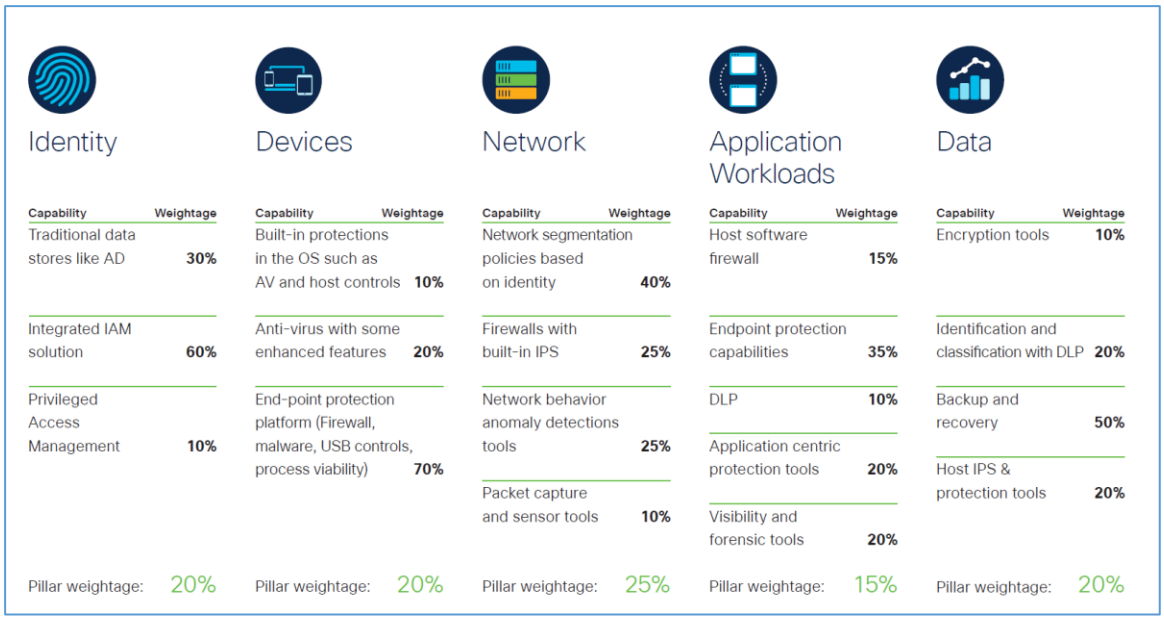
Εικόνα 10: Ετοιμότητα για προστασία του φόρτου εργασίας της εφαρμογών. (Cisco-Secure, 2023)

Από τις εκτιμήσεις του κλάδου, το 2022, δισεκατομμύρια σύνολα δεδομένων κλάπηκαν ως αποτέλεσμα παραβιάσεων της ασφάλειας στον κυβερνοχώρο. Για τις επιχειρήσεις, ο αντίκτυπος των διαρροών δεδομένων μπορεί να είναι πολύ σημαντικός. Οι εταιρείες ξοδεύουν σημαντικό χρόνο για την επίλυση της παραβίασης και την αποκατάσταση από καταστροφές, αλλά υπάρχουν εξίσου σημαντικές επιπτώσεις όταν τελειώσει η αρχική κρίση. Οι ερωτηθέντες της έρευνα φαίνεται να κατανοούν αυτές τις επιπτώσεις και το 98% αναφέρει ότι οι οργανισμοί τους έχουν λύσεις για την κατάλληλη προστασία των δεδομένων. Οι περισσότεροι έχουν επιλέξει είτε να κρυπτογραφήσουν τα δεδομένα είτε να διασφαλίσουν ότι μπορούν να δημιουργήσουν αντίγραφα ασφαλείας και να ανακτήσουν τα χαμένα δεδομένα. Περισσότερο από τα δύο τρίτα των επιχειρήσεων (67%) έχουν επιλέξει αυτές τις λύσεις για αυτόν τον πυλώνα προστασίας.



Εικόνα 11: Ετοιμότητα για προστασία δεδομένων. (Cisco-Secure, 2023)

Η έκθεσή (Cisco-Secure, 2023) παρουσιάζει ότι και στους πέντε τομείς, οι επιχειρήσεις σε όλο τον κόσμο σημειώνουν πρόοδο (Εικόνα 12). Από την έρευνα, η σημασία κάθε πυλώνα σταθμίστηκε ως δίκτυο (25%), ταυτότητα (20%), συσκευές (20%), δεδομένα (20%) και φόρτος εργασίας εφαρμογών (15%).



Εικόνα 12: Μέτρηση ετοιμότητας ασφαλείας – βαρύτητα. (Cisco-Secure, 2023)

2.5. Η κυβερνοασφάλειας στις ΜμΕ

Ο οικονομικός αντίκτυπος των περιστατικών στον κυβερνοχώρο μπορεί να κοστίσει από εκατοντάδες χιλιάδες ευρώ έως εκατομμύρια ανά εταιρεία και ανά έτος στην Ευρωπαϊκή Ένωση (ΕΕ). Σε παγκόσμιο επίπεδο, αυτός ο οικονομικός αντίκτυπος μπορεί να ποικίλλει από τον χαμηλότερο μέσο όρο των 16.400 ευρώ έως τον υψηλότερο μέσο όρο των 14,1 εκατομμυρίων ευρώ. Μια επιτυχημένη κυβερνοεπίθεση σε ΜμΕ θα μπορούσε να είναι καταστροφική. Σε έρευνα 250 ΜμΕ αναφέρεται ότι το 66% των εταιρειών έμειναν εκτός λειτουργίας ή έπρεπε να κλείσουν για μια ημέρα ή περισσότερο μετά από κυβερνοεπίθεση. (Juan, Marcos, Leire, Saioa, & Josune, 2020)

Η μελέτη που έγινε από την National Cyber Security Alliance (NCSA) και τη Symantec (Dhoha, και συν., 2018), δείχνει ότι το 71% των ΜμΕ εξαρτώνται σε μεγάλο βαθμό από το Διαδίκτυο για να εκτελέσουν τις καθημερινές λειτουργίες. Επιπλέον, το 87% των ΜμΕ δεν έχουν επίσημη τεκμηριωμένη «πολιτική ασφάλειας διαδικτύου» και το 69% δεν έχουν καθόλου «πολιτική ασφάλειας στο διαδίκτυο». Τα συστήματα των μικρών επιχειρήσεων πιθανότατα δεν είναι ασφαλή έναντι επιθέσεων στον κυβερνοχώρο επειδή δεν διαθέτουν τεχνογνωσία και δεξιότητες σε θέματα ασφάλειας. Τέλος, μεγάλο ενδιαφέρον έχει η μελέτη που έγινε στη Σαουδική Αραβία και δείχνει ότι οι περισσότεροι από τους υπαλλήλους της τεχνολογίας πληροφοριών (IT) έχουν κάποιες λανθασμένες ιδέες σχετικά με τις πρακτικές ασφάλειας πληροφοριών.

Από την άλλη πλευρά, η έρευνα της KPMG αποκάλυψε ότι οι μισές μικρές επιχειρήσεις πίστευαν ότι υπήρχε μικρός κίνδυνος να γίνουν στόχος επίθεσης. Στην ετήσια έκθεσή της για το 2016, η Symantec ανέφερε ότι το 43% των επιθέσεων spear-phishing στόχευαν επιχειρήσεις με 1–250 υπαλλήλους. Σύμφωνα με τον Toni Allen του Βρετανικού Ινστιτούτου Προτύπων, «οι ΜμΕ δεν ήταν ιστορικά στόχος του εγκλήματος στον κυβερνοχώρο, αλλά το 2015, κάτι άλλαξε δραστικά». Υπάρχουν πολλές υποθέσεις σχετικά με αυτήν την τάση, που συνήθως συγκλίνουν σε τρεις κύριες ιδέες:

1) Οι ΜμΕ είναι ιδιαίτερα ευάλωτες.
2) Οι εγκληματίες του κυβερνοχώρου αντιμετωπίζουν λιγότερες νομικές επιπτώσεις.
3) Οι εγκληματίες του κυβερνοχώρου χρησιμοποιούν ΜμΕ για να έχουν πρόσβαση σε μεγαλύτερες εταιρείες.

Η μελέτη του 2012 έδειξε ότι περίπου το 60 τοις εκατό των ΜμΕ που έπεσαν θύματα κυβερνοεπίθεσης έσβησαν μέσα σε έξι μήνες. Ακόμη και οι μικρές επιχειρήσεις που πιστεύουν ότι η ασφάλεια στον κυβερνοχώρο είναι σημαντική, συχνά δεν την κάνουν προτεραιότητα και οι περισσότερες δεν είναι προετοιμασμένες για κυβερνοεπίθεση. (KPMG, 2015) (Paulsen, 2016)

2.6. Προβλήματα που αντιμετωπίζουν οι ΜμΕ

Η αξία μιας επιχείρησης έγκειται στα δεδομένα και το σύστημα πληροφοριών της. Για τον λόγο αυτό η ασφάλεια έχει γίνει ένας σημαντικός παράγοντας που επηρεάζει το σύστημα πληροφοριών της επιχείρησης. Οι ΜμΕ για να συμβαδίζουν με την τρέχουσα εποχή και τον ανταγωνισμό, εξαρτώνται κυρίως από την τεχνολογία, ενώ παράλληλα έχουν ελάχιστη επίγνωση της κατάστασης της ασφάλειας των πληροφοριών τους. Με την ανάπτυξη της τεχνολογίας και την εξάρτηση των οργανισμών από αυτήν, η ασφάλεια του πληροφοριακού συστήματος έγινε μια από τις πιο σημαντικές πτυχές για τις οποίες πρέπει να ανησυχούν οι οργανισμοί, καθώς τα πληροφοριακά συστήματα ασχολούνται με πολλές ευαίσθητες και σημαντικές πληροφορίες για τον οργανισμό. (Dhoha, et al., 2018)

Η κατάσταση της κυβερνοασφάλειας για τις ΜμΕ είναι ανησυχητική. Οι επιθέσεις των κυβερνοεγκληματιών είναι συνεχείς και όλο και περισσότερες μικρομεσαίες επιχειρήσεις καταλήγουν να γίνονται στόχος τους. Οι κυβερνοεπιθέσεις μπορούν να έχουν δυσάρεστες συνέπειες για τις επιχειρήσεις, όπως τη διαρροή ευαίσθητων πληροφοριών, την καταστροφή δεδομένων, την απώλεια εμπιστοσύνης των πελατών και την πρόκληση σοβαρών οικονομικών ζημιών.

Το συνεχώς εξελισσόμενο τοπίο απειλών στον κυβερνοχώρο είναι ένα πρόβλημα για τις εταιρείες και αυτό ισχύει ιδιαίτερα για τις ΜμΕ, οι οποίες έχουν περιορισμένους πόρους για να αντιμετωπίσουν τις απειλές. Η παραδοσιακή προσέγγιση της κυβερνοασφάλειας για την προστασία από γνωστές απειλές δεν μπορεί να αντέξει τις ταχέως εξελισσόμενες τεχνολογίες και απειλές που χρησιμοποιούνται από τους εγκληματίες του κυβερνοχώρου. Επιπλέον, οι ΜμΕ ως ομάδα, αντιπροσωπεύουν ένα ωφέλιμο φορτίο για εκμετάλλευση από τους εγκληματίες του κυβερνοχώρου. (Juan, Marcos, Leire, Saioa, & Josune, 2020)

Ως εκ τούτου, η παραδοσιακή άποψη της κυβερνοασφάλειας πρέπει να μετατραπεί σε μια προσέγγιση που μπορεί να αντιμετωπίσει γρήγορες αλλαγές, που διατηρεί την επιχειρηματική συνέχεια παρά τις άγνωστες, απροσδόκητες και δυσμενείς καταστάσεις και που είναι βιώσιμη ανεξάρτητα από τις αλλαγές στο πλαίσιο. Μια αναδυόμενη προσέγγιση (Juan, Marcos, Leire, Saioa, & Josune, 2020), για την αντιμετώπιση αυτού του προβλήματος είναι η ανθεκτικότητα στον κυβερνοχώρο (Cyber Resilience). Αυτή η προσέγγιση ορίζεται συνήθως ως η ικανότητα πρόβλεψης, ανίχνευσης, αντοχής, ανάκτησης και εξέλιξης από περιστατικά στον κυβερνοχώρο, από οργανωτική, τεχνολογική και ανθρώπινη άποψη. Ο κύριος σκοπός του Cyber Resilience, σε αντίθεση με τις παραδοσιακές απόψεις για την ακυβερνοασφάλεια, είναι να προετοιμάσει την εταιρεία να είναι ένα σύστημα «ασφαλούς προς αποτυχία» προκειμένου να διατηρηθεί η επιχειρηματική συνέχεια παρά κάθε είδους δυσμενείς καταστάσεις, συμπεριλαμβανομένων απροσδόκητων και άγνωστων καταστάσεων.

Ωστόσο, η ανθεκτικότητα στον κυβερνοχώρο δεν είναι εύκολο να λειτουργήσει, επειδή είναι μια πολυδιάστατη έννοια που περιλαμβάνει τη διακυβέρνηση, την ευαισθητοποίηση και την εκπαίδευση και τη διαχείριση της επιχειρηματικής συνέχειας, μεταξύ άλλων διαστάσεων για τις οποίες οι ΜμΕ συνήθως δεν έχουν εκχωρήσει πόρους. Επιπλέον, η ανθεκτικότητα στον κυβερνοχώρο περιλαμβάνει επίσης την επένδυση σε διάφορες πολιτικές, όπως η προετοιμασία για άγνωστες απειλές, η διατήρηση της επιχειρηματικής συνέχειας, η συνεργασία με εξωτερικούς ενδιαφερόμενους και λοιπές. Αυτές οι προστιθέμενες πολιτικές είναι περίπλοκες καθώς απαιτούν στρατηγική, σχεδιασμό, δοκιμές, συντονισμό με εξωτερικές οντότητες και άλλα. Οι ΜμΕ συνήθως δεν διαθέτουν τους εξειδικευμένους πόρους για την υλοποίησή τους. Στην πραγματικότητα, οι περισσότερες ΜμΕ αγνοούν την ανάγκη εφαρμογής

αυτών των πολιτικών και έχουν αντιδραστική στάση απέναντι στην ασφάλεια. (Juan, Marcos, Leire, Saioa, & Josune, 2020)

Τα τελευταία χρόνια, ο αριθμός και το μέγεθος των κυβερνητικών και μη κερδοσκοπικών πρωτοβουλιών που βοηθούν τις μικρές επιχειρήσεις να αποκτήσουν μεγαλύτερη γνώση σχετικά με την ασφάλεια στον κυβερνοχώρο έχουν αυξηθεί σημαντικά. Παρά τη πληθώρα δωρεάν διαθέσιμων διαδικτυακών πληροφοριών για μικρές επιχειρήσεις, τις πολυάριθμες προσπάθειες ευαισθητοποίησης και κατάρτισης που διατίθενται στο εμπόριο σε μικρές επιχειρήσεις και τις συντονισμένες προσπάθειες των εταιρειών ασφάλειας στον κυβερνοχώρο να προσεγγίσουν αυτήν την αγορά, η πλειονότητα των μικρών επιχειρήσεων δεν ανταποκρίνεται (KPMG, 2015) (Paulsen, 2016).

Από την άλλη πλευρά, σύμφωνα με τις (KPMG, 2015) (Paulsen, 2016) οι μεγάλες εταιρείες για να προστατεύσουν τη δική τους επωνυμία, συχνά επιβάλλουν απαιτήσεις κυβερνοασφάλειας στους προμηθευτές τους, οι οποίες είναι μικρές επιχειρήσεις. Ορισμένες παρέχουν τη δική τους εκπαίδευση στον τομέα της κυβερνοασφάλειας και ελέγχουν προσωπικά τον προμηθευτή αντί να βασίζονται στις απαιτήσεις της σύμβασης. Επιπλέον, πολλές ενώσεις του κλάδου εκπαιδεύουν τακτικά τα μέλη τους σχετικά με τις βέλτιστες πρακτικές κυβερνοασφάλειας προσαρμοσμένες σε αυτόν τον κλάδο.

Στη βιβλιογραφία, σύμφωνα με τους (Juan, Marcos, Leire, Saioa, & Josune, 2020) υπάρχουν πολλά πλαίσια κυβερνοασφάλειας και ανθεκτικότητας στον κυβερνοχώρο. Τα περισσότερα όμως από αυτά τα πλαίσια δεν έχουν σχεδιαστεί για ΜμΕ, καθώς συχνά περιλαμβάνουν εκατοντάδες συγκεκριμένες πολιτικές που ενδέχεται να μην ισχύουν όλα για τις ΜμΕ. Για το λόγο αυτό είναι σημαντικό να καθοριστεί ένα πλαίσιο ανθεκτικότητας στον κυβερνοχώρο προσανατολισμένο στις ΜμΕ.

Ωστόσο, παρά τις προσπάθειες αυτές, οι ΜμΕ πρέπει να αναλάβουν οι ίδιοι την ασφάλεια των πληροφοριακών συστημάτων τους και την ευθύνη για τα δεδομένα τους από κυβερνοεπιθέσεις. Αυτό σημαίνει ότι πρέπει να λάβουν μέτρα για την πρόληψη κυβερνοεπιθέσεων, όπως την ενημέρωση και κατάρτιση των εργαζομένων τους για τους κινδύνους και τις απειλές, την εγκατάσταση τεχνικών μέτρων ασφάλειας όπως αντιικά προγράμματα ανίχνευσης και αντιμετώπισης επιθέσεων, καθώς και την τακτική ενημέρωση και αναβάθμιση των λογισμικών και των συστημάτων τους. Επίσης, είναι σημαντικό για τους οργανισμούς να υπάρχουν σαφείς πολιτικές και διαδικασίες για την πρόληψη πιθανών απειλών.

Τέλος, είναι σημαντικό για τις μικρομεσαίες επιχειρήσεις και τους οργανισμούς να αναγνωρίζουν ότι η κυβερνοασφάλεια είναι μια διαδικασία συνεχόμενη και όχι μια προσπάθεια ή ένα προϊόν που το αγοράζουν μια φορά. Αυτό σημαίνει ότι πρέπει να διατηρούν μια συνεχή αναβάθμιση ώστε να προσαρμόζονται στις νέες τεχνολογίες και τις νέες απειλές κυβερνοασφάλειας. Συνολικά, η κυβερνοασφάλεια αποτελεί μια πρόκληση για τις ΜμΕ καθώς η έλλειψη πόρων και εμπειρογνωμοσύνης μπορεί να τις καθιστά ευάλωτες σε κυβερνοεπιθέσεις. Ωστόσο, με την κατάλληλη εκπαίδευση, εξοπλισμό και συνεχή αναβάθμιση, μπορούν να λάβουν μέτρα προστασίας και να ανταποκριθούν στις απειλές κυβερνοασφάλειας με επιτυχία.

3. Βέλτιστες Πρακτικές

3.1. Πρότυπα και πλαίσια

Το πρότυπο (standard) είναι μια προδιαγραφή που καθορίζει ένα σύνολο κατευθυντήριων αρχών ή κανόνων, πρακτικών ή κριτηρίων που πρέπει να ακολουθηθούν για να ορίσουν ένα κοινό σημείο αναφοράς και για να επιτευχθεί μια συγκεκριμένη λειτουργικότητα, ποιότητα ή ασφάλεια σε ένα προϊόν ή υπηρεσία. Τα πρότυπα συνήθως αναπτύσσονται από οργανισμούς τυποποίησης ή παγκόσμιους οργανισμούς όπως η ISO (Διεθνής Οργάνωση Τυποποίησης) και μπορούν να αναφέρονται σε πολλά πράγματα, όπως προϊόντα, υπηρεσίες, διαδικασίες, συστήματα διαχείρισης, ποιότητας, περιβάλλοντος, ασφάλειας, πληροφοριακής τεχνολογίας, κ.λπ. Τα πρότυπα βοηθούν στη διασφάλιση της συνοχής και της ποιότητας και μπορούν επίσης να βελτιώσουν την ασφάλεια, την αποτελεσματικότητα και την αποδοτικότητα. Τα πρότυπα που σχετίζονται με την ασφάλεια των πληροφοριών και των πληροφοριακών συστημάτων είναι πολλά. Τα πιο γνωστά είναι το ISO/IEC 27001 (ISO/IEC27001, 2023), το οποίο αναφέρεται στα συστήματα διαχείρισης ασφάλειας των πληροφοριών και έχει ως στόχο την προστασία των πληροφοριών με τη διασφάλιση της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας τους και το ISO/IEC 27002 που παρέχει οδηγίες για την ασφάλεια των πληροφοριών και τις πρακτικές που μπορούν να εφαρμοστούν για την προστασία της ακεραιότητας, της εμπιστευτικότητας και της διαθεσιμότητας των πληροφοριών. (Malatji, 2023)

Από την άλλη πλευρά, το πλαίσιο (framework) είναι ένα σύνολο κανονισμών, προτύπων και εργαλείων που χρησιμοποιούνται για την υποστήριξη ενός συγκεκριμένου τρόπου εργασίας. Το πιο γνωστό πλαίσιο είναι το NIST Cybersecurity Framework για τη βελτίωση της ασφάλειας των πληροφοριών. Η κύρια διαφορά μεταξύ προτύπων και πλαισίων είναι ότι τα πρότυπα ορίζουν ένα σύνολο από κανόνες που πρέπει να ακολουθηθούν για να επιτευχθεί μια συγκεκριμένη λειτουργικότητα, ποιότητα ή ασφάλεια σε ένα προϊόν ή υπηρεσία, ενώ τα πλαίσια παρέχουν ένα σύνολο εργαλείων, οδηγιών και πρακτικών που βοηθούν στην εφαρμογή των προτύπων και στη βελτιστοποίηση της διαδικασίας ανάπτυξης ή λήψης αποφάσεων.

3.2. Διεθνή Πρότυπα Ασφάλειας Πληροφοριών

Η οικογένεια προτύπων ISO 27000 βοηθάει τους οργανισμούς να διατηρούν τα περιουσιακά στοιχεία και τις πληροφορίες ασφαλείς, δηλαδή, είναι ένας οδηγός βέλτιστων πρακτικών για τη διαχείριση της ασφάλειας πληροφοριών και τη διαχείριση της σχετικής επικινδυνότητας που αντιμετωπίζει ένας οργανισμός. Το κεντρικό πρότυπο είναι το ISO/IEC 27001 (ISO/IEC27001, 2023), με το οποίο μπορεί ένας οργανισμός ανεξαρτήτως μεγέθους και δραστηριότητας, να εναρμονιστεί και να πιστοποιηθεί από έναν τρίτο ανεξάρτητο φορέα. Το πρότυπο ISO/IEC 27001 καθορίζει τις απαιτήσεις για την καθιέρωση, εφαρμογή, διατήρηση, παρακολούθηση, επανεξέτασης και συνεχούς βελτίωσης των ISMS (Information Security Management System). Ένα ISMS είναι ουσιαστικά μια δομή διακυβέρνησης που αποτελείται από ένα σύνολο πρακτικών, μεθόδων και διαδικασιών με τις οποίες διαχειρίζεται κίνδυνοι για την ασφάλεια των πληροφοριών.

Με την πάροδο των χρόνων, το πρότυπο ISO 27001 έχει υποστεί συνεχείς βελτιώσεις και προέρχεται από ένα προηγούμενο σύνολο προτύπων. Το ISO 27001 περιγράφει τρεις βασικές πτυχές ή "πυλώνες" της αποτελεσματικής ασφάλειας πληροφοριών: άνθρωποι, διαδικασίες και τεχνολογία. Η τριμερής αυτή προσέγγιση βοηθά τους οργανισμούς να αμυνθούν από τις οργανωμένες επιθέσεις και από τις κοινές εσωτερικές απειλές, όπως οι τυχαίες παραβιάσεις, οι επιθέσεις και τα ανθρώπινα λάθη. Η εφαρμογή μιας διαχείρισης της ασφάλειας πληροφοριών συστήματος σύμφωνα με το ISO/IEC 27001 έχει τα εξής πλεονεκτήματα για τους οργανισμούς:

- Επιτρέπει τον εντοπισμό και την εξάλειψη των απειλών και τρωτών σημείων.
- Παρέχει ασφάλεια και εμπιστοσύνη σε όλα τα ενδιαφερόμενα μέρη (πελάτες, συνεργάτες και άλλους).
- Βελτιώνει την ευαισθητοποίηση σε θέματα ασφάλειας.
- Αυξάνει την ικανότητα πρόβλεψης και διαχείρισης μιας καταστροφής, και επιβίωσης.
- Εμβαθύνει τις γνώσεις σχετικά με τον οργανισμό και τις διαδικασίες, τα περιουσιακά στοιχεία και τις υποχρεώσεις του.
- Παρέχει πραγματική γνώση του κινδύνου που διατρέχει ο οργανισμός.
- Διασφαλίζει την επιχειρησιακή συνέχεια.
- Συμβάλλει στη μείωση του κόστους και στην στη βελτίωση των διαδικασιών και των υπηρεσιών.
- Διασφαλίζει τη συμμόρφωση με την ισχύουσα νομοθεσία.
- Μειώνει το κόστος που συνδέεται με τη "μη ασφάλεια".

Το πρότυπο εδράζεται σε επτά υποχρεωτικές απαιτήσεις του ISMS για την πιστοποίηση κατά ISO, επίσης γνωστές ως ρήτρες, οι οποίες αφορούν περισσότερο το σύστημα διαχείρισης παρά τους ελέγχους ασφαλείας, (Malatji, 2023) και οι οποίες είναι:

- Πλαίσιο του οργανισμού
- Ηγεσία
- Σχεδιασμός
- Υποστήριξη
- Λειτουργία
- Αξιολόγηση της απόδοσης
- Βελτίωση

Το ISO 27001: 2013, σύμφωνα με τους (Lopes, Guarda, & Oliveira, 2019) (Monev, 2020), έχει 14 ρήτρες ελέγχου ασφάλειας που περιέχουν συνολικά 35 στόχους ελέγχου και 114 ελέγχους. Στις 25 Οκτωβρίου 2022 εκδόθηκε η τρίτη έκδοση του προτύπου ISO/IEC 27001:2022 για την αντιμετώπιση της παγκόσμιας ασφάλειας στον κυβερνοχώρο και τη βελτίωση της ψηφιακής εμπιστοσύνης. Σύμφωνα με το IAF MD 26:2023, Issue 2, στην νέα έκδοση του ISO/IEC 27001:2022 τροποποιούνται 11 σημεία της αντίστοιχης έκδοσης του 2013.

Ένα άλλο πρότυπο της ίδιας οικογένειας είναι το ISO/IEC 27005:2022 (ISO/IEC27005:2022, 2023), σχετικά με την « Ασφάλεια πληροφοριών, κυβερνοασφάλεια και προστασία της ιδιωτικής ζωής» παρέχει οδηγίες για τη διαχείριση κινδύνων για την ασφάλεια των πληροφοριών ώστε να βοηθήσει τους οργανισμούς να πληρούν τις απαιτήσεις του προτύπου ISO/IEC 27001 σχετικά με ενέργειες για την αντιμετώπιση κινδύνων ασφάλειας πληροφοριών και να εκτελεί δραστηριότητες διαχείρισης κινδύνων για την ασφάλεια των πληροφοριών.

Εξίσου σημαντικό πρότυπο είναι και το ISO 20000 (ISO/IEC20000-1:2018, 2023), το οποίο καθορίζει τις απαιτήσεις για έναν οργανισμό για τη δημιουργία, την εφαρμογή, τη συντήρηση και τη συνεχή βελτίωση ενός συστήματος διαχείρισης υπηρεσιών (SMS). Το πρότυπο αυτό μπορεί να χρησιμοποιηθεί όταν:

- ο πελάτης αναζητά υπηρεσίες και απαιτεί βεβαιότητα σχετικά με την ποιότητα αυτών των υπηρεσιών,
- ο πελάτης απαιτεί συνεπή προσέγγιση στον κύκλο ζωής της υπηρεσίας από όλους τους παρόχους υπηρεσιών του, συμπεριλαμβανομένων εκείνων που βρίσκονται σε μια αλυσίδα εφοδιασμού,
- ένας οργανισμός επιδεικνύει την ικανότητά του για τον προγραμματισμό, το σχεδιασμό, τη μετάβαση, την παράδοση και τη βελτίωση των υπηρεσιών του,

- ένας οργανισμός ή άλλο μέρος διενεργεί αξιολογήσεις συμμόρφωσης σύμφωνα με τις απαιτήσεις που καθορίζονται στο πρότυπο,

Παρόλο που το πρότυπο ISO 20000 έχει μια διαδικασία διαχείρισης της ασφάλειας των πληροφοριών, σύμφωνα με τους (Tanović & Marjanovic, 2019) εξακολουθεί να περιέχει μόνο βασικές κατευθυντήριες γραμμές για την εφαρμογή της ασφάλειας πληροφοριών.

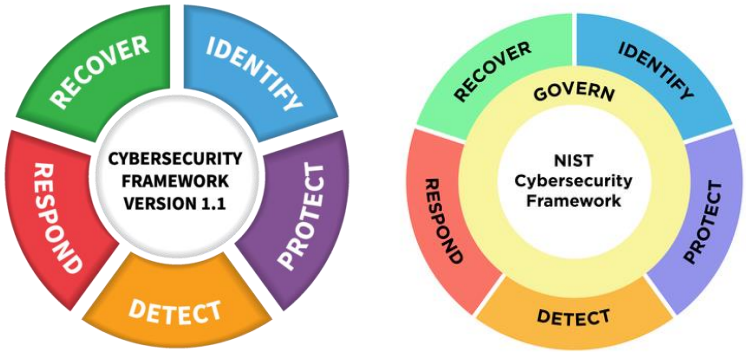
Σήμερα, σημαντικό πρότυπο στον τομέα των συστημάτων διαχείρισης που σχετίζονται με την ασφάλεια των πληροφοριών είναι και το ISO 22301. Το ISO 22301 (ISO22301:2019, 2023), είναι για τη διαχείριση της επιχειρησιακής συνέχειας, το οποίο καθορίζει τις απαιτήσεις για την εγκαθίδρυση, την υλοποίηση, τη λειτουργία, την αξιολόγηση, τη συντήρηση και τη βελτίωση ενός συστήματος διαχείρισης επιχειρησιακής συνέχειας. Η επιχειρησιακή συνέχεια αφορά την ικανότητα μιας επιχείρησης να συνεχίσει να λειτουργεί κανονικά ή να επανέλθει στην κανονική της λειτουργία μετά από διακοπή της παροχής υπηρεσιών, μιας φυσικής καταστροφής, μιας κυβερνοεπίθεσης ή άλλου σοβαρού περιστατικού. Το πρότυπο ISO 22301 βοηθά τις επιχειρήσεις να αναπτύξουν σχέδια και διαδικασίες που θα εξασφαλίζουν τη συνέχιση της λειτουργίας τους σε περίπτωση διακοπής και να μειώσουν τις επιπτώσεις αυτής της διακοπής στην επιχείρηση και στους πελάτες της

Όλα όσα αναφέρθηκαν παραπάνω είναι μερικά από τα γνωστά πρότυπα ασφαλείας που σχετίζονται με την ασφάλεια των πληροφοριών. Είναι σημαντικό για τις επιχειρήσεις να συμμορφώνονται με αυτά τα πρότυπα για να διασφαλίσουν την προστασία των πληροφοριών και την αποφυγή παραβιάσεων δεδομένων.

3.3. NIST Cybersecurity Framework

Ένα πλαίσιο κυβερνοασφάλειας μπορεί να είναι ένας ζωτικός οδηγός. Το NIST Cybersecurity Framework (NIST, 2014) αναπτύχθηκε από το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας (National Institute of Standards and Technology - NIST) των Ηνωμένων Πολιτειών για να βοηθήσει τις επιχειρήσεις και τις κυβερνήσεις να διαχειριστούν τον κίνδυνο και να βελτιώσουν την κυβερνοασφάλεια τους. Αυτό το πλαίσιο παρέχει μια μεθοδολογία για τη βελτίωση της ασφάλειας των πληροφοριών σε διάφορους τομείς. Συγκεκριμένα, το NIST SP 800-53 αποτελεί μια σειρά από κατευθυντήριες γραμμές ασφαλείας για την προστασία της απορρήτου και της ασφάλειας των πληροφοριών στις Ηνωμένες Πολιτείες. Οι κατευθυντήριες γραμμές αυτές περιλαμβάνουν πάνω από 900 απαιτήσεις ασφαλείας, που καλύπτουν ένα ευρύ φάσμα θεμάτων από τη διαχείριση των κινδύνων ασφαλείας μέχρι την αποτελεσματική ανίχνευση και αντίδραση σε παραβάσεις ασφαλείας. Αυτό το πρότυπο ασφάλειας είναι κατάλληλο για κυβερνητικούς οργανισμούς, όπως και για επιχειρήσεις και άλλους φορείς που έχουν σχέση με την κυβερνοασφάλεια στις Ηνωμένες Πολιτείες. Οι λειτουργίες αυτού του πλαισίου δεν προορίζονται να αποτελέσουν μια σειριακή διαδρομή με αποτέλεσμα μια στατική επιθυμητή κατάσταση. Οι λειτουργίες αυτές μπορούν να εκτελεστούν ταυτόχρονα και συνεχώς για να διαμορφώσουν μια επιχειρησιακή κουλτούρα ώστε να αντιμετωπίσουν τον κίνδυνο.

Τον Αύγουστο του 2023 (NIST_2023, 2023), ο NIST συντάσσει σημαντική ενημέρωση για το ευρέως χρησιμοποιούμενο πλαίσιο ασφάλειας στον κυβερνοχώρο και έχει αναθεωρήσει το πλαίσιο για να βοηθήσει όλους τους τομείς, όχι μόνο τις υποδομές ζωτικής σημασίας. Είναι η πρώτη πλήρη ανανέωση μετά από εννέα έτη. Ο NIST έχει δημοσιεύσει ένα προσχέδιο, το NIST CSWP 29 - Cybersecurity Framework 2.0 και δέχεται δημόσια σχόλια μέχρι 4 Νοεμβρίου 2023. Τα σχόλια από αυτό το προσχέδιο θα ενημερώσουν την ανάπτυξη του τελικού CSF 2.0, το οποίο θα δημοσιευτεί στις αρχές του 2024. Η Εικόνα 13 από αριστερά παρουσιάζει τις βασικές λειτουργίες του πλαισίου και από δεξιά το προσχέδιο, στο οποίο έχει προσθέσει μια έκτη λειτουργία, την "διακυβέρνηση", με την οποία τονίζει ότι η κυβερνοασφάλεια είναι μια σημαντική πηγή επιχειρηματικού κινδύνου και λαμβάνεται υπόψη η ανώτερη ηγεσία.



Εικόνα 13: Βασικές λειτουργίες του NIST Cybersecurity Framework. (NIST, 2014) (NIST_2023, 2023)

Οι πέντε βασικές λειτουργίες του πλαισίου είναι σύμφωνα με το (NIST, 2014) είναι:

Προσδιορισμός (Identify) - Ανάπτυξη της οργανωτικής κατανόησης για τη διαχείριση του κινδύνου κυβερνοασφάλειας για τα συστήματα, τα περιουσιακά στοιχεία, τα δεδομένα και τις δυνατότητες.

Προστασία (Protect) - Ανάπτυξη και εφαρμογή των κατάλληλων διασφαλίσεων για να εξασφαλιστεί η παροχή υπηρεσιών υποδομής ζωτικής σημασίας. Η λειτουργία αυτή υποστηρίζει την ικανότητα περιορισμού των επιπτώσεων ενός πιθανόν συμβάντος κυβερνοασφάλειας.

Ανίχνευση (Detect) - Ανάπτυξη και εφαρμογή των κατάλληλων δραστηριοτήτων για τον έγκαιρο εντοπισμό της εμφάνισης ενός συμβάντος κυβερνοασφάλειας.

Απόκριση (Respond) - Ανάπτυξη και εφαρμογή των κατάλληλων δραστηριοτήτων για την ανάληψη δράσης σχετικά με ένα ανιχνευμένο συμβάν κυβερνοασφάλειας.

Ανάκαμψη (Recover) - Ανάπτυξη και εφαρμογή των κατάλληλων δραστηριοτήτων για τη διατήρηση των σχεδίων για ανθεκτικότητας και για αποκατάσταση τυχόν δυνατοτήτων ή υπηρεσιών που έχουν μειωθεί λόγω ενός συμβάντος κυβερνοασφάλειας. Η λειτουργία αυτή υποστηρίζει την έγκαιρη αποκατάσταση των κανονικών λειτουργιών και την μείωση του αντίκτυπου από ένα συμβάν κυβερνοασφάλειας.

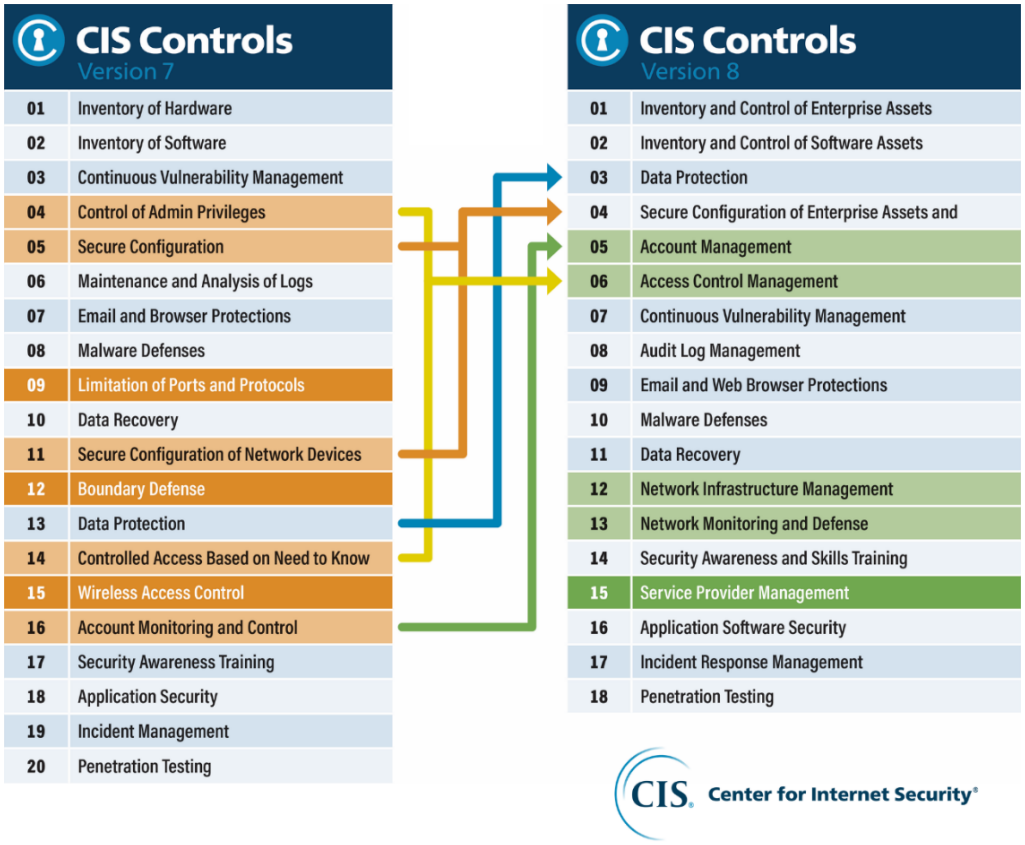
Ενώ, η προσθήκη του **Govern** σύμφωνα με το προσχέδιο καθιερώνει και παρακολουθεί τη στρατηγική διαχείρισης κινδύνων στον κυβερνοχώρο, τις προσδοκίες και την πολιτική του οργανισμού. (NIST_Draft, 2023)

3.4. CIS Controls

Τα Critical Security Controls - CIS Controls (CIS, 2021), είναι ένα συνιστώμενο σύνολο ενεργειών για την άμυνα στον κυβερνοχώρο που παρέχουν συγκεκριμένους και πρακτικούς τρόπους για την αποτροπή των πιο διάχυτων επιθέσεων, με μια σχετικά σύντομη λίστα με υψηλής προτεραιότητας και με εξαιρετικά αποτελεσματικές αμυντικές ενέργειες που παρέχουν ένα σημείο εκκίνησης για κάθε επιχείρηση που επιδιώκει να βελτιώσει την άμυνα στον κυβερνοχώρο. Τα CIS Controls αναπτύχθηκαν ξεκινώντας το 2008 από μια διεθνή κοινοπραξία βάσης που φέρνει σε επαφή εταιρείες, κρατικούς φορείς, ιδρύματα και άτομα από κάθε μέρος του οικοσυστήματος (κυβερνοαναλυτές, ανιχνευτές

ευπάθειας, πάροχοι λύσεων, χρήστες, σύμβουλοι, κατασκευαστές, στελέχη, ακαδημαϊκοί, ελεγκτές, κ.λπ.) οι οποίοι ενώθηκαν για να δημιουργήσουν, να υιοθετήσουν και να υποστηρίξουν τα CIS Controls.

Τα CIS Controls αντιστοιχίζονται στα περισσότερα σημαντικά πλαίσια συμμόρφωσης, όπως το NIST Cybersecurity Framework, NIST 800-53, ISO 27000 και κανονισμούς όπως PCI DSS, HIPAA, NERC CIP και FISMA. Οι έλεγχοι CIS είναι ελεύθεροι να χρησιμοποιηθούν από οποιονδήποτε για να βελτιώσει τη δική του ασφάλεια στον κυβερνοχώρο. Στις 18 Μαΐου 2021, η SANS κυκλοφόρησε την έκδοση 8 με 18 σημεία ελέγχου και παρουσιάστηκαν στο παγκόσμιο συνέδριο RSA 2021. Η Εικόνα 14 παρουσιάζει τις αλλαγές στα σημεία ελέγχου της έκδοσης 7 και 8.



Εικόνα 14: Αλλαγές στο CIS controls Version 8. (SANS-Institute, 2021)

Σύμφωνα με το (CIS, 2021), οι ομάδες υλοποίησης (Implementation Groups - IG) χωρίζονται σε 3 ομάδες. Μια επιχείρηση IG1 είναι μικρού έως μεσαίου μεγέθους με περιορισμένη τεχνογνωσία σε θέματα πληροφορικής και κυβερνοασφάλειας για την προστασία των περιουσιακών στοιχείων και του προσωπικού πληροφορικής. Μια επιχείρηση IG2 απασχολεί άτομα που είναι υπεύθυνα για τη διαχείριση και την προστασία της πληροφοριακής υποδομής. Μια επιχείρηση IG3 απασχολεί εμπειρογνώμονες ασφαλείας που ειδικεύονται στις διάφορες πτυχές της ασφάλειας στον κυβερνοχώρο (π.χ. διαχείριση κινδύνων, δοκιμές διείσδυσης, ασφάλεια εφαρμογών). Οι ανησυχίες αυτών των επιχειρήσεων είναι διαφορετικές, έχουν διαφορετική ανοχή στη διακοπή λειτουργίας, διαφορετικά δεδομένα που πρέπει να προστατεύσουν και έτσι οι διασφαλίσεις επιλέγονται με διαφορετικό τρόπο και βοηθούν στη αντίστοιχη πολυπλοκότητα που έχουν να αντιμετωπίσουν.

Εικόνα 15: Σημείο ελέγχου 3 - Προστασία Δεδομένων με τις διασφαλίσεις ανά IG. (CIS, 2021)

Κάθε έλεγχος (Control) από τα 18 σημεία αποτελείται από διασφαλίσεις (Safeguards). Οι διασφαλίσεις αυτές κατηγοριοποιούνται για την κάθε ομάδα υλοποίησης. Για παράδειγμα, στο 3ο σημείο ελέγχου, το οποίο αφορά την προστασία δεδομένων, όπως φαίνεται και στην Εικόνα 15, οι εταιρείες που ανήκουν στο IG1 έχουν 6 από τις 14 διασφαλίσεις, η εταιρεία στο IG2 έχει 12 από τις 14 διασφαλίσεις ενώ η IG3 όλες. Στην Εικόνα 16 παρουσιάζονται όλες οι διασφαλίσεις και ποιες ανήκουν στην κάθε κατηγορία IG. Επίσης, φαίνεται σε ποιόν τύπο περιουσιακού στοιχείου (asset type) ανήκουν και ποια η λειτουργία ασφάλειας (security function).

NUMBER	TITLE/DESCRIPTION	ASSET TYPE	SECURITY FUNCTION	IG1	IG2	IG3
3.1	**Establish and Maintain a Data Management Process** Establish and maintain a data management process. In the process, address data sensitivity, data owner, handling of data, data retention limits, and disposal requirements, based on sensitivity and retention standards for the enterprise. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	Data	Identify	●	●	●
3.2	**Establish and Maintain a Data Inventory** Establish and maintain a data inventory, based on the enterprise's data management process. Inventory sensitive data, at a minimum. Review and update inventory annually, at a minimum, with a priority on sensitive data.	Data	Identify	●	●	●
3.3	**Configure Data Access Control Lists** Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	Data	Protect	●	●	●
3.4	**Enforce Data Retention** Retain data according to the enterprise's data management process. Data retention must include both minimum and maximum timelines.	Data	Protect	●	●	●
3.5	**Securely Dispose of Data** Securely dispose of data as outlined in the enterprise's data management process. Ensure the disposal process and method are commensurate with the data sensitivity.	Data	Protect	●	●	●
3.6	**Encrypt Data on End-User Devices** Encrypt data on end-user devices containing sensitive data. Example implementations can include: Windows BitLocker®, Apple FileVault®, Linux® dm-crypt.	Devices	Protect	●	●	●
3.7	**Establish and Maintain a Data Classification Scheme** Establish and maintain an overall data classification scheme for the enterprise. Enterprises may use labels, such as "Sensitive," "Confidential," and "Public," and classify their data according to those labels. Review and update the classification scheme annually, or when significant enterprise changes occur that could impact this Safeguard.	Data	Identify		●	●
3.8	**Document Data Flows** Document data flows. Data flow documentation includes service provider data flows and should be based on the enterprise's data management process. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	Data	Identify		●	●
3.9	**Encrypt Data on Removable Media** Encrypt data on removable media.	Data	Protect		●	●
3.10	**Encrypt Sensitive Data in Transit** Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).	Data	Protect		●	●
3.11	**Encrypt Sensitive Data at Rest** Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.	Data	Protect		●	●
3.12	**Segment Data Processing and Storage Based on Sensitivity** Segment data processing and storage based on the sensitivity of the data. Do not process sensitive data on enterprise assets intended for lower sensitivity data.	Network	Protect		●	●
3.13	**Deploy a Data Loss Prevention Solution** Implement an automated tool, such as a host-based Data Loss Prevention (DLP) tool to identify all sensitive data stored, processed, or transmitted through enterprise assets, including those located onsite or at a remote service provider, and update the enterprise's sensitive data inventory.	Data	Protect			●
3.14	**Log Sensitive Data Access** Log sensitive data access, including modification and disposal.	Data	Detect			●

Εικόνα 16: Safeguards – Control 3 Data Protection. (CIS, 2021)

4. Νόμοι, Κανονισμοί & Οδηγίες

4.1. Γενικός Κανονισμός για την Προστασία των Δεδομένων (GDPR)

Ο Κανονισμός 2016/679, Γενικός Κανονισμός για την Προστασία Δεδομένων – ΓΚΠΔ (General Data Protection Regulation – GDPR) (EUR-LEX, 2018) (N.4624/2019, 2023) είναι ο πιο πρόσφατος και ένας από τους πιο αυστηρούς κανονισμούς σχετικά με την προστασία δεδομένων που θεσπίστηκε από την Ευρωπαϊκή Ένωση. Ο GDPR ισχύει σε όλα τα κράτη μέλη της Ευρωπαϊκής Ένωσης, συμπεριλαμβανομένης της Ελλάδας, από τις 25 Μαΐου 2018. Στη χώρα ενσωματώθηκε στην εθνική νομοθεσία με το νόμο 4624/2019, καθώς επίσης και ρύθμισε τη συγκρότηση και λειτουργία της «Αρχής Προστασία Δεδομένων Προσωπικού Χαρακτήρα - ΑΠΔΠΧ». Η ΑΠΔΠΧ έχει την αρμοδιότητα να ελέγχει τη συμμόρφωση των οργανισμών με τον GDPR, να επιβάλλει κυρώσεις σε περίπτωση παραβάσεων και να παρέχει καθοδήγηση και συμβουλές στους ενδιαφερόμενους. Επιπλέον, οι πολίτες έχουν το δικαίωμα να υποβάλλουν καταγγελίες στην ΑΠΔΠΧ σχετικά με παραβάσεις του GDPR από επιχειρήσεις.

Όλες οι επιχειρήσεις και οργανισμοί που επεξεργάζονται προσωπικά δεδομένα πολιτών της ΕΕ πρέπει να συμμορφώνονται με τους κανόνες του GDPR, ανεξαρτήτως της τοποθεσίας τους. Ο νέος αυτός κανονισμός είναι εκτεταμένος, πολύπλοκος και έχει πολλές εφαρμογές προκαλώντας συζητήσεις σε ακαδημαϊκούς κύκλους και δικηγορικά γραφεία. Υποχρέωσε τους οργανισμούς να αλλάξουν όλες τις διαδικασίες με τις οποίες επεξεργάζονται προσωπικά δεδομένα των ευρωπαίων πολιτών. Μία από τις κύριες αλλαγές είναι οι γραπτές συμφωνίες με όλους τους προμηθευτές και συνεργάτες, οι οποίοι μοιράζονται δεδομένα προσωπικού χαρακτήρα. Οι νέες ευθύνες που φέρνει ο ΓΚΠΔ επηρεάζουν τον άνθρωπο, τους πόρους, τα οργανωτικά συστήματα και την κουλτούρα στα διάφορα επιχειρηματικά μοντέλα. (Freitas & Silva, 2022)

Ο GDPR σχεδιάστηκε για να εναρμονίσει τους νόμους περί ιδιωτικότητας και προστασίας του απορρήτου σε ολόκληρη την Ευρώπη προκειμένου να παρέχει μεγαλύτερη προστασία και δυνατότητες στα άτομα για τον έλεγχο των προσωπικών τους δεδομένων ενόψει νέων τεχνολογικών εξελίξεων. Η συμμόρφωση με το GDPR έχει γίνει κορυφαία για οργανισμούς παγκοσμίως. Οι οργανισμοί πρέπει να υιοθετήσουν κατάλληλες πολιτικές και διαδικασίες για την προστασία των προσωπικών δεδομένων που κατέχουν. Οι ομοιότητες μεταξύ του πλαισίου ISO27001 και των απαιτήσεων του GDPR είναι πολλές. Σύμφωνα με (Ayala-Rivera & Pasquale, 2018) παρατηρήθηκε ότι συχνά οι επαγγελματίες της πληροφορικής δεν έχουν καθοδήγηση για να κατανοήσουν ποιες είναι οι απαιτήσεις που πρέπει να τεθούν σε λειτουργία ώστε να εφαρμοστούν σε ένα πληροφοριακό σύστημα ενός οργανισμού για την υποστήριξη της συμμόρφωσης. Αυτό συμβαίνει πιο συχνά στις μικρομεσαίες επιχειρήσεις ή ανεξάρτητους ερευνητές και συμβούλους, οι οποίοι συνήθως δεν διαθέτουν επαρκείς πόρους για να παρέχουν νομική υποστήριξη. (EUR-LEX, 2018)

Σύμφωνα με τους (Lopes, Guarda, & Oliveira, 2019) και (EUR-LEX, 2018), οι κύριες καινοτομίες της Γενικής Προστασίας Δεδομένων είναι οι εξής:

1) Τα νέα δικαιώματα για τους πολίτες: το δικαίωμα στη λήθη και το δικαίωμα στη φορητότητα των δεδομένων ενός χρήστη από ένα ηλεκτρονικό σύστημα σε άλλο.
2) Η δημιουργία της θέσης του Υπεύθυνου Προστασίας Δεδομένων (DPO).
3) Η υποχρέωση διενέργειας ανάλυσης κινδύνου και εκτίμηση επιπτώσεων για τον προσδιορισμό της συμμόρφωσης με τον κανονισμό.
4) Η υποχρέωση του υπευθύνου επεξεργασίας και του εκτελούντος την επεξεργασία δεδομένων να τεκμηριώνουν τις πράξεις επεξεργασίας.
5) Οι νέες κοινοποιήσεις προς την Εποπτική Αρχή σε παραβιάσεις ασφαλείας και προηγούμενη έγκριση για ορισμένα είδη επεξεργασίας.

6) Οι νέες υποχρεώσεις ενημέρωσης του υποκειμένου των δεδομένων και καθορισμός υποχρεώσεων για νέες ειδικές κατηγορίες δεδομένων.
7) Η αύξηση του μεγέθους των κυρώσεων.
8) Η καθιέρωση υποχρεώσεων για νέες ειδικές κατηγορίες δεδομένων.
9) Η διαφάνεια και ελαχιστοποίηση των δεδομένων.

Όπως αναφέρεται και από του (Gobeo, Fowler, & Buchanan, 2020), η κατανόηση της συνολικής χρήσης και του πεδίου εφαρμογής των αρχών και των εργαλείων για την ασφάλεια στον κυβερνοχώρο επιτρέπει μεγαλύτερη αποτελεσματικότητα και πιο αποδοτική διαχείριση των Πληροφοριακών Συστημάτων. Οι βασικοί τομείς που πρέπει να καλυφθούν με την Κυβερνοασφάλεια και τη συμμόρφωση με τον GDPR είναι: αρχές και δικαιώματα στο πλαίσιο του GDPR, ασφάλεια πληροφοριών, προστασία δεδομένων από σχεδιασμό και προεπιλογή, διαδικασίες εφαρμογής, μέθοδοι κρυπτογράφησης, απόκριση και διαχείριση συμβάντων και παραβιάσεις δεδομένων.

Στο σημείο αυτό μπορεί να σημειωθεί ότι σε συνέχεια από τον GDPR, σχεδιάστηκε το ISO/IEC 27701:2019, το οποίο αποτελεί επέκταση των προτύπων ISO 27001 και ISO 27002 με πρόσθετες απαιτήσεις για την ανάπτυξη ενός ολοκληρωμένου ΣΔΑΠ και Προστασίας Προσωπικών Δεδομένων. Το πρότυπο βοηθάει τους οργανισμούς να διαχειρίζονται προσωπικά δεδομένα σύμφωνα με τις προσδοκίες των πελατών και τις κανονιστικές απαιτήσεις.

4.2. Οδηγία NIS

Η Οδηγία (ΕΕ) 2016/1148 (NIS-eur-lex.europa, 2016) σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση , γνωστή και ως Οδηγία για την Ασφάλεια των Δικτύων και των Πληροφοριακών Συστημάτων (NIS Directive), είναι μια νομοθετική πράξη της Ευρωπαϊκής Ένωσης που εγκρίθηκε την 6η Ιουλίου του 2016 και πρέπει να εφαρμοστεί σε όλα τα κράτη μέλη της ΕΕ. Η Οδηγία NIS έχει στόχο να βελτιώσει την ασφάλεια των δικτύων και των πληροφοριακών συστημάτων στην Ευρώπη και να ενισχύσει την αντιμετώπιση των κυβερνοεπιθέσεων και των ανεπιθύμητων συμβάντων. Σύμφωνα με το άρθρο 1 (NIS-eur-lex.europa, 2016), η παρούσα οδηγία θεσπίζει μέτρα για την επίτευξη υψηλού κοινού επιπέδου ασφάλειας συστημάτων δικτύου και πληροφοριών εντός της Ένωσης, με σκοπό την καλύτερη λειτουργία της εσωτερικής αγοράς. Για τον σκοπό αυτό, η οδηγία προβλέπει υποχρεώσεις, θέσπιση εθνικής στρατηγικής, δημιουργεί ομάδα συνεργασίας και δίκτυο ομάδων απόκρισης συμβάντων, θεσπίζει απαιτήσεις ασφαλείας και προβλέπει υποχρεώσεις για τα κράτη μέλη.

Η Οδηγία NIS επιβάλλει τη λήψη μέτρων από τα κράτη μέλη για τη βελτίωση της ασφάλειας των κρίσιμων δικτύων και πληροφοριακών συστημάτων σε επιλεγμένους τομείς. Επιπλέον, περιλαμβάνει απαιτήσεις για τους τομείς της ενέργειας, των μεταφορών, των τραπεζών, των χρηματοπιστωτικών αγορών, τους τομείς υγείας, της προμήθειας και διανομής πόσιμου νερού και της ψηφιακής υποδομής. Επίσης, περιλαμβάνει απαιτήσεις για τη δημιουργία εθνικών στρατηγικών για την ασφάλεια των δικτύων και των πληροφοριακών συστημάτων. Η οδηγία αποσκοπεί στη δημιουργία ενός ενιαίου επιπέδου ασφάλειας στην Ευρωπαϊκή Ένωση, εισάγοντας κατευθυντήριες αρχές για την πρόληψη και αντιμετώπιση κυβερνοαπειλών και καθιστώντας υποχρεωτική την αναφορά κρισιμων συμβάντων ασφαλείας από τους παρόχους υπηρεσιών στα κράτη μέλη.

4.3. Οδηγία NIS2

Η Οδηγία (ΕΕ) 2022/2555 αλλιώς Οδηγία NIS2 (NIS2-Eur-lex.eu, 2022) του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 14ης Δεκεμβρίου 2022 σχετικά με μέτρα για υψηλό κοινό επίπεδο κυβερνοασφάλειας σε ολόκληρη την Ένωση, την τροποποίηση του κανονισμού (ΕΕ) αριθ. 910/2014 και

της οδηγίας (ΕΕ) 2018/1972, και για την κατάργηση της οδηγίας (ΕΕ) 2016/1148, τέθηκε σε ισχύ τον Ιανουάριο του 2023. Ο ENISA (ENISA_NIS, 2023), θεωρεί ότι η NIS2 βελτιώνει την υφιστάμενη κατάσταση της ασφάλειας στον κυβερνοχώρο σε ολόκληρη την ΕΕ με διάφορους τρόπους, όπως με τη δημιουργία της απαραίτητης δομή διαχείρισης κρίσεων στον κυβερνοχώρο (CyCLONe), αυξάνοντας το επίπεδο εναρμόνισης όσον αφορά τις απαιτήσεις ασφάλειας και τις υποχρεώσεις υποβολής εκθέσεων ενθαρρύνοντας τα κράτη μέλη να εισαγάγουν νέους τομείς ενδιαφέροντος, με την εισαγωγή νέων ιδεών και καλύπτοντας μεγαλύτερο μέρος της οικονομίας και της κοινωνίας με τη συμπερίληψη περισσότερων τομέων, πράγμα που σημαίνει ότι περισσότερες οντότητες υποχρεούνται να λάβουν μέτρα για να αυξήσουν το επίπεδο κυβερνοασφάλειας.

Η οδηγία εφαρμόζεται σε δημόσιες ή ιδιωτικές οντότητες των τύπων που αναφέρονται στο Παράρτημα Ι της, δηλαδή τομείς υψηλής κρισιμότητας όπως ενέργεια, μεταφορές, τράπεζες, υποδομές χρηματοπιστωτικών αγορών, υγεία, πόσιμο νερό, λύματα, ψηφιακές υποδομές, διαχείριση υπηρεσιών ΤΠΕ, οντότητες δημόσιας διοίκησης και φορείς που υποστηρίζουν την παροχή διαστημικών υπηρεσιών ή στο παράρτημα ΙΙ της, δηλαδή άλλοι κρίσιμοι τομείς όπως ταχυδρομικές υπηρεσίες και υπηρεσίες ταχυμεταφορών, διαχείριση αποβλήτων, παρασκευή, παραγωγή και διανομή χημικών προϊόντων, παραγωγή, μεταποίηση και διανομή τροφίμων, κατασκευαστικός τομέας, ψηφιακοί πάροχοι και οργανισμοί έρευνας. Οι οντότητες αυτές σύμφωνα με το άρθρο 2 του παραρτήματος της σύστασης 2003/361/ΕΚ χαρακτηρίζονται ως μεσαίες επιχειρήσεις ή υπερβαίνουν τα ανώτατα όρια για τις μεσαίες επιχειρήσεις που αναφέρονται στο εν λόγω άρθρο και οι οποίες παρέχουν τις υπηρεσίες τους ή ασκούν τις δραστηριότητές τους εντός της ΕΕ. (NIS2-Eur-lex.eu, 2022)

Όπως περιγράφει το άρθρο 21, τα μέτρα διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας, βασίζονται στην προσέγγιση του κινδύνου, που αποσκοπεί στην προστασία των συστημάτων δικτύου και πληροφοριών και του φυσικού περιβάλλοντος των εν λόγω συστημάτων από περιστατικά. Αυτά τα μέτρα, περιλαμβάνουν πολιτικές για την ανάλυση κινδύνου και την ασφάλεια των πληροφοριακών συστημάτων, τον χειρισμό των περιστατικών, την επιχειρησιακή συνέχεια, την ασφάλεια της αλυσίδας εφοδιασμού, την ασφάλεια στην απόκτηση, την ανάπτυξη και συντήρηση συστημάτων δικτύου και πληροφοριών, συμπεριλαμβανομένου του χειρισμού και της γνωστοποίησης ευπαθειών, καθώς επίσης και τις πολιτικές και τις διαδικασίες για την αξιολόγηση της αποτελεσματικότητας των μέτρων διαχείρισης κινδύνων. Επίσης, τις βασικές πρακτικές και την κατάρτιση στην κυβερνοασφάλεια, τις πολιτικές και τις διαδικασίες σχετικά με τη χρήση κρυπτογραφίας, την ασφάλεια των ανθρώπινων πόρων, την χρήση λύσεων πολυπαραγοντικής επαλήθευσης ταυτότητας και άλλα. (NIS2-Eur-lex.eu, 2022)

Επιπλέον, το άρθρο 23 (NIS2-Eur-lex.eu, 2022), θέτει υποχρεώσεις αναφοράς περιστατικών. Σύμφωνα με την παράγραφο 3, Ένα περιστατικό θεωρείται σημαντικό εάν:

α) έχει προκαλέσει ή μπορεί να προκαλέσει σοβαρή λειτουργική διατάραξη των υπηρεσιών ή οικονομική ζημία για την οικεία οντότητα,
β) έχει επηρεάσει ή μπορεί να επηρεάσει άλλα φυσικά ή νομικά πρόσωπα προκαλώντας σημαντική υλική ή μη υλική ζημία.

Εκτός από τους τομείς που είχαν συμπεριληφθεί στην οδηγία NIS, η οδηγία NIS2 επεκτείνεται σε περισσότερους δημόσιους και ιδιωτικούς τομείς με αυστηρότερες απαιτήσεις. Σύμφωνα με το άρθρο 41, έως τις 17 Οκτωβρίου 2024, τα κράτη μέλη θεσπίζουν και δημοσιεύουν τα μέτρα που απαιτούνται προκειμένου να συμμορφωθούν προς την παρούσα οδηγία.

4.4. Εθνικό σχέδιο δράσης για την κυβερνοασφάλεια

Η Οδηγία NIS έχει εφαρμογή σε όλα τα κράτη μέλη της ΕΕ, συμπεριλαμβανομένης της Ελλάδας. Η Ελλάδα εφάρμοσε την Οδηγία με τον Νόμο 4577/2018 και ενσωματώνει στην ελληνική νομοθεσία

της Οδηγίας 2016/1148/ΕΕ. Η χώρα μας, αναγνωρίζοντας τη σημασία της θωράκισης της ασφάλειας των συστημάτων και των δικτύων πληροφορικής και επικοινωνιών, έχει λάβει ήδη μια σειρά από σημαντικές πρωτοβουλίες με γνώμονα την ανταπόκριση στις απαιτήσεις της ΕΕ. Η Εθνική Αρχή Κυβερνοασφάλειας του Υπουργείου Ψηφιακής Διακυβέρνησης επικαιροποίησε τον εθνικό στρατηγικό σχεδιασμό για την κυβερνοασφάλεια με την διαμόρφωση ενός κατάλληλου στρατηγικού πλαισίου και δημοσίευσε την «Εθνική Στρατηγική Κυβερνοασφάλειας 2020-2025».

Η Ελλάδα, σύμφωνα με (ΥΨΔ_ΕΑΚ, 2020) υιοθετεί τα ευρωπαϊκά πρότυπα και μεθοδολογίες για την κατάρτιση του στρατηγικού σχεδιασμού. Συγκεκριμένα, αξιοποιήθηκε το εργαλείο αξιολόγησης «national cybersecurity strategies evaluation tool» το οποίο έχει αναπτυχθεί από τον ENISA και συμπεριλαμβάνει συνολικά 15 στόχους. Από την ανάλυση των κενών (Gap Analysis) που πραγματοποίησε η Εθνική Αρχή Κυβερνοασφάλειας, οι τομείς στρατηγικού ενδιαφέροντος εκτείνονται σε 6 διαστάσεις. Συγκεκριμένα:

- Σχεδιασμός έκτακτης ανάγκης
- Αναφορές περιστατικών
- Ασφάλεια και προστασία της ιδιωτικότητας
- Έρευνα και ανάπτυξη
- Συμπράξεις δημοσίου και ιδιωτικού τομέα
- Επενδύσεις στα μέτρα ασφάλειας

Στην (ΥΨΔ_ΕΑΚ, 2020) υπάρχουν 5 στρατηγικοί στόχοι ανάπτυξης του στρατηγικού σχεδιασμού και για τον κάθε έναν αναπτύσσονται ειδικοί στόχοι. Οι ειδικοί στόχοι εξειδικεύονται σε δραστηριότητες, οι οποίες καλύπτουν όλο το φάσμα της αναγνώρισης, πρόληψης και προστασίας, αποτροπής και ανάκαμψης από κυβερνοεπιθέσεις.

Εικόνα 17: Οι 5 στρατηγικοί στόχοι ανάπτυξης του στρατηγικού σχεδίου. (ΥΨΔ_ΕΑΚ, 2020)

Κάποιες εμβληματικές δραστηριότητες με βάση τους στόχους είναι ο στόχος βελτιστοποίησης μεθόδων, τεχνικών και εργαλείων ανάλυσης, η απόκριση και κοινοποίηση συμβάντων με δραστηριότητες δημιουργία κέντρου παρακολούθησης κρίσιμων υποδομών (SOC), η δημιουργία Cyber hotline και άλλα (Εικόνα 18).

Στόχοι	Δραστηριότητες	Ορόσημα
3.Α. Βελτιστοποίηση μεθόδων, τεχνικών και εργαλείων ανάλυσης, απόκρισης και κοινοποίησης συμβάντων	**3.Α.1.** Δημιουργία Κέντρου Παρακολούθησης Κρίσιμων Υποδομών Security Operations Center - SOC	Q4 2022 - Συνεχής δραστηριότητα
	3.Α.2. Δημιουργία Cyber hotline	Q2 2023 - Συνεχής δραστηριότητα
	3.Α.3. Ορισμός πλαισίου διαχείρισης συμβάντων ασφάλειας	Q2 2022
	3.Α.4. Κατάρτιση και διαχείριση μητρώου συμβάντων (επίσημα ή/και ανώνυμα), συμπεριλαμβανομένων όλων των πληροφοριών που αφορούσαν το συμβάν, ενέργειες που έλαβαν χώρα, αποτελέσματα, lessons learned.	Q4 2023 - Συνεχής δραστηριότητα
	3.Α.5. Λειτουργία συστήματος προστασίας κυβερνητικών ιστοτόπων	Q4 2021 - Συνεχής δραστηριότητα
	3.Α.6. Πρόγραμμα παρακολούθησης και αξιολόγησης επιπέδου ασφάλειας ελληνικού κυβερνοχώρου (threat intelligence tool)	Q1 2022 - Συνεχής δραστηριότητα
	3.Α.7. Εγκατάσταση και παραμετροποίηση open source εργαλείου συστήματος αυτόματης ειδοποίησης για την διαθεσιμότητα των ιστοτόπων και των δικτυακών συσκευών	Q4 2022 - Συνεχής δραστηριότητα
	3.Α.8. Εγκατάσταση open source πλατφόρμας για vulnerability assessment και διενέργεια ελέγχων Τρωτότητας (Penetration tests)	Q4 2022 - Συνεχής δραστηριότητα
	3.Α.9. Εγκατάσταση και παραμετροποίηση εργαλείου log file & malware analysis	Q4 2022 - Συνεχής δραστηριότητα
	3.Α.10. Εγκατάσταση και παραμετροποίηση open source εργαλείου για ανταλλαγή δεικτών IOCs με άλλους οργανισμούς κυβερνοασφάλειας (Εθνικό CERT, CERT/ΔΙΚΥΒ, CERT ΕΔΗΤΕ, FORTHcert)	Q4 2023 - Συνεχής δραστηριότητα
	3.Α.11. Συγκρότηση κεντρικού συντονιστικού μηχανισμού για τη διαχείριση αναφορών στο πλαίσιο του GDPR, NISD, art. 13a, eIDAS	Q2 2023 - Συνεχής δραστηριότητα
	3.Α.12. Εκπόνηση ετήσιων δελτίων και landscape reports για περιστατικά κυβερνοεπιθέσεων	Q4 2024 - Συνεχής δραστηριότητα
	3.Α.13. Λειτουργία εργαστηρίου για ανάλυση log files και κυβερνοπεριστατικών	Q4 2024 - Συνεχής δραστηριότητα

Εικόνα 18: Στόχοι 3.Α – δραστηριότητες / Εθνικό σχέδιο δράσης για την κυβερνοασφάλεια (ΥΨΔ_ΕΑΚ, 2020).

5. Πλαίσιο STAM - Security Technology and Management

5.1. Βέλτιστες πρακτικές κυβερνοασφάλειας

Η ανάγκη για τον καθορισμό βέλτιστων πρακτικών κυβερνοασφάλειας που μπορούν να ακολουθήσουν οι ΜμΕ για να διαχειριστούν τον κίνδυνο ασφάλειας στον κυβερνοχώρο έχει μεγαλώσει. Η δημιουργία μιας κοινή γλώσσα και η βελτίωσης της αποτελεσματικότητας είναι απαραίτητες όσο ποτέ. Όπως επισημάνθηκε και από άλλους ερευνητές στις προηγούμενες ενότητες, οι ΜμΕ θα πρέπει να δημιουργήσουν πολιτικές ασφαλείας, δηλαδή ένα σύνολο κανόνων που βοηθούν στον καθορισμό ενός αποδεκτού επιπέδου ασφάλειας.

Οι διάφοροι οργανισμοί έχουν διαφορετικές απαιτήσεις ασφαλείας, επομένως πρέπει να καθορίζονται διαφορετικές πολιτικές ασφαλείας για αυτούς. Οι πολιτικές ασφαλείας των οργανισμών πρέπει να περιλαμβάνουν ένα σύνολο λειτουργιών και κατευθύνσεων, οι οποίες θα παρέχουν το ζητούμενο επίπεδο ασφάλειας. Οι πολιτικές αυτές είναι απαραίτητο να περιλαμβάνουν ζητήματα όπως για παράδειγμα τη διαχείριση των λογαριασμών των χρηστών, το πώς να αντιμετωπίσουμε την απώλεια ενός κωδικού πρόσβασης, καθώς και τον τρόπο αλλαγής του, τον τρόπο δημιουργίας αντιγράφων ασφαλείας, την ασφαλή παραμετροποίηση των συσκευών, τους τρόπους προστασίας από το κακόβουλο λογισμικό, τον έλεγχο των διαδικασιών, την εκπαίδευση και κατάρτιση των υπαλλήλων και άλλα.

Ο σκοπός της πολιτικής ασφαλείας είναι η διαφύλαξη των περιουσιακών στοιχείων και των βασικών αρχών της ασφάλειας. Στην ουσία, μια πολιτική ασφαλείας αποτελεί ένα έγγραφο στο οποίο περιγράφονται οι στόχοι της ασφάλειας και οι αντίστοιχες διαδικασίες που πρέπει να ακολουθούνται για να επιτευχθούν αυτοί. Η πολιτική καθορίζεται από την Διοίκηση και υποστηρίζεται από τον Υπεύθυνο Ασφαλείας, ενώ πρέπει να κάνει σαφές τα όρια της εφαρμογής της ,δηλαδή τον τόπο εφαρμογής και τα χρονικά πλαίσια.

Οι πολιτικές ασφαλείας λειτουργούν σε συνδυασμό με ένα σύνολο οργανωτικών, φυσικών και τεχνικών μέτρων ασφαλείας. Τα οργανωτικά μέτρα ασφάλειας αναφέρονται στους ρόλους και τις εξουσιοδοτήσεις, την διαχείριση των πληροφοριακών αγαθών, την εκπαίδευση, τον έλεγχο, την επιθεώρηση και άλλα. Τα φυσικά μέτρα ασφάλειας περιλαμβάνουν την ελεγχόμενη πρόσβαση, το προσωπικό ασφαλείας, την περιβαλλοντική προστασία, την φύλαξη αρχείων και εγγράφων και άλλα. Ενώ τα τεχνικά μέτρα ασφάλειας αποτελούν τα μέσα αποθήκευσης, η ασφάλεια του δικτύου και των συστημάτων (firewall, antivirus), η συντήρηση του εξοπλισμού, τα αντίγραφα ασφαλείας (backup systems) και άλλα.

Σε συνέχεια της εκτεταμένης έρευνας που προηγήθηκε στα διάφορα σχετικά πεδία, όπως αναφέρθηκαν και στις προηγούμενες ενότητες, αναπτύχθηκε το Πλαίσιο με ονομασία STAM (Security Technology and Management). Το προτεινόμενο πλαίσιο STAM, περιλαμβάνει 20 θεματικές ενότητες, δηλαδή, 20 σημεία ελέγχου. Οι ενότητες αυτές έχουν επιλεγεί με βάση τα παγκόσμια πλαίσια και την προσαρμογή τους στην Εθνική Στρατηγική Κυβερνοασφάλειας. Συγκεκριμένα, το πλαίσιο αποτελείται από τις εξής ενότητες:

1) Διοίκηση και διαχείριση κυβερνοασφάλειας
2) Καταγραφή και έλεγχος περιουσιακών στοιχείων
3) Καταγραφή και έλεγχος λογισμικού
4) Ασφαλής διαμόρφωση υλικού και λογισμικού
5) Προστασία Δεδομένων
6) Διαχείριση λογαριασμών
7) Διαχείριση ελέγχου πρόσβασης
8) Διαχείριση αρχείων καταγραφής

9) Διαχείριση παρόχων υπηρεσιών
10) Διαχείριση διαδικτυακής υποδομής
11) Προστασία ηλεκτρονικού ταχυδρομείου και προγραμμάτων περιήγησης
12) Προστασία από κακόβουλο λογισμικό
13) Ασφάλεια εφαρμογών λογισμικού
14) Παρακολούθηση και άμυνα του δικτύου
15) Εκπαίδευση και ενημέρωση για την ασφάλεια
16) Ανάκτηση δεδομένων
17) Διαχείριση αντιμετώπισης περιστατικών
18) Δοκιμές διείσδυσης
19) Συνεχής διαχείριση ευπαθειών
20) Φυσική ασφάλεια

Το κάθε ένα από τα σημεία ελέγχου περιλαμβάνει διασφαλίσεις. Τα σημεία ελέγχου περιλαμβάνουν συνολικά 148 διασφαλίσεις. Οι διασφαλίσεις αυτές έχουν στηριχθεί στα παγκόσμια πλαίσια και στις βέλτιστες πρακτικές για την κυβερνοασφάλεια, προσαρμοσμένες σε μικρομεσαίους οργανισμούς και επιχειρήσεις (ΜμΕ) και σύμφωνα με την Εθνική Στρατηγική Κυβερνοασφάλειας 2020-2025 και το Εθνικό Σχέδιο Δράσης για την κυβερνοασφάλεια. Επιπλέον, το πλαίσιο εναρμονίζεται με τις Οδηγίες της Ε.Ε. σχετικά με τα μέτρα για υψηλό κοινό επίπεδο κυβερνοασφάλειας σε ολόκληρη την Ένωση, Οδηγία (ΕΕ) 2016/1148 (Οδηγία NIS) και Οδηγία (ΕΕ) 2022/2555 (Οδηγία NIS2).

Τα σημεία ελέγχου και οι διασφαλίσεις έχουν επιλεγεί για ΜμΕ μικρού έως μεσαίου μεγέθους, με περιορισμένη τεχνογνωσία σε θέματα κυβερνοασφάλειας αλλά έχουν τη δυνατότητα να απασχολούν τουλάχιστον έναν (1) άνθρωπο ο οποίος ασχολείται υπεύθυνα με την διαχείριση και την προστασία της πληροφοριακής υποδομής. Στις ενότητες που ακολουθούν παρουσιάζονται τα σημεία ελέγχου, οι διασφαλίσεις για το κάθε σημείο ελέγχου και τα ερωτήματα που προκύπτουν σε κάθε σημείο ελέγχου ώστε να χρησιμοποιηθούν στην συνέχεια στη σχεδίαση του εργαλείου αξιολόγησης.

5.2. Διοίκηση και διαχείριση κυβερνοασφάλειας

Η διοίκησης και διαχείρισης της κυβερνοασφάλειας, αντιπροσωπεύει τη στάση του οργανισμούς όπου συγκλίνουν η στρατηγική για την κυβερνοασφάλειας και η τεχνογνωσία σχετικά με την προστασία του πληροφοριακού συστήματος του οργανισμού. Η ανάλυση των απειλών και η υιοθέτηση τεχνολογικών και πολιτικών μέτρων, ώστε να εξασφαλίζει την απρόσκοπτη λειτουργικά του πληροφοριακού συστήματος και την προστασία των δεδομένων, είναι ζωτικής σημασίας. Η πολιτική της Διοίκησης μέσα από συντονισμένες ενέργειες, αναλαμβάνει να αναπτύξει και να εφαρμόσει πολυεπίπεδες στρατηγικές για την κυβερνοασφάλειας. Η διαχείριση της κυβερνοασφάλειας πρέπει να αποτελείται από ξεκάθαρους ρόλους και ευθύνες στο σύνολο του προσωπικού όπως IT, CISO, DPO κλπ, καθώς επίσης και από τους απαραίτητους υλικοτεχνικούς, οικονομικούς και ανθρώπινους πόρους για την άσκηση των καθηκόντων. Ο προϋπολογισμός που αφορά την υλοποίηση των έργων κυβερνοασφάλειας είναι εξίσου σημαντικός.

Η διοίκηση και η διαχείριση της κυβερνοασφάλειας περιλαμβάνει έξι (6) διασφαλίσεις:

1) Καταγεγραμμένη πολιτική ασφαλείας.
2) Πολιτική ασφαλείας με έγκριση από την Διοίκηση.
3) Πολιτική ασφαλείας με επιμέρους πολιτικές και διαδικασίες σε εξειδικευμένα πεδία.
4) Ξεκάθαροι ρόλοι και ευθύνες όσον αφορά την κυβερνοασφάλεια για το σύνολο του προσωπικού, καθώς επίσης έλεγχος και αναθεώρηση τους σε ετήσια βάση.
5) Ετήσιος προϋπολογισμός για την διαχείριση και υλοποίηση έργων κυβερνοασφάλειας.

6) Αποτίμηση επικινδυνότητας (risk assessment) για την ασφάλεια του πληροφοριακού συστήματος.

Το πλαίσιο, στο σημείο ελέγχου διοίκησης και διαχείρισης της κυβερνοασφάλειας, θέτει δώδεκα (12) ερωτήματα:

1) Ο οργανισμός, διαθέτει καταγεγραμμένη πολιτική ασφάλειας, επικεντρωμένη στην ασφάλεια του πληροφοριακού συστήματος και την κυβερνοασφάλεια, εγκεκριμένη από την Διοίκηση;
2) Ο οργανισμός, διαθέτει επιμέρους πολιτικές ασφαλείας, διαδικασίες, κανόνες και οδηγίες για συγκεκριμένα πεδία, στις οποίες περιγράφει τον τρόπο εφαρμογής των τεχνικών και οργανωτικών μέτρων προστασίας;
3) Ο οργανισμός, επανεξετάζει και αναθεωρεί την πολιτική ασφαλείας και τις επιμέρους πολιτικές και διαδικασίες, τουλάχιστον σε ετήσια βάση ή όταν συμβούν σημαντικές αλλαγές τεχνικές, νομοθετικές και κανονιστικές στο επιχειρησιακό περιβάλλον του;
4) Ο οργανισμός, διενεργεί αποτίμηση επικινδυνότητας (Risk Assessment) με διεθνώς αποδεκτές μεθοδολογίες, με την οποία εντοπίζονται, αναλύονται, αξιολογούνται και διαχειρίζονται οι κίνδυνοι που σχετίζονται με την κυβερνοασφάλεια;
5) Ο οργανισμός, διαθέτει τμήμα αρμόδιο για την ασφάλεια του πληροφοριακού συστήματος;
6) Ο οργανισμός, έχει ορίσει στέλεχος υπεύθυνο ασφαλείας του πληροφοριακού συστήματος (Chief Information Security Officer – CISO), με αρμοδιότητες την διαχείριση της ασφάλειας του πληροφοριακού συστήματος;
7) Ο οργανισμός, παρέχει στον CISO τους απαραίτητους οικονομικούς, υλικοτεχνικούς και ανθρώπινους πόρους για την άσκηση των καθηκόντων του;
8) Ο οργανισμός, έχει ορίσει στέλεχος υπεύθυνο προστασίας δεδομένων (Data Protection Officer – DPO), με αρμοδιότητες τη συμμόρφωση του οργανισμού με τον GDPR και τις υποχρεώσεις του σχετικά με την προστασία των προσωπικών δεδομένων, της ιδιωτικότητας και του απορρήτου;
9) Ο οργανισμός, έχει ορίσει ξεκάθαρους ρόλους και ευθύνες σε ότι αφορά την κυβερνοασφάλεια για το σύνολο του προσωπικού και τους συνεργάτες; Για την διασφάλιση της καταλληλόλητας οι ρόλοι επανεξετάζονται και αναθεωρούνται τουλάχιστον ετησίως;
10) Ο οργανισμός, δεσμεύει ποσό κατά τον ετήσιο προϋπολογισμό του, για την διαχείριση και υλοποίηση των έργων σχετικά με την ασφάλεια του πληροφοριακού συστήματος και την κυβερνοασφάλεια;
11) Ο οργανισμός, έχει πιστοποιηθεί ότι υλοποιεί ένα ολοκληρωμένο Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών (Information Security Management System – ISMS), όπως ISO 27001 ή άλλο διεθνώς αποδεκτό;
12) Ο οργανισμός, διαθέτει καταγεγραμμένη πολιτική για την διασφάλιση της επιχειρηματικής συνέχειας και έχει αναπτύξει σχέδιο αποκατάστασης από καταστροφή (Disaster Recovery Plan), με σκοπό την άμεση αποκατάσταση από ανεπιθύμητο συμβάν;

5.3. Καταγραφή και έλεγχος περιουσιακών στοιχείων

Αυτό το σημείο ελέγχου, περιλαμβάνει την ενεργή διαχείριση των επιχειρησιακών περιουσιακών στοιχείων (Enterprise Assets), δηλαδή τις συσκευές των τελικών χρηστών, συμπεριλαμβανομένων των φορητών και κινητών συσκευών, τις συσκευές δικτύου, τις συσκευές IoT, τους διακομιστές και τις περιφερειακές συσκευές που συνδέονται φυσικά, καθώς και τα εικονικά και απομακρυσμένα περιβάλλοντα και τα περιβάλλοντα cloud. Η διαχείριση, αφορά και τα πρόσθετα περιουσιακά στοιχεία που συνδέονται στο δίκτυο και μπορεί να είναι προσωρινά, δοκιμαστικά, συσκευές επισκεπτών και άλλα. Η διατήρηση μιας τρέχουσας και ακριβούς εικόνας των περιουσιακών στοιχείων του οργανισμού, είναι μια συνεχής και δυναμική διαδικασία. Ο οργανισμός, μπορεί να σαρώνει ενεργά σε τακτική βάση, για τον εντοπισμό περιουσιακών στοιχείων που συνδέονται με το δίκτυο του.

Η καταγραφή και ο έλεγχος των περιουσιακών στοιχείων περιλαμβάνει τέσσερις (4) διασφαλίσεις:

1) Διατήρηση λεπτομερούς απογραφής των περιουσιακών στοιχείων του οργανισμού.
2) Αντιμετώπιση μη εξουσιοδοτημένων περιουσιακών στοιχείων.
3) Χρήση ενός εργαλείου εντοπισμού περιουσιακών στοιχείων που είναι συνδεμένα στο δίκτυο, με εβδομαδιαία σάρωση.
4) Χρήση καταγραφής DHCP (Dynamic Host Configuration Protocol) με ενημέρωση και επανεξέταση εβδομαδιαίως.

Το πλαίσιο, στο σημείο ελέγχου καταγραφής και ελέγχου των περιουσιακών στοιχείων, θέτει επτά (7) ερωτήματα:

1) Ο οργανισμός, διαθέτει καταγεγραμμένη πολιτική και διαδικασίες που αφορούν την καταγραφή και τον έλεγχο των πληροφοριακών περιουσιακών στοιχείων;
2) Ο οργανισμός, διαθέτει καταγεγραμμένη πολιτική και διαδικασίες που αφορούν την ορθή χρήση των πληροφοριακών στοιχείων (υπολογιστές, εκτυπωτές, φορητοί υπολογιστές, κινητά τηλέφωνα, φορητά μέσα αποθήκευσης και άλλα);
3) Ο οργανισμός, διατηρεί επικαιροποιημένο και λεπτομερή κατάλογο (Asset Inventory) με τα υλικά αγαθά πληροφορικής;
4) Ο οργανισμός, έχει ορίσει έναν ιδιοκτήτη (owner) σε κάθε αγαθό πληροφορικής;
5) Ο οργανισμός, τηρεί ειδική πολιτική για την απόσυρση των πληροφοριακών αγαθών σχετικά με την ασφάλεια των δεδομένων;
6) Ο οργανισμός, διασφαλίζει ότι άλλες συσκευές όπως smartphones και laptops υπαλλήλων δεν έχουν δυνατότητα πρόσβασης σε κρίσιμα ή ευαίσθητα συστήματα;
7) Ο οργανισμός, χρησιμοποιεί εβδομαδιαίως, εργαλείο που προγραμματισμένα σαρώνει το δίκτυο του και εντοπίζει όλες τις συνδεμένες σε αυτό συσκευές, για τον εντοπισμό των μη εξουσιοδοτημένων συσκευών;

5.4. Καταγραφή και έλεγχος λογισμικού

Αυτό το σημείο ελέγχου, περιλαμβάνει την ενεργή διαχείριση όλου του λογισμικού του οργανισμού, έτσι ώστε να εγκαθίσταται και να εκτελείται μόνο εξουσιοδοτημένο λογισμικό. Το μη εξουσιοδοτημένο και μη διαχειριζόμενο λογισμικό, εντοπίζεται και αποτρέπεται από την εγκατάσταση ή την εκτέλεση. Ο οργανισμός, θα πρέπει να επανεξετάσει την απογραφή λογισμικού του, ώστε να εντοπίσει τυχόν περιουσιακά στοιχεία που εκτελούν λογισμικό το οποίο δεν είναι απαραίτητο για τους σκοπούς του. Είναι ζωτικής σημασίας, η απογραφή, η κατανόηση, η αξιολόγηση και η διαχείριση όλου του λογισμικού που συνδέεται με την υποδομή του οργανισμού.

Η καταγραφή και ο έλεγχος του λογισμικού περιλαμβάνει έξι (6) διασφαλίσεις:

1) Απογραφή και διατήρηση λεπτομερούς καταλόγου όλων των αδειοδοτημένων λογισμικών που είναι εγκατεστημένα στα περιουσιακά στοιχεία του οργανισμού.
2) Το εξουσιοδοτημένο λογισμικό υποστηρίζεται από τον κατασκευαστή του. Για λογισμικά που έχουν σταματήσει να υποστηρίζονται από τον κατασκευαστή τους πρέπει να διενεργείται ανάλυση κινδύνων και να δημιουργείται τεκμηριωμένη εξαίρεση με την αποδοχή των κινδύνων.
3) Αντιμετώπιση μη εξουσιοδοτημένου λογισμικού και διασφάλιση ότι το μη εξουσιοδοτημένο λογισμικό είτε αφαιρείται είτε λαμβάνει τεκμηριωμένη εξαίρεση. Μηνιαία επανεξέταση.
4) Χρήση αυτοματοποιημένων εργαλείων καταγραφής λογισμικού.
5) Εξουσιοδοτημένο λογισμικό “Allowlist” και εξαμηνιαία επανεξέταση.
6) Εξουσιοδοτημένες βιβλιοθήκες ”Allowlist” για την φόρτωση διεργασιών συστήματος. Αποκλεισμός των μη εξουσιοδοτημένων και εξαμηνιαία επαναξιολόγηση της λίστας.

Το πλαίσιο, στο σημείο ελέγχου καταγραφής και ελέγχου του λογισμικού, θέτει έξι (6) ερωτήματα:

1) Ο οργανισμός, διαθέτει καταγεγραμμένη πολιτική και διαδικασίες, οι οποίες αφορούν την καταγραφή και τον έλεγχο του λογισμικού που είναι εγκατεστημένο στα περιουσιακά του στοιχεία;
2) Ο οργανισμός, διαθέτει καταγεγραμμένη πολιτική και διαδικασίες, οι οποίες αφορούν την ορθή χρήση του λογισμικού;
3) Ο οργανισμός, διατηρεί επικαιροποιημένο και λεπτομερή κατάλογο (Software Inventory) με τα αδειοδοτημένα λογισμικά του;
4) Ο οργανισμός, χρησιμοποιεί αυτοματοποιημένο εργαλείο καταγραφής λογισμικού;
5) Ο οργανισμός, διασφαλίζει ότι οι συσκευές του έχουν εγκατεστημένο μόνο εξουσιοδοτημένο αδειοδοτημένο λογισμικό;
6) Ο οργανισμός, χρησιμοποιεί εβδομαδιαίως, εργαλείο που προγραμματισμένα σαρώνει τις συσκευές του και εντοπίζει το λογισμικό που είναι εγκατεστημένο σε αυτές;

5.5. Ασφαλής διαμόρφωση υλικού και λογισμικού

Η ασφαλής διαμόρφωση των επιχειρησιακών περιουσιακών στοιχείων (Enterprise Assets) είναι ζωτικής σημασίας. Αναγνωρίζονται και ταξινομούνται τα στοιχεία βάσει της ευαισθησίας τους και εφαρμόζονται ισχυρά μέτρα πρόληψης. Το σημείο ελέγχου της καθιέρωσης και διατήρησης της ασφαλούς διαμόρφωσης των επιχειρησιακών περιουσιακών στοιχείων, περιλαμβάνει τις συσκευές των τελικών χρηστών, συμπεριλαμβανομένων των φορητών και των κινητών συσκευών, τις δικτυακές συσκευές, τους διακομιστές, τις συσκευές IoT και του λογισμικού (λειτουργικά συστήματα και εφαρμογές). Οι ανοικτές υπηρεσίες και θύρες, οι προεπιλεγμένοι λογαριασμοί ή κωδικοί πρόσβασης, οι προκαθορισμένες ρυθμίσεις του συστήματος ονομάτων τομέα (DNS) και η προεγκατάσταση περιττού λογισμικού μπορούν να γίνουν αντικείμενο εκμετάλλευσης εάν αφεθούν στην προεπιλεγμένη κατάστασή τους. Οι ρυθμίσεις ασφαλείας, πρέπει να διαχειρίζονται και να συντηρούνται κατά τη διάρκεια του κύκλου ζωής των επιχειρησιακών περιουσιακών στοιχείων και του λογισμικού και να ενημερώνονται. Το ίδιο ισχύει για τις απομακρυσμένες συσκευές και τα περιβάλλοντα cloud. Η παρουσία προεπιλεγμένων λογαριασμών ή κωδικών πρόσβασης, υπερβολικής πρόσβασης ή περιττών υπηρεσιών, είναι συνηθισμένες στις προεπιλεγμένες διαμορφώσεις και αποτελούν αδυναμία. Η διαμόρφωση πρέπει να ακολουθεί τα πρότυπα, ενώ οι αποκλίσεις από αυτά πρέπει να τεκμηριώνονται.

Η ασφαλής διαμόρφωση υλικού και λογισμικού περιλαμβάνει δέκα (10) διασφαλίσεις:

1) Καθιέρωση και διατήρηση ασφαλούς διαμόρφωσης του υλικού και λογισμικού, με ετήσια επανεξέταση.
2) Καθιέρωση και διατήρηση ασφαλούς διαμόρφωσης και παραμετροποίησης των δικτυακών συσκευών, με ετήσια επανεξέταση.
3) Εφαρμογή και διαχείριση τείχους προστασίας, σε διακομιστές και συσκευές τελικού χρήστη.
4) Ασφαλής διαχείριση υλικού και λογισμικού, μέσω ελεγχόμενης υποδομής και ασφαλών πρωτοκόλλων.
5) Διαχείριση προεπιλεγμένων λογαριασμών, σε υλικό και λογισμικό, όπως root, administrator και άλλοι προκαθορισμένοι λογαριασμοί.
6) Απενεργοποίηση περιττών υπηρεσιών σε υλικό και λογισμικό.
7) Διαμόρφωση αξιόπιστων DNS servers στο υλικό του οργανισμού.
8) Ρύθμιση του αυτόματου κλειδώματος του υλικού (υπολογιστές, φορητοί υπολογιστές κλπ) μετά από μια καθορισμένη περίοδο αδράνειας. Η περίοδος δεν πρέπει να υπερβαίνει τα 15 λεπτά.
9) Επιβολή αυτόματου κλειδώματος συσκευής, μετά από ένα προκαθορισμένο όριο τοπικών αποτυχημένων προσπαθειών ελέγχου ταυτότητας, σε φορητές συσκευές τελικών χρηστών.

10) Δυνατότητα απομακρυσμένης διαγραφής των φορητών συσκευών, όταν κρίνεται σκόπιμο, όπως για παράδειγμα κλεμμένες ή χαμένες.

Το πλαίσιο, στο σημείο ελέγχου ασφαλής διαμόρφωσης υλικού και λογισμικού, θέτει δεκαεννέα (19) ερωτήματα:

1) Ο οργανισμός, διαθέτει καταγεγραμμένη πολιτική για την ασφαλή διαμόρφωση του εξοπλισμού και του λογισμικού;
2) Ο οργανισμός, εφαρμόζει διαδικασία ασφαλούς παραμετροποίησης, με βάση τα διεθνώς αποδεκτά πρότυπα, στις δικτυακές συσκευές, στους διακομιστές και στους σταθμούς εργασίας; Η διαδικασία, είναι προσαρμοσμένη στην πολιτική ασφαλείας του οργανισμού και επανεξετάζεται σε τακτά χρονικά διαστήματα;
3) Ο οργανισμός, χρησιμοποιεί μόνο υποστηριζόμενες εκδόσεις λειτουργικών συστημάτων, για τους διακομιστές, τους σταθμούς εργασία και τις δικτυακές συσκευές;
4) Ο οργανισμός, εφαρμόζει τουλάχιστον μηνιαίως, αυτοματοποιημένες διαδικασίες για την λήψη και εγκατάσταση ενημερώσεων ασφαλείας, στις δικτυακές συσκευές, στους διακομιστές και στους σταθμούς εργασίας;
5) Ο οργανισμός, διασφαλίζει κατά την πρώτη εγκατάσταση του λογισμικού και του εξοπλισμού, ότι όλα τα προεπιλεγμένα συνθηματικά τροποποιούνται;
6) Ο οργανισμός, διασφαλίσει ότι στα κρίσιμα συστήματα δεν είναι εφικτή η σύνδεση φορητών μέσων αποθήκευσης (USB flash memory, εξωτερικοί δίσκοι);
7) Ο οργανισμός, εφαρμόζει διαδικασία απόσυρσης, σε εξοπλισμό, λειτουργικά συστήματα και εφαρμογές, στα οποία έχει λήξει η υποστήριξη από τον κατασκευαστή τους;
8) Ο οργανισμός, εφαρμόζει τείχος προστασίας, σε διακομιστές και συσκευές τελικού χρήστη;
9) Ο οργανισμός, εφαρμόζει αυθεντικοποίηση πολλαπλών παραγόντων (Multi Factor Authentication -MFA), για πρόσβαση στο διαχειριστικό περιβάλλον των κρίσιμων δικτυακών συσκευών;
10) Ο οργανισμός, απενεργοποιεί τις περιττές υπηρεσίες στις δικτυακές συσκευές;
11) Ο οργανισμός, απενεργοποιεί τις θύρες που δεν χρησιμοποιούνται στα switches;
12) Ο οργανισμός, ενεργοποιεί τη λειτουργία port security στα switches;
13) Ο οργανισμός, απενεργοποιεί τα πρωτόκολλα δρομολόγησης και τα interfaces που δεν χρησιμοποιούνται στους δρομολογητές;
14) Ο οργανισμός, εφαρμόζει ρύθμιση αυτόματου κλειδώματος, μετά από μια καθορισμένη περίοδο αδράνειας στο υλικό (υπολογιστές, φορητοί υπολογιστές και άλλα);
15) Ο οργανισμός, χορηγεί στους υπαλλήλους όπου απαιτείται απομακρυσμένη εργασία ή τηλεργασία, φορητές συσκευές, οι οποίες έχουν διαμορφωθεί κατάλληλα και διαθέτουν τις απαιτούμενες ρυθμίσεις ασφάλειας;
16) Ο οργανισμός, εφαρμόζει τεχνικά την δυνατότητα απομακρυσμένης διαγραφής των φορητών συσκευών όταν κρίνεται σκόπιμο, όπως για παράδειγμα κλεμμένες ή χαμένες συσκευές;
17) Ο οργανισμός, επιβάλλει αυτόματο κλείδωμα συσκευής, μετά από ένα προκαθορισμένο όριο αποτυχημένων προσπαθειών ελέγχου ταυτότητας στις φορητές συσκευές των τελικών χρηστών;
18) Ο οργανισμός, παρέχει στους υπαλλήλους οδηγίες, για την αποδεκτή χρήση τους εξοπλισμού;
19) Ο οργανισμός, διασφαλίζει ότι οι χρήστες (non-privileged) δεν μπορούν να παραμετροποιήσουν το λειτουργικό σύστημα και τις ρυθμίσεις ασφαλείας;

5.6. Προστασία Δεδομένων

Το σημείο ελέγχου της προστασίας των δεδομένων, περιλαμβάνει την ανάπτυξη διαδικασιών και τεχνικών ελέγχων για τον εντοπισμό, την ταξινόμηση, τον χειρισμό, τη διατήρηση και τη διάθεση των δεδομένων. Τα δεδομένα, δεν βρίσκονται μόνο εντός των συνόρων ενός οργανισμού, αλλά, στο

σύννεφο, σε φορητές συσκευές και συχνά μοιράζονται με συνεργάτες ή διαδικτυακές υπηρεσίες. Επιπλέον, τα ευαίσθητα δεδομένα που κατέχει ο οργανισμός σχετικά με τα οικονομικά στοιχεία, την πνευματική ιδιοκτησία και τα δεδομένα πελατών, μπορεί να εμπίπτουν σε διεθνείς κανονισμούς, όπως για την προστασία προσωπικών δεδομένων, της ιδιωτικότητας και του απορρήτου. Οι κανονισμοί αυτοί μπορεί να είναι περίπλοκοι ακόμη και για πολυεθνικές εταιρείες, ωστόσο, υπάρχουν θεμελιώδεις αρχές που μπορούν να εφαρμοστούν σε όλους.

Τα δεδομένα, πρέπει να διαχειρίζονται κατάλληλα καθ' όλη τη διάρκεια του κύκλου ζωής τους. Η απώλεια του ελέγχου του οργανισμού επί των προστατευόμενων ή ευαίσθητων δεδομένων, είναι ένας σοβαρός και συχνά αναφερόμενος επιχειρηματικός αντίκτυπος. Η υιοθέτηση της κρυπτογράφησης των δεδομένων, τόσο κατά τη μεταφορά όσο και κατά την ηρεμία, μπορεί να προσφέρει μετριασμό κατά της παραβίασης των δεδομένων και ακόμη πιο σημαντικό, αποτελεί κανονιστική απαίτηση για τα περισσότερα ελεγχόμενα δεδομένα. Επίσης, είναι σημαντικό για τον οργανισμό, να αναπτύξει μια διαδικασία διαχείρισης δεδομένων, η οποία να περιλαμβάνει ένα πλαίσιο διαχείρισης δεδομένων, τις κατευθυντήριες γραμμές ταξινόμησης δεδομένων και τις απαιτήσεις για την προστασία, το χειρισμό, τη διατήρηση και τη διάθεση αυτών των δεδομένων. Τέλος, πρέπει να υπάρχει μια διαδικασία για την παραβίαση, η οποία να συνδέεται με ένα σχέδιο αντιμετώπισης συμβάντων.

Η προστασία των δεδομένων περιλαμβάνει δώδεκα (12) διασφαλίσεις:

1) Καθιέρωση και διατήρηση διαδικασίας διαχείρισης δεδομένων. Ένα πλαίσιο με τον χειρισμό των δεδομένων, τα όρια διατήρησης των δεδομένων και τις απαιτήσεις διάθεσης. Επανεξέταση και επικαιροποίηση της τεκμηρίωσης τουλάχιστον ετησίως.
2) Καθιέρωση και διατήρηση καταλόγου δεδομένων, με βάση τη διαδικασία διαχείρισης δεδομένων του οργανισμού. Επανεξέταση και επικαιροποίηση του καταλόγου ετησίως.
3) Διαμόρφωση και εφαρμογή λιστών ελέγχου πρόσβασης σε δεδομένα, σύμφωνα με τις αρμοδιότητες των χρηστών.
4) Διατήρηση δεδομένων σύμφωνα με τη διαδικασία διαχείρισης δεδομένων του οργανισμού.
5) Διάθεση δεδομένων με ασφάλεια.
6) Κρυπτογράφηση δεδομένων σε συσκευές τελικών χρηστών. Όπως, για παράδειγμα, Windows BitLocker ή Apple FileVault ή Linux dm-crypt κλπ.
7) Κρυπτογράφηση δεδομένων σε αφαιρούμενα μέσα.
8) Κρυπτογράφηση ευαίσθητων δεδομένων κατά τη μεταφορά. Όπως, για παράδειγμα, υλοποίηση Transport Layer Security (TLS) και Open Secure Shell (OpenSSH).
9) Κρυπτογράφηση ευαίσθητων δεδομένων σε κατάσταση ηρεμίας, σε διακομιστές, εφαρμογές και βάσεις δεδομένων.
10) Καθιέρωση και διατήρηση ενός συστήματος ταξινόμησης, με τη χρήση ετικετών, όπως "Ευαίσθητο", "Εμπιστευτικό" και "Δημόσιο". Επανεξέταση και επικαιροποίηση του σύστημα ταξινόμησης ετησίως.
11) Τεκμηρίωση των ροών δεδομένων. Ετήσια επανεξέταση και επικαιροποίηση.
12) Τμηματοποίηση της επεξεργασίας και της αποθήκευσης των δεδομένων, με βάση την ευαισθησία των δεδομένων. Ευαίσθητα δεδομένα δεν πρέπει να επεξεργάζονται σε επιχειρησιακά περιουσιακά στοιχεία που προορίζονται για δεδομένα χαμηλότερης ευαισθησίας.

Το πλαίσιο, στο σημείο ελέγχου προστασία των δεδομένων, θέτει δεκατέσσερα (14) ερωτήματα:

1) Ο οργανισμός, έχει διενεργήσει χαρτογράφηση των δεδομένων του;
2) Ο οργανισμός, έχει καθιερώσει και διατηρεί διαδικασία διαχείρισης των δεδομένων, η οποία επανεξετάζεται τουλάχιστον ετησίως;
3) Ο οργανισμός, διατηρεί κατάλογο δεδομένων βάσει της διαδικασίας διαχείρισης δεδομένων, ο οποίος επανεξετάζεται και επικαιροποιείται τουλάχιστον ετησίως;
4) Ο οργανισμός, έχει κατηγοριοποιήσει/ταξινομήσει τα δεδομένα του ως “Δημόσια”, “Εσωτερικά”, “Εμπιστευτικά” και “Περιορισμένα”;

5) Ο οργανισμός, εφαρμόζει λίστες ελέγχου πρόσβασης στα δεδομένα, σύμφωνα με τους ρόλους και τις αρμοδιότητες των χρηστών;
6) Ο οργανισμός, διατηρεί τα δεδομένα του σύμφωνα με τη διαδικασία διαχείρισης δεδομένων του;
7) Ο οργανισμός, παρέχει διάθεση στα δεδομένα του με ασφάλεια;
8) Ο οργανισμός, εφαρμόζει τεχνικά μέτρα κρυπτογράφησης δεδομένων σε συσκευές τελικών χρηστών; Όπως για παράδειγμα χρήση Windows BitLocker ή Apple FileVault ή Linux dm-crypt κλπ.
9) Ο οργανισμός, διασφαλίζει ότι τα κρίσιμα δεδομένα κρυπτογραφούνται κατά τη μετάδοση τους;
10) Ο οργανισμός, εφαρμόζει τεχνικά μέτρα κρυπτογράφησης δεδομένων στους φορητούς υπολογιστές (laptop, netbook, tablet, smart phone);
11) Ο οργανισμός, εφαρμόζει τεχνικά μέτρα κρυπτογράφησης δεδομένων στα αφαιρούμενα μέσα (εξωτερικοί δίσκοι, usb flash memory και άλλα);
12) Κατά την εφαρμογή της κρυπτογράφησης, χρησιμοποιούνται μόνο τελευταίες εκδόσεις εγκεκριμένων κρυπτογραφικών πρωτοκόλλων και λογισμικού και το κατάλληλο μήκος κλειδιών;
13) Ο οργανισμός, εφαρμόζει κατάλληλα τεχνικά και οργανωτικά μέτρα για τα δεδομένα προσωπικού χαρακτήρα και συμμορφώνεται με την εθνική και ευρωπαϊκή νομοθεσία;
14) Ο οργανισμός, συνάπτει συμβάσεις με όλους τους συνεργάτες του συμπεριλαμβανομένης της δέσμευσης τήρησης της εμπιστευτικότητας και του απορρήτου;

5.7. Διαχείριση λογαριασμών

Το σημείο ελέγχου της διαχείρισης των λογαριασμών, αναφέρεται στις πολιτικές και στα διάφορα εφαρμοσμένα μέτρα για την ασφαλή διαχείριση των λογαριασμών των χρηστών. Περιλαμβάνει τη χρήση διαδικασιών και εργαλείων, για την ανάθεση και διαχείριση εξουσιοδοτήσεων σε διαπιστευτήρια για λογαριασμούς χρηστών, συμπεριλαμβανομένων των λογαριασμών διαχειριστών, καθώς επίσης και λογαριασμούς υπηρεσιών για περιουσιακά στοιχεία και λογισμικό του οργανισμού. Τα διαπιστευτήρια είναι περιουσιακά στοιχεία που πρέπει να απογράφονται και να παρακολουθούνται, όπως τα περιουσιακά στοιχεία του οργανισμού και το λογισμικό, καθώς αποτελούν το κύριο σημείο εισόδου στον οργανισμό. Ο οργανισμός, πρέπει να αναπτύσσει κατάλληλες πολιτικές και οδηγίες για τους κωδικούς πρόσβασης. Ένας αδρανής λογαριασμός, πρέπει να απενεργοποιείται και να αφαιρείται από το σύστημα. Ο οργανισμός, πρέπει να διενεργεί περιοδικούς ελέγχους, για να διασφαλίζει ότι όλοι οι ενεργοί λογαριασμοί εντοπίζονται σε εξουσιοδοτημένους χρήστες. Οι χρήστες, με πρόσβαση διαχειριστή ή άλλη προνομιακή πρόσβαση, θα πρέπει να έχουν ξεχωριστούς λογαριασμούς για αυτές τις εργασίες και να τους χρησιμοποιούν μόνο κατά την εκτέλεση αυτών των ιδιαίτερων εργασιών. Επιπλέον, οι χρήστες, πρέπει να χρησιμοποιούν εφαρμογή διαχείρισης κωδικών πρόσβασης και να μην διατηρούν σε λογιστικά φύλλα ή αρχεία κειμένου τους κωδικούς. Οι χρήστες, πρέπει να αποσυνδέονται αυτόματα από το σύστημα μετά από μια περίοδο αδράνειας, καθώς επίσης και να εκπαιδεύονται ώστε να κλειδώνουν την οθόνη τους όταν αφήνουν τη συσκευή. Για την απομακρυσμένη πρόσβαση, πρέπει να υπάρχει έλεγχος ταυτότητας πολλών παραγόντων (Multi Factor Authentication -MFA).

Η διαχείριση των λογαριασμών περιλαμβάνει πέντε (5) διασφαλίσεις:

1) Δημιουργία και διατήρηση καταλόγου όλων των λογαριασμών που διαχειρίζεται ο οργανισμός. Επικύρωση των ενεργών λογαριασμών και των εξουσιοδοτημένων χρηστών τουλάχιστον ανά τρίμηνο.
2) Χρήση μοναδικών κωδικών πρόσβασης για όλα τα περιουσιακά στοιχεία του οργανισμού. Συμπεριλαμβανομένων τεχνικών όπως για παράδειγμα, τουλάχιστον έναν κωδικό πρόσβασης 8 χαρακτήρων για λογαριασμούς που χρησιμοποιούν MFA και έναν κωδικό πρόσβασης 14 χαρακτήρων για λογαριασμούς που δεν χρησιμοποιούν MFA.

3) Απενεργοποίηση και διαγραφή αδρανών λογαριασμών μετά από περίοδο αδράνειας 45 ημερών.
4) Περιορισμός των προνομίων διαχειριστή σε ειδικούς λογαριασμούς διαχειριστή. Τα άτομα στο ρόλο διαχειριστή, να διατηρούν κύριο, μη προνομιούχο λογαριασμό, για υπολογιστικές δραστηριότητες, όπως περιήγηση στο διαδίκτυο, ηλεκτρονικό ταχυδρομείο και χρήση σουίτας παραγωγικότητας.
5) Διαχείρισης λογαριασμών μέσω ενός καταλόγου ή μιας υπηρεσίας ταυτότητας.

Το πλαίσιο, στο σημείο ελέγχου της διαχείρισης λογαριασμών, θέτει δεκατρία (13) ερωτήματα:

1) Ο οργανισμός, διαθέτει καταγεγραμμένη πολιτική και διαδικασίες υλοποίησης για την διαχείριση των λογαριασμών και τον έλεγχο πρόσβασης σε όλα τα συστήματα του;
2) Ο οργανισμός, διατηρεί κατάλογο όλων των λογαριασμών που διαχειρίζεται, με ονοματεπώνυμο και προνόμια;
3) Ο οργανισμός, επικυρώνει τουλάχιστον ανά τρίμηνο, τους ενεργούς λογαριασμούς και τους εξουσιοδοτημένους χρήστες;
4) Ο οργανισμός, εκχωρεί δικαιώματα, σύμφωνα με τον ρόλο και τις αρμοδιότητες του υπαλλήλου; Επανεξετάζονται, τουλάχιστον εξαμηνιαίως;
5) Ο οργανισμός, εφαρμόζει αυτοματοποιημένη διαδικασία χορήγησης πρόσβασης και δικαιωμάτων, σύμφωνα με το ρόλο του χρήστη;
6) Ο οργανισμός, χρησιμοποιεί μοναδικούς κωδικούς πρόσβασης, για όλα τα περιουσιακά του στοιχεία;
7) Ο οργανισμός, χρησιμοποιεί κωδικούς πρόσβασης, τουλάχιστον 14 χαρακτήρων σε λογαριασμούς που δεν χρησιμοποιούν MFA και 8 χαρακτήρων στους λογαριασμούς που χρησιμοποιούν MFA;
8) Ο οργανισμός, απενεργοποιεί και διαγράφει τους αδρανής λογαριασμούς μετά από περίοδο 45 ημερών αδράνειας;
9) Ο οργανισμός, περιορίζει τα προνόμια διαχειριστή στους ειδικούς λογαριασμούς διαχειριστή και οι διαχειριστές, διατηρούν κύριο λογαριασμό μη προνομιούχο για υπολογιστικές δραστηριότητες (πχ περιήγηση στο διαδίκτυο, ηλεκτρονικό ταχυδρομείο κλπ);
10) Ο οργανισμός, διαχειρίζεται τους λογαριασμούς μέσω ενός καταλόγου ή μιας υπηρεσίας ταυτότητας;
11) Ο οργανισμός, διασφαλίζει ότι όλοι όσοι αποκτούν πρόσβαση αναγνωρίζονται με μοναδικό τρόπο και διαθέτουν ξεχωριστό λογαριασμό χρήστη;
12) Ο οργανισμός, διασφαλίζει ότι οι χρήστες χρησιμοποιούν ειδική εφαρμογή διαχείρισης κωδικών πρόσβασης (Password Manager) και δεν διατηρούν σε λογιστικά φύλλα ή αρχεία κειμένου τους κωδικούς;
13) Ο οργανισμός, παρέχει στους υπαλλήλους οδηγίες για την κατασκευή ισχυρών κωδικών πρόσβασης;

5.8. Διαχείριση ελέγχου πρόσβασης

Η διαχείριση ελέγχου πρόσβασης, περιλαμβάνει τη χρήση διαδικασιών και εργαλείων για τη δημιουργία, διαχείριση και ανάκληση διαπιστευτηρίων πρόσβασης και προνομίων για τους λογαριασμούς των χρηστών, των διαχειριστών και των υπηρεσιών για επιχειρησιακά περιουσιακά στοιχεία και λογισμικό. Επικεντρώνεται στη διαχείριση της πρόσβασης των λογαριασμών, διασφαλίζοντας ότι οι χρήστες έχουν μόνο πρόσβαση στα δεδομένα ή τα επιχειρησιακά περιουσιακά στοιχεία που είναι κατάλληλα για το ρόλο τους, και διασφαλίζοντας ότι υπάρχει ισχυρός έλεγχος ταυτότητας. Πιο συγκεκριμένα, οι λογαριασμοί πρέπει να έχουν μόνο την ελάχιστη εξουσιοδότηση που απαιτείται για το ρόλο τους και πρέπει να υπάρχει μια διαδικασία με την οποία θα χορηγούνται και θα ανακαλούνται τα

προνόμια για τους λογαριασμούς των χρηστών, καθώς επίσης συνίσταται η χρήση τεχνολογικών εργαλείων που βοηθούν στη διαχείριση αυτής της διαδικασίας. Η χρήση MFA πρέπει να είναι καθολική για όλους τους προνομιακούς λογαριασμούς ή τους λογαριασμούς διαχειριστών. Επίσης, σημαντική είναι η ολοκληρωμένη αποδέσμευση λογαριασμού. Τέλος, οι λογαριασμοί υψηλού προνομίου δεν πρέπει να χρησιμοποιούνται για καθημερινή χρήση.

Η διαχείριση του ελέγχου πρόσβασης περιλαμβάνει οκτώ (8) διασφαλίσεις:

1) Καθιέρωση διαδικασίας χορήγησης πρόσβασης.
2) Καθορισμός και διατήρηση του ελέγχου πρόσβασης, βάσει ρόλων, μέσω του προσδιορισμού και της τεκμηρίωσης των δικαιωμάτων πρόσβασης που απαιτούνται για κάθε ρόλο.
3) Καθιέρωση διαδικασίας ανάκλησης πρόσβασης. Η απενεργοποίηση λογαριασμών, αντί διαγραφής λογαριασμών, μπορεί να είναι απαραίτητη για τη διατήρηση των διαδρομών ελέγχου.
4) Απαίτηση MFA, για εφαρμογές που εκτίθενται εξωτερικά.
5) Απαίτηση MFA, για απομακρυσμένη πρόσβαση στο δίκτυο.
6) Απαίτηση MFA, για πρόσβαση λογαριασμών διαχειριστών.
7) Καθιέρωση και διατήρηση καταλόγου των συστημάτων ελέγχου ταυτότητας και εξουσιοδότησης. Ετήσια επανεξέταση και επικαιροποίηση.
8) Κεντρικοποίηση ελέγχου πρόσβασης για όλα τα περιουσιακά στοιχεία του οργανισμού μέσω μιας υπηρεσίας καταλόγου ή ενός παρόχου SSO.

Το πλαίσιο, στο σημείο ελέγχου της διαχείρισης του ελέγχου πρόσβασης, θέτει δέκα (10) ερωτήματα:

1) Ο οργανισμός, διαθέτει καταγεγραμμένη πολιτική και διαδικασία υλοποίησης για την χορήγηση πρόσβασης;
2) Ο οργανισμός, έχει καθορίσει και διατηρεί τον έλεγχο πρόσβασης, βάσει ρόλων, μέσω του προσδιορισμού και της τεκμηρίωσης των δικαιωμάτων πρόσβασης που απαιτούνται για κάθε ρόλο;
3) Ο οργανισμός, διαθέτει διαδικασία ανάκλησης πρόσβασης;
4) Ο οργανισμός, υλοποιεί μηχανισμούς αυθεντικοποίησης, οι οποίοι επιβάλλουν την δημιουργία ισχυρών κωδικών πρόσβαση, όπως συγκεκριμένο αριθμό χαρακτήρων, τουλάχιστον έναν αριθμό, ένα κεφαλαίο γράμμα, ένα μικρό γράμμα και έναν ειδικό χαρακτήρα;
5) Ο οργανισμός, εφαρμόζει MFA (Multi Factor Authentication), για εφαρμογές που εκτίθενται εξωτερικά;
6) Ο οργανισμός, εφαρμόζει MFA, για απομακρυσμένη πρόσβαση στο δίκτυο;
7) Ο οργανισμός, εφαρμόζει MFA, για πρόσβαση λογαριασμών διαχειριστών;
8) Ο οργανισμός, εφαρμόζει MFA, για πρόσβαση σε κρίσιμα δεδομένα;
9) Ο οργανισμός, διατηρεί κατάλογο των συστημάτων ελέγχου ταυτότητας και εξουσιοδότησης και τον επανεξετάζει, τουλάχιστον ετησίως;
10) Ο οργανισμός, έχει κεντρικοποιήσει τον ελέγχο πρόσβασης για όλα τα περιουσιακά του στοιχεία, μέσω μιας υπηρεσίας καταλόγου ή ενός παρόχου SSO;

5.9. Διαχείριση αρχείων καταγραφής

Η διαχείριση αρχείων καταγραφής ενισχύει την ασφάλειας, επιτρέπει τον εντοπισμό ανωμαλιών και βοηθάει στην πρόληψη κυβερνοαπειλών. Το σημείο ελέγχου της διαχείρισης αρχείων καταγραφής περιλαμβάνει την συλλογή, ειδοποίηση, επανεξέταση και διατήρηση των αρχείων καταγραφής ελέγχου των συμβάντων που μπορούν να βοηθήσουν στην ανίχνευση και κατανόηση μιας επίθεσης, καθώς επίσης και της ανάκαμψης από αυτήν. Η συλλογή και ανάλυση αρχείων καταγραφής είναι κρίσιμη για την ικανότητα του οργανισμού να εντοπίσει γρήγορα μια κακόβουλη δραστηριότητα, καθώς

επίσης και να αποδείξει την δραστηριότητα αυτή. Τα αρχεία καταγραφής συστήματος (System Logs) και τα αρχεία καταγραφής ελέγχου (Audit Logs) αποτελούν τους δυο τύπους αυτής της διαχείρισης.

Τα system logs είναι εγγενή στα συστήματα, παρέχουν πληροφορία σε συμβάντα συστήματος και απαιτούν λιγότερες ρυθμίσεις για να ενεργοποιηθούν. Τα audit logs παρέχουν πληροφορίες όπως για παράδειγμα πότε ένας χρήστης συνδέθηκε ή είχε πρόσβαση σε ένα αρχείο. Τα αρχεία καταγραφής είναι κρίσιμα για την αντιμετώπιση των περιστατικών και μπορούν να παρέχουν πληροφορίες όπως για παράδειγμα πότε έγινε μια επίθεση και την έκταση της, αν υπήρξε διαρροή δεδομένων και άλλα. Τα περισσότερα επιχειρησιακά περιουσιακά στοιχεία και το λογισμικό προσφέρουν δυνατότητες καταγραφής. Επίσης, εξίσου σημαντικό είναι η διατήρηση των δεδομένων καταγραφής.

Η διαχείριση των αρχείων καταγραφής περιλαμβάνει έντεκα (11) διασφαλίσεις:

1) Καθιέρωση και διατήρηση μιας διαδικασίας διαχείρισης των audit logs που καθορίζει τις απαιτήσεις καταγραφής του οργανισμού. Επανεξέταση τουλάχιστον ετησίως.
2) Συλλογή των audit logs.
3) Διασφάλιση επαρκούς χώρου αποθήκευσης των audit logs
4) Τυποποιήστε τον συγχρονισμό του χρόνου. Διαμόρφωση με τουλάχιστον δύο συγχρονισμένες πηγές χρόνου σε όλα τα περιουσιακά στοιχεία της επιχείρησης.
5) Συλλογή λεπτομερειών στα audit logs, όπως ημερομηνία, όνομα χρήστη, διευθύνσεις πηγής/προορισμού κλπ.
6) Συλλογή audit logs αιτημάτων DNS και URL.
7) Συλλογή audit logs σε αρχεία και διεργασίες διακομιστών
8) Συλλογή audit logs σε απόπειρες χρήσης ειδικών προνομίων.
9) Συλλογή audit logs αλλαγών σε λογαριασμούς και στην πολιτική ασφαλείας.
10) Συλλογή audit logs μεταφοράς δεδομένων από και προς φορητά μέσα αποθήκευσης.
11) Συγκέντρωση των audit logs.
12) Διατήρηση των αρχείων καταγραφής ελέγχου, τουλάχιστον για ένα (1) έτος.
13) Διεξαγωγή ελέγχων των audit logs.
14) Προστασία από μη εξουσιοδοτημένη πρόσβαση, τροποποίηση και διαγραφή.

Το πλαίσιο, στο σημείο ελέγχου διαχείριση των αρχείων καταγραφής, θέτει δεκατέσσερα (14) ερωτήματα:

1) Ο οργανισμός, έχει καταγεγραμμένη πολιτική, για την καταγραφή, παρακολούθηση, ανάλυση και διαχείριση των συμβάντων ασφαλείας, η οποία επανεξετάζεται ετησίως;
2) Ο οργανισμός, έχει ενεργοποιήσει τη λειτουργία καταγραφής συμβάντων ασφαλείας, στους διακομιστές, στους σταθμούς εργασίας και στις δικτυακές συσκευές;
3) Ο οργανισμός, έχει τυποποιήσει τον συγχρονισμό των ρολογιών σε όλες τις συσκευές, με διαμόρφωση τουλάχιστον δυο συγχρονισμένων πηγών χρόνου;
4) Ο οργανισμός, έχει διασφαλίσει επαρκή χώρο αποθήκευσης των αρχείων καταγραφής;
5) Ο οργανισμός, έχει διασφαλίσει ότι τα αρχεία καταγραφής τηρούνται για περίοδο τουλάχιστον ενός (1) έτους;
6) Ο οργανισμός, έχει διασφαλίσει τη συλλογή λεπτομερών αρχείων καταγραφής, όπως ημερομηνία, όνομα χρήστη, διευθύνσεις πηγής/προορισμού κλπ;
7) Ο οργανισμός, συλλέγει αρχεία καταγραφής αιτημάτων DNS και URL;
8) Ο οργανισμός, συλλέγει αρχεία καταγραφής σε αρχεία και διεργασίες διακομιστών;
9) Ο οργανισμός, συλλέγει αρχεία καταγραφής απο απόπειρες χρήσης ειδικών προνομίων;
10) Ο οργανισμός, συλλέγει αρχεία καταγραφής αλλαγών σε λογαριασμούς;
11) Ο οργανισμός, συλλέγει αρχεία καταγραφής αλλαγών στην πολιτική ασφαλείας;
12) Ο οργανισμός, συλλέγει αρχεία καταγραφής μεταφοράς δεδομένων από και προς φορητά μέσα αποθήκευσης;
13) Ο οργανισμός, συγκεντρώνει τα αρχεία καταγραφής;

14) Ο οργανισμός, διεξάγει ελέγχους των αρχείων καταγραφής;

5.10. Διαχείριση παρόχων υπηρεσιών

Το σημείο ελέγχου διαχείρισης των παρόχων υπηρεσιών, περιλαμβάνει την ανάπτυξη μιας διαδικασίας αξιολόγησης των παρόχων υπηρεσιών, οι οποίοι κατέχουν ευαίσθητα δεδομένα ή είναι υπεύθυνοι για τις κρίσιμες τεχνολογίες πληροφορικής του οργανισμού, όπως οι πλατφόρμες, ώστε να διασφαλίζεται ότι οι εν λόγω πάροχοι προστατεύουν κατάλληλα τις εν λόγω πλατφόρμες και τα δεδομένα. Συχνά, οι οργανισμοί βασίζονται σε προμηθευτές και συνεργάτες για τη διαχείριση των δεδομένων τους ή βασίζονται σε υποδομές τρίτων για βασικές εφαρμογές ή λειτουργίες. Οι περισσότεροι κανονισμοί για την ασφάλεια των δεδομένων, την προστασία της ιδιωτικής ζωής και του απορρήτου, απαιτούν η προστασία τους να επεκτείνεται στους τρίτους παρόχους υπηρεσιών. Ανεξάρτητα από το μέγεθος του οργανισμού, πρέπει να υπάρχει μια πολιτική σχετικά με την επανεξέταση παρόχων υπηρεσιών, μια καταγραφή αυτών των προμηθευτών και μια αξιολόγηση κινδύνου που σχετίζεται με τις πιθανές επιπτώσεις τους στον οργανισμό στην περίπτωση συμβάντος. Επίσης, η σύμβαση, πρέπει να τους καθιστά υπεύθυνους σε περίπτωση περιστατικού που επηρεάζει τον οργανισμό.

Η διαχείριση των παρόχων υπηρεσιών, περιλαμβάνει πέντε (5) διασφαλίσεις:

1) Κατάρτιση και διατήρηση καταλόγου παρόχων υπηρεσιών, με τουλάχιστον ετήσια επανεξέταση.
2) Δημιουργία και διατήρηση πολιτικής διαχείρισης των παρόχων υπηρεσιών, για την ταξινόμηση, απογραφή, αξιολόγηση, παρακολούθηση και παροπλισμού των παρόχων υπηρεσιών. Επανεξέταση και επικαιροποίηση της πολιτικής τουλάχιστον ετησίως.
3) Ταξινόμηση των παρόχων υπηρεσιών. Η εξέταση της ταξινόμησης μπορεί να περιλαμβάνει ένα ή περισσότερα χαρακτηριστικά, όπως ευαισθησία δεδομένων, όγκος δεδομένων, απαιτήσεις διαθεσιμότητας, ισχύοντες κανονισμοί, εγγενής και μετριασμένος κίνδυνος. Ετήσια επικαιροποίηση και επανεξέταση των ταξινομήσεων ή όταν συμβαίνουν σημαντικές αλλαγές στον οργανισμό που θα μπορούσαν να επηρεάσουν την παρούσα διασφάλιση.
4) Οι συμβάσεις παρόχων υπηρεσιών περιλαμβάνουν απαιτήσεις ασφαλείας, όπως για παράδειγμα ελάχιστες απαιτήσεις προγράμματος ασφάλειας, κοινοποίηση και αντιμετώπιση περιστατικών ασφάλειας ή/και παραβίασης δεδομένων, απαιτήσεις κρυπτογράφησης δεδομένων και δεσμεύσεις διάθεσης δεδομένων. Ετήσια επανεξέταση των συμβάσεων για να διασφαλιστεί ότι δεν λείπουν απαιτήσεις ασφαλείας.
5) Ασφαλής παροπλισμός των παρόχων υπηρεσιών, όπως για παράδειγμα την απενεργοποίηση λογαριασμών χρηστών και υπηρεσιών και τον τερματισμό των ροών δεδομένων.

Το πλαίσιο, στο σημείο ελέγχου διαχείρισης των παρόχων υπηρεσιών, θέτει πέντε (5) ερωτήματα:

1) Ο οργανισμός, διατηρεί κατάλογο παρόχων υπηρεσιών, με τουλάχιστον ετήσια επανεξέταση;
2) Ο οργανισμός, διαθέτει καταγεγραμμένη πολιτική διαχείρισης των παρόχων υπηρεσιών, για την ταξινόμηση, την απογραφή, την αξιολόγηση, την παρακολούθηση και τον παροπλισμό των παρόχων υπηρεσιών, με τουλάχιστον ετήσια επανεξέταση και επικαιροποίηση;
3) Ο οργανισμός, ταξινομεί τους παρόχους υπηρεσιών συμπεριλαμβάνοντας χαρακτηριστικά όπως ευαισθησία δεδομένων, όγκος δεδομένων, απαιτήσεις διαθεσιμότητας, ισχύοντες κανονισμοί, εγγενής και μετριασμένος κίνδυνος, με επικαιροποίηση και επανεξέταση των ταξινομήσεων τουλάχιστον ετησίως ή όταν συμβαίνουν σημαντικές αλλαγές στον οργανισμό που θα μπορούσαν να επηρεάσουν την παρούσα διασφάλιση;
4) Ο οργανισμός, διασφαλίζει ότι οι συμβάσεις παρόχων υπηρεσιών περιλαμβάνουν απαιτήσεις ασφαλείας, όπως για παράδειγμα ελάχιστες απαιτήσεις προγράμματος ασφάλειας, κοινοποίηση και αντιμετώπιση περιστατικών ασφάλειας ή παραβίασης δεδομένων, απαιτήσεις

κρυπτογράφησης δεδομένων και δεσμεύσεις διάθεσης δεδομένων; Ετήσια επανεξέταση των συμβάσεων για να διασφαλιστούν οι απαιτήσεις ασφαλείας;
5) Ο οργανισμός, εφαρμόζει διαδικασία για τον ασφαλής παροπλισμός των παρόχων υπηρεσιών;

5.11. Διαχείριση δικτυακής υποδομής

Το σημείο ελέγχου διαχείρισης της δικτυακής υποδομής, περιλαμβάνει την καθιέρωση, εφαρμογή και ενεργή διαχείριση των συσκευών δικτύου (physical και virtualized gateways, firewalls access points, switches κλπ), προκειμένου να αποτρέψει τους επιτιθέμενους από την εκμετάλλευση των ευάλωτων υπηρεσιών δικτύου και σημεία πρόσβασης. Η ασφαλής δικτυακή υποδομή, αποτελεί την βασική άμυνα κατά των επιθέσεων, η οποία περιλαμβάνει την κατάλληλη αρχιτεκτονική ασφάλειας που αντιμετωπίζει τα τρωτά σημεία, την παρακολούθηση των αλλαγών και την επανεκτίμηση των τρέχουσων ρυθμίσεων. Ο οργανισμός, πρέπει μα διασφαλίσει ότι η δικτυακή υποδομή είναι τεκμηριωμένη και η αρχιτεκτονική και τα διαγράμματα ενημερωμένα. Επίσης, όλα τα στοιχεία της υποδομής πρέπει να έχουν υποστήριξη από τον κατασκευαστή για διορθώσεις και αναβαθμίσεις λειτουργιών. Επιπλέον, σημαντικό θεμέλιο αποτελούν η διαχείριση λογαριασμών, η καταγραφή, η παρακολούθηση και τα ασφαλή πρωτόκολλα.

Η διαχείριση της δικτυακής υποδομή περιλαμβάνει έξι (6) διασφαλίσεις:

1) Καθιέρωση και διατήρηση ασφαλούς αρχιτεκτονικής δικτύου.
2) Ασφαλή διαχείριση της υποδομή δικτύου, όπως για παράδειγμα χρήση ασφαλών πρωτοκόλλων δικτύου (SSH, HTTPS, κλπ).
3) Δημιουργία και διατήρηση διαγραμμάτων αρχιτεκτονικής και/ή άλλης τεκμηρίωσης του συστήματος δικτύου, με τουλάχιστον ετήσια επανεξέταση και επικαιροποίηση.
4) Κεντρικοποίηση της αυθεντικοποίησης, της εξουσιοδότησης και του ελέγχου (Authentication Authorization Audit - AAA) του δικτύου.
5) Ασφαλής διαχείρισης δικτύου και χρήση πρωτοκόλλων επικοινωνίας, όπως για παράδειγμα. 802.1X, Wi-Fi Protected Access 2 (WPA2) Enterprise.
6) Χρήση VPN από τις απομακρυσμένες συσκευές για σύνδεση στην υποδομή του οργανισμού.

Το πλαίσιο, στο σημείο ελέγχου διαχείρισης της δικτυακής υποδομής, θέτει έντεκα (11) ερωτήματα:

1) Ο οργανισμός, διαθέτει καταγεγραμμένη πολιτική για τη διατήρηση ασφαλούς αρχιτεκτονικής δικτύου;
2) Ο οργανισμός, τηρεί διάγραμμα δικτύου και ροής δεδομένων ή άλλη τεκμηρίωσης στην οποία απεικονίζονται όλες οι δικτυακές συνδέσεις και οι ροές μετάδοσης των δεδομένων του, με τουλάχιστον ετήσια επανεξέταση;
3) Ο οργανισμός, έχει κεντρικοποιήσει την αυθεντικοποίηση, την εξουσιοδότηση και τον έλεγχο (Authentication Authorization Audit - AAA) του δικτύου;
4) Ο οργανισμός, χρησιμοποιεί ασφαλή πρωτόκολλα δικτύου (SSH, HTTPS, κλπ);
5) Ο οργανισμός, χρησιμοποιεί ασφαλή πρωτόκολλα επικοινωνίας (802.1X, WPA2);
6) Ο οργανισμός, χρησιμοποιεί Virtual Private Network (VPN) για σύνδεση απομακρυσμένων συσκευών στην υποδομή του;
7) Ο οργανισμός, εφαρμόζει διεθνώς αποδεκτές ρυθμίσεις ασφαλείας για τη χρήση του Remote Desktop Protocol (RDP);
8) Ο οργανισμός, έχει διαχωρίσει το εσωτερικό του δίκτυο σε διακριτά υποδίκτυα, βάσει της ευαισθησίας των επιχειρησιακών στόχων;
9) Ο οργανισμός, έχει εφαρμόσει τείχος προστασίας στην εξωτερική περίμετρο του δικτύου, το οποίο επιτρέπει μόνο την εισερχόμενη και εξερχόμενη ροή της πληροφορίας που είναι απαραίτητη για την εκτέλεση των επιχειρησιακών λειτουργιών του;

10) Ο οργανισμός, διασφαλίζει ότι τα ασύρματα δίκτυα δημόσιας πρόσβαση που διαθέτει είναι διαχωρισμένα από το υπόλοιπο δίκτυο του;
11) Ο οργανισμός, υλοποιεί συστήματα δικτυακού ελέγχου πρόσβασης, με σκοπό τον αποκλεισμό της σύνδεσης μη εξουσιοδοτημένων συσκευών στο δίκτυο του;

5.12. Προστασία ηλεκτρονικού ταχυδρομείου και προγραμμάτων περιήγησης

Το σημείο ελέγχου προστασίας του ηλεκτρονικού ταχυδρομείου και των προγραμμάτων περιήγησης, περιλαμβάνει την βελτίωση της προστασίας και της ανίχνευσης απειλών από το ηλεκτρονικό ταχυδρομείο και φορείς του διαδικτύου. Για τους επιτιθέμενους, αποτελούν ευκαιρία για κοινωνική μηχανική (Social Engineering), δηλαδή, χειραγώγηση της ανθρώπινης συμπεριφοράς λόγω της άμεσης αλληλεπίδρασης με τους χρήστες του οργανισμού. Το ηλεκτρονικό ταχυδρομείο και τα προγράμματα περιήγησης ιστού, είναι κρίσιμα σημεία εισόδου για τους επιτιθέμενους. Τις βέλτιστες πρακτικές, αποτελούν το φιλτράρισμα περιεχομένου, ο αποκλεισμός αναδυόμενων παραθύρων, η χρήση υπηρεσιών φιλτραρίσματος DNS, η εκπαίδευση των χρηστών έναντι του ηλεκτρονικού ψαρέματος (phishing) και του social engineering, η χρήση εργαλείων σάρωσης κακόβουλου λογισμικού και ανεπιθύμητης αλληλογραφίας και η εγκατάσταση εργαλείων κρυπτογράφησης για την ασφάλεια του ηλεκτρονικού ταχυδρομείου.

Η προστασίας του ηλεκτρονικού ταχυδρομείου και των προγραμμάτων περιήγησης περιλαμβάνει έξι (6) διασφαλίσεις:

1) Χρήση μόνο πλήρως υποστηριζόμενων φυλλομετρητών (browsers) και email client, με τις τελευταίες ενημερώσεις.
2) Χρήση υπηρεσιών φιλτραρίσματος DNS.
3) Επιβολή φίλτρων διευθύνσεων URL, πχ βάσει κατηγορίας ή βάση λιστών αποκλεισμού.
4) Περιορισμός περιττών ή μη εξουσιοδοτημένων browsers και email client, καθώς και πρόσθετων επεκτάσεων.
5) Εφαρμογή πολιτικής DMARC, Sender Policy Framework (SPF) και DomainKeys Identified Mail (DKIM), για την πρόληψη ανεπιθύμητων μηνυμάτων, επιθέσεων ηλεκτρονικού ψαρέματος και άλλων κινδύνων για την ασφάλεια των emails.
6) Αποκλεισμός περιττών τύπων αρχείων, οι οποίοι επιχειρούν να εισέλθουν από το email του οργανισμού.

Το πλαίσιο, στο σημείο ελέγχου ηλεκτρονικού ταχυδρομείου και προγραμμάτων περιήγησης, θέτει οκτώ (8) ερωτήματα:

1) Ο οργανισμός, διασφαλίζει τη χρήση μόνο πλήρως υποστηριζόμενων φυλλομετρητών (browsers) και email client, με τις τελευταίες τους ενημερώσεις;
2) Ο οργανισμός, υλοποιεί τεχνολογίες προστασίας από spam emails σε όλα τα σημεία εισόδου και εξόδου της υποδομής του, με σκοπό τον αποκλεισμό κακόβουλου περιεχομένου;
3) Ο οργανισμός, περιορίζει τους περιττούς ή μη εξουσιοδοτημένους browsers και email clients, καθώς και των πρόσθετων επεκτάσεων αυτών;
4) Ο οργανισμός, χρησιμοποιεί υπηρεσίες φιλτραρίσματος DNS;
5) Ο οργανισμός, επιβάλλει δικτυακά φίλτρα διευθύνσεων URL, όπως για παράδειγμα βάσει κατηγορίας ή βάση λιστών αποκλεισμού, με σκοπό τον περιορισμό σύνδεσης σε ιστότοπους μη εγκεκριμένους από την πολιτική ασφαλείας του;

6) Ο οργανισμός, εφαρμόζει Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM) και Domain-based Message Authentication, Reporting και Conformance (DMARC);
7) Ο οργανισμός, αποκλείει περιττούς τύπους αρχείων, οι οποίοι επιχειρούν να εισέλθουν μέσω email στον οργανισμό;
8) Ο οργανισμός, υλοποιεί τεχνολογίες προστασίας από spam emails σε όλα τα σημεία εισόδου και εξόδου της υποδομής του, με σκοπό τον αποκλεισμό κακόβουλου περιεχομένου;

5.13. Προστασία από κακόβουλο λογισμικό

Το σημείο ελέγχου προστασίας από κακόβουλο λογισμικό, περιλαμβάνει τον έλεγχο και τον αποκλεισμό της εγκατάστασης, της διάδοσης και της εκτέλεσης κακόβουλων εφαρμογών, κώδικα ή σεναρίων σε περιουσιακά στοιχεία του οργανισμού. Το κακόβουλο λογισμικό, εισέρχεται σε έναν οργανισμό μέσω των τρωτών σημείων του, όπως από τις συσκευές του τελικού χρήστη, τα συνημμένα στα emails, τις ιστοσελίδες, τις υπηρεσίες cloud, τις κινητές συσκευές και τα αφαιρούμενα μέσα. Επίσης, το κακόβουλο λογισμικό, βασίζεται συχνά στη συμπεριφορά του τελικού χρήστη, χρησιμοποιώντας τεχνικές social engineering. Επιπλέον, το σύγχρονο κακόβουλο λογισμικό, έχει σχεδιαστεί για να αποφεύγει, να εξαπατά ή να απενεργοποιεί τις άμυνες.

Η άμυνα για το κακόβουλο λογισμικό, πρέπει να είναι σε θέση να λειτουργεί σε δυναμικό περιβάλλον, μέσω αυτοματοποιημένη διαδικασίας και να ανιχνεύει και να αποτρέπει την εξάπλωση του κακόβουλου λογισμικού ή κώδικα. Η παραδοσιακή λύση για την πρόληψη όλης της υποδομής, είναι οι σουίτες λογισμικού στο τελικό σημείο, με αυτόματες ενημερώσεις και κεντρική διαχείριση. Για τη διασφάλιση των ενημερωμένων σουιτών κατά του κακόβουλου λογισμικού, οι οργανισμοί μπορούν να λαμβάνουν αυτοματοποιημένες ενημερώσεις από τον προμηθευτή και τον εμπλουτισμό άλλων δεδομένων σχετικά με ευπάθειες ή απειλές. Τα εργαλεία αυτά είναι σημαντικό να διαχειρίζονται κεντρικά για να παρέχουν συνοχή σε ολόκληρη την υποδομή.

Η προστασία από κακόβουλο λογισμικό περιλαμβάνει επτά (7) διασφαλίσεις:

1) Ανάπτυξη και συντήρηση λογισμικού anti-malware σε όλα τα περιουσιακά στοιχεία του οργανισμού.
2) Αυτόματες ενημερώσεις για τα αρχεία υπογραφών anti-malware σε όλα τα περιουσιακά στοιχεία του οργανισμού.
3) Απενεργοποίηση των λειτουργιών αυτόματης εκτέλεσης και αυτόματης αναπαραγωγής για αφαιρούμενα μέσα.
4) Διαμόρφωση του λογισμικού anti-malware για αυτόματη σάρωση αφαιρούμενων μέσων.
5) Ενεργοποίηση λειτουργιών κατά της εκμετάλλευσης (anti-exploitation) στα επιχειρησιακά περιουσιακά στοιχεία και λογισμικό, όπως Microsoft Data Execution Prevention (DEP) ή Windows Defender Exploit Guard (WDEG) ή Apple System Integrity Protection (SIP) ή Gatekeeper.
6) Κεντρική διαχείριση του λογισμικού προστασίας από κακόβουλο λογισμικό.
7) Χρήση λογισμικού κατά του κακόβουλου λογισμικού που βασίζεται στη συμπεριφορά.

Το πλαίσιο, στο σημείο ελέγχου προστασία από κακόβουλο λογισμικό, θέτει οκτώ (8) ερωτήματα:

1) Ο οργανισμός, διαθέτει καταγεγραμμένη πολιτική και διαδικασίες υλοποίησης για την προστασία των συστημάτων του από το κακόβουλο λογισμικό;
2) Ο οργανισμός, διαθέτει εγκατεστημένο λογισμικό κατά του κακόβουλου λογισμικού (anti-malware) σε όλα τα περιουσιακά στοιχεία του;
3) Ο οργανισμός, λαμβάνει ενημερώσεις για τα αρχεία υπογραφών anti-malware σε όλα τα περιουσιακά στοιχεία του, με αυτοματοποιημένο τρόπο και σε τακτά χρονικά διαστήματα;

4) Ο οργανισμός, έχει απενεργοποιήσει την λειτουργία αυτόματης εκτέλεσης και αυτόματης αναπαραγωγής των αφαιρούμενων μέσων;
5) Ο οργανισμός, έχει διαμορφώσει κατάλληλα το λογισμικό anti-malware ώστε να εκτελεί αυτόματη σάρωση των αφαιρούμενων μέσων;
6) Ο οργανισμός, έχει ενεργοποιήσει λειτουργίες κατά της εκμετάλλευσης (anti-exploitation) στα επιχειρησιακά περιουσιακά στοιχεία και το λογισμικό του, όπως με Microsoft Data Execution Prevention ή Apple System Integrity Protection ή Windows Defender Exploit Guard ή Gatekeeper;
7) Ο οργανισμός, εφαρμόζει κεντρική διαχείριση του λογισμικού anti-malware;
8) Ο οργανισμός, χρησιμοποιεί λογισμικό anti-malware που βασίζεται στη συμπεριφορά;

5.14. Ασφάλεια εφαρμογών λογισμικού

Το σημείο ελέγχου της ασφάλειας εφαρμογών λογισμικού, περιλαμβάνει τη διαχείριση του κύκλου ζωής της ασφάλειας του λογισμικού που αναπτύσσεται εσωτερικά, φιλοξενείται ή αποκτάται για την πρόληψη, τον εντοπισμό και την αποκατάσταση της ασφάλειας πριν επηρεάσουν τον οργανισμό. Σήμερα, οι εφαρμογές αναπτύσσονται, λειτουργούν και συντηρούνται σε ένα εξαιρετικά πολύπλοκο, ποικιλόμορφο, και δυναμικό περιβάλλον και συχνά ο φορέας επίθεσης είναι η έλλειψη διαπιστευτηρίων και τα ελαττώματα των εφαρμογών. Οι εφαρμογές εκτελούνται σε πολλαπλές πλατφόρμες στο διαδίκτυο, στα κινητά και το cloud, με αρχιτεκτονικές εφαρμογών που είναι πιο πολύπλοκες από τις παλαιές αρχιτεκτονικές πελάτη-εξυπηρετητή ή δομές βάσεων δεδομένων-διακομιστή ιστού. Επίσης, οι κύκλοι ζωής της ανάπτυξης έχουν γίνει μικρότεροι, μεταβαίνοντας από μήνες ή χρόνια σε μακρές μεθοδολογίες καταρράκτη, σε κύκλους DevOps με συχνές ενημερώσεις κώδικα. Επιπλέον, δεν δημιουργούνται από το μηδέν και συναρμολογούνται από ένα σύνθετο μείγμα πλαισίων ανάπτυξης, βιβλιοθηκών, υφιστάμενου κώδικα και νέου κώδικα. Τέλος, οι σύγχρονοι και εξελισσόμενοι κανονισμοί προστασίας δεδομένων που αφορούν την προστασία της ιδιωτικής ζωής των χρηστών και του απορρήτου απαιτούν τη συμμόρφωση τους με αυτούς.

Η ασφάλεια εφαρμογών λογισμικού περιλαμβάνει έντεκα (11) διασφαλίσεις:

1) Καθιέρωση και διατήρηση μιας ασφαλούς διαδικασίας ανάπτυξης εφαρμογών, κατά την οποία αντιμετωπίζονται στοιχεία όπως: πρότυπα σχεδιασμού εφαρμογών, πρακτικές κωδικοποίησης, εκπαίδευση προγραμματιστών, διαχείριση ευπαθειών, ασφάλεια σε κώδικα τρίτων και διαδικασίες δοκιμών ασφάλειας εφαρμογών, με τουλάχιστον ετήσια επανεξέταση.
2) Καθιέρωση και διατήρηση μιας διαδικασίας για την αποδοχή και αντιμετώπιση αναφορών για ευπάθειες λογισμικού, συμπεριλαμβανομένης της παροχής μέσων για την υποβολή αναφορών από εξωτερικές οντότητες. Η διαδικασία πρέπει να περιλαμβάνει στοιχεία όπως: πολιτική χειρισμού ευπαθειών που προσδιορίζει τη διαδικασία αναφοράς, τον υπεύθυνο για το χειρισμό των αναφορών ευπάθειας και μια διαδικασία για την παραλαβή, ανάθεση, αποκατάσταση και δοκιμή αποκατάστασης.
3) Ανάλυση της αιτίας των τρωτών σημείων ασφαλείας.
4) Καθιέρωση και διαχείριση ενός ενημερωμένου καταλόγου με στοιχεία τρίτων που χρησιμοποιούνται στην ανάπτυξη, ο οποίος πρέπει να περιλαμβάνει τυχόν κινδύνους που κάθε συστατικό τρίτου μέρους θα μπορούσε να προκαλέσει. Μηνιαία αξιολόγηση του καταλόγου για τυχόν αλλαγές ή ενημερώσεις σε αυτά τα συστατικά.
5) Χρήση ενημερωμένων και αξιόπιστων στοιχείων λογισμικού τρίτων κατασκευαστών.
6) Καθιέρωση και διατήρηση διαδικασίας αξιολόγησης της σοβαρότητας των τρωτών σημείων των εφαρμογών, η οποία διευκολύνει την ιεράρχηση των προτεραιοτήτων και τη σειρά με την οποία διορθώνονται οι ανακαλυφθείσες ευπάθειες, με τουλάχιστον ετήσια επανεξέταση.

7) Χρήση τυποποιημένων Hardening Configuration Templates, τα οποία περιλαμβάνουν servers, databases, web servers, cloud containers, Platform as a Service (PaaS) και Software as a Service (SaaS) στοιχεία.
8) Διατήρηση ξεχωριστών συστημάτων για περιβάλλοντα παραγωγής και μη παραγωγής.
9) Εκπαίδευση προγραμματιστών στην ασφάλεια εφαρμογών και την ανάπτυξη λογισμικού με συγγραφή ασφαλούς κώδικα.
10) Εφαρμογή αρχών ασφαλούς σχεδιασμού σε αρχιτεκτονικές εφαρμογών, ο οποίος περιλαμβάνει την έννοια των ελάχιστων προνομίων και την επιβολή διαμεσολάβησης για την επικύρωση κάθε λειτουργίας που πραγματοποιεί ο χρήστης.
11) Αξιοποίηση ελεγμένων υπηρεσιών για την ασφάλεια των εφαρμογών, όπως διαχείριση ταυτότητας, κρυπτογράφηση, έλεγχος και καταγραφή. Χρήση μόνο τυποποιημένων, αποδεκτών επί του παρόντος και εκτενώς αναθεωρημένους αλγόριθμους κρυπτογράφησης και μηχανισμούς των λειτουργικών συστημάτων για τη δημιουργία και τη διατήρηση ασφαλών αρχείων καταγραφής ελέγχου.

Το πλαίσιο, στο σημείο ελέγχου ασφάλειας εφαρμογών λογισμικού, θέτει δώδεκα (12) ερωτήματα:

1) Ο οργανισμός, διατηρεί μια ασφαλή διαδικασία ανάπτυξης εφαρμογών, κατά την οποία αντιμετωπίζονται στοιχεία όπως: πρότυπα σχεδιασμού εφαρμογών, πρακτικές κωδικοποίησης, εκπαίδευση προγραμματιστών, διαχείριση ευπαθειών, ασφάλεια σε κώδικα τρίτων και διαδικασίες δοκιμών ασφάλειας εφαρμογών, με τουλάχιστον ετήσια επανεξέταση;
2) Ο οργανισμός, έχει καθιερώσει μια διαδικασίας για την αποδοχή και αντιμετώπιση αναφορών για ευπάθειες λογισμικού, συμπεριλαμβανομένης της παροχής μέσων για την υποβολή αναφορών από εξωτερικές οντότητες;
3) Ο οργανισμός, αναλύει την αιτία των τρωτών σημείων ασφαλείας;
4) Ο οργανισμός, διασφαλίζει ότι στην ανάπτυξη διαδικτυακών εφαρμογών λαμβάνονται υπόψη κοινοί τύποι ευπαθειών, όπως για παράδειγμα OWASP Top-10;
5) Ο οργανισμός, έχει καθιερώσει και διαχειρίζεται έναν ενημερωμένο κατάλογο στοιχείων τρίτων που χρησιμοποιούνται στην ανάπτυξη, ο οποίος πρέπει να περιλαμβάνει τυχόν κινδύνους που θα μπορούσε να προκαλέσει κάθε συστατικό τρίτου μέρους;
6) Ο οργανισμός, χρησιμοποιεί ενημερωμένα και αξιόπιστα στοιχεία λογισμικού τρίτων κατασκευαστών;
7) Ο οργανισμός, διατηρεί διαδικασία αξιολόγησης της σοβαρότητας των τρωτών σημείων των εφαρμογών, η οποία διευκολύνει την ιεράρχηση των προτεραιοτήτων και τη σειρά με την οποία διορθώνονται οι ανακαλυφθείσες ευπάθειες, με τουλάχιστον ετήσια επανεξέταση;
8) Ο οργανισμός, χρησιμοποιεί τυποποιημένα Hardening Configuration Templates, τα οποία περιλαμβάνουν servers, databases, web servers, cloud containers, Platform as a Service (PaaS) και Software as a Service (SaaS) στοιχεία;
9) Ο οργανισμός, διατηρεί ξεχωριστά συστήματα για περιβάλλοντα παραγωγής και μη παραγωγής;
10) Ο οργανισμός, εκπαιδεύει τους προγραμματιστές στην ασφάλεια των εφαρμογών και στην ανάπτυξη λογισμικού με συγγραφή ασφαλούς κώδικα;
11) Ο οργανισμός, εφαρμόζει τις αρχές ασφαλούς σχεδιασμού σε αρχιτεκτονικές εφαρμογών, οι οποίες περιλαμβάνουν την έννοια των ελάχιστων προνομίων και την επιβολή διαμεσολάβησης για την επικύρωση κάθε λειτουργίας που πραγματοποιεί ο χρήστης;
12) Ο οργανισμός, αξιοποιεί ελεγμένες υπηρεσίες για την ασφάλεια των εφαρμογών, όπως διαχείριση ταυτότητας, κρυπτογράφηση, έλεγχος και καταγραφή; Χρησιμοποιεί μόνο τυποποιημένους, αποδεκτών επί του παρόντος και εκτενώς αναθεωρημένους αλγόριθμους κρυπτογράφησης και μηχανισμούς των λειτουργικών συστημάτων για τη δημιουργία και τη διατήρηση ασφαλών αρχείων καταγραφής ελέγχου;

5.15. Παρακολούθηση και άμυνα του δικτύου

Το σημείο ελέγχου παρακολούθησης και άμυνας του δικτύου, περιλαμβάνει τη λειτουργία διαδικασιών και εργαλείων για τη δημιουργία και τη διατήρηση ολοκληρωμένης παρακολούθησης και άμυνας του δικτύου έναντι απειλών ασφαλείας σε όλη την υποδομή δικτύου του οργανισμού. Οι λανθασμένες ρυθμίσεις, λόγω του ανθρώπινου λάθους ή έλλειψης γνώσης, δίνουν συχνά στους οργανισμούς λανθασμένη αίσθηση ασφάλειας. Δεν απαιτείται να δημιουργηθεί ένα Κέντρο Επιχειρήσεων Ασφαλείας (Security Operations Center - SOC) για να αποκτηθεί επίγνωση της κατάστασης. Αρκεί η κατανόηση των κρίσιμων επιχειρηματικών λειτουργιών, των αρχιτεκτονικών δικτύων και διακομιστών, των δεδομένων και των ροών δεδομένων, των υπηρεσιών και των συνδέσεων με τους επιχειρηματικούς εταίρους, τις συσκευές και τους λογαριασμούς των τελικών χρηστών. Αυτή η κατανόηση ενημερώνει αντίστοιχα την αρχιτεκτονικής ασφάλειας, τους τεχνικούς ελέγχους, την παρακολούθηση και τις διαδικασίες απόκρισης.

Η παρακολούθηση και η άμυνα του δικτύου περιλαμβάνει έξι (6) διασφαλίσεις:

1) Συγκεντρωτική ειδοποίηση συμβάντων ασφαλείας σε όλα τα περιουσιακά στοιχεία της επιχείρησης για συσχέτιση και ανάλυση αρχείων καταγραφής. Η βέλτιστη πρακτική εφαρμογή απαιτεί τη χρήση ενός Security Information Event Management (SIEM).
2) Ανάπτυξη λύσης ανίχνευσης εισβολών με βάση τον κεντρικό υπολογιστή σε επιχειρησιακά περιουσιακά στοιχεία.
3) Ανάπτυξη λύσης ανίχνευσης εισβολών μέσω δικτύου σε περιουσιακά στοιχεία του οργανισμού, όπως για παράδειγμα χρήση συστήματος ανίχνευσης εισβολών δικτύου (NIDS) ή ισοδύναμη υπηρεσία του παρόχου υπηρεσιών νέφους (Cloud Service Provider - CSP).
4) Διενέργεια φιλτραρίσματος κυκλοφορίας μεταξύ τμημάτων δικτύου.
5) Διαχείριση του ελέγχου πρόσβασης για περιουσιακά στοιχεία που συνδέονται εξ αποστάσεως σε επιχειρησιακούς πόρους. Καθορισμός της πρόσβασης στους επιχειρησιακούς πόρους με βάση: το ενημερωμένο εγκατεστημένο λογισμικό κατά του κακόβουλου λογισμικού, τη συμμόρφωση της διαμόρφωσης με τη διαδικασία ασφαλούς διαμόρφωσης του οργανισμού και τη διασφάλιση της επικαιροποίησης του λειτουργικού συστήματος και των εφαρμογών.
6) Συλλογή αρχείων καταγραφής ροής κίνησης δικτύου.

Το πλαίσιο, στο σημείο ελέγχου παρακολούθησης και άμυνας του δικτύου, θέτει επτά (7) ερωτήματα:

1) Ο οργανισμός, διαθέτει συγκεντρωτική ειδοποίηση συμβάντων ασφαλείας σε όλα τα περιουσιακά στοιχεία της επιχείρησης για συσχέτιση και ανάλυση αρχείων καταγραφής;
2) Ο οργανισμός, έχει αναπτύξει λύση ανίχνευσης εισβολών σε επιχειρησιακά περιουσιακά στοιχεία βάσει του κεντρικού υπολογιστή (Host-Based Intrusion Detection Solution);
3) Ο οργανισμός, έχει αναπτύξει λύση ανίχνευσης εισβολών μέσω δικτύου σε περιουσιακά στοιχεία του οργανισμού, όπως για παράδειγμα, χρήση συστήματος ανίχνευσης εισβολών δικτύου (Network Intrusion Detection System - NIDS) ή ισοδύναμη υπηρεσία του Cloud Service Provider (CSP);
4) Ο οργανισμός, διενεργεί φιλτράρισμα της κυκλοφορίας μεταξύ τμημάτων δικτύου;
5) Ο οργανισμός, διαθέτει διαδικασία για την διαχείριση του ελέγχου πρόσβασης των περιουσιακών στοιχείων που συνδέονται εξ' αποστάσεως σε επιχειρησιακούς πόρους;
6) Ο οργανισμός, επιτρέπει την πρόσβαση στους επιχειρησιακούς πόρους με βάση το ενημερωμένο εγκατεστημένο λογισμικό κατά του κακόβουλου λογισμικού, τη συμμόρφωση με την ασφαλή διαμόρφωση και τη διασφάλιση της επικαιροποίησης του λειτουργικού συστήματος και των εφαρμογών;
7) Ο οργανισμός, συλλέγει αρχεία καταγραφής ροής κίνησης δικτύου;

5.16. Εκπαίδευση και ενημέρωση για την ασφάλεια

Η εκπαίδευση και ενημέρωση για την ασφάλεια, περιλαμβάνει την καθιέρωση και διατήρηση προγράμματος ευαισθητοποίησης σε θέματα ασφάλειας για να επηρεάσει τη συμπεριφορά του εργατικού δυναμικού έτσι, ώστε να είναι συνειδητοποιημένο και κατάλληλα καταρτισμένο, με αποτέλεσμα τη μείωση των κινδύνων κυβερνοασφάλειας για τον οργανισμό. Η συμπεριφορά και οι ενέργειες των ανθρώπων διαδραματίζουν κρίσιμο ρόλο στην επιτυχία ή την αποτυχία του προγράμματος ασφάλειας ενός οργανισμού. Για έναν εισβολέα είναι ευκολότερο να παρακάμψει την ασφάλεια μέσω του ανθρώπου, όπως για παράδειγμα, να τον πείσει να κάνει κλικ σε έναν σύνδεσμο ή να ανοίξει ένα συνημμένο email, με αποτέλεσμα την εγκατάσταση κακόβουλου λογισμικού προκειμένου να εισέλθει σε έναν οργανισμό, παρά να βρει ένα exploit δικτύου. Επίσης, οι χρήστες τόσο εκούσια όσο και ακούσια, μπορούν να προκαλέσουν περιστατικά, όπως για παράδειγμα ο κακός χειρισμός δηλαδή στέλνοντας ένα μήνυμα ηλεκτρονικού ταχυδρομείου με ευαίσθητα δεδομένα σε λάθος παραλήπτη ή η απώλεια μιας φορητής συσκευής τελικού χρήστη ή η χρήση αδύναμων κωδικών πρόσβασης και άλλα. Ο ανθρώπινος παράγοντας αποτελεί ευπάθεια στον οργανισμό και για το λόγο αυτό η εκπαίδευση θα πρέπει να επικαιροποιείται τακτικά.

Ένα αποτελεσματικό εκπαιδευτικό πρόγραμμα ευαισθητοποίησης σε θέματα ασφάλειας, δεν θα πρέπει να είναι απλώς ένα εκπαιδευτικό βίντεο που προβάλλεται μία φορά το χρόνο σε συνδυασμό με τακτικές δοκιμές τύπου phishing. Η ετήσια εκπαίδευση είναι απαραίτητη, αλλά παράλληλα θα πρέπει να υπάρχουν πιο συχνά, επίκαιρα μηνύματα και ειδοποιήσεις σχετικά με την ασφάλεια. Αυτό, μπορεί να περιλαμβάνει μηνύματα σχετικά με την ισχυρή χρήση κωδικών πρόσβασης, την αύξηση του phishing κατά την περίοδο της φορολογίας ή την αυξημένη ευαισθητοποίηση σχετικά με τα κακόβουλα μηνύματα ηλεκτρονικού ταχυδρομείου παράδοσης πακέτων κατά τη διάρκεια των διακοπών. Η εκπαίδευση θα πρέπει επίσης να λαμβάνει υπόψη τον διαφορετικό τύπο του οργανισμού, τους διάφορους ρόλους των υπαλλήλων, τις αρμοδιότητες τους και τα δικαιώματα τους στα συστήματα. Η εκπαίδευση σε θέματα social engineering, όπως οι δοκιμές phishing, θα πρέπει επίσης να περιλαμβάνει ευαισθητοποίηση των τακτικών που στοχεύουν σε διαφορετικούς ρόλους.

Η εκπαίδευση και ενημέρωση για την ασφάλεια περιλαμβάνει δέκα (10) διασφαλίσεις:

1) Καθιέρωση και διατήρηση προγράμματος ευαισθητοποίησης σε θέματα ασφάλειας, με σκοπό την εκπαίδευση του συνόλου του προσωπικού του οργανισμού, σχετικά με τον ασφαλή τρόπο που αλληλοεπιδρούν με τα περιουσιακά στοιχεία και τα δεδομένα του οργανισμού. Επανεξέταση και επικαιροποίηση τουλάχιστον ετησίως.
2) Εκπαίδευση των υπαλλήλων για την αναγνώριση επιθέσεων social engineering, όπως το phishing, το pre-texting και το tailgating.
3) Εκπαίδευση των υπαλλήλων στις βέλτιστες πρακτικές αυθεντικοποίησης, όπως για παράδειγμα MFA, σύνθεση κωδικών πρόσβασης και διαχείριση διαπιστευτηρίων.
4) Εκπαίδευση των υπαλλήλων στις βέλτιστες πρακτικές χειρισμού δεδομένων, στην ορθή αποθήκευση, μεταφορά, αρχειοθέτηση και καταστροφή ευαίσθητων δεδομένων και στις βέλτιστες πρακτικές καθαρής οθόνης και γραφείου, όπως το κλείδωμα της οθόνης τους όταν απομακρύνονται από το επιχειρησιακό μέσο, τη διαγραφή φυσικών και εικονικών πινάκων στο τέλος των συσκέψεων και την ασφαλή αποθήκευση δεδομένων και περιουσιακών στοιχείων.
5) Εκπαίδευση των υπαλλήλων για τις αιτίες ακούσιας έκθεσης δεδομένων, όπως για παράδειγμα η εσφαλμένη παράδοση ευαίσθητων δεδομένων, η απώλεια μιας φορητής συσκευής τελικού χρήστη ή η δημοσίευση δεδομένων σε μη προβλεπόμενο κοινό.
6) Εκπαίδευση των υπαλλήλων στην αναγνώριση και αναφορά περιστατικών ασφαλείας.
7) Εκπαίδευση των υπαλλήλων για τον τρόπο αναγνώρισης και την αναφορά επιχειρησιακών περιουσιακών στοιχείων που στερούνται ενημερώσεων ασφαλείας.
8) Εκπαίδευση των υπαλλήλων σχετικά με τους κινδύνους της σύνδεσης και μετάδοσης επιχειρησιακών δεδομένων μέσω μη ασφαλών δικτύων.

9) Διεξαγωγή ευαισθητοποίησης σε θέματα ασφάλειας για κάθε ρόλο και εκπαίδευση σε δεξιότητες.
10) Εκπαίδευση των υπαλλήλων για την σημασία των πολιτικών ασφαλείας, των διαδικασιών και των τεχνικών μέτρων.

Το πλαίσιο, στο σημείο ελέγχου εκπαίδευσης και ενημέρωσης για την ασφάλεια, θέτει δεκατέσσερα (14) ερωτήματα:

1) Ο οργανισμός, διαθέτει καταγεγραμμένη πολιτική και διαδικασίες υλοποίησης που αφορούν την εκπαίδευση των υπαλλήλων σε θέματα κυβερνοασφάλειας;
2) Ο οργανισμός, έχει καθιερώσει και διατηρεί ένα πρόγραμμα ευαισθητοποίησης σε θέματα ασφάλειας, με σκοπό την εκπαίδευση του συνόλου του προσωπικού του οργανισμού, σχετικά με τον ασφαλή τρόπο που αλληλοεπιδρούν με τα περιουσιακά στοιχεία και τα δεδομένα του, το οποίο επανεξετάζεται και επικαιροποιείται τουλάχιστον ετησίως;
3) Ο οργανισμός, εκπαιδεύει και ενημερώνει τους υπαλλήλους για την αναγνώριση επιθέσεων social engineering, όπως το phishing, το pre-texting και το tailgating;
4) Ο οργανισμός, εκπαιδεύει τους υπαλλήλους στις βέλτιστες πρακτικές αυθεντικοποίησης, όπως για παράδειγμα MFA, σύνθεση κωδικών πρόσβασης και διαχείριση διαπιστευτηρίων;
5) Ο οργανισμός, εκπαιδεύει τους υπαλλήλους στις βέλτιστες πρακτικές χειρισμού δεδομένων, όπως η ορθή αποθήκευση, μεταφορά, αρχειοθέτηση και καταστροφή ευαίσθητων δεδομένων και στις βέλτιστες πρακτικές καθαρής οθόνης και καθαρού γραφείου, καθώς επίσης και στην ασφαλή αποθήκευση των περιουσιακών στοιχείων;
6) Ο οργανισμός, εκπαιδεύει τους υπαλλήλους για τις αιτίες ακούσιας έκθεσης δεδομένων, όπως για παράδειγμα η εσφαλμένη παράδοση ευαίσθητων δεδομένων, η απώλεια μιας φορητής συσκευής τελικού χρήστη ή η δημοσίευση δεδομένων σε μη προβλεπόμενο κοινό;
7) Ο οργανισμός, εκπαιδεύει τους υπαλλήλους στην αναγνώριση και αναφορά περιστατικών ασφαλείας;
8) Ο οργανισμός, εκπαιδεύει τους υπαλλήλους στον τρόπο αναγνώρισης και αναφοράς επιχειρησιακών περιουσιακών στοιχείων που στερούνται ενημερώσεων ασφαλείας;
9) Ο οργανισμός, ενημερώνει τους υπαλλήλους σχετικά με τους κινδύνους της σύνδεσης και μετάδοσης επιχειρησιακών δεδομένων μέσω μη ασφαλών δικτύων;
10) Ο οργανισμός, διεξάγει ευαισθητοποίηση σε θέματα ασφάλειας και εκπαίδευση σε δεξιότητες για κάθε ρόλο;
11) Ο οργανισμός, εκπαιδεύει τους υπαλλήλους για την σημασία των πολιτικών ασφαλείας, των διαδικασιών και των τεχνικών μέτρων;
12) Ο οργανισμός, διενεργεί σε περιοδική βάση ασκήσεις προσομοίωσης περιστατικών κυβερνοασφάλειας όπως για παράδειγμα phishing mail;
13) Ο οργανισμός, επικοινωνεί τις πολιτικές ασφαλείας, τις διαδικασίες και τους κανόνες στους υπαλλήλους, στους συνεργάτες και σε όλα τα ενδιαφερόμενα μέρη;
14) Ο οργανισμός, εκπαιδεύει τους υπαλλήλους στις πολιτικές ασφαλείας, στις διαδικασίες και στους κανόνες του οργανισμού;

5.17. Αντίγραφα ασφαλείας & ανάκτηση δεδομένων

Το σημείο ελέγχου των αντιγράφων ασφαλείας και της ανάκτησης των δεδομένων, περιλαμβάνει την καθιέρωση και διατήρηση επαρκών πρακτικών ανάκτησης δεδομένων για την αποκατάσταση των επιχειρησιακών περιουσιακών στοιχείων. Οι κακόβουλες ενέργειες ή το ανθρώπινο λάθος μπορεί να προκαλέσουν απώλεια των δεδομένων. Έτσι είναι σημαντικό να υπάρχουν πρόσφατα αντίγραφα ασφαλείας για την ανάκτηση των περιουσιακών στοιχείων και δεδομένων του οργανισμού, σε μια γνωστή αξιόπιστη κατάσταση. Η διαδικασία ανάκτησης δεδομένων πρέπει να ορίζεται και να περιλαμβάνει την δημιουργία των αντιγράφων ασφαλείας βάσει της αξίας των δεδομένων, την ευαισθησία

και τις απαιτήσεις διατήρησης, την δοκιμή και την αξιολόγηση σε ένα τυχαίο δείγμα για αποκατάσταση και την επαλήθευση ότι το λειτουργικό, οι εφαρμογές και τα δεδομένα είναι άθικτα.

Τα αντίγραφα ασφαλείας και η ανάκτηση των δεδομένων περιλαμβάνουν πέντε (5) διασφαλίσεις:

1) Καθιέρωση και διατήρηση μιας διαδικασίας ανάκτησης δεδομένων, με τουλάχιστον εξαμηνιαία επανεξέταση.
2) Εκτέλεση αυτοματοποιημένων διαδικασιών αντίγραφών ασφαλείας, με τουλάχιστον ημερήσια συχνότητα, ανάλογα με την ευαισθησία των δεδομένων.
3) Προστασία των αντιγράφων ασφαλείας με ελέγχους ισοδύναμους με τους ελέγχους των αρχικών δεδομένων, όπως για παράδειγμα κρυπτογράφηση.
4) Δημιουργία και διατήρηση απομονωμένων αντιγράφων ασφαλείας, όπως για παράδειγμα μέσω συστημάτων ή υπηρεσιών εκτός σύνδεσης, νέφους ή εκτός τοποθεσίας.
5) Έλεγχος ακεραιότητας των αντιγράφων ασφαλείας σε περιοδική βάση.
6) Δοκιμή ανάκτησης δεδομένων από τα αντίγραφα ασφαλείας τουλάχιστον ανά τρίμηνο.

Το πλαίσιο, στο σημείο ελέγχου των αντιγράφων ασφαλείας και της ανάκτησης των δεδομένων, θέτει δώδεκα (12) ερωτήματα:

1) Ο οργανισμός, διαθέτει καταγεγραμμένη πολιτική και διαδικασίες υλοποίησης σχετικά με τα αντίγραφα ασφαλείας και την ανάκτηση των δεδομένων;
2) Ο οργανισμός, καθιέρωσε και διατηρεί μια διαδικασία ανάκτησης δεδομένων, με τουλάχιστον εξαμηνιαία επανεξέταση;
3) Ο οργανισμός, εκτελεί αυτοματοποιημένη διαδικασία αντίγραφών ασφαλείας, με τουλάχιστον ημερήσια συχνότητα στα κρίσιμα και ευαίσθητα δεδομένα;
4) Ο οργανισμός, συνδυάζει με τον κατάλληλο τρόπο τις τεχνολογίες Full, Incremental και Differential Backup;
5) Ο οργανισμός, προστατεύει τα αντίγραφα ασφαλείας με ελέγχους ισοδύναμους με τους ελέγχους των αρχικών δεδομένων, όπως για παράδειγμα κρυπτογράφηση, φυσική ασφάλεια, administrative credentials και άλλους;
6) Ο οργανισμός, διασφαλίζει την ολοκλήρωση των διαδικασιών αντιγράφων ασφαλείας, όπως για παράδειγμα με την ειδοποίηση μέσω email για επιτυχή ή ανεπιτυχή ολοκλήρωση των αντιγράφων ασφαλείας;
7) Ο οργανισμός, διασφαλίζει ότι το λογισμικό και το υλικό που αποτελεί το σύστημα αντιγράφων ασφαλείας ενημερώνεται σύμφωνα με τις τελευταίες αναβαθμίσεις που παρέχονται από τους κατασκευαστές του;
8) Ο οργανισμός, δημιουργεί και διατηρεί απομονωμένα αντίγραφα ασφαλείας, όπως για παράδειγμα μέσω συστημάτων ή υπηρεσιών εκτός σύνδεσης, νέφους ή εκτός τοποθεσίας;
9) Ο οργανισμός, διασφαλίζει ότι το αντίγραφο ασφαλείας είναι ίδιο με το πρωτότυπο αρχείο;
10) Ο οργανισμός, διενεργεί δοκιμή ανάκτησης δεδομένων από τα αντίγραφα ασφαλείας τουλάχιστον ανά τρίμηνο;
11) Ο οργανισμός, διατηρεί αρχείο από τους ελέγχους για την ορθή λειτουργία και την κατάσταση του συστήματος αντιγράφων ασφαλείας;
12) Ο οργανισμός, τηρεί τον κανόνα αντιγράφων ασφαλείας 3-2-1-1-0;

5.18. Διαχείριση αντιμετώπισης περιστατικών

Η διαχείριση αντιμετώπισης περιστατικών κυβερνοασφάλειας, αναφέρεται στο σύνολο των πολιτικών, διαδικασιών και μέτρων που εφαρμόζονται από τον οργανισμό για την αντιμετώπιση, αποτροπή και ανάκτηση από τις κυβερνοεπιθέσεις και τις κυβερνοαπειλές. Το σημείο ελέγχου διαχείρισης της αντιμετώπισης περιστατικών, περιλαμβάνει την καθιέρωση προγράμματος για την ανάπτυξη και τη

διατήρηση της ικανότητας αντιμετώπισης ενός συμβάντος που περιλαμβάνει πολιτικές, σχέδια, διαδικασίες, καθορισμένους ρόλους, εκπαίδευση και επικοινωνία, δηλαδή την προετοιμασία, τον εντοπισμό και την γρήγορη ανταπόκριση σε ένα συμβάν ασφαλείας (π.χ. επίθεση). Ένα ολοκληρωμένο πρόγραμμα κυβερνοασφάλειας περιλαμβάνει προστασία, εντοπισμό, αντίδραση, και δυνατότητες ανάκτησης.

Όταν ένα περιστατικό συμβεί, είναι αδύνατον οι άνθρωποι του οργανισμού να γνωρίζουν τις σωστές διαδικασίες διερεύνησης, αναφοράς και συλλογής δεδομένων, τα νομικά ζητήματα και τις ρυθμιστικές αρχές, τους ρόλους των προσώπων που θα συμμετέχουν και τη στρατηγική επικοινωνίας, ώστε να διαχειριστούν το συμβάν και να ανακάμψουν με επιτυχία. Η ομάδα αντιμετώπισης περιστατικών, πρέπει να συμμετέχει σε περιοδική εκπαίδευση βάσει σεναρίων, διεκπεραιώνοντας μια σειρά από σενάρια επίθεσης, προσαρμοσμένων στις απειλές και τις πιθανές επιπτώσεις που αντιμετωπίζει ο οργανισμός. Τα σενάρια αυτά, βοηθούν την ομάδα να κατανοήσει το ρόλο της στη διαδικασία αντιμετώπισης περιστατικών και επιπλέον, εντοπίζει τα κενά στα σχέδια και τις διαδικασίες, καθώς στη συνέχεια μπορεί να επικαιροποιήσει το σχέδιο.

Η διαχείριση αντιμετώπισης περιστατικών περιλαμβάνει οκτώ (8) διασφαλίσεις:

1) Ορισμός ρόλων για τη διαχείριση του χειρισμού περιστατικών.
2) Καθιέρωση και διατήρηση στοιχείων επικοινωνίας για την υποβολή εκθέσεων περιστατικών ασφαλείας.
3) Καθιέρωση και διατήρηση μιας επιχειρησιακής διαδικασίας για την αναφορά συμβάντων.
4) Καθιέρωση και διατήρηση μιας διαδικασίας αντιμετώπισης περιστατικών, η οποία αφορά ρόλους και αρμοδιότητες, απαιτήσεις συμμόρφωσης, καθώς και ένα σχέδιο επικοινωνίας, με τουλάχιστον ετήσια επανεξέταση.
5) Καθορισμός βασικών ρόλων και αρμοδιοτήτων για την αντιμετώπιση περιστατικών, συμπεριλαμβανομένου προσωπικού από το νομικό τμήμα, το τμήμα πληροφορικής, της ασφάλειας πληροφοριών, τις εγκαταστάσεις, τις δημόσιες σχέσεις, το ανθρώπινο δυναμικό, τους ανταποκριτές συμβάντων και τους αναλυτές. Τουλάχιστον, ετήσια επανεξέταση.
6) Καθορισμός μηχανισμών επικοινωνίας κατά τη διάρκεια της αντιμετώπισης περιστατικών, με ετήσια επανεξέταση.
7) Σχεδιασμός και διεξαγωγή ασκήσεων και σεναρίων αντιμετώπισης συμβάντων ρουτίνας, για το βασικό προσωπικό που εμπλέκεται στο συμβάν ώστε να προετοιμαστούν για την αντιμετώπιση πραγματικών περιστατικών, με δοκιμές σε ετήσια βάση.
8) Διεξαγωγή ανασκοπήσεων μετά το συμβάν, οι οποίες συμβάλλουν στην πρόληψη της επανάληψης του συμβάντος μέσω του εντοπισμού των διδαγμάτων και της δράσης παρακολούθησης.

Το πλαίσιο, στο σημείο ελέγχου διατήρησης και αντιμετώπισης περιστατικών, θέτει εννέα (9) ερωτήματα:

1) Ο οργανισμός, διαθέτει καταγεγραμμένη πολιτική για την αντιμετώπιση περιστατικών κυβερνοασφάλειας;
2) Ο οργανισμός, έχει ορίσει ρόλους για τη διαχείριση του χειρισμού περιστατικών;
3) Ο οργανισμός, έχει καθορίσει βασικούς ρόλους και αρμοδιότητες για την αντιμετώπιση περιστατικών, συμπεριλαμβανομένου προσωπικού από το νομικό τμήμα, το τμήμα πληροφορικής, της ασφάλειας πληροφοριών, τις εγκαταστάσεις, τις δημόσιες σχέσεις, το ανθρώπινο δυναμικό και άλλους, με τουλάχιστον ετήσια επανεξέταση;
4) Ο οργανισμός, έχει καθιερώσει και διατηρεί στοιχεία επικοινωνίας για την υποβολή εκθέσεων περιστατικών ασφαλείας;
5) Ο οργανισμός, έχει καθιερώσει και διατηρεί μια επιχειρησιακή διαδικασίας για την αναφορά συμβάντων;

6) Ο οργανισμός, έχει καθιερώσει και διατηρεί μια διαδικασία αντιμετώπισης περιστατικών που αφορά ρόλους και αρμοδιότητες, απαιτήσεις συμμόρφωσης, καθώς και ένα σχέδιο επικοινωνίας, με τουλάχιστον ετήσια επανεξέταση;
7) Ο οργανισμός, έχει καθορίσει τους μηχανισμούς επικοινωνίας κατά τη διάρκεια της αντιμετώπισης περιστατικών, με ετήσια επανεξέταση;
8) Ο οργανισμός, έχει σχεδιάσει και διεξάγει ασκήσεις και σενάρια αντιμετώπισης συμβάντων για το βασικό προσωπικό που εμπλέκεται στο συμβάν ώστε να προετοιμαστεί για την αντιμετώπιση πραγματικών περιστατικών, με δοκιμές σε ετήσια βάση;
9) Ο οργανισμός, διεξάγει ανασκοπήσεις μετά το συμβάν, οι οποίες συμβάλλουν στην πρόληψη της επανάληψης του συμβάντος μέσω του εντοπισμού των διδαγμάτων και της δράσης παρακολούθησης;

5.19. Δοκιμές διείσδυσης

Το σημείο ελέγχου των δοκιμών διείσδυσης (Penetration Testing – PenTest), περιλαμβάνει την δοκιμή της αποτελεσματικότητας και της ανθεκτικότητας των περιουσιακών στοιχείων του οργανισμού μέσω του εντοπισμού και της εκμετάλλευση των αδυναμιών του, κατά τους ελέγχους και την προσομοίωση των στόχων και των ενεργειών ενός επιτιθέμενου. Η δοκιμή διείσδυσης, μπορεί να είναι από εξωτερικό δίκτυο, εσωτερικό δίκτυο, εφαρμογή, σύστημα ή συσκευή, καθώς επίσης, μπορεί να περιλαμβάνει social engineering των χρηστών ή ακόμη και φυσική πρόσβαση για την παράκαμψη του ελέγχου. Αυτές οι δοκιμές, παρέχουν πολύτιμες πληροφορίες σχετικά με την ύπαρξη τρωτών σημείων στα περιουσιακά στοιχεία του οργανισμού και στον ανθρώπινο παράγοντα. Ελέγχουν την αποτελεσματικότητα της άμυνας και αποκαλύπτουν αδυναμίες των διαδικασιών.

Ένας έλεγχος τρωτότητας, απλώς ελέγχει την παρουσία γνωστών, μη ασφαλών περιουσιακών στοιχείων του οργανισμού και σταματάει. Οι δοκιμές ευπάθειας, είναι αυτοματοποιημένη σάρωση και μερικές φορές χειροκίνητη επικύρωση των ψευδώς θετικών αποτελεσμάτων. Ενώ, ο έλεγχος διείσδυσης προχωράει και εκμεταλλεύεται τις αδυναμίες ώστε να αποκαλύψει σε ποιο βαθμό ένας εισβολέας μπορεί να φτάσει και ποιες επιχειρηματικές διαδικασίες ή δεδομένα θα επηρεαστούν μέσω της εκμετάλλευσης της ευπάθειας. Ο έλεγχος διείσδυσης, απαιτεί μεγαλύτερη ανθρώπινη συμμετοχή και ανάλυση, υποστηρίζεται με τη χρήση προσαρμοσμένων εργαλείων ή σεναρίων. Οι δοκιμές διείσδυσης, είναι δαπανηρές, πολύπλοκες και δυνητικά ενέχουν τους δικούς τους κινδύνους, λόγω αυτού πρέπει να διεξάγονται από έμπειρους ανθρώπους ή αξιόπιστους συνεργάτες. Ο οργανισμός, πρέπει να καθορίσει ένα σαφές πεδίο εφαρμογής και τους κανόνες εμπλοκής για τις δοκιμές διείσδυσης.

Οι δοκιμές διείσδυσης περιλαμβάνουν τέσσερις (4) διασφαλίσεις:

1) Καθιέρωση και διατήρηση ενός προγράμματος δοκιμών διείσδυσης, κατάλληλου για το μέγεθος, την πολυπλοκότητα και την ωριμότητα του οργανισμού.
2) Εκτέλεση περιοδικών δοκιμών εξωτερικής διείσδυσης, βάσει των απαιτήσεων του προγράμματος, τουλάχιστον ετησίως.
3) Απαίτηση εξειδικευμένης δεξιότητας και εμπειρίας, δηλαδή πρέπει να διεξάγονται μέσω ειδικευμένου ανθρώπου ή φορέα.
4) Αποκατάσταση των ευρημάτων της δοκιμής διείσδυσης, βάσει της πολιτικής του οργανισμού για το εύρος και την ιεράρχηση της αποκατάστασης.

Το πλαίσιο, στο σημείο ελέγχου των δοκιμών διείσδυσης, θέτει τέσσερα (4) ερωτήματα:

1) Ο οργανισμός, έχει καθιερώσει και διατηρεί ένα πρόγραμμα δοκιμών διείσδυσης (Penetration Testing – PenTest), κατάλληλο για το μέγεθος, την πολυπλοκότητα και την ωριμότητα του οργανισμού;

2) Ο οργανισμός, εκτελεί περιοδικές δοκιμές εξωτερικής διείσδυσης, βάσει των απαιτήσεων του προγράμματος, τουλάχιστον ετησίως;
3) Ο οργανισμός, απαιτεί εξειδικευμένη δεξιότητα και εμπειρία του ανθρώπου ή του φορέα που εκτελεί το PenTest;
4) Ο οργανισμός, διαθέτει διαδικασία αποκατάσταση των ευρημάτων των PenTests, βάσει της πολιτικής του οργανισμού για το εύρος και την ιεράρχηση της αποκατάστασης;

5.20. Συνεχής διαχείριση ευπαθειών

Το σημείο ελέγχου της συνεχής διαχείρισης των ευπαθειών, περιλαμβάνει την ανάπτυξη σχεδίου για τη συνεχή αξιολόγηση και παρακολούθηση των τρωτών σημείων σε όλα τα περιουσιακά στοιχεία του οργανισμού, προκειμένου να αποκατασταθεί και να ελαχιστοποιηθεί η ευκαιρία για τους επιτιθέμενους. Ο οργανισμός, πρέπει να έχει στη διάθεση του ενημερώσεις λογισμικού, επιδιορθώσεις, συμβουλές ασφαλείας, δελτία απειλών, βέλτιστες πρακτικές και άλλα. Επίσης, πρέπει να επανεξετάζει τακτικά το περιβάλλον του για τον εντοπισμό τρωτών σημείων. Η κατανόηση και η διαχείριση των ευπαθειών είναι μια συνεχής δραστηριότητα ώστε ο οργανισμός να μην εκτεθεί σε κίνδυνο. Η χρήση εργαλείων σάρωσης τρωτών σημείων είναι αναγκαία.

Η συνεχής διαχείριση των ευπαθειών περιλαμβάνει επτά (7) διασφαλίσεις:

1) Καθιέρωση και διατήρηση μιας τεκμηριωμένης διαδικασίας διαχείρισης τρωτών σημείων. Επανεξέταση τουλάχιστον εξαμηνιαίως.
2) Καθιέρωση και διατήρηση μιας τεκμηριωμένης στρατηγικής αποκατάστασης με βάση τον κίνδυνο.
3) Αυτοματοποιημένη διαχείριση ενημερώσεων και διορθώσεων των λειτουργικών συστημάτων, τουλάχιστον σε μηνιαία βάση.
4) Αυτοματοποιημένη διαχείριση ενημερώσεων και διορθώσεων εφαρμογών, τουλάχιστον σε μηνιαία βάση.
5) Αυτοματοποιημένες σαρώσεις τρωτότητας των εσωτερικών επιχειρησιακών περιουσιακών στοιχείων, τουλάχιστον σε τριμηνιαία βάση.
6) Αυτοματοποιημένες σαρώσεις τρωτότητας των εξωτερικών εκτεθειμένων επιχειρησιακών περιουσιακών στοιχείων, τουλάχιστον σε μηνιαία βάση.
7) Αποκατάσταση των εντοπισμένων ευπαθειών στο λογισμικό μέσω διαδικασιών και εργαλείων.

Το πλαίσιο, στο σημείο ελέγχου της συνεχής διαχείρισης των ευπαθειών, θέτει επτά (7) ερωτήματα:

1) Ο οργανισμός, έχει καθιερώσει και διατηρεί μια τεκμηριωμένη διαδικασία διαχείρισης τρωτών σημείων, με τουλάχιστον εξαμηνιαία επανεξέταση;
2) Ο οργανισμός, έχει καθιερώσει και διατηρεί μια τεκμηριωμένη στρατηγική αποκατάστασης βάσει κινδύνου;
3) Ο οργανισμός, εφαρμόζει αυτοματοποιημένη διαχείριση ενημερώσεων και διορθώσεων των λειτουργικών συστημάτων, τουλάχιστον σε μηνιαία βάση;
4) Ο οργανισμός, εφαρμόζει αυτοματοποιημένη διαχείριση ενημερώσεων και διορθώσεων εφαρμογών, τουλάχιστον σε μηνιαία βάση;
5) Ο οργανισμός, εφαρμόζει αυτοματοποιημένες σαρώσεις τρωτότητας των εσωτερικών επιχειρησιακών περιουσιακών στοιχείων, τουλάχιστον σε τριμηνιαία βάση;
6) Ο οργανισμός, εφαρμόζει αυτοματοποιημένες σαρώσεις τρωτότητας των εξωτερικών εκτεθειμένων επιχειρησιακών περιουσιακών στοιχείων, τουλάχιστον σε μηνιαία βάση;
7) Ο οργανισμός, διαθέτει διαδικασία και εργαλεία για την αποκατάστασης των εντοπισμένων ευπαθειών στο λογισμικό;

5.21. Φυσική ασφάλεια

Το σημείο ελέγχου της φυσικής ασφάλειας, περιλαμβάνει ολόκληρη την περιβαλλοντική προστασία του πληροφοριακού συστήματος από απειλές. Η φυσική προστασία των συστημάτων πρέπει να λαμβάνεται υπόψη ώστε στο χώρο να μην εισέρχονται μη εξουσιοδοτημένα άτομα που μπορεί να έχουν κακόβουλο σκοπό, όπως για παράδειγμα, κλοπή συσκευών ή μόλυνση συστημάτων ή κλοπή δεδομένων και άλλα. Επίσης, πρέπει να λαμβάνεται υπόψη η ακούσια συμπεριφορά εξουσιοδοτημένων ατόμων. Ο οργανισμός, είναι απαραίτητο να εφαρμόζει μέτρα άρνησης πρόσβασης στις εγκαταστάσεις του, στον εξοπλισμό του και στους πόρους του από μη εξουσιοδοτημένα άτομα. Επίσης, τα φυσικά μέτρα ασφάλειας λαμβάνονται για την αποτροπή και την ανίχνευσης μιας πιθανής εισβολής. Ο περιορισμός και ο έλεγχος πρόσβασης στις εγκαταστάσεις, στον εξοπλισμό, σε κρίσιμο εξοπλισμό όπως computer room και σε ευάλωτες συσκευές όπως φορητές συσκευές και αποθηκευτικά μέσα είναι απαραίτητος.

Η φυσική ασφάλεια περιλαμβάνει επτά (7) διασφαλίσεις:

1) Καθιέρωση και διατήρηση μιας τεκμηριωμένης διαδικασίας διαχείρισης της περιβαλλοντικής ασφάλειας.
2) Καθιέρωση ειδικών κανόνων και μέτρων για τη διαχείρισης της ασφάλειας των κρίσιμων εγκαταστάσεων (πχ computer room).
3) Διατήρηση διαδικασίας ελέγχου φυσικής πρόσβασης.
4) Προστασία ευάλωτων συσκευών όπως φορητοί υπολογιστές, usb flash memory.
5) Πλεονασμός σε κρίσιμα δικτυακά συστήματα.
6) Αδιάλειπτη παροχή ενέργειας σε κρίσιμα συστήματα (πχ server).
7) Εφαρμογή ελεγκτών, για ανίχνευση πυρκαγιάς, διαρροή νερού, θερμοκρασίας, υγρασίας και πίεσης στον χώρο όπου φιλοξενείται κρίσιμος εξοπλισμός, όπως για παράδειγμα το computer room.

Το πλαίσιο, στο σημείο ελέγχου της φυσικής ασφάλειας, θέτει δεκατέσσερα (14) ερωτήματα:

1) Ο οργανισμός, έχει καθιερώσει και διατηρεί μια διαδικασία διαχείρισης της περιβαλλοντικής ασφάλειας;
2) Ο οργανισμός, έχει καθιερώσει ειδικούς κανόνες για την διαχείριση της ασφάλειας των κρίσιμων εγκαταστάσεων, όπως για παράδειγμα στο computer room;
3) Ο οργανισμός, έχει διασφαλίσει ότι οι κρίσιμες εγκαταστάσεις (πχ computer room) διαθέτουν μηχανισμούς ελέγχου για την προστασία από μη εξουσιοδοτημένη πρόσβαση, όπως για παράδειγμα κλειδαριές ή συναγερμό;
4) Ο οργανισμός, τηρεί κατάλογο των εξουσιοδοτημένων ατόμων με πρόσβαση στον κρίσιμο εξοπλισμό ή στον χώρο που φιλοξενείται ο κρίσιμος εξοπλισμός;
5) Ο οργανισμός, εφαρμόζει διαδικασία για ελεγχόμενη πρόσβαση των επισκεπτών στις εγκαταστάσεις του, όπως για παράδειγμα, ένας χώρος υποδοχής και συνοδεία από εξουσιοδοτημένο άτομο για την πρόσβαση στους εσωτερικούς χώρους των εγκαταστάσεων;
6) Ο οργανισμός, καταγράφει τους επισκέπτες που αποκτούν πρόσβαση στις εγκαταστάσεις;
7) Ο οργανισμός, καταγράφει κάθε είσοδο σε χώρους με κρίσιμο εξοπλισμό, όπως για παράδειγμα, την είσοδο για τεχνική συντήρηση ή βλάβη ή καθαριότητα, καθώς επίσης και την απομακρυσμένη πρόσβαση στον κρίσιμο εξοπλισμό;
8) Ο οργανισμός, διαθέτει σύστημα Uninterruptible Power Supply (UPS), για την αδιάλειπτη παροχή ρεύματος του κρίσιμου εξοπλισμού;
9) Ο οργανισμός, διαθέτει σύστημα πυρανίχνευσης και πυρόσβεσης;
10) Ο οργανισμός, διαθέτει αυτοματοποιημένους ελεγκτές θερμοκρασίας, υγρασία και πίεσης στις εγκαταστάσεις που φιλοξενούν τον κρίσιμο εξοπλισμό;
11) Ο οργανισμός, διαθέτει σύστημα κλιματισμού για την ορθή ψύξη του χώρου όπου φιλοξενεί κρίσιμο εξοπλισμό;

12) Ο οργανισμός, διαθέτει πλεονασμό (redundancy) σε κρίσιμα συστήματα και κυκλώματα δικτύωσης;
13) Ο οργανισμός, διαθέτει κάμερες ασφαλείας για την παρακολούθηση και την επιτήρηση του χώρου;
14) Ο οργανισμός, χρησιμοποιεί access control ή μαγνητικές/έξυπνες κάρτες για την είσοδο των υπαλλήλων στον χώρο;

6. Υλοποίηση & Αξιολόγηση του Πλαισίου STAM

6.1. Περιγραφή

Το πλαίσιο STAM, αποτελεί έναν μηχανισμό με τον οποίο μπορεί να διενεργηθεί αξιολόγηση του επιπέδου κυβερνοασφάλειας ενός οργανισμού. Στηρίζεται σε ένα ερωτηματολόγιο (διασφαλίσεις), το οποίο είναι χωρισμένο σε κατηγορίες (σημεία ελέγχου), οι οποίες αποτελούν βέλτιστες πρακτικές κυβερνοασφάλειας. Το εργαλείο αυτό, είναι χρήσιμο για τους ειδικούς ασφαλείας ώστε να έχουν μια αρχική εκτίμηση της κατάσταση της κυβερνοασφάλειας σε έναν οργανισμό. Επίσης, μπορεί να χρησιμοποιηθεί και από τον ίδιο τον οργανισμό για την αυτοαξιολόγηση του, καθώς επίσης και να συμβάλει στην χάραξη στρατηγικών κυβερνοασφάλειας.

Πιο συγκεκριμένα, το STAM, αποτελείται από 20 θεματικές ενότητες, οι οποίες αντιστοιχούν στα 20 σημεία ελέγχου που περιγράφει το προηγούμενο κεφάλαιο. Οι ενότητες αυτές, περιλαμβάνουν ερωτήματα, τα οποία έχουν προκύψει από τις διασφαλίσεις του κάθε σημείου ελέγχου. Το STAM, συνολικά αποτελείται από 205 ερωτήματα, τα οποία αναπτύχθηκαν με βάση τις 148 διασφαλίσεις. Ο στόχος των ερωτημάτων είναι να επαληθευτούν οι διασφαλίσεις των σημείων ελέγχου. Η κάθε διασφάλιση μπορεί να αποτελείται από ένα ή πολλαπλά ερωτήματα. Όλες οι ερωτήσεις, είναι σαφείς και δεν εισάγουν προκαταλήψεις.

Σε κάθε ενότητα, διαμορφώνεται μια βαθμολογία, η οποία προκύπτει από τις απαντήσεις που δίνονται απ' τον χρήστη. Επίσης, διαμορφώνεται και μια συνολική βαθμολόγια για το επίπεδο της κυβερνοασφάλειας (Cyber Security Level) του οργανισμού. Έτσι, ο οργανισμός διαπιστώνει ποια είναι τα κενά και οι ελλείψεις του για την επίτευξη ενός υψηλού επιπέδου κυβερνοασφάλειας. Η επίτευξη ενός υψηλού επιπέδου κυβερνοασφάλειας και το χαμηλό επίπεδο επικινδυνότητας, βοηθάει τα πληροφοριακά συστήματα του οργανισμού να είναι προστατευμένα από τις συνεχώς αυξανόμενες και εξελισσόμενες κυβερνοαπειλές, καθώς επίσης και στην ικανότητα του οργανισμού να ανταποκρίνεται έγκαιρα σε κυβερνοεπιθέσεις ώστε να ανακτά άμεσα τη λειτουργικότητα του και την επιχειρηματική του συνέχεια.

Το STAM, κατά την αξιολόγηση των οργανισμών, λαμβάνει υπόψη του τα τεχνολογικά τους μέτρα, τις διαδικασίες τους και το ανθρώπινο δυναμικό. Το πλεονέκτημα του STAM έναντι των άλλων πλαισίων κυβερνοασφάλειας είναι ότι έχει επικεντρωθεί στις ΜμΕ και δεν αποτελείται από πολύπλοκες διαδικασίες και μέτρα που δύσκολα μπορούν να εφαρμόσουν. Επιπλέον, έχει αναπτυχθεί βάσει ενός συνδυασμού του πλαισίου NIST και των CIS controls και έχει προσαρμοστεί στην Εθνική Αρχή Κυβερνοασφάλειας. Επίσης, εναρμονίζεται με τις οδηγίες NIS και NIS2. Το STAM, χρησιμοποιεί μεθοδολογίες και μέτρα που μπορεί να λάβει η ΜμΕ και όχι πολυεπίπεδες μεθοδολογίες. Στην πράξη, δίνεται η δυνατότητα στον οργανισμό να προσδιορίσει την ωριμότητα του σχετικά με το πόσο έτοιμος είναι να αντιμετωπίσει μια κυβερνοαπειλή και να χαράξει τη στρατηγική του.

Το STAM, απευθύνεται σε μικρομεσαίες επιχειρήσεις (ΜμΕ) και οργανισμούς του δημοσίου και ιδιωτικού τομέα, οι οποίοι αποτελούν και τον πληθυσμό του ερωτηματολογίου. Τα ερωτήματα είναι απαραίτητο να απαντηθούν από άτομο, εφεξής χρήστη, το οποίο σχετίζεται με την πληροφοριακή υποδομή του οργανισμού είτε ως υπάλληλος είτε ως συνεργάτης υποστήριξης. Ο χρήστης αυτός, είναι αναγκαίο να έχει τις απαραίτητες τεχνολογικές γνώσεις, ώστε να δώσει τις κατάλληλες απαντήσεις που ανταποκρίνονται στην πραγματική εικόνα του οργανισμού. Επιπλέον, είναι αναγκαίο να γνωρίζει την δομή του οργανισμού καθώς και τις πολιτικές και τις διαδικασίες που υλοποιούνται εσωτερικά. Συνηθίζεται, τέτοιοι χρήστες να είναι οι διαχειριστές συστημάτων, οι διευθυντές πληροφορικής, το τμήμα IT, η συνεργαζόμενη εταιρεία που υποστηρίζει το πληροφοριακό σύστημα του οργανισμού ή άλλοι σύμβουλοι.

6.2. Βαθμολογία & Επικινδυνότητα

Η κυβερνοασφάλεια, έχει στόχο να προστατέψει τα assets του οργανισμού που έχουν αξία. Σύμφωνα με τον (Μαυρίδης, 2015), το asset μπορεί να εκτίθεται σε έναν κίνδυνο, ο οποίος αντιπροσωπεύει την αιτία για να περιοριστεί η αξία του asset. Ο περιορισμός της αξίας του asset ονομάζεται ζημιά. Η κατάσταση όπου υπάρχει το ενδεχόμενο πρόσκλησης ζημιών του πληροφοριακού συστήματος, αποτελεί μια απειλή για το πληροφοριακό σύστημα. Οι ζημιές, προκαλούνται μετά από επιθέσεις (attack) ως αποτέλεσμα της εκμετάλλευσης μιας ευπάθειας (vulnerability). Η αξία των assets, είναι ανάλογη των επιπτώσεων που θα έχουν από μια επιτυχημένη επίθεση και πιθανή ζημιά ή απώλεια.

Στο πλαίσιο της ερευνητικής εργασίας, ήταν αναγκαία η ανάλυση επικινδυνότητας (Risk Analysis), η οποία αποτελείται από την αναγνώριση κινδύνων (Risk Identification) και την αποτίμηση επικινδυνότητας (Risk Estimation). Έτσι, αντιστοιχούνται αριθμητικές τιμές στην πιθανότητα εμφάνισης ενός περιστατικού κατά την διάρκεια ζωής του οργανισμού και στον αντίκτυπο. Το επίπεδο κινδύνου, υπολογίζεται πολλαπλασιάζοντας τη βαθμολογία του αντίκτυπου και τη βαθμολογία της πιθανότητας. Τα κριτήρια για τον προσδιορισμό του αντίκτυπου και της πιθανότητα ορίζονται στους Πίνακες 1, 2, 3 και 4. Ο στόχος αυτής της διαδικασίας, είναι η αντιμετώπιση της επικινδυνότητας και η επιλογή κατάλληλων μέτρων ασφαλείας ώστε να μειωθεί ο κίνδυνος.

Πίνακας 1: Περιγραφή επιπέδων αντίκτυπου και κριτηρίων.

Αντίκτυπος (βαθμός)	**Ορισμός**
Ελάχιστο (1,0)	• Ελάχιστη οικονομική ζημία στον οργανισμό. • Γρήγορη επανόρθωση. • Δεν απαιτείται αναφορά σε ρυθμιστική Αρχή. • Μεμονωμένη δυσαρέσκεια στο προσωπικό.
Μικρό (2,0)	• Μικρή οικονομική ζημία στον οργανισμό. • Τοπική ζημία στη φήμη. • Απαιτείται αναφορά σε ρυθμιστική Αρχή, χωρίς παρακολούθηση. • Προβλήματα του ηθικού του προσωπικού.
Μέτριο (3,0)	• Μέτρια οικονομική ζημία στον οργανισμό. • Βραχυπρόθεσμη ζημία στη φήμη σε εθνικό επίπεδο. • Απαιτείται αναφορά σε ρυθμιστική Αρχή με άμεση διόρθωση που πρέπει να εφαρμοστεί. • Εκτεταμένα προβλήματα του ηθικού του προσωπικού.
Υψηλό (4,0)	• Σημαντική οικονομική ζημία στον οργανισμό. • Μακροπρόθεσμη ζημία στη φήμη σε εθνικό επίπεδο. • Σημαντική απώλεια μεριδίου της αγοράς. • Απαιτείται αναφορά σε ρυθμιστική Αρχή και σημαντικές διορθωτικές ενέργειες. • Υψηλά στελέχη και έμπειρο προσωπικό αποχωρούν.

Πολύ υψηλό (5,0)	• Τεράστια οικονομική ζημία στον οργανισμό. • Μακροχρόνια αρνητική ζημία στη φήμη και κάλυψη από τα μέσα ενημέρωσης. • Μεγάλη απώλεια μεριδίου αγοράς. • Σημαντική δίωξη και πρόστιμα, δικαστικές διαφορές, ομαδικές αγωγές, φυλάκιση ηγεσίας. • Ανώτερα στελέχη αποχωρούν.

Πίνακας 2: Περιγραφή επιπέδων και κριτηρίων πιθανότητας.

Πιθανότητα (Συντελεστής βαρύτητας)	**Ορισμός**
Σπάνιο (1,0)	• Μία φορά στα 100 χρόνια ή λιγότερο • <10% πιθανότητα εμφάνισης κατά τη διάρκεια ζωής του οργανισμού
Απίθανο (2,0)	• Μία φορά στα 50 έως 100 χρόνια • 10% έως 35% πιθανότητα εμφάνισης κατά τη διάρκεια ζωής του οργανισμού
Πιθανό (3,0)	• Μία φορά στα 25 έως 50 χρόνια • 35% έως 65% πιθανότητα εμφάνισης κατά τη διάρκεια ζωής του οργανισμού
Υψηλή Πιθανότητα (4,0)	• Μία φορά στα 2 έως 25 χρόνια • 65% έως 90% πιθανότητα εμφάνισης κατά τη διάρκεια ζωής του οργανισμού
Σχεδόν Βέβαιο(5,0)	• Έως μία φορά στα 2 χρόνια ή περισσότερα • 90% ή μεγαλύτερη πιθανότητα εμφάνισης κατά τη διάρκεια ζωής του οργανισμού

Πίνακας 3: Βαθμολογία εκτίμησης κινδύνου.

Βαθμολογία Κινδύνου	**Εκτίμηση Κινδύνου**
Μικρότερος ή ίσος με 4,0	Χαμηλός Κίνδυνος
Μεγαλύτερος από 4,0 αλλά μικρότερος ή ίσος του 9,0	Μεσαίος Κίνδυνος
Μεγαλύτερος από 9,0 αλλά μικρότερος ή ίσος με 16,0	Υψηλός Κίνδυνος
Μεγαλύτερος από 16,0	Κρίσιμος Κίνδυνος

Πίνακας 4: Πίνακας Εκτίμησης Κινδύνου.

		Επίπτωση				
Πιθανότητα		Ελάχιστη (1,0)	Μικρή (2,0)	Μέτρια (3,0)	Υψηλή (4,0)	Πολύ Υψηλή (5,0)
	Σπάνιο (1,0)	1,0x1,0 = 1,0 Χαμηλός Κίνδυνος	2,0x1,0 = 2,0 Χαμηλός Κίνδυνος	3,0x1,0 = 3,0 Χαμηλός Κίνδυνος	4,0x1,0 = 4,0 Χαμηλός Κίνδυνος	5,0x1,0 = 5,0 Μεσαίος Κίνδυνος
	Απίθανο (2,0)	1,0x2,0 = 2,0 Χαμηλός Κίνδυνος	2,0x2,0 = 4,0 Χαμηλός Κίνδυνος	3,0x2,0 = 6,0 Μεσαίος Κίνδυνος	4,0x2,0 = 8,0 Μεσαίος Κίνδυνος	5,0x2,0 = 10,0 Υψηλός Κίνδυνος
	Πιθανό (3,0)	1,0x3,0 = 3,0 Χαμηλός Κίνδυνος	2,0x3,0 = 6,0 Μεσαίος Κίνδυνος	3,0x3,0 = 9,0 Μεσαίος Κίνδυνος	4,0x3,0 = 12,0 Υψηλός Κίνδυνος	5,0x3,0 = 15,0 Υψηλός Κίνδυνος
	Πιθανότατα (4,0)	1,0x4,0 = 4,0 Χαμηλός Κίνδυνος	2,0x4,0 = 8,0 Μεσαίος Κίνδυνος	3,0x4,0 = 12,0 Υψηλός Κίνδυνος	4,0x4,0 = 16,0 Υψηλός Κίνδυνος	5,0x4,0 = 20,0 Κρίσιμος Κίνδυνος
	Σχεδόν Βέβαιο (5,0)	1,0x5,0 = 5,0 Μεσαίος Κίνδυνος	2,0x5,0 = 10,0 Υψηλός Κίνδυνος	3,0x5,0 = 15,0 Υψηλός Κίνδυνος	4,0x5,0 = 20,0 Κρίσιμος Κίνδυνος	5,0x5,0 = 25,0 Κρίσιμος Κίνδυνος

Η εκτίμηση της επικινδυνότητας (βλ. Πίνακα 4), πραγματοποιείται ώστε να αποδοθεί η βαρύτητα των σημείων ελέγχου και ο αντίστοιχα ο βαθμός των ερωτήσεων. Στο παράδειγμα του Πίνακα 5, πραγματοποιείται εκτίμηση της επικινδυνότητας στο σημείο ελέγχου της φυσικής ασφάλειας. Για τον κάθε κίνδυνο, έχει αποδοθεί ο αντίκτυπος και η πιθανότητα. Έτσι, υπολογίστηκε ο βαθμός κινδύνου. Η εκτίμηση του κινδύνου βοηθάει ώστε να ληφθούν μέτρα για την μείωση της επικινδυνότητας. Η στήλη «ενέργεια μείωσης επικινδυνότητας» παρουσιάζει ενδεικτικά κάποια παραδείγματα.

Πίνακας 5: Παράδειγμα εκτίμησης επικινδυνότητας.

Κίνδυνος	**Αντίκτυπος**	**Πιθανότητα**	**Βαθμός κινδύνου**	**Εκτίμηση κινδύνου**	**Ενέργεια μείωσης επικινδυνότητας**
Κλοπή φορητής συσκευής	3	4	12	Υψηλός κίνδυνος	Κρυπτογράφηση
Απώλεια φορητής συσκευής	3	4	12	Υψηλός κίνδυνος	Κρυπτογράφηση
Διακοπή παροχής ενέργειας σε κρίσιμα συστήματα	4	5	20	Κρίσιμος Κίνδυνος	Συστήματα UPS για αδιάλειπτη παροχή ρεύματος
Πυρκαγιά σε κρίσιμα συστήματα (computer room)	3	4	12	Υψηλός κίνδυνος	Ανιχνευτές καπνού
Αυξημένη θερμοκρασία στον κρίσιμο εξοπλισμό (computer room)	2	8	8	Μεσαίος Κίνδυνος	Αισθητήρες θερμοκρασίας Κλιματισμός
Διαρροή νερού σε χώρο με κρίσιμο εξοπλισμό	3	3	9	Μεσαίος Κίνδυνος	Αισθητήρες υγρασίας

Είναι σημαντικό, να σημειωθεί ότι, ο υπολογισμός της επικινδυνότητας είναι υποκειμενικός και εξαρτάται από το περιβάλλον του οργανισμού, το είδος των δεδομένων, τα μέτρα ασφαλείας και άλλους παράγοντες, για τον λόγο αυτό είναι σκόπιμο η περιπτωσιολογική μελέτη της επικινδυνότητας του οργανισμού ώστε να ληφθούν οι κατάλληλες αποφάσεις σχετικά με τις προτεραιότητες της ασφάλειας.

Στο STAM, τα ερωτήματα λαμβάνουν απαντήσεις κλειστού τύπου της κλίμακας Likert (1-3), δηλαδή, "δεν υλοποιείται", "υλοποιείται μερικώς" και "υλοποιείται πλήρως". Αυτές οι απαντήσεις, αντιστοιχούν σε συγκεκριμένους βαθμούς, όπως παρουσιάζεται στον Πίνακα 6.

Πίνακας 6: Βαθμολογία απαντήσεων.

Απάντηση	Βαθμοί
Δεν απαντήθηκε	0
Δεν υλοποιείται	0
Υλοποιείται μερικώς	0,5 x βαθμοί ερωτήματος
Υλοποιείται πλήρως	1 x βαθμοί ερωτήματος

Το κάθε ερώτημα, έχει έναν βαθμό βάσει της επικινδυνότητας. Αν υλοποιείται πλήρως, τότε η απάντηση λαμβάνει όλο το βαθμό. Αν υλοποιείται μερικώς, τότε η απάντηση λαμβάνει το 0,5 του βαθμού. Στην περίπτωση που δεν υλοποιείται ή δεν έχει απαντηθεί το ερώτημα, τότε δεν λαμβάνει κανέναν βαθμό. Το άθροισμα αυτών των βαθμών δίνει την συνολική βαθμολογία της κάθε θεματικής ενότητας. Το σύνολο των βαθμών των ερωτημάτων σε κάθε κατηγορία είναι 99. Το επίπεδο κυβερνοασφάλειας της κατηγορίας αποτυπώνεται με %. Όταν υλοποιούνται πλήρως όλα τα ερωτήματα αποδίδεται 99% στο επίπεδο της κυβερνοασφάλειας και 1% επικινδυνότητα. Δεν αποδίδεται σε καμία κατηγορία το 100%, λόγω του ότι δεν μπορεί να υπάρξει εγγύηση για 100% κυβερνοασφάλεια.

Πίνακας 7: Παράδειγμα υπολογισμού επιπέδου κυβερνοασφάλειας ανά κατηγορία.

ΚΩΔΙΚΟΣ ΕΡΩΤΗΜΑΤΟΣ	ΒΑΘΜΟΣ ΕΡΩΤΗΜΑΤΟΣ	ΑΠΑΝΤΗΣΗ ΧΡΗΣΤΗ	ΥΠΟΛΟΓΙΣΜΟΣ	ΤΕΛΙΚΗ ΒΑΘΜΟΛΟΓΙΑ ΕΡΩΤΗΜΑΤΟΣ
100	10	Υλοποιείτε μερικώς	10 x 0,5	5
101	10	Υλοποιείτε πλήρως	10 x 1	10
102	9	Υλοποιείτε μερικώς	9 x 0,5	4,5
103	10	Υλοποιείτε μερικώς	10 x 0,5	5
104	5	Υλοποιείτε πλήρως	5 x 1	5
105	10	Υλοποιείτε πλήρως	10 x 1	10
106	10	Υλοποιείτε μερικώς	10 x 0,5	5
107	5	Υλοποιείτε πλήρως	5 x 1	5
108	5	Υλοποιείτε μερικώς	5 x 0,5	2,5
109	5	Δεν υλοποιείτε	5 x 0	0
110	10	Δεν υλοποιείτε	10 x 0	0
111	10	Δεν απαντήθηκε	10 x 0	0
ΣΥΝΟΛΙΚΟΙ ΒΑΘΜΟΙ ΕΡΩΤΗΜΑΤΩΝ	**99**	**ΣΥΝΟΛΙΚΗ ΒΑΘΜΟΛΟΓΙΑ ΚΑΤΗΓΟΡΙΑΣ**		**52**

Το παράδειγμα του Πίνακα 7, παρουσιάζει τον υπολογισμό των απαντήσεων του χρήστη σε μια κατηγορία. Το επίπεδο κυβερνοασφάλειας του οργανισμού στη συγκεκριμένη θεματική ενότητα είναι 52%. Η συνολική βαθμολογία όλων των θεματικών ενοτήτων, δηλαδή, ένας βαθμός του επίπεδου της κυβερνοασφάλειας (CyberSecurity Level) του οργανισμού, λαμβάνει υπόψη τη βαρύτητα των σημείων ελέγχου. Δεδομένου ότι όλα τα σημεία ελέγχου δεν έχουν την ίδια βαρύτητα, η συνολική

βαθμολογία προκύπτει από τον συντελεστής βαρύτητας που έχει δοθεί σε κάθε θεματική ενότητα. Ο συντελεστής βαρύτητας του κάθε σημείου ελέγχου παρουσιάζεται στον Πίνακα 3.

Πίνακας 8: Συντελεστής βαρύτητας των σημείων ελέγχου.

Συντελεστής Βαρύτητας	**Σημείο Ελέγχου**
0,03	Διοίκηση και διαχείριση κυβερνοασφάλειας
0,02	Καταγραφή και έλεγχος περιουσιακών στοιχείων
0,02	Καταγραφή και έλεγχος λογισμικού
0,05	Ασφαλής διαμόρφωση υλικού και λογισμικού
0,06	Προστασία Δεδομένων
0,05	Διαχείριση λογαριασμών
0,05	Διαχείριση ελέγχου πρόσβασης
0,03	Διαχείριση αρχείων καταγραφής
0,05	Διαχείριση παρόχων υπηρεσιών
0,07	Διαχείριση δικτυακής υποδομής
0,06	Προστασία ηλεκτρονικού ταχυδρομείου και προγραμμάτων περιήγησης
0,07	Προστασία από κακόβουλο λογισμικό
0,05	Ασφάλεια εφαρμογών λογισμικού
0,08	Παρακολούθηση και άμυνα του δικτύου
0,07	Εκπαίδευση και ενημέρωση για την ασφάλεια
0,09	Αντίγραφα ασφαλείας & ανάκτηση δεδομένων
0,04	Διαχείριση αντιμετώπισης περιστατικών
0,03	Δοκιμές διείσδυσης
0,04	Συνεχής διαχείριση ευπαθειών
0,04	Φυσική ασφάλεια
1	**Συνολικά**

Η βαρύτητα της κάθε κατηγορίας και η βαθμολογία του κάθε ερωτήματος σχετίζεται με τη βαρύτητα του σημείου ελέγχου και των διασφαλίσεων, η οποία λαμβάνει υπόψη παράγοντες όπως ο κίνδυνος, η πιθανότητα παραβίασης ή εκδήλωσης βλάβης, η προστασία ευαίσθητων δεδομένων, η επίπτωση στον οργανισμό και άλλοι σχετικοί παράγοντες που αξιολογούν τη σημασία και την επίδραση ενός συγκεκριμένου ελέγχου στην κυβερνοασφάλεια, καθώς επίσης εξετάζεται και η ευκολία και η αποτελεσματικότητα της εφαρμογής του ελέγχου. Έτσι, καθ' ένας από αυτούς τους παράγοντες αξιολογείται και αποτελεί μέρος της διαδικασίας καθορισμού της βαρύτητας του σημείου ελέγχου. Αυτές οι βαθμολογίες βαρύτητας μπορούν να βοηθήσουν τους οργανισμούς να κατανοήσουν ποιοι έλεγχοι είναι πιο σημαντικοί και πρέπει να εφαρμοστούν πρώτοι. Το άθροισμα των συντελεστών βαρύτητας, σε αυτήν την εφαρμογή είναι ένα (1).

Για τον υπολογισμό της συνολικής βαθμολογίας (Cyberecurity Level), χρησιμοποιείται ο τύπος:

$$\sum_{i=1}^{20} x_i \times y_i = x_i \times y_i + x_{i+1} \times y_{i+1} + \cdots + x_{20} \times y_{20}$$

Συνολική βαθμολογία κατηγορίας = x

Συντελεστής βαρύτητας κατηγορίας = y

Κατηγορία = i

Ο υπολογισμό της επικινδυνότητας (Risk) του κάθε σημείου ελέγχου, απαιτεί τη αξιολόγηση πολλών παραγόντων που μπορεί να επηρεάζουν την ασφάλεια ενός συστήματος ή ενός οργανισμού. Όπως προαναφέρθηκε, οι παράγοντες περιλαμβάνουν την πιθανότητα εκδήλωσης των απειλών, την πιθανότητα εκμετάλλευσης των ευπαθειών, τις επιπτώσεις μιας πιθανής παραβίασης και άλλους παράγοντες. Η επικινδυνότητα μπορεί να κατηγοριοποιηθεί σε διάφορα επίπεδα. Το εργαλείο αυτό, λειτουργεί ως μέσο μέτρησης του επιπέδου κυβερνοασφάλειας του οργανισμού και συγχρόνως βοηθάει τον οργανισμό να εντοπίσει ελλείψεις, οι οποίες αυξάνουν τον βαθμό επικινδυνότητας του πληροφοριακού του συστήματος. Επίσης, αποτελεί ένα εργαλείο για την λήψη αποφάσεων σε σχέση με την κυβερνοασφάλεια και την πολιτική ασφαλείας του οργανισμού. Από την βαθμολογία (cybersecurity level) προκύπτει η απομένουσα επικινδυνότητα όπως απεικονίζεται στον Πίνακα 9.

Πίνακας 9: Απεικόνιση της κατάστασης επικινδυνότητας.

Βαθμολογία	Κατάσταση επικινδυνότητας	Χρώμα γραφήματος
76%-100%	Χαμηλή επικινδυνότητα	Μπλε
51%-75%	Μεσαίου επιπέδου επικινδυνότητα	Πράσινο
26%-50%	Υψηλού επιπέδου επικινδυνότητα	Πορτοκαλί
0%-25%	Κρίσιμος επίπεδο επικινδυνότητας	Κόκκινο

Η κατάσταση επικινδυνότητας κατηγοριοποιείται σε χαμηλό, μεσαίο, υψηλό και κρίσιμο επίπεδο. Τα επίπεδα αυτά υποδεικνύουν τη σοβαρότητα της κατάσταση και το πιθανό επίπεδο κινδύνου που πρέπει να αντιμετωπιστεί από τον οργανισμό. Στο χαμηλό επίπεδο, η κατάσταση είναι σχετικά ασφαλής και δεν απαιτούνται ιδιαίτερα μέτρα, αλλά η επίβλεψη και η προετοιμασία εξακολουθούν να είναι σημαντικές. Στο μεσαίο επίπεδο, η κατάσταση μπορεί να προκαλέσει προβλήματα, αλλά είναι διαχειρίσιμη, καθώς επίσης απαιτούνται και πρόσθετα μέτρα προστασίας. Στο υψηλό επίπεδο, η κατάσταση είναι σοβαρή, υπάρχουν σοβαροί κίνδυνοι και απειλές για την ασφάλεια και απαιτούνται πολλά μέτρα προστασίας. Στο κρίσιμο επίπεδο, ο οργανισμός βρίσκεται σε έκτακτη ανάγκη και απαιτείται άμεση αντίδραση και μέτρα προστασίας για την αντιμετώπιση της κρίσης.

6.3. Διερεύνηση για την εφαρμογή σε ΜμΕ

Η έρευνα για την κατάσταση της κυβερνοασφάλειας των ΜμΕ στην Ελλάδα επιλέχθηκε για να εξάγει χρήσιμα συμπεράσματα για την ασφάλεια των ΜμΕ και να αναδείξει τα προβλήματα που αντιμετωπίζουν σήμερα οι ΜμΕ, καθώς επίσης και τα σημεία όπου ενδεχομένως πρέπει να επισημανθούν. Για την διεξαγωγή της έρευνα απαιτεί οι ΜμΕ να απαντήσουν στα ερωτήματα που τέθηκαν στο πλαίσιο STAM. Η αρχική προσέγγιση ήταν μια επαφή σε μορφή συνέντευξης με κάποιες εταιρείες και τον κατάλληλο άνθρωπο τους. Από τις επικοινωνίες αυτές, διαπιστώθηκε ότι υπάρχουν πρακτικά προβλήματα για την συλλογή των δεδομένων, καθώς και ζητήματα ασφάλειας που τέθηκαν από τους ερωτηθέμενους. Συγκεκριμένα:

α) Η συντριπτική πλειοψηφία, έθεσε ζητήματα ασφάλειας και εμπιστευτικότητας σχετικά με την συλλογή των δεδομένων. Λόγω της φύσης των ερωτημάτων, οι ερωτηθέμενοι ήταν αρνητικοί να απαντήσουν επώνυμα σε ερωτήματα τα οποία αποκάλυπταν ολόκληρη την δομή του οργανισμού, τις πολιτικές ασφαλείας, τα τεχνικά μέτρα και να διακύβευαν την ασφάλεια του οργανισμού τους.

β) Ο χρόνος που απαιτείται να αφιερώσει κάποιος για να απαντήσει στα ερωτήματα του πλαισίου STAM είναι αρκετά μεγάλος. Από τις μετρήσεις προέκυψε ένας μέσος όρος 20 δευτερολέπτων για την ανάγνωση, κατανόηση και απάντηση ενός ερωτήματος. Συνολικά, απαιτείται τουλάχιστον 1,5 ώρα για την συμμετοχή στην έρευνα.

γ) Ο τρόπος παρουσίασης ενώ επιλέχθηκε να είναι σε μορφή φόρμας, όπως για παράδειγμα google form ή microsoft form, δεν ήταν αποδοτικός για ανώνυμη συμπλήρωση καθώς θα έπρεπε ο χρήστης να μην διακόψει την συμπλήρωση των ερωτημάτων μέχρι την υποβολή της. Πράγμα αδύνατο για την ποσότητα των ερωτημάτων. Επιπλέον, με το ρίσκο σε περίπτωση διακοπής, ο χρήστης να μη συνεχίσει.

δ) Το όφελος της έρευνας ως προς τον χρήστη, ήταν και αυτός ένας παράγοντας που απέρριπτε την χρήση forms για τα ερωτήματα. Οι ερωτηθέμενοι, επισήμαναν πως μετά από τόσο χρόνο που απαιτεί η συμμετοχή στην έρευνα, θα ήταν αναγκαίο ο οργανισμός ή ο χρήστης να έχει κάποια οφέλη (ανταποδοτικότητα).

Για τους παραπάνω λόγους, κρίθηκε αναγκαίο τα ερωτήματα να παρουσιαστούν στον χρήστη μέσω του ιστού και να μην απαιτούν αυθεντικοποίηση που προσδίδει σύνδεση των απαντήσεων με την εταιρεία ή τον χρήστη. Δηλαδή, οι απαντήσεις να μην συνδέονται σε καμία περίπτωση με κάποια επωνυμία, email και άλλα μοναδικά χαρακτηριστικά. Έτσι, η έρευνα περιορίστηκε στα ελάχιστα α-παραίτητα στοιχεία για τους σκοπούς της.

6.4. Σχεδιασμός & Υλοποίηση έρευνας και αξιολόγησης του πλαισίου STAM

Η παρουσίαση του STAM για την διεξαγωγή της έρευνας, πραγματοποιήθηκε μέσω του ιστότοπου https://users.it.teithe.gr/~ait52019/ (Εικόνα 19). Η παρουσίαση των ερωτημάτων και η συλλογή των δεδομένων πραγματοποιήθηκε μόνο διαδικτυακά. Η χρήση ευρέως γνωστών εργαλείων και τε-χνολογιών βοήθησαν στην παρουσίαση των ερωτημάτων στον χρήστη και στην συλλογή των απα-ντήσεων σε βάση δεδομένων. Για την διαχείριση της σχεσιακής βάσης δεδομένων, χρησιμοποιήθηκε η MySQL και το ανοιχτού λογισμικού εργαλείο phpMyAdmin για την διαχείριση της MySQL. Καθώς επίσης, τεχνολογίες HTML, CSS και PHP Scripting για το δυναμικό περιεχόμενο του ιστότοπου. Για τα γραφικά χρησιμοποιήθηκε το template SmartAdmin, το οποίο παρέχει Bootstrap τεχνικές, φιλικές προς τον χρήστη. Για την αξιολόγηση του πλαισίου από τους Ειδικούς (Experts), δημιουργήθηκε μια φόρμα μέσω της εφαρμογή Microsoft Form ώστε να υπάρχει δυνατότητα καταχώρηση των στοιχείων και παρουσίαση των ερωτημάτων αξιολόγησης.

Εικόνα 19: Ιστοσελίδα ανάρτησης της έρευνας.

Η συλλογή των δεδομένων από τους χρήστες για την έρευνα στις ΜμΕ, αποτελείται από μια ολοκληρωμένη δομή που την απαρτίζουν τα εξής:

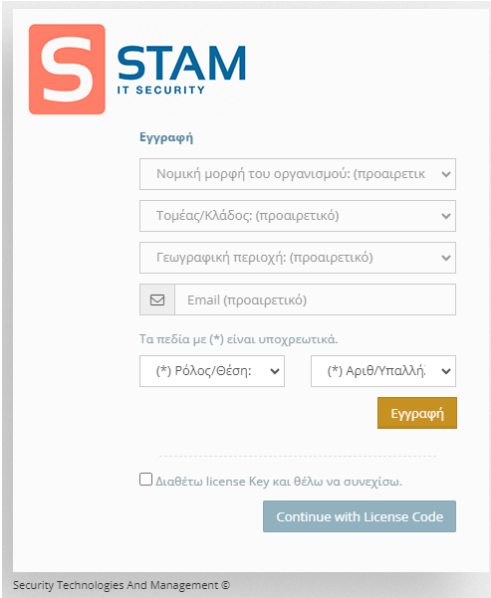
α) Είσοδος του χρήστη & προφίλ χρήστη (Εικόνα 20).
β) Περιβάλλον ερωτημάτων & απαντήσεων (Εικόνα 30).
γ) Υποβολή απαντήσεων & αξιολόγηση (feedback) από τον χρήστη (Εικόνα 34).

Η συλλογή δεδομένων της αξιολόγησης του πλαισίου από Ειδικούς χρήστες αποτελείται από τα εξής:

α) Στοιχεία του χρήστη που αξιολογεί (Εικόνα 38).
β) Ερωτήματα αξιολόγησης.
γ) Σχόλια αξιολόγησης.

6.4.1. Είσοδος του χρήστη & προφίλ χρήστη

Η συμμετοχή του χρήστη στην έρευνα, απαιτεί την συμπλήρωση κάποιων στοιχείων. Λόγω των προβλημάτων που αναφέρθηκαν σε προηγούμενη ενότητα σχετικά με την ασφάλεια και την εμπιστευτικότητα, ο χρήστης δεν ταυτοποιείται ως φυσικό πρόσωπο και δεν συσχετίζεται με στοιχεία της εταιρείας του. Το προφίλ χρήστη, περιλαμβάνει βασικές πληροφορίες για τον χρήστη και τον οργανισμό που συμμετέχουν στην έρευνα (Εικόνα 20). Τα στοιχεία που κρίθηκαν απαραίτητα για την συμμετοχή στην έρευνα είναι ο ρόλος/θέση (Εικόνα 23) του χρήστη και ο αριθμός των υπαλλήλων (Εικόνα 25). Επιπλέον, υπάρχουν προαιρετικά πεδία για συλλογή άλλων πληροφοριών όπως νομική μορφή οργανισμού (Εικόνα 22), κλάδος/τομέας (Εικόνα 24) , γεωγραφική περιοχή (Εικόνα 21) και email.



Εικόνα 20: Εγγραφή χρήστη στο πλαίσιο STAM

geoarea_id	geoarea_perig
1	Θράκη
2	Μακεδονία
3	Θεσσαλία
4	Ήπειρος
5	Στ.Ελλάδα
6	Πελοπόννησος
7	Κρήτη
8	Νησιά Αιγαίου
9	Νησιά Ιονίου

Εικόνα 21: Πίνακας επιλογών Γεωγραφική Περιοχή.

legal_id	legal_perig
1	Ατομική Επιχείρηση
2	Ομόρρυθμη Εταιρεία
3	Ετερόρρυθμη Εταιρεία
4	Εταιρεία Περιορισμένης Ευθύνης
5	Συνεταιρισμός
6	Δημόσια Υπηρεσία
7	Ανώνυμη Εταιρεία
8	άλλη..

Εικόνα 22: Πίνακας επιλογών Νομική Μορφή.

thesi_id	thesi_perig
1	CISO
2	CIO
3	CEO
4	DPO
6	IT Manager
7	IT Administrator
8	Cyber Security Expert
5	άλλο...

Εικόνα 23: Πίνακας επιλογών Ρόλος/Θέση.

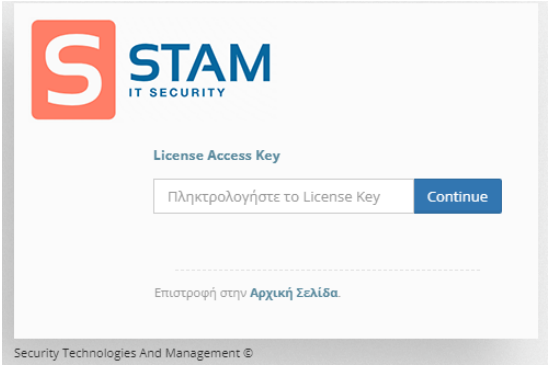
tomeas_id	tomeas_perig
1	Τροφίμων
2	Φαρμάκων/καλλυντικών
3	Ένδυσης/υπόδησης
4	Πετρελαιοειδών
5	Ηλεκτρολογικού εξοπλισμού
6	Πληροφορικής
7	Τηλεπικοινωνίες
8	Εκπαίδευσης
9	Οικονομικών/λογιστικών
10	Τραπεζικός
11	Μεταφορές/ταχυμεταφορές
12	Νομικός
13	Συμβούλων
14	Εστίασης
15	άλλο...

Εικόνα 24: Πίνακας επιλογών Τομέας/Κλάδος.

employees_id	employees_perig
1	1-10
2	11-50
3	51-100
4	101-250

Εικόνα 25: Πίνακας επιλογών Αριθμός Υπαλλήλων.

Ο χρήστης συμπληρώνοντας τα απαραίτητα πεδία λαμβάνει έναν κωδικό (License Code/License Key) και με αυτό μπορεί να συνδεθεί ώστε όλες οι απαντήσεις που δίνει να σχετίζονται μόνο με αυτόν τον κωδικό. Για την ευκολία του χρήστη, δίνεται η δυνατότητα να κάνει download το license key σε αρχείο .txt. Ο χρήστης μπορεί να συνδεθεί όποτε επιθυμεί, χρησιμοποιώντας αυτό τον κωδικό και να αλλάξει ή να τροποποιήσει τις απαντήσεις του, μέχρι να ολοκληρώσει το ερωτηματολόγιο και να πατήσει υποβολή. Μετά την υποβολή δεν έχει δυνατότητα να τροποποιήσει τις απαντήσεις του, αλλά συνεχίζει να έχει πρόσβαση σε αυτές.



Εικόνα 26: Είσοδος στο πλαίσιο STAM με License Key.

Το κάθε License Key είναι στην πραγματικότητα το προφίλ ενός χρήστη (Εικόνα 27). Για την αξιοπιστία της έρευνας συλλέχθηκαν οι IP διευθύνσεις.

gen_id	license_id	license_protect_id	license_date_start	license_date_end	thesi_id	tomeas_id	employees_id	legal_id	geoarea_id	license_login_ip	license_login_date	license_lock
39	STAM_US_64EDD44	[redacted]	2023-08-29 00:00:00	2023-09-28 00:00:00	6	0	2	0	0	188.11	2023-08-29 14:19:40	open
38	STAM_US_64ED9AE	[redacted]	2023-08-29 00:00:00	2023-09-28 00:00:00	8	15	4	6	2	79.103	2023-08-29 10:14:45	open
36	STAM_US_64EC299	[redacted]	2023-08-28 00:00:00	2023-09-27 00:00:00	8	0	1	0	0	79.103	2023-08-28 07:59:05	open
35	STAM_US_64EB023	[redacted]	2023-08-27 00:00:00	2023-09-26 00:00:00	1	14	2	3	2	79.131	2023-08-27 10:58:40	open
34	STAM_US_64E84BF3	[redacted]	2023-08-25 00:00:00	2023-09-24 00:00:00	8	6	3	1	1	87.202	2023-08-25 09:36:35	open
33	STAM_US_64E66202	[redacted]	2023-08-23 00:00:00	2023-09-22 00:00:00	1	0	4	0	0	79.130	2023-08-23 22:46:10	open
32	STAM_US_64E5C888	[redacted]	2023-08-23 00:00:00	2023-09-22 00:00:00	3	15	1	8	2	87.202	2023-08-23 11:51:20	open
31	STAM_US_64E4CC1	[redacted]	2023-08-22 00:00:00	2023-09-21 00:00:00	8	0	4	8	0	2.85.1	2023-08-22 17:54:22	open
30	STAM_US_64E44D47	[redacted]	2023-08-22 00:00:00	2023-09-21 00:00:00	7	6	1	1	2	94.67.	2023-08-22 08:53:11	open
29	STAM_US_64E33930	[redacted]	2023-08-21 00:00:00	2023-09-20 00:00:00	7	1	4	7	0	62.74.	2023-08-21 13:15:12	open
28	STAM_US_64E1DFC	[redacted]	2023-08-20 00:00:00	2023-09-19 00:00:00	4	0	2	0	0	91.140	2023-08-20 12:41:30	open

Εικόνα 27: Πίνακας License - Προφίλ Χρήστη.

6.4.2. Περιβάλλον ερωτημάτων & απαντήσεις

Η κεντρική σελίδα, περιλαμβάνει όλο το περιβάλλον που παρουσιάζονται τα ερωτήματα και δίνονται οι απαντήσεις. Υπάρχουν οι 20 ενότητες (σημεία ελέγχου) του πλαισίου, με τα αντίστοιχα ερωτήματα σε μορφή δέντρου. Σε κάθε ενότητα, αρχικά παρουσιάζεται μια σύντομη περιγραφή της ενότητας (Εικόνα 30). Δίνεται η δυνατότητα επιλογής 3 απαντήσεων (Εικόνα 28), όπως περιγράφετε στο κεφάλαιο 6.2. Από τις απαντήσεις που δίνει ο χρήστης, διαμορφώνεται η βαθμολογία και απεικονίζεται γραφικά το cybersecurity level (Εικόνα 31) και αντίστοιχα η επικινδυνότητα, σύμφωνα με τον υπολογισμό που περιγράφεται στο κεφάλαιο 6.2. (Εικόνα 29).

answers_status	answers_perig	answers_score
A	Δεν υλοποιείτε	0.00
B	Υλοποιείτε μερικώς	0.50
C	Υλοποιείτε πλήρως	1.00

Εικόνα 28: Πίνακας Απαντήσεων.

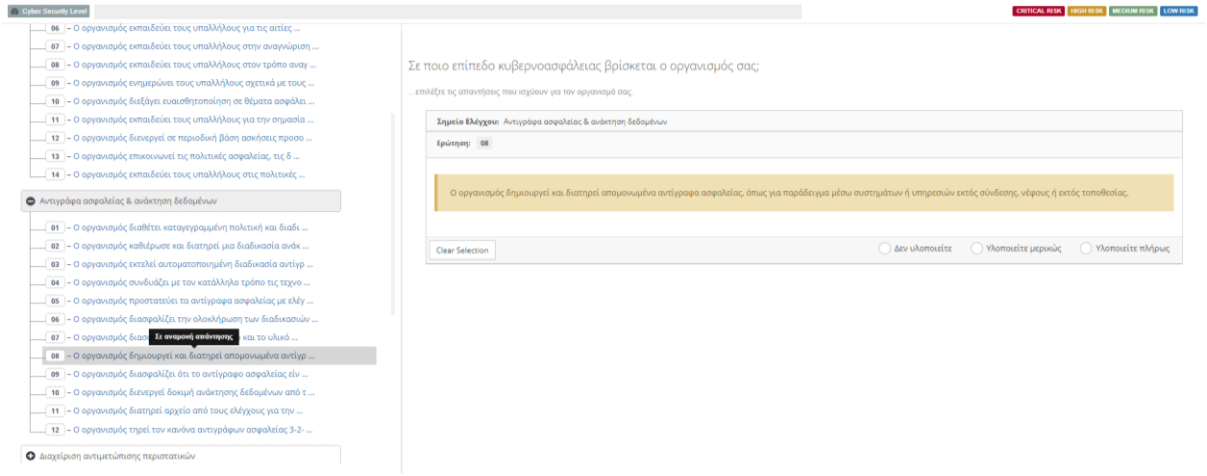
katig_id	katig_perig	katig_keimeno_text	katig_gravity
11	Διοίκηση και διαχείριση της κυβερνοασφάλειας	Η διοίκηση και διαχείριση της κυβερνοασφάλειας αντ...	0.03
12	Καταγραφή και ελέγχος των περιουσιακών στοιχείων	Η καταγραφή και ο έλεγχος των περιουσιακών στοιχεί...	0.02
13	Καταγραφή και ελέγχος λογισμικού	Η καταγραφή και ο έλεγχος του λογισμικού περιλαμβά...	0.02
14	Ασφαλή διαμόρφωση υλικού και λογισμικού	Η ασφαλής διαμόρφωση των επιχειρησιακών περιουσιακ...	0.05
15	Προστασία δεδομένων	Η προστασίας των δεδομένων περιλαμβάνει την ανάπτυ...	0.06
16	Διαχείριση λογαριασμών	Η διαχείριση των λογαριασμών αναφέρεται στις πολιτ...	0.05
17	Διαχείριση ελέγχου πρόσβασης	Η διαχείριση ελέγχου πρόσβασης περιλαμβάνει τη χρή...	0.05
18	Διαχείριση αρχείων καταγραφής	Η διαχείριση αρχείων καταγραφής ενισχύει την ασφάλ...	0.03
19	Διαχείριση παρόχων υπηρεσιών	Η διαχείριση των παρόχων υπηρεσιών περιλαμβάνει τη...	0.05
20	Διαχείριση δικτυακής υποδομής	Το σημείο ελέγχου διαχείρισης της δικτυακής υποδομ...	0.07
21	Προστασία ηλεκτρονικού ταχυδρομείου και προγραμμάτ...	Η προστασία του ηλεκτρονικού ταχυδρομείου και των ...	0.06
22	Προστασία από κακόβουλο λογισμικό	Η προστασίας από κακόβουλο λογισμικό περιλαμβάνει ...	0.07
23	Ασφάλεια εφαρμογών λογισμικού	Η ασφάλειας εφαρμογών λογισμικού περιλαμβάνει τη δ...	0.05
24	Παρακολούθηση και άμυνα δικτύου	Η παρακολούθηση και η άμυνα του δικτύου περιλαμβάν...	0.08
25	Εκπαίδευση και ενημέρωση για την ασφάλεια	Η εκπαίδευση και ενημέρωση για την ασφάλεια περιλα...	0.07
26	Αντιγράφα ασφαλείας & ανάκτηση δεδομένων	Το σημείο ελέγχου της ανάκτησης των δεδομένων περι...	0.09
27	Διαχείριση αντιμετώπισης περιστατικών	Η διαχείριση αντιμετώπισης περιστατικών κυβερνοασφ...	0.04
28	Δοκιμή διείσδυσης (PenTest)	Οι δοκιμές διείσδυσης (Penetration Testing – PenTe...	0.03
29	Συνεχή διαχείριση ευπαθειών	Η συνεχής διαχείρισης των ευπαθειών περιλαμβάνει τ...	0.04
30	Φυσική ασφάλεια	Το σημείο ελέγχου της φυσικής ασφάλειας περιλαμβάν...	0.04

Εικόνα 29: Πίνακας Κατηγορίες (Σημεία Ελέγχου).

Εικόνα 30: Παρουσίαση θεματικής ενότητας.

Εικόνα 31: Γραφήματα αξιολόγησης.

Τα αποτελέσματα, απεικονίζονται με γραφιστικό τρόπο (Εικόνα 31) και εξάγονται αυτόματα με την επιλογή της κάθε απάντησης. Συγκεκριμένα, υπάρχουν δυο είδη γραφημάτων, τα γραφήματα των θεματικών ενοτήτων και το συνολικό γράφημα. Η βαθμολογία παρουσιάζεται σε ποσοστό.



Εικόνα 32: Ερωτήσεις-Απαντήσεις του πλαισίου STAM.

Ο χρήστης, έχει τη δυνατότητα να κάνει download τις απαντήσεις που έδωσε, σε μορφή csv (Εικόνα 33). Με τον τρόπο αυτό μπορεί να διατηρήσει στο αρχείο του, τα ερωτήματα και τις απαντήσεις του, και να διαμορφώσει ανάλογα την στρατηγική του για την κυβερνοασφάλεια του οργανισμού.

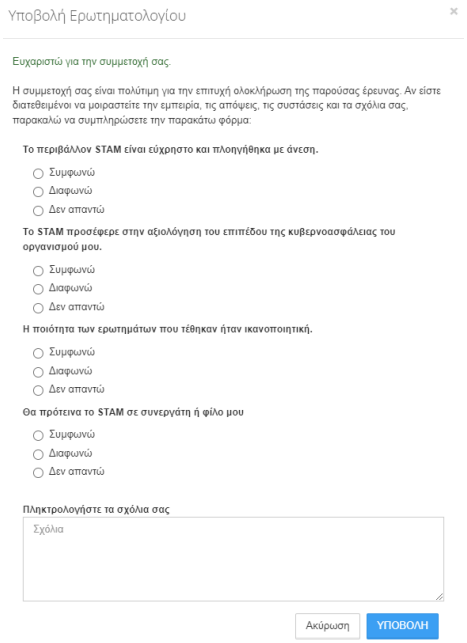
LICENSE	CATEGORY CODE	CATEGORY	CATEGORY GRAVITY	RISK STATUS	RISK	QUESTION CODE	QUESTION	QUESTION GRAVITY	ANSWER	SCORE
STAM_US_64D3DD38	11	Διοίκηση και διαχείρι	0,03	MEDIUM RISK	48%	100	Ο οργανισμός δι	10	Υλοποιείτε μερ	5
STAM_US_64D3DD38	11	Διοίκηση και διαχείρι	0,03	---	---	101	Ο οργανισμός δι	10	Υλοποιείτε πλή	10
STAM_US_64D3DD38	11	Διοίκηση και διαχείρι	0,03	---	---	102	Ο οργανισμός επ	9	Υλοποιείτε μερ	4,5
STAM_US_64D3DD38	11	Διοίκηση και διαχείρι	0,03	---	---	103	Ο οργανισμός δι	10	Υλοποιείτε μερ	5
STAM_US_64D3DD38	11	Διοίκηση και διαχείρι	0,03	---	---	104	Ο οργανισμός δι	5	Υλοποιείτε πλή	5
STAM_US_64D3DD38	11	Διοίκηση και διαχείρι	0,03	---	---	105	Ο οργανισμός έχ	10	Υλοποιείτε πλή	10
STAM_US_64D3DD38	11	Διοίκηση και διαχείρι	0,03	---	---	106	Ο οργανισμός πο	10	Υλοποιείτε μερ	5
STAM_US_64D3DD38	11	Διοίκηση και διαχείρι	0,03	---	---	107	Ο οργανισμός έχ	5	Υλοποιείτε πλή	5
STAM_US_64D3DD38	11	Διοίκηση και διαχείρι	0,03	---	---	108	Ο οργανισμός έχ	5	Υλοποιείτε μερ	2,5
STAM_US_64D3DD38	11	Διοίκηση και διαχείρι	0,03	---	---	109	Ο οργανισμός δε	5	Δεν υλοποιείτε	0
STAM_US_64D3DD38	11	Διοίκηση και διαχείρι	0,03	---	---	110	Ο οργανισμός έχ	10	Δεν υλοποιείτε	0
STAM_US_64D3DD38	11	Διοίκηση και διαχείρι	0,03	---	---	111	Ο οργανισμός δι	10	Δεν υλοποιείτε	0
STAM_US_64D3DD38	12	Καταγραφή και ελέγχ	0,02	MEDIUM RISK	45%	112	Ο οργανισμός έχ	20	Υλοποιείτε μερ	10
STAM_US_64D3DD38	12	Καταγραφή και ελέγχ	0,02	---	---	113	Ο οργανισμός έχ	19	Υλοποιείτε μερ	9,5
STAM_US_64D3DD38	12	Καταγραφή και ελέγχ	0,02	---	---	114	Ο οργανισμός δι	15	Υλοποιείτε πλή	15
STAM_US_64D3DD38	12	Καταγραφή και ελέγχ	0,02	---	---	115	Ο οργανισμός έχ	10	Δεν υλοποιείτε	0
STAM_US_64D3DD38	12	Καταγραφή και ελέγχ	0,02	---	---	116	Ο οργανισμός τη	10	Υλοποιείτε μερ	5
STAM_US_64D3DD38	12	Καταγραφή και ελέγχ	0,02	---	---	117	Ο οργανισμός δι	15	Υλοποιείτε πλή	15
STAM_US_64D3DD38	12	Καταγραφή και ελέγχ	0,02	---	---	118	Ο οργανισμός χρ	10	Δεν υλοποιείτε	0
STAM_US_64D3DD38	13	Καταγραφή και ελέγχ	0,02	CRITICAL RISK	85%	119	Ο οργανισμός δι	20	Δεν υλοποιείτε	0
STAM_US_64D3DD38	13	Καταγραφή και ελέγχ	0,02	---	---	120	Ο οργανισμός δι	19		0
STAM_US_64D3DD38	13	Καταγραφή και ελέγχ	0,02	---	---	121	Ο οργανισμός δι	15	Υλοποιείτε πλή	15
STAM_US_64D3DD38	13	Καταγραφή και ελέγχ	0,02	---	---	122	Ο οργανισμός χρ	20	Δεν υλοποιείτε	0
STAM_US_64D3DD38	13	Καταγραφή και ελέγχ	0,02	---	---	123	Ο οργανισμός δι	15	Δεν υλοποιείτε	0
STAM_US_64D3DD38	13	Καταγραφή και ελέγχ	0,02	---	---	124	Ο οργανισμός χρ	10	Δεν υλοποιείτε	0
STAM_US_64D3DD38	14	Ασφαλή διαμόρφωση	0,05	LOW RISK	24%	125	Ο οργανισμός δι	9	Δεν υλοποιείτε	0
STAM_US_64D3DD38	14	Ασφαλή διαμόρφωση	0,05	---	---	126	Ο οργανισμός εφ	10	Υλοποιείτε πλή	10

Εικόνα 33: Αρχείο CSV με απαντήσεις του χρήστη.

6.4.3. Αξιολόγηση εργαλείου από τον χρήστη

Η αξιολόγηση του εργαλείου από τον χρήστη, αναφέρεται στην συλλογή στοιχείων ανατροφοδότησης από τους χρήστες που συμμετείχαν στην έρευνα. Κατά την υποβολή των απαντήσεων του πλαισίου STAM, ο χρήστης καλείται να συμπληρώσει την φόρμα αξιολόγησης. Η αξιολόγηση αυτή, διαδραματίζει σημαντικό ρόλο για τη βελτίωση και τη μελλοντική ανάπτυξη του STAM. Η αξιολόγηση (Εικόνα 34), περιλαμβάνει 4 ερωτήματα κλειστού τύπου, τα οποία αφορούν την ευχρηστία (usability), δηλαδή πόσο εύκολη είναι η χρήση του εργαλείου και αν ο χρήστης μπορεί να πλοηγηθεί με άνεση, την βοήθεια που πρόσφερε το εργαλείο στο χρήστη για την αξιολόγηση του επιπέδου κυβερνοασφάλειας του

οργανισμού του, την ικανοποίηση του χρήστη για την ποιότητα των ζητημάτων που τέθηκαν και τέλος για την πρόθεση που έχει ο χρήστης να προτείνει τη χρήση του εργαλείου σε κάποιον συνεργάτη του ή φίλο του. Επιπλέον, δίνεται η δυνατότητα στο χρήστη να καταχωρήσει τυχόν σχόλια.



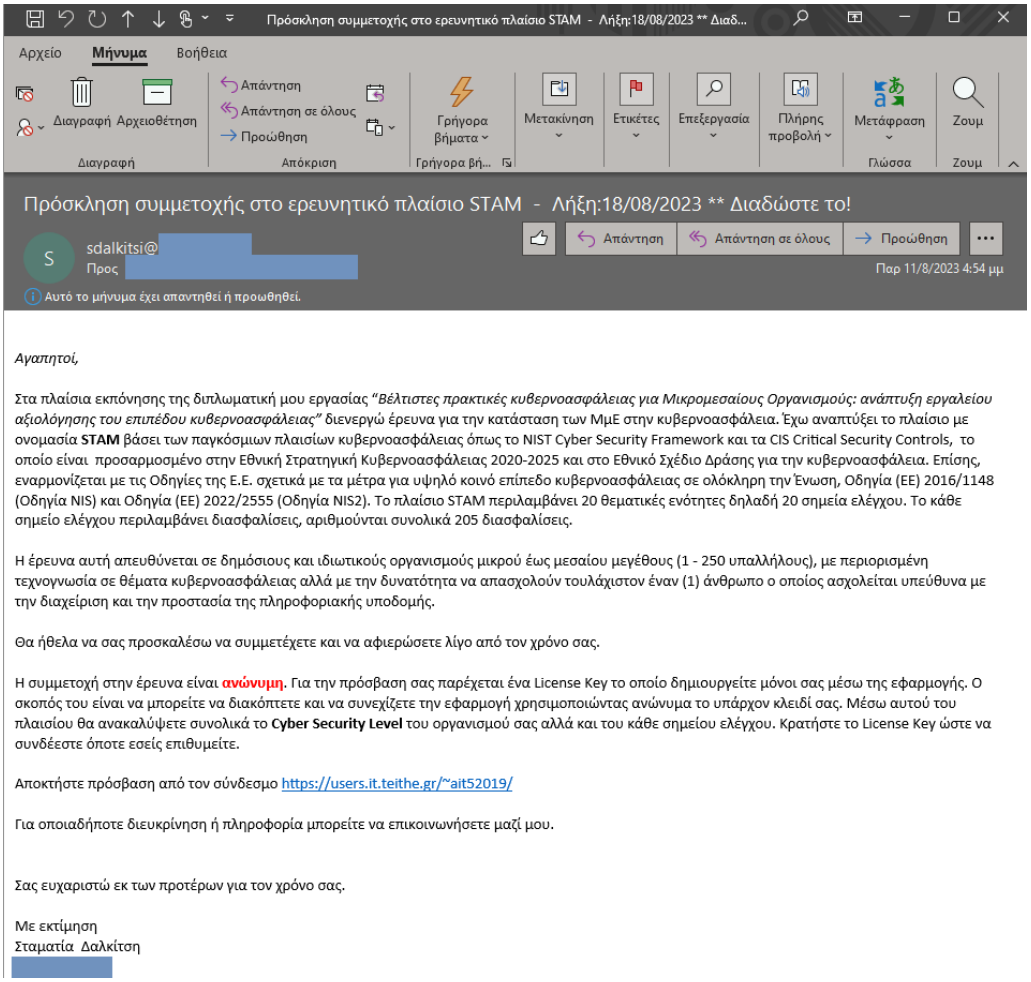
Εικόνα 34: Φόρμα αξιολόγησης σχετικά με την εμπειρία του χρήστη.

6.4.4. Εισαγωγή και οδηγίες για τη συμμετοχή στην έρευνα

Η συμμετοχή σε αυτή την έρευνα προϋποθέτει την αρχική ενημέρωση των χρηστών, λόγω του ότι κάποιοι πιθανοί χρήστες μπορεί να επιλέξουν να μη συμμετέχουν στην έρευνας εάν δεν υπάρχουν σαφείς πληροφορίες σχετικά με το σκοπό της, τον χρόνο που απαιτείται, το τρόπο με τον οποίο θα συλλεχθούν τα δεδομένα και πως θα χρησιμοποιηθούν στη συνέχεια. Έτσι, επιλέχθηκε μια σύντομη εισαγωγική ενημέρωση. Αυτό περιλαμβάνει :

- Ποιος διεξάγει την έρευνα και στοιχεία επικοινωνίας
- Το σκοπό της έρευνας
- Την ανταποδοτικότητα της συμμετοχής
- Τη διασφάλισης της εμπιστευτικότητας και της ανωνυμίας
- Τον τρόπος συμμετοχής στην έρευνα
- Τον χρόνος που απαιτείται
- Τις οδηγίες χρήσης

Οι πληροφορίες αυτές δόθηκαν σε σύντομη μορφή στο email (Εικόνα 35), με το οποίο προσκλήθηκαν οι συμμετέχοντες, στον ιστότοπο πριν την είσοδο τους στο ερωτηματολόγιο (Εικόνα 19), καθώς επίσης και περισσότερες πληροφορίες μετά την είσοδο τους (Εικόνα 36).



Πρόσκληση συμμετοχής στο ερευνητικό πλαίσιο STAM - Λήξη:18/08/2023 ** Διαδ...

Αρχείο Μήνυμα Βοήθεια

Διαγραφή Αρχειοθέτηση Απάντηση Απάντηση σε όλους Προώθηση Γρήγορα βήματα Μετακίνηση Ετικέτες Επεξεργασία Πλήρης προβολή Μετάφραση Ζουμ

Διαγραφή Απόκριση Γρήγορα βή... Γλώσσα Ζουμ

Πρόσκληση συμμετοχής στο ερευνητικό πλαίσιο STAM - Λήξη:18/08/2023 ** Διαδώστε το!

S sdalkitsi@ Προς

Απάντηση Απάντηση σε όλους Προώθηση

Παρ 11/8/2023 4:54 μμ

Αυτό το μήνυμα έχει απαντηθεί ή προωθηθεί.

Αγαπητοί,

Στα πλαίσια εκπόνησης της διπλωματική μου εργασίας "*Βέλτιστες πρακτικές κυβερνοασφάλειας για Μικρομεσαίους Οργανισμούς: ανάπτυξη εργαλείου αξιολόγησης του επιπέδου κυβερνοασφάλειας*" διενεργώ έρευνα για την κατάσταση των ΜμΕ στην κυβερνοασφάλεια. Έχω αναπτύξει το πλαίσιο με ονομασία **STAM** βάσει των παγκόσμιων πλαισίων κυβερνοασφάλειας όπως το NIST Cyber Security Framework και τα CIS Critical Security Controls, το οποίο είναι προσαρμοσμένο στην Εθνική Στρατηγική Κυβερνοασφάλειας 2020-2025 και στο Εθνικό Σχέδιο Δράσης για την κυβερνοασφάλεια. Επίσης, εναρμονίζεται με τις Οδηγίες της Ε.Ε. σχετικά με τα μέτρα για υψηλό κοινό επίπεδο κυβερνοασφάλειας σε ολόκληρη την Ένωση, Οδηγία (ΕΕ) 2016/1148 (Οδηγία NIS) και Οδηγία (ΕΕ) 2022/2555 (Οδηγία NIS2). Το πλαίσιο STAM περιλαμβάνει 20 θεματικές ενότητες δηλαδή 20 σημεία ελέγχου. Το κάθε σημείο ελέγχου περιλαμβάνει διασφαλίσεις, αριθμούνται συνολικά 205 διασφαλίσεις.

Η έρευνα αυτή απευθύνεται σε δημόσιους και ιδιωτικούς οργανισμούς μικρού έως μεσαίου μεγέθους (1 - 250 υπαλλήλους), με περιορισμένη τεχνογνωσία σε θέματα κυβερνοασφάλειας αλλά με την δυνατότητα να απασχολούν τουλάχιστον έναν (1) άνθρωπο ο οποίος ασχολείται υπεύθυνα με την διαχείριση και την προστασία της πληροφοριακής υποδομής.

Θα ήθελα να σας προσκαλέσω να συμμετέχετε και να αφιερώσετε λίγο από τον χρόνο σας.

Η συμμετοχή στην έρευνα είναι **ανώνυμη**. Για την πρόσβαση σας παρέχεται ένα License Key το οποίο δημιουργείτε μόνοι σας μέσω της εφαρμογής. Ο σκοπός του είναι να μπορείτε να διακόπτετε και να συνεχίζετε την εφαρμογή χρησιμοποιώντας ανώνυμα το υπάρχον κλειδί σας. Μέσω αυτού του πλαισίου θα ανακαλύψετε συνολικά το **Cyber Security Level** του οργανισμού σας αλλά και του κάθε σημείου ελέγχου. Κρατήστε το License Key ώστε να συνδέεστε όποτε εσείς επιθυμείτε.

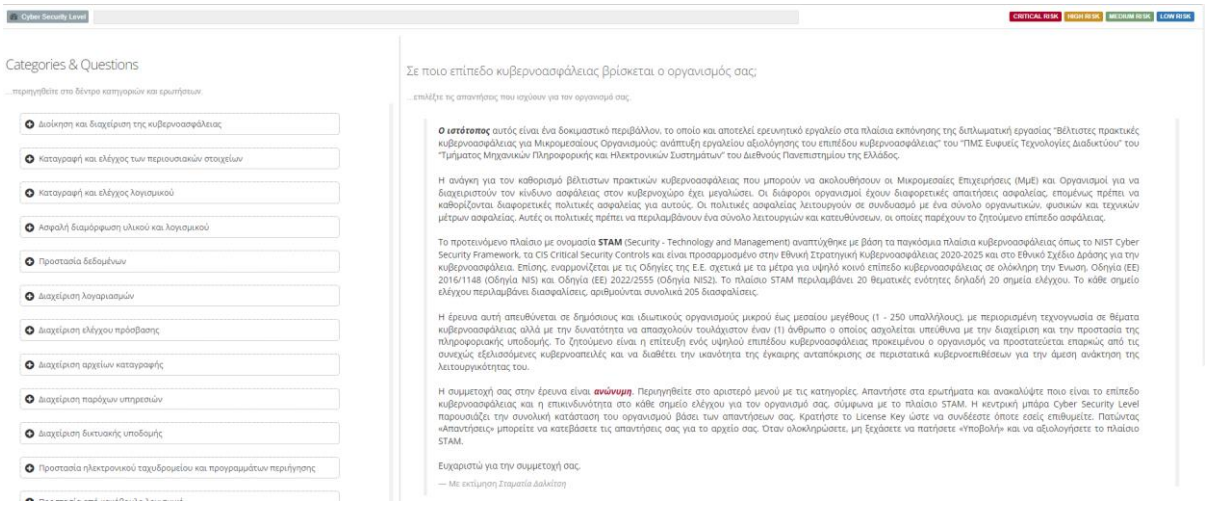
Αποκτήστε πρόσβαση από τον σύνδεσμο https://users.it.teithe.gr/~ait52019/

Για οποιαδήποτε διευκρίνηση ή πληροφορία μπορείτε να επικοινωνήσετε μαζί μου.

Σας ευχαριστώ εκ των προτέρων για τον χρόνο σας.

Με εκτίμηση
Σταματία Δαλκίτση

Εικόνα 35: Email πρόσκληση συμμετοχής στο ερευνητικό πλαίσιο STAM.



Cyber Security Level

CRITICAL RISK HIGH RISK MEDIUM RISK LOW RISK

Categories & Questions

...περιηγηθείτε στο δέντρο κατηγοριών και ερωτήσεων.

- Διοίκηση και διαχείριση της κυβερνοασφάλειας
- Καταγραφή και ελέγχος των περιουσιακών στοιχείων
- Καταγραφή και ελέγχος λογισμικού
- Ασφαλή διαμόρφωση υλικού και λογισμικού
- Προστασία δεδομένων
- Διαχείριση λογαριασμών
- Διαχείριση ελέγχου πρόσβασης
- Διαχείριση αρχείων καταγραφής
- Διαχείριση παρόχων υπηρεσιών
- Διαχείριση δικτυακής υποδομής
- Προστασία ηλεκτρονικού ταχυδρομείου και προγραμμάτων περιήγησης

Σε ποιο επίπεδο κυβερνοασφάλειας βρίσκεται ο οργανισμός σας;

...επιλέξτε τις απαντήσεις που ισχύουν για τον οργανισμό σας.

Ο ιστότοπος αυτός είναι ένα δοκιμαστικό περιβάλλον, το οποίο και αποτελεί ερευνητικό εργαλείο στα πλαίσια εκπόνησης της διπλωματική εργασίας "Βέλτιστες πρακτικές κυβερνοασφάλειας για Μικρομεσαίους Οργανισμούς: ανάπτυξη εργαλείου αξιολόγησης του επιπέδου κυβερνοασφάλειας" του "ΠΜΣ Ευφυείς Τεχνολογίες Διαδικτύου" του "Τμήματος Μηχανικών Πληροφορικής και Ηλεκτρονικών Συστημάτων" του Διεθνούς Πανεπιστημίου της Ελλάδος.

Η ανάγκη για τον καθορισμό βέλτιστων πρακτικών κυβερνοασφάλειας που μπορούν να ακολουθήσουν οι Μικρομεσαίες Επιχειρήσεις (ΜμΕ) και Οργανισμοί για να διαχειριστούν τον κίνδυνο ασφάλειας στον κυβερνοχώρο έχει μεγαλώσει. Οι διάφοροι οργανισμοί έχουν διαφορετικές απαιτήσεις ασφαλείας, επομένως πρέπει να καθορίζονται διαφορετικές πολιτικές ασφαλείας για αυτούς. Οι πολιτικές ασφαλείας λειτουργούν σε συνδυασμό με ένα σύνολο οργανωτικών, φυσικών και τεχνικών μέτρων ασφαλείας. Αυτές οι πολιτικές πρέπει να περιλαμβάνουν ένα σύνολο λειτουργιών και κατευθύνσεων, οι οποίες παρέχουν το ζητούμενο επίπεδο ασφάλειας.

Το προτεινόμενο πλαίσιο με ονομασία **STAM** (Security - Technology and Management) αναπτύχθηκε με βάση τα παγκόσμια πλαίσια κυβερνοασφάλειας όπως το NIST Cyber Security Framework, τα CIS Critical Security Controls και είναι προσαρμοσμένο στην Εθνική Στρατηγική Κυβερνοασφάλειας 2020-2025 και στο Εθνικό Σχέδιο Δράσης για την κυβερνοασφάλεια. Επίσης, εναρμονίζεται με τις Οδηγίες της Ε.Ε. σχετικά με τα μέτρα για υψηλό κοινό επίπεδο κυβερνοασφάλειας σε ολόκληρη την Ένωση, Οδηγία (ΕΕ) 2016/1148 (Οδηγία NIS) και Οδηγία (ΕΕ) 2022/2555 (Οδηγία NIS2). Το πλαίσιο STAM περιλαμβάνει 20 θεματικές ενότητες δηλαδή 20 σημεία ελέγχου. Το κάθε σημείο ελέγχου περιλαμβάνει διασφαλίσεις, αριθμούνται συνολικά 205 διασφαλίσεις.

Η έρευνα αυτή απευθύνεται σε δημόσιους και ιδιωτικούς οργανισμούς μικρού έως μεσαίου μεγέθους (1 - 250 υπαλλήλους), με περιορισμένη τεχνογνωσία σε θέματα κυβερνοασφάλειας αλλά με την δυνατότητα να απασχολούν τουλάχιστον έναν (1) άνθρωπο ο οποίος ασχολείται υπεύθυνα με την διαχείριση και την προστασία της πληροφοριακής υποδομής. Το ζητούμενο είναι η επίτευξη ενός υψηλού επιπέδου κυβερνοασφάλειας προκειμένου ο οργανισμός να προστατεύεται επαρκώς από τις συνεχώς εξελισσόμενες κυβερνοαπειλές και να διαθέτει την ικανότητα της έγκαιρης ανταπόκρισης σε περιστατικά κυβερνοεπιθέσεων για την άμεση ανάκτηση της λειτουργικότητας του.

Η συμμετοχή σας στην έρευνα είναι **ανώνυμη**. Περιηγηθείτε στο αριστερό μενού με τις κατηγορίες. Απαντήστε στα ερωτήματα και ανακαλύψτε ποιο είναι το επίπεδο κυβερνοασφάλειας και η επικινδυνότητα στο κάθε σημείο ελέγχου για τον οργανισμό σας, σύμφωνα με το πλαίσιο STAM. Η κεντρική μπάρα Cyber Security Level παρουσιάζει την συνολική κατάσταση του οργανισμού βάσει των απαντήσεων σας. Κρατήστε το License Key ώστε να συνδέεστε όποτε εσείς επιθυμείτε. Πατώντας «Απαντήσεις» μπορείτε να κατεβάσετε τις απαντήσεις σας για το αρχείο σας. Όταν ολοκληρώσετε, μη ξεχάσετε να πατήσετε «Υποβολή» και να αξιολογήσετε το πλαίσιο STAM.

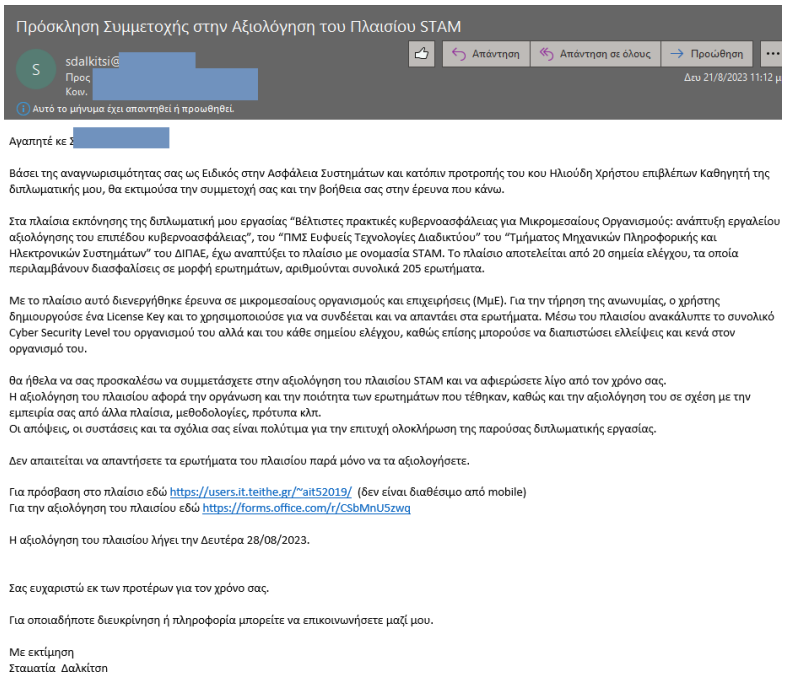
Ευχαριστώ για την συμμετοχή σας.

— Με εκτίμηση Σταματία Δαλκίτση

Εικόνα 36: Πληροφορίες που δόθηκαν στο ερωτηματολόγιο του πλαισίου STAM.

6.4.5. *Αξιολόγηση εργαλείου από Ειδικούς Ασφαλείας (CyberSecurity Experts)*

Η αξιολόγηση του πλαισίου STAM πραγματοποιήθηκε από Ειδικούς στην ασφάλεια συστημάτων και στην κυβερνοασφάλεια. Για την συμμετοχή στην αξιολόγηση χρησιμοποιήθηκε μια πρόσκληση μέσω email (Εικόνα 37).



Πρόσκληση Συμμετοχής στην Αξιολόγηση του Πλαισίου STAM

Απάντηση | Απάντηση σε όλους | Προώθηση

S sdalkitsi@[redacted]
Προς [redacted]
Κοιν.
Δευ 21/8/2023 11:12 μ

Αυτό το μήνυμα έχει απαντηθεί ή προωθηθεί.

Αγαπητέ κε [redacted]

Βάσει της αναγνωρισιμότητας σας ως Ειδικός στην Ασφάλεια Συστημάτων και κατόπιν προτροπής του κου Ηλιούδη Χρήστου επιβλέπων Καθηγητή της διπλωματικής μου, θα εκτιμούσα την συμμετοχή σας και την βοήθεια σας στην έρευνα που κάνω.

Στα πλαίσια εκπόνησης της διπλωματική μου εργασίας "Βέλτιστες πρακτικές κυβερνοασφάλειας για Μικρομεσαίους Οργανισμούς: ανάπτυξη εργαλείου αξιολόγησης του επιπέδου κυβερνοασφάλειας", του "ΠΜΣ Ευφυείς Τεχνολογίες Διαδικτύου" του "Τμήματος Μηχανικών Πληροφορικής και Ηλεκτρονικών Συστημάτων" του ΔΙΠΑΕ, έχω αναπτύξει το πλαίσιο με ονομασία STAM. Το πλαίσιο αποτελείται από 20 σημεία ελέγχου, τα οποία περιλαμβάνουν διασφαλίσεις σε μορφή ερωτημάτων, αριθμούνται συνολικά 205 ερωτήματα.

Με το πλαίσιο αυτό διενεργήθηκε έρευνα σε μικρομεσαίους οργανισμούς και επιχειρήσεις (ΜμΕ). Για την τήρηση της ανωνυμίας, ο χρήστης δημιουργούσε ένα License Key και το χρησιμοποιούσε για να συνδέεται και να απαντάει στα ερωτήματα. Μέσω του πλαισίου ανακάλυπτε το συνολικό Cyber Security Level του οργανισμού του αλλά και του κάθε σημείου ελέγχου, καθώς επίσης μπορούσε να διαπιστώσει ελλείψεις και κενά στον οργανισμό του.

θα ήθελα να σας προσκαλέσω να συμμετάσχετε στην αξιολόγηση του πλαισίου STAM και να αφιερώσετε λίγο από τον χρόνο σας.
Η αξιολόγηση του πλαισίου αφορά την οργάνωση και την ποιότητα των ερωτημάτων που τέθηκαν, καθώς και την αξιολόγηση του σε σχέση με την εμπειρία σας από άλλα πλαίσια, μεθοδολογίες, πρότυπα κλπ.
Οι απόψεις, οι συστάσεις και τα σχόλια σας είναι πολύτιμα για την επιτυχή ολοκλήρωση της παρούσας διπλωματικής εργασίας.

Δεν απαιτείται να απαντήσετε τα ερωτήματα του πλαισίου παρά μόνο να τα αξιολογήσετε.

Για πρόσβαση στο πλαίσιο εδώ https://users.it.teithe.gr/~ait52019/ (δεν είναι διαθέσιμο από mobile)
Για την αξιολόγηση του πλαισίου εδώ https://forms.office.com/r/CSbMnU5zwq

Η αξιολόγηση του πλαισίου λήγει την Δευτέρα 28/08/2023.

Σας ευχαριστώ εκ των προτέρων για τον χρόνο σας.

Για οποιαδήποτε διευκρίνηση ή πληροφορία μπορείτε να επικοινωνήσετε μαζί μου.

Με εκτίμηση
Σταματία Δαλκίτση

Εικόνα 37: email Πρόσκληση συμμετοχής στην αξιολόγηση του πλαισίου STAM.

Η αξιολόγηση αυτή, δεν απαιτούσε συμπλήρωση του ερωτηματολογίου από τους Ειδικούς, παρά μόνο την μελέτη των σημείων ελέγχου, των διασφαλίσεων και των ερωτημάτων που τέθηκαν κατά την έ-ρευνα. Αυτή, πραγματοποιήθηκε μέσω της φόρμας https://forms.office.com/r/CSbMnU5zwq . Ζητή-θηκε από του Ειδικούς χρήστες να δηλώσουν:

- Ονοματεπώνυμο
- Επαγγελματικός Τίτλος / Θέση
- Email Επικοινωνίας
- Τηλέφωνο Επικοινωνίας

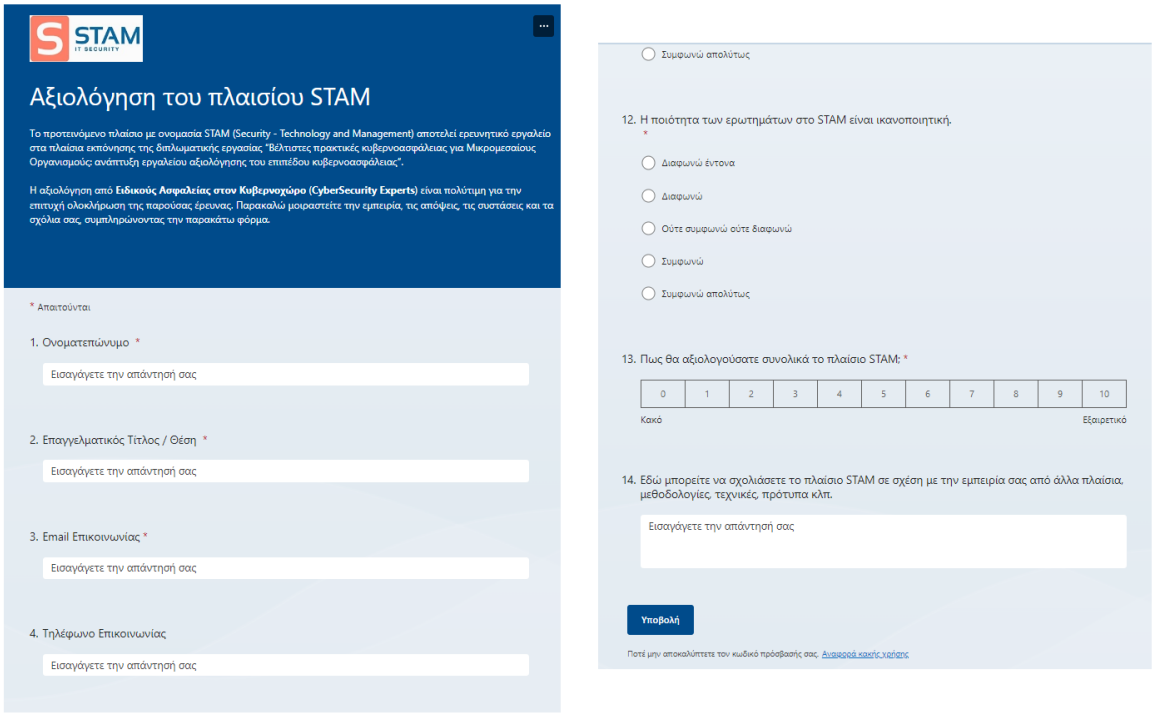
Στη συνέχεια να απαντήσουν στα παρακάτω ερωτήματα:

1) Το πλαίσιο STAM αποτελεί ένα γενικό πλαίσιο αξιολόγησης του επιπέδου κυβερνοασφάλειας των μικρομεσαίων οργανισμών και επιχειρήσεων (ΜμΕ).
2) Το STAM συνεισφέρει στις ΜμΕ για την λήψη στρατηγικών αποφάσεων σχετικά με την κυ-βερνοασφάλεια.
3) Τα σημεία ελέγχου του STAM καλύπτουν τις βέλτιστες πρακτικές κυβερνοασφάλειας.
4) Το STAM ακολουθεί τις τεχνολογικές εξελίξεις.
5) Το STAM αποτελεί ένα αρχικό σημείο για τον έλεγχο της θωράκισης των συστημάτων των ΜμΕ μέσω ενισχυμένων απαιτήσεων ασφαλείας.
6) Το STAM συμβάλει στον σχεδιασμό και την ενδυνάμωση των μηχανισμών ασφαλείας.

7) Το STAM προάγει την προστασία των κρίσιμων υποδομών.
8) Η ποιότητα των ερωτημάτων στο STAM είναι ικανοποιητική.

Τέλος, δόθηκε η δυνατότητα να βαθμολογήσουν το πλαίσιο STAM και να αφήσουν δικά τους σχόλια. Συγκεκριμένα:

- Πως θα αξιολογούσατε συνολικά το πλαίσιο STAM;
- Εδώ μπορείτε να σχολιάσετε το πλαίσιο STAM σε σχέση με την εμπειρία σας από άλλα πλαίσια, μεθοδολογίες, τεχνικές, πρότυπα κλπ

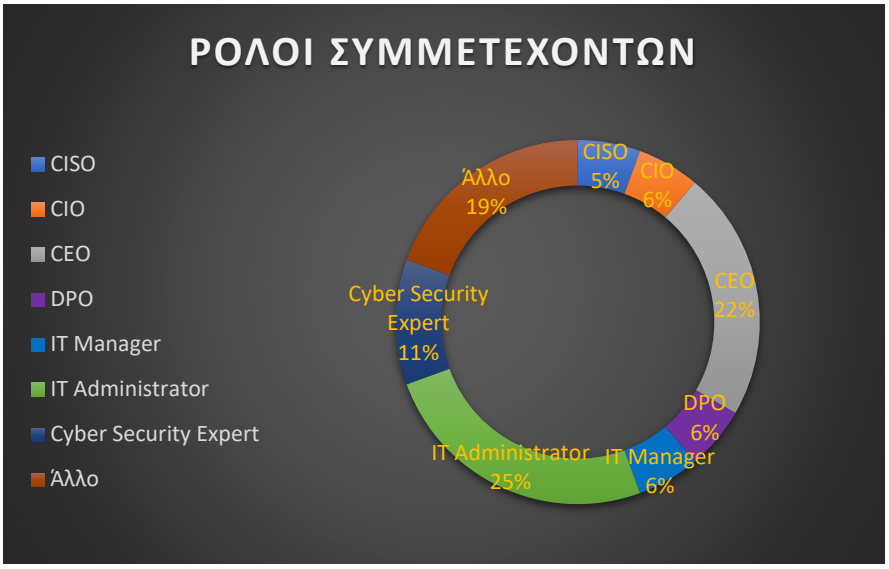


Εικόνα 38: Φόρμα αξιολόγησης του πλαισίου STAM.

6.5. Αποτελέσματα εργαλείου

Στην έρευνα αυτή, προσκλήθηκαν περισσότερες από 40 ΜμΕ και πραγματοποιήθηκαν 36 εγγραφές. Οι ρόλοι αυτών των χρηστών παρουσιάζονται στο Διάγραμμα 3. Ενώ, ο αριθμός των υπαλλήλων αυτών των ΜμΕ παρουσιάζεται στο Διάγραμμα 4. Συμμετείχαν, επτά (7) μικρές επιχειρήσεις όπου ο αριθμός των υπαλλήλων κυμαίνεται από 1 έως 10 και δεκατέσσερις (14) επιχειρήσεις όπου ο αριθμός των υπαλλήλων κυμαίνεται από 11 έως 50. Επίσης, δεκαπέντε (15) μεσαίες επιχειρήσεις, όπου οι δύο από αυτές διαθέτουν αριθμό υπαλλήλων από 51 έως 100 και οι υπόλοιπες περισσότερους.

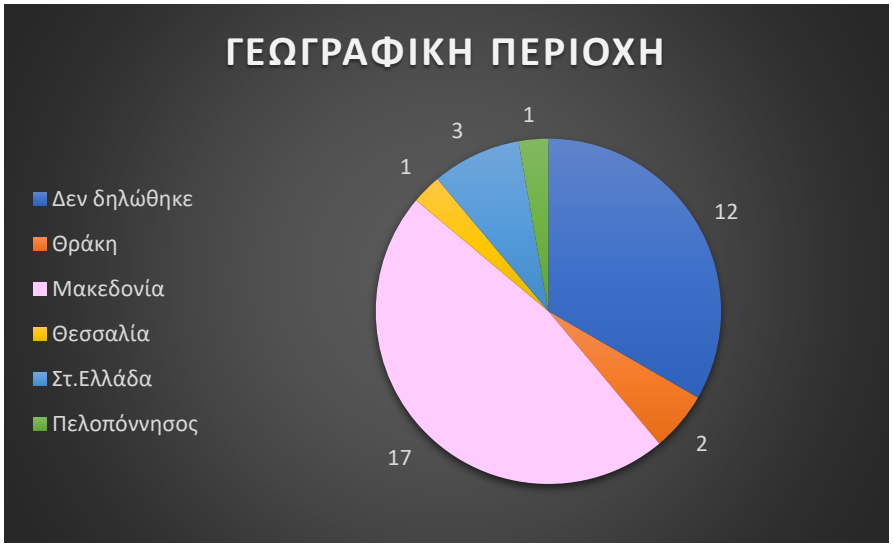
Διάγραμμα 3: Ρόλοι/Θέσεις των συμμετεχόντων.



Διάγραμμα 4: ΜμΕ σύμφωνα με τον αριθμό των υπαλλήλων τους.

Σύμφωνα με τα προαιρετικά στοιχεία που δηλώθηκαν, οι περιοχές που συμμετείχαν στην έρευνα είναι πέντε (5), Θράκη, Μακεδονία, Θεσσαλία, Στερεά Ελλάδα και Πελοπόννησος, όπως παρουσιάζονται στο Διάγραμμα 5. Οι πέντε (5) διαφορετικές νομικές μορφές των ΜμΕ που συμμετείχαν στην έρευνα παρουσιάζονται στο Διάγραμμα 6.

Διάγραμμα 5: Γεωγραφική περιοχή συμμετεχόντων.



Διάγραμμα 6: Νομική μορφή των ΜμΕ που συμμετείχαν.

Οι χρήστες δεν ολοκλήρωσαν όλοι το ερωτηματολόγιο, ενώ κάποιοι ολοκλήρωσαν και δεν προχώρησαν στην υποβολή των απαντήσεων τους. Μόνο 21 από αυτούς προχώρησαν σε υποβολή των απαντήσεων τους. Ιδιαίτερο ενδιαφέρον παρουσιάζουν τα παρακάτω στοιχεία:

- Οι 18 οργανισμοί, διαθέτουν καταγεγραμμένη πολιτική ασφάλειας, επικεντρωμένη στην ασφάλεια του πληροφοριακού συστήματος και την κυβερνοασφάλεια, εγκεκριμένη από την Διοίκηση.
- Οι 17 οργανισμοί, διαθέτουν επιμέρους πολιτικές ασφαλείας, διαδικασίες, κανόνες και οδηγίες για συγκεκριμένα πεδία, στις οποίες περιγράφεται ο τρόπος εφαρμογής των τεχνικών και οργανωτικών μέτρων προστασίας.
- Οι 12 οργανισμοί, έχουν ορίσει στέλεχος υπεύθυνο ασφαλείας του πληροφοριακού συστήματος (Chief Information Security Officer – CISO), με αρμοδιότητες την διαχείριση της ασφάλειας του πληροφοριακού συστήματος.
- Οι 13 οργανισμοί, έχουν ορίσει στέλεχος υπεύθυνο προστασίας δεδομένων (Data Protection Officer – DPO), με αρμοδιότητες τη συμμόρφωση του οργανισμού με τον GDPR και τις

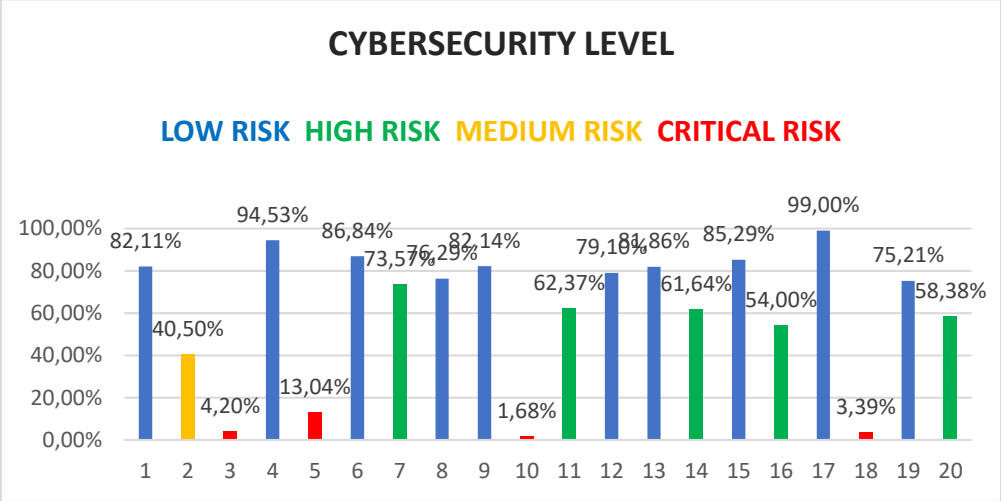
υποχρεώσεις του σχετικά με την προστασία των προσωπικών δεδομένων, της ιδιωτικότητας και του απορρήτου.

- Οι 5 οργανισμοί, δήλωσαν ότι έχουν πιστοποιηθεί και υλοποιούν ένα ολοκληρωμένο Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών (ISMS), όπως ISO 27001 ή άλλο διεθνώς αποδεκτό.
- Οι 4 οργανισμοί, δεσμεύουν ποσό κατά τον ετήσιο προϋπολογισμό τους, για την διαχείριση και υλοποίηση των έργων σχετικά με την ασφάλεια του πληροφοριακού συστήματος και την κυβερνοασφάλεια.
- Οι 5 οργανισμοί. διαθέτουν καταγεγραμμένη πολιτική για την διασφάλιση της επιχειρηματικής συνέχειας και έχουν αναπτύξει σχέδιο αποκατάστασης από καταστροφή (Disaster Recovery Plan), με σκοπό την άμεση αποκατάσταση από ανεπιθύμητο συμβάν. Ενώ άλλοι 5 οργανισμοί το υλοποιούν μερικώς.
- Όλοι οι οργανισμοί, διαθέτουν τμήμα αρμόδιο για την ασφάλεια του πληροφοριακού συστήματος.
- Οι 12 οργανισμοί, διαθέτουν επικαιροποιημένο και λεπτομερή κατάλογο (Asset Inventory) με τα υλικά αγαθά πληροφορικής.
- Οι 12 οργανισμοί, διαθέτουν επικαιροποιημένο και λεπτομερή κατάλογο (Software Inventory) με τα αδειοδοτημένα λογισμικά του.
- Ενώ εννέα (9) οργανισμοί, διαθέτουν Asset Inventory και Software Inventory.
- Οι 10 οργανισμοί, εφαρμόζουν διαδικασία ασφαλούς παραμετροποίησης με βάση τα διεθνώς αποδεκτά πρότυπα στις δικτυακές συσκευές, στους διακομιστές και στους σταθμούς εργασίας και χρησιμοποιούν μόνο υποστηριζόμενες εκδόσεις λειτουργικών συστημάτων για τους διακομιστές, τους σταθμούς εργασία και τις δικτυακές συσκευές.
- Οι 12 οργανισμοί, διασφαλίζουν κατά την πρώτη εγκατάσταση του λογισμικού και του εξοπλισμού πως όλα τα προεπιλεγμένα συνθηματικά τροποποιούνται.
- Οι 8 οργανισμοί εφαρμόζουν τεχνικά μέτρα κρυπτογράφησης δεδομένων στους φορητούς υπολογιστές (laptop, netbook, tablet, smart phone).
- Οι 5 οργανισμοί, εφαρμόζουν τεχνικά μέτρα κρυπτογράφησης δεδομένων στα αφαιρούμενα μέσα (εξωτερικοί δίσκοι, usb flash memory και άλλα).
- Οι 12 οργανισμοί, διατηρούν κατάλογο όλων των λογαριασμών που διαχειρίζονται, με ονοματεπώνυμο και προνόμια.
- Οι 3 οργανισμοί, διατηρούν κατάλογο παρόχων υπηρεσιών, διαθέτουν καταγεγραμμένη πολιτική διαχείρισης των παρόχων υπηρεσιών, ταξινομούν τους παρόχους υπηρεσιών συμπεριλαμβάνοντας χαρακτηριστικά όπως ευαισθησία δεδομένων, διασφαλίζουν ότι οι συμβάσεις παρόχων υπηρεσιών περιλαμβάνουν απαιτήσεις ασφαλείας και εφαρμόζουν διαδικασία για τον ασφαλής παροπλισμός των παρόχων υπηρεσιών.
- Όλοι οι οργανισμοί, εφαρμόζουν πλήρως ή μερικώς MFA (Multi Factor Authentication) για εφαρμογές που εκτίθενται εξωτερικά ή/και για απομακρυσμένη πρόσβαση στο δίκτυο ή/και για πρόσβαση λογαριασμών διαχειριστών ή/και για πρόσβαση σε κρίσιμα δεδομένα.
- Οι 9 οργανισμοί, έχουν κεντρικοποιήσει πλήρως την αυθεντικοποίηση, την εξουσιοδότηση και τον έλεγχο (Authentication Authorization Audit - AAA) του δικτύου.
- Οι 14 οργανισμοί, έχουν διαχωρίσει πλήρως το εσωτερικό τους δίκτυο σε διακριτά υποδίκτυα βάσει της ευαισθησίας των επιχειρησιακών στόχων.
- Οι 12 οργανισμοί, επιβάλλουν δικτυακά φίλτρα διευθύνσεων URL, με σκοπό τον περιορισμό σύνδεσης σε ιστότοπους μη εγκεκριμένους από την πολιτική ασφαλείας τους.
- Οι 13 οργανισμοί, αποκλείουν περιττούς τύπους αρχείων που επιχειρούν να εισέλθουν μέσω email στον οργανισμό.
- Οι 14 οργανισμοί, διαθέτουν εγκατεστημένο λογισμικό κατά του κακόβουλου λογισμικού (anti-malware) σε όλα τα περιουσιακά στοιχεία τους, λαμβάνουν ενημερώσεις για τα αρχεία υπογραφών anti-malware με αυτοματοποιημένο τρόπο και σε τακτά χρονικά διαστήματα, και έχουν εφαρμόσει κεντρική διαχείριση του anti-malware.
- Οι 9 οργανισμοί, διασφαλίζουν ότι στην ανάπτυξη διαδικτυακών εφαρμογών λαμβάνονται υπόψη κοινοί τύποι ευπαθειών, όπως για παράδειγμα OWASP Top-10.

- Οι 12 οργανισμοί, επιτρέπουν την πρόσβαση στους επιχειρησιακούς πόρους με βάση το ενημερωμένο εγκατεστημένο λογισμικό κατά του κακόβουλου λογισμικού, τη συμμόρφωση με την ασφαλής διαμόρφωση και τη διασφάλιση της επικαιροποίησης του λειτουργικού συστήματος και των εφαρμογών.
- Οι 10 οργανισμοί, εκπαιδεύουν και ενημερώνουν τους υπαλλήλους για την αναγνώριση επιθέσεων social engineering και μόνο 5 από αυτούς διενεργούν σε περιοδική βάση ασκήσεις προσομοίωσης περιστατικών κυβερνοασφάλειας όπως για παράδειγμα phishing mail.
- Οι 15 οργανισμοί, εκτελούν αυτοματοποιημένη διαδικασία αντίγραφών ασφαλείας, με τουλάχιστον ημερήσια συχνότητα στα κρίσιμα και ευαίσθητα δεδομένα. Οι 14 από αυτούς προστατεύουν τα αντίγραφα ασφαλείας με ελέγχους ισοδύναμους με τους ελέγχους των αρχικών δεδομένων, όπως για παράδειγμα κρυπτογράφηση, φυσική ασφάλεια και administrative credentials, και συγχρόνως διασφαλίζουν την ολοκλήρωση των διαδικασιών των αντιγράφων ασφαλείας. Ενώ μόνο οι 13 από αυτούς συνδυάζουν με τον κατάλληλο τρόπο τις τεχνολογίες Full, Incremental και Differential Backup. Από αυτούς, μόνο 4 οργανισμοί δημιουργούν και διατηρούν απομονωμένα αντίγραφα ασφαλείας, όπως για παράδειγμα μέσω συστημάτων ή υπηρεσιών εκτός σύνδεσης, νέφους ή εκτός τοποθεσίας και οι 3 τηρούν τον κανόνα αντιγράφων ασφαλείας 3-2-1-1-0.
- Οι 10 οργανισμοί, διαθέτουν καταγεγραμμένη πολιτική για την αντιμετώπιση περιστατικών κυβερνοασφάλειας και έχουν καθορίσει βασικούς ρόλους και αρμοδιότητες για την αντιμετώπιση περιστατικών, ενώ μόνο 3 έχουν σχεδιάσει και διεξάγει ασκήσεις και σενάρια αντιμετώπισης συμβάντων για το βασικό προσωπικό που εμπλέκεται στο συμβάν ώστε να προετοιμαστεί για την αντιμετώπιση πραγματικών περιστατικών, με δοκιμές σε ετήσια βάση.
- Οι 8 οργανισμοί, έχουν καθιερώσει και διατηρούν ένα πρόγραμμα δοκιμών διείσδυσης (Penetration Testing – PenTest) κατάλληλο για το μέγεθος, την πολυπλοκότητα και την ωριμότητα του οργανισμού. Οι 5 από αυτούς εκτελούν περιοδικές δοκιμές εξωτερικής διείσδυσης τουλάχιστον ετησίως, απαιτούν εξειδικευμένη δεξιότητα και εμπειρία του ανθρώπου ή του φορέα που εκτελεί το PenTest και διαθέτουν διαδικασία αποκατάσταση των ευρημάτων των.
- Οι 11 οργανισμοί, δήλωσαν ότι εφαρμόζουν αυτοματοποιημένη διαχείριση ενημερώσεων και διορθώσεων των λειτουργικών συστημάτων, τουλάχιστον σε μηνιαία βάση. Οι 9 από αυτούς, εφαρμόζουν αυτοματοποιημένη διαχείριση ενημερώσεων και διορθώσεων εφαρμογών, τουλάχιστον σε μηνιαία βάση. Ενώ μόνο 7 από αυτούς, εφαρμόζουν αυτοματοποιημένες σαρώσεις τρωτότητας των εσωτερικών επιχειρησιακών περιουσιακών στοιχείων, τουλάχιστον σε τριμηνιαία βάση. Καθώς επίσης, 5 από αυτούς εφαρμόζουν αυτοματοποιημένες σαρώσεις τρωτότητας των εξωτερικών εκτεθειμένων επιχειρησιακών περιουσιακών στοιχείων, τουλάχιστον σε μηνιαία βάση.
- Οι 15 οργανισμοί, διαθέτουν σύστημα Uninterruptible Power Supply (UPS) για την αδιάλειπτη παροχή ρεύματος του κρίσιμου εξοπλισμού.
- Οι 10 οργανισμοί, διαθέτουν αυτοματοποιημένους ελεγκτές θερμοκρασίας, υγρασία και πίεσης στις εγκαταστάσεις που φιλοξενούν τον κρίσιμο εξοπλισμό.
- Οι 10 οργανισμοί, διαθέτουν πλεονασμό (redundancy) σε κρίσιμα συστήματα και κυκλώματα δικτύωσης. Ενώ 8 είναι οι οργανισμοί, που διαθέτουν UPS και redundancy στον κρίσιμο εξοπλισμό.
- Οι 5 οργανισμοί, έχουν καθιερώσει ειδικούς κανόνες για την διαχείριση της ασφάλειας των κρίσιμων εγκαταστάσεων και διασφαλίζουν ότι οι κρίσιμες εγκαταστάσεις διαθέτουν μηχανισμούς ελέγχου για την προστασία από μη εξουσιοδοτημένη πρόσβαση. Οι 4 από αυτούς τηρούν κατάλογο των εξουσιοδοτημένων ατόμων με πρόσβαση στον κρίσιμο εξοπλισμό ή στον χώρο που φιλοξενείται ο κρίσιμος εξοπλισμός.

Στο Διάγραμμα 7, παρουσιάζεται το συνολικό επίπεδο ασφάλειας της κάθε εταιρείας, σύμφωνα με τις απαντήσεις που έδωσαν στα σημεία ελέγχου. Το cybersecurity level είναι σε ποσοστό (%) και το χρώμα αποτυπώνει τον βαθμό επικινδυνότητας.

Διάγραμμα 7: Cybersecurity Level των ΜμΕ.

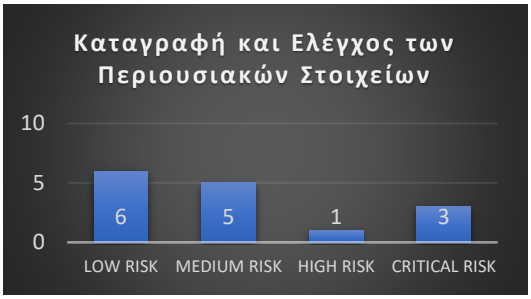


Κατά την υποβολή του ερωτηματολογίου, κάποιοι χρήστες άφησαν κάποια ερωτήματα αναπάντητα. Για στατιστικούς λόγους χρησιμοποιήθηκαν μόνο 15 εταιρείες που έχουν ολοκληρώσει πλήρως το ερωτηματολόγιο και το έχουν υποβάλει.

Διάγραμμα 8: Επικινδυνότητα οργανισμών στο σημείο ελέγχου Διοίκηση και Διαχείριση της Κυβερνοασφάλειας.

Διάγραμμα 9: Επικινδυνότητα οργανισμών στο σημείο ελέγχου Καταγραφή και Ελέγχος Λογισμικού.

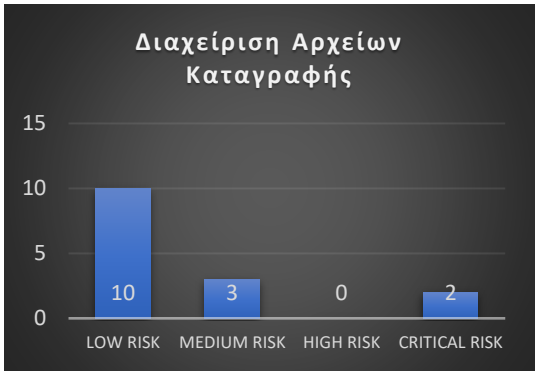
Διάγραμμα 10: Επικινδυνότητα οργανισμών στο σημείο ελέγχου Καταγραφή και Ελέγχος των Περιουσιακών Στοιχείων.



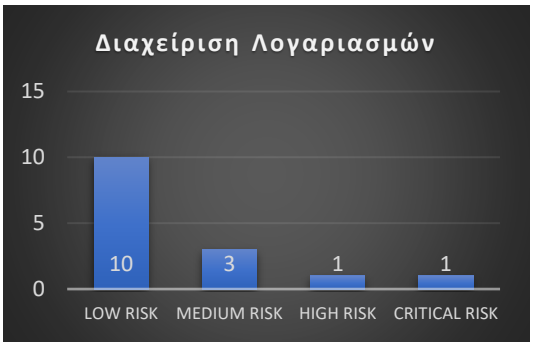
Διάγραμμα 11: Επικινδυνότητα οργανισμών στο σημείο ελέγχου Ασφαλή Διαμόρφωση Υλικού και Λογισμικού.

Διάγραμμα 12: Επικινδυνότητα οργανισμών στο σημείο ελέγχου Προστασία Δεδομένων.

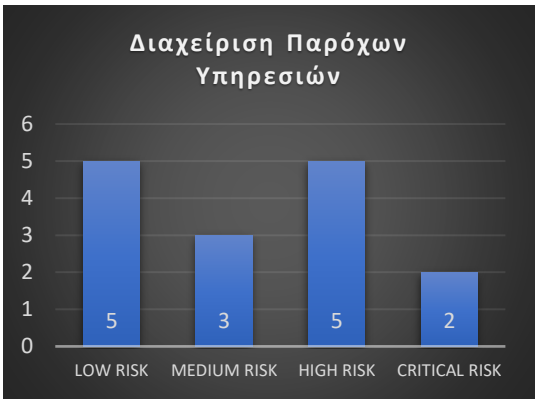
Διάγραμμα 13: Επικινδυνότητα οργανισμών στο σημείο ελέγχου Διαχείριση Αρχείων Καταγραφής.



Διάγραμμα 14: Επικινδυνότητα οργανισμών στο σημείο ελέγχου Διαχείριση Λογαριασμών.

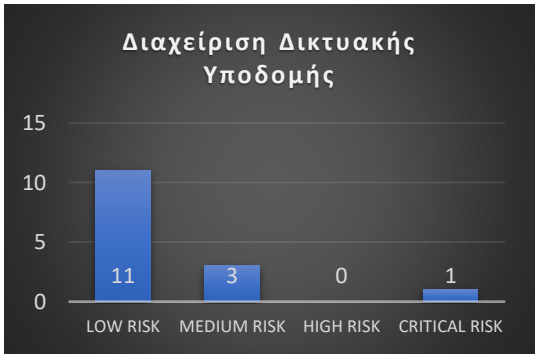


Διάγραμμα 15: Επικινδυνότητα οργανισμών στο σημείο ελέγχου Διαχείριση Παρόχων Υπηρεσιών.



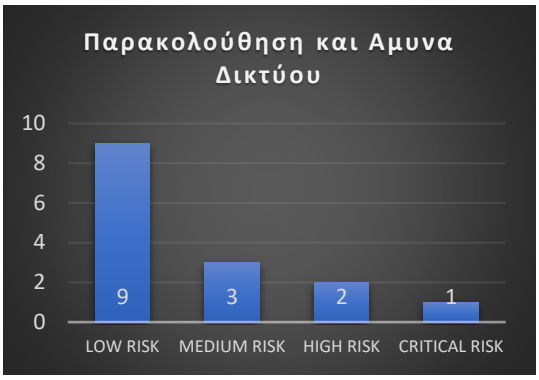
Διάγραμμα 16: Επικινδυνότητα οργανισμών στο σημείο ελέγχου Διαχείριση Ελέγχου Πρόσβασης.

Διάγραμμα 17: Επικινδυνότητα οργανισμών στο σημείο ελέγχου Διαχείριση Δικτυακής Υποδομής.

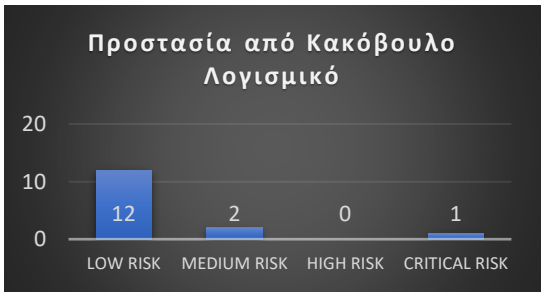


Διάγραμμα 18: Επικινδυνότητα οργανισμών στο σημείο ελέγχου Προστασία Ηλεκτρονικού Ταχυδρομείου και Προγραμμάτων Περιήγησης.

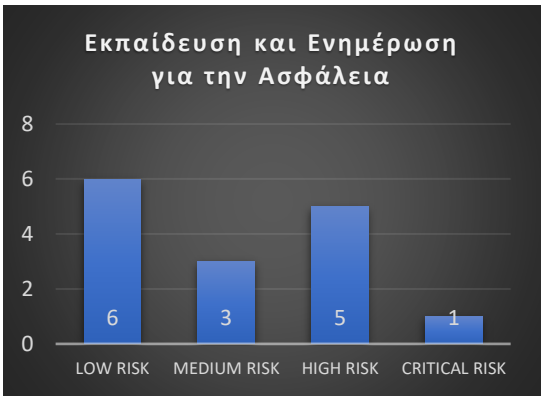
Διάγραμμα 19: Επικινδυνότητα οργανισμών στο σημείο ελέγχου Παρακολούθηση και Άμυνα Δικτύου.



Διάγραμμα 20: Επικινδυνότητα οργανισμών στο σημείο ελέγχου Προστασία από Κακόβουλο Λογισμικό.

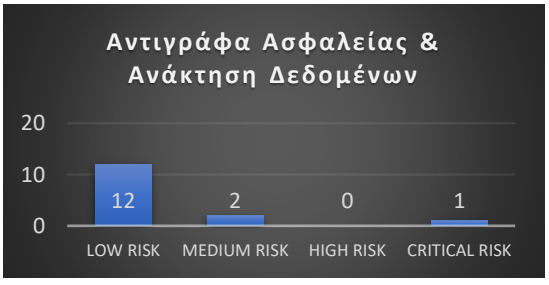


Διάγραμμα 21: Επικινδυνότητα οργανισμών στο σημείο ελέγχου Εκπαίδευση και Ενημέρωση για την Ασφάλεια.



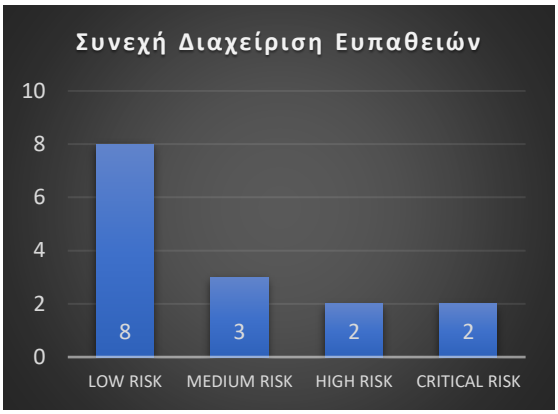
Διάγραμμα 22: Επικινδυνότητα οργανισμών στο σημείο ελέγχου Ασφάλεια Εφαρμογών Λογισμικού.

Διάγραμμα 23: Επικινδυνότητα οργανισμών στο σημείο ελέγχου Αντίγραφα Ασφαλείας & Ανάκτηση Δεδομένων.

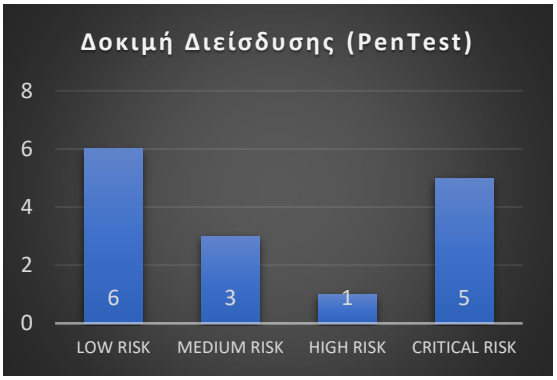


Διάγραμμα 24: Επικινδυνότητα οργανισμών στο σημείο ελέγχου Διαχείριση Αντιμετώπισης Περιστατικών.

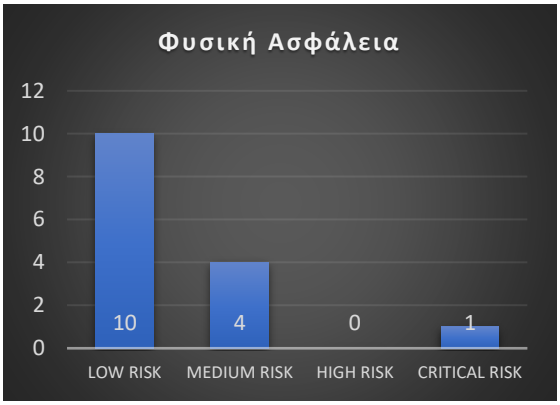
Διάγραμμα 25: Επικινδυνότητα οργανισμών στο σημείο ελέγχου Συνεχή Διαχείριση Ευπαθειών.



Διάγραμμα 26: Επικινδυνότητα οργανισμών στο σημείο ελέγχου Δοκιμή Διείσδυσης (Pen Test).



Διάγραμμα 27: Επικινδυνότητα οργανισμών στο σημείο ελέγχου Φυσική Ασφάλεια.



Από την διεξαχθείσα έρευνα, όπως απεικονίζεται και στα παραπάνω Διαγράμματα, διαπιστώθηκαν τα εξής:

- Οι οργανισμοί, βρίσκονται σε διαρκή προσπάθεια και λαμβάνουν αρκετά μέτρα για την συνεχή διαχείριση των ευπαθειών.
- Όλοι οι οργανισμοί που συμμετείχαν στην έρευνα, λαμβάνουν υψηλά μέτρα για την φυσική ασφάλεια.
- Όλοι οι οργανισμοί, λαμβάνουν μέτρα για τα αντίγραφα ασφαλείας και την ανάκτηση δεδομένων.
- Το μεγαλύτερο ποσοστό των οργανισμών, έχει ενσωματώσει στα συστήματα του μέτρα για την διαχείριση των αρχείων καταγραφής.
- Οι περισσότεροι οργανισμοί, εφαρμόζουν διαδικασίες και έχουν ενσωματώσει μέτρα για την καταγραφή και την διαχείριση των περιουσιακών στοιχείων και του λογισμικού. Καθώς επίσης και για την ασφαλή διαμόρφωση υλικού και λογισμικού και για την διαχείριση ελέγχου πρόσβασης.
- Οι οργανισμοί, φροντίζουν για την προστασία του ηλεκτρονικού ταχυδρομείου και των προγραμμάτων περιήγησης και λαμβάνουν μέτρα για την παρακολούθηση και την άμυνα του δικτύου.
- Αρκετοί οργανισμοί, έχουν προχωρήσει σε μέτρα σχετικά με την δοκιμή διείσδυσης (PenTest).
- Οι περισσότεροι οργανισμοί, έχουν λάβει σοβαρά μέτρα για την αντιμετώπιση των περιστατικών.
- Υψηλό ποσοστό των οργανισμών, παρατηρήθηκε στην προστασία από κακόβουλο λογισμικό και στην διαχείριση της δικτυακής υποδομής.

- Οι οργανισμοί, δεν έχουν ωριμάσει στην διοίκηση και την διαχείριση της κυβερνοασφάλειας. Μόνο το 25% έχει λάβει σοβαρά υπόψη του το διαχειριστικό μέρος της κυβερνοασφάλειας και έχει ενσωματώσει διαδικασίες και μέτρα στον οργανισμό.
- Αρκετοί οργανισμοί, δεν έχουν εναρμονιστεί πλήρως με τα μέτρα προστασίας των δεδομένων.
- Το 50% των οργανισμών, εναρμονίζεται με μέτρα για την ασφαλή διαχείριση των παρόχων υπηρεσιών.
- Σημαντικό είναι το ποσοστό των οργανισμών, που δεν λαμβάνει μέτρα για την ασφάλεια των εφαρμογών λογισμικού.
- Αρκετοί είναι οι οργανισμοί, που δεν λαμβάνουν σοβαρά υπόψη τους την εκπαίδευση και την ενημέρωση του προσωπικού για την ασφάλεια.

Από την ανατροφοδότηση των χρηστών, διαπιστώθηκε ότι όλοι συμφώνησαν στο ότι το περιβάλλον ήταν εύχρηστο και πλοηγήθηκαν με άνεση, προσέφερε στην αξιολόγηση του επιπέδου της κυβερνοασφάλειας του οργανισμού τους και πως η ποιότητα των ερωτημάτων που τέθηκαν ήταν ικανοποιητική. Επίσης, ότι θα πρότειναν το STAM σε έναν συνεργάτη ή φίλο τους (Εικόνα 39).

license_id	feedback1	feedback2	feedback3	feedback4	feedback_text	feedback_login_date	feedback_lock
STAM_US_64D92CC2	Yes	Yes	Yes	Yes	Up to date questionnaire with the latest trends in...	2023-08-13 23:18:34	open
STAM_US_64D9D9CF	Yes	Yes	Yes	Yes		2023-08-14 11:03:53	open
STAM_US_64D9E122	Yes	Yes	Yes	Yes	Το ερωτηματολόγιο έχει εξαιρετικές ερωτήσεις που α...	2023-08-14 11:38:47	open
STAM_US_64DB9DC6	Yes	Yes	Yes	Yes	Το usetr interface χρήζει βελτίωση.	2023-08-15 19:25:04	open
STAM_US_64DC5940	Yes	Yes	Yes	Yes		2023-08-16 08:53:39	open
STAM_US_64DC921C	Yes	Yes	Yes	Yes	Το ερωτηματολόγιο βοήθησε στον εντοπισμό κενών ασφ...	2023-08-16 12:58:32	open
STAM_US_64DCA14B	Yes	Yes	Yes	Yes		2023-08-16 13:46:01	open
STAM_US_64DC859D	Yes	Yes	Yes	Yes		2023-08-16 16:55:35	open
STAM_US_64DCA114	Yes	Yes	Yes	Yes		2023-08-17 10:02:58	open
STAM_US_64D3DD38	Yes	Yes	Yes	Yes	Το ερωτηματολόγιο είναι οργανωμένο. Δείχνει ότι μπ...	2023-08-19 18:05:54	open
STAM_US_64E0E0AB	Yes	Yes	Yes	Yes	Κατά τη συμπλήρωση του ερωτηματολογίου εντοπίστηκα...	2023-08-19 19:30:57	open
STAM_US_64E0DD15	Yes		Yes	Yes	Το ερωτηματολόγιο είναι καλά ενημερωμένο στις καλέ...	2023-08-19 19:50:49	open
STAM_US_64E0DE8A	Yes	Yes	Yes	Yes	Ευχαριστώ, έβγαλα αξιολογα συμπεράσματα για την κα...	2023-08-19 20:26:56	open
STAM_US_64E0FC1F	Yes	Yes	Yes	Yes	ΕΓΙΝΕ ΚΑΛΗ ΔΟΥΛΕΙΑ ΜΕ ΤΙΣ ΕΡΩΤΗΣΕΙΣ.	2023-08-19 21:10:51	open
STAM_US_64E108A8	Yes	Yes	Yes	Yes		2023-08-19 23:02:43	open

Εικόνα 39: Feedback χρηστών.

Τέλος, στο σημείο αυτό μπορούν να αναφερθούν κάποια από τα σχόλια των χρηστών:

"Up to date questionnaire with the latest trends in cybersecurity."

"Το ερωτηματολόγιο έχει εξαιρετικές ερωτήσεις που ακολουθούν τα best practices και θα αποτελούσαν τις πρώτες κατευθυντήριες γραμμές για έναν οργανισμό που τώρα θέλει να εφαρμόσει ασφαλή πρωτόκολλα. Το ερωτηματολόγιο θα έπρεπε να βγάζει διαφορετικές ερωτήσεις ανάλογα με το μέγεθος της εταιρίας καθώς μια εταιρία 10 ατόμων δεν έχει τις ίδιες ανάγκες με μια εταιρία 250 ατόμων. Επίσης, δεν είναι όλες οι ερωτήσεις σχετικές για κάθε εταιρία. Θα έπρεπε να γίνεται κάποιου είδους scoping ώστε ερωτήσεις οι οποίες δεν ανταποκρίνονται σε αυτόν που συμπληρώνει το ερωτηματολόγιο να μην υπολογίζονται."

"Το ερωτηματολόγιο βοήθησε στον εντοπισμό κενών ασφαλείας. Ανάδειξε σημαντικά κενά στην ασφάλεια τα οποία θα αντιμετωπίσει η εταιρεία με μελλοντικές ενέργειες."

"Κατά τη συμπλήρωση του ερωτηματολογίου εντοπίστηκαν κάποια τεχνικά μέτρα που δεν υλοποιούνται στην εταιρεία. Συγχαρητήρια για τη δουλειά σας."

"Το ερωτηματολόγιο είναι καλά ενημερωμένο στις καλές πρακτικές για την ασφάλεια."

"Ευχαριστώ, έβγαλα αξιόλογα συμπεράσματα για την κατάσταση της ασφάλειας στην εταιρείας μας."

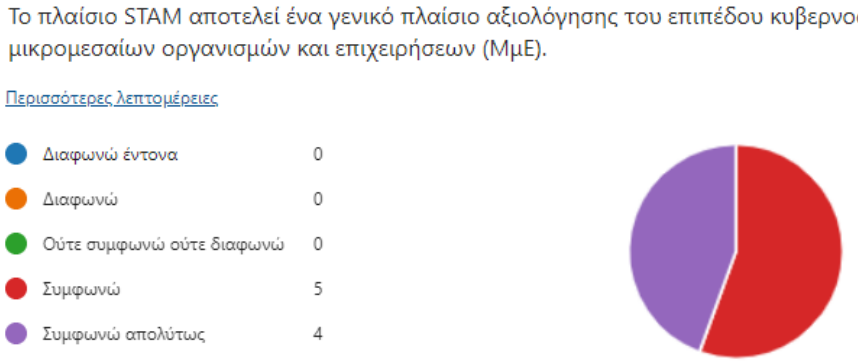
6.6. Αποτελέσματα αξιολόγησης εργαλείου από Ειδικούς στην ασφάλεια

Η αξιολόγηση του εργαλείου από τους Ειδικούς στην Ασφάλεια, πραγματοποιήθηκε από εννέα (9) φυσικά πρόσωπα με επαγγελματικούς τίτλους στην ασφάλεια και την κυβερνοασφάλεια. Τα πλήρη στοιχεία τους για επικοινωνία είναι διαθέσιμα. Οι συμμετέχοντες στην αξιολόγηση, επιλέχθηκαν βάσει του προφίλ τους και της αναγνωρισιμότητας τους στον ιδιωτικό και δημόσιο τομέα, καθώς επίσης και στην ακαδημαϊκή επιστημονική κοινότητα (Εικόνα 40).

Μηχανικός Ασφάλειας Πληροφοριών
POST DOC RESEARCHER
CISO
ΕΡΕΥΝΗΤΗΣ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ
Cyber security expert
Σύμβουλος cybersecurity
ΔΙΕΥΘΥΝΤΗΣ ΗΛΕΚΤΡΟΝΙΚΗΣ ΔΙΑΚΥΒΕΡΝΗΣΗΣ
L1 SOC Analyst
Security Solutions Architect

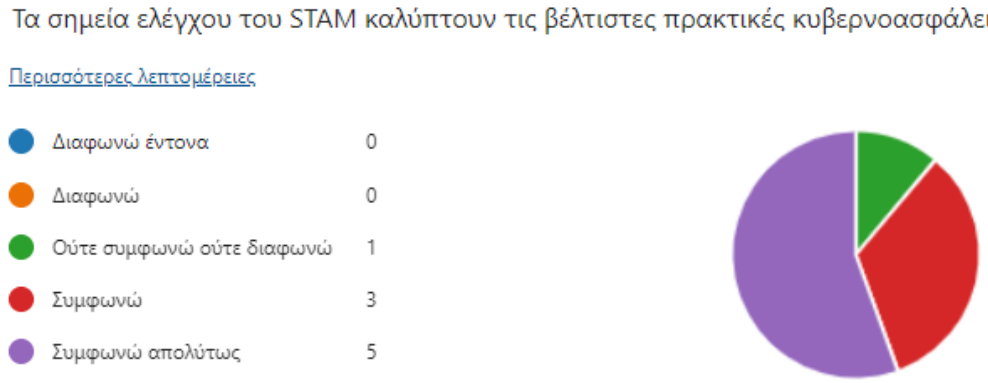
Εικόνα 40: Επαγγελματικοί Τίτλοι Αξιολογητών.

Τα Διαγράμματα 41 έως 49, παρουσιάζουν τις απαντήσεις που δόθηκαν από τους ειδικούς στα οκτώ (8) ερωτήματα που τέθηκαν σχετικά με το πλαίσιο STAM.

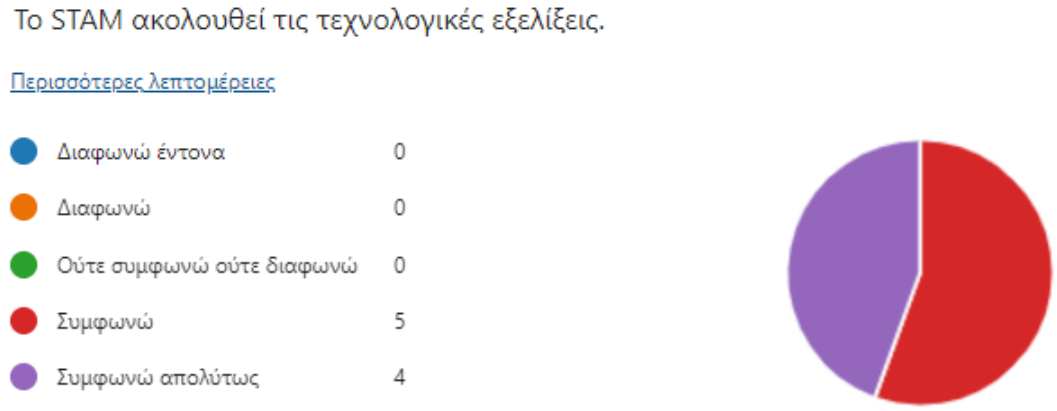


Εικόνα 41: Απαντήσεις στο 1ο ερώτημα.

Εικόνα 42: Απαντήσεις στο 2ο ερώτημα.



Εικόνα 43: Απαντήσεις στο 3ο ερώτημα.



Εικόνα 44: Απαντήσεις στο 4ο ερώτημα.

Το STAM αποτελεί ένα αρχικό σημείο για τον έλεγχο της θωράκισης των συστημάτων των ΜμΕ μέσω ενισχυμένων απαιτήσεων ασφαλείας.

Περισσότερες λεπτομέρειες

Διαφωνώ έντονα	0
Διαφωνώ	0
Ούτε συμφωνώ ούτε διαφωνώ	0
Συμφωνώ	2
Συμφωνώ απολύτως	7

Εικόνα 45: Απαντήσεις στο 5ο ερώτημα.

Το STAM συμβάλει στον σχεδιασμό και την ενδυνάμωση των μηχανισμών ασφαλείας.

Περισσότερες λεπτομέρειες

Διαφωνώ έντονα	0
Διαφωνώ	0
Ούτε συμφωνώ ούτε διαφωνώ	1
Συμφωνώ	2
Συμφωνώ απολύτως	6

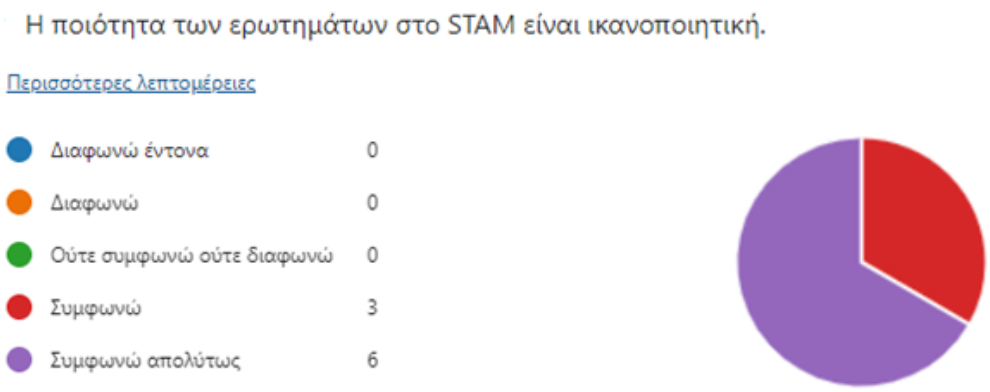
Εικόνα 46: Απαντήσεις στο 6ο ερώτημα.

Το STAM προάγει την προστασία των κρίσιμων υποδομών.

Περισσότερες λεπτομέρειες

Διαφωνώ έντονα	0
Διαφωνώ	0
Ούτε συμφωνώ ούτε διαφωνώ	1
Συμφωνώ	5
Συμφωνώ απολύτως	3

Εικόνα 47: Απαντήσεις στο 7ο ερώτημα.

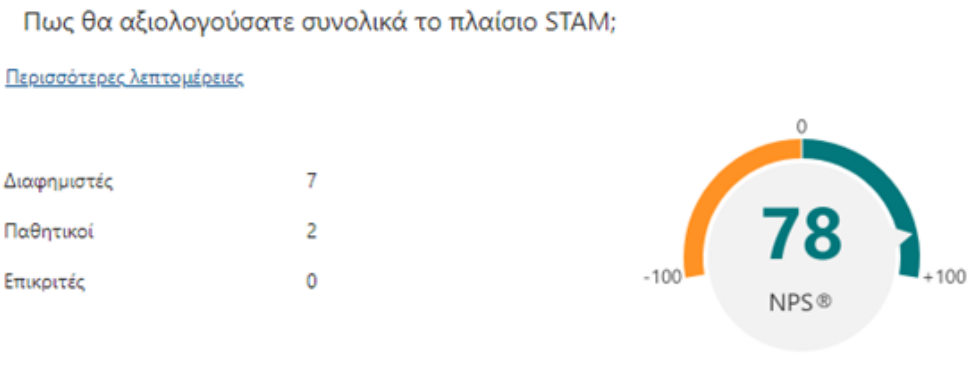


Εικόνα 48: Απαντήσεις στο 8ο ερώτημα.

Για την συνολική εικόνα ικανοποίησης του πλαισίου STAM ως υπηρεσία, χρησιμοποιήθηκε ο δείκτης μέτρηση NPS (Net Promoter Score) και υπολογίστηκε σύμφωνα με τον τύπο:

NPS = (Promoters – Detractors) / αριθμός ατόμων που ερωτήθηκαν

Οι διαφημιστές – υποστηρικτές (Promoters), είναι αυτοί που έχουν μείνει απόλυτα ικανοποιημένοι και έχουν δώσει βαθμό 9 ή 10. Οι παθητικοί (Passives), είναι αυτοί που κρατούν ουδέτερη στάση, μπορεί να μην έμειναν δυσαρεστημένοι αλλά δεν υπήρχε και κάτι που τους ενθουσίασε και έχουν δώσει βαθμολογία 7 ή 8. Οι επικριτές (Detractors), είναι οι δυσαρεστημένοι που ενδέχεται να δυσφημήσουν το STAM μέσω αρνητικών σχολιασμών και έχουν δώσει βαθμολογία μεταξύ 0-6. Από την μέτρηση το NPS είναι 78%.



Εικόνα 49: Απαντήσεις με NPS (Net Promoter Score).

Τέλος, από τα σχόλια που άφησαν οι συμμετέχοντες, σε σχέση με την εμπειρία τους από άλλα πλαίσια, μεθοδολογίες, τεχνικές και πρότυπα προέκυψαν αξιόλογα συμπεράσματα για την μελλοντική εξέλιξη του πλαισίου. Ο πίνακας που ακολουθεί παρουσιάζει τα σχόλια ανά επαγγελματικό τίτλο συμμετέχοντα.

Πίνακας 10: Σχόλια Ειδικών Ασφαλείας.

Α/Α	Επαγγελματικός Τίτλος	Σχόλια
1	Μηχανικός Ασφάλειας Πληροφοριών	Το πλαίσιο STAM διαθέτει δυνατότητες που του επιτρέπουν την ένταξη και την ενσωμάτωση στις διεργασίες ενός Οργανισμού και στη συνολική δομή διαχείρισης, προκειμένου η ασφάλεια πληροφοριών να λαμβάνεται υπόψη κατά τον σχεδιασμό των διεργασιών, των πληροφοριακών συστημάτων, καθώς και των ελέγχων.
2	POST DOC RESEARCHER	Ως επέκταση του προτείνω την μεγαλύτερη αξιοποίηση του NIST CyberSecurity Framework.
3	CISO	Συγχαρητήρια για την εξαιρετική σου δουλειά που πράγματι μπορεί να βοηθήσει ουσιαστικά στην δημιουργία κουλτούρας κυβερνοασφάλειας. Πραγματικά πρόκειται για πάρα πολύ καλή και επιμελημένη δουλειά.
4	ΕΡΕΥΝΗΤΗΣ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ	Το πλαίσιο STAM είναι ένα πολύ καλό εργαλείο για την αξιολόγηση του επιπέδου της κυβερνοασφάλειας των ΜμΕ. Κάποιες μικρές παρατηρήσεις οι οποίες δεν είναι κρίσιμης σημασίας. 1.) Υπάρχουν κάποιες γενικές - λίγο ασαφής ερωτήσεις οι οποίες θα μπορούσαν ή να παραλειφθούν ή να επαναπροσδιοριστούν με μεγαλύτερη στόχευση. Η μικρή εμπειρία μου έχει δείξει ότι σε τέτοιου είδους αξιολογήσεις καλό είναι οι ερωτήσεις να είναι στοχευμένες και συγκεκριμένες για το καλύτερο και αποδοτικότερο αποτέλεσμα. Τέτοιες ερωτήσεις είναι: - από την κατηγορία Προστασία Δεδομένων οι 6,7,13. - από την κατηγορία Παρακολούθηση και Άμυνα 2,6. - από την κατηγορία Διαχείριση Αρχείων Καταγραφής 13. 2.) Από την κατηγορία Ασφάλεια Εφαρμογών Λογισμικού θα μπορούσαν να ενσωματωθούν οι ερωτήσεις 3 και 7 δεδομένου ότι ουσιαστικά ελέγχουν το ίδιο πράγμα. 3.) Στην κατηγορία Διαχείριση Αρχείων Καταγραφής ίσως να έπρεπε να υπήρχε κάποια ερώτηση σχετική με το που αποθηκεύονται τα αρχεία καταγραφής και τι ρυθμίσεις ασφάλειας είναι υλοποιημένες για την προστασία της αποθήκευσης. 4.) Ίσως θα έπρεπε να υπήρχαν ερωτήσεις για το είδος του firewall που υπάρχει, αν υπάρχουν honeypots, αν υπάρχει DMZ, καθώς επίσης και αν είναι υλοποιημένα VLANs.
5	Cyber Security Expert	Πρωτότυπο, καλύπτει τις σύγχρονες απαιτήσεις και προαπαιτούμενα για την διασφάλιση της κυβερνοασφάλειας

6	Σύμβουλος Cybersecurity	Το πλαίσιο STAM μπορεί να αποτελέσει ένα αρχικό στάδιο ελέγχου της ασφάλειας στη συνολική δομή ενός οργανισμού. Συμπεριλαμβάνει τις τελευταίες τάσεις στο cybersecurity.
7	Διευθυντής Ηλεκτρονικής Διακυβέρνησης	Είναι πολύ αναλυτικό και ιδιαίτερα χρήσιμο. Θεωρώ ότι η θεματολογία καθώς και το συγκεκριμένη πλατφόρμα αξιολόγησης μπορεί να αναδειχθεί ένα σημαντικό εργαλείο στα χέρια των στελεχών της αυτοδιοίκησης και γενικότερα του Δημόσιου Τομέα.
8	L1 SOC Analyst	-δεν άφησε σχόλια-
9	Security Solutions Architect	Θα βοηθούσαν: Κωδικοποίηση controls, π.χ. IAM1.1., IAM1.2, κλπ. Περισσότερες απαντήσεις, π.χ. Μη εφαρμόσιμο. Παροχή καθοδήγησης εναπομείναντων απαντήσεων (πόσες / ποιες ερωτήσεις δεν έχουν απαντηθεί).

Στα παραπάνω σχόλια δίνονται οι εξής απαντήσεις:

- Έχει αξιοποιηθεί ως έναν βαθμό το NIST CyberSecurity Framework. Η παρατήρηση κρίνεται αναγκαία για την μελλοντική εξέλιξη του πλαισίου.
- Τα ερωτήματα, είναι στοχευμένα βάσει των διασφαλίσεων που έχουν οριστεί αρχικά. Τα ερωτήματα, δεν περιλαμβάνουν λεπτομέρειες γιατί αφορούν μια αρχική αξιολόγηση της κατάστασης της κυβαρνοασφάλειας του οργανισμού και όχι την συμμόρφωση του ή μη με το πλαίσιο STAM. Επιπλέον, σε κάποιες μεθοδολογίες, τεχνικές και πρωτόκολλα, οι ερωτήσεις δεν είναι συγκεκριμένες και αλληλοκαλύπτονται από συμπληρωματικά ερωτήματα που διασφαλίζουν τις διεθνής αποδεκτές μεθοδολογίες ή τεχνικές της τρέχουσας περιόδου.
- Στην προστασία δεδομένων, στο ερώτημα 13 το οποίο και αναφέρθηκε, δεν είναι εφικτό να συμπεριλαμβάνει λεπτομέρειες για τα τεχνικά και οργανωτικά μέτρα σχετικά με τα προσωπικά δεδομένα και την συμμόρφωση του οργανισμού με τον GDPR. Μέχρι έναν επίπεδο, εξετάζονται κάποια κοινά μέτρα ασφάλειας του GDPR και της κυβερνοασφάλειας. Τα υπόλοιπα που προβλέπονται από τον Κανονισμό, δεν είναι αντικείμενο εξέτασης αυτού του πλαισίου, παράλληλα το ερώτημα τίθεται ώστε να εξετάσει εάν ο οργανισμός παρακολουθεί και προσαρμόζεται σύμφωνα με τις εξελίξεις στη νομοθεσία σχετικά με τα προσωπικά δεδομένα.
- Στην διαχείριση αρχείων καταγραφής, σχετικά με την αποθήκευση και τις ρυθμίσεις των αρχείων καταγραφή έχουν τεθεί ερωτήματα που αφορούν τον χώρο αποθήκευσης, τον τρόπο συλλογής, τα είδη των αρχείων, τις ρυθμίσεις χρόνου και άλλα, παρόλα αυτά δεν υπάρχει η δυνατότητα για επιπλέον λεπτομέρειες. Σε μελλοντική έρευνα να μπορούσε να πραγματοποιηθεί μεγαλύτερη ανάλυση σε κάθε ερώτημα.
- Σε ότι αφορά την παρατήρηση σχετικά με το είδος του firewall, το DMZ και τα VLANs, μπορεί να ειπωθεί ότι ελέγχονται καθώς υπάρχουν άλλα ερωτήματα σχετικά με τις υλοποιημένες υπηρεσίες ή τον διαχωρισμός του δικτύου σε υποδίκτυα βάσει της ευαισθησίας των επιχειρησιακών στόχων κλπ. Ενώ, ότι αφορά την αναφορά στα honeypots πρέπει να σημειωθεί ότι δεν κρίνονται απαραίτητα για την ασφάλεια στις ΜμΕ.
- Υπάρχει αρίθμηση των ερωτημάτων. Η κωδικοποίηση των controls είναι χρήσιμη παρατήρηση για μελλοντική εξέλιξη του πλαισίου και θα μπορούσε να βοηθήσει έναν οργανισμό για την καταγραφή της συμμόρφωσης ή μη με το πλαίσιο STAM.

- Περισσότερες απαντήσεις όπως πχ μη εφαρμόσιμο, δε υλοποιήθηκαν λόγω του ότι δεν έχει προσδιοριστεί ποιος είναι ο διαχειριστής των ερωτήσεων, όπως πχ ένας σύμβουλος, ένας ελεγκτής ή ένας εσωτερικός υπεύθυνος ασφαλείας. Σε περίπτωση που συμπληρώνεται από έναν ειδικό ασφαλείας θα μπορούσε να απαντηθεί ως μη εφαρμόσιμο. Το ερωτηματολόγιο, δόθηκε σε άτομα που γνωρίζουν την υποδομή, τις διαδικασίες και τα μέτρα του οργανισμού αλλά δεν είναι ειδικοί στην κυβερνοασφάλεια άρα δεν είναι σε θέση να κρίνουν εάν ένα μέτρο είναι μη εφαρμόσιμο.
- Οι εναπομείναντες απαντήσεις εφαρμόζονται στην παρουσίαση των ερωτημάτων.

7. Επίλογος

7.1. Σύνοψη και συμπεράσματα

Στη μελέτη αυτή, επιτεύχθηκαν οι αρχικοί στόχοι και απαντήθηκαν τα ερωτήματα που είχαν τεθεί. Η βιβλιογραφική έρευνα που διεξήχθη αποτέλεσε τους βασικούς πυλώνες της ανάπτυξης του πλαισίου STAM. Το πλαίσιο αυτό, αναπτύχθηκε σε δοκιμαστικό περιβάλλον και με εκπαιδευτικό σκοπό. Λόγω του τύπου των ερωτημάτων, η έρευνα αντιμετώπισε αρκετά προβλήματα κυρίως εμπιστευτικότητας και ασφάλειας. Από την έρευνα στις ΜμΕ, διαπιστώθηκε ότι οι οργανισμοί βρίσκονται σε συνεχή προσπάθεια και λαμβάνουν αρκετά οργανωτικά και τεχνικά μέτρα για την ασφάλεια των πληροφοριακών συστημάτων τους. Τα αποτελέσματα της έρευνας έδειξαν αρκετά υψηλό επίπεδο κυβερνοασφάλειας. Τουλάχιστον το 50%, βρίσκεται σε χαμηλό επίπεδο επικινδυνότητας. Επίσης, εντοπίστηκαν χρήσιμα στοιχεία σχετικά με τον τρόπο που οι οργανισμοί λαμβάνουν μέτρα ασφαλείας.

Η τελική αξιολόγηση από τους χρήστες, έδειξε ότι βρίσκουν το πλαίσιο STAM εύχρηστο και προσέφερε στην αξιολόγηση του επιπέδου της κυβερνοασφάλειας του οργανισμού τους. Από τα σχόλια των χρηστών, προκύπτει ότι το πλαίσιο STAM βοήθησε στον εντοπισμό των κενών ασφαλείας και είχε καθοριστικό ρόλο για τα νέα μέτρα ασφαλείας. Επίσης, η ποιότητα των ερωτημάτων που τέθηκαν ήταν ικανοποιητική τόσο για τους χρήστες όσο και για τους Ειδικούς ασφαλείας.

Η αξιολόγηση από τους Ειδικούς ασφαλείας είχε θετικά αποτελέσματα. Οι Ειδικοί, συμφώνησαν ότι το πλαίσιο STAM αποτελεί ένα πλαίσιο αξιολόγησης του επιπέδου κυβερνοασφάλειας των ΜμΕ και συνεισφέρει στην λήψη στρατηγικών αποφάσεων σχετικά με την κυβερνοασφάλεια. Επίσης, τα σημεία ελέγχου του πλαισίου καλύπτουν τις βέλτιστες πρακτικές κυβερνοασφάλειας και το πλαίσιο ακολουθεί τις τεχνολογικές εξελίξεις. Το πλαίσιο STAM, αποτελεί ένα αρχικό σημείο για τον έλεγχο της θωράκισης των συστημάτων των ΜμΕ μέσω ενισχυμένων απαιτήσεων ασφαλείας και συμβάλει στον σχεδιασμό και την ενδυνάμωση των μηχανισμών ασφαλείας. Τα σχόλια των Ειδικών ασφαλείας βοήθησαν να εντοπιστούν σημεία για μελλοντική εξέλιξη του πλαισίου.

7.2. Αποτελέσματα

Τα προσδοκώμενα αποτελέσματα αυτής της μελέτης ήταν να επιτευχθούν οι στόχοι της και να απαντηθούν τα ερωτήματα τους. Από την έρευνα που πραγματοποιήθηκε κρίνεται αναγκαίο να απαντηθούν τα ερωτήματα που τέθηκαν εξ' αρχής:

1) Ποια είναι η έννοια της Κυβερνοασφάλειας;

   Η απάντηση στο ερώτημα αυτό, δίνεται στην ενότητα 2.1.

2) Ποια είναι η σημερινή κατάσταση της κυβερνοασφάλειας στις ΜμΕ;

   Μια εκτεταμένη παρουσίαση της κατάστασης της κυβερνοασφάλειας πραγματοποιείται στην ενότητα 2.4., ενώ μια επικεντρωμένη στις ΜμΕ στην ενότητα 2.5.

3) Ποιες είναι οι κυβερνοαπειλές που πρέπει να αντιμετωπίσουν οι ΜμΕ;

   Η απάντηση στο ερώτημα αυτό, βρίσκεται στην ενότητα 2.3. με τα πλέον πρόσφατα στοιχεία των κυβερνοαπειλών.

4) Με ποιόν τρόπο επηρεάζεται η ασφάλεια της επιχείρησης;

   Το ερώτημα αυτό, αναλύεται διεξοδικά στην ενότητα 2.6.

5) Ποιοι κανονισμοί και πλαίσια εφαρμόζονται για την κυβερνοασφάλειας στις ΜμΕ;

Τα πλαίσια για την κυβερνοασφάλεια, παρουσιάζονται στις ενότητες 3.2., 3.2. και 3.4. Ενώ, οι Οδηγίες NIS και NIS2 της ΕΕ για την κυβερνοασφάλεια παρουσιάζονται στις ενότητες 4.2. και 4.3. Ο Κανονισμός GDPR αποτελεί και αυτός ένα μέρος της κυβερνοασφάλειας των οργανισμών και παρουσιάζεται στην ενότητα 4.1. Επίσης, στην ενότητα 4.4. παρουσιάζεται το Εθνικό Σχέδιο Δράσης για την κυβερνοασφάλεια.

6) Ποιοι είναι τα σημεία ελέγχου της ασφάλειας σε μια ΜμΕ;

Από την έρευνα που διεξήχθη, τα σημεία ελέγχου της ασφάλειας σε μια ΜμΕ είναι οι 20 θεματικές ενότητες (σημεία ελέγχου) του πλαισίου STAM, τα οποία και παρουσιάζονται στο κεφάλαιο 5.

7) Ποιες είναι οι βέλτιστες πρακτικές ασφάλειας για μια ΜμΕ;

Η απάντηση σε αυτό το ερώτημα βρίσκεται στην ενότητα 5.1., στις βέλτιστες πρακτικές κυβερνοασφάλειας του πλαισίου STAM και συγκεκριμένα στις 20 θεματικές ενότητες.

8) Έχει η ΜμΕ τεκμηριωμένη πολιτική και διαδικασίες σχετικά με την κυβερνοασφάλεια;

Τα αποτελέσματα της έρευνα παρουσιάζονται στην ενότητα 6.5. Επιπλέον, τα διαγράμματα είναι διαθέσιμα για την συνολική εικόνα των οργανισμών που συμμετείχαν. Πιο συγκεκριμένα, διαπιστώθηκε ότι από τους 21 οργανισμούς, οι 18 διαθέτουν καταγεγραμμένη πολιτική ασφάλειας, επικεντρωμένη στην ασφάλεια του πληροφοριακού συστήματος και την κυβερνοασφάλεια, εγκεκριμένη από την Διοίκηση. Επίσης, 17 οργανισμοί διαθέτουν επιμέρους πολιτικές ασφαλείας, διαδικασίες, κανόνες και οδηγίες για συγκεκριμένα πεδία, στις οποίες περιγράφουν τον τρόπο εφαρμογής των τεχνικών και οργανωτικών μέτρων προστασίας.

9) Ακολουθεί η ΜμΕ τις κατευθυντήριες γραμμές σύμφωνα με παγκόσμια πλαίσια για την ασφάλεια;

Η έρευνα έδειξε ότι, το μεγαλύτερο μέρος των οργανισμών που συμμετείχαν, ακολουθούν τουλάχιστον μερικώς τις κατευθυντήριες γραμμές των παγκόσμιων πλαισίων. Η ενότητα 6.5 παρουσιάζει τα αποτελέσματα, καθώς επίσης στο Διάγραμμα 6 αποτυπώνεται η κατάσταση αυτών των οργανισμών.

10) Μπορεί να βοηθήσει ένα εργαλείο αυτοαξιολόγησης του επιπέδου κυβερνοασφάλειας μια ΜμΕ;

Στην ενότητα 6.5. παρουσιάζονται τα σχόλια των χρηστών που συμμετείχαν στην έρευνα και αναφέρουν ότι οι ερωτήσεις βοήθησαν στον εντοπισμό των κενών ασφαλείας και το πλαίσιο ανέδειξε σημαντικά κενά στην ασφάλεια τα οποία θα αντιμετωπιστούν σε μελλοντικές ενέργειες. Επίσης, το πλαίσιο βοήθησε στον εντοπισμό τεχνικών μέτρων που δεν υλοποιούνται στον οργανισμό, καθώς και στην εξαγωγή συμπερασμάτων για την κατάσταση της ασφάλειας του οργανισμού.

11) Είναι ικανοποιητική την ποιότητα των ζητημάτων που τέθηκαν;

Η ανατροφοδότηση έδειξε ότι οι χρήστες και οι Ειδικοί στην ασφάλεια έμειναν ικανοποιημένοι από την ποιότητα των ζητημάτων που τέθηκαν.

7.3. Μελλοντικές επεκτάσεις

Το πλαίσιο STAM, αναπτύχθηκε για την αξιολόγηση της κυβερνοασφάλειας των ΜμΕ, η έρευνα διεξήχθη σε δοκιμαστικό περιβάλλον και σε έναν μικρό πληθυσμό. Παρόλα τα προβλήματα που αντιμετωπίστηκαν κατά την διάρκεια της έρευνα και αναφέρθηκαν στις προηγούμενες ενότητες, η έρευνα αυτή αναδεικνύει την ανάγκη και το κενό που υπάρχει στο χώρο για ένα πλαίσιο κυβερνοασφάλειας προσαρμοσμένο στις ΜμΕ σε εθνικό επίπεδο. Σε μελλοντική εξέλιξη η έρευνα αυτή θα μπορούσε να διερευνήσει και να επεκτείνει τα ακόλουθα σημεία:

1. Ο καθορισμός του χρήστη, είναι σημαντικός για την αξιοποίηση του πλαισίου. Διαπιστώθηκε ότι, υπάρχει ανάγκη από ασφαλιστικές εταιρείες για τον έλεγχο της κατάστασης της κυβερνοασφάλειας σε οργανισμούς ώστε να προσφέρουν το αντίστοιχο ασφαλιστήριο συμβόλαιο. Το ίδιο ισχύει για όλες τις επιχειρήσεις που μοιράζονται δεδομένα και υπηρεσίες και θέλουν να ελέγχουν τους συνεργάτες τους σχετικά με την κατάσταση της κυβερνοασφάλειας τους. Ο καθορισμός του ποιος θα χρησιμοποιεί το πλαίσιο ως εργαλείο, πχ ένας ελεγκτής, επηρεάζει την δομή του ερωτηματολογίου και του βάθους των ερωτημάτων.

2. Η προσθήκη σημείων ελέγχου, για την κάλυψη μεγαλύτερου εύρους ελέγχων και διασφαλίσεων δίνει την δυνατότητα μεγαλύτερης ακρίβειας στην εκτίμηση της κατάστασης.

3. Η κωδικοποίηση των ελέγχων θα βοηθούσε στην αποτίμηση της κατάστασης.

4. Ο αποκλεισμός ερωτημάτων, σύμφωνα με τον τύπο του οργανισμού και με το εάν είναι απαραίτητο το μέτρο, όπως για παράδειγμα μη εφαρμόσιμα, θα διαμόρφωναν διαφορετικά την τελική αξιολόγησης, αποτυπώνοντας την πραγματική κατάσταση του οργανισμού.

5. Η εκτεταμένη έρευνα στους παράγοντες που λαμβάνονται υπόψη για την εκτίμηση της επικινδυνότητας θα μπορούσε να δημιουργήσει ένα εργαλείο τύπου Risk Assessment.

6. Η σχεδίαση και ανάπτυξη ενός ολοκληρωμένου διαδικτυακού περιβάλλοντος, για την κάθετη εφαρμογή του πλαισίου, με αρχιτεκτονική που προσφέρει αυτοματοποιημένη διαχείριση και αναθεώρηση του πλαισίου στις τρέχουσες εξελίξεις, θα μπορούσε να αποτελέσει ένα εμπορικό εργαλείο.

7. Η εφαρμογή του πλαισίου σε συγκεκριμένους τομείς όπως υγεία, βιομηχανία, δήμους και πανεπιστήμια, θα μπορούσε να διαμορφώσει διαφορετικά το πλαίσιο και να διαφοροποιηθεί.

8. Αναφορές

27005:2022, I. (2023, Ιουλίου 25). *ISO*. Ανάκτηση από https://www.iso.org/standard/80585.html

Alladean, C., Sebastian, Z., & Polychronis, K. (2022). A Survey on the Cyber Security of Small-to-Medium Businesses: Challenges, Research Focus and Recommendations. *IEEE Access (Volume: 10)*.

Ayala-Rivera, V., & Pasquale, L. (2018). The grace period has ended: An approach to operationalize GDPR requirements. *Proceedings - 2018 IEEE 26th International Requirements Engineering Conference*, σσ. 136-146. doi:10.1109/RE.2018.00023

Bertrand, C., & Keane, M. (2022). *How Tape Technology Can Be Used to Defeat Ransomware.* HPE - Enterprise Strategy Group.

Cawthra, J., Ekstrom, M., Lusty, L., Sexton, J., Sweetnam, J., & Townsend, A. (2020). *NIST SPECIAL PUBLICATION 1800-25A. Data Integrity: Identifying and Protecting Assets Against Ransomware and Other Destructive Events. Volume A.* NIST.

CheckPoint. (2023). *Check Point Software's 2023 Cyber Security Report.* CheckPoint.

CIS. (2021). *CIS Controls Version 8.* Center for Internet Security.

Cisco. (2022). *How modern security teams fight today's cyber threats.*

Cisco-Secure. (2023). *Cisco Cybersecurity Readiness Index - Resilience in a Hybrid World.* Cisco.

Commission, E. (2020). *Unleashing the full potential of European SMEs.* EE.

Dhoha, A., Mashael, A.-k., Ghadeer, A., Manal, A., Rouqaiah, A.-R., & Naya, N. (2018). Security Related Issues In Saudi Arabia Small Organizations: A Saudi Case Study. *IEEE - 2018 21st Saudi Computer Society National Computer Conference (NCC)*.

ENISA. (2015). Definition of Cybersecurity - Gaps and overlaps in standardisation V1.0. European Union Agency For Network And Information Security.

ENISA_2. (2023). *ENISA THREAT LANDSCAPE: HEALTH SECTOR. (January 2021 to March 2023).* EUROPEAN UNION AGENCY FOR CYBERSECURITY.

ENISA_3. (2020). *ENISA Threat Landscape. Top threats.* EUROPEAN UNION AGENCY FOR CYBERSECURITY.

ENISA_NIS. (2023). Supporting the implementation of Union policy and law regarding cybersecurity. NIS Directive. EE: European Union Agency for Cybersecurity.

Esmaeil, L., Yosef, M., Farhad, F., & Saber, G. (2013). Influencing Factors of Information Security Management in Small- and Medium-Sized Enterprises and Organizations. *IEEE - 2013 International Conference on Communication Systems and Network Technologies*.

EUR-LEX. (2018). GDPR - ΚΑΝΟΝΙΣΜΌΣ (ΕΕ) 2016/679 ΕΥΡΩΠΑΪΚΟΎ ΚΟΙΝΟΒΟΥΛΊΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΊΟΥ της 27ης Απριλίου. Βρυξέλλες: EE-Access to European Union Law. Retrieved from https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX:32016R0679

Freitas, M. d., & Silva, M. M. (2022). 2022 17th Iberian Conference on Information Systems and Technologies (CISTI). *GDPR and Suppliers in SMEs. IEEE*.

Gobeo, A., Fowler, C., & Buchanan, W. J. (2020). GDPR and Cyber Security for Business Information Systems. IEEE. *River Publishers*.

Heinrihs, K. S., Julija, S., & Andrejs, R. (2020). The Information System Security Governance Tasks in Small and Medium Enterprises. *IEEE - 2020 61st International Scientific Conference on Information Technology and Management Science of Riga Technical University (ITMS)*.

ISO/IEC20000-1:2018. (2023, Ιουλίου 25). *ISO/IEC 20000-1:2018 - Information technology — Service management — Part 1: Service management system requirements*. Ανάκτηση από ISO/IEC 20000-1:2018: https://www.iso.org/standard/70636.html

ISO/IEC27001. (2023, Ιουνίου 10). *ISO/IEC 27001*. Ανάκτηση από ISO/IEC 27001 INFORMATION SECURITY MANAGMENT: https://www.iso.org/isoiec-27001-information-security.html

ISO/IEC27005:2022. (2023, Ιουλίου 25). *ISO*. Ανάκτηση από https://www.iso.org/standard/80585.html

ISO22301:2019. (2023, Ιουλίου 27). *ISO 22301:2019*. Ανάκτηση από ISO 22301:2019 - Security and resilience — Business continuity management systems — Requirements: https://www.iso.org/standard/75106.html

Juan, F. C., Marcos, B., Leire, L., Saioa, A., & Josune, H. (2020). Systematic Approach to Cyber Resilience Operationalization in SMEs. *IEEE Access (Volume: 8)*.

KPMG. (2015). *SMALL BUSINESS REPUTATION & THE CYBER RISK.* Cyberstreetwise.

Liset, R.-B., Rosa, L.-S., Carlos, C., Mitchell, A.-D., Sandra, G. H., & Joe, P.-E. (2022). Business Cybersecurity. Case study in Peruvian and Mexican SMEs. *2022 3rd International Conference for Emerging Technology (INCET) IEEE*.

Lopes, I. M., Guarda, T., & Oliveira, P. (2019). How ISO 27001 Can Help Achieve GDPR Compliance. IEEE. *Iberian Conference on Information Systems and Technologies (CISTI)*.

Malatji, M. (2023). Management of enterprise cyber security: A review of ISO/IEC 27001:2022. IEEE. *2023 International Conference On Cyber Management And Engineering (CyMaEn)*.

Megat, M. A., Zuraini, Z., & Mohd, H. M. (2022). Mitigating Malware Threats at Small Medium Enterprise (SME) Organisation: A Review and Framework. *2021 6th IEEE International Conference on Recent Advances and Innovations in Engineering (ICRAIE)*.

Monev, V. (2020). Organisational Information Security Maturity Assessment Based on ISO 27001 and ISO 27002. IEEE. *Proceedings of the 2020 IEEE International Conference on Information Technologies (InfoTech-2020)*.

NIS2-Eur-lex.eu. (2022). ΟΔΗΓΙΑ (ΕΕ) 2022/2555 ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ. *Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης*.

NIS-eur-lex.europa. (2016). ΟΔΗΓΊΑ (ΕΕ) 2016/1148 ΤΟΥ ΕΥΡΩΠΑΪΚΟΎ ΚΟΙΝΟΒΟΥΛΊΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΊΟΥ. *Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης*.

NIST. (2014). *Framework for Improving Critical Infrastructure Cybersecurity. Version 1.0.*

NIST_2023. (2023, Σεπτέμβριος 10). NIST_Drafts Major Update to Its Widely Used Cybersecurity Framework. Ανάκτηση από nist.gov: https://www.nist.gov/news-events/news/2023/08/nist-drafts-major-update-its-widely-used-cybersecurity-framework

NIST_Draft. (2023). Discussion Draft: The NIST Cybersecurity Framework 2.0 Core with Implementation Examples. NIST.

Patel, A., Suthar, D., & Parekh, M. (2021). *Principles of Cyber Security - Master of Science MSCCS - 101.* Dr. Babasaheb Ambedkar Open University, Ahmedabad.

Paulsen, C. (2016). Cybersecuring Small Businesses. *Cybertrust, IEEE*.

Putra, S. J., Gunawan, M. N., Sobri, A. F., Muslimin, J., Amilin, & Saepudin, D. (2020). Information Security Risk Management Analysis Using ISO 27005: 2011 For The Telecommunication Company. IEEE. *2020 8th International Conference on Cyber and IT Service Management (CITSM)*.

Roy, P. P. (2020). A High-Level Comparison between the NIST Cyber Security Framework and the ISO 27001 Information Security Standard.IEEE. *2020 National Conference on Emerging Trends on Sustainable Technology and Engineering Applications (NCETSTEA)*.

SANS_Institute. (2023, Ιούνιος 15). *SANS Security Policy Templates*. Ανάκτηση από www.sans.org: https://www.sans.org/information-security-policy/?per-page=100

SANS-Institute. (2021). CIS Controls v8. *SANS*.

Schatz, D., Bashroush, R., & Wall, J. (2017). Towards a Mor ds a More Representativ esentative Definition of Cyber Security. *The Association of Digital Forensics, Security and Law (ADFSL)*.

Sophos. (2023). *Maturing criminal marketplaces present new challenges to defenders. Sophos 2023 Threat Report. .* Sophos X-Ops.

Tanović, A., & Marjanovic, I. S. (2019). Development of a new improved model of ISO 20000 standard based on recommendations from ISO 27001 standard. IEEE. *2019 42nd International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO),*.

Whitaker, C. (2023, Feb). The Top Cybersecurity Threats in 2022 . *Cisco Umbrella*.

Μαυρίδης, Ι. (2015). *Ασφάλεια Πληροφοριών Στο Διαδίκτυο.* Αθήνα: ΣΕΑΒ.

Ν.4624/2019, Φ. 1.-8.-2. (2023, Ιουνίου 5). *Τραπεζα Πληροφοριών Νομοθεσίας*. Ανάκτηση από e-nomothesia.gr: https://www.e-nomothesia.gr/kat-dedomena-prosopikou-kharaktera/nomos-4624-2019-phek-137a-29-8-2019.html

ΥΨΔ_ΕΑΚ, Υ. Ψ.-Ε. (2020). Εθνική Στρατηγική Κυβερνοασφάλειας 2020-2025.