Πανεπιστήμιο Πειραιώς – Τμήμα Πληροφορικής
Πρόγραμμα Μεταπτυχιακών Σπουδών

«Κατανεμημένα Συστήματα, Ασφάλεια και Αναδυόμενες Τεχνολογίες Πληροφορίας»

**Μεταπτυχιακή Διατριβή**

| | |
|---|---|
| Τίτλος Διατριβής<br><br>Thesis Title | **Ανάπτυξη πλατφόρμας αξιολόγησης και καταγραφής επιπέδου ωριμότητας οργανισμών σε θέματα κυβερνοασφάλειας και κυβερνοάμυνας**<br><br>**Development of a cybersecurity and cyberdefence maturity assessment and documentation platform for organizations** |
| Ονοματεπώνυμο Φοιτητή | **Βάββας Κωνσταντίνος** |
| Πατρώνυμο | **Δημήτριος** |
| Αριθμός Μητρώου | **ΜΠΚΣΑ20005** |
| Επιβλέπων | **Κοτζανικολάου Παναγιώτης** |

**Ημερομηνία Παράδοσης Ιανουάριος 2023**

## Τριμελής Εξεταστική Επιτροπή

| | | |
|---|---|---|
| Παναγιώτης Κοτζανικολάου<br>Καθηγητής | Κωνσταντίνος Πατσάκης<br>Αναπληρωτής Καθηγητής | Μιχαήλ Ψαράκης<br>Αναπληρωτής Καθηγητής |

# ΠΕΡΙΛΗΨΗ

Οι απειλές στον κυβερνοχώρο αποτελούν ένα σημαντικό ρίσκο για κάθε οργανισμό. Απαιτείται από όλους τους οργανισμούς να αξιολογήσουν αυτές τις απειλές και να λάβουν τα κατάλληλα αντίμετρα έτσι ώστε να διασφαλίσουν την ομαλή και εύρυθμη λειτουργία των επιχειρηματικών διαδικασιών, ψηφιακών υποδομών και πληροφοριών που αυτές εμπεριέχουν.Η ανάλυση ρίσκου είναι μια ευρέως διαδεδομένη και αποδοτική πρακτική μέσω της οποίας μπορεί ένας οργανισμός να αξιολογεί κίνδυνους και να λαμβάνει τα κατάλληλα μέτρα. Ανεξάρτητα από την ανάλυση ρίσκου μπορεί να εκτελείται κυκλικά και μια αξιολόγηση επιπέδου ωριμότητας κυβερνοασφάλειας έτσι ώστε ο οργανισμός να εντάξει στους κόλπους του δυνατότητες κυβερνοάμυνας, οι οποίες βασίζονται σε μια πληθώρα διεθνών προτύπων, πλαισίων και βέλτιστων πρακτικών κυβερνοασφάλειας.Η αξιολόγηση επιπέδου ωριμότητας, είναι μια σύντομη επαναλαμβανομένη ανά τακτά χρονικά διαστήματα διαδικασία, μπορεί να εκτελεστεί από ένα μόνο άτομο του οργανισμού όπως IT Director, Information Security Officer, IT Compliance Officer, θέτοντας στόχους ανά κύκλο αξιολόγησης.Η εφαρμογή που αναπτύχθηκε σε αυτή την διατριβή μπορεί να αποτελέσει το κατάλληλο εργαλείο στα χεριά μικρομεσαίων και μεγάλων οργανισμών για την εκτέλεση αξιολογήσεων επιπέδου ωριμότητα κυβερνοασφάλειας.

Η εφαρμογή προσφέρει 4 συναρτήσεις για την αξιολόγηση του επιπέδου ωριμότητας:

- Συνάρτηση αξιολόγησης βασισμένη στα CIS Controls που αποτελεί την πρώτη υψηλού επιπέδου προσέγγιση
- CDM Master Mapping, οπου κάθε CIS μέτρο ασφάλειας αποκτά ένα ξεχωριστό βάρος ανάλογα με την (υπο-)τεχνικές MITRE Attack που μετριάζει.
- NIST Security Funtion, επίσης μια υψηλού επιπέδου προσέγγιση που έρχεται να δώσει μια μεγαλύτερη εικόνα για την κατανομή των μέτρων κυβερνοασφάλειας και το ρόλο τους.
- CDM Reverse Mapping, σε αυτή την συνάρτηση αξιολόγησης το βάρος των CIS μέτρων ασφάλειας αξιολογούνται σύμφωνα με την ικανότητα τους να μετριάσουν 5 συγκεκριμένες απειλές.

Βασιζομένη στις παραπάνω συναρτήσεις αξιολόγησης, η εφαρμογή προτείνει τα κατάλληλα αντίμετρα τα οποία πρέπει ο εξεταζόμενος οργανισμός να λάβει υπόψιν για να καλύψει τα κενά του.

# ABSTRACT

In the era of digitalization, cyber threats represent an important risk for every organization. The organizations are forced to assess these threats against the impact they can cause on their digital assets and implement the necessary countermeasures. Risk Analysis is a common and effective practice which an organization must execute in frequent time frames in order to mitigate the relevant cyber risks.
Regardless of the Risk Assessment a frequently executed Cybersecurity Maturity Assessment based on global Cybersecurity frameworks, standards and best practices, can assist an organization to prepare and evolve against cyberthreats.The Cybersecurity Maturity Assessment is a short procedure. It can be performed from a single person expert of the IT infrastructure of the assessed organization, such as the IT Director, the Information Security Officer or the IT Compliance Officer but it must be performed as a circular process (GAP assessment) and should set/meet higher targets in each cycle. The Cybersecurity Maturity Assessment Tool developed in this thesis can serve SME and large organizations to perform these kind of assessments. The Tool is based on the CIS Controls and uses the CIS CDM to implement the MITRE Attack Framework. he tool provides 4 different maturity assessment scores:

- Based on the CIS controls, a high-level approach which could also serve as a compliance report against these controls.
- CIS Community Defense Model1, Master Mapping approach. During this maturity assessment each CIS control takes the value of the amount of all MITRE Attack (sub)techniques it mitigates.
- NIST2 Security Functions based assessment scores, provides a bigger picture of the implemented controls and the role they serve.
- CIS Community Defense Model Reverse Mapping security score. Based on the CDM study the score

- results from the efficiency to mitigate the Top5 Threads, which are Malware, Ransomware, Web Application Hacking, Insider Privilege Misuse, Targeted Intrusion.

Based on the above scores, the tool provides the corresponding rule-based recommendations so that the organization can take the necessary measures.

# Κεφάλαιο 1: Εισαγωγή

Καθώς οι τεχνολογίες πληροφορικής και επικοινωνιών δημιουργούν έναν κόσμο διαρκώς αυξανόμενης πολυπλοκότητας σε διασυνδεδεμένα συστήματα και συσκευές, η δημόσια συζήτηση για τα θέματα κυβερνοασφάλειας και ιδιωτικότητας βρίσκεται συνεχώς στο προσκήνιο, αναδεικνύοντας την ανάγκη για ενίσχυση της προστασίας και ανθεκτικότητας των εν λόγω συστημάτων από τις συνεχώς εξελισσόμενες απειλές του σύγχρονου κυβερνοχώρου [1].

Η βελτίωση του επιπέδου της κυβερνοασφάλειας των πληροφοριακών συστημάτων όλων των οργανισμών θεωρείται πλέον επιτακτική και απαραίτητη για την εύρυθμη λειτουργία τους. Μια πρακτική για την αξιολόγηση και βελτιστοποίηση του επιπέδου κυβερνοασφάλειας ενός οργανισμού αποτελεί η αξιολόγηση του επιπέδου ωριμότητας του – Maturity Gap Assessment [2].

Στόχος της αξιολόγησης ωριμότητας είναι να προσφέρει ένα στιγμιότυπο της τρέχουσας κατάστασης στην οποία βρίσκεται ο οργανισμός και να υποδείξει γενικά και ειδικά τα κατάλληλα μέτρα που πρέπει να πάρει για φτάσει σε μια βελτιωμένη ή επιθυμητή κατάσταση μέσα σε ένα ορισμένο χρονικό διάστημα, καθώς πρόκειται για μια επαναληπτική διαδικασία. Το επίπεδο ωριμότητας κυβερνοασφάλειας απαιτεί χρόνο για να βελτιωθεί Αλλεπάλληλες μετρήσεις σε τακτά χρονικά διαστήματα είναι σε θέση να παρακολουθήσουν την πορεία της και εν μέρει την αποδοτικότητά των μέτρων προστασίας που έχουν παρθεί. Η αξιολόγηση ωριμότητας είναι ένα συμπληρωματικό εργαλείο για την αξιολόγηση κυβερνοασφάλειας ενός οργανισμού και δεν μπορεί να αντικαταστήσει την ανάλυση ρίσκου (Risk Analysis).

Πλεονεκτήματα αυτή της πρακτικής αποτελούν ο χρόνος διεξαγωγής, το γεγονός ότι απευθύνεται σε όλες τις κατηγορίες οργανισμών (μικρομεσαίους, μεγάλους και κρίσιμους οργανισμούς), μπορεί να εκτελεστεί συμπληρωματικά με μια αξιολόγηση ρίσκου και δεν είναι ανάγκη να εκτελεστεί από πολύ εξειδικευμένο ή πιστοποιημένο προσωπικό. Επίσης, το αποτέλεσμα είναι μετρήσιμο, μπορεί να χρησιμοποιηθεί ως μετρό σύγκρισης με συνεργαζόμενους οργανισμούς ή για επικοινωνία προς την διοίκηση του οργανισμού αλλά και για την λήψη αποφάσεων.

Κάποια από τα μειονεκτήματα της αυτό-αξιολόγησης είναι ότι μπορεί να αφήνει κενά για υποκειμενικότητες, και το γεγονός ότι κάποιες φορές είναι σύνθετο να εκτιμηθεί εάν ένα μετρό έχει υλοποιηθεί πλήρως, εν μέρη ή καθόλου. Οι ενδιάμεσες καταστάσεις είναι αρκετές και μπορεί να διαφέρουν από οργανισμό σε οργανισμό.

## 1.1 Σκοπός της Διατριβής

Σκοπός της διατριβής είναι να αναπτυχθεί μια εφαρμογή αξιολόγησης του επιπέδου ωριμότητας κυβερνοασφάλειας με βάση τον πίνακα https://attack.mitre.org/matrices/enterprise/. Με την βοήθεια αυτής της εφαρμογής ένας οργανισμός χωρίς πολλούς πόρους και σε σύντομο χρονικό διάστημα θα είναι σε θέση να αξιολογήσει το επίπεδο ωριμότητάς του έναντι διεθνών προτύπων, πλαισίων και βέλτιστών πρακτικών. Με την κατάλληλη χρήση διαδικασιών και επενδύσεων θα είναι σε θέση και να βελτιώσει το επίπεδο κυβερνοάμυνας.

Τα πλαίσια, πρότυπα, βέλτιστες πρακτικές και έρευνες στα οποία βασίζεται η παρούσα διατριβή είναι τα εξής:

- Center for Internet Security Critical Security Controls®, CIS Controls®v84F
- CIS Community Defense Model v2.05F
- Enterprise MITRE Adversarial Tactics, Techniques, and Common Knowledge® v8.2(MITRE ATT&CK® Enterprise Matrix)
- NIST Cyber Security Framework

## 1.2 Δομή της Διατριβής

Αρχικά, στο κεφάλαιο 2 παρουσιάζεται το θεωρητικό υπόβαθρο πάνω στο οποίο βασίζεται η εφαρμογή 'CyberDefenseAssessmentTool' και το οποίο αποτελείται από τις βέλτιστες πρακτικές, τις έρευνες και τα πρότυπα κυβερνοασφάλειας. Στην συνέχεια παρουσιάζονται οι τέσσερις συναρτήσεις αξιολόγησης οι οποίες χρησιμοποιούνται και η διατριβή τελειώνει με το κεφάλαιο της αρχιτεκτονικής και τις τεχνολογίες ανάπτυξης της εφαρμογής. Αναπόσπαστο κομμάτι τις διατριβής αποτελούν και τα παρατήματα που αναφέρονται στις μεταφράσεις των CIS CS Controls και στις προτεινόμενες συστάσεις κυβερνοασφάλειας που περιλαμβάνονται στην εφαρμογή.

# Κεφάλαιο 2: Πλαίσια, Πρότυπα και Βέλτιστες Πρακτικές Κυβερνοασφάλειας

Παρακάτω θα παρουσιαστούν τα πλαίσια, τα πρότυπα, οι βέλτιστες πρακτικές και μια έρευνα κυβερνοασφάλειας πάνω στις οποίες βασίστηκαν οι συναρτήσεις αξιολόγησης ωριμότητας κυβερνοασφάλειας της εφαρμογής 'CyberDefenseAssessmentTool' που αποτελεί και το αντικείμενο αυτής της εργασίας.

## 2.1 Center for Internet Security Critical Security Controls

Τα Critical Security Controls αναπτύχθηκαν από το Center for Internet Security (CIS) και είναι ένα σαφώς καθορισμένο, ιεραρχημένο σύνολο βέλτιστων πρακτικών και αμυντικών ενεργειών για την ασφάλεια στον κυβερνοχώρο, που μπορούν να βοηθήσουν στην πρόληψη και να υποστηρίξουν τη συμμόρφωση στα περισσότερα γνωστά πλαίσια κυβερνοασφάλειας. Αυτές οι βέλτιστες πρακτικές για κυβερνοάμυνα διατυπώνονται από μια ομάδα ειδικών στον χώρο της ασφάλειας πληροφοριακών συστημάτων, χρησιμοποιώντας τις πληροφορίες που συλλέγονται από πραγματικές επιθέσεις και την αποτελεσματική άμυνά τους. Τα CIS Controls παρέχουν συγκεκριμένη καθοδήγηση και μια σαφή διαδρομή που πρέπει να ακολουθήσουν οι οργανισμοί για να επιτύχουν τους δικούς τους στόχους αλλά και αυτούς που περιγράφονται από πολλαπλά νομικά, κανονιστικά πλαίσια. Τα CIS Controls αποτελούν μια συνέχεια των SANS Top 20 Controls [3].

Στόχοι των CIS Controls:

- Αξιοποιούν την κυβερνοεπίθεση για την ενημέρωση της κυβερνοάμυνας, εστιάζοντας σε τομείς υψηλής απόδοσης.
- Διασφαλίζουν ότι οι επενδύσεις στον τομέα της ασφάλειας επικεντρώνονται στην αντιμετώπιση των σημαντικότερων απειλών.
- Μεγιστοποιούν τη χρήση του αυτοματισμού για την επιβολή ελέγχων ασφαλείας, αποφεύγοντας έτσι τα ανθρώπινα λάθη.
- Χρησιμοποιούν τη «διαδικασία ομοφωνίας (μη ένστασης-consensus process)» για την συλλογή των βέλτιστων πληροφοριών/πρακτικών.

Τα CIS Controls αποτελούνται από 18 ομάδες (Controls) μέτρων ασφάλειας. Κάθε ομάδα περιέχει από 5 έως 14 μέτρα προστασίας (Safeguards) με συνολικά 153 μέτρα [4]. Οι 18 ομάδες είναι οι ακόλουθες:

1. Inventory and Control of Enterprise Assets
2. Inventory and Control of Software Assets
3. Data Protection
4. Secure Configuration of Enterprise Assets and Software
5. Account Management
6. Access Control Management
7. Continuous Vulnerability Management
8. Audit Log Management

9. Email and Web Browser Protections
10. Malware Defenses
11. Data Recovery
12. Network Infrastructure Management
13. Network Monitoring and Defense
14. Security Awareness and Skills Training
15. Service Provider Management
16. Application Software Security
17. Incident Response Management
18. Penetration Testing

Αναλυτικά, στο Παράρτημα Α' βρίσκεται η μετάφραση των CIS Critical Security Controls στη ελληνική ή στην αγγλική γλώσσα https://www.cisecurity.org/controls/v8 .

Κάθε μέτρο προστασίας εκτελεί και μια Λειτουργία Ασφάλειας (Security Function). Η Λειτουργία Ασφάλειας έρχεται να κατηγοριοποιήσει το μέτρο προστασίας με βάση τη λειτουργία που του αποδίδεται από το πλαίσιο των CIS Controls, κατηγοριοποίηση που βρίσκει εφαρμογή σε αρκετά αντίστοιχα πρότυπα, πλαίσια, κανονισμούς και έρευνες κυβερνοασφάλειας όπως για παράδειγμα στο NIST Cybersecurity Framework. Οι Λειτουργίες Ασφάλειας:

— Identify (Αναγνώριση)

— Respond (Ανταπόκριση)

— Detect (Ανίχνευση)

— Protect (Προστασία)

— Recover (Ανάκτηση)

Κάθε μέτρο προστασίας των CIS Controls αντιστοιχεί σε έναν τύπο αγαθού του πληροφοριακού συστήματος . Δηλαδή σε ένα αγαθό όπου βρίσκει εφαρμογή. Τύποι αγαθών:

1 Applications (Εφαρμογές)

2 Devices (Συσκευές)

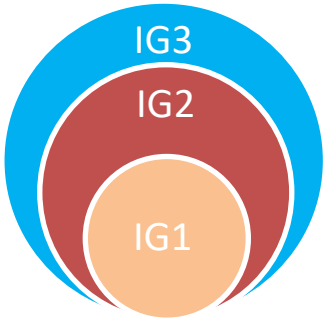
3 Network (Δίκτυο)

4 Data (Δεδομένα)

5 Users (Χρήστες)

6 Not Available (Δεν υπάρχει συγκεκριμένη αντιστοίχιση σε τύπο αγαθού)

Στο πλαίσιο των CIS Controls οι οργανισμοί κατατάσσονται σε 3 κατηγορίες, το Implementation Group 1(IG1), Implementation Group 2(IG2) και Implementation Group 3(IG3). Τα μέτρα προστασίας του Implementation Group 1 αποτελούν υποσύνολο των μέτρων του Implementation Group 2, και αυτά τα δυο μαζί αποτελούν υποσύνολο των μέτρων του Implementation Group 3.




**Εικόνα 2.1 – Δομή των Implementation Groups του CIS CSC**

*Implementation Group 1:*

Στην 1η κατηγορία υλοποίησης ανήκουν τα βασικά μετρά προστασίας τα οποία κάθε οργανισμός θα πρέπει να υλοποιήσει. Έχουν σχετικά χαμηλό κόστος και δεν απαιτούν εξειδικευμένη γνώση για να υλοποιηθούν και να συντηρηθούν. Αναφέρεται σε μικρομεσαίους οργανισμούς με περιορισμένη υποδομή πληροφορικής και περιορισμένη εξειδικευμένη γνώση σε θέματα κυβερνοασφάλειας. Ο πρωτεύον στόχος του οργανισμού είναι να διατηρηθεί η λειτουργικότητα της επιχείρησης. Ο βαθμός ευαισθησίας των δεδομένων που διαχειρίζονται είναι χαμηλός και αφορά κυρίως πληροφορίες για υπαλλήλους ή οικονομικά στοιχεία. Τα μέτρα προστασίας είναι δομημένα έτσι ώστε να μπορούν να λειτουργήσουν με τυποποιημένο λογισμικό το οποίο προσφέρεται στο εμπόριο, έχει περιορισμένες δυνατότητες παραμετροποίησης και ανήκει στην κατηγορία εμπορευμάτων COTS (Commercial Of The Shelf). Σύνολο 56 μέτρα προστασίας.

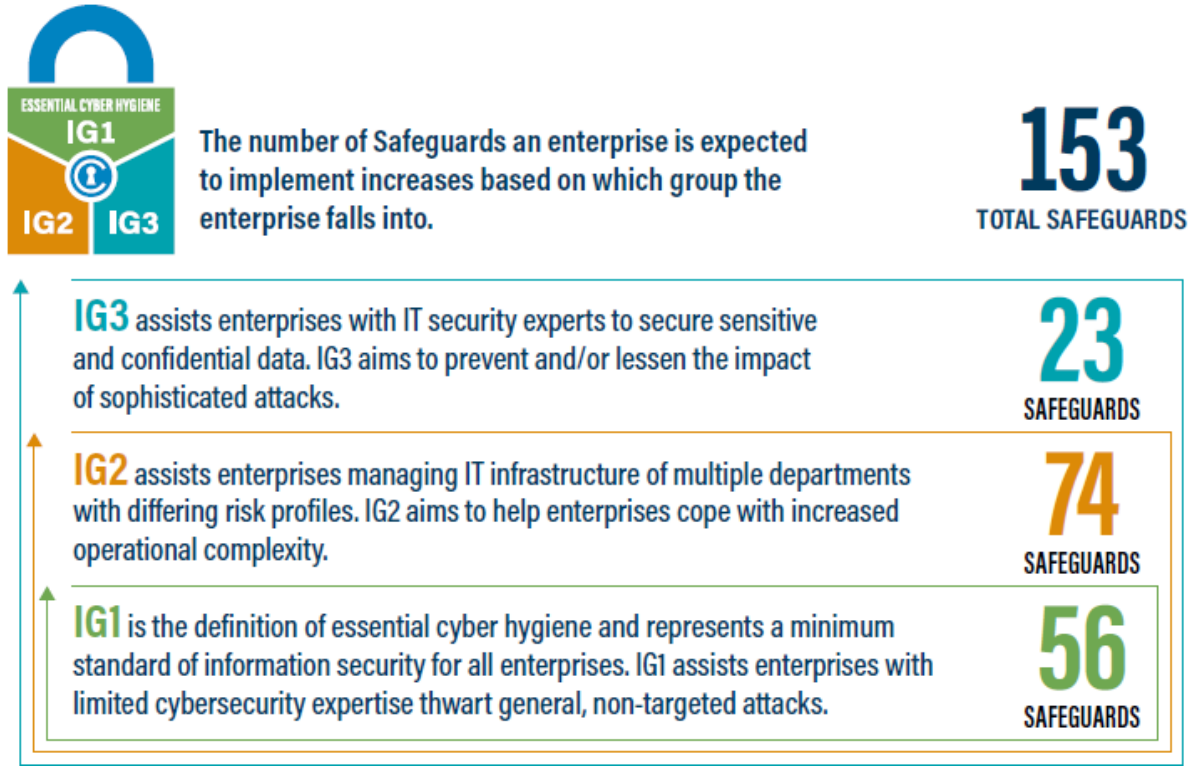
Implementation Group 2:

Ένας οργανισμός κατηγορίας 2 απασχολεί προσωπικό το οποίο είναι υπεύθυνο για την διαχείριση και προστασία του πληροφοριακού συστήματος. Τέτοιοι οργανισμοί αποτελούνται από τμήματα τα οποία έχουν διαφορετικά επίπεδα ρίσκου βασισμένα στον ρόλο, στον σκοπό και,σε κάποιο βαθμό, στη συμμόρφωση με κανονισμούς και νόμους. Οργανισμοί της κατηγορίας 2 συχνά επεξεργάζονται και

αποθηκεύουν ευαίσθητα δεδομένα πελατών και τρίτων οργανισμών και είναι σε θέση να αντέξουν βραχυπρόθεσμες διακοπές στις υπηρεσίες τους. Μια σημαντική ανησυχία αποτελεί η απώλεια της εμπιστοσύνης του κοινού σε περίπτωση παραβίασης. Τα μέτρα προστασίας της κατηγορίας υλοποίησής 2 είναι σε θέση να προστατέψουν έναν οργανισμό με αυξημένη λειτουργική πολυπλοκότητα.
Ορισμένα μέτρα προστασίας εξαρτώνται από το επίπεδο κατάρτισης του τεχνικού προσωπικο
Σύνολο 129 μέτρα προστασίας.

Implementation Group 3:

Ένας οργανισμός της κατηγορίας 3 απασχολεί προσωπικό σε διάφορες ειδικότητες της κυβερνοασφάλειας (π.χ. Risk Management, Penetration Testing, Application Security). Τα πάγια/αγαθά και δεδομένα του οργανισμού εμπεριέχουν ευαίσθητα δεδομένα ή κρίσιμες υπηρεσίες που υπόκεινται σε κανονιστική εποπτεία ή και σε εποπτεία συμμόρφωσης. Ένας οργανισμός της κατηγορίας 3 πρέπει να αντιμετωπίσει θέματα διαθεσιμότητας των υπηρεσιών του και την διαφύλαξη της ακεραιότητας και εμπιστευτικότητας των δεδομένων που κρατεί. Πετυχημένες επιθέσεις μπορεί να βλάψουν το κοινωνικό σύνολο. Μέτρα προστασίας της κατηγόριας 3 μπορούν να μειώσουν τον κίνδυνο εκδήλωσης στοχευμένης επίθεσης/εισβολής από ομάδες APT και την επίπτωση επιθέσεων από εκμετάλλευση zero-day ευπαθειών. Σύνολο 153 μέτρα προστασίας.




**Εικόνα 2.2 - Implementation Groups**

Το σύνολο ή υποσύνολο των CIS Controls προσφέρουν αντιστοίχιση στο σύνολο ή υποσύνολο των παρακάτω προτύπων και πλαισίων [5]:

| | | |
|---|---|---|
| NIST 800-53 rev4 | NSA Top 10 | FFIEC CAT |
| ISO 27002-2005 | Australian Top 35 | FFIEC Examination Handbook |
| ISO 27002-2013 | Australian Essential 8 | FFIEC Booklet 2016 |
| DHS CDM Program | DHS Chem Anti-Terrorism | HIPAA |
| NIST SMB Guide | NSA MNT | PCI DSS 3.0 |
| NIST 800-82 rev2 | NIST 800-171 | PCI DSS 3.1 |
| NIST CSF 1.1 | IEC 62443-3-3-2013 | PCI DSS 3.2 |
| UK Cyber Essentials | AICPA SOC2 and SOC3 TSPC | FY15 FISMA Metrics |

| | | |
|---|---|---|
| GCHQ 10 Steps | AICPA SOC2 and SOC3 TSC 2017 | SEC OCIE Audit Guide for AWS |
| Canadian CSE Top 10 | COBIT 5 | CSA CCM v3 |
| NERC CIP v3 | NERC CIP v4 | NERC CIP v5 |
| NERC CIP v7 | Saudi AMA | SG MAS TRM |
| SWIFT | IRS Pub1075 | AICPA GAPP |
| ANSSI - 40 Measures | Victorian PDSF v1.0 | NYCRR 500 |
| CoM 201 CMR 17.00 | NV Gaming MICS | ITIL 2011 KPIs |
| MITRE Att&ack | | |

**Πίνακας 1 - Παγκόσμια Πρότυπα για Information Security, IT Service Management, Risk Management**

## 2.2 MITRE Att&ck

Ο οργανισμός MITRE είναι ένας μη κυβερνητικός οργανισμός που έχει αποσπαστεί από το Τεχνολογικό Ινστιτούτο Μασαχουσέτης(MIT). Ως αποτέλεσμα ερευνών στον κυβερνοχώρο Fort Meade Experiment (FMX) προέκυψε το πλαίσιο MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK).

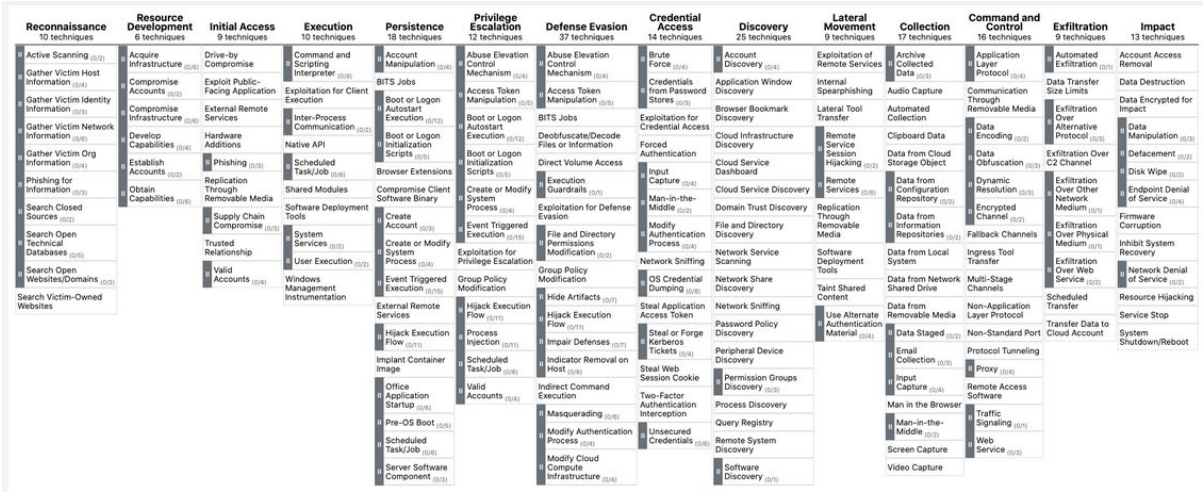
Το πλαίσιο MITRE Attack αποτελεί τη βάση γνώσεων και μοντελοποίησης των πρακτικών που χρησιμοποιούν κακόβουλες οντότητες για να επιτεθούν σε πληροφοριακά συστήματα οργανισμών καθώς και τον ολοκληρωμένο κύκλο ζωής (kill chain) αυτών των επιθέσεων [6]. Το μοντέλο ταξινομεί τις πρακτικές των επιθέσεων των κακόβουλων οργανισμών σε Τακτικές, Τεχνικές και Υπο-Τεχνικές (Tactics and Sub-Techniques), έτσι ώστε να γίνουν κατανοητές από πλευράς επίθεσης και άμυνας κυβερνοχώρου. Στην δομή ενός πίνακα είναι καταγεγραμμένες όλες οι γνώστες Τεχνικές και Υποτεχνικές που μπορούν να χρησιμοποιηθούν για επιθέσεις και είναι κατηγοριοποιημένες σε Τακτικές. Σχεδόν σε κάθε τεχνική αντιστοιχεί ένα ή περισσότερα αντίμετρα (Mitigations) με τα οποία μπορεί να αντιμετωπιστεί.

Από τις 530 τεχνικές και υποτεχνικές, οι 84 δεν αντιστοιχούν σε κάποιο αντίμετρο, δηλαδή πρόκειται για τεχνικές που δεν μπορούν να αντιμετωπιστούν ή μπορούν να αντιμετωπιστούν πολύ δύσκολα.

Πίνακες Mitre Attack:

1) Attack for Enterprise και Pre-Attack: Επικεντρώνεται στα λειτουργικά σύστημα Windows, Mac, Linux και Cloud περιβάλλοντα.

2) Attack for Mobile: Επικεντρώνεται σε λειτουργικά συστήματα iOS και Android




**Εικόνα 2.3 - Στιγμιότυπο του πίνακα MITRE Attack Enterprise**

Τακτικές MITRE Attack for Enterprise και Pre-Attack:

1. Reconnaissance: Συλλογή πηλοφοριών για το σχεδιασμό και την προετοιμασία μιας κυβερνοεπίθεσης
2. Resource Development: Ανάπτυξη της κατάλληλης υποδομής για την διεξαγωγή μιας ολοκληρωμένης επίθεσης
3. Initial Access: Απόκτηση αρχικής πρόσβασης
4. Excution: Εκτέλεση κακόβουλου κώδικα
5. Persistance: Απόκτηση μόνιμης πρόσβασης
6. Priviledge Escalation: Επαύξηση δικαιωμάτων
7. Defense Evasion: Αποφυγή συστημάτων εντοπισμού παραβίασης
8. Credential Access: Υποκλοπή κωδίκων πρόσβασης και λογαριασμών
9. Discovery: Αναγνώριση δικτυακής υποδομής και συστημάτων
10. Lateral Movement: Απόκτηση πρόσβασης σε γειτονικά συστήματα και δίκτυα εντός των υποδομών του πληροφοριακού συστήματος
11. Collection: Συλλογή δεδομένων ενδιαφέροντος που αποτελούν τον στόχο ή τον εν μέρει στόχο της επίθεσης
12. Command & Control: Απομακρυσμένος έλεγχος των παραβιασμένων συστημάτων
13. Exfiltration: Εξαγωγή των δεδομένων χωρίς να αποκαλυφθεί η κίνηση
14. Impact: Επίπτωση στην εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα των συστημάτων και των δικτύων του στόχου

## 2.3 CIS Community Defense Model

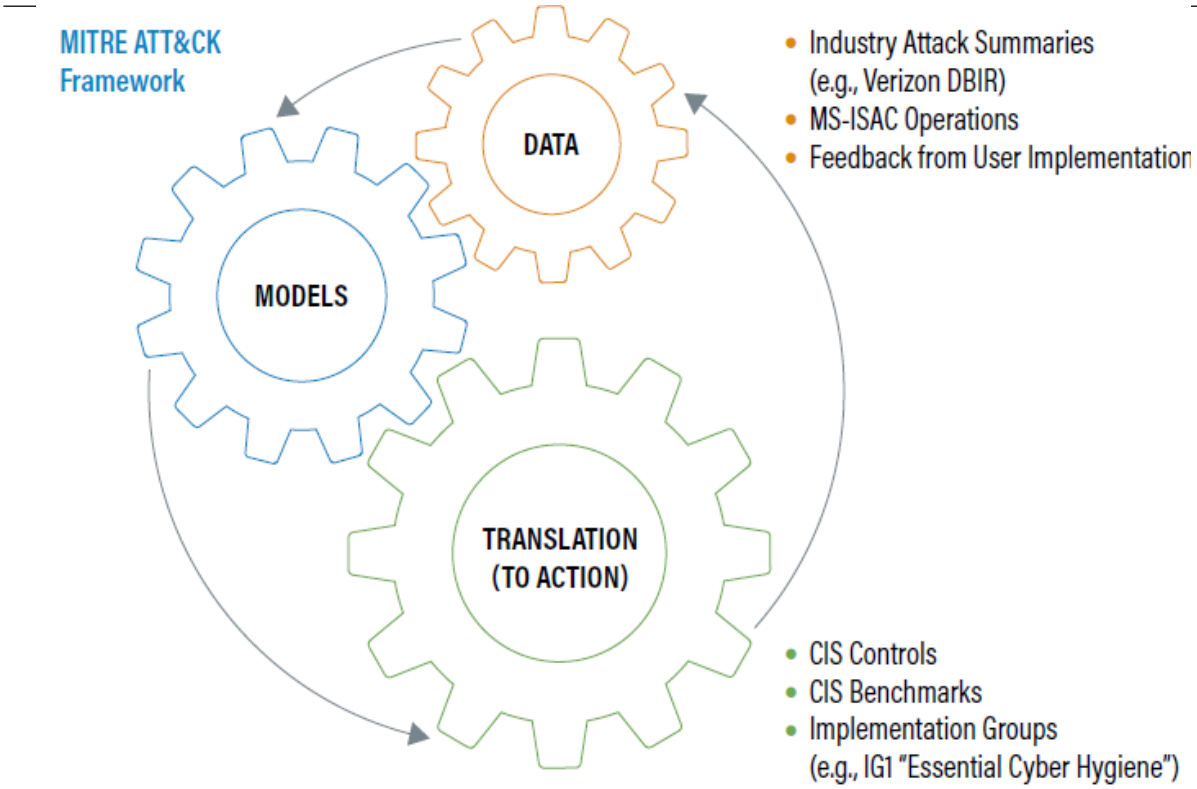
Το CIS Community Defense Model (CDM) αποτελεί μια μελέτη του Center for Internet Security. Γεφυρώνει τα πλαίσια των CIS Controls και Mitre Attack. Έρχεται να απαντήσει σε ζητήματα όπως είναι η ιεράρχηση μέτρων προστασίας με γνώμονα «Ποιο μέτρο προστασίας πρέπει να εφαρμοστεί πρώτο» και την Αξία Ασφάλειας (Security Value) του κάθε μέτρου προστασίας ενάντια στις απειλές του κυβερνοχώρου [7].

| Data Source | Publish Date | Type | Longevity | CIS Access to Underlying Data |
|---|---|---|---|---|
| Verizon DBIR | May 19, 2020 | Self-reported data, Sensor data, Incident response data | 2008 | No[7] |
| IBM X-Force Threat Intelligence Index | February 24, 2021 | Sensor data, Incident response data | 2017 | No |
| ENISA Threat Landscape – The Year in Review | October 20, 2020 | Open-source intelligence | 2012 | No |
| CrowdStrike Services Cyber Front Lines Report | 2020 | Sensor data, Incident response data, Product usage data | 2020 | No |
| Akamai The State of the Internet: A Year in Review | 2020 | Sensor data, Product usage data | 2008 | No |

**Εικόνα 2.4 - Πηγές δεδομένων της έρευνας CDM του CIS**

Το CDM εστιάζει σε 2 κύριες έννοιες, την Λειτουργία Ασφάλειας(Security Function) και την Αξία Ασφάλειας(Security Value). Η Λειτουργία Ασφάλειας μπορεί να οριστεί ως η δυνατότητα ενός μέτρου προστασίας να αντιμετωπίσει μια ή περισσότερες MITRE Attack τεχνικές ανεξαρτήτως του τύπου επίθεσης. Η 'Λειτουργία Ασφάλειας' δεν απαντάει στο γιατί να υλοποιηθεί το συγκεκριμένο μέτρο Προστασίας, αλλά προσφέρει τη βάση ώστε να αξιολογηθεί η 'Αξία Ασφάλειάς' του, η οποία μπορεί να οριστεί ως το όφελος που προκύπτει από την αντιμετώπιση μίας ή περισσοτέρων τύπων επιθέσεων ή απειλών.

Το CDM παίρνει δεδομένα επιθέσεων (Εικόνα 2.4), από Verizon Data Breach Investigations Report [8], IBM X-Force Threat Landscape [9], ENISA Threat Landscape [10], CrowedStrike Services Cyber Front Lines Report [11], Akamai The State of the Internet [12] και τα μοντελοποιεί μέσω του πλαισίου MITRE Attack. Το πλαίσιο MITRE Attack επιτρέπει να εκφραστεί κάθε κυβερνοεπίθεση μέσω ενός συνόλου τεχνικών και υποτεχνικών, δηλαδή μέσω ενός μοτίβου επίθεσης. Στην συνέχεια, εντοπιστήκαν τα μετρά προστασίας / αντίμετρα των CIS Controls. Αυτή η μεθοδολογία επιτρέπει να εντοπιστούν ποια μέτρα προστασίας των CIS Controls είναι τα πιο αξιόπιστα ενάντια σε όλους τους τύπους επιθέσεων.



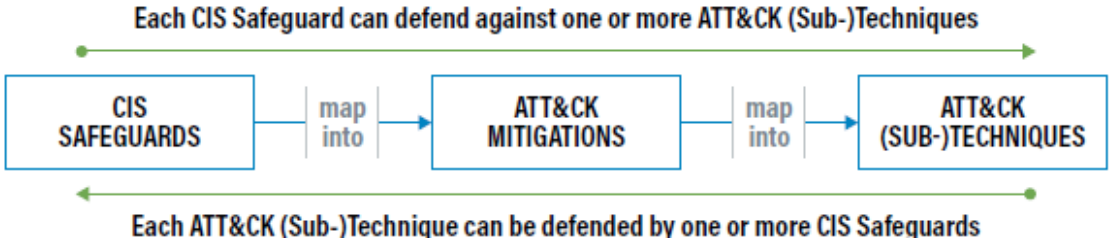

**Εικόνα 2.5 -Σχηματική απεικόνιση μεθοδολογίας / High Level**

Διαδικασία σε 7 βήματα

- Create master mapping. Αντιστοίχιση των CIS Controls v8 στο Enterprise MITRE Attack v8.2
- Analyze security function. Ανάλυση των Λειτουργιών Ασφάλειας των CIS μέτρων προστασίας έναντι των MITRE Attack (υπο-)τεχνικών μέσω του master mapping του βήματος 1.
- Identify top five attack type. Μέσω διάφορων πηγών εντοπίστηκαν οι 5 επικρατέστερες κατηγορίες επιθέσεων, οι οποίες είναι οι ακόλουθες: Malware, Ransomware, Web Application Hacking, Insider Privilege and Misuse, Targeted Intrusions.
- Construct attack pattern. Για κάθε τύπο επίθεσης χρησιμοποιήθηκαν διάφορες πήγες για την δημιουργία μοτίβων επίθεσης – το σύνολο των τεχνικών επίθεσης (MITRE Attack τεχνικές και πυροτεχνικές)
- Perform reverse mapping. Έγινε χρήση του master mapping CIS Controls προς MITRE Attack (υπό-)τεχνικές (βήμα 1) που συνδέονται με έναν τύπο επίθεσης προς τα μέτρα προστασίας CIS.
- Analyze Security Value. Το reverse mapping επιτρέπει την ανάλυση της Αξίας Ασφάλειας υλοποίησης ενός μέτρου προστασίας CIS έναντι ενός ή περισσοτέρων τύπων επίθεσης, δηλαδή αξιολογεί την απόδοση κυβερνοάμυνας ενός CIS μέτρου προστασίας έναντι των 5 τύπων επιθέσεων.

— Create Visualizations. Ο MITRE Attack Navigator επιτρέπει στους χρήστες να δημιουργήσουν οπτικά τα επίπεδα επιθέσεων.

Η αντιστοίχιση γίνεται από ένα CIS μέτρο προστασίας (Safeguard) προς ένα αντίμετρο (Mitigation)του πίνακα MITRE Attack και στην συνέχεια από εκεί προς μια (υπό-) τεχνική. Αυτές οι σχέσεις αντιστοίχισης προκαλούν μια σχέση «πολλά προς πολλά» στην αντιστοίχιση μέτρων προστασίας CIS προς MITRE Attack (υπο-)τεχνικών. Επομένως, αξίζει να σημειωθεί ότι η υλοποίηση ενός CIS μέτρου προστασίας μπορεί να προστατέψει από μια ή περισσότερες (υπό-) τεχνικές MITRE Attack και μια (υπό-) τεχνική μπορεί να αντιμετωπιστεί από ένα ή περισσότερα μέτρα προστασίας CIS.

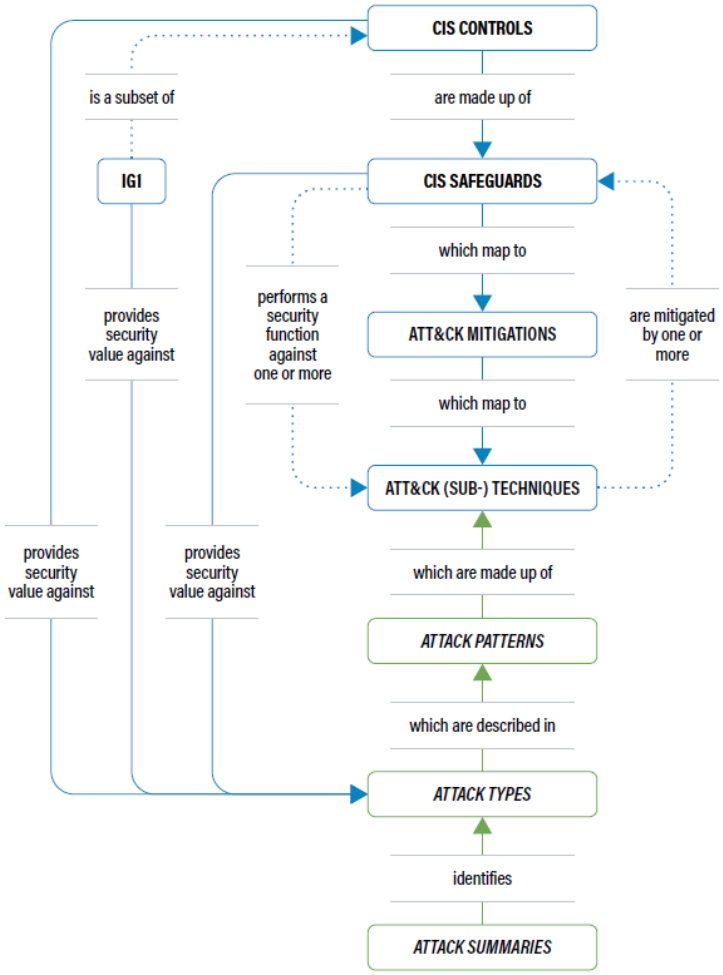



**Εικόνα 2.6 - Αντιστοίχιση Mitre Attack vs CIS Controls**

Η Λειτουργία Ασφάλειας είναι ανεξάρτητη από την κατηγορία απειλής και αφορά την δυνατότητα ενός μέτρου προστασίας CIS να προστατέψει από μια ή περισσότερες τεχνικές MITRE Attack. Το πρώτο βήμα αφορά την αντιστοίχιση των CIS μέτρων προστασίας στα αντίμετρα MITRE Attack, όπου ένα μέτρο προστασίας μπορεί να αντιστοιχηθεί με περισσότερα του ενός αντίμετρα και αντίστροφα. Τα CIS μέτρα προστασίας αντιστοιχήθηκαν με MITRE Attack αντιμέτρα κατά 93%. Στον πίνακα που απεικονίζεται στην εικόνα 2.7 παρουσιάζονται τα πρώτα 10.Στην συνέχεια αντιστοιχούνται οι (υπό-) τεχνικές MITRE Attack σε CIS μέτρα προστασίας. Στην εικόνα 2.9 απεικονίζονται οι πρώτες 20 αντιστοιχίσεις. Για να μετριαστεί μια τεχνική δεν απαιτείται το σύνολο των μέτρων προστασίας που αναφέρονται μιας και ένα μέτρο προστασίας μπορεί να αντιμετωπίσει πολλαπλές τεχνικές. Από τις 446 MITRE Attack (υπό-τεχνικές) που έχουν καταλληλά αντιμέτρα, τα 383 αντιστοιχήθηκαν σε μέτρα προστασίας CIS.

| Rank | ATT&CK Mitigation ID | ATT&CK Mitigation Name | Number of ATT&CK Mitigations Mapped to CIS Safeguards |
|---|---|---|---|
| 1 | M1047 | Audit | 23 |
| 2 | M1051 | Update Software | 19 |
| 3 | M1016 | Vulnerability Scanning | 17 |
| 4 | M1018 | User Account Management | 16 |
| 5 | M1026 | Privileged Account Management | 15 |
| 6 | M1042 | Disable or Remove Feature or Program | 14 |
| 7 | M1029 | Remote Data Storage | 14 |
| 8 | M1035 | Limit Access to Resource Over Network | 13 |
| 9 | M1037 | Filter Network Traffic | 12 |
| 10 | M1030 | Network Segmentation | 10 |

**Εικόνα 2.7 - Αντιστοίχιση MITRE Attack mitigations σε CIS safeguards**




**Εικόνα 2.8 - Ροές διαδικασίας**

Αντίστοιχα, με την αντίστροφη φορά αντιστοιχήθηκαν τα CIS μέτρα προστασίας στις υπό-τεχνικές MITRE Attack. Από την αντιστοίχιση προέκυψε ότι από τα 153 μέτρα προστασίας το 68% προστατεύει από μια ή περισσότερες (υπό-)τεχνικές MITREAttack και 19 μέτρα προστασίας αντιμετωπίζουν 50 και πλέον (υπό)τεχνικές. Στ παρακάτω πίνακα που απεικονίζεται στην εικόνα 2.11 αναφέρονται τα πρώτα 20, με το μέτρο προστασίας «4.1 Δημιουργία και Συντήρηση Διαδικασίας Ασφαλούς Διαμόρφωσης Εξοπλισμού» να ξεχωρίζει, με 342 αντιστοιχήσεις. Το σύνολο των αντιστοιχίσεων CIS Controls vs. MITRE Attack μπορεί να βρεθεί στο Master Mapping (Παράρτημα Β').

Η αξία ασφάλειας εκφράζει τη δυνατότητα ενός CIS μέτρου προστασίας να μετριάσει έναν ή περισσοτέρους τύπους επιθέσεων. Ανεξάρτητα από το Master Mapping όπου αντιστοιχούνται τα CIS Controls με τις τεχνικές MITRE Attack, έγινε στο πλαίσιο του CIS CDM και μια ανάλυση για τις 5 πιο σημαντικές απειλές, οι όπως απεικονίζονται στην εικόνα 2.10 και παρουσιάζονται αναλυτικά στο Reverse Mapping (Παράρτημα Γ'). Το συμπέρασμα των αντιστοιχίσεων ήταν ότι τα μέτρα προστασίας του Implementation Group 1 είναι σε θέση να προστατέψουν τουλάχιστον 77% από τις τεχνικές που χρησιμοποιούν οι κατηγορίες επιθέσεων, όπως απεικονίζεται στον πίνακας της εικόνας 2.11

| Rank | ATT&CK (Sub-) Technique ID | ATT&CK (Sub-)Technique Name | Number of CIS Safeguards Mapped to an ATT&CK (Sub-)Technique |
|---|---|---|---|
| 1 | T1021.001 | Remote Desktop Protocol | 42 |
| 2 | T1563.002 | RDP Hijacking | 41 |
| 3 | T1552 | Unsecured Credentials | 39 |
| 4 | T1072 | Software Deployment Tools | 38 |
| 5 | T1210 | Exploitation of Remote Services | 35 |
| 6 | T1190 | Exploit Public-Facing Application | 33 |
| 7 | T1059 | Command and Scripting Interpreter | 30 |
| 8 | T1557 | Man-in-the-Middle | 29 |
| 9 | T1530 | Data from Cloud Storage Object | 28 |
| 10 | T1574 | Hijack Execution Flow | 27 |
| 11 | T1003 | OS Credential Dumping | 25 |
| 12 | T1133 | External Remote Services | 24 |
| 13 | T1543.002 | Systemd Service | 24 |
| 14 | T1563 | Remote Service Session Hijacking | 24 |
| 15 | T1059.001 | PowerShell | 24 |
| 16 | T1021.005 | VNC | 23 |
| 17 | T1542.005 | TFTP Boot | 23 |
| 18 | T1548 | Abuse Elevation Control Mechanism | 22 |
| 19 | T1602.001 | SNMP (MIB Dump) | 22 |
| 20 | T1543 | Create or Modify System Process | 22 |

**Εικόνα 2.9 - Αντιστοίχιση MITRE Attack τεχνικών με CIS safeguards**

Η ερεύνα του CIS CDM αποτελεί μια γέφυρα μεταξύ των CIS Controls και του πίνακα Mitre Attack και αποτελεί την βάση για τις δυο από τις τέσσερις συναρτήσεις αξιολόγησης ωριμότητας κυβερνοασφάλειας που χρησιμοποιήθηκαν στην εφαρμογή.

| Attack Type | % of ATT&CK (Sub-)Techniques Defended Against by IG1 CIS Safeguards | % of ATT&CK (Sub-)Techniques Defended Against by CIS Safeguards |
|---|---|---|
| Malware | 77% | 94% |
| Ransomware | 78% | 92% |
| Web Application Hacking | 86% | 98% |
| Insider Privilege and Misuse | 86% | 90% |
| Targeted Intrusions | 83% | 95% |

**Εικόνα 2.10 - High Level αποτέλεσμα reverse mapping των top5 threats**

| Rank | CIS Safeguard | CIS Safeguard Title | Number of ATT&CK (Sub-) Techniques Defended by a CIS Safeguard | IG1 | IG2 | IG3 |
|---|---|---|---|---|---|---|
| 1 | 4.1 | Establish and Maintain a Secure Configuration Process | 342 | ✓ | ✓ | ✓ |
| 2 | 6.1 | Establish an Access Granting Process | 217 | ✓ | ✓ | ✓ |
| 3 | 6.2 | Establish an Access Revoking Process | 217 | ✓ | ✓ | ✓ |
| 4 | 18.3 | Remediate Penetration Test Findings | 214 | | ✓ | ✓ |
| 5 | 6.8 | Define and Maintain Role-Based Access Control | 206 | | | ✓ |
| 6 | 4.7 | Manage Default Accounts on Enterprise Assets and Software | 188 | ✓ | ✓ | ✓ |
| 7 | 18.5 | Perform Periodic Internal Penetration Tests | 187 | | | ✓ |
| 8 | 5.4 | Restrict Administrator Privileges to Dedicated Administrator Accounts | 164 | ✓ | ✓ | ✓ |
| 9 | 5.3 | Disable Dormant Accounts | 155 | ✓ | ✓ | ✓ |
| 10 | 2.5 | Allowlist Authorized Software | 101 | | ✓ | ✓ |
| 11 | 2.7 | Allowlist Authorized Scripts | 81 | | | ✓ |
| 12 | 3.3 | Configure Data Access Control Lists | 75 | ✓ | ✓ | ✓ |
| 13 | 4.2 | Establish and Maintain a Secure Configuration Process for Network Infrastructure | 73 | ✓ | ✓ | ✓ |
| 14 | 2.3 | Address Unauthorized Software | 67 | ✓ | ✓ | ✓ |
| 15 | 4.4 | Implement and Manage a Firewall on Servers | 60 | ✓ | ✓ | ✓ |
| 16 | 4.8 | Uninstall or Disable Unnecessary Services on Enterprise Assets and Software | 54 | | ✓ | ✓ |
| 17 | 13.8 | Deploy a Network Intrusion Prevention Solution | 53 | | | ✓ |
| 18 | 13.3 | Deploy a Network Intrusion Detection Solution | 53 | | ✓ | ✓ |
| 19 | 12.2 | Establish and Maintain a Secure Network Architecture | 51 | | ✓ | ✓ |
| 20 | 5.2 | Use Unique Passwords | 47 | ✓ | ✓ | ✓ |

**Εικόνα 2.11 - Αντιστοίχιση CIS Safeguards με MITRE Attack τεχνικές**

## 2.4 NIST Cybersecurity Framework

Το πλαίσιο κυβερνοασφάλειας του NIST αποτελεί μια πρακτική εκούσιας καθοδήγησης βασισμένη σε υπάρχοντα πρότυπα και οδηγίες, έτσι ώστε να υποστηρίξει οργανισμούς να βελτιώσουν τη διαχείριση και να μειώσουν το ρίσκο κυβερνοασφάλειας. Το πλαίσιο είναι οργανωμένο σε 5 βασικούς πυλώνες λειτουργικότητας ασφάλειας (Security Functions) - Identify, Project, Detect, Respond, Recover. Αυτοί οι 5 ευρέως κατανοητοί όροι, εφόσον συνδυαστούν, μπορούν να αποτελέσουν μια περιεκτική εικόνα του κύκλου ζωής και διαχείρισης της κυβερνοασφάλειας. Παρουσιάζουμε συνοπτικά τις θεματικές που πραγματεύονται οι 5 Λειτουργικότητες Ασφάλειας [13].


**Εικόνα 2.12 – Βασικές λειτουργικότητές του πλαισίου NIST CSF**

**Identify,** αφορά τη διαχείριση και την κατανόηση στη διαχείριση ρίσκων κυβερνοασφάλειας σε συστήματα, αγαθά, δεδομένα και δυνατότητες του οργανισμού. Οι βασικοί άξονες είναι οι ακόλουθοι:

- Αναγνώριση κρίσιμων διεργασιών και αγαθών του πληροφοριακού συστήματος ενός οργανισμού
- Καταγραφή ροών δεδομένων
- Διατήρηση μητρώου καταγραφής Hardware και Software αγαθών του οργανισμού
- Δημιουργία πολιτικών κυβερνοασφάλειας οι οποίες εμπεριέχουν ρόλους και ευθύνες
- Εντοπισμός, σε κάθε αγαθό, των απειλών, ευπαθειών και ρίσκων που του αντιστοιχούν

**Protect,** αφορά την υλοποίηση των κατάλληλων μηχανισμών προστασίας, έτσι ώστε να είναι ο οργανισμός σε θέση να παρέχει υπηρεσίες. Οι βασικοί άξονες είναι οι ακόλουθοι:

- Διαχείριση πρόσβασης σε αγαθά και δεδομένα του πληροφοριακού συστήματος
- Προστασία ευαίσθητων δεδομένων
- Διεξαγωγή backup σε τακτικά χρονικά διαστήματα
- Προστασία συσκευών/συστημάτων του πληροφοριακού συστήματος
- Διαχείριση ευπαθειών
- Εκπαίδευση χρηστών

**Detect,** αφορά την υλοποίηση και ανάπτυξη κατάλληλων μηχανισμών για τον εντοπισμό συμβάντων κυβερνοασφάλειας.

Οι βασικοί άξονες είναι οι ακόλουθοι:

- Δοκιμή και ενημέρωση διαδικασίας εντοπισμού μη εξουσιοδοτημένων ενεργειών στο πληροφοριακό σύστημα του οργανισμού
- Διαχείριση και επίβλεψη αρχείων καταγραφής συμβάντων
- Αναγνώριση και έλεγχος των ροών δεδομένων του οργανισμού
- Κατανόηση των επιπτώσεων συμβάντων κυβερνοασφάλειας

**Respond,** αφορά την υλοποίηση και ανάπτυξη κατάλληλων ενεργειών για την ανταπόκριση σε συμβάν κυβερνοασφάλειας. Οι βασικοί άξονες είναι οι ακόλουθοι:

- Διασφάλιση ότι τα πλανά ανταπόκρισης συμβάντων κυβερνοασφάλειας είναι κατανοητά και δοκιμασμένα
- Διασφάλιση ότι τα πλάνα ανταπόκρισης είναι ενημερωμένα

- Συντονισμός με εξωτερικούς και εσωτερικούς εμπλεκομένους/παράγοντες σε ότι αφορά το πλάνα ανταπόκρισης.

**Recover,** αφορά την υλοποίηση και ανάπτυξη κατάλληλων πρακτικών για την επαναφορά του πληροφοριακού συστήματος μετά από μια κυβερνοεπίθεση και την ανθεκτικότητα του. Οι βασικοί άξονες είναι οι ακόλουθοι:

- Επικοινωνία με εξωτερικούς και εσωτερικούς εμπλεκομένους/παράγοντες για να διασφαλιστεί ότι τα πλάνα ανάκτησης είναι ενημερωμένα
- Διαχείριση δημοσίων σχέσεων και φήμης του οργανισμού

# Κεφάλαιο 3: Δομή και Περιεχόμενο της Εφαρμογής “Cyber Defense Assessment Tool”

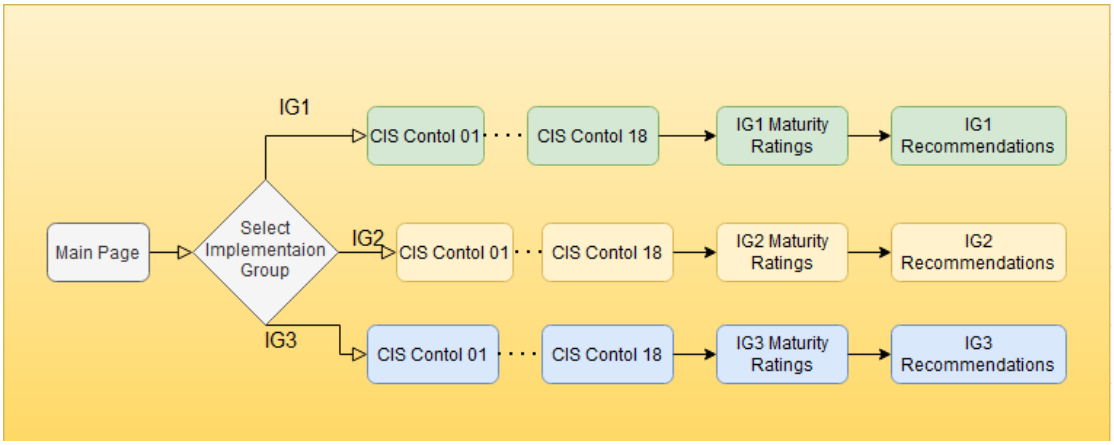
Με βάση τα πλαίσια, πρότυπα, βέλτιστες πρακτικές και τις έρευνες που αναφέρθηκαν πιο πάνω υλοποιήθηκε το εργαλείο «CyberDefenseAssessmentTool». Πρόκειται για ένα εργαλείο το οποίο λειτουργεί ως ερωτηματολόγιο. Οι ερωτήσεις είναι αντίστοιχες με τα μέτρα ασφαλείας CIS. Υπολογίζει βαθμούς/δείκτες επιπέδου ωριμότητας κυβερνοασφάλειας ενός πληροφοριακού συστήματος και προτείνει ιεραρχημένες συστάσεις για την επίτευξη βελτίωσης του επιπέδου ωριμότητας του οργανισμού που αξιολογείται.

## 3.1 Δομή Ερωτηματολογίου

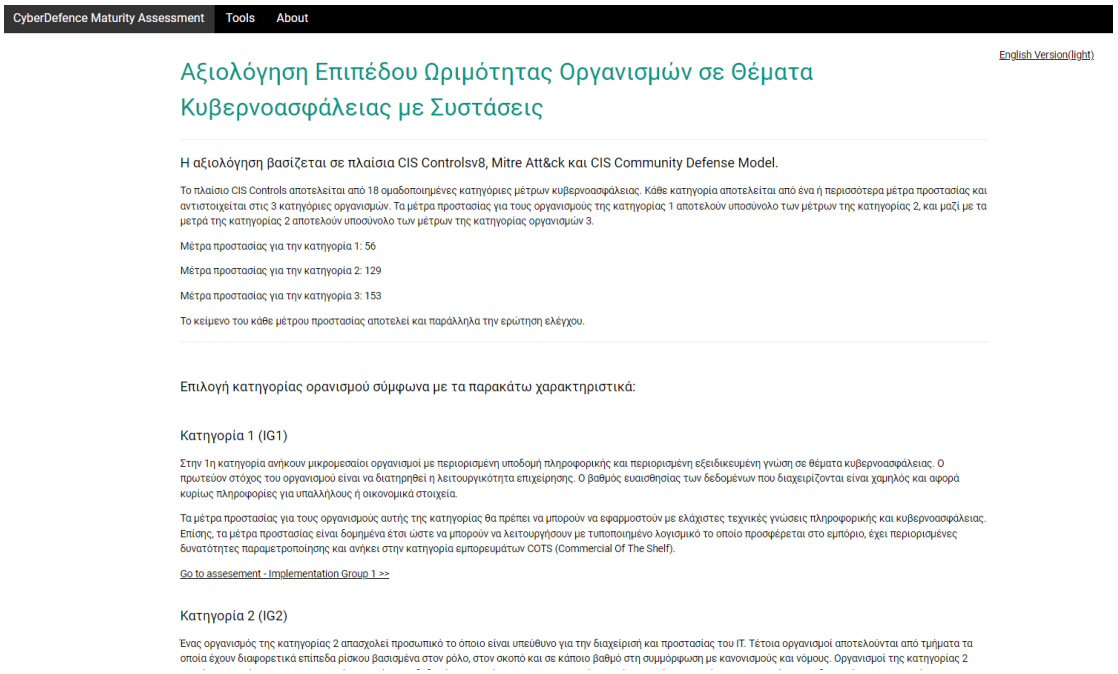
Το ερωτηματολόγιο αποτελείται από την έναρξη, όπου πρέπει να επιλεχθεί αρχικά σε ποια κατηγορία υλοποίησης ανήκει ο εξεταζόμενος οργανισμός. Στην συνέχεια ξεκινάνε οι ερωτήσεις/μέτρα προστασίας που πρέπει να απαντηθούν από το άτομα ή την ομάδα ατόμων που το συμπληρώνει. Στη τελική φάση παρουσιάζονται τα αποτελέσματα της αξιολόγησης ωριμότητας κυβερνοασφάλειας και οι αντίστοιχες συστάσεις. Στην εικόνα 3.1 απεικονίζεται η ροή της εφαρμογής.

## 3.2 Ερωτηματολόγιο - Έναρξη

Οι ερωτήσεις στις οποίες καλείται να ανταποκριθεί το υποκείμενο που συμπληρώνει το ερωτηματολόγιο, αποτελείται από το σύνολο των CIS Critical Security Controls. Η έναρξη του ερωτηματολογίου αποτελείται από μια μικρή εισαγωγή των πλαισίων στα οποία βασίζεται η αξιολόγηση του επιπέδου ωριμότητας κυβερνοασφάλειας και από την παρουσίαση των κύριων χαρακτηριστικών των κατηγοριών υλοποίησης (Implementation Group) 1,2 και 3. Το υποκείμενο καλείται να επιλέξει την κατηγορία υλοποίησης στην οποία ανήκει ο οργανισμός, ο οποίος αποτελεί και αντικείμενο της αξιολόγησης.



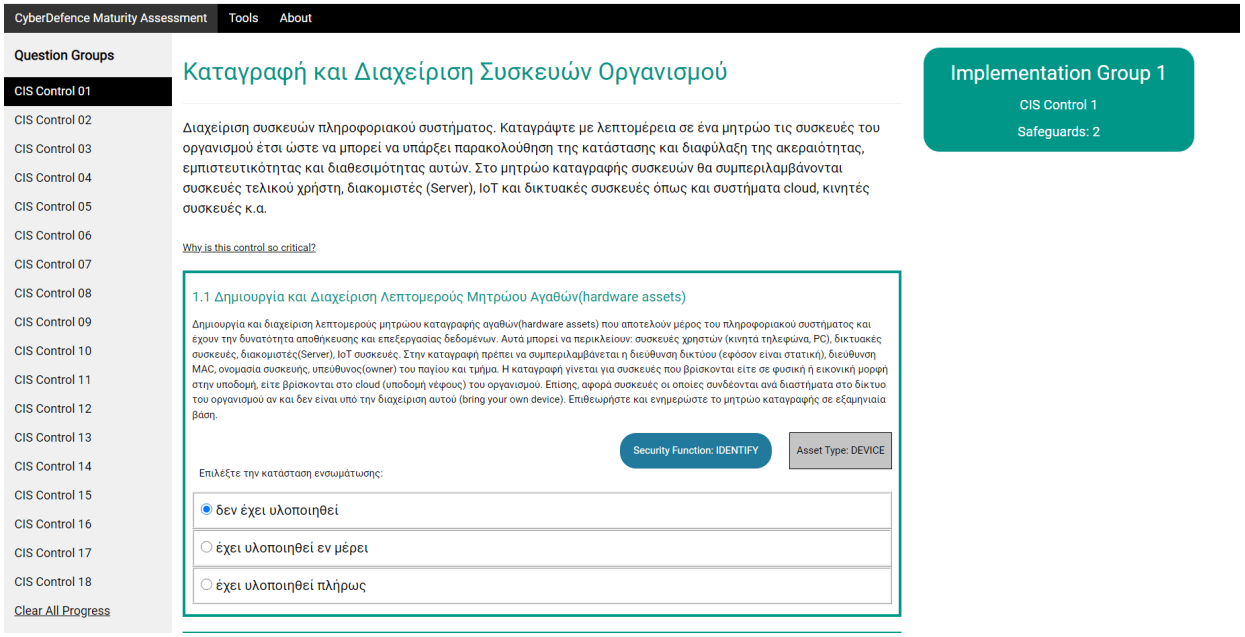

**Εικόνα 3.1 - Ροές ερωτηματολογίου**



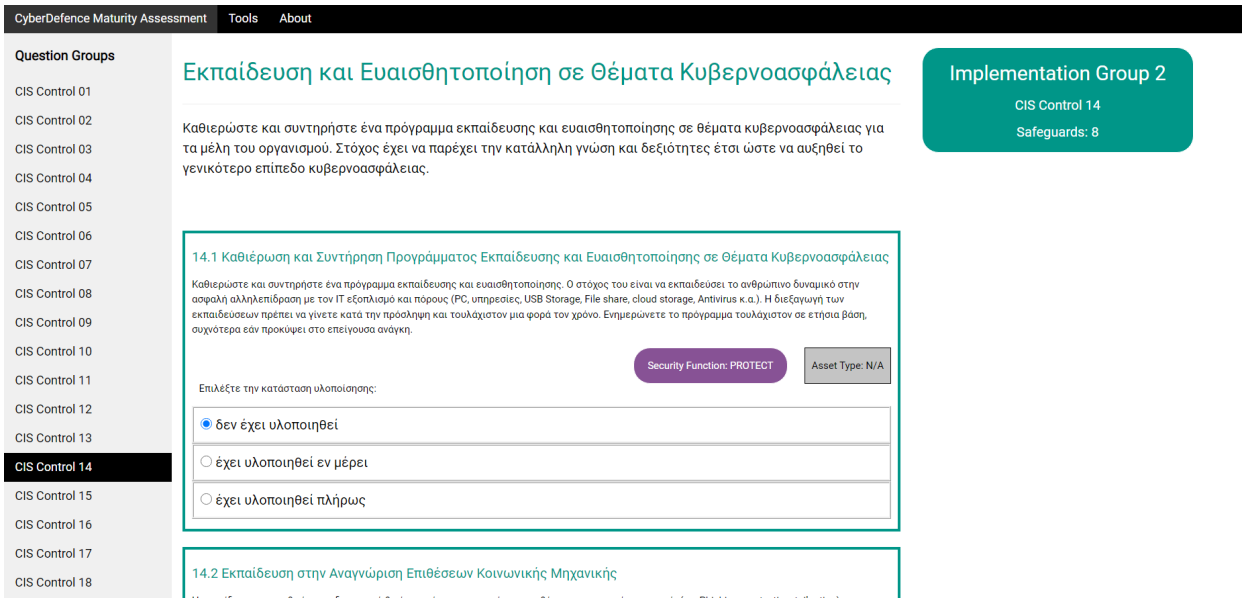

**Εικόνα 3.2 - Στιγμιότυπο της έναρξης του εργαλείου αξιολόγησης επιπέδου ωριμότητας κυβερνοασφάλειας**

## 3.2 Ερωτήσεις Ερωτηματολογίου

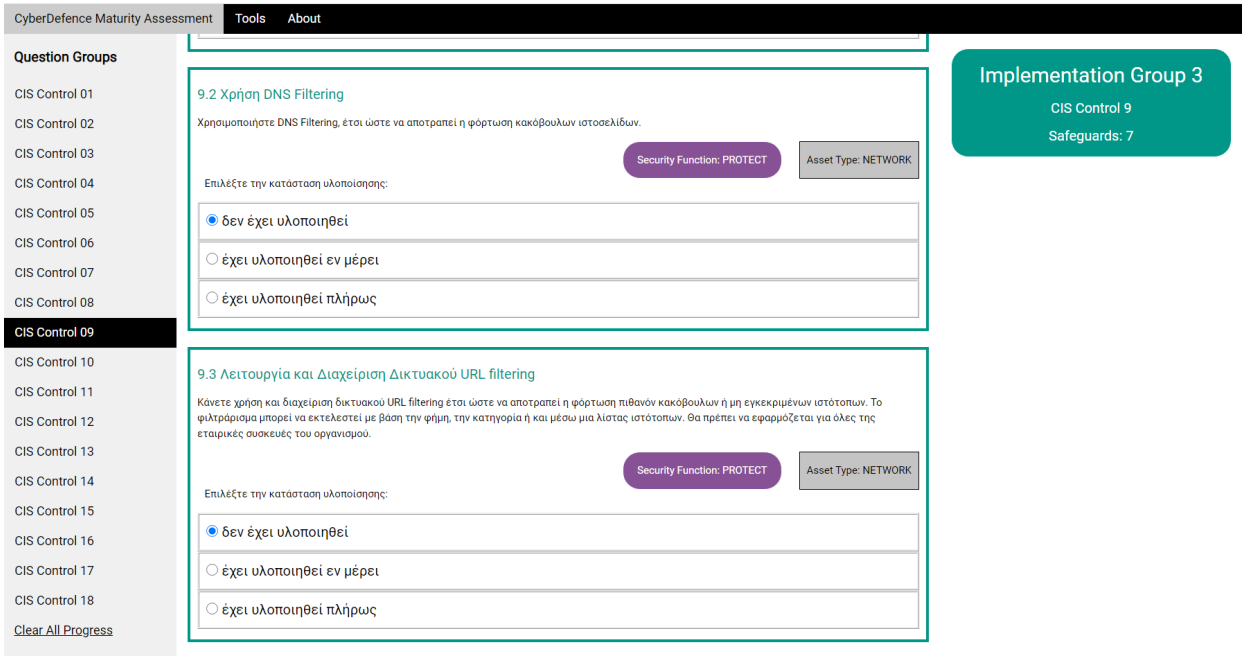
Τα θέματα προς απάντηση προέρχονται από τα CIS CS Controls. Είναι οργανωμένα σε 18 ενότητες/ομάδες. Κάθε ενότητα/ομάδα έχει ένα ή περισσότερα θέματα προς απάντηση τα οποία αντιστοιχούν στα μετρά προστασίας(safeguards) των CIS Controls. Για την κατηγορία υλοποίησης 1 (Implementation Group1) πρέπει τα απαντηθούν 56 θέματα. Για την κατηγορία υλοποίησης 2 (Implementation Group2) πρέπει να απαντηθούν 129 θέματα. Για την κατηγορία υλοποίησης 3 (Implementation Group3) πρέπει να απαντηθούν 153 θέματα. Η ανταπόκριση στις απαντήσεις αποτελεί την κύρια φάση της διαδικασίας συμπλήρωσης του ερωτηματολογίου.




**Εικόνα 3.3 - Στιγμιότυπο ερωτηματολογίου. Κατηγορία μέτρων 1, κατηγορία υλοποίησης 1**




**Εικόνα 3.4 - Στιγμιότυπο ερωτηματολογίου. Κατηγορία μέτρων 14, κατηγορία υλοποίησης 2**

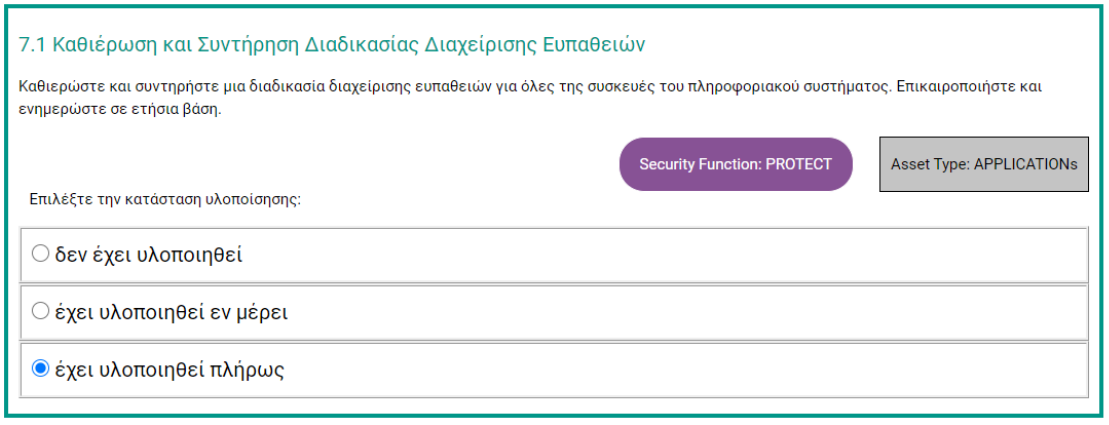



**Εικόνα 3.5 - Στιγμιότυπο ερωτηματολογίου. Κατηγορία μέτρων 9, κατηγορία υλοποίησης 3**

## 3.3 Απαντήσεις Ερωτηματολογίου

Η ομάδα ή το άτομο που συμπληρώνει το ερωτηματολόγιο πρέπει να επιλέξει την κατάσταση υλοποίησης. Δηλαδή κατά ποσό έχει προχωρήσει ο οργανισμός, ο οποίος αποτελεί αντικείμενο της αξιολόγησης, στην υλοποίηση του συγκεκριμένου μέτρου. Οι πιθανές ανταποκρίσεις/βαθμίδες είναι τρεις και μπορούν να επιλεχθούν με radio buttons:

1.) δεν έχει υλοποιηθεί
2.) έχει υλοποιηθεί εν μέρει
3.) έχει υλοποιηθεί πλήρως




**Εικόνα 3.6 – Στιγμιότυπο απάντησης μέτρου προστασίας 7.1**

Η ομάδα ή το άτομο που θα απαντήσει θα πρέπει να κατέχει την κατάλληλη γνώση για να ανταποκριθεί στα θέματα, να φέρει την αντίστοιχη ευθύνη και συχνά να ανήκει σε μια από τις παρακάτω βαθμίδες του οργανισμού:

- IT Director
- IT Admin Group and Network Engineer
- Information Security Officer
- Chief Information Officer
- Chief Technology Officer
- Ή άλλες παρόμοιες βαθμίδες ανάλογης λεπτομερούς γνώσης για την οργάνωση, διεύθυνση, διαχείριση και εξοπλισμό του πληροφοριακού συστήματος.

Η ομάδα ή το άτομο που απαντάει στα θέματα πρέπει να χρησιμοποιήσει την γνώση του για το πληροφοριακό σύστημα που αξιολογεί. Μπορεί να επιλέξει την απάντηση ανάλογα με την κρίση του. Αυτός ο τρόπος ανταπόκρισης είναι αποδεκτός για να επιφέρει ένα ικανοποιητικό αποτέλεσμα στην αξιολόγηση ωριμότητας κυβερνοασφάλειας. Παράλληλα, όμως, εισάγει τον παράγοντα της υποκειμενικότητας. Επειδή η αξιολόγηση επιπέδου ωριμότητας είναι επαναληπτική διαδικασία, θα πρέπει με την ίδια κρίση να ανταποκριθεί και σε μελλοντικές αξιολογήσεις. Για να αντιμετωπιστεί αυτό μπορεί να χρησιμοποιηθεί ενισχυτικά ένας οδηγός ελεγκτικής [14] για τα CIS Controls, ο οποίος περιγράφει τα ακριβή βήματα έτσι ώστε να μπορεί να απαντηθεί εάν η κατάσταση υλοποίησης είναι: «έχει υλοποιηθεί πλήρως» ή όχι. Εφόσον δεν έχει υλοποιηθεί πλήρως, είναι σχετικά εύκολα να επιλεχθεί μια από τις απαντήσεις: «έχει υλοποιηθεί εν μέρει» ή «δεν έχει υλοποιηθεί».
Οι απαντήσεις που λαμβάνονται εκχωρούνται σε πρώτο στάδιο με τις ακόλουθες τιμές/αξίες :

| Απάντηση | Αξία/Συντελεστής |
|---|---|
| δεν έχει υλοποιηθεί | 0 |
| έχει υλοποιηθεί εν μέρει | 0,5 |
| έχει υλοποιηθεί πλήρως | 1 |

**Πίνακας 2 – Απαντήσεις και οι αντίστοιχοι συντέλεσες**

Όλες οι ερωτήσεις έχουν ως προεπιλογή το 0, δηλαδή η κατάσταση είναι «δεν έχει υλοποιηθεί == 0». Όταν απαντηθούνε και οι 18 ομάδες/ενότητες θεμάτων, η ομάδα ή το άτομο που αξιολογεί, συνεχίζει στην επόμενη σελίδα για να λάβει τα αποτελέσματα της αξιολόγησης επιπέδου ωριμότητας κυβερνοασφάλειας του οργανισμού σε μορφή δεικτών και στην συνέχεια τα προτεινόμενα αντίμετρα.

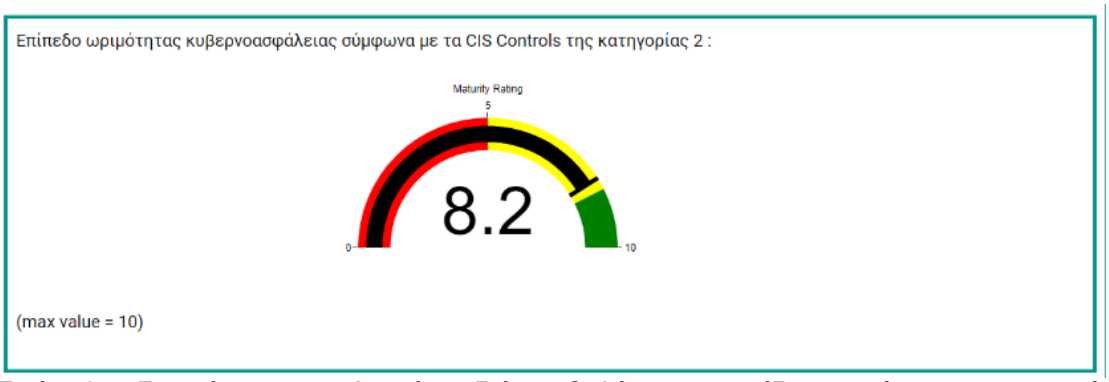
Επίσης να σημειωθεί ότι συνίσταται το ερωτηματολόγιο να συμπληρώνεται από περισσότερα άτομα, ιδανικά να αντιμετωπίζεται ως μια ομαδική διαδικασία οπού συμμετέχουν όλοι οι αρμόδιοι του πληροφοριακού συστήματος.

## 3.4 Αποτελέσματα Αξιολόγησης

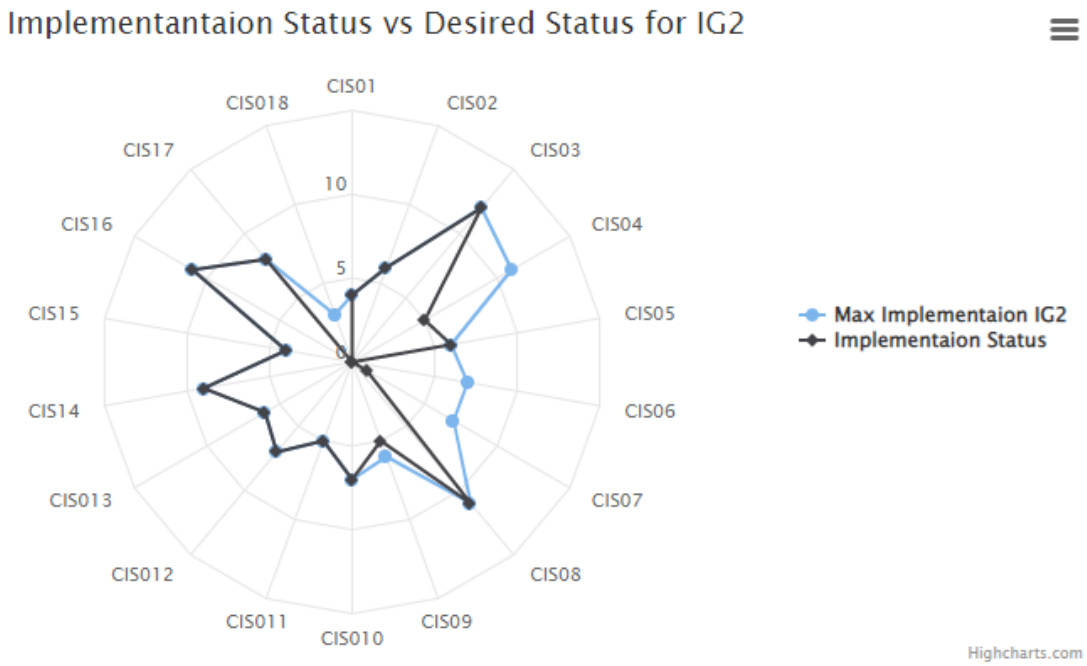
Μετά το πέρας της κύριας φάσης του ερωτηματολογίου επιστρέφονται στον χρήστη τα αποτελέσματα της αξιολόγησης σε μορφή δεικτών. Οι δείκτες υπολογίζονται με βάση τις συναρτήσεις αξιολόγησης που θα παρουσιαστούν στο κεφάλαιο 4. Τα αποτελέσματα αποτελούνται από 4 διαφορετικές προσεγγίσεις και είναι βασισμένες σε 4 διαφορετικές συναρτήσεις αξιολόγησης.

### 3.4.1 Προσέγγιση αξιολόγησης ωριμότητας κυβερνοασφάλειας με βάση τα CIS Controls

Ο δείκτης αξιολόγησης επιπέδου ωριμότητας κυβερνοασφάλειας για αυτή τη συνάρτηση αξιολόγησης αντιστοιχείται στην κλίμακα 1 έως 10. Ένα στιγμιότυπο ακολουθεί στην εικόνα 3.7, με τον δείκτη αξιολόγησης να παίρνει την τιμή '8,2'. Η συνάρτηση αξιολόγησης στην ενότητα 4.1.




**Εικόνα 3.7 - Στιγμιότυπο αποτελεσμάτων δείκτη αξιολόγησης επιπέδου ωριμότητας οργανισμού κατηγορίας υλοποίησης 2 με προσέγγιση βασισμένη στα CIS Controls**

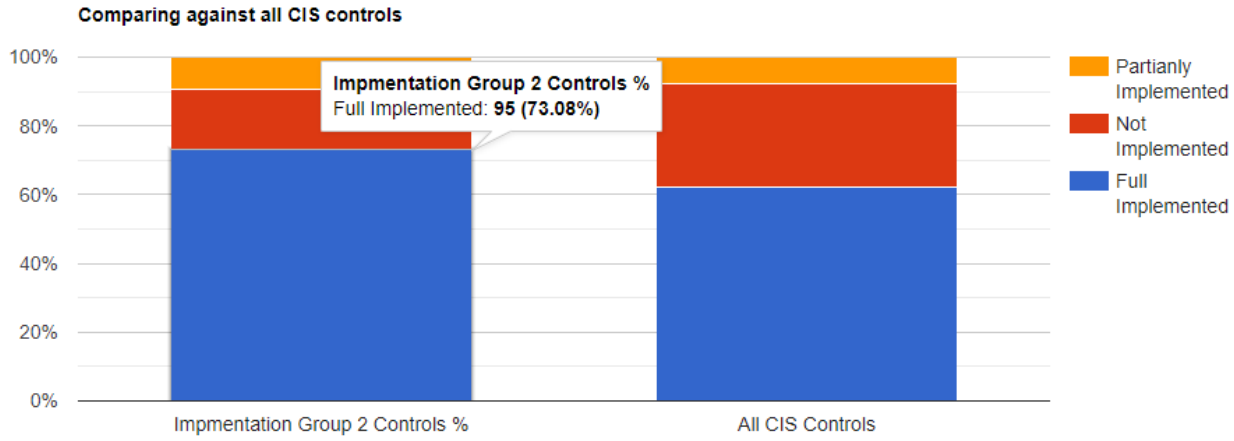



**Εικόνα 3.8 - Στιγμιότυπο αποτελεσμάτων σε γραφική παράσταση web chart οργανισμού κατηγορίας υλοποίησης 2**

Τα αποτελέσματα του ερωτηματολογίου δίνονται και σε μορφή web chart (εικόνα 3.8), παρέχοντας έτσι μια συνολική αποτύπωση που αποτελεί παράλληλα και περίληψη του ερωτηματολογίου.

Τα αποτελέσματα του ερωτηματολογίου δίνονται και σε απλή μορφή stacked chart (εικόνα 3.9) και συγκρίνονται με το σύνολο (IG3) των μέτρων προστασίας του πλαισίου CIS Controls. Στόχος είναι να

δώσει και μια συγκριτική εικόνα και να ληφθεί υπόψιν ότι υπάρχουν επιπρόσθετα μέτρα προστασίας όπως και μια επιπλέον συνοπτική εικόνα των αποτελεσμάτων του ερωτηματολογίου, αν και δεν ανήκουν στην συγκεκριμένη κατηγορία υλοποίησης. Στην γραφική παράσταση δίνονται τα αποτελέσματα σε ποσοστό % και επιστρέφει το πλήθος των μέτρων προστασίας που δεν είναι καθόλου υλοποιημένα, το πλήθος των μέτρων προστασίας που είναι ‘εν μέρει’ ή και ‘πλήρως’ υλοποιημένα. Η συγκεκριμένη προσέγγιση αποτελεί μια αξιολόγηση υψηλού επιπέδου που δίνει μια γενικότερη εικόνα την κατάστασης κυβερνοασφάλειας του οργανισμού και μπορεί να χρησιμοποιηθεί και ως αξιολόγηση συμμόρφωσης στο πλαίσιο των CIS Controls.



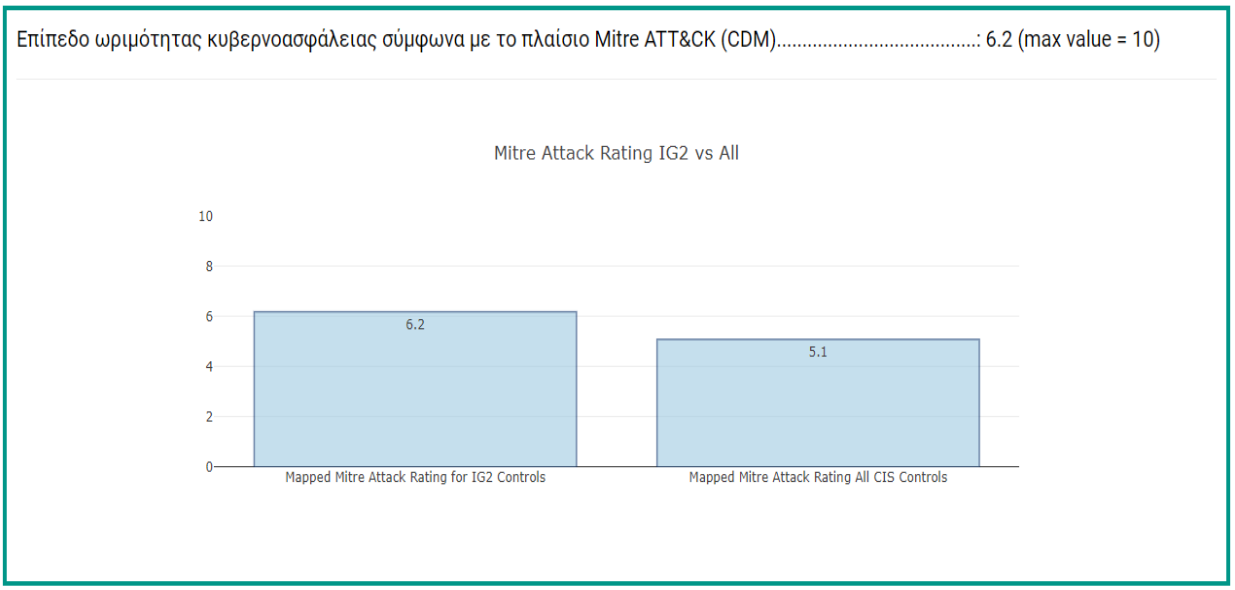

**Εικόνα 3.9 - Στιγμιότυπο αποτελεσμάτων σε γραφική παράσταση stacked chart κατηγορίας 2**

### 3.4.2 Προσέγγιση αξιολόγησης επιπέδου ωριμότητας κυβερνοασφάλειας με βάση το CIS Community Defense Model – CDM Master Mapping/Security Function Based

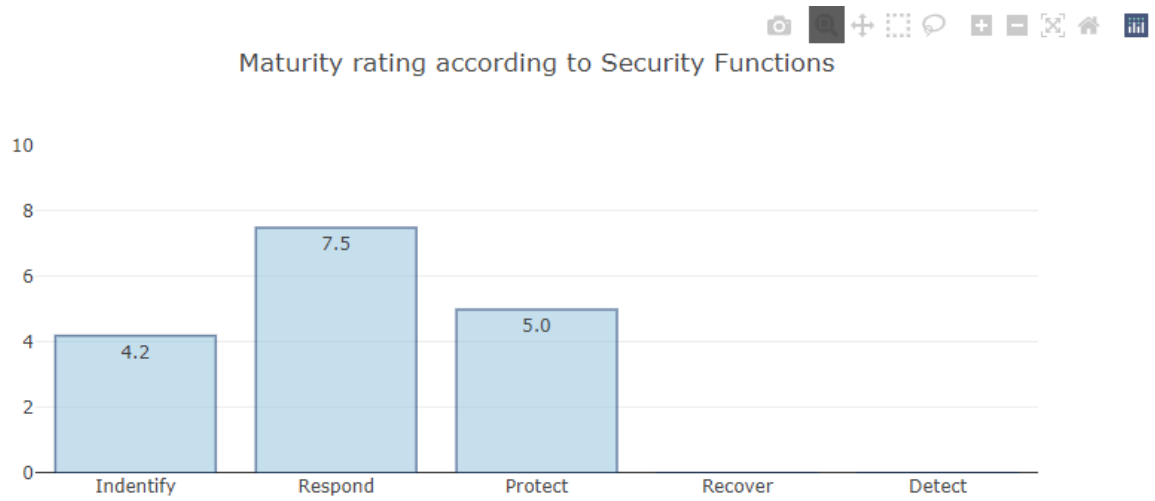
Ο δείκτης επιπέδου ωριμότητας κυβερνοασφάλειας για αυτή τη συνάρτηση αξιολόγησης αντιστοιχείται στην κλίμακα 1 έως 10. Ένα στιγμιότυπο ακολουθεί στην εικόνα 3.10, με τον δείκτη αξιολόγησης να παίρνει την τιμή ‘6,2’ για την κατηγορία υλοποίησης για την οποία αξιολογείται. Επίσης ο δείκτης αξιολόγησης επιστρέφεται και σε μορφή stacked chart ώστε να γίνει μια αντιπαράθεση με τα μέτρα ασφάλειας ενός οργανισμού της κατηγορίας υλοποίησης 3. Η συνάρτηση αξιολόγησης στην ενότητα 4.2.

### 3.4.3 Αξιολόγηση επιπέδου ωριμότητας κυβερνοασφάλειας με βάση τα Key Functions Προσέγγιση NIST

Επιστρέφεται μια γραφική παράσταση (Εικόνα 3.11) που δείχνει τον καταμερισμό των μέτρων ασφάλειας ανά security function κατά NIST. Η συνάρτηση αξιολόγησης στην ενότητα 4.3.




**Εικόνα 3.10 – Στιγμιότυπο δείκτη αξιολόγησης CDM Master Mapping/Security Function Based**




**Εικόνα 3.11 – Stacked Chart με τα αποτελέσματα της συναρτήσεις που βασίζεται στα NIST Security Functions**

### 3.4.4 Προσέγγιση αξιολόγησης βασισμένη στο CIS Community Defense Model για τις 5 πιο σημαντικές απειλές – CDM Reverse Mapping/Security Value Based

Το επίπεδο ωριμότητας του οργανισμού αξιολογείται ενάντια τις 5 πιο σημαντικές απειλές του έτους 2021. Η συνάρτηση αξιολόγησης παρουσιάζεται στην ενότητα 4.4.

## Top 5 Attacks Maturity Rating according to MitreAtt&ck mapping

max value = 10

Επίπεδο ωριμότητας ενάντια σε κακόβουλου λογισμικού για τα αντίμετρα τις κατηγορίας 2.....: 5.9
Επίπεδο ωριμότητας ενάντια σε κακόβουλου λογισμικού για σύνολο των CIS Controls.....: 4.9

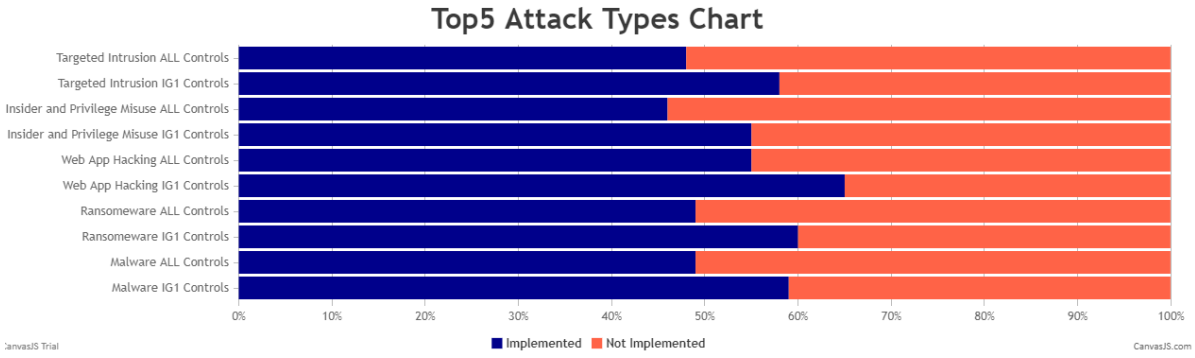
Επίπεδο ωριμότητας ενάντια σε ransomeware για τα αντίμετρα τις κατηγορίας 2.....: 6
Επίπεδο ωριμότητας ενάντια σε ransomeware για σύνολο των CIS Controls.....: 4.9

Επίπεδο ωριμότητας ενάντια σε Web Application Hacking για τα αντίμετρα τις κατηγορίας 2.....: 6.5
Επίπεδο ωριμότητας ενάντια σε Web Application Hacking για σύνολο των CIS Controls.....: 5.5

Επίπεδο ωριμότητας ενάντια σε insider and priviledge missue για τα αντίμετρα τις κατηγορίας 2.....: 5.5
Επίπεδο ωριμότητας ενάντια σε insider and priviledge missue general για σύνολο των CIS Controls.....: 4.6

Επίπεδο ωριμότητας ενάντια σε στοχοποιημένη εισβολή/επίθεση από APT για τα αντίμετρα τις κατηγορίας 2...: 5.8
>Επίπεδο ωριμότητας ενάντια σε στοχοποιημένη εισβολή/επίθεση από APT για για σύνολο των CIS Controls.....: 4.8

**Εικόνα 3.12 - Παράδειγμα δεικτών αξιολόγησης ενός οργανισμού της κατηγορίας υλοποίησης 2, στην κλίμακα 1 έως 10. Αξιολογείται και έναντι των μέτρων ασφαλείας της κατηγορίας υλοποίησης 3, έτσι ώστε να φανεί η διαφορά επιπέδου έναντι όλων των μέτρων ασφαλείας CIS.**



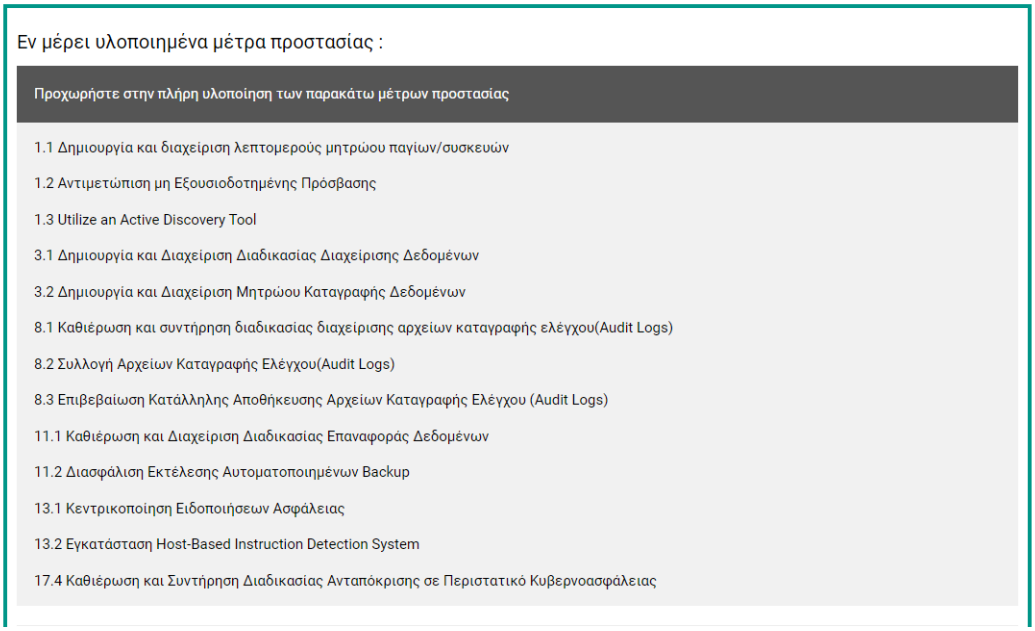

**Εικόνα 3.13 – Αποτελέσματα επιστέφονται και σε μορφή παράστασης %**

## 3.5 Συστάσεις Κυβερνοασφάλειας

Οι συστάσεις κυβερνοασφάλειας αποτελούν και την τελευταία φάση της εφαρμογής. Οι συστάσεις επιστρέφονται στο χρήστη που συμπληρώνει το ερωτηματολόγιο, υλοποιείται με “Rule-Based” μηχανισμό, ο οποίος βασίζεται πλήρως στα αποτελέσματα του ερωτηματολογίου, που παίρνουν τις τιμές του πίνακα2.

Όλες οι απαντήσεις «Εν μέρει υλοποιημένα» στο ερωτηματολόγιο συλλέγονται και επιστρέφονται σε μια λίστα με την απλή σύσταση να προχωρήσουν προς την πλήρη υλοποίηση αυτών των μέτρων, όπως φαίνεται στον στιγμιότυπο της εικόνας 3.14.

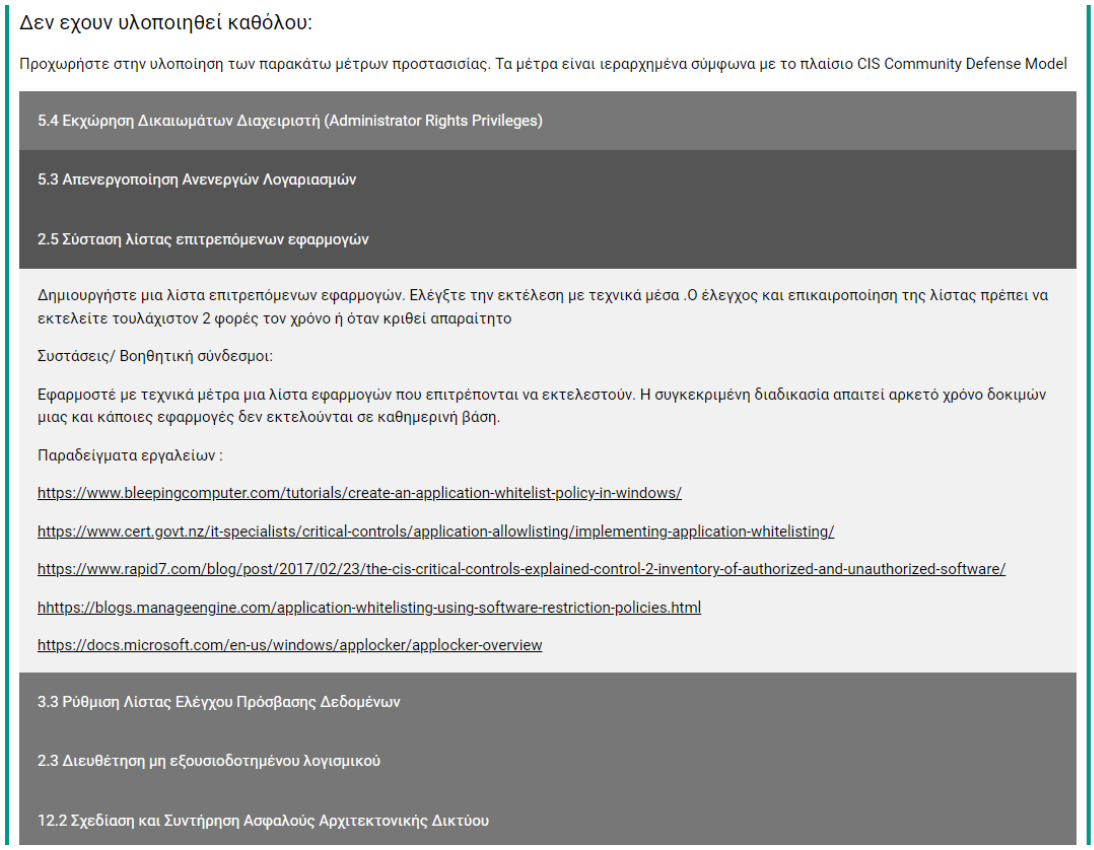
Ακολουθήστε τις παρακάτω συστάσεις:




**Εικόνα 3.14 - Εν μέρη υλοποιημένα μέτρα ασφαλείας - Ο εξεταζόμενος καλείτε να προχωρήσει στην πλήρης υλοποίηση τους**

Όλες οι ερωτήσεις που έχουν απαντηθεί με : «δεν έχει υλοποιηθεί», συλλέγονται σε μια ιεραρχημένη λίστα βάση της έρευνας CIS CDM. Οι υπεύθυνοι του οργανισμού μπορούν να ακολουθήσουν τις συστάσεις για κάθε μέτρο προστασίας το οποίο δεν έχει υλοποιηθεί. Οι συστάσεις αποτελούνται από συντόμους οδηγούς, παραπομπές σε οδηγούς, επιστημονικά άρθρα και άρθρα των κατασκευαστών λογισμικού που συστήνονται.

Όλες οι συστάσεις βρίσκονται στο παράρτημα Δ’ και είναι αποτέλεσμα έρευνας στο παγκόσμιο διαδίκτυο. Ακολουθούν κάποιες συστάσεις που χρησιμοποιηθήκαν στην εφαρμογή ’Cyber Defense Assessment Tool’.




**Εικόνα 3.15 - Καθόλου υλοποιημένα μέτρα ασφαλείας - Ο εξεταζόμενος καλείτε να προχωρήσει στην υλοποίηση τους ακολουθώντας τις σχετικές συστάσεις**

### 3.5.1 Σύσταση μέτρου ασφάλειας CIS CSC 4.1

Δημιουργήστε και συντηρήστε μια διαδικασία ασφαλούς διαμόρφωσης εξοπλισμού πληροφορικής και εφαρμογών. Να επικαιροποιείτε και να ενημερώνετε τη διαδικασία σε ετήσια βάση ή όταν αυτό κριθεί απαραίτητο.

Συστάσεις/ Βοηθητικοί σύνδεσμοι: Αποτελεί ένα από τα πιο σημαντικά μέτρα των πρακτικών του CIS CSC, δώστε ιδιαίτερη προσοχή σε αυτό το μέτρο. Η διαδικασία ασφαλούς διαμόρφωσης περιλαμβάνει την προσαρμογή των προεπιλεγμένων ρυθμίσεων ενός συστήματος/εφαρμογής/συσκευής προκειμένου να αυξηθεί η ασφάλεια και να μετριαστεί ο κίνδυνος. Η διαδικασία εντοπίζει εσφαλμένες ρυθμίσεις παραμέτρων των προεπιλεγμένων ρυθμίσεων ενός συστήματος
Καθορίστε μέσω της διαδικασίας τα εξής σημεία τουλάχιστον:

- Δημιουργία και συντήρηση διαδικασίας ασφαλούς ρύθμισης δικτυακής υποδομής
- Ρύθμιση αυτομάτου κλειδώματος επιφάνειας εργασίας
- Υλοποίηση και ρύθμιση Firewall σε συστήματα (servers)
- Υλοποίηση και ρύθμιση Firewall στους σταθμούς εργασίας (PC, Desktop, Laptop)
- Ασφαλής Διαχείριση Εξοπλισμού και Εφαρμογών
- Διαχείριση προεγκατεστημένων λογαριασμών σε Συσκευές και Εφαρμογές
- Το προσωπικό που θα φέρει την ευθύνη για την ασφαλή διαμόρφωση καθώς και τα χρονικά διαστήματα που πρέπει να εκτελείται, σε κρίσιμα και λιγότερο κρίσιμα συστήματα και εφαρμογές.

Ανατρέξτε στα σημεία αναφοράς (benchmarks) σύμφωνα με τον κατασκευαστή/διανομέα ή και σύμφωνα με έναν αναγνωρισμένο οργανισμό/πρότυπο κυβερνοασφάλειας όπως είναι το CIS, SANS, NIST, ISO27001, BSI κ.α. Το CIS συγκεκριμένα προσφέρει τέτοια benchmarks για ένα πλήθος συσκευών και εφαρμογών:
https://www.cisecurity.org/cybersecurity-tools/ [15]
https://www.cisecurity.org/cis-benchmarks/ [16]
Σύμφωνα με τα σημεία αναφοράς, δημιουργήστε checklists για κάθε ομάδα συσκευών/εφαρμογών. Προχωρήστε στην διαμόρφωση και επανελέγξετε εάν αυτή εκτελέστηκε σύμφωνα με τις οδηγίες του κατασκευαστή.
Άλλο βοηθητικό υλικό:
https://www.microsoft.com/en-us/download/details.aspx?id=55319 [17]
https://www.calcomsoftware.com/cis-hardening-and-configuration-security-guide/#secure [18]
https://www.itgovernance.co.uk/secure-configuration [19]
https://www.hysolate.com/blog/system-hardening-guidelines-best-practices/ [20]
https://kirkpatrickprice.com/blog/industry-accepted-hardening-standards/ [21]
https://security.utexas.edu/os-hardening-checklist [22]
https://www.securitymetrics.com/blog/system-hardening-standards-how-comply-pci-requirement-22 [23]

### 3.5.2 Σύσταση μέτρου ασφάλειας CIS CSC 13.3

Εγκαταστήστε Network Instruction Detection System στο δίκτυο του οργανισμού.

Συστάσεις/ Βοηθητικοί σύνδεσμοι:
Ένα Network IDS (NIDS) χρησιμοποιείται για την παρακολούθηση και ανάλυση της κυκλοφορίας του δικτύου και για την προστασία ενός ή περσότερων συστημάτων από απειλές του εξωτερικού δικτύου.
Ένα NIDS διαβάζει όλα τα εισερχόμενα πακέτα και αναζητά τυχόν ύποπτα μοτίβα. Όταν εντοπίζονται απειλές, με βάση τη σοβαρότητά τους, το σύστημα μπορεί να λάβει μέτρα όπως να ειδοποιήσει τους διαχειριστές ή να εμποδίσει την πρόσβαση της διεύθυνσης IP προέλευσης στο δίκτυο.
https://www.comodo.com/siem/network-ids.php [24]
Ενδεικτικά κάποια εργαλεία :
https://suricata.io/ [25]
https://www.snort.org/ [26]
https://www.splunk.com/ [27]
https://securityonionsolutions.com/ [28]
https://www.paloaltonetworks.com/cyberpedia/what-is-an-intrusion-detection-system-ids [29]

### 3.5.3 Σύσταση μέτρου ασφάλειας CIS CSC 3.10

Κρυπτογράφηση ευαίσθητων δεδομένων κατά τη μεταφορά τους μέσω δικτύου.
Για παράδειγμα με χρήση: TLS, OpenSSH

Συστάσεις/ Βοηθητικοί σύνδεσμοι:
Η ασφαλής αποστολή πληροφοριών μέσω του διαδικτύου αποτελεί θεμελιώδη αρχή για το ηλεκτρονικό εμπόριο, την ιατρική και άλλες ευαίσθητες συναλλαγές. Για αυτές και πολλές ακόμα χρήσεις, θεωρείται κρίσιμο ζήτημα οι μεταδιδόμενες πληροφορίες να μην παραβιάζονται, αλλά και να μη διαβάζονται από οποιονδήποτε άλλον εκτός από τον αποστολέα και τον παραλήπτη. Τα χαρακτηριστικά αυτά αποτελούν βασικό κομμάτι της ανάπτυξης του διαδικτύου και είναι εξαιρετικά κρίσιμα για πολλές καινοτόμες χρήσεις. Αν και η προέλευση της ευρύτατα χρησιμοποιούμενης τεχνολογίας που παρέχει ασφάλεια επιπέδου στις μεταφορές δεδομένων μέσω διαδικτύου εντοπίζεται εδώ και 20 χρόνια στο SSL, η

τελευταία ολοκληρωμένη έκδοση TLS 1.3 είναι μια σημαντική αναθεώρηση που σχεδιάστηκε για το σύγχρονο Internet. Το πρωτόκολλο αυτό φέρνει σημαντικές βελτιώσεις στους τομείς της ασφάλειας, των επιδόσεων και της ιδιωτικότητας. [30]

https://security.berkeley.edu/data-encryption-transit-guideline [31]
https://www.internetsociety.org/deploy360/tls/basics/ [32] [32]
https://docs.microsoft.com/ enable-tls-1-2-server [33]
https://www.sslmarket.com/ssl/help-ssl-certificate-installation [34]
https://www.openssl.org/ [35]
https://developer.visa.com/pages/trusted_certifying_authorities [36]

### 3.5.4 Σύσταση μέτρου ασφάλειας CIS CSC 10.5

Ενεργοποιήστε δυνατότητες anti-exploitation σε λογισμικό και συσκευές του οργανισμού όπως: Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), Apple® System Integrity Protection (SIP) and Gatekeeper

Συστάσεις/ Βοηθητικοί σύνδεσμοι:
Η εφαρμογή αυτού του λογισμικού είναι πολύ σημαντική για την άμυνα του οργανισμού, αλλά δεν χρησιμοποιείται πάντα στο μέγιστο των δυνατοτήτων του. Βεβαιωθείτε ότι το λογισμικό που μπορεί να αποτρέψει ή να μειώσει τις επιθέσεις στα συστήματά σας χρησιμοποιείται όποτε είναι δυνατόν.
https://cybersecurity.yale.edu/mss/5/1/2 [37]
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/enable-exploit-protection?view=o365-worldwide [38]
https://scadahacker.com/library/Documents/Best_Practices/NSA%20-%20IA%20-%20AntExploitation.pdf [39]
https://docs.microsoft.com/en-us/enable-exploit-protection [40]

### 3.5.5 Σύσταση μέτρου ασφάλειας CIS CSC 13.1

Συγκεντρώστε κεντρικά τις ειδοποιήσεις συμβάντων ασφαλείας όλων των συσκευών του οργανισμού για την καλύτερη συσχέτιση και ανάλυση αυτών. Η καλύτερη πρακτική διαχείρισης είναι μέσω ενός SIEM (Security Information and Event Management system). Επίσης, μία πλατφόρμα ανάλυσης αρχείων καταγραφής συμβάντων ασφάλειας ικανοποιεί το συγκεκριμένο μέτρο.

Συστάσεις/ Βοηθητικοί σύνδεσμοι:
Το SIEM παρέχει στους οργανισμούς δυνατότητες εντοπισμού, ανάλυσης και ανταπόκρισης. Το λογισμικό SIEM συνδυάζει τη διαχείριση πληροφοριών ασφαλείας (SIM) και τη διαχείριση συμβάντων ασφαλείας (SEM) για την ανάλυση των ειδοποιήσεων ασφαλείας που παράγονται από εφαρμογές και συσκευές του δικτύου σε πραγματικό χρόνο . Το λογισμικό SIEM αντιστοιχεί συμβάντα με κανόνες και μηχανές ανάλυσης και τα απαριθμεί για δευτερεύουσα αναζήτηση για να ανιχνεύσει και να αναλύσει προηγμένες απειλές χρησιμοποιώντας παγκόσμια συλλογή πληροφοριών. Αυτό δίνει στις ομάδες ασφαλείας πληροφορίες και ιστορικό των δραστηριοτήτων στο IT περιβάλλον του οργανισμού παρέχοντας ανάλυση δεδομένων, συσχέτιση συμβάντων, συγκέντρωση, αναφορά και διαχείριση αρχείων καταγραφής.
Ενδεικτικά κάποια εργαλεία :
https://www.softwaretestinghelp.com/siem-tools [41]
https://www.manageengine.com/products/eventlog [42]

# Κεφάλαιο 4: Συναρτήσεις Αξιολόγησης Ωριμότητας Κυβερνοασφάλειας

Τα αποτελέσματα της αξιολόγησης υπολογίζονται σε μορφή δεικτών από τέσσερις διαφορετικές συναρτήσεις. Κάθε τέτοιος δείκτης είναι αυτοτελής και μπορεί από μονός του να σταθεί ως αποτέλεσμα της αξιολόγησης, ωστόσο συνίσταται να ληφθούν υπόψιν όλοι οι δείκτες αξιολόγησης. Κάθε δείκτης έχει διαφορετική ή μερικώς διαφορετική προσέγγιση στην αξιολόγηση επιπέδου ωριμότητας κυβερνοασφάλειας.

- Αξιολόγηση με βάση τα CIS Critical Security Controls – “Επίπεδο ωριμότητας κυβερνοασφάλειας σύμφωνα με τα CIS Controls”
- Αξιολόγησης με βάση το CIS Community Defense Model – CDM Master Mapping/Security Function Based –“Επίπεδο ωριμότητας κυβερνοασφάλειας σύμφωνα με το πλαίσιο MITRE ATT&CK (CDM)”
- Αξιολόγηση με βάση τα Key Functions προσέγγιση NIST CSF– “NIST Key Functions”
- Προσέγγιση αξιολόγησης βασισμένη στο CIS Community Defense Model για τις 5 πιο σημαντικές απειλές – Security Value bases/Reverse Mapping - “Top5 Threats”

## 4.1 Συνάρτηση Αξιολόγησης Επιπέδου Ωριμότητας Κυβερνοασφάλειας με Βάση το CIS Community Defense Model – CDM Master Mapping/Security Function Based

Ο συγκεκριμένος δείκτης αξιολόγησης είναι πλήρως βασισμένος στο πλαίσιο των CIS Controls. Όλα τα μέτρα προστασίας έχουν το ίδιο βάρος για αυτή την προσέγγιση. Χρησιμοποιείται απλή αναλογική για να προκύψει ο δείκτης επιπέδου ωριμότητας. Το αποτέλεσμα κάθε μέτρου προστασίας μπορούν να πάρουν τις τιμές 0, 0.5 ,1 όπως έχει δηλωθεί στον πίνακα 2 και για την συγκεκριμένη προσέγγιση αποτελούν τους συντελεστές κάθε μέτρου προστασίας.

Ο δείκτης αποτελείται από τον λόγο του αθροίσματος όλων των απαντήσεων ως προς το άθροισμα των μέτρων προστασίας της κατηγορίας υλοποίησης. Το άθροισμα των απαντήσεων υπολογίζεται από την τιμή/αξία κάθε απάντησης, όπως προκύπτει από τον παρακάτω τύπο:

$\text{SurveyResult} = \sum (Result\ IG_x 1.1\alpha + Result\ IG_x 1.2\alpha + \cdots + Result\ IG_x N\alpha)$

N = τελευταίο CIS μέτρο προστασίας
α = δείκτης (0|0,5|1)
x= IG1 | IG2 | IG3
maxIG1 Survey Result = 56
max IG2 Survey Result = 130
max IG3 Survey Result = 153

| Rating = SurveyResult * 10 / $max\ IG_x$ Survey Result |
|---|

Στις εικόνες 3.7, 3,8 και 3.9 παρουσιάζεται ο δείκτης ωριμότητας κυβερνοασφάλειας στην εφαρμογή για την συγκεκριμένη συνάρτηση αξιολόγησης.

## 4.2 Προσέγγιση Αξιολόγησης Επιπέδου Ωριμότητας Κυβερνοασφάλειας με Βάση το CIS Community Defense Model – CDM Master Mapping/Security Function Based

Αυτή η προσέγγιση βασίζεται στην μελέτη CIS Community Defense Model. Κάθε μέτρο προστασίας των CIS Controls αντιστοιχείται σε τεχνικές (Techniques/Sub-Techniques) και αντίμετρα(Mitigations) του πίνακα MITRE Attack. Με αυτή την προσέγγισή τα CIS Controls αποκτούν μια διαφορετική αξία το καθένα, γεγονός το οποίο συνεπάγεται την δυνατότητα ιεράρχησης των μέτρων προστασίας όπως είδαμε στην ενότητα 3.5. Η αξία κάθε μέτρου προστασίας (safeguard) των CIS Controls είναι αποτέλεσμα του αθροίσματος των τεχνικών MITRE Attack που μετριάζει.

Η μεθοδολογία του CIS CDM που χρησιμοποιήθηκε για την αντιστοίχιση αναφέρεται στην ενότητα 2.3. Τα αναλυτικά αποτέλεσμα αυτής της μελέτης περιέχονται στο master mapping, για όλα τα μέτρα προστασίας των CIS Controls (reference βιβλιογραφία CIS Controls v8 to Enterprise ATT&CK v8.2 Master Mapping - 5.26.2021.xlsx). Στο παράρτημα Β' βρίσκονται όλες οι αξίες(Security Function - Master Maping ) των CIS μέτρων προστασίας σε μορφή περίληψης.

$$\text{SurveyResult} \sum \left(Result\ IG_x 1.1\alpha\ V_{1.1} + Result\ IG_x 1.2\alpha\ V_{1.2} + \cdots + Result\ IG_x N\alpha\ V_N\right)$$

N = τελευταίο CIS μέτρο προστασίας
α = δείκτης (0|0,5|1)
$V_y$ = αξία (y = μέτρο προστασίας)
x= IG1 | IG2 | IG3
maxIG1 Value = 2056
max IG2 Survey Result = 3011
max IG3 Survey Result = 3630
Rating = SurveyResult * 10 / $max\ IG_x$ Value

Όπως απεικονίζεται στον πίνακα 3 το μέτρο προστασίας CIS 5.2 που παίρνουμε ως παράδειγμα έχει αξία 47, το οποίο προκύπτει από το άθροισμα των τεχνικών MITRE Attack που μετριάζει. Στον ίδιο πίνακα αναφέρονται οι τεχνικές (T) και τα αντιμέτρα (M) MITRE Attack.

Το αποτέλεσμα ενός μέτρου προστασίας/ερώτησης που μπορεί να πάρει τις τιμές που απεικονίζεται στον πίνακα 2 πολλαπλασιάζεται με την αξία του. Όλα τα αποτελέσματα αθροίζονται με βάση αυτή την λογική. Ο δείκτης επιπέδου ωριμότητας κυβερνοασφάλειας σε αυτή τη προσέγγιση είναι το αποτέλεσμα αυτού του αθροίσματος προς την μέγιστη τιμή που μπορεί να πάρει ανά κατηγορία υλοποίησης, η οποία περιλαμβάνει όλα τα μέτρα προστασίας του πλαισίου CIS, και είναι συνολικά 3.630 για την κατηγορία 3. Στην συνέχεια, το αποτέλεσμα αντιστοιχείται στην κλίμακα 1 έως 10.

Ένα αφηρημένο παράδειγμα για να γίνει κατανοητή η μεθοδολογία αξιολόγησης:

Έστω ένα πλαίσιο με 5 μέτρα προστασίας.
Μετρο1 ένα μετριάζει 23 τεχνικές MITRE Attack
Μετρο2 ένα μετριάζει 13 τεχνικές MITRE Attack
Μετρο3 ένα μετριάζει 13 τεχνικές MITRE Attack
Μετρο4 ένα μετριάζει 8 τεχνικές MITRE Attack
Μετρο5 ένα μετριάζει 2 τεχνικές MITRE Attack
Σύνολο 59 τεχνικές που αποτελεί και την μέγιστη τιμή που μπορεί να πάρει η αξιολόγηση αυτού του

παραδείγματος. Έστω ότι τα αποτελέσματα του ερωτηματολογίου είναι :
Μετρο1 = πλήρως υλοποιημένο -> 1
Μετρο2 = εν μέρη υλοποιημένο -> 0,5
Μετρο3 = καθόλου υλοποιημένο -> 0
Μετρο4 = πλήρως υλοποιημένο -> 1
Μετρο5 = πλήρως υλοποιημένο -> 1
Αποτέλεσμα αξιολόγησης επιπέδου ωριμότητας :
1*23 + 0,5*13 + 0*13 + 1*8 + 1*2 = 39.5
Δείκτης επιπέδου ωριμότητας στην κλίματα του max.10:
39*10 / 59 = 6,69

Στην εικόνα 3.10 παρουσιάζεται το αποτέλεσμα του δείκτη ωριμότητας στην εφαρμογή για την συγκεκριμένη συνάρτησης αξιολόγησης.

## 4.3 Συνάρτηση Αξιολόγησης Επιπέδου Ωριμότητας Κυβερνοασφάλειας με Βάση τα key Functions Προσέγγιση NIST

Σκοπός αυτής της αξιολόγησης είναι να αναδείξει το επίπεδο ωριμότητας σχετικά με τα “Key Functions” όπως αυτά ορίζονται στο NIST CSF και να δώσει μια γενικότερη εικόνα κατανομής των μέτρων προστασίας. Κάθε CIS μετρό προστασίας έχει ως χαρακτηριστικό την κατηγοριοποίηση σε ‘Key Function’ το οποίο αποτελεί τον βασικό πυλώνα του πλαισίου κυβερνοασφάλειας NIST.

Αναπτύχθηκε μια συνάρτηση αξιολόγησης επιπέδου ωριμότητας με βάση αυτά τα 5 χαρακτηριστικά κλειδιά:
Identify, Protect, Detect, Respond, Recover. Ως μεθοδολογία χρησιμοποιήθηκε η απλή αναλογική. Υπολογίζεται ξεχωριστό άθροισμα για κάθε Key Function. Το άθροισμα προκύπτει από την απάντηση του κάθε μέτρου προστασίας και μπορεί να πάρει τις τιμές 0, 0.5 και 1. Στην συνέχεια αθροίστηκαν οι απαντήσεις, διαιρεθήκαν με το μέγιστο score και αναπροσαρμοστήκαν στην κλίμακα 1 έως 10.

Στον πίνακα 4 απεικονίζονται τα ‘Key Functions’ για κάθε CIS CSC safeguard και κάθε Implementation Group.

Στην εικόνα 3.11 παρουσιάζεται το αποτέλεσμα του δείκτη ωριμότητας στην εφαρμογή για την συγκεκριμένη συνάρτησης αξιολόγησης.

| CIS Contol | ATT&CK V8.2 Enterprise Mitigation ID | ATT&CK Technique ID | ATT&CK Sub-Technique ID |
|---|---|---|---|
| 5.2 | M1026 | T1546 | 0.003 |
| 5.2 | M1026 | T1556 | 0.004 |
| 5.2 | M1026 | T1601 | |
| 5.2 | M1026 | T1601 | 0.001 |
| 5.2 | M1026 | T1601 | 0.002 |
| 5.2 | M1026 | T1599 | |
| 5.2 | M1026 | T1599 | 0.001 |
| 5.2 | M1026 | T1550 | |
| 5.2 | M1026 | T1550 | 0.002 |
| 5.2 | M1026 | T1078 | 0.002 |
| 5.2 | M1026 | T1047 | |
| 5.2 | M1027 | T1110 | |
| 5.2 | M1027 | T1110 | 0.001 |
| 5.2 | M1027 | T1110 | 0.002 |
| 5.2 | M1027 | T1110 | 0.003 |
| 5.2 | M1027 | T1110 | 0.004 |
| 5.2 | M1027 | T1555 | |
| 5.2 | M1027 | T1555 | 0.001 |
| 5.2 | M1027 | T1187 | |
| 5.2 | M1027 | T1601 | |
| 5.2 | M1027 | T1601 | 0.001 |
| 5.2 | M1027 | T1601 | 0.002 |
| 5.2 | M1027 | T1599 | |
| 5.2 | M1027 | T1599 | 0.001 |
| 5.2 | M1027 | T1003 | |
| 5.2 | M1027 | T1003 | 0.006 |
| 5.2 | M1027 | T1003 | 0.001 |
| 5.2 | M1027 | T1003 | 0.002 |
| 5.2 | M1027 | T1003 | 0.007 |
| 5.2 | M1027 | T1003 | 0.008 |
| 5.2 | M1027 | T1003 | 0.005 |
| 5.2 | M1027 | T1003 | 0.004 |
| 5.2 | M1027 | T1003 | 0.003 |
| 5.2 | M1027 | T1563 | 0.001 |
| 5.2 | M1027 | T1021 | 0.002 |
| 5.2 | M1027 | T1072 | |
| 5.2 | M1027 | T1558 | |
| 5.2 | M1027 | T1558 | 0.002 |
| 5.2 | M1027 | T1558 | 0.003 |
| 5.2 | M1027 | T1558 | 0.004 |
| 5.2 | M1027 | T1552 | |
| 5.2 | M1027 | T1552 | 0.004 |
| 5.2 | M1027 | T1550 | 0.003 |
| 5.2 | M1027 | T1078 | |
| 5.2 | M1027 | T1078 | 0.003 |
| 5.2 | M1027 | T1078 | 0.004 |
| 5.2 | M1027 | T1078 | 0.001 |

**Πίνακας 3 - Αντιστοίχιση μέτρου προστασίας 5.2 σε Τεχνικές MITRE Attack**

| Contros\ Safeguards | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | Inde | Resp | Dete | Inder | Detect | | | | | | | | | |
| 2 | Inde | Inder | Resp | Dete | Prote | Prot | Protect | | | | | | | |
| 3 | Inde | Inder | Prote | Prote | Prote | Prot | Inde | Inde | Prot | Prote | Pro | Prote | Prote | Dete |
| 4 | Prote | Prote | Prote | Prote | Prote | Prot | Prot | Prot | Prot | Resp | Pro | Protect | | |
| 5 | Inde | Prote | Resp | Prote | Inder | Protect | | | | | | | | |
| 6 | Prote | Prote | Prote | Prote | Prote | Inde | Prot | Protect | | | | | | |
| 7 | Prote | Resp | Prote | Prote | Inder | Inde | Respond | | | | | | | |
| 8 | Prote | Dete | Prote | Prote | Dete | Dete | Dete | Dete | Dete | Prote | Det | Detect | | |
| 9 | Prote | Prote | Prote | Prote | Prote | Prot | Protect | | | | | | | |
| 10 | Prote | Prote | Prote | Dete | Prote | Prot | Detect | | | | | | | |
| 11 | Reco | Reco | Prote | Reco | Recover | | | | | | | | | |
| 12 | Prote | Prote | Prote | Inder | Prote | Prot | Prot | Protect | | | | | | |
| 13 | Dete | Dete | Dete | Prote | Prote | Dete | Prot | Prot | Prot | Prote | Detect | | | |
| 14 | Prote | Prote | Prote | Prote | Prote | Prot | Prot | Prot | Protect | | | | | |
| 15 | Inde | Inder | Inde | Prote | Inder | Dete | Protect | | | | | | | |
| 16 | Prote | Prote | Prote | Prote | Prote | Prot | Prot | Prot | Prot | Prote | Pro | Prote | Prote | Prote |
| 17 | Resp | Resp | Resp | Resp | Resp | Resp | Reco | Reco | Recover | | | | | |
| 18 | Inde | Inder | Prote | Prote | Indentify | | | | | | | | | |
| | IG1 | IG2 | IG3 | | | | | | | | | | | |
| | | | | | | | | | | | | | | |

**Πίνακας 4 - Πίνακας 3.2 - Οι τιμές των Key Functions για κάθε CIS Controls Safeguard**

## 4.4 Συνάρτηση Αξιολόγησης Βασισμένη στο CIS Community Defense Model για τις 5 πιο Σημαντικές Απειλές του 2021 – CDM Reverse Mapping/Security Value Based

Η συγκεκριμένη συνάρτηση έρχεται να αξιολογήσει την ωριμότητα του οργανισμού έναντι των 5 πιο σημαντικών απειλών του 2021. Βασίζεται στην Reverse Mapping της ερευνάς του CIS CDM.

Οι εξεταζόμενες απειλές:

| Απειλή | Τεχνικές MitreAtt&ck |
|---|---|
| Malware | 1191 |
| Ransomware | 1480 |
| Web Application Hacking | 923 |
| Insider Privilege and Misuse | 895 |
| Targeted Intrusions | 1259 |

**Πίνακας 5**

Κάθε απειλή/επίθεση μεταφράστηκε σε “attack patterns” μέσω του πίνακα MITRE Attack. Τα “attack patterns” μας έδωσαν τις τεχνικές και υπό-τεχνικές οι οποίες χρησιμοποιήθηκαν για να εκδηλωθούν αυτές οι απειλές/επιθέσεις. Με την σειρά τους αυτές αντιστοιχήθηκαν μέσω των MITRE
Attack Mitigations σε μετρά προστασίας των CIS Controls (CIS CSC safeguards). Οι μετρήσεις ελήφθησαν (περιληπτικά στο Παράτημα Γ’) από το reverse mapping της έρευνας CIS CDM όπου κάθε μέτρο προστασίας αξιολογήθηκε κατά πόσο είναι ικανό να μετριάσει μια ή περισσότερες από τις 5 απειλές/επιθέσεις.

| CIS Safeguards ALL IG | Malware | Ransome ware | Web App Hacking | Insider and Privilege Misuse | Targeted Intrusion |
|---|---|---|---|---|---|
| 3.12 | 9 | 18 | 13 | 15 | 19 |

**Πίνακας 6 – Στιγμιότυπο του Παραρτήματος Γ’ για το CIS Control 3.12**

Στο παραπάνω πίνακα 6 βλέπουμε ότι το CIS μέτρο ασφάλειας 3.12 είναι σε θέση να μετριάσει 9 τεχνικές για την απειλή Malware, 18 τεχνικές για την απειλή Ransomware, 13 απειλές για την απειλή Web Application Hacking, 15 τεχνικές για την απειλή Insider and Privilege Missue και 19 τεχνικές για την απειλή Targeted Intrusion.

Ανάλογα λοιπόν με τον αριθμό και τα μέτρα ασφάλειας που έχει υλοποιήσει ο οργανισμός που βασίζονται στις απαντήσεις του ερωτηματολογίου βάση του πίνακα 2 υπολογίζεται ο δείκτης ωριμότητας για την συγκεκριμένη συνάρτηση αξιολόγησης.

Ο υπολογισμός του δείκτη επιπέδου ωριμότητάς εκτελείται ξεχωριστά για κάθε απειλή :

$$\text{SurveyResult} \sum \ (Result\ IG_x 1.1\alpha\ V_{1.1} + \ Result\ IG_x 1.2\alpha\ V_{1.2} + \cdots + \ Result\ IG_x N\alpha\ V_N)$$

N = τελευταίο CIS μέτρο προστασίας
α = δείκτης (0|0,5|1)
$V_y$= αξία για κάθε απειλή
x= IG1 | IG2 | IG3

max_ Malware Value = 1191
max_ Ransomware = 1480
max_ Web App Hacking = 923
max_ Insider and Privilege Misuse = 895
max_ Targeted Intrusion = 1259

Rating = SurveyResult * 10 / $max_x$

Στις εικόνες 3.12 και 3.13 παρουσιάζετε το αποτέλεσμα του δείκτη ωριμότητας στην εφαρμογή για την συγκεκριμένη συνάρτηση αξιολόγησης.

## 4.5 Συνάρτηση Αξιολόγησης Βασισμένη στο CIS Community Defense Model για τις 5 πιο Σημαντικές Απειλές του 2021 – Οριζόντια Προσέγγιση

Η συγκεκριμένη συνάρτηση έρχεται να αξιολογήσει την ωριμότητα του οργανισμού έναντι των 5 πιο σημαντικών απειλών του 2021. Βασίζεται στην Reverse Mapping της ερευνάς του CIS CDM.

Οι εξεταζόμενες απειλές προβάλλονται στον πίνακα 5. Κάθε απειλή/επίθεση μεταφράστηκε σε “attack patterns” μέσω του πίνακα MITRE Attack. Τα “attack patterns” μας έδωσαν τις τεχνικές και υπό-τεχνικές οι οποίες χρησιμοποιήθηκαν για να εκδηλωθούν αυτές οι απειλές/επιθέσεις. Με την σειρά τους αυτές αντιστοιχήθηκαν μέσω των MITRE Attack Mitigations σε μετρά προστασίας των CIS Controls (CIS CSC safeguards). Οι μετρήσεις ελήφθησαν (περιληπτικά στο Παράτημα Γ’) από το reverse mapping της έρευνας CIS CDM όπου κάθε μέτρο προστασίας αξιολογήθηκε με βάση το κατά πόσο είναι ικανό να μετριάσει μια ή περισσότερες από τις 5 απειλές/επιθέσεις.

| CIS Safeguards ALL IG | Malware | Ransomeware | Web App Hacking | Insider and Privilege Misuse | Targeted Intrusion | Accumulated Horizontal Value |
|---|---|---|---|---|---|---|
| 3.12 | 9 | 18 | 13 | 15 | 19 | 74 |

**Πίνακας 7 – Στιγμιότυπο του Παραρτήματος Ε’ για το CIS Control 3.12**

Στο παραπάνω πίνακα 7 βλέπουμε ότι το CIS μέτρο ασφάλειας 3.12 είναι σε θέση να μετριάσει 9 τεχνικές για την απειλή Malware, 18 τεχνικές για την απειλή Ransomware, 13 απειλές για την απειλή Web Application Hacking, 15 τεχνικές για την απειλή Insider and Privilege Misuse και 19 τεχνικές για την απειλή Targeted Intrusion τα οποία αθροίζονται ορίζονται. Από το οριζόντιο άθροισμα προκύπτει η συγκεκριμένη συνάρτηση αξιολόγησης, η οποία προσθέτει αξία σε κάθε μέτρο προστασίας ανάλογα με την τεχνικές που μετριάζει για το σύνολο των 5 απειλών. Οι οριζόντιες αξίες είναι αποτυπωμένες στον πίνακα του Παραρτήματος Ε’.

Ανάλογα λοιπόν με τον αριθμό και τα μέτρα ασφάλειας που έχει υλοποιήσει ο οργανισμός, τα οποία βασίζονται στις απαντήσεις του ερωτηματολογίου βάσει του πίνακα 2, υπολογίζεται ο δείκτης ωριμότητας για την συγκεκριμένη συνάρτηση αξιολόγησης.

Υπολογισμός δείκτη επιπέδου ωριμότητάς οριζόντια αθροίζοντας τις τιμές όλων των απειλών :

$$\text{SurveyResult} \sum \ (Result\ IG_x 1.1\alpha\ V_{1.1} + \ Result\ IG_x 1.2\alpha\ V_{1.2} + \cdots + \ Result\ IG_x N\alpha\ V_N)$$

N = τελευταίο CIS μέτρο προστασίας
α = δείκτης (0|0,5|1)
$V$ = οριζόντια αξία μέτρου προστασίας
x= IG1 | IG2 | IG3

max = max_ Malware Value + max_ Ransomware + max_ Web App Hacking + max_ Insider + max_Privilege Misuse = 1191 + 1480 + 923 + 895 + 1259 = 5748

Rating = SurveyResult * 10 / $max$

Ο συγκεκριμένος δείκτης δεν έχει ενσωματωθεί στην εφαρμογή ‘Cyber Defense Assessment Tool’.

# Κεφάλαιο 5: Αρχιτεκτονική και Τεχνολογίες Ανάπτυξης της Εφαρμογής CyberDefenseAssessmentTool

## 5.1 Απαιτήσεις Εφαρμογής

Οι τεχνικές απαιτήσεις της εφαρμογής βασίζονται σε εκείνες του Cybersecurity Capability Maturity Model [43] . Πρόκειται για μια εφαρμογή που εκτελείται τοπικά και δεν απαιτείται διαδικτυακή σύνδεση. Ο χρήστης μπορεί ανά πάσα στιγμή να τερματίσει την εφαρμογή χωρίς να χάσει τα δεδομένα εισόδου και να συνεχίσει κάποια άλλη στιγμή. Η εφαρμογή επιτρέπει εκτύπωση του αποτελεσμάτων αξιολόγησης και των συστάσεων σε PDF.

## 5.2 Αρχιτεκτονική Εφαρμογής

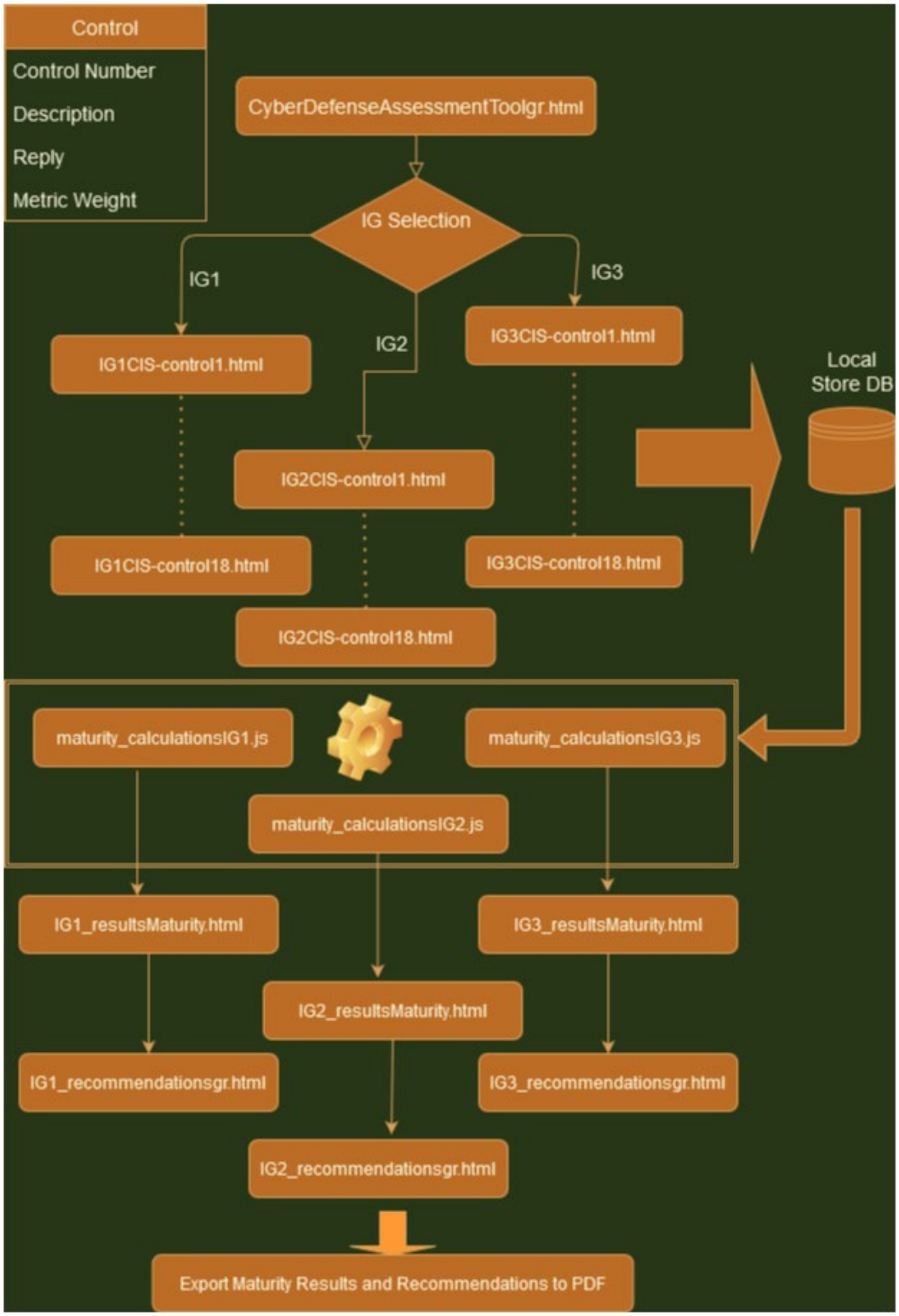
Στην εικόνα 5.1 παρουσιάζεται η υψηλού επιπέδου αρχιτεκτονική υλοποίησης της εφαρμογής.
Οι απαντήσεις του ερωτηματολογίου καταχωρούνται στην τοπική βάση δεδομένων (local storage) του web browser. Όταν ολοκληρωθεί η διαδικασία των απαντήσεων ξεκινάει η φάση υπολογισμού των δεικτών αξιολόγησης ωριμότητας κυβερνοασφάλειας και επιστέφονται στην οθόνη άμεσα. Στην συνέχεια μπαίνοντας στην τελική φάση επιστρέφονται με βάση τους δείκτες αξιολογήσεις οι κατάλληλες συστάσεις.

## 5.3 Τεχνολογίες

Η εφαρμογή αναπτύχθηκε σε HTML, CSS, JavaScipt. Στόχος ήταν η εφαρμογή να τρέχει σε διαφορετικά λειτουργικά συστήματα χωρίς πολλές τοπικές εξαρτήσεις και χωρίς να υπάρχει εξάρτηση από web server. επίσης, στόχος ήταν να μεταφορτώνεται και να προωθείται ευκολά. Παράλληλα δίνεται η επιλογή να λειτουργήσει και ως web εφαρμογή στην επόμενη φάση ανάπτυξής της. Η εφαρμογή είναι συμβατή με τους εξής web browsers :

1 Google Chrome
2 MS Edge
3 Opera

Ο λόγος για αυτό είναι ότι για την αποθήκευση των αποτελεσμάτων στην βάση δεδομένων, χρησιμοποιήθηκε ο μηχανισμός “Local Storage”, ο οποίος θεωρητικά είναι συμβατός με όλους τους συγχρόνους web browser, στην πράξη όμως σε low performance web browser δεν λειτουργεί αρκετά αξιόπιστα, με αποτέλεσμα να είναι μη αποδεκτή η χρήση του. Μέσω του local storage όλα τα αποτελέσματα αποθηκεύονται για μελλοντική χρήση. Στο κάθετο μενού υπάρχει επιλογή διαγράφης του local storage.




**Εικόνα 5.1 – Υψηλού επιπέδου αρχιτεκτονική υλοποίησης της εφαρμογής**

# Κεφάλαιο 6: Συμπεράσματα

## 6.1 Κύρια Συμπεράσματα

Με βάση τα CIS Controls που αποτελούν μια βασική γραμμή κυβερνοασφάλειας και το πλαίσιο Mitre Attack που συγκεντρώνει, ομαδοποιεί και συνδυάζει όλες τις γνωστές τεχνικές κυβερνοεπιθέσεων, η αξιολόγηση επιπέδου ωριμότητας κυβερνοασφάλειας που παρουσιάζεται σε αυτή την εργασία θα έπρεπε να αποτελεί μια άμεση, πρακτική και γρήγορη μέθοδο για την βελτίωση της κυβερνοάμυνας ενός οργανισμού, εφόσον εκτελείται περιοδικά και με υπευθυνότητα. Παρατηρήσαμε μια αντίστροφη προσέγγιση σε σχέση με την αξιολόγηση ρίσκου Η αξιολόγηση ρίσκου ακολουθεί τη σειρά Assets-> Threats -> Likelihood of Impact -> Risk -> Controls. Η αξιολόγηση επιπέδου ωριμότητας, όπως παρουσιάζεται σε αυτή την εργασία ακολουθεί τη σειρά Available Security Controls Groups -> Offensive Technique/Threats -> Assets.

Σε καμία περίπτωση η αξιολόγηση επίπεδου ωριμότητας δεν μπορεί να αντικαταστήσει την αξιολόγηση ρίσκου αλλά έρχεται να την συμπληρώσει ή και να την επαληθεύσει. Ωστόσο, για να έχουμε χειροπιαστά αποτελέσματα, θα πρέπει να εφαρμοστεί σε μια ομάδα οργανισμών όλων των κατηγοριών, με την κατάλληλη ερευνητή μεθοδολογία και να ακολουθήσει σύγκριση με την αξιολόγηση ρίσκου.

## 6.2 Προτάσεις Ανάπτυξης και Μελλοντικά Ερευνητικά Ζητήματα

Μελλοντικά θα μπορούσε να συμπληρωθεί στην εφαρμογή αξιολόγησης επιπέδου ωριμότητας κυβερνοασφάλειας το πρότυπο ISO270001 όπως και η έρευνα MITRE Def3nbd.

Δεν ήταν δυνατόν στο πλαίσιο αυτής της διατριβής να συγγράφουν κατάλληλες και ολοκληρωμένες συστάσεις για οργανισμούς κάθε κατηγορίας υλοποίησης και ίσως μια τέτοια

προσπάθεια ξεπερνά κατά πολύ τις ατομικές προσδοκίες μιας μεταπτυχιακής διατριβής.
Στην επομένη τεχνική φάση η εφαρμογή θα μπορούσε να ενσωματωθεί σε ένα web server περιβάλλον.

# ΑΝΑΦΟΡΕΣ


[1] «mindigital.gr,» [Ηλεκτρονικό]. Available: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwj_s_aRr-X7AhVZR_EDHZtKDHwQFnoECBkQAQ&url=https%3A%2F%2Fmindigital.gr%2Fwp-content%2Fuploads%2F2021%2F06%2F%25CE%2595%25CE%25B3%25CF%2587%25CE%25B5%25CE%25B9%25CF%2581.

[2] «rapid7.com,» [Ηλεκτρονικό]. Available: https://www.rapid7.com/globalassets/_pdfs/product-and-service-briefs/rapid7-csma-service-brief.pdf#:~:text=The%20Cyber%20Security%20Maturity%20Assessment,surrounding%20your%20existing%20security%20program..

[3] SANS, «sans.org,» [Ηλεκτρονικό]. Available: https://www.sans.org/blog/cis-controls-v8/.

[4] CIS, «cisecurity.org,» [Ηλεκτρονικό]. Available: https://www.cisecurity.org/insights/white-papers/cis-community-defense-model.

[5] A. Scripts, «auditscripts.com,» [Ηλεκτρονικό]. Available: https://www.auditscripts.com/free-resources/critical-security-controls/.

[6] MITRE, «MITRE ATT&CK,» 2022. [Ηλεκτρονικό]. Available: https://attack.mitre.org/.

[7] C. C. f. I. S. CDM, «CIS Center for Internet Security,» 2022. [Ηλεκτρονικό]. Available: https://www.cisecurity.org/insights/white-papers/cis-community-defense-model-2-0.

[8] verizon.com, «verizon.com,» [Ηλεκτρονικό]. Available: https://www.verizon.com/business/resources/reports/dbir/.

[9] IBM, «ibm.com,» [Ηλεκτρονικό]. Available: https://www.ibm.com/downloads/cas/ADLMYLAZ.

[10] ENISA, «enisa.europa.eu,» [Ηλεκτρονικό]. Available: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021.

[11] crowdstrike, «crowdstrike.com,» [Ηλεκτρονικό]. Available: https://www.crowdstrike.com/resources/reports/cyber-front-lines/#:~:text=The%20CrowdStrike%20Services%20Cyber%20Front,recover%20from%20intrusions%20every%20day..

[12] akamai.com. [Ηλεκτρονικό]. Available: https://www.akamai.com/our-thinking/the-state-of-the-internet.

[13] N. I. o. S. a. T. U. D. C. NIST, «NIST CyberSecurity Framwork,» 2022. [Ηλεκτρονικό]. Available: https://www.nist.gov/cyberframework.

[14] C. A. Specification, «Controls Assessment Specification,» 2022. [Ηλεκτρονικό]. Available: https://controls-assessment-specification.readthedocs.io/en/stable/about/controls.html.

[15] CIS, «https://www.cisecurity.org/cybersecurity-tools/,» [Ηλεκτρονικό].

[16] CIS, «https://www.cisecurity.org/cis-benchmarks/,» [Ηλεκτρονικό]. Available: https://www.cisecurity.org/cis-benchmarks/.

[17] Microsoft, «https://www.microsoft.com/en-us/download/details.aspx?id=55319,» [Ηλεκτρονικό]. Available: https://www.microsoft.com/en-us/download/details.aspx?id=55319.

[18] K. Pollack, «https://www.calcomsoftware.com/cis-hardening-and-configuration-security-guide/#secure,» [Ηλεκτρονικό]. Available: https://www.calcomsoftware.com/cis-hardening-and-configuration-security-guide/#secure.

[19] itgovernance.co.uk, «itgovernance.co.uk,» [Ηλεκτρονικό]. Available: https://www.itgovernance.co.uk/secure-configuration.

[20] O. Zlotnik, «hysolate.com,» [Ηλεκτρονικό]. Available: https://www.hysolate.com/blog/system-

hardening-guidelines-best-practices/.

[21] S. Harvey, «kirkpatrickprice.com,» [Ηλεκτρονικό]. Available: https://kirkpatrickprice.com/blog/industry-accepted-hardening-standards/.

[22] utexas.edu, «utexas.edu,» [Ηλεκτρονικό]. Available: https://security.utexas.edu/os-hardening-checklist.

[23] securitymetrics.com, «securitymetrics.com,» [Ηλεκτρονικό]. Available: https://www.securitymetrics.com/blog/system-hardening-standards-how-comply-pci-requirement-22.

[24] comodo.com, «comodo.com,» [Ηλεκτρονικό]. Available: https://www.comodo.com/siem/network-ids.php.

[25] suricata.io, «suricata.io,» [Ηλεκτρονικό]. Available: https://suricata.io/.

[26] snort.org, «https://www.snort.org/,» [Ηλεκτρονικό]. Available: https://www.snort.org/.

[27] splunk.com, «splunk.com,» [Ηλεκτρονικό]. Available: https://www.splunk.com/.

[28] securityonionsolutions.com, «securityonionsolutions.com,» [Ηλεκτρονικό]. Available: https://securityonionsolutions.com/.

[29] P. Alto, «paloaltonetworks.com,» [Ηλεκτρονικό]. Available: https://www.paloaltonetworks.com/cyberpedia/what-is-an-intrusion-detection-system-ids.

[30] S.CH., «nowmag.gr,» [Ηλεκτρονικό]. Available: https://nowmag.gr/%CF%80%CF%81%CF%89%CF%84%CF%8C%CE%BA%CE%BF%CE%BB%CE%BB%CE%BF-%CE%BA%CF%81%CF%85%CF%80%CF%84%CE%BF%CE%B3%CF%81%CE%AC%CF%86%CE%B7%CF%83%CE%B7%CF%82-tls-1-3/.

[31] berkeley.edu, «security.berkeley.edu,» [Ηλεκτρονικό]. Available: https://security.berkeley.edu/data-encryption-transit-guideline.

[32] internetsociety.org, «internetsociety.org,» [Ηλεκτρονικό]. Available: https://www.internetsociety.org/deploy360/tls/basics/.

[33 MITRE, «attack.mitre.org,» [Ηλεκτρονικό]. Available: https://attack.mitre.org/.

[34] sslmarket.com, «sslmarket.com,» [Ηλεκτρονικό]. Available: https://www.sslmarket.com/ssl/help-ssl-certificate-installation.

[35] openssl.org, «openssl.org,» [Ηλεκτρονικό]. Available: https://www.openssl.org/.

[36] Visa.com, «Visa.com,» [Ηλεκτρονικό]. Available: https://developer.visa.com/pages/trusted_certifying_authorities.

[37] yale.edu, «cybersecurity.yale.edu,» [Ηλεκτρονικό]. Available: https://cybersecurity.yale.edu/mss/5/1/2.

[38] Microsoft, «learn.microsoft.com,» [Ηλεκτρονικό]. Available: https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/enable-exploit-protection?view=o365-worldwide.

[39] NSA, «scadahacker.com,» [Ηλεκτρονικό]. Available: https://scadahacker.com/library/Documents/Best_Practices/NSA%20-%20IA%20-%20Anti-Exploitation.pdf.

[40] microsoft.com, «learn.microsoft.com,» [Ηλεκτρονικό]. Available: https://learn.microsoft.com/en-us/azure/sentinel/.

[41] softwaretestinghelp.com, «softwaretestinghelp.com,» [Ηλεκτρονικό]. Available: https://www.softwaretestinghelp.com/siem-tools .

[42] manageengine.com, «manageengine.com,» [Ηλεκτρονικό]. Available: https://www.manageengine.com/products/eventlog/.

[43] E. S. a. E. R. Office of Cybersecurity, «energy.gov,» [Ηλεκτρονικό]. Available: https://www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2.

[44] C. o. I. S. CIS, «CIS Center of Internert Security,» 2022. [Ηλεκτρονικό]. Available: https://www.cisecurity.org/.

[45] C. f. I. Security, «cisecurity.org,» [Ηλεκτρονικό]. Available: https://www.cisecurity.org/controls.

[46] NIST, «nist.gov,» [Ηλεκτρονικό]. Available: https://csrc.nist.gov/Projects/cybersecurity-framework/nist-cybersecurity-framework-a-quick-start-guide.

[47] ginger-anderson, « ControlsAssessmentSpecification,» [Ηλεκτρονικό]. Available: https://github.com/CISecurity/ControlsAssessmentSpecification.

[48] Microsoft, «learn.microsoft.com,» [Ηλεκτρονικό]. Available: https://learn.microsoft.com/en-us/mem/configmgr/core/plan-design/security/enable-tls-1-2-server.

[49] Microsft, «learn.microsoft.com,» [Ηλεκτρονικό]. Available: https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/defender-endpoint-plan-1-2?view=o365-worldwide#compare-microsoft-endpoint-security-plans-1.

[50] sslmarket.com, « www.sslmarket.com,» [Ηλεκτρονικό]. Available: https://www.sslmarket.com/ssl/help-ssl-certificate-installation.
_]

# ΠΑΡΑΡΤΗΜΑ Α' - CIS Critical Security Controls – Μετάφραση στην Ελληνική Γλώσσα

## 01 Καταγραφή και Διαχείριση Συσκευών Οργανισμού

Διαχείριση συσκευών πληροφοριακού συστήματος του οργανισμού. Καταγράψτε με λεπτομέρεια σε ένα μητρώο τις συσκευές του οργανισμού έτσι ώστε να είστε σε θέση να παρακολουθείτε την κατάσταση τους ως προς την διαφύλαξη της ακεραιότητας, της εμπιστευτικότητας και της διαθεσιμότητας αυτών. Στο μητρώο καταγραφής συσκευών θα συμπεριλαμβάνονται συσκευές τελικού χρήστη, διακομιστές (Server), IoT και δικτυακές συσκευές όπως και συστήματα cloud, κινητές συσκευές κ.α.

1.1 Δημιουργία και Διαχείριση Λεπτομερούς Μητρώου Παγίων/Συσκευών

Δημιουργία και διαχείριση λεπτομερούς μητρώου καταγραφής παγίων/συσκευών που αποτελούν μέρος του πληροφοριακού συστήματος του οργανισμού και έχουν την δυνατότητα αποθήκευσης και επεξεργασίας δεδομένων. Αυτά μπορεί να περικλείουν : συσκευές χρηστών (κινητά τηλεφώνα, PC), δικτυακές συσκευές, διακομιστές(Server), IoT συσκευές. Στην καταγραφή πρέπει να συμπεριλαμβάνεται η διεύθυνση δικτύου (εφόσον είναι στατική), διεύθυνση MAC, ονομασία συσκευής, υπεύθυνος(owner) του παγίου και τμήμα. Η καταγραφή γίνεται για συσκευές που βρίσκονται είτε σε φυσική ή εικονική μορφή στην υποδομή, είτε βρίσκονται στο cloud (υποδομή νέφους) του οργανισμού. Επίσης, αφορά συσκευές οι οποίες συνδέονται ανά διαστήματα στο δίκτυο του οργανισμού αν και δεν είναι υπό την διαχείριση αυτού (bring your own device).
Επιθεωρήστε και ενημερώστε το μητρώο καταγραφής σε εξαμηνιαία βάση.

1.2 Αντιμετώπιση μη Εξουσιοδοτημένης Πρόσβασης

Διασφαλίστε την ύπαρξη διαδικασίας αντιμετώπισης μη εξουσιοδοτημένης πρόσβασης συσκευών στο δίκτυο του οργανισμού σε εβδομαδιαία βάση. Ο οργανισμός πρέπει να έχει την δυνατότητα να αφαιρέσει ή να απομονώσει μια ή περισσότερες συσκευή/συσκευές από το δίκτυο του.

1.3 Ενσωμάτωση Ενεργητικού (active) Εργαλείου Ανίχνευσης

Ενσωμάτωση και εκτέλεση εργαλείου/τεχνικού μηχανισμού που εντοπίζει όλες τις συσκευές που είναι συνδεδεμένες στο δίκτυο του οργανισμού. Θα πρέπει να εκτελείται τουλάχιστον σε καθημερινή βάση.

1.4 Χρήση Αρχείων Καταγραφής DHCP για την Ενημέρωση του Μητρώου Καταγραφής παγίων/συσκευών του οργανισμού.

Χρήση αρχείων καταγραφής DHCP για την ενημέρωση του μητρώου καταγραφής παγίων/συσκευών του οργανισμού σε εβδομαδιαία βάση.

1.5 Χρήση Παθητικών(passive) Εργαλείων Ανίχνευσης

Χρήση παθητικών(passive) εργαλείων ανίχνευσης συσκευών του οργανισμού που συνδέονται στο δίκτυο αυτού, έτσι ώστε να πραγματοποιείται συνεχής έλεγχος του δικτύου και να ενημερώνεται το μητρώο καταγραφής συσκευών αυτόματα.

## 02 Καταγραφή και Διαχείριση Λογισμικού

Διαχείριση λογισμικού πληροφοριακού συστήματος του οργανισμού. Λεπτομερής καταγραφή του λογισμικού έτσι ώστε να είναι δυνατή η εγκατάσταση και η εκτέλεση μόνο εξουσιοδοτημένου λογισμικού. Επίσης, να είναι δυνατός ο εντοπισμός μη εξουσιοδοτημένου λογισμικού και να μπορεί να αφαιρεθεί από το πληροφοριακό σύστημα, ώστε να διαφυλαχθεί η ακεραιότητα, η εμπιστευτικότητα και η διαθεσιμότητα αυτού.

2.1 Δημιουργία και Διαχείριση Λεπτομερούς Μητρώου Καταγραφής Λογισμικού

Δημιουργία και διαχείριση λεπτομερούς μητρώου καταγραφής λογισμικού του πληροφοριακού συστήματος του οργανισμού. Το μητρώο θα αναφέρει την ονομασία, τον διανομέα, την ημερομηνία εγκατάστασης, τον σκοπό λειτουργίας, την έκδοση, το URL, τον μηχανισμό εγκατάστασης και την ημερομηνία απεγκατάστασης. Επικαιροποίηση και ενημέρωση πρέπει να εκτελείται τουλάχιστον 2 φορές τον χρόνο.

2.2 Διασφάλιση ότι το εν Χρήση Λογισμικό Υποστηρίζεται

Διασφαλίστε ότι το λογισμικό που χρησιμοποιείτε υποστηρίζεται και λαμβάνει τις κατάλληλες ενημερώσεις από τον αρμόδιο διανομέα/πάροχο. Σε περίπτωση που δεν εμπίπτει σε αυτή την κατηγορία θα πρέπει να λαμβάνονται τα κατάλληλα αντίμετρα και να ενημερώνονται οι εμπλεκόμενοι, δηλαδή ο υπεύθυνος (owner) του αγαθού και η διεύθυνση πληροφορικής. Ο έλεγχος εκτελείται τουλάχιστον μια φορά τον μηνά.

2.3 Διευθέτηση μη Εξουσιοδοτημένου Λογισμικού

Διασφαλίστε ότι δεν έχει εγκατασταθεί μη εξουσιοδοτημένο λογισμικό σε συσκευές του πληροφοριακού συστήματος. Αναφορά και αξιολόγηση ρίσκου σε περίπτωση που κριθεί απαραίτητη η χρήση μη εξουσιοδοτημένου λογισμικού. Ο έλεγχος πρέπει να εκτελείται τουλάχιστον μια φορά τον μηνά.

2.4 Αυτοματοποίηση Καταγραφής Λογισμικού με Χρήση Κατάλληλου Εργαλείου.

Εγκαταστήστε κατάλληλο σύστημα αυτοματοποιημένης διαχείρισης και καταγραφής λογισμού.

2.5 Σύσταση Λίστας Επιτρεπόμενων Εφαρμογών

Δημιουργήστε μια λίστα επιτρεπόμενων εφαρμογών. Ο έλεγχος και επικαιροποίηση της λίστας πρέπει να εκτελείτε τουλάχιστον 2 φορές τον χρόνο ή όταν κριθεί απαραίτητο.

2.6 Σύσταση Λίστας Επιτρεπόμενων Βιβλιοθηκών

Δημιουργήστε μια λίστα επιτρεπόμενων βιβλιοθηκών , όπως .dll, .ocx, .so, κτλ.. Ο έλεγχος και η επικαιροποίηση της λίστας πρέπει να εκτελείται, όταν κρίνεται απαραίτητο και τουλάχιστον 2 φορές τον χρόνο.

2.7 Σύσταση Λίστας Επιτρεπόμενων scripts

Δημιουργήστε μια λίστα από scripts που επιτρέπονται να εκτελεστούν, .ps1, .py, .cmd, .bat κτλ. σε σταθμούς χρηστών (PC) και διακομιστές (Server).Ελέγξτε την εκτέλεση με τεχνικά μέσα. Επικαιροποίηση και ενημέρωση της λίστας πρέπει να εκτελείταιτουλάχιστον 2 φορές τον χρόνο ή όταν κριθεί απαραίτητο.

## 03 Προστασία Δεδομένων

Ανάπτυξη διαδικασιών και τεχνικών μέτρων για τον εντοπισμό, την κατηγοριοποίηση, τον ασφαλή χειρισμό, τη διατήρηση/αποθήκευση και τη διαγραφή/απόρριψη δεδομένων.

3.1 Δημιουργία και Διαχείριση Διαδικασίας Διαχείρισης Δεδομένων

Δημιουργήστε και συντηρήστε μια ειδική διαδικασία διαχείρισης δεδομένων. Η διαδικασία αυτή θα πρέπει να αφορά: την κρισιμότητα των δεδομένων, τον υπεύθυνο δεδομένων, το χειρισμό δεδομένων, τα χρονικά όρια διατήρησης και τις προϋποθέσεις διαγραφής δεδομένων σύμφωνα με τις ανάγκες καθώς και τις νομικές και εμπορικές δεσμεύσεις του οργανισμού.

3.2 Δημιουργία και Διαχείριση Μητρώου Καταγραφής Δεδομένων

Βασιζόμενοι στη διαδικασία διαχείρισης δεδομένων δημιουργήστε και συντηρήστε ένα μητρώο καταγραφής δεδομένων. Θα πρέπει να καταγράφονται δεδομένα τα οποία είναι ευαίσθητα έστω και σε ένα ελάχιστο βαθμό. Η επικαιροποίηση θα πραγματοποιείται τουλάχιστον μια φορά τον χρόνο.

3.3 Ρύθμιση Λίστας Ελέγχου Πρόσβασης Δεδομένων

Διαμορφώστε και διατηρήστε μια λίστα ελέγχου πρόσβασης χρηστών σε δεδομένα. Η συγκεκριμένη λίστα θα καθορίζει ποιοι χρήστες χρειάζεται να έχουν πρόσβαση σε ποια δεδομένα. Αφορά φακέλους αρχείων στο file system από PC, Servers, βάσεις δεδομένων και εφαρμογές.

3.4 Διατήρηση Δεδομένων

Διατηρήστε/αποθηκεύστε τα δεδομένα σύμφωνα με την διαδικασία/πολιτική διαχείρισης δεδομένων (μέτρο 1.3) του οργανισμού σας. Η διατήρηση αφορά το ελάχιστο και μέγιστο χρονικό διάστημα διατήρησης μίας ή περισσότερων ομάδων δεδομένων του οργανισμού.

3.5 Ασφαλής Διαγραφή Δεδομένων

Η διαγραφή δεδομένων πρέπει να γίνεται σύμφωνα με τη διαδικασία διαχείρισης δεδομένων και να λαμβάνει υπόψιν της το βαθμό κρισιμότητας.

3.6 Κρυπτογράφηση Δεδομένων σε Συσκευές χρηστών

Κρυπτογραφήστε συσκευές χρηστών που περιέχουν ευαίσθητα δεδομένα. Τεχνολογίες/εφαρμογές: Windows BitLocker®, Apple FileVault®, Linux® dm-crypt.

3.7 Καθιέρωση και Διαχείριση Κατηγοριοποίησης Δεδομένων

Δημιουργήστε και διατηρήστε έναν τρόπο κατηγοριοποίησης του βαθμού ευαισθησίας των δεδομένων του οργανισμού. Ενδεικτικά μπορείτε να χρησιμοποιήσετε τις κατηγορίες «Ευαίσθητα», «Εμπιστευτικά», «Δημοσιά» και καταχωρίστε τα δεδομένα σε αυτές. Επικαιροποιήστε τις κατηγοριοποιήσεις σε ετησία βάση ή όταν το κρίνει ο οργανισμός σας απαραίτητο.

3.8 Καταγραφή Ροής Δεδομένων

Καταγράψτε την ροή των δεδομένων στο πληροφοριακό σύστημά σας βασιζόμενοι στην διαδικασία διαχείρισης δεδομένων, συμπεριλάβετε όλους τους παρόχους εκτός του οργανισμού σας. Επικαιροποιήστε τις κατηγοριοποιήσεις ετησίως ή όταν το κρίνει ο οργανισμός απαραίτητο.

3.9 Κρυπτογράφηση Δεδομένων σε Αναιρούμενα Μέσα Αποθήκευσης

Κρυπτογραφήστε δεδομένα σε αφαιρούμενα μέσα αποθήκευσης, πχ USB συσκευές, εξωτερική σκληρή δίσκοι, SD κάρτες.

3.10 Κρυπτογράφηση στην Μεταφορά Ευαίσθητων Δεδομένων Μέσω Δικτύου

Κρυπτογράφηση ευαίσθητων δεδομένων κατά τη μεταφορά τους μέσω δικτύου.
Για παράδειγμα με χρήση: TLS, OpenSSH

3.11 Κρυπτογράφηση Αποθηκευμένων/Αρχειοθετημένων Ευαίσθητων Δεδομένων

Κρυπτογραφήστε ευαίσθητα δεδομένα τα οποία βρίσκονται αποθηκευμένα / αρχειοθετημένα σε server, σε βάσεις δεδομένων και σε εφαρμογές. Σε αυτό το μέτρο η κρυπτογράφηση σε επίπεδο αποθηκευτικού μέσου/δίσκου αποτελεί την ελάχιστη προϋπόθεση. Επιπρόσθετα, θα πρέπει να ληφθεί μέριμνα για την κρυπτογράφηση σε επίπεδο εφαρμογής.

3.12 Διαχωρισμός Επεξεργασίας και Αποθήκευσης Δεδομένων Βασισμένη στην Ευαισθησία αυτών

Διαχωρίστε την επεξεργασία και την αποθήκευση δεδομένων ανάλογα με το βαθμό ευαισθησίας.

3.13 Χρήση Λογισμικού για Αποτροπή Απώλειας Δεδομένων

Εγκαταστήστε μια εφαρμογή για αποτροπή απώλειας δεδομένων, έτσι ώστε να εντοπίζονται τα ευαίσθητα δεδομένα που αποθηκεύονται, επεξεργάζονται και μεταδίδονται μέσα από την συσκευές του πληροφοριακού συστήματος του οργανισμού, είτε τοπικά είτε απομακρυσμένα και να ενημερώνετε το μητρώο καταγραφής παγίων/συσκευών αναλόγως.

3.14 Συντήρηση Μητρώου Καταγραφής Πρόσβασης Δεδομένων

Δημιουργήστε και ενημερώστε ένα μητρώο καταγραφής πρόσβασης/αλλαγής/διαγράφης δεδομένων.

## 04 Ασφαλής Διαμόρφωση Εξοπλισμού και Εφαρμογών

Διενεργήστε σε τακτική βάση ασφαλή διαμόρφωση (secure configuration) σε σταθμούς εργασίας (desktops, laptops), διακομιστές (servers), δικτυακές συσκευές (routers, switches, access points, firewalls), IoT και κινητές συσκευές και εφαρμογές.

4.1 Δημιουργία και Συντήρηση Διαδικασίας Ασφαλούς Διαμόρφωσης Εξοπλισμού

Δημιουργήστε και συντηρήστε μια διαδικασία ασφαλούς διαμόρφωσης εξοπλισμού πληροφορικής και εφαρμογών. Να επικαιροποιείτε και να ενημερώνετε τη διαδικασία σε ετήσια βάση ή όταν αυτό κριθεί απαραίτητο.

4.2 Δημιουργία και Συντήρηση Διαδικασίας Ασφαλούς Διαμόρφωσης Δικτυακής Υποδομής

Δημιουργήστε και συντηρήστε μια διαδικασία ασφαλούς ρύθμισης της δικτυακής υποδομής. Να επικαιροποιείτε και να ενημερώνετε την διαδικασία σε ετήσια βάση ή όταν αυτό κριθεί απαραίτητο.

4.3 Ρύθμιση Αυτομάτου Κλειδώματος Επιφάνειας Εργασίας

Ρυθμίστε το αυτόματο κλείδωμα στους σταθμούς εργασίας και στις κινητές συσκευές. Δηλ. να μην υπάρχει πια δυνατότητα χειρισμού από κάποιο άτομο το οποίο δεν είναι εξουσιοδοτημένο. Οι σταθμοί εργασίας πρέπει να κλειδώνουν τουλάχιστον μετά από 15 λεπτά, οι κινητές συσκευές τουλάχιστον μετά από 2 λεπτά.

4.4 Υλοποίηση και Ρύθμιση Firewall σε Συστήματα (servers)

Υλοποιείστε και ρυθμίστε καταλληλά firewall σε συστήματα/διακομιστές (servers) όπου αυτό υποστηρίζεται. Μπορεί να χρησιμοποιηθεί Virtual Firewall, Firewall του Λειτουργικού Συστήματος και κάποιου άλλου παρόχου.

4.5 Υλοποίηση και Ρύθμιση Firewall στους Σταθμούς Εργασίας (PC, Desktop, Laptop)

Υλοποιείστε και ρυθμίστε καταλληλά firewall στους σταθμούς εργασίας (PC, Desktop, Laptop. Μπορεί να χρησιμοποιηθεί Virtual Firewall, Firewall του Λειτουργικού Συστήματος και κάποιου άλλου παρόχου. Να ρυθμιστεί σύμφωνα με την λογική “Default Deny – Explicitly Allow”
Υλοποιείστε firewall ως εφαρμογή στους σταθμούς εργασίας τελικού χρήστη (PC, Desktop, Laptop), το οποίο να εμποδίζει κάθε δικτυακή σύνδεση από και προς τη συσκευή με εξαίρεση τις θύρες και τις υπηρεσίες που απαιτούνται με βάση τις επιχειρησιακές ανάγκες.

4.6 Ασφαλής Διαχείριση Εξοπλισμού και Εφαρμογών

Ασφαλίστε την διαχείριση του εξοπλισμού και των εφαρμογών. Αυτό το μέτρο αφορά για παράδειγμα την ασφαλή ρύθμιση του εξοπλισμού/εφαρμογών μέσω version-controlled-infrastructure-as-code και την πρόσβαση στα συστήματα μέσω ασφαλών δικτυακών πρωτοκόλλων HTTPS, SSH, VPN.
Μην χρησιμοποιείτε μη ασφαλή πρωτόκολλα όπως Telnet και HTTP.

4.7 Διαχείριση Προ-Εγκατεστημένων Λογαριασμών σε Συσκευές και Εφαρμογές

Διαχειριστείτε λογαριασμούς σε συσκευές και εφαρμογές οι οποίοι έχουν ρυθμιστεί από τον πάροχο/κατασκευαστή. Τέτοιοι λογαριασμοί μπορεί να είναι οι λεγόμενοι “root”, “default admin”, “admin” κ.α. Διαγράψτε ή απενεργοποιήστε αυτούς τους λογαριασμούς. Εάν αυτό δεν είναι εφικτό, αλλάξτε το password με ένα πιο ισχυρό.

4.8 Απενεργοποίηση Μη Αναγκαίων Υπηρεσιών σε Συσκευές και Εφαρμογές

Διασφαλίστε ότι δεν τρέχουν σε συσκευές και εφαρμογές(συστήματα,PC κ.α.) μη αναγκαίες υπηρεσίες και προγράμματα.

4.9 Ρύθμιση Έμπιστων DNS-Server

Ρυθμίστε/ορίστε για το δίκτυο του οργανισμού εμπίστους DNS-Server.

4.10 Αυτοματοποιημένο Κλείδωμα Λογαριασμών σε Κινητές Συσκευές

Υλοποιήστε με τεχνικό μηχανισμό όπως π.χ. Microsoft® InTune Device Lock and Apple® Configuration Profile maxFailedAttempts, έτσι ώστε μετά από έναν ορισμένο αριθμό αποτυχημένων προσπαθειών εισόδου στην κινητή συσκευή αυτή να κλειδώνει.

4.11 Υλοποιήστε Απομακρυσμένη Διαγραφή Δεδομένων σε Κινητές Συσκευές

Υλοποιήστε με τεχνικό μηχανισμό την αυτόματη διαγραφή δεδομένων σε εταιρικές κινητές συσκευές εφόσον αυτό κρίνεται αναγκαίο, δηλαδή σε περίπτωση κλοπής ή απώλειας της συσκευής ή μη χρήσης αυτής.

4.12 Διαχωρισμός Προφίλ σε Κινητές Συσκευές

Εφαρμόστε λύσεις σε εταιρικές κινητές συσκευές οι οποίες διαχωρίζουν το προσωπικό προφίλ χρήστη από το εταιρικό, Apple® Configuration Profile ή Android™ Work Profile.

## 05 Διαχείριση Λογαριασμών

Χρήση κατάλληλων τεχνικών εργαλείων και διαδικασιών για την διαχείριση πρόσβασης σε λογαριασμούς χρηστών, administrator, υπηρεσιακούς λογαριασμούς(service accounts) για εταιρικές συσκευές και εφαρμογές.

5.1 Δημιουργία και Συντήρηση Μητρώου λογαριασμών

Δημιουργήστε και συντηρήστε ένα μητρώο καταγραφής όλων των χρησιμοποιουμένων λογαριασμών του οργανισμού. Αυτό το μητρώο θα πρέπει να αποτελείται από λογαριασμούς (user accounts) χρηστών και διαχειριστών (administrator accounts). Θα πρέπει τουλάχιστον να περιέχει το ονοματεπώνυμο του ατόμου που το χρησιμοποιεί, το όνομα χρήστη, την έναρξη / λήξη λογαριασμού και το τμήμα. Αξιολογήστε τις προσβάσεις στους λογαριασμούς τουλάχιστον ανά τρίμηνο.

5.2 Χρήση Ξεχωριστών/Μοναδικών Κωδικών Πρόσβασης

Χρησιμοποιήστε ξεχωριστούς/μοναδικούς κωδικούς για κάθε εταιρική συσκευή στον οργανισμό. Για λογαριασμό που χρησιμοποιεί multifactor authentication (MFA) χρησιμοποιήστε τουλάχιστον 8 χαρακτήρες, για τους άλλους τουλάχιστον 14 χαρακτήρες.

5.3 Απενεργοποίηση Ανενεργών Λογαριασμών

Απενεργοποιήστε ή διαγράψτε λογαριασμούς οι οποίοι είναι ανενεργοί για πάνω από 45 μέρες.

5.4 Εκχώρηση Δικαιωμάτων Διαχειριστή (Administrator Rights Privileges)

Αναθέστε τα ελάχιστα απαιτούμενα δικαιώματα σε όλους το λογαριασμούς του οργανισμού, εκτός από ορισμένος λογαριασμούς διαχειριστών που απαιτούνται για την διαχείριση των εταιρικών συσκευών, δικτύου και υπηρεσιών (administrator accounts).

5.5 Δημιουργία και Συντήρηση Μητρώου Υπηρεσιακών Λογαριασμών (Service Accounts)

Δημιουργήστε και συντηρήστε ένα μητρώο όλων των χρησιμοποιουμένων υπηρεσιακών λογαριασμών (service accounts) του οργανισμού. Θα πρέπει να περιέχει τον υπεύθυνο τμήματος, την ημερομηνία επικαιροποίησης, τη χρήση. Επικαιροποιήστε το μητρώο τουλάχιστον κάθε τρίμηνο.

5.6 Χρήση Κεντρικής Διαχείρισης Λογαριασμών

Χρησιμοποιείτε κεντρική διαχείριση λογαριασμών, π.χ Domain Controller – Active Directory Users and Computers.

## 06 Διαχείριση Ελέγχου Πρόσβασης

Χρήση κατάλληλων τεχνικών εργαλείων και διαδικασιών για την παροχή δικαιωμάτων και προνομίων σε χρήστες, διαχειριστές και υπηρεσιακούς λογαριασμούς, σε εταιρικές συσκευές και σε εφαρμογές του οργανισμού.

6.1 Καθιερώστε Διαδικασία Παροχής Δικαιωμάτων

Δημιουργήστε και ακολουθήστε μια διαδικασία παροχής δικαιωμάτων σε πόρους του πληροφοριακού συστήματος, κατά προτίμηση αυτοματοποιημένη . Αυτή η διαδικασία θα ορίζει τα δικαιώματα που θα έχουν νεοεισερχόμενοί χρήστες, τα αιτήματα χορήγησης δικαιωμάτων και την αλλαγή ρολών.

6.2 Καθιερώστε Διαδικασία Ανάκλησης Δικαιωμάτων

Δημιουργήστε και ακολουθήστε μια διαδικασία ανάκλησης δικαιωμάτων σε πόρους του πληροφοριακού συστήματος, κατά προτίμηση αυτοματοποιημένη. Η διαδικασία θα ορίζει πως και πότε θα απενεργοποιείται ένας λογαριασμός σε περιπτώσεις αποχώρησης εργαζομένου, ανάκλησης δικαιωμάτων χρήστη και αλλαγής ρόλου μέσα στον οργανισμό. Να προτιμάτε την απενεργοποίηση από τη διαγραφή λογαριασμών, για να διασφαλιστεί ο έλεγχος ενεργειών του λογαριασμού.

6.3 Ενεργοποίηση Πολυπαραγοντικής Αυθεντικοποίησης σε Εξωτερικά (Internet Facing) συστήματα

Ενεργοποιήστε την πολυπαραγοντική αυθεντικοποίηση (MFA) σε συστήματα τα οποία είναι συνδεδεμένα απευθείας με το παγκόσμιο διαδίκτυο όπου αυτό υποστηρίζεται. Η υλοποίηση MFA μέσω Directory Services (π.χ. Domain Controller) ή μέσω Single Sign On provider είναι ικανοποιητικοί μηχανισμοί για αυτό το μετρό.

6.4 Ενεργοποίηση Πολυπαραγοντικής Αυθεντικοποίησης κατά την Απομακρυσμένη Πρόσβαση από Εξωτερικό Δίκτυο.

Απαιτείται η ενεργοποίηση πολυπαραγοντικής αυθεντικοποίησης κατά την απομακρυσμένη πρόσβαση (Remote Control) από εξωτερικό/δημόσιο δίκτυο.

6.5 Ενεργοποίηση Πολυπαραγοντικής Αυθεντικοποίησης σε Λογαριασμούς Διαχειριστή

Απαιτείται η ενεργοποίηση πολυπαραγοντικής αυθεντικοποίησης σε λογαριασμούς διαχειριστή όπου αυτό υποστηρίζεται.

6.6 Δημιουργία και Συντήρηση Μητρώου Καταγραφής Συστημάτων Αυθεντικοποίησης και Εξουσιοδότησης

Δημιουργήστε και συντηρήστε ένα μητρώο καταγραφής συστημάτων αυθεντικοποίησης και εξουσιοδότησης.

6.7 Κεντρική Διαχείρισης Ελέγχου Πρόσβασης

Διαχειριστείτε κεντρικά τον έλεγχο πρόσβασης μέσω Directory Services (Domain Controller – Active Directory Users and Computers) ή μέσω Single Sign On provider.

6.8 Σύσταση Διαδικασίας/Μηχανισμού Ελέγχου Πρόσβασης Βασισμένη σε Διακριτούς Πόλους

Καθορίστε και καταγράψτε διακριτούς ρόλους που αντιστοιχούν σε εργασίες και τμήματα του οργανισμού

και αναθέστε τα καταλληλά δικαιώματα πρόσβασης. Ελέγξτε την πρόσβασή στις εταιρικές συσκευές (PC, Server) για να επιβεβαιώσετε ότι έχει γίνει σωστή αντιστοίχιση. Επικαιροποιήστε την διαδικασία σε ετήσια βάση.

## 07 Συνεχής Διαχείριση Ευπαθειών

Αναπτύξτε διαδικασία συνεχούς ανίχνευσης και εκτίμησης ευπαθειών σε όλες τις εταιρικές συσκευές της υποδομής του πληροφοριακού συστήματος, έτσι ώστε να εξαλειφθούν ή να ελαχιστοποιηθούν οι δυνατότητες εκμετάλλευσης από κακόβουλες ενέργειες. Ελέγξτε εσωτερικούς και εξωτερικούς πόρους του πληροφοριακού συστήματος για νέες απειλές και ευπάθειες.

7.1 Καθιέρωση και Συντήρηση Διαδικασίας Διαχείρισης Ευπαθειών

Καθιερώστε και συντηρήστε μια διαδικασία διαχείρισης ευπαθειών για όλες τις συσκευές του πληροφοριακού συστήματος. Επικαιροποιήστε και ενημερώστε σε ετήσια βάση.

7.2 Καθιέρωση και Συντήρηση Διαδικασίας Αντιμετώπισης Ευπαθειών

Καθιερώστε και συντηρήστε μια διαδικασία βασιζομένη σε αξιολόγηση ρίσκου για αντιμετώπιση ευπαθειών, σε μηνιαία βάση.

7.3 Αυτοματοποίηση Διαχείρισης Ενημερώσεων Λειτουργικών Συστημάτων

Αυτοματοποιήστε τις ενημερώσεις λειτουργικών συστημάτων σε όλες τις συσκευές του πληροφοριακού συστήματος. Οι ενημερώσεις θα πρέπει να ελέγχονται και να εγκαθίστανται τουλάχιστον μια φορά τον μηνά.

7.4 Αυτοματοποίηση Διαχείρισης Ενημερώσεων Εφαρμογών

Αυτοματοποιήστε τις ενημερώσεις εφαρμογών σε όλα τα συστήματα (PC, Server) του δικτύου. Οι ενημερώσεις θα πρέπει να ελέγχονται και να εγκαθίστανται τουλάχιστον μια φορά τον μηνά.

7.5 Αυτοματοποίηση Σάρωσης Ευπαθειών για Συστήματα Εσωτερικού Δικτύου

Αυτοματοποιήστε την διαδικασία σάρωσης σε συστήματα εσωτερικά του δικτύου. Εκτελέστε αυθεντικοποιημένη και μη αυθεντικοποιημένη σάρωση. Εκτελέστε την σάρωσή τουλάχιστον κάθε τρίμηνό, με SCAP συμβατό εργαλείο σάρωσής.

7.6 Αυτοματοποίηση Σάρωσης Ευπαθειών για Συστήματα Προσβάσιμα από το Παγκόσμιο Διαδίκτυο

Αυτοματοποιήστε τη διαδικασία σάρωσης ευπαθειών σε συστήματα που είναι προσβάσιμα από το παγκόσμιο διαδίκτυο. Εκτελέστε αυθεντικοποιημένη και μη αυθεντικοποιημένη σάρωση. Εκτελέστε τη σάρωση κάθε τρίμηνο τουλάχιστον με SCAP συμβατό εργαλείο σάρωσης.

7.7 Αντιμετώπιση Εντοπισμένων Ευπαθειών

Αντιμετωπίστε τις ευπάθειες που έχουν εντοπιστεί μέσω διαδικασιών και κατάλληλων εργαλείων, σε τουλάχιστον μηνιαία βάση. Η αντιμετώπιση είναι μια βασική πτυχή της διαδικασίας και αποτελεί τελικά αυτό που μειώνει τον κίνδυνο, είτε με αποκατάσταση, είτε μέσω άλλης διαδικασίας (π.χ. παροπλισμός συστήματος, αποδοχή ρίσκου, ανάθεση σε 3ους κ.α.). Εάν δεν προβείτε σε αποκατάσταση ή αποτύχετε να ιεραρχήσετε σωστά τα αποτελέσματά, θέτετε ολόκληρο το πληροφοριακό σύστημα του οργανισμού σε κίνδυνο.

## 08 Διαχείριση Αρχείων Καταγραφής Ελέγχου (Audit Logs)

Συλλογή, ανασκόπηση και διατήρηση αρχείων καταγραφής ελέγχου συμβάντων έτσι ώστε να ειστε σε θέση να εντοπίσετε, να κατανοήσετε, να αντιμετωπίσετε και να επανακάμψετε από μια κυβερνοεπίθεση.

8.1 Καθιέρωση και Συντήρηση Διαδικασίας Διαχείρισης Αρχείων Καταγραφής Ελέγχου(Audit Logs)

Καθιερώστε και συντηρήστε μια διαδικασία διαχείρισης αρχείων καταγραφής ελέγχου συμβάντων η οποία θα ορίζει τις απαιτήσεις του οργανισμού. Η διαδικασία θα πρέπει τουλάχιστον να καλύπτει το θέμα της καταγραφής / συλλογής, ανασκόπησης και διατήρησης. Επικαιροποιήστε και ενημερώστε τη διαδικασία σε ετήσια βάση.

8.2 Συλλογή Αρχείων Καταγραφής Ελέγχου(Audit Logs)

Συλλέξτε αρχεία καταγραφής ελέγχου συμβάντων. Βεβαιωθείτε ότι η καταγραφή συμβάντων είναι ενεργοποιημένη συμφώνα με την διαδικασία που έχει οριστεί (8.1 Καθιέρωση και συντήρηση διαδικασίας διαχείρισης αρχείων καταγραφής ελέγχου συμβάντων.)

8.3 Επιβεβαίωση Κατάλληλης Αποθήκευσης Αρχείων Καταγραφής Ελέγχου (Audit Logs)

Επιβεβαιώστε ότι τα αρχεία καταγραφής είναι κατάλληλα αποθηκευμένα σύμφωνα με την διαδικασία που έχει οριστεί (8.1 Καθιέρωση και συντήρηση διαδικασίας διαχείρισης αρχείων καταγραφής ελέγχου συμβάντων.)

8.4 Συγχρονισμός Ημερομηνίας και Ώρας

Φροντίστε έτσι ώστε όλα τα συστήματα(Server&PC) και κατ' επέκταση τα αρχεία καταγραφής ελέγχου να έχουν κοινή ημερομηνία και ώρα. Δηλώστε τουλάχιστον δυο πήγες με τις οποίες θα συγχρονίζονται όλα τα σύστημα του οργανισμού. Διασφαλίστε τον συγχρονισμό ανάμεσα στα ρολόγια όλων των συσκευών, έτσι ώστε να επιτυγχάνεται ακρίβεια στη συσχέτιση συμβάντων μεταξύ διαφορετικών συστημάτων.

8.5 Συλλογή Αναλυτικών Αρχείων Καταγραφής (Audit Logs) ανά περίπτωση

Συλλέξτε αναλυτικά αρχεία καταγραφής για κρίσιμα συστήματα ή για συστήματα που αποθηκεύουν και επεξεργάζονται ευαίσθητα δεδομένα, τα οποία θα μπορούσαν να βοηθήσουν στην ψηφιακή σήμανση σε περίπτωση παραβίασης των συστημάτων. Τα επιπλέον στοιχεία/συμβάντα των αρχείων καταγραφής πρέπει να είναι:event source, date, username, timestamp, source addresses, destination addresses κ.α.

8.6 Συλλογή DNS Query Αρχείων Καταγραφής Ελέγχου (Audit Logs)

Συλλέξτε αρχεία καταγραφής ελέγχου για DNS αναζήτησης στα συστήματα(Server&PC) του οργανισμού οπού αυτό υποστηρίζεται και απαιτείται.

8.7 Συλλογή URL Request Αρχείων Καταγραφής Ελέγχου (Audit Logs)

Συλλέξτε αρχεία καταγραφής ελέγχου για URL Requests στα συστήματα(Server&PC) του οργανισμού οπού αυτό υποστηρίζεται/απαιτείται..

8.8 Συλλογή Αρχείων Καταγραφής Ελέγχου από Command Line

Συλλέξτε αρχεία καταγραφής ελέγχου για Command Line εργαλεία στα συστήματα(Server&PC) του οργανισμού. Για παράδειγμα cmd, powershell, bash..

8.9 Κεντρικοποίηση Αρχείων Καταγραφής Ελέγχου

Κεντρικοποίηστε στο μέγιστο βαθμό, την συλλογή και διατήρηση των αρχείων καταγραφής ελέγχου των συστημάτων(PC&Server) του οργανισμού.

8.10 Διατήρηση Αρχείων Καταγραφής Ελέγχου

Διατήρησε τα αρχεία καταγραφής ελέγχου των συστημάτων του οργανισμού για τουλάχιστον 90 μέρες.

8.11 Επιθεώρηση Αρχείων Καταφανής Ελέγχου

Επιθεωρήστε τα αρχεία καταγραφής ελέγχου σε τακτά χρονικά διαστήματα, τουλάχιστον μια φορά την εβδομάδα. Η επιθεώρηση έχει ως σκοπό τον εντοπισμό μη συνηθισμένων συμβάντων τα οποία μπορεί να συντελούν μια απειλή για το πληροφοριακό σύστημα του οργανισμού.
Η συλλογή αρχείων καταγραφής δεν αρκεί, θα πρέπει σε τακτά χρονικά διαστήματα να γίνεται επιθεώρηση αυτών έτσι ώστε να εντοπιστούν τυχόν κυβερνοεπίθεσεις και παραβιάσεις συστημάτων.

8.12 Συλλογή Αρχείων Καταγραφής από Παρόχους Υπηρεσιών

Συλλέξτε αρχεία καταγραφής παρόχων υπηρεσιών, οπού αυτό υποστηρίζεται. Για παράδειγμα αρχεία καταγραφής: αυθεντικοποίησης, εξουσιοδότησης, δημιουργίας και διαγραφής δεδομένων.

## 09 Προστασία Ηλεκτρονικού Ταχυδρομείου (Email) και Περιηγητή Ιστού (Web Browser)

Αυξήστε τις δυνατότητες προστασίας και εντοπισμού από τις απειλές που μπορούν να προκύψουν μέσω email και web browser, μιας και προσφέρουν την κύρια πύλη εισόδου σε συσκευές τελικών χρηστών από κακόβουλες οντότητες.

9.1 Εξασφάλιση Χρήσης μόνο Υποστηριζόμενων Προγραμμάτων Περιήγησης Ιστότοπων και Ηλεκτρονικού Ταχυδρομείου

Εξασφαλίστε ότι στον οργανισμό χρησιμοποιούνται μόνο πλήρως υποστηριζόμενα προγράμματα email και web browser και αυτά μόνο με τις τελευταίες εκδόσεις τους.

9.2 Χρήση DNS Filtering

Χρησιμοποιήστε DNS Filtering, έτσι ώστε να αποτραπεί η φόρτωση κακόβουλων ιστοσελίδων.

9.3 Λειτουργία και Διαχείριση Δικτυακού URL filtering

Κάνετε χρήση και διαχείριση δικτυακού URL filtering έτσι ώστε να αποτραπεί η φόρτωση πιθανόν κακόβουλων ή μη εγκεκριμένων ιστότοπων. Το φιλτράρισμα μπορεί να εκτελεστεί με βάση την φήμη, την κατηγορία ή και μέσω μια λίστας ιστότοπων. Θα πρέπει να εφαρμόζεται για όλες τις εταιρικές συσκευές του οργανισμού.

9.4 Περιορισμός Μη Αναγκαίων ή Μη Εγκεκριμένων Πρόσθετων σε Προγράμματα Περιήγησης Ιστότοπων (web broswer) και Ηλεκτρονικού Ταχυδρομείου (email client)

Περιορίστε, απενεργοποιήστε ή απεγκαταστήστε οποιοδήποτε μη εγκεκριμένο ή μη αναγκαίο πρόσθετο

(plugin, addon, extension) σε email client και web browser.

9.5 Εφαρμογή Πολιτικής DMARC

Για τον μετριασμό λήψης παραποιημένων μηνυμάτων ηλεκτρονικού ταχυδρομείου εφαρμόστε την πολιτική DMARC, ξεκινώντας με την ενσωμάτωση SPF και DKIM.

9.6 Φραγή Μη Αναγκαίων Τύπων Αρχείων ως Επισυναπτόμενα

Εκτελέστε φραγή ορισμένων τύπων επισυναπτόμενων αρχείων τα οποία δεν χρειάζονται/είναι χρήσιμα στον οργανισμό, μέσω του email server.

9.7 Υλοποίηση και Διαχείριση Υπηρεσίας Προστασίας από Κακόβουλο Λογισμικό για Διακομιστές Ηλεκτρονικού Ταχυδρομείου (Email Server Anti-Malware Protection)

## 10 Προστασία από Κακόβουλο Λογισμικό

Πρόληψη και έλεγχος από εγκατάσταση, διάδοση και εκτέλεση κακόβουλου λογισμικού, κώδικα ή scripts σε εταιρικές συσκευές.

10.1 Εγκατάσταση και Διαχείριση Λογισμικού Antivirus

Εγκαταστήστε και διαχειριστείτε antivirus λογισμικό σε όλες τις συσκευές του οργανισμού.

10.2 Ρύθμιση Αυτομάτων Ενημερώσεων για το Λογισμικό Antivirus

Ρυθμίστε το λογισμικό antivirus ώστε να λαμβάνει αυτόματα ενημερώσεις definitions/signatures για τον εντοπισμό κακόβουλου λογισμικού σε όλες τις συσκευές του οργανισμού.

10.3 Απενεργοποίηση Αυτόματης Εκτέλεσης σε Συσκευές Αποθήκευσης USB

Απενεργοποιήστε την λειτουργία αυτόματης εκτέλεσης των συσκευές αποθήκευσης USB.

10.4 Ρύθμιση Αυτόματης Σάρωσης για Κακόβουλο Λογισμικό σε Συσκευές Αποθήκευσης USB

10.5 Ενεργοποίηση Δυνατοτήτων Anti-Exploitation

Ενεργοποιήστε δυνατότητες anti-exploitation σε λογισμικό και συσκευές του οργανισμού όπως: Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), Apple® System Integrity Protection (SIP) and Gatekeeper

10.6 Κεντρική Διαχείριση Λογισμικού Antivirus

Διαχειριστείτε κεντρικά τις εγκαταστάσεις και ρυθμίσεις λογισμικού antivirus του οργανισμού.

10.7 Χρήση Λογισμικού Συμπεριφοράς (Behavior-Based)

Χρησιμοποιήστε λογισμικό antivirus το οποίο προστατεύει το σύστημα με βάση την συμπεριφορά (συνδέσεις, πόρους) των προγραμμάτων.

# 11 Επαναφορά Δεδομένων

Υλοποιήστε και διαχειριστείτε πρακτικές και διαδικασίες επαναφοράς δεδομένων έτσι ώστε να είστε σε θέση να επαναφέρετε συστήματα στην αρχική κατάσταση, πριν από την εκτέλεση μιας επιτυχημένης κυβερνοεπίθεσης.

11.1 Καθιέρωση και Διαχείριση Διαδικασίας Επαναφοράς Δεδομένων

Καθιερώστε μια διαδικασία επαναφοράς δεδομένων. Στην διαδικασία καθορίστε τις ενέργειες για την λήψη αντιγράφων ασφαλείας και επαναφοράς δεδομένων (ποια συστήματα, ποια δεδομένα, ποια συχνότητα), την προτεραιότητα επαναφοράς και την ασφάλεια των αντιγράφων ασφαλείας. Επικαιροποιήστε την διαδικασία σε ετήσια βάση.

11.2 Διασφάλιση Εκτέλεσης Αυτοματοποιημένων Backup

Αυτοματοποιήστε την διαδικασία λήψης backup αρχείων. Λαμβάνετε backup σε εβδομαδιαία τουλάχιστον βάση ή και πιο συχνά ανάλογα με τον βαθμό ευαισθησίας και κρισιμότητας των δεδομένων.

11.3 Προστασία των Αντιγράφων Ασφαλείας

Προστατέψτε τα αντίγραφα ασφαλείας με αντίστοιχα μέτρα ασφαλείας, όπως τα δεδομένα που βρίσκονται στην «παραγωγή». Διαχωρίστε και κρυπτογραφήστε τα δεδομένα ανάλογα με τις απαιτήσεις.

11.4 Καθιέρωση και Συντήρηση μιας Απομονωμένης Μονάδας Αντιγράφων Ασφαλείας

Καθιερώστε και συντηρήστε μονάδα απομονωμένων αντιγράφων ασφαλείας. Τεχνικά αυτό σημαίνει να εκτελείτε ένα ακόμα backup, το οποίο μπορεί να αποθηκεύεται off-site (σε συστήματα σε άλλη γεωγραφική περιοχή), off-line (σε συστήματα απομονωμένα από το δίκτυο του οργανισμού ή και από το internet), είτε στο cloud (σε κάποια cloud υπηρεσία).

11.5 Δοκιμή Επαναφοράς Δεδομένων

Να εκτελείτε δοκιμαστικές επαναφορές δεδομένων από τα αντίγραφα ασφάλειας σε τακτά χρονικά διαστήματα. Διενεργήστε έλεγχο ακεραιότητας των αντιγράφων ασφαλείας σε περιοδική βάση.
Διενεργήστε δοκιμή επαναφοράς δεδομένων (restoration), ώστε να διασφαλίσετε ότι η λήψη αντιγράφων λειτουργεί με σωστό τρόπο.

# 12 Διαχείριση Δικτυακής Υποδομής

Διαχειριστείτε κατάλληλα τις δικτυακές συσκευές του οργανισμού έτσι ώστε να αποτρέψετε κυβερνοεπίθεσεις σε δικτυακές υπηρεσίες και πύλες εισόδου.

12.1 Έλεγχος Ενημερώσεων Δικτυακής Υποδομής

Βεβαιωθείτε ότι το λογισμικό και firmware των δικτυών συσκευών είναι καταλληλά ενημερωμένο σύμφωνα με τις οδηγίες του παρόχου, είτε η υποδομή βρίσκεται στους χώρους του οργανισμού είτε παρέχεται ως υπηρεσία network-as-a-service. Εκτελείτε ενημερώσεις δικτυακού εξοπλισμού σε μηνιαία τουλάχιστον βάση.

12.2 Σχεδίαση και Συντήρηση Ασφαλούς Αρχιτεκτονικής Δικτύου

Σχεδιάστε και συντηρήστε ασφαλή αρχιτεκτονική δικτύου η οποία θα περιλαμβάνει και θαδιευθετεί τουλάχιστον το διαχωρισμό(segregation) δικτυών, την αρχή ελάχιστων δικαιωμάτων και τη διασφάλιση διαθεσιμότητας των.

12.3 Ασφαλή Διαχείριση Δικτυακής Υποδομής

Διαμορφώστε και εφαρμόστε τα κατάλληλα μέτρα ασφάλειας στην δικτυακή υποδομή του οργανισμού. Αυτό αφορά για παράδειγμα την ενεργοποίηση πρωτοκόλλων HTTPS, SSH κ.α.

12.4 Καθιέρωση και Συντήρηση Διαγράμματος Δικτύου
Σχεδιάστε και συντηρήστε ένα διάγραμμα που χαρτογραφεί όλο το δίκτυο του οργανισμού. Να το ενημερώνετε όταν γίνονται αλλαγές στο δίκτυο ή όταν γίνεται αντικατάσταση συσκευών.

12.5 Κεντρικοποίηση Δικτυακής Ταυτοποίησης, Εξουσιοδότησης και Ελέγχου (Authentication, Authorization, and Auditing)
Συγκεντρώστε σε ένα συστήματα την ταυτοποίηση, την εξουσιοδότηση και τον έλεγχο του δικτύου του οργανισμού.(Centralized AAA).

12.6 Χρήση Ασφαλούς Διαχείρισης Δικτύου και Πρωτοκόλλων

Ενεργοποιήστε ασφαλή πρωτόκολλα επικοινωνίας και διαχείρισης (π.χ., 802.1X, Wi-Fi Protected Access 2 (WPA2) Enterprise or greater).Αυτό το μέτρο αφορά την χρήση ασφαλών πρωτοκόλλων μέσα στο δίκτυο του οργανισμού, όπως για παράδειγμα: 802.1X, Wi-Fi Protected Access, IPsec, HTTPS, SSL/TLS, SSH

12.7 Χρήση VPN Απομακρυσμένης Πρόσβασης και Σύνδεση σε Σύστημα AAA

Βεβαιωθείτε ότι οι τελικοί χρήστες συνδέονται μέσω του VPN στο δίκτυο του οργανισμού.

12.8 Καθιέρωση και Συντήρηση Διαχωρισμένης Υποδομής για Διαχειριστικές Εργασίες

Διαχωρίστε την υποδομή που απαιτείται για την διαχείριση από το κύριο κορμό του δικτύου. Αυτή η συγκεκριμένη υποδομή θα πρέπει να είναι απομονωμένη από το παγκόσμιο διαδίκτυο.

## 13 Συνεχής Παρακολούθηση και Προστασία Δικτύου

Υλοποίηση διαδικασιών και εργαλείων για τη συνεχή παρακολούθηση, έλεγχο και προστασία του δικτύου έναντι απειλών στην δικτυακή υποδομή και τελικούς χρήστες.

13.1 Κεντρικοποίηση Ειδοποιήσεων Ασφάλειας

Συγκεντρώστε κεντρικά τα αρχεία καταγραφής συμβάντων ασφαλείας όλων των συσκευών του οργανισμού για την καλύτερη συσχέτιση και ανάλυσης αυτών. Η καλύτερη πρακτική διαχείρισης είναι μέσω ενός SIEM (Security Information and Event Management system). Επίσης το συγκεκριμένο μέτρο ικανοποιεί και μια πλατφόρμα ανάλυσης αρχείων καταγραφής συμβάντων ασφάλειας.

13.2 Εγκατάσταση Host-Based Instruction Detection System

Εγκαταστήστε Host-Based Instruction Detection System στα συστήματα(Server) του οργανισμού.

13.3 Εγκατάσταση Network Instruction Detection System

Εγκαταστήστε Network Instruction Detection System στο δίκτυο του οργανισμού.

13.4 Έλεγχος Δικτυακής Κίνησης Μεταξύ Τμημάτων του Δικτύου

Φιλτράρετε/Ελέγξτε την δικτυακή κίνηση μεταξύ των τμημάτων(segments) του δικτύου του οργανισμού.

13.5 Διαχείριση Ελέγχου Πρόσβασης για τις Απομακρυσμένες Συσκευές του Οργανισμού

Ρυθμίστε κατάλληλα το δίκτυο, ώστε να ελέγχει τις προϋποθέσεις που πρέπει να πληρούν οι απομακρυσμένες συσκευές προκειμένου να συνδεθούν σε πόρους του πληροφοριακού συστήματος. Προσδιορίστε τον έλεγχο πρόσβασης με βάση: το εγκατεστημένο ενημερωμένο antivirus λογισμικό, τη συμφόρηση ρυθμίσεων συμφώνα με τις προκαθορισμένες πολιτικές του οργανισμού και την επιβεβαίωση ότι το λειτουργικό σύστημα και οι εγκατεστημένες εφαρμογές έχουν λάβει τις τελευταίες ενημερώσεις.

13.6 Συλλογή Αρχείων Καταγραφής Ροής Δικτύου

Συλλέξτε τα αρχεία καταγραφής ροής της κίνησης του δικτύου από τις δικτυακές συσκευές του οργανισμού.

13.7 Εγκατάσταση Host-Based Intrusion Prevention System

Εγκαταστήστε Host-Based Instruction Prevention System στα συστήματα(Server) του οργανισμού. Σε αυτό το σημείο συμπεριλαμβάνεται και Endpoint Detection & Response.

13.8 Εγκατάσταση Network Intrusion Prevention System

Εγκαταστήστε και λειτουργήστε ένα Network Intrusion Prevention σύστημα.

13.9 Υλοποίηση Ελέγχου Πρόσβασης σε Επίπεδο Θυρών Δικτύου

Υλοποιήστε έλεγχο πρόσβασης σε επίπεδο θυρών δικτύου με χρήση του 802.1x ή παρομοίου πρωτοκόλλου όπως και με certificates για την πιστοποίηση χρηστών και συσκευών.

13.10 Υλοποίηση Ελέγχου στο Επίπεδο Εφαρμογών του TCP/IP

Υλοποιήστε φιλτράρισμα της δικτυακής κίνηση μέσω ενός application layer firewall, proxy server ή gateway.

13.11 Ρύθμιση Επιπέδου Ειδοποιήσεων για Συμβάντα Ασφάλειας

Ρυθμίστε το επίπεδο ειδοποιήσεων των αρχείων καταγραφής συμβάντων ασφαλείας τουλάχιστον μια φορά τον μήνα.

## 14. Εκπαίδευση και Ευαισθητοποίηση σε Θέματα Κυβερνοασφάλειας

Καθιερώστε και συντηρήστε ένα πρόγραμμα εκπαίδευσης και ευαισθητοποίησης σε θέματα κυβερνοασφάλειας για τα όλα μέλη του οργανισμού. Στόχος είναι να παρέχει την κατάλληλη γνώση και δεξιότητες, έτσι ώστε να αυξηθεί το γενικότερο επίπεδο αντίληψης κυβερνοασφάλειας.

14.1 Καθιέρωση και Συντήρηση Προγράμματος Εκπαίδευσης και Ευαισθητοποίησης σε Θέματα Κυβερνοασφάλειας

Καθιερώστε και συντηρήστε ένα πρόγραμμα εκπαίδευσης και ευαισθητοποίησης. Ο στόχος του είναι να

εκπαιδεύσει το ανθρώπινο δυναμικό στην ασφαλή αλληλεπίδραση με τον IT εξοπλισμό και με τους πόρους (PC, υπηρεσίες, USB Storage, File share, cloud storage, Antivirus κ.α.) του οργανισμού. Η διεξαγωγή των εκπαιδεύσεων πρέπει να γίνεται κατά την πρόσληψη και τουλάχιστον μια φορά τον χρόνο. Να ενημερώνετε το πρόγραμμα σε ετήσια τουλάχιστον βάση ή και συχνότερα, εάν προκύψει επείγουσα ανάγκη.

14.2 Εκπαίδευση στην Αναγνώριση Επιθέσεων Κοινωνικής Μηχανικής

Η εκπαίδευση του ανθρώπινου δυναμικού θα έχει ως στόχο την αναγνώριση επιθέσεων κοινωνικής μηχανικής(πχ. Phishing, pre-texting, tailgating).

14.3 Εκπαίδευση στην Εφαρμογή Καλών Πρακτικών σε Θέματα Αυθεντικοποίησης

Η εκπαίδευση του ανθρώπινου δυναμικού έχει ως στόχο την καλύτερη διαχείριση πρακτικών αυθεντικοποίησης, π.χ. MFA οπού αυτό υποστηρίζεται, τη σύνθεση κωδικού πρόσβασης και τη γενική διαχείριση στοιχειών πρόσβασης (credentials).

14.4 Εκπαίδευση στην Εφαρμογή Καλών Πρακτικών σε Θέματα Διαχείρισης Δεδομένων (ευαίσθητων και μη)

14.5 Εκπαίδευση στην Αποφυγή Ακούσιας Έκθεσης Ευαίσθητων Δεδομένων

Η εκπαίδευση του ανθρώπινου δυναμικού θα έχει ως στόχο την αναγνώριση πιθανών αιτίων και την αποφυγή ακουσίας έκθεσης ευαίσθητων δεδομένων. Παραδείγματα θεμάτων μπορεί να είναι η λανθασμένη αποστολή μέσω email, η απώλεια φορητών μέσων αποθήκευσης, η δημοσίευση δεδομένων σε μη κατάλληλους ισότοπους ή σε ακατάλληλο κοινό.

14.6 Εκπαίδευση στην Αναγνώριση και Αναφορά Συμβάντων Κυβερνοασφάλειας

Εκπαιδεύστε το ανθρώπινο δυναμικό κατάλληλα, έτσι ώστε να είναι σε θέση να αναγνωρίζει ένα πιθανό συμβάν κυβερνοασφάλειας και να το αναφέρει στο αρμόδιο πρόσωπο/ομάδα/αρχή.

14.7 Εκπαίδευση στην Αναγνώριση και Αναφορά Έλλειψης Ενημερώσεων Ασφάλειας

Εκπαιδεύστε το ανθρώπινο δυναμικό κατάλληλα, έτσι ώστε να είναι σε θέση να αναγνωρίζει την έλλειψη ή αποτυχία εγκατάστασης ενημερώσεων ασφάλειας στις συσκευές (PC & κινητά τηλεφωνά) τους, αλλά και να ενημερώνει το κατάλληλο τμήμα πληροφορικής/υποστήριξης για την επιδιόρθωση.

14.8 Εκπαίδευση στην Ασφαλή Σύνδεση στον Παγκόσμιο Ιστό

Εκπαιδεύστε κατάλληλα το ανθρώπινο δυναμικό που εργάζεται εξ αποστάσεως, έτσι ώστε να είναι σε θέση να αναγνωρίζει τους κίνδυνους σύνδεσης μέσω μη ασφαλών δικτυών. Αυτό μπορεί να συμπεριλαμβάνει δημόσια σημεία σύνδεσης Wifi (wifi public access points), τη δικτυακή υποδομή στις οικίες των υπάλληλων κ.α..

14.9 Εκπαίδευση με Βάση Διακριτούς Οργανικούς Ρόλους

Να διεξάγονται εξειδικευμένες εκπαιδεύσεις με βάση του διακριτούς ρόλους των εργαζομένων μέσα στον οργανισμό. Για παράδειγμα, κατάλληλες εκπαιδεύσεις κυβερνοασφάλειας διαχειριστών συστημάτων πληροφορικής, OWASP Top10 εκπαιδεύσεις για την αναγνώριση και αποφυγή ευπαθειών στην ανάπτυξη εφαρμογών/λογισμικού για τους προγραμματιστές, προχωρημένες εκπαιδεύσεις ενάντια σε επιθέσεις κοινωνικής μηχανικής σε πρόσωπα με περισσότερες ή πιο συγκεντρωτικές ευθύνες και στη γραμματειακή υποστήριξη.

# 15 Διαχείριση Παρόχων Υπηρεσιών

Καθιερώστε και συντηρήστε μια διαδικασία αξιολόγησης των παρόχων υπηρεσιών, οι οποίοι αποθηκεύουν ή διαχειρίζονται ευαίσθητες πληροφορίες ή παρέχουν κρίσιμες υπηρεσίες για τον οργανισμό, ώστε να διασφαλιστεί ότι τα ευαίσθητα δεδομένα και οι κρίσιμες υπηρεσίες του οργανισμού προστατεύονται κατάλληλα.

15.1 Καθιέρωση και Συντήρηση Μητρώου Καταγραφής Παρόχων Υπηρεσιών

Καθιερώστε και συντηρήστε μια λίστα παρόχων υπηρεσιών. Συμπεριλάβετε μια κατηγορία και στοιχεία επικοινωνίας για τον καθένα. Επιθεωρήστε και ενημερώστε την λίστα σε ετήσια βάση ή και πιο σύντομα άμα προκύψει ανάγκη για αλλαγή.

15.2 Καθιέρωση και Συντήρηση Πολιτικής Διαχείρισης Παρόχων Υπηρεσιών

Καθιερώστε και συντηρήστε μια πολιτική διαχείρισης των παρόχων υπηρεσιών. Θα πρέπει να καθορίζει την κατηγοριοποίηση, την καταγραφή, την αξιολόγηση, την παρακολούθηση συμμόρφωσης, τον παροπλισμό των υπηρεσιών και το επίπεδο κυβερνοασφάλειας που πρέπει να τηρεί κάθε πάροχος υπηρεσιών. Επιθεωρήστε και ενημερώστε την πολιτική σε ετήσια βάση ή πιο σύντομά άμα προκύψει ανάγκη για αλλαγή.

15.3 Κατηγοριοποίηση Παρόχων Υπηρεσιών

Στη σύσταση της πολιτικής για τη διαχείριση των παρόχων υπηρεσιών (15.2) καθορίστε μια κατηγοριοποίηση αυτών των παρόχων. Επιβεβαιώστε ότι εμπεριέχει μία ή περισσότερες κατηγορίες, οι οποίες θα μπορούσαν να είναι: επίπεδο ευαισθησίας δεδομένων, πλήθος δεδομένων, επίπεδο διαθεσιμότητας, εφαρμογή νομοθεσιών, μεταφερόμενο ρίσκο. Επιθεωρήστε και ενημερώστε την κατηγοριοποίηση σε ετήσια βάση ή πιο σύντομα εάν προκύψει ανάγκη για αλλαγή.

15.4 Επιβεβαίωση Απαιτήσεων Ασφάλειας σε Παρεχόμενες Υπηρεσίες

Επιβεβαιώστε σε επίπεδο παρόχου υπηρεσιών ότι λαμβάνουν τα κατάλληλα μέτρα σε θέματα κυβερνοασφάλειας. Αυτά μπορεί να είναι: ελάχιστες απαιτήσεις ασφάλειας λογισμικού που χρησιμοποιείται, ενημέρωση σε περίπτωση συμβάντος κυβερνοασφάλειας και παραβίαση εμπιστευτικότητας δεδομένων, απαιτήσεις κρυπτογράφησης δεδομένων, κ.α. Αυτές οι απαιτήσεις πρέπει να συμπεριληφθούν στην πολιτική διαχείρισης παρόχων υπηρεσιών (15.2). Επιθεωρήστε και ενημερώστε την πολιτική σε ετήσια βάση ή πιο σύντομά, εάν προκύψει ανάγκη για αλλαγή

15.5 Αξιολόγηση Παρόχων Υπηρεσιών

Αξιολογήστε τη συνέπεια των παρόχων υπηρεσιών σε θέματα κυβερνοασφάλειας με βάση την πολιτική διαχείρισης παρόχων υπηρεσιών (15.2). Το πεδίο εφαρμογής της αξιολόγησης μπορεί να ποικίλλει σύμφωνα με την κατηγοριοποίηση που έχει οριστεί στην πολιτική και μπορεί να περικλείει τυποποιημένες εκθέσεις αξιολόγησης όπως: Service Organization Control 2 (SOC 2), Payment Card Industry,(PCI) Attestation of Compliance (AoC), ερωτηματολόγια, ή άλλες διαδικασίες αξιολόγησης. Εκτελείτε την αξιολόγηση σε ετήσια βάση ή πιο συχνά άμα προκύψει ανάγκη.

15.6 Παρακολούθηση Παρόχων Υπηρεσιών

Παρακολούθηση των παρόχων υπηρεσιών σύμφωνα με την πολιτική διαχείρισης παρόχων υπηρεσιών

(15.2) που έχει συσταθεί. Η παρακολούθηση μπορεί να γίνεται μέσω της επαναξιολόγησης συμμόρφωσης με βάση τα συμβόλαια, τον οδηγό λειτουργίας/συμβόλαιο παροχής και το dark web monitoring.

15.7 Ασφαλής και Ελεγχόμενος Παροπλισμός Παρεχόμενων Υπηρεσιών

Ορίστε και διασφαλίστε διαδικασία για τον ασφαλή και ελεγχόμενο παροπλισμό των υπηρεσιών του παρόχου. Αυτή μπορεί να αφορά την απενεργοποίηση λογαριασμών χρηστών και πρόσβασης, τον τερματισμό ροών δεδομένων, την ελεγχόμενη και ασφαλή διαγραφή δεδομένων που ήταν αποθηκευμένα στην υποδομή του παρόχου.

## 16 Ασφάλεια Λογισμικού

Διαχειριστείτε και συντηρήστε διαδικασίες για την ασφάλεια λογισμικού, είτε αυτό αναπτύχθηκε είτε πρόκειται για προμηθευόμενο λογισμικό.

16.1 Καθιέρωση και Συντήρηση Διαδικασίας Ασφαλούς Ανάπτυξης Λογισμικού

Καθιερώστε και συντηρήστε μια διαδικασία ασφαλούς ανάπτυξης λογισμικού. Στην διαδικασία καταγράψτε θέματα όπως: αρχές ασφαλές αρχιτεκτονικής λογισμικού, πρακτικές ασφαλούς προγραμματισμού, εκπαιδεύεις προγραμματιστών, διαχείριση ευπαθειών, ασφάλεια κώδικα αναπτυγμένο εκτός οργανισμού και διαδικασίες ελέγχου λογισμικού. Επιθεωρήστε και ενημερώστε την διαδικασία σε ετήσια βάση ή πιο σύντομά εάν προκύψει ανάγκη για αλλαγή.

16.2 Καθιέρωση και Συντήρηση Διαδικασίας Διευθέτησης και Αποδοχής Ευπαθειών λογισμού

Καθιερώστε και συντηρήστε μια διαδικασία διευθέτησης και πιθανής αποδοχής ευπαθειών λογισμικού συμπεριλαμβάνοντας ένα σύστημα/μέσο/πλατφόρμα για αναφορά ευπαθειών από εξωτερικές πήγες. Η διαδικασία θα αποτελείται από: μία πολιτική χειρισμού ευπαθειών που προσδιορίζει την διαδικασία αναφορών, μία υπεύθυνη ομάδα για το χειρισμό αναφορών ευπαθειών και μια διαδικασία για την εισαγωγή, ανάθεση, αποκατάσταση και έλεγχο αποκατάστασης. Ως μέρος της διαδικασίας

χρησιμοποιήστε ένα σύστημα παρακολούθησης ευπαθειών, το οποίο θα συμπεριλαμβάνει ταξινόμηση βαρύτητας (severity ratings) και στοιχεία για τη μέτρηση χρονικών διαστημάτων για τον εντοπισμό, την ανάλυση και την αποκατάσταση των ευπαθειών. Επιθεωρήστε και ενημερώστε τη διαδικασία σε ετήσια βάση ή πιο σύντομά, εάν προκύψει ανάγκη για αλλαγή.

16.3 Εφαρμογή Ανάλυσης/Εξακρίβωσης Βαθύτερων Αίτιων για Ευπάθειες Ασφάλειας σε Λογισμό

Εφαρμόστε τηνι ανάλυση βαθύτερων αιτίων για τις ευπάθειες. . Όταν αναλύετε μια ευπάθεια πρέπει να εκτελείται και έλεγχος των βαθύτερων αίτιων που οδήγησαν στην εκδήλωση μιας ή περισσοτέρων ευπαθειών σε επίπεδο κώδικα, έτσι ώστε να υπάρχει πλήρη εικόνα της ευπάθειας και των επιπτώσεων της.

16.4 Καθιέρωση και Συντήρηση Μητρώου Καταγραφής Παρεχόμενου Λογισμικού

Καθιερώστε και συντηρήστε ένα μητρώο που θα καταγράφεται το λογισμικό/ ο κώδικας που έχει αναπτυχθεί από παράγοντες εκτός οργανισμού. Θα πρέπει να αναφέρεται και μια εκτίμηση ρίσκου για κάθε εγγραφή του μητρώου. Επιθεωρήστε και ενημερώστε το μητρώο τουλάχιστον σε μηνιαία βάση ή πιο σύντομά, άμα προκύψει ανάγκη για αλλαγή, και αξιολογήστε εάν το λογισμικό υποστηρίζεται

16.5 Χρήση Ενημερωμένου Λογισμικού και Προμηθευόμενο από Επίσημες και Έμπιστες Πήγες

Το λογισμικό ή ο κώδικας που χρησιμοποιείτε από εξωτερικές πήγες θα πρέπει να είναι ενημερωμένο και

από έμπιστες/διαπιστευμένες πήγες. Εφόσον είναι δυνατόν, χρησιμοποιήστε δοκιμασμένο λογισμικό και δοκιμασμένες βιβλιοθήκες , που έχουν ελεγχθεί σε θέματα ασφάλειας. Προμηθευτείτε το λογισμικό από έμπιστες πήγες ή ελέγξτε το λογισμικό για ευπάθειες.

16.6 Καθιέρωση και Συντήρηση Συστήματος Ταξινόμηση Βαρύτητας (Severity Rating)

Καθιερώστε και συντηρήστε ένα σύστημα ταξινόμησης βαρύτητας για τις ευπάθειες των λογισμικών έτσι ώστε να είναι δυνατή η ιεράρχηση τους με στόχο την προτεραιοποίηση των επιδιορθώσεων. Θέστε ένα ελάχιστο όριο αποδοχής ρίσκου ευπαθειών κατά την παραγωγή κώδικα και εφαρμογών. Η ταξινόμηση βαρύτητας εισάγει έναν τρόπο διαλογής των ευπαθειών, γεγονός που βελτιώνει την διαχείριση ρίσκου προτεραιοποιώντας την επιδιόρθωση ευπαθειών. Επιθεωρήστε και ενημερώστε το σύστημα/διαδικασία σε ετήσια βάση.

16.7 Χρήση Προτύπων Βελτιστοποίησης Διαμόρφωσης Ασφάλειας για τα Συστήματα Εφαρμογών (Application Servers)

Χρησιμοποιήστε αναγνωρισμένα πρότυπα βελτιστοποίησης ασφάλειας ρυθμίσεων για συστήματα εφαρμογών. Αυτό περιλαμβάνει συστήματα άμεσα συνδεδεμένα σε συστήματα εφαρμογών, συστήματα βάσεων δεδομένων, web server και μονάδες cloud containers, PaaS , SaaS.

16.8 Διαχωρισμός Συστημάτων Παραγωγής

Διαχωρίστε συστήματα παραγωγής από μη παραγωγικά συστήματα.

16.9 Εκπαίδευση Προγραμματιστών στις Αρχές Ασφαλούς Προγραμματισμού

Διασφαλίστε ότι όλοι οι προγραμματιστές του οργανισμού λαμβάνουν την απαραίτητη εκπαίδευση σύμφωνα με το προγραμματιστικό περιβάλλον και τη θέση ευθύνης που καλύπτουν. Η εκπαίδευση μπορεί να καλύπτει γενικές αρχές κυβερνοασφάλειας και ασφάλειας λογισμικού. Επαναλάβετε τις εκπαιδεύσεις σε ετήσια βάση και διαμορφώστε το εκπαιδευτικό πρόγραμμα έτσι ώστε να είναι σε θέση να αναπτύξει μια κουλτούρα κυβερνοασφάλειας μεταξύ της ομάδας των προγραμματιστών.

16.10 Εφαρμογή Αρχών Αρχιτεκτονικής Ασφάλειας στην Ανάπτυξη Λογισμικού

Εφαρμόστε αρχές αρχιτεκτονικής ασφάλειας στην ανάπτυξη λογισμικού. Οι αρχές αρχιτεκτονικής ασφάλειας περιλαμβάνουν τη λογική των ελάχιστων δικαιωμάτων και την επιβολή ελέγχου κάθε εισόδου που ένας χρήστης έχει την δυνατότητα να εκτέλεσει προωθώντας την λογική “never trust user input” Συμπεριλαμβάνοντας τη διαδικασία «explicit error checking» καθώς και τεκμηρίωση αυτών για όλες τις μορφές εισόδου, όπως μέγεθος και τύπος δεδομένων, αποδεκτά όρια τιμών των μεταβλητών και formats. Ασφαλής σχεδιασμός σημαίνει επίσης ελαχιστοποίηση της εκτεθειμένης επιφάνειας για επιθέσεις όπως απενεργοποίηση απροστάτευτων δικτυακών θυρών και υπηρεσιών, διαγραφή μη χρήσιμων ή μη χρησιμοποιουμένων εφαρμογών και αρχείων και μετονομασία ή απομάκρυνση προεπιλεγμένων λογαριασμών.

16.11 Αξιοποίηση Γνωστών Μηχανισμών ή Υπηρεσιών Ασφάλειας στο Λογισμικό που Αναπτύσσετε

Αξιοποιήστε γνωστούς μηχανισμούς ή υπηρεσίας για της ενότητες του λογισμικού που αναπτύσσετε, όπως: identity management, κρυπτογράφηση, μητρώο ελέγχου(audit logs) και καταγραφής(logs). Η χρήση έτοιμων υλοποιήσεων από προγραμματιστικές πλατφόρμες σε κρίσιμες συναρτήσεις ασφάλειας μπορεί να μειώσει το φόρτο εργασίας των προγραμματιστών και την πιθανότητα σφαλμάτων σχεδιασμού και υλοποίησης. Τα σύγχρονα λειτουργικά σύστημα παρέχουν αποτελεσματικούς μηχανισμούς αναγνώρισης, ταυτοποίησης και εξουσιοδότησης και παρέχουν αυτούς τους μηχανισμούς σε εφαρμογές. Κάνετε χρήση

γνωστών και ενημερωμένων προτύπων κρυπτογράφησης. Επίσης τα λειτουργικά συστήματα παρέχουν δυνατότητες χρήσης μητρώων καταγραφής και ελέγχου.

16.12 Εφαρμογή Ελέγχων Ασφαλείας σε Επίπεδο Κώδικα

Ενσωματώστε εργαλεία στατικής και δυναμικής ανάλυσης στον κύκλο ζωής μιας εφαρμογής για να βεβαιωθείτε ότι τηρούνται ασφαλείς πρακτικές προγραμματισμού.

16.13 Διεξαγωγή Ελέγχου Εισβολής Εφαρμογών

Εκτελέστε διεξαγωγή ελέγχου εισβολής εφορμών. Για κρίσιμες εφαρμογές είναι προτιμότερο να εκτελείτε ο έλεγχος εισβολής από ταυτοποιημένο χρήστη έτσι ώστε να μεγιστοποιηθεί η αποτελεσματικότητά και να εντοπιστούν ευπάθειες επιχειρησιακής λογικής(Business Logic Vulnerabilities) έναντι της σάρωσης κώδικα και πρακτικές αυτοματοποιημένου ελέγχου εισβολής.

# 17 Διαχείριση Ανταπόκρισης Περιστατικών Ασφάλειας (Incident Response Management)

Καθιερώστε και συντηρήστε μια διαδικασία ανταπόκρισης και διαχείρισης περιστατικών ασφάλειας (πολικές, playbooks, πλάνα ανταπόκρισης, ορισμός ρόλων, εκπαίδευση, επικοινωνία) για την βέλτιστη προετοιμασία, αναγνώριση και ανταπόκριση σε μια κυβερνοεπίθεση.

17.1 Ανάθεση Προσωπικού στην Διαχείριση Περιστατικών

Ορίστε ένα άτομο κλειδί και ένα επιπλέον σε εφεδρεία, τα οποία θα διαχειρίζονται την διαδικασία ανταπόκρισης σε περιστατικά ασφάλειας. Αυτά τα άτομα θα είναι υπεύθυνα για τον συγχρονισμό και την τεκμηρίωση της ανταπόκρισης καθώς και την ανάκαμψη από περιστατικά ασφάλειας και μπορούν να προέρχονται από το προσωπικό του οργανισμού, από εξωτερικούς συνεργάτες ή να προτιμηθεί μια υβριδική λύση. Σε περίπτωση που ανατίθεται σε εξωτερικό συνεργάτη θα πρέπει να οριστεί ένας υπάλληλος του οργανισμού που θα έχει την επίβλεψη. Επιθεωρήστε και ενημερώστε την διαδικασία σε ετήσια βάση ή πιο σύντομά άμα προκύψει ανάγκη για αλλαγή.

17.2 Καθιέρωση και Συντήρηση Στοιχείων Επικοινωνίας για Αναφορά Περιστατικών Ασφάλειας

Καθιερώστε και συντηρήστε μια λίστα στοιχείων επικοινωνίας ατόμων που πρέπει να ενημερωθούνε σε περίπτωση περιστατικού ασφάλειας. Η λίστα μπορεί να συμπεριλαμβάνει υπαλλήλους/στελέχη του οργανισμοί, εξωτερικούς συνεργάτες, νομική αντιπροσώπευση, τις αρμόδιες αρχές(π.χ. Δίωξη Ηλεκτρονικού Εγχύματος, αρμόδιο υπουργείο, CSIRT), ασφαλιστικούς παρόχους ή και άλλους ενδιαφερόμενους. Επιθεωρήστε και ενημερώστε την λίστα σε τουλάχιστον ετήσια βάση ή πιο σύντομά, άμα προκύψει ανάγκη για αλλαγή.

17.3 Καθιέρωση και Συντήρηση Διαδικασίας Αναφοράς Περιστατικών για τον Οργανισμό

Καθιερώστε και συντηρήστε μια διαδικασία αναφοράς περιστατικών κυβερνοασφάλειας για όλα τα μέλη του οργανισμού. Η διαδικασία θα συμπεριλαμβάνει χρονικό περιθώριο αναφοράς, προϊστάμενο του ατόμου που κάνει την αναφορά, μηχανισμό αναφοράς και την ελάχιστη απαιτούμενη πληροφορία για την αναφορά. Η διαδικασία θα πρέπει να είναι διαθέσιμη σε όλο το προσωπικό του οργανισμού. Επιθεωρήστε και ενημερώστε την διαδικασία σε ετήσια βάση ή πιο σύντομά, εάν προκύψει ανάγκη για αλλαγή.

17.4 Καθιέρωση και Συντήρηση Διαδικασίας Ανταπόκρισης σε Περιστατικό Κυβερνοασφάλειας

Καθιερώστε και συντηρήστε διαδικασία ανταπόκρισης σε περιστατικό ασφάλειας η οποία θα καθορίζει ρόλους και ευθύνες, απαιτήσεις συμμόρφωσης και πλανά επικοινωνίας. Επιθεωρήστε και ενημερώστε την διαδικασία σε ετήσια βάση ή πιο σύντομά εάν προκύψει ανάγκη για αλλαγή.

17.5 Ανάθεση Ρόλων και Ευθυνών

Αναθέστε κατάλληλους ρόλους κλειδιά και ευθύνες για την ανταπόκριση σε περιστατικά, αποτελούμενο από ένα ή περισσότερα άτομα του προσωπικού των τμημάτων: νομικό τμήμα, IT, κυβερνοασφάλεια, εγκαταστάσεις, δημοσίων σχέσεων, ανθρωπίνου δυναμικό, ανταπόκριση περιστατικών και αναλυτές ασφάλειας, εφόσον υφίστανται. Επιθεωρήστε και ενημερώστε την ανάθεση σε ετήσια βάση ή πιο σύντομά εάν προκύψει ανάγκη για αλλαγή.

17.6 Ορισμός Μέσων Επικοινωνίας κατά την Διάρκεια Διαδικασίας Ανταπόκρισης Περιστατικού ασφάλειας

Καθορίστε τα μέσα επικοινωνίας κατά την διάρκεια διαδικασίας ανταπόκρισης περιστατικού ασφάλειας. Τα μέσα μπορεί να αποτελούν η τηλεφωνική επικοινωνία, το email, οι επιστολές κ.α. Λάβετε υπόψιν ότι κατά την διαδικασία ανταπόκρισης και ανάκαμψης κάποιο μέσο μπορεί να μην είναι διαθέσιμο ή να μην θεωρείται δεδομένη η εμπιστευτικότητα του. Επιθεωρήστε και ενημερώστε σε ετήσια βάση ή πιο σύντομά άμα προκύψει ανάγκη για αλλαγή.

17.7 Διεξαγωγή Ασκήσεων Προσομοίωσης Κυβερνοεπιθέσεων

Προγραμματίστε σε τουλάχιστον ετήσια βάση ασκήσεις που θα προσομοιώνουν αληθινές κυβερνοεπίθεσεις διαφόρων κατηγοριών, με στόχο την εξάσκηση του προσωπικού που βρίσκονται σε ρόλους κλειδιά στην διαδικασία ανταπόκρισης σε περιστατικά κυβερνοασφάλειας. Στις ασκήσεις αξιολογήστε τα κανάλια επικοινωνίας, τη λήψη αποφάσεων και τις ροές καθηκόντων.

17.8 Ανασκόπηση Μετά την Ολοκλήρωση των Περιστατικών Ασφάλειας

Μετα το τέλος ενός περιστατικού ασφάλειας κάντε μια ανασκόπηση και μια αξιολόγηση για την καλύτερη κατανόηση της απειλής και της διαδικασίας. Εξάγετε συμπεράσματα και βρείτε κενά ή βελτιώστε τις πολιτικές /διαδικασίες/playooks ανταπόκρισης σε περιστατικά κυβερνοασφάλειας.

17.9 Καθιέρωση και Συντήρηση Κλίμακας Ταξινόμησης Περιστατικών Κυβερνοασφάλειας

Καθιερώστε και συντηρήστε κλίμακες ταξινόμησης για περιστατικά ασφάλειας, κατά το ελάχιστο διαχωρίζοντας τα περιστατικά από τα συμβάντα. Παραδείγματα μπορούν να αποτελούν: η μη κανονική δραστηριότητα, η ευπάθεια ασφάλειας, τα αδύναμα σημεία ασφάλειας, η έκθεση ευαίσθητων δεδομένων, περιστατικό εμπιστευτικότητας κ.α. Επιθεωρήστε και ενημερώστε την ανάθεση σε ετήσια βάση ή πιο σύντομά εάν προκύψει ανάγκη για αλλαγή.

# 18 Έλεγχος Εισβολής Δικτυών και Συστημάτων (Penetration Testing)

Ελέγξτε τα μέτρα ασφαλείας και ανθεκτικότητας (προσωπικό, διαδικασίας, τεχνολογίες) που έχετε λάβει για την προστασία του πληροφοριακού συστήματος μέσω της προσομοίωσης κυβερνοεπιθέσεων, η οποία έχει ως στόχο την αναγνώριση και εκμετάλλευση όλων των ευπαθειών των συστημάτων και δικτυών.

18.1 Καθιερώστε και Συντηρήστε ένα Πρόγραμμα Ελέγχου Εισβολής Δικτυών και Συστημάτων

Καθιερώστε σε τουλάχιστον ετήσια βάση ελέγχους εισβολής στο πληροφοριακό σύστημα του οργανισμού ανάλογα με το μέγεθος, το επίπεδο ωριμότητας και το πόσο σύνθετο είναι. Πρέπει να οριστεί η στοχοθέτηση: δίκτυο, συστήματα, διαδικτυακές εφαρμογές, API, υπηρεσίες, μέτρα ασφάλειας εγκαταστάσεων

18.2 Περιοδική Διεξαγωγή Εξωτερικού Ελέγχου Εισβολής

Ο εξωτερικός έλεγχος εισβολής συμπεριλαμβάνει αναγνώριση, σάρωση, εντοπισμό και εκμετάλλευση πληροφοριών και ευπαθειών του πληροφοριακού συστήματος ανάλογα με την στοχοθέτηση. Ο έλεγχος πρέπει να εκτελείται από ειδικευμένη ομάδα ατόμων και να διαχωρίζεται σε blackbox και whitebox.

18.3 Επιδιόρθωση Ευρημάτων ελέγχου Εισβολής

Επιδιορθώστε τα ευρήματα του ελέγχου σύμφωνα με την αναφορά και τις πολικές του οργανισμού.

18.4 Επικύρωση Μέτρων Ασφάλειας

Επικυρώστε τα μέτρα ασφάλειας μετά από κάθε έλεγχο εισβολής δικτύων και συστημάτων αναλόγως με τα αποτελέσματα, τροποποιήστε κανόνες και μηχανισμούς ασφάλειας για την βέλτιστη ανταπόκριση.

18.5 Περιοδική Διεξαγωγή Εσωτερικού Ελέγχου Εισβολής

Διεξάγετε σε ετήσια τουλάχιστον βάση εσωτερικό έλεγχο εισβολής συστημάτων. Δηλαδή η ειδικευμένη ομάδα θα προσπαθήσει να εισβάλει από το εσωτερικό του δικτύου του πληροφοριακού συστήματος του οργανισμού. Διαχωρίστε σε Whitebox και Blackbox.

# ΠΑΡΑΡΤΗΜΑ Β' – Αντιστοίχιση Μέτρων Προστασίας CIS με το Άθροισμα Τεχνικών MITRE Att&ck που Μετριάζουν – Master Mapping Περίληψη

| CIS Safeguards ALL IG | Maped Mitre Attack Techniques | CIS Safeguards ALL IG | Maped Mitre Attack Techniques |
|---|---|---|---|
| 4.1 | 342 | 16.11 | 6 |
| 6.1 | 217 | 2.1 | 4 |
| 6.2 | 217 | 2.2 | 4 |
| 18.3 | 212 | 2.4 | 4 |
| 6.8 | 206 | 4.1 | 4 |
| 4.7 | 188 | 9.4 | 4 |
| 18.5 | 187 | 9.7 | 4 |
| 5.4 | 164 | 10.3 | 4 |
| 5.3 | 155 | 12.1 | 4 |
| 2.5 | 101 | 12.7 | 4 |
| 2.7 | 81 | 13.5 | 4 |
| 3.3 | 75 | 3.4 | 3 |
| 4.2 | 73 | 8.5 | 3 |
| 2.3 | 67 | 8.11 | 3 |
| 4.8 | 54 | 12.5 | 3 |
| 12.2 | 51 | 14.5 | 3 |
| 13.3 | 51 | 14.9 | 3 |
| 13.8 | 51 | 16.12 | 3 |
| 7.5 | 50 | 18.1 | 3 |
| 5.2 | 47 | 1.1 | 2 |
| 7.6 | 39 | 1.2 | 2 |
| 7.7 | 39 | 15.7 | 2 |
| 12.8 | 36 | 1.4 | 1 |
| 3.12 | 34 | 4.9 | 1 |
| 6.5 | 33 | 9.1 | 1 |
| 6.4 | 31 | 12.6 | 1 |
| 13.4 | 29 | 13.9 | 1 |
| 18.2 | 28 | 1.3 | 0 |
| 2.6 | 27 | 1.5 | 0 |
| 7.1 | 27 | 3.5 | 0 |
| 7.2 | 27 | 3.7 | 0 |
| 11.3 | 27 | 3.8 | 0 |

| | | | |
|---|---|---|---|
| 14.1 | 25 | 3.9 | 0 |
| 7.3 | 24 | 3.13 | 0 |
| 9.3 | 23 | 3.14 | 0 |
| 13.7 | 21 | 4.3 | 0 |
| 11.4 | 20 | 4.11 | 0 |
| 13.2 | 19 | 4.12 | 0 |
| 16.1 | 19 | 5.6 | 0 |
| 3.1 | 18 | 6.6 | 0 |
| 6.3 | 17 | 6.7 | 0 |
| 14.2 | 17 | 8.4 | 0 |
| 14.6 | 17 | 8.6 | 0 |
| 7.4 | 16 | 8.7 | 0 |
| 5.5 | 15 | 8.8 | 0 |
| 14.3 | 14 | 8.12 | 0 |
| 4.5 | 13 | 9.5 | 0 |
| 16.9 | 13 | 10.4 | 0 |
| 3.11 | 12 | 10.6 | 0 |
| 16.8 | 12 | 12.3 | 0 |
| 3.1 | 11 | 12.4 | 0 |
| 10.5 | 11 | 13.1 | 0 |
| 11.1 | 11 | 13.6 | 0 |
| 11.2 | 11 | 13.11 | 0 |
| 11.5 | 11 | 14.7 | 0 |
| 16.13 | 10 | 14.8 | 0 |
| 5.1 | 9 | 15.1 | 0 |
| 9.6 | 9 | 15.2 | 0 |
| 14.4 | 9 | 15.3 | 0 |
| 3.2 | 8 | 15.4 | 0 |
| 8.1 | 8 | 15.5 | 0 |
| 8.2 | 8 | 15.6 | 0 |
| 8.3 | 8 | 16.6 | 0 |
| 9.2 | 8 | 16.7 | 0 |
| 13.1 | 8 | 16.1 | 0 |
| 10.1 | 7 | 16.14 | 0 |
| 10.7 | 7 | 17.1 | 0 |
| 3.6 | 6 | 17.2 | 0 |
| 4.6 | 6 | 17.3 | 0 |
| 8.9 | 6 | 17.4 | 0 |

| | | | |
|---|---|---|---|
| 8.1 | 6 | 17.5 | 0 |
| 10.2 | 6 | 17.6 | 0 |
| 16.2 | 6 | 17.7 | 0 |
| 16.3 | 6 | 17.8 | 0 |
| 16.4 | 6 | 17.9 | 0 |
| 16.5 | 6 | 18.4 | 0 |

## ΠΑΡΑΡΤΗΜΑ Γ' – Reverse Mapping

| CIS Safeguards ALL IG | Malware | Ransomeware | Web App Hacking | Insider and Privilege Misuse | Targeted Intrusion |
|---|---|---|---|---|---|
| 1.1 | | | | | |
| 1.2 | | | | | |
| 1.3 | | | | | |
| 1.4 | | | | | |
| 1.5 | | | | | |
| 2.1 | 3 | 3 | 1 | 2 | 3 |
| 2.2 | 3 | 3 | 1 | 2 | 3 |
| 2.3 | 30 | 31 | 22 | 18 | 18 |
| 2.4 | 3 | 3 | 1 | 2 | 3 |
| 2.5 | 35 | 40 | 30 | 21 | 26 |
| 2.6 | 2 | 7 | 10 | 2 | 7 |
| 2.7 | 12 | 28 | 19 | 9 | 17 |
| 3.1 | 3 | 6 | 2 | 11 | 6 |
| 3.2 | 3 | 5 | 1 | 8 | 4 |
| 3.3 | 13 | 23 | 9 | 28 | 24 |
| 3.4 | 3 | 1 | 1 | 3 | 2 |
| 3.5 | | | | | |
| 3.6 | | | | | |
| 3.7 | | | | | |
| 3.8 | | | | | |
| 3.9 | | | | | |
| 3.1 | 7 | 5 | 4 | 9 | 6 |
| 3.11 | 1 | 5 | 4 | 10 | 8 |

| CIS Safeguards ALL IG | Malware | Ransomeware | Web App Hacking | Insider and Privilege Misuse | Targeted Intrusion |
|---|---|---|---|---|---|
| 3.12 | 9 | 18 | 13 | 15 | 19 |
| 3.13 | | | | | |
| 3.14 | | | | | |

| | | | | | |
|---|---|---|---|---|---|
| 4.1 | 79 | 94 | 71 | 54 | 82 |
| 4.2 | 20 | 18 | 18 | 9 | 16 |
| 4.3 | | | | | |
| 4.4 | 20 | 20 | 16 | 11 | 19 |
| 4.5 | 6 | 7 | 6 | 2 | 6 |
| 4.6 | 1 | 1 | 2 | 1 | |
| 4.7 | 55 | 60 | 41 | 40 | 68 |
| 4.8 | 25 | 30 | 22 | 3 | 21 |
| 4.9 | 1 | | | | 1 |
| 4.1 | 3 | 2 | 4 | 4 | 2 |
| 4.11 | | | | | |
| 4.12 | | | | | |
| 5.1 | | 5 | 3 | 5 | 3 |
| 5.2 | 21 | 21 | 16 | 16 | 25 |
| 5.3 | 52 | 58 | 37 | 36 | 66 |
| 5.4 | 49 | 56 | 34 | 36 | 62 |
| 5.5 | 7 | 8 | 4 | 5 | 8 |
| 5.6 | | | | | |
| 6.1 | 62 | 70 | 47 | 45 | 75 |
| 6.2 | 62 | 70 | 48 | 45 | 75 |
| 6.3 | 8 | 8 | 9 | 12 | 7 |
| 6.4 | 13 | 11 | 14 | 14 | 13 |
| 6.5 | 14 | 12 | 14 | 15 | 13 |
| 6.6 | | | | | |
| 6.7 | | | | | |
| 6.8 | 55 | 68 | 41 | 43 | 68 |
| 7.1 | 9 | 15 | 10 | 7 | 11 |
| 7.2 | 9 | 15 | 10 | 7 | 11 |
| 7.3 | 8 | 14 | 9 | 7 | 11 |
| 7.4 | 6 | 13 | 4 | 5 | 8 |
| 7.5 | 8 | 14 | 9 | 8 | 10 |
| 7.6 | 13 | 17 | 18 | 1 | 9 |
| 7.7 | 13 | 15 | 18 | 2 | 8 |

| CIS Safeguards ALL IG | Malware | Ransomeware | Web App Hacking | Insider and Privilege Misuse | Targeted Intrusion |
|---|---|---|---|---|---|
| 8.1 | 3 | 1 | 1 | 4 | 3 |
| 8.2 | 3 | 2 | 1 | 4 | 3 |
| 8.3 | 4 | 2 | 2 | 4 | 3 |

| | | | | | |
|---|---|---|---|---|---|
| 8.4 | | | | | |
| 8.5 | | | | | 1 |
| 8.6 | | | | | |
| 8.7 | | | | | |
| 8.8 | | | | | |
| 8.9 | 2 | 1 | 1 | 3 | 4 |
| 8.1 | 3 | 1 | 1 | 3 | 3 |
| 8.11 | | | | 0 | 1 |
| 8.12 | | | | | |
| 9.1 | 1 | 1 | 1 | | |
| 9.2 | 3 | 1 | | | 3 |
| 9.3 | 16 | 13 | 6 | 6 | 10 |
| 9.4 | 2 | 2 | 1 | | |
| 9.5 | | | | | |
| 9.6 | 7 | 9 | 3 | 3 | 5 |
| 9.7 | 4 | 4 | 1 | 3 | 4 |
| 10.1 | 6 | 7 | 2 | 4 | 6 |
| 10.2 | 6 | 7 | 2 | 4 | 6 |
| 10.3 | 1 | 1 | 1 | 4 | |
| 10.4 | | | 8 | | |
| 10.5 | 7 | 11 | | 1 | 6 |
| 10.6 | | | | | |
| 10.7 | 5 | 7 | 2 | 4 | 6 |
| 11.1 | | 3 | | 7 | 2 |
| 11.2 | | | | 7 | 2 |
| 11.3 | 6 | 9 | 4 | 16 | 11 |
| 11.4 | 5 | 7 | 2 | 12 | 8 |
| 11.5 | | 3 | | 7 | 2 |
| 12.1 | 1 | 1 | 1 | | 1 |
| 12.2 | 17 | 20 | 14 | 8 | 16 |

| CIS Safeguards ALL IG | Malware | Ransomeware | Web App Hacking | Insider and Privilege Misuse | Targeted Intrusion |
|---|---|---|---|---|---|
| 12.2 | 17 | 20 | 14 | 8 | 16 |
| 12.3 | | | | | |
| 12.4 | | | | | |

| | | | | | |
|---|---|---|---|---|---|
| 12.5 | | | | | |
| 12.6 | | | | | |
| 12.7 | 3 | 4 | 3 | 2 | 2 |
| 12.8 | 18 | 18 | 11 | 13 | 17 |
| 13.1 | | | | | |
| 13.2 | 12 | 13 | 3 | 4 | 9 |
| 13.3 | 31 | 28 | 4 | 2 | 25 |
| 13.4 | 9 | 7 | 7 | 3 | 7 |
| 13.5 | 3 | 4 | 3 | 1 | 2 |
| 13.6 | | | | | |
| 13.7 | 12 | 13 | 4 | 4 | 9 |
| 13.8 | 31 | 28 | 6 | 2 | 25 |
| 13.9 | | | | | |
| 13.1 | 7 | 7 | 4 | | 5 |
| 13.11 | | | | | |
| 14.1 | 13 | 16 | 3 | 6 | 9 |
| 14.2 | 7 | 12 | 2 | 2 | 4 |
| 14.3 | 10 | 7 | 5 | 7 | 8 |
| 14.4 | 3 | 3 | 3 | 5 | 3 |
| 14.5 | | 1 | | 3 | |
| 14.6 | 7 | 12 | 2 | 2 | 4 |
| 14.7 | | | | | |
| 14.8 | | | | | |
| 14.9 | 2 | 2 | 1 | 3 | 2 |
| 15.1 | | | | | |
| 15.2 | | | | | |
| 15.3 | | | | | |
| 15.4 | | | | | |
| 15.5 | | | | | |

| CIS Safeguards ALL IG | Malware | Ransomeware | Web App Hacking | Insider and Privilege Misuse | Targeted Intrusion |
|---|---|---|---|---|---|
| 15.6 | | | | | |
| 15.7 | | 1 | 1 | 2 | |
| 16.1 | 13 | 11 | 4 | 11 | 10 |

| | | | | | |
|---|---|---|---|---|---|
| 16.2 | | 2 | 2 | 3 | 2 |
| 16.3 | | 2 | 3 | 3 | 2 |
| 16.4 | | 2 | 1 | 3 | 2 |
| 16.5 | | 2 | 1 | 3 | 2 |
| 16.6 | | | | | |
| 16.7 | | | | | |
| 16.8 | 5 | 7 | 6 | 4 | 5 |
| 16.9 | 9 | 9 | 3 | 9 | 8 |
| 16.1 | 10 | 12 | 8 | 7 | 9 |
| 16.11 | | 2 | 1 | 3 | 2 |
| 16.12 | | 2 | 1 | 3 | 2 |
| 16.13 | 4 | 5 | 6 | 1 | 6 |
| 16.14 | | | | | |
| 17.1 | | | | | |
| 17.2 | | | | | |
| 17.3 | | | | | |
| 17.4 | | | | | |
| 17.5 | | | | | |
| 17.6 | | | | | |
| 17.7 | | | | | |
| 17.8 | | | | | |
| 17.9 | | | | | |
| 18.1 | 2 | 2 | 1 | | 2 |
| 18.2 | 11 | 11 | 10 | 1 | 6 |
| 18.3 | 65 | 78 | 62 | 53 | 62 |
| 18.4 | | | | | |
| 18.5 | 56 | 72 | 55 | 53 | 58 |

# ΠΑΡΑΤΗΜΑ Δ' – Συστάσεις Κυβερνοασφάλειας

## Control 01

1.1 Δημιουργία και Διαχείριση Λεπτομερούς Μητρώου Αγαθών(hardware assets)

Σε αρχικό στάδιο μπορεί να χρησιμοποιηθεί ένα απλό υπολογιστικό φύλλο, στην συνέχεια να μεταφερθεί και να συντηρηθεί σε μια βάση δεδομένων ή σε αυτοματοποιημένο σύστημα που θα καλύπτει και τα άλλα αντίμετρα της ενότητας "CIS μέτρο 01". Στην καταγραφή μπορεί να συνδράμει το λογιστήριο ή και το τμήμα προμήθειων του οργανισμού. Τα απαραίτητα πεδία που πρέπει να καταγραφούν είναι:
- οι διευθύνσεις δικτύου των συσκευών (εφόσον είναι στατικές)
- διευθύνσεις MAC
- ονομασία συσκευής
-έκδοση/μοντέλο
- υπεύθυνος(owner) του αγαθού
- τμήμα
- ημερομηνία έναρξης της λειτουργίας διότι είναι πρέπει να γίνεται κατάλληλη
διαχείριση του κύκλου ζωής των παγίων/συσκευών αυτών ανάλογα με την πολιτική ασφάλειας του οργανισμού.
-Τοποθεσία
-Ταξινόμηση ανάλογα με την κρισιμότητα του αγαθού
Σκοπός είναι ***η διαμόρφωση πλήρους αντίληψης για το εύρος των αγαθών και τα αναγκαία μέτρα προστασίας και συντήρησής τους.***
Βοηθητικοί σύνδεσμοι:
https://www.isms.online/iso-27001/how-to-develop-an-asset-inventory-for-iso-27001/
https://manageengine.com/products/asset-explorer/asset-inventory-management.html
https://www.cybergrx.com/resources/research-and-insights/blog/smb-cybersecurity-series-asset-inventory-is-the-foundation-of-cybersecurity
https://www.rapid7.com/blog/post/2017/03/02/the-cis-critical-controls-explained-control-1-inventory-of-authorized-and-unauthorized-devices/
https://www.assetpanda.com/
https://www.axonius.com/
https://divvycloud.com/
https://www.itil-docs.com/blogs/asset-management/it-asset-management-process

1.2 Διευθέτηση Μη Εξουσιοδοτημένων Συσκευών

Πρέπει να καθοριστεί μια διαδικασία/πολιτική απαγόρευσης/αποτροπής σύνδεσης μη εξουσιοδοτημένων συσκευών στο δίκτυο του οργανισμού. Και να ενισχυθεί τεχνικά μέσω της εγκαταστάτης Domain Controller,μέσω εργαλείων διαχείρισης δικτύου ή μέσω της παρακολούθησης του αρχείου καταγραφής του συστήματος DHCP ή μέσω αποτροπής της σύνδεσης με χρήση Firewall.
https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview
https://www.comparitech.com/net-admin/network-monitoring-tools/
https://www.rapid7.com/blog/post/2017/03/02/the-cis-critical-controls-explained-control-1-inventory-of-authorized-and-unauthorized-devices/

1.3 Ενσωμάτωση Ενεργητικού(active) Εργαλείου Αναγνώρισης Συσκευών

Αυτό το μέτρο μπορεί να υλοποιηθεί με την χρήση συστήματος διαχείρισης δικτύων.
Το εργαλείο σαρώνει το δίκτυο για συσκευές. Μειονέκτημα είναι η αυξημένη κίνηση στο δίκτυο.

Πλεονέκτημα η εύκολη χρήση και ρύθμιση.
https://www.softwaresuggest.com/blog/best-it-asset-discovery-tools/#
https://www.comparitech.com/net-admin/network-monitoring-tools/
https://www.automationworld.com/products/data/blog/13319123/choosing-between-passive-or-active-asset-discovery

1.4 Χρήση Αρχείων Καταγραφής DHCP για την Ενημέρωση του Μητρώου Καταγραφής Αγαθών(hardware assets) του Οργανισμού.

Απαιτείται η χρήση αρχείων καταγραφής DHCP για την ενημέρωση του μητρώου καταγραφής παγίων/συσκευών του οργανισμού.
https://docs.rapid7.com/nexpose/discovering-assets-through-dhcp-log-queries/
https://www.manageengine.com/products/eventlog/dhcp-server-auditing-monitoring-on-windows-and-linux.html
https://www.rapid7.com/blog/post/2017/03/02/the-cis-critical-controls-explained-control-1-inventory-of-authorized-and-unauthorized-devices/

1.5 Χρήση Παθητικών(passive) Εργαλείων Αναγνώρισης Συσκευών

Εγκατάσταση εργαλείου εντοπισμού(passive) δικτυακών συσκευών .
Το εργαλείο λαμβάνει και καταγράφει δικτυακή κίνηση “broadcast”.
Εργαλεία:
https://www.spiceworks.com/homepage/
https://cybersecurity.att.com/products/ossim
https://www.open-audit.org/
https://www.opennms.com/
https://www.automationworld.com/products/data/blog/13319123/choosing-between-passive-or-active-asset-discovery

## Control 02

2.1 Δημιουργία και Διαχείριση Λεπτομερούς Μητρώου Καταγραφής Λογισμικού

Συστάσεις/ Βοηθητικοί σύνδεσμοι:
Σε αρχικό στάδιο μπορεί να χρησιμοποιηθεί ένα απλό υπολογιστικό φύλλο, στην συνέχεια να μεταφερθεί και να διατηρηθεί σε μια βάση δεδομένων.
Τα απαραίτητα πεδία που πρέπει να καταγράφουν είναι:
- ονομασία
- διανομέας
- ημερομηνία εγκατάστασης
- σκοπός λειτουργίας
- έκδοση
- URL
- μηχανισμός εγκατάστασης
- ημερομηνία διαγράφης
-υπεύθυνος (owner) του αγαθού
https://www.sciencedirect.com/topics/computer-science/software-inventory
https://www.manageengine.com/products/desktop-central/software-inventory.html
https://www.rapid7.com/blog/post/2017/02/23/the-cis-critical-controls-explained-control-2-inventory-of-authorized-and-unauthorized-software/

Μια βέλτιστη μέθοδος διαχείρισης :
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-126r3.pdf

2.2 Έλεγχος Υποστήριξης Λογισμικού

Σύσταση διαδικασίας ελέγχου και διαχείρισης λογισμικού.
Κατά την διαδικασία θα πρέπει να διασφαλίζεται ότι τα εν χρήση λογισμικά λαμβάνουν ενημερώσεις και υποστηρίζονται από τον αρμόδιο διανομέα. Αποσύρετε λειτουργικά συστήματα και εφαρμογές για τα οποία έχει σταματήσει η υποστήριξη από τον πάροχο.
Σε περίπτωση που αυτό δεν είναι δυνατόν, θα πρέπει να ορίζονται αντίμετρα, να γίνεται αξιολόγηση ρίσκου και άμα είναι εφικτό να δρομολογείται η αντικατάσταση του λογισμικού.
Εκτελέστε τον έλεγχο με βάση το μητρώο καταγραφής λογισμικού. Χρησιμοποιήστε ως βασική πηγή ενημέρωσης τις επίσημες ιστοσελίδες των παρόχων/διανομέων λογισμικού ή απευθυνθείτε στην τεχνική του υποστήριξη. Μια βέλτιστη μέθοδος διαχείρισης :
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-126r3.pdf

2.3 Διευθέτηση Μη Εξουσιοδοτημένου Λογισμικού

Σύσταση πολιτικής και διαδικασίας ελέγχου εγκαταστάτης μη εξουσιοδοτημένου λογισμικού. Συντηρήστε μια λίστα απαγορευμένων\μη εξουσιοδοτημένων εφαρμογών/λογισμικών. Διασφαλίστε ότι οι χρήστες δεν έχουν local administrator δικαιώματα στον υπολογιστή τους.
Σε περίπτωση που κριθεί αναγκαία η εγκατάσταση ενός λογισμικού που βρίσκεται στην λίστα των απαγορευμένων\μη εξουσιοδοτημένων εφαρμογών/λογισμικών, θα πρέπει να καταγράφει και να γίνει αξιολόγηση ρίσκου λειτουργίας του συγκεκριμένου λογισμικού και άμα κριθεί αναγκαίο να παρθούν κατάλληλα αντίμετρα.
Εργαλεία:
https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/applocker/applocker-overview
https://www.techtarget.com/searchwindowsserver/definition/Microsoft-System-Center-Configuration-Manager-2012
https://www.manageengine.com/application-control/remove-admin-rights.html
https://www.manageengine.com/products/desktop-central/software-inventory.html
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/microsoft-defender-endpoint?view=o365-worldwide
https://www.rapid7.com/blog/post/2017/02/23/the-cis-critical-controls-explained-control-2-inventory-of-authorized-and-unauthorized-software/

2.4 Αυτοματοποίηση Καταγραφής Λογισμικού με Χρήση Κατάλληλου Εργαλείου.

Εγκαταστήστε κατάλληλο σύστημα αυτοματοποιημένης διαχείρισης και καταγραφής λογισμικού
Παραδείγματα εργαλείων:
https://www.network-inventory-advisor.com/best-software-inventory-tools.html
https://www.techtarget.com/searchwindowsserver/definition/Microsoft-System-Center-Configuration-Manager-2012
https://www.manageengine.com/products/desktop-central/software-inventory.html
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/microsoft-defender-endpoint?view=o365-worldwide
https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/applocker/applocker-overview
https://www.rapid7.com/blog/post/2017/02/23/the-cis-critical-controls-explained-control-2-inventory-of-authorized-and-unauthorized-software/

2.5 Σύσταση Λίστας Επιτρεπόμενων Εφαρμογών

Εφαρμόστε με τεχνικά μέτρα μια λίστα εφαρμογών που επιτρέπονται να εκτελεστούν. Η συγκεκριμένη διαδικασία απαιτεί αρκετό χρόνο δοκιμών μιας και κάποιες εφαρμογές δεν εκτελούνται σε καθημερινή βάση.
Παραδείγματα εργαλείων :
https://www.bleepingcomputer.com/tutorials/create-an-application-whitelist-policy-in-windows/
https://www.cert.govt.nz/it-specialists/critical-controls/application-allowlisting/implementing-application-whitelisting/
https://www.rapid7.com/blog/post/2017/02/23/the-cis-critical-controls-explained-control-2-inventory-of-authorized-and-unauthorized-software/

https://blogs.manageengine.com/corporate/general/2018/10/25/application-whitelisting-using-software-restriction-policies.html
https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/applocker/applocker-overview

2.6 Σύσταση Λίστας Επιτρεπόμενων Βιβλιοθηκών

Εφαρμόστε τεχνικά μέτρα για την σύσταση λίστας βιβλιοθηκών που επιτρέπονται να χρησιμοποιηθούν
Παραδείγματα εργαλείων :
https://www.bleepingcomputer.com/tutorials/create-an-application-whitelist-policy-in-windows/
https://www.cert.govt.nz/it-specialists/critical-controls/application-allowlisting/implementing-application-whitelisting/
https://blogs.manageengine.com/corporate/general/2018/10/25/application-whitelisting-using-software-restriction-policies.html
https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/applocker/applocker-overview
https://www.rapid7.com/blog/post/2017/02/23/the-cis-critical-controls-explained-control-2-inventory-of-authorized-and-unauthorized-software/
https://social.technet.microsoft.com/Forums/Azure/en-US/7b2edad6-82da-4761-ade6-9b11636bfc09/how-to-disable-a-dll-file-using-group-policy?forum=winserverDS

2.7 Σύσταση Λίστας Επιτρεπόμενων scripts
Εφαρμόστε με τεχνικά μέτρα μια λίστα επιτρεπόμενων scripts που θα επιτρέπεται να εκτελεστούν σε PC και Server. Μπορείτε να χρησιμοποιήστε συναρτήσεις κατακερματισμού.
Παραδείγματα εργαλείων :
https://www.bleepingcomputer.com/tutorials/create-an-application-whitelist-policy-in-windows/
https://www.cert.govt.nz/it-specialists/critical-controls/application-allowlisting/implementing-application-whitelisting/
https://blogs.manageengine.com/corporate/general/2018/10/25/application-whitelisting-using-software-restriction-policies.html
https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/applocker/applocker-overview
https://www.rapid7.com/blog/post/2017/02/23/the-cis-critical-controls-explained-control-2-inventory-of-authorized-and-unauthorized-software/
https://virtualengine.co.uk/using-software-restriction-policies-to-block-scripts/

## Control 03

3.1 Δημιουργία και Διαχείριση Διαδικασίας Διαχείρισης Δεδομένων
Οι πολίτικες που πρέπει να καθοριστούν είναι οι εξής:

- Ταξινόμηση κρισιμότητας δεδομένων
- Ιδιοκτήτης (owner)/Υπεύθυνος δεδομένων
- Γενικός χειρισμός δεδομένων
- Χρονικά όρια διατήρησης/αποθήκευσης δεδομένων
- Πολιτική συμμόρφωσης συμφώνων και νομικών πλαισίων σχετικά με την προστασία προσωπικών δεδομένων και δεδομένων πελατών
- Προϋποθέσεις διαγραφής δεδομένων

https://gsu.uts.edu.au/policies/data-governance-policy.html
https://www.komprise.com/glossary_terms/data-management-policy/
https://assets.contentstack.io/v3/assets/blt36c2e63521272fdc/bltab7d19ca9100e50e/5e9ddae7674ec260f325c3ca/data_breach_response.pdf
https://cloud.netapp.com/blog/clc-blg-data-governance-policy-4-foundational-policies

Κάποια πρότυπα άλλων πολιτικών:
https://www.sans.org/information-security-policy/

3.2 Δημιουργία και Διαχείριση Μητρώου Καταγραφής Δεδομένων

Σε ένα αρχικό στάδιο μπορεί να χρησιμοποιηθεί ένα απλό υπολογιστικό φύλλο, στην συνέχεια να μεταφερθεί και να συντηρηθεί σε μια βάση δεδομένων . Τα συμπεριλαμβανόμενα πεδία είναι :
- ονομασία της ομαδοποίησης δεδομένων ή του project
- καθορισμός κρισιμότητας δεδομένων
- καθορισμός υπευθύνου(owner)/ιδιοκτήτη δεδομένων
- καθορισμός περιορισμών χειρισμού δεδομένων
- όρια και νομικές δεσμεύσεις διατήρησης/αποθήκευσης δεδομένων
- προϋποθέσεις διαγραφής δεδομένων

https://labs.centerforgov.org/data-governance/data-inventory/
https://blog.pagefreezer.com/what-is-data-inventory-data-mapping
https://bigid.com/blog/data-inventory/

3.3 Ρύθμιση Λίστας Ελέγχου Πρόσβασης Δεδομένων

Μπορεί να συνταχθεί και σε ένα απλό υπολογιστικό φύλλο ως λίστα, ωστόσο ο έλεγχος πρόσβασης θα πρέπει να εφαρμόζεται με τεχνικά μέσα.
Σε δίκτυα/πληροφοριακά συστήματα οργανισμών όπου η διαχείριση γίνεται μέσω Domain Controller, οι προσβάσεις σε δεδομένα μπορεί να διευθετούνται μέσω “Security Groups”. Κάτι αντίστοιχο προσφέρεται και σε Linux/Unix περιβάλλον.
Κάθε εμπορική εφαρμογή, κάθε σύστημα διαχείρισης βάσεων δεδομένων ή cloud περιβάλλον προσφέρουν λειτουργία διαχείρισης δικαιωμάτων και εξουσιοδότησης αρκεί να διαμορφωθούν κατάλληλα.
https://docs.microsoft.com/en-us/windows/security/identity-protection/access-control/active-directory-security-groups
https://docs.oracle.com/cd/E19859-01/820-3252-11/FP44ucgACL.html
https://docs.microsoft.com/en-us/azure/storage/blobs/data-lake-storage-access-control

3.4 Διατήρηση Δεδομένων

Δημιουργήστε και συντηρήστε μια λίστα για κάθε σετ/ομάδα δεδομένων και δηλώστε τα χρονικά όρια

που έχουν οριστεί από την διαδικασία διαχείρισης δεδομένων του οργανισμού σας. Η λίστα αρχικά μπορεί να είναι ένα απλό υπολογιστικό φύλλο και στην συνέχεια κάποια εφαρμογή που αποστέλλει αναφορές κατάστασης. Μπορεί επίσης να ενσωματωθεί στο μητρώο καταγραφής δεδομένων.
https://www.r2docuo.com/en/how-to-enforce-your-data-retention-policy-through-automation
https://kirkpatrickprice.com/blog/best-practices-for-data-retention/

3.5 Ασφαλής Διαγραφή Δεδομένων

Ένα οποιοδήποτε αρχείο, είτε πρόκειται για κείμενο, είτε για μουσική, είτε για ταινία είτε για οτιδήποτε άλλο, είναι δεδομένα. Είναι δηλαδή ένα σύνολο από πληροφορίες, δομημένες με συγκεκριμένο τρόπο ώστε να γίνονται κατανοητές από τα προγράμματα με τα οποία διαβάζουμε τα αρχεία αυτά. Αυτές οι πληροφορίες κωδικοποιούνται με βάση ένα συγκεκριμένο τρόπο, μετατρέπονται σε αριθμούς και αποθηκεύονται στο δίσκο μας (ή όποιο μέσο αποθήκευσης χρησιμοποιούμε) ως μία σειρά 0 και 1.

Διαγράφοντας ένα αρχείο από τον υπολογιστή μας, ακόμα και να αδειάσουμε τον κάδο ανακύκλωσης, δεν διαγράφουμε πραγματικά τα δεδομένα από τον δίσκο. Αυτό που διαγράφουμε είναι η αναφορά στα δεδομένα αυτά. Το λειτουργικό μας σύστημα δεν μπαίνει στη διαδικασία να σβήσει τα 0 και 1,που αναφέραμε προηγουμένως, από το σκληρό δίσκο. Απλά μαρκάρει το χώρο που καταλαμβάνεται από τα δεδομένα του αρχείου που διαγράψαμε ως αχρησιμοποίητο. Έτσι, το αρχείο συνεχίζει να υπάρχει στο δίσκο, ακόμα και αν δεν εμφανίζεται στο λειτουργικό μας σύστημα και θα συνεχίσει να υπάρχει μέχρις ότου κάποιο άλλο αρχείο γραφτεί στο χώρο που βρισκόταν το παλιό μας αρχείο.
https://kirkpatrickprice.com/blog/secure-data-destruction-guide/
https://www.securitymagazine.com/articles/89540-clear-purge-destroy-when-data-must-be-eliminated-part-2
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf
https://files.eric.ed.gov/fulltext/ED585293.pdf
https://www.certcoop.eu/wp-content/uploads/2019/04/Secure_file_deletion.ogv

3.6 Κρυπτογράφηση δεδομένων σε συσκευές χρηστών

Κρυπτογράφηση ονομάζουμε τη διαδικασία κωδικοποίησης της πληροφορίας, ώστε να παρεμποδίζεται η ανάγνωσή της από μη εξουσιοδοτημένα μέρη.

Η ισχύς της κρυπτογράφησης επιτυγχάνεται με το μέγιστο μήκος του κλειδιού (bits) και τον αλγόριθμο κρυπτογράφησης που χρησιμοποιείται.

Για να “σπάσει” η κρυπτογράφηση, θα πρέπει να δοκιμαστούν όλα τα πιθανά κλειδιά. Αλλά πλέον το μήκος των κλειδιών κρυπτογράφησης έχει κάνει αυτή την προσέγγιση αναποτελεσματική. Εφαρμόστε τεχνολογίες κρυπτογράφησης στις τελικές συσκευές των χρηστών . Απαιτείται μια δομημένη προσέγγιση μιας και πρέπει τα recovery keys να φυλάσσονται κατάλληλα. Οι απλοί χρήστες είναι εύκολο να απωλέσουν recovery key ή να ξεχάσουν το κωδικό πρόσβασης. Μια λύση θα αποτελούσε ένα κεντρικό σύστημα διαχείρισης κρυπτογράφησης τερματικών. Μια υλοποίηση της Microsoft:
https://docs.microsoft.com/en-us/microsoft-desktop-optimization-pack/mbam-v25/
Άλλοι σύνδεσμοι:
https://csrc.nist.gov/publications/detail/sp/800-111/final
https://docs.microsoft.com/en-us/mem/intune/protect/encrypt-devices
https://docs.microsoft.com/en-us/windows/security/information-protection/bitlocker/bitlocker-overview
https://www.kernel.org/doc/html/latest/admin-guide/device-mapper/dm-crypt.html
https://www.certcoop.eu/wp-content/uploads/2019/04/Veracrypt_use.ogv
https://docs.microsoft.com/en-us/azure/security/fundamentals/data-encryption-best-practices

3.7 Καθιέρωση και Διαχείριση Κατηγοριοποίησης Δεδομένων

Ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων (**GDPR**) ενεργοποιείται από τις 25 Μαΐου 2018. Ένα από τα βασικά ζητήματα για έναν οργανισμό είναι να κατηγοριοποιήσει τα δεδομένα

προσωπικού χαρακτήρα σε τουλάχιστον ευαίσθητα και μη ευαίσθητα. Παρατίθεται η κατηγοριοποίηση Προσωπικών Δεδομένων όπως έχουν χαρακτηριστεί και εκδοθεί από την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα.
https://www.niriis.gr/gdpr/katigories-prosopikon-dedomenon/
https://www.imperva.com/learn/data-security/data-classification/
https://docs.microsoft.com/en-us/azure/information-protection/what-is-information-protection
https://kirkpatrickprice.com/blog/classifying-data/#:~:text=Typically%2C%20there%20are%20four%20classifications,only%2C%20confidential%2C%20and%20restricted

3.8 Καταγραφή Ροής Δεδομένων

Ένα διάγραμμα ροής δεδομένων (DFD) χαρτογραφεί τη ροή πληροφοριών για οποιαδήποτε διαδικασία ή σύστημα. Χρησιμοποιεί καθορισμένα σύμβολα όπως ορθογώνια, κύκλους και βέλη, καθώς και σύντομες ετικέτες κειμένου, για να εμφανίζει τις εισόδους δεδομένων, τις εξόδους, τα σημεία αποθήκευσης και τις διαδρομές μεταξύ κάθε προορισμού. Τα διαγράμματα ροής δεδομένων μπορεί να κυμαίνονται από απλές, ακόμη και χειρόγραφες επισκοπήσεις διεργασιών, έως σε βάθος- πολλαπλών επιπέδων DFD που εξετάζουν σταδιακά και βαθύτερα τον τρόπο χειρισμού των δεδομένων. Μπορούν να χρησιμοποιηθούν για την ανάλυση ενός υπάρχοντος συστήματος ή για τη μοντελοποίηση ενός νέου. Όπως όλα τα διαγράμματα και τα γραφήματα, ένα DFD μπορεί συχνά να εκφράσει οπτικά, πράγματα που θα ήταν δύσκολο να εξηγηθούν με λόγια και αφορούν τόσο το τεχνικό όσο και το μη τεχνικό κοινό, από τον προγραμματιστή εώς τον CEO. Γι' αυτό τα DFD παραμένουν τόσο δημοφιλή μετά από τόσα χρόνια.
Μπορείτε να χρησιμοποιήσετε το διάγραμμα δικτύου και τα μητρώα καταγραφής υλικού/λογισμικού για βοήθεια.
https://www.lucidchart.com/pages/data-flow-diagram
https://blog.hubspot.com/marketing/data-flow-diagram

3.9 Κρυπτογράφηση δεδομένων σε αφαιρούμενα μέσα αποθήκευσης

Κρυπτογραφήστε δεδομένα σε αφαιρούμενα μέσα αποθήκευσης, πχ USB συσκευές, εξωτερική σκληρή δίσκοι, SD κάρτες.
Το μέτρο μπορεί να ενισχυθεί τεχνικά και μέσω Group Policy: https://docs.microsoft.com/en-us/windows/security/information-protection/bitlocker/bitlocker-group-policy-settings#bkmk-driveaccess2
Άλλοι βοηθητικοί σύνδεσμοι:
https://security.berkeley.edu/data-encryption-removable-media-guideline
https://www.winmagic.com/encryption-solutions/removable-media-encryption-rme-rmce
https://protonmail.com/blog/usb-encryption/
https://security.utexas.edu/iso-policies/approved-encryption-methods/removable-media

3.10 Κρυπτογράφηση στην Μεταφορά Ευαίσθητων Δεδομένων μέσω δικτύου

Η ασφαλής αποστολή πληροφοριών μέσω του διαδικτύου αποτελεί θεμελιώδη αρχή για το ηλεκτρονικό εμπόριο, την ιατρική και άλλες ευαίσθητες συναλλαγές. Για αυτές και πολλές ακόμα χρήσεις, θεωρείται κρίσιμο ζήτημα οι μεταδιδόμενες πληροφορίες να μην παραβιάζονται, αλλά και να μη διαβάζονται από οποιονδήποτε άλλον εκτός από τον αποστολέα και τον παραλήπτη. Τα χαρακτηριστικά αυτά αποτελούν βασικό κομμάτι της ανάπτυξης του διαδικτύου και είναι εξαιρετικά κρίσιμα για πολλές καινοτόμες χρήσεις. Αν και η προέλευση της ευρύτατα χρησιμοποιούμενης τεχνολογίας, που παρέχει ασφάλεια επιπέδου στις μεταφορές δεδομένων μέσω διαδικτύου, εντοπίζεται εδώ και 20 χρόνια στο SSL, η τελευταία ολοκληρωμένη έκδοση TLS 1.3 είναι μια σημαντική αναθεώρηση που σχεδιάστηκε για το σύγχρονο Internet. Το πρωτόκολλο αυτό φέρνει σημαντικές βελτιώσεις στους τομείς της ασφάλειας, των επιδόσεων και της ιδιωτικότητας.
https://security.berkeley.edu/data-encryption-transit-guideline

https://www.webhostingsecretrevealed.net/el/blog/web-business-ideas/an-ssl-tls-certificate-buyers-guide/
https://docs.microsoft.com/en-us/mem/configmgr/core/plan-design/security/enable-tls-1-2-server
https://www.sslmarket.com/ssl/help-ssl-certificate-installation
https://www.openssl.org/
https://developer.visa.com/pages/trusted_certifying_authorities

3.11 Κρυπτογράφηση Αποθηκευμένων/Αρχειοθετημένων Ευαίσθητων Δεδομένων
Συστάσεις/ Βοηθητικοί σύνδεσμοι:
https://en.wikipedia.org/wiki/Data_at_rest
https://blog.iinfosec.com/securing-data-at-rest-with-encryption
https://www.endpointprotector.com/blog/how-to-protect-your-data-at-rest/
https://docs.microsoft.com/en-us/azure/security/fundamentals/encryption-atrest

3.12 Διαχωρισμός Επεξεργασίας και Αποθήκευσης Δεδομένων Βασισμένη στην Ευαισθησία αυτών

Διαχωρίστε την επεξεργασία και αποθήκευση δεδομένων ανάλογα με το βαθμό ευαισθησίας.
Ορίστε συστήματα τα οποία θα επεξεργάζονται ευαίσθητα δεδομένα. Αυτά τα συστήματα δεν θα πρέπει να επεξεργάζονται και δεδομένα πιο χαμηλών βαθμίδων ευαισθησίας. Π.χ. οι κατηγορίες «Ευαίσθητα», «Εμπιστευτικά», «Δημόσια». Τα συστήματα που επεξεργάζονται δεδομένα της κατηγόριας «Δημόσια» δεν θα πρέπει να επεξεργάζονται δεδομένα και της κατηγορίας «Ευαίσθητα».
https://www.datamation.com/security/data-segmentation/
https://www.unifiedcompliance.com/products/search-controls/control/1289/

3.13 Χρήση Λογισμικού για Αποτροπή Απώλειας Δεδομένων

Οι εξωτερικές επιθέσεις ή οι εσωτερικές απειλές είναι αναπόφευκτες, αλλά οι διαρροές, η απώλεια και η κλοπή δεδομένων μπορούν να μετριαστούν. Μια λύση DLP (Data Loss Prevention) με επίγνωση περιεχομένου μπορεί να επιθεωρεί και να ελέγχει τις μεταφορές αρχείων που περιέχουν ευαίσθητες πληροφορίες, όπως προσωπικά δεδομένα ή πνευματική ιδιοκτησία, να διαχειρίζεται ποιες συσκευές αποθήκευσης USB μπορούν ή δεν μπορούν να χρησιμοποιηθούν και να διασφαλίζει ότι χρησιμοποιείται η επιβεβλημένη κρυπτογράφηση.
https://blog.netwrix.com/2019/07/16/10-best-practices-essential-for-your-data-loss-prevention-dlp-policy/
https://docs.microsoft.com/en-us/microsoft-365/compliance/dlp-overview-plan-for-dlp?view=o365-worldwide
https://www.mcafee.com/enterprise/es-es/security-awareness/data-protection/choose-dlp-solution.html

3.14 Συντήρηση Μητρώου Καταγραφής Πρόσβασης Δεδομένων

Η διατήρηση και ο έλεγχος αρχείων καταγραφής πρόσβασης σε ευαίσθητα δεδομένα μπορεί να παρέχει αποδεικτικά στοιχεία για το πώς συνέβη ένα περιστατικό ασφάλειας.
https://www.dataguardstore.com/Sensitive-Data-Auditing.asp
https://www.sap.com/documents/2015/07/ce47288f-5b7c-0010-82c7-eda71af511fa.html

## Control 04

4.1 Δημιουργία και Συντήρηση Διαδικασίας Ασφαλούς Διαμόρφωσης Εξοπλισμού

Αποτελεί ένα από τα πιο σημαντικά μέτρα του πλαισίου CIS, δώστε ιδιαίτερη προσοχή σε αυτό το μέτρο.

Η διαδικασία ασφαλούς διαμόρφωσης περιλαμβάνει την προσαρμογή των προεπιλεγμένων ρυθμίσεων ενός συστήματος/εφαρμογής/συσκευής προκειμένου να αυξηθεί η ασφάλεια και να μετριαστεί ο κίνδυνος. Η διαδικασία εντοπίζει εσφαλμένες ρυθμίσεις παραμέτρων των προεπιλεγμένων ρυθμίσεων ενός συστήματος.

Καθορίστε μέσω της διαδικασίας τουλάχιστον τα εξής σημεία:
- Δημιουργία και συντήρηση διαδικασίας ασφαλούς ρύθμισης δικτυακής υποδομής
- Ρύθμιση αυτομάτου κλειδώματος επιφάνειας εργασίας
- Υλοποίηση και ρύθμιση Firewall σε συστήματα (servers)
- Υλοποίηση και ρύθμιση Firewall στους σταθμούς εργασίας (PC, Desktop, Laptop)
- Ασφαλής Διαχείριση Εξοπλισμού και Εφαρμογών
- Διαχείριση Προ-Εγκατεστημένων Λογαριασμών σε Συσκευές και Εφαρμογές

- Το προσωπικό που θα φέρει την ευθύνη για την ασφαλή διαμόρφωση καθώς και τα χρονικά διαστήματα που πρέπει να εκτελείται, σε κρίσιμα και λιγότερο κρίσιμα συστήματα και εφαρμογές.
-Σημεία αναφοράς (benchmarks) σύμφωνα με τον κατασκευαστή/διανομέα ή και σύμφωνα με έναν αναγνωρισμένο οργανισμό/πρότυπο κυβερνοασφάλειας όπως είναι το CIS, SANS, NIST, ISO2700, BSI κ.α. Το CIS συγκεκριμένα προσφέρει τέτοια benchmarks για ένα πλήθος συσκευών και εφαρμογών:
https://www.cisecurity.org/cybersecurity-tools/
https://www.cisecurity.org/cis-benchmarks/

Σύμφωνα με τα σημεία αναφοράς, δημιουργήστε checklist για κάθε ομάδα συσκευών/εφαρμογών. Προχωρήστε στη διαμόρφωση και επανελέγξετε εάν αυτή εκτελέστηκε σύμφωνα με τις οδηγίες του κατασκευαστή.

Άλλο βοηθητικό υλικό:
https://docs.microfocus.com/SM/9.60/Hybrid/Content/BestPracticesGuide_PD/ConfigurationManagementBestPractice/Configuration_Management_within_the_ITIL_framework.htm
https://www.calcomsoftware.com/cis-hardening-and-configuration-security-guide/#secure
https://www.itgovernance.co.uk/secure-configuration
https://www.hysolate.com/blog/system-hardening-guidelines-best-practices/
https://kirkpatrickprice.com/blog/industry-accepted-hardening-standards/
https://security.utexas.edu/os-hardening-checklist
https://www.securitymetrics.com/blog/system-hardening-standards-how-comply-pci-requirement-22

4.2 Δημιουργία και Συντήρηση Διαδικασίας Ασφαλούς Διαμόρφωσης Δικτυακής Υποδομής

Η διαδικασία ασφαλούς διαμόρφωσης περιλαμβάνει την προσαρμογή των προεπιλεγμένων ρυθμίσεων ενός συστήματος/εφαρμογής/συσκευής προκειμένου να αυξηθεί η ασφάλεια και να μετριαστεί ο κίνδυνος. Η διαδικασία εντοπίζει εσφαλμένες ρυθμίσεις παραμέτρων των προεπιλεγμένων ρυθμίσεων

ενός συστήματος.

Καθορίστε μέσω της διαδικασίας το προσωπικό που θα φέρει την ευθύνη για την ασφαλή διαμόρφωση καθώς και τα χρονικά διαστήματα που πρέπει να εκτελείται, σε κρίσιμα και λιγότερο κρίσιμα συστήματα και εφαρμογές. Από τεχνικής άποψης, πρέπει να καθοριστούν σημεία αναφοράς (benchmarks) σύμφωνα με τον κατασκευαστή/διανομέα ή και σύμφωνα με έναν αναγνωρισμένο οργανισμό/πρότυπο κυβερνοασφάλειας όπως είναι το CIS, SANS, NIST, ISO2700, BSI κ.α. Το CIS συγκεκριμένα προσφέρει τέτοια benchmarks για ένα μεγάλο πλήθος συσκευών και εφαρμογών:
https://www.cisecurity.org/cybersecurity-tools/
https://www.cisecurity.org/cis-benchmarks/

Προχωρήστε στην διαμόρφωση και επανελέγξετε εάν αυτή εκτελέστηκε σύμφωνα με τις οδηγίες του

κατασκευαστή.

Γενικές συστάσεις δικτυακών συσκευών:
- Απενεργοποιήστε κάθε περιττή υπηρεσία (service),
- Ενεργοποιήστε τη λειτουργία “port security” στα switches,
- Απενεργοποιήστε τα interfaces και τα πρωτόκολλα δρομολόγησης (στους routers), καθώς και τις θύρες (στα switches), που δεν χρησιμοποιούνται.
- Εφαρμόστε αυθεντικοποίηση δύο παραγόντων (2-factor authentication) για την πρόσβαση στο διαχειριστικό περιβάλλον όλων των κρίσιμων δικτυακών συσκευών

Άλλο βοηθητικό υλικό:
https://www.cisecurity.org/cis-benchmarks/
https://media.defense.gov/2020/Aug/18/2002479461/-1/-1/0/HARDENING_NETWORK_DEVICES.PDF
https://docs.microfocus.com/SM/9.60/Hybrid/Content/BestPracticesGuide_PD/ConfigurationManagementBestPractice/Configuration_Management_within_the_ITIL_framework.htm
https://www.calcomsoftware.com/cis-hardening-and-configuration-security-guide/#secure
https://www.itgovernance.co.uk/secure-configuration

4.3 Ρύθμιση Αυτομάτου Κλειδώματος Επιφάνειας Εργασίας

Συστάσεις/ Βοηθητικοί σύνδεσμοι:
Για την συγκεκριμένη ρύθμιση μπορείτε να ανατρέξετε στο manual του λειτουργικού συστήματος. Ή μέσω Group Policy, εάν υπάρχει domain controller.

4.4 Υλοποίηση και Ρύθμιση Firewall σε Συστήματα (servers)

Ενεργοποιήστε κατάλληλα firewall ως εφαρμογή σε κάθε Server (host-based), το οποίο να εμποδίζει κάθε δικτυακή σύνδεση από και προς τη συσκευή, με εξαίρεση τις θύρες και τις υπηρεσίες που απαιτούνται με βάση τις επιχειρησιακές ανάγκες.

https://docs.microsoft.com/en-us/answers/questions/267482/hyper-v-for-virtual-firewall.html
https://linux.die.net/man/8/iptables
https://www.cisecurity.org/cis-benchmarks/
https://docs.rackspace.com/support/how-to/best-practices-for-firewall-rules-configuration/
https://www.checkpoint.com/cyber-hub/network-security/what-is-firewall/8-firewall-best-practices-for-securing-the-network/

4.5 Υλοποίηση και Ρύθμιση Firewall Στους Σταθμούς Εργασίας (PC, Desktop, Laptop)

Συστάσεις/ Βοηθητικοί σύνδεσμοι:

https://docs.microsoft.com/en-us/answers/questions/267482/hyper-v-for-virtual-firewall.html
https://linux.die.net/man/8/iptables
https://www.cisecurity.org/cis-benchmarks/
https://docs.rackspace.com/support/how-to/best-practices-for-firewall-rules-configuration/
https://www.checkpoint.com/cyber-hub/network-security/what-is-firewall/8-firewall-best-practices-for-securing-the-network/

4.6 Ασφαλής Διαχείριση Εξοπλισμού και Εφαρμογών

Βεβαιωθείτε ότι η πρόσβαση στα συστήματα είναι κρυπτογραφημένη. Εφαρμόστε βασικές ρυθμίσεις ασφάλειας με βάση διεθνώς αποδεκτά πρότυπα και οδηγίες για τα λειτουργικά συστήματα των σταθμών εργασίας, των servers και των δικτυακών συσκευών, προσαρμοσμένες στην πολιτική ασφάλειας του Οργανισμού. Οι εν λόγω ρυθμίσεις θα πρέπει να αποθηκεύονται σε αρχείο.
Χρησιμοποιήστε μόνο υποστηριζόμενες εκδόσεις των λειτουργικών συστημάτων στους σταθμούς εργασίας, στους servers και στις δικτυακές συσκευές. Ρυθμίστε ώστε να λαμβάνουν ενημερώσεις με αυτοματοποιημένο τρόπο.

*Εφαρμόστε εργαλεία που με αυτοματοποιημένο τρόπο εγκαθιστούν ενημερώσεις και επιδιορθώσεις (patches) στα λειτουργικά συστήματα και στις εφαρμογές του Οργανισμού.*

*Ρυθμίστε, σε όσα συστήματα έχουν ταξινομηθεί ως κρίσιμα, να μην είναι εφικτή η σύνδεση φορητών μέσων αποθήκευσης (USB, εξωτερικών σκληρών δίσκων, CD, DVD), εάν δεν υπάρχει γι' αυτό αυστηρή επιχειρησιακή ανάγκη.*

*Διαχειριστείτε με ασφάλεια τους λογαριασμούς υπηρεσιών (service accounts), κατά προτίμηση με αυτοματοποιημένο τρόπο:*
*- εκχωρείστε τα ελάχιστα απαιτούμενα δικαιώματα πρόσβασης,*
*- αλλάζετε τα συνθηματικά σε τακτά χρονικά διαστήματα,*
*- απενεργοποιείστε τους λογαριασμούς υπηρεσιών που δεν χρειάζονται πλέον για τις επιχειρησιακές λειτουργίες του Φορέα.*
https://www.cisecurity.org/cis-benchmarks/
https://www.cisecurity.org/cybersecurity-tools/

4.7 Διαχείριση Προ-Εγκατεστημένων Λογαριασμών σε Συσκευές και Εφαρμογές

Διαχειριστείτε λογαριασμούς σε συσκευές και εφαρμογές οι οποίοι έχουν ρυθμιστεί από τον πάροχο/κατασκευαστή. Τέτοιοι λογαριασμοί μπορεί να είναι οι λεγόμενοι "root", "default admin", "admin" κ.α. Διαγράψτε ή απενεργοποιήστε αυτούς τους λογαριασμούς. Εάν αυτό δεν είναι εφικτό αλλάξτε το password με ένα πιο ισχυρό.

4.8 Απενεργοποίηση Μη Αναγκαίων Υπηρεσιών σε Συσκευές και Εφαρμογές

Οι υπηρεσίες που είναι αναγκαίες θα πρέπει να έχουν οριστεί με σαφήνεια σε προηγούμενο μετρό. Μπορείτε να πάρετε για βοήθεια το μητρώο συσκευών και λογισμικού. Με το κατάλληλο πρόγραμμα (π.χ. task manager, services.msc) να ελέγξετε άμα μια υπηρεσία είναι αναγκαία για την διεκπεραίωση της εργασίας του οργανισμού ή όχι.

4.9 Ρύθμιση Έμπιστων DNS-Server

Ως βασικό στοιχείο του διαδικτύου, το DNS έχει τεράστια σημασία και θα πρέπει να είναι σωστά διαμορφωμένο.
Ρυθμίστε PC, συστήματα(Server) και δικτυακές συσκευές εάν χρειαστεί να επικοινωνούν με έναν οι περισσοτέρους DNS-Server που έχουν οριστεί από τον οργανισμό. Κατάλληλο εγχειρίδιο: https://sansorg.egnyte.com/dl/TglvVmGDmF/
https://www.manageengine.com/products/active-directory-audit/best-practices/dns-security-best-practices.html

4.10 Αυτοματοποιημένο Κλείδωμα Λογαριασμών σε Κινητές Συσκευές

Προτείνουμε έτοιμες λύσεις/υπηρεσίες διαχείρισης συσκευών σε IG2 και IG3 οργανισμούς. Ωστόσο αυτό το μέτρο μπορεί να ενεργοποιηθεί και αποκεντροποιημένα ή χειροκίνητα από τις ρυθμίσεις των περισσότερων συσκευών. Υπάρχει πληθώρα λύσεων στο πλαίσιο του Mobile Devices Management.
https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/account-lockout-policy
https://docs.microsoft.com/en-us/mem/intune/remote-actions/device-remote-lock
https://support.apple.com/el-gr/guide/deployment/dep4d6a472a/web

4.11 Υλοποιήστε Απομακρυσμένη Διαγραφή Δεδομένων σε Κινητές Συσκευές

Υπάρχει πληθώρα λύσεων στο πλαίσιο του Mobile Devices Management.
https://drivestrike.com/mobile-device-management-policy-examples/
https://support.apple.com/en-is/guide/deployment/dep0a819891e/web
https://docs.trendmicro.com/all/ent/tmms-ee/v9.8/en-us/tmms-ee_9.8_ssdm_olh_server/t_remote_wipe.html

4.12 Διαχωρισμός Προφίλ σε Κινητές Συσκευές

Το να διατηρείτε τον προσωπικό σας χώρο εργασίας και τον εταιρικό χώρο εργασίας χωριστά στις κινητές συσκευές σας είναι σημαντικό, επειδή έτσι μειώνεται ο κίνδυνος οι εισβολείς να μπορούν να αξιοποιήσουν ό,τι κάνετε για προσωπική χρήση με απώτερο στόχο να αποκτήσουν πρόσβαση στο εταιρικό δίκτυο.

Τι είναι τα εταιρικά προφίλ:
https://support.google.com/work/android/answer/6191949?hl=en
https://support.apple.com/el-gr/guide/apple-configurator-2/pmd85719196/mac
https://docs.microsoft.com/en-us/mem/intune/user-help/enroll-device-android-work-profile

## Control 05

5.1 Δημιουργία και Συντήρηση Μητρώου λογαριασμών

Το μητρώο καταγραφής, εφόσον δεν χρησιμοποιείται η κεντρική διαχείριση λογαριασμών, μπορεί να συσταθεί σε ένα υπολογιστικό φύλλο και να αναγράφονται τουλάχιστον τα ακόλουθα στοιχεία:
ονοματεπώνυμο του ατόμου που το χρησιμοποιεί
όνομα χρήστη
έναρξη / λήξη λογαριασμού
τμήμα
τύπος λογαριασμού (admin, user)
Αξιολογήστε τις προσβάσεις στους λογαριασμούς τουλάχιστον κάθε τρίμηνο.

Χρειάζομαι έναν Domain Controller;

Σε γενικές γραμμές, ναι. Οργανισμοί και επιχειρήσεις που βρίσκονται στην ομάδα ενσωμάτωσης 2 & 3 – ανεξάρτητα από το μέγεθος – που αποθηκεύουν δεδομένα πελατών στο δίκτυό τους χρειάζονται έναν Domain Controller για να βελτιώσουν την ασφάλεια του δικτύου τους. Θα μπορούσαν να υπάρχουν εξαιρέσεις: ορισμένες επιχειρήσεις, για παράδειγμα, χρησιμοποιούν μόνο λύσεις CRM και πληρωμών που βασίζονται στο cloud. Σε αυτές τις περιπτώσεις, η υπηρεσία cloud προστατεύει τα δεδομένα των πελατών.

Η βασική ερώτηση που πρέπει να κάνετε είναι "πού βρίσκονται τα δεδομένα των πελατών μου και ποιος μπορεί να έχει πρόσβαση σε αυτά;"

5.2 Χρήση Ξεχωριστών/Μοναδικών Κωδικών Πρόσβασης

Εφόσον δεν χρησιμοποιείτε κεντρική διαχείριση λογαριασμών, θα πρέπει να ρυθμιστεί το ΛΣ κατάλληλα ώστε να υιοθετηθεί αυτή η πολιτική ή θα πρέπει ο διαχειριστής του δικτύου να θέτει και να εκδίδει τους κωδικούς.
Η διαχείριση μπορεί να γίνει κεντρικά Μέσω Domain Controller, με χρήση group policy.

5.3 Απενεργοποίηση Ανενεργών Λογαριασμών

Εφόσον δεν χρησιμοποιείτε κεντρική διαχείριση λογαριασμών, θα πρέπει να βασιστείτε στο μητρώο λογαριασμών(5.1) και να πραγματοποιείτε κατάλληλη επίβλεψη και επικαιροποίηση αυτών. Απενεργοποιείστε ή διαγράψτε τους λογαριασμούς που δεν σχετίζονται πλέον με κάποιον χρήστη ή όταν δεν υφίσταται άλλο υπηρεσιακή ανάγκη χρήσης τους.

5.4 Εκχώρηση Δικαιωμάτων Διαχειριστή (Administrator Rights Privileges)

Αφαιρέστε τα administrator δικαιώματα από όλους τους λογαριασμούς χρηστών. Ορίστε συγκεκριμένους λογαριασμούς για την διαχείριση του δικτύου, για την εγκατάσταση εφαρμογών και για λειτουργίες υπηρεσιών που απαιτούν επαυξημένα δικαιώματα, τους οποίους θα διαχειρίζεται ο διαχειριστής του δικτύου και των συστημάτων.

5.5 Δημιουργία και Συντήρηση Μητρώου Υπηρεσιακών Λογαριασμών (Service Accounts)

Συστάσεις/ Βοηθητικοί σύνδεσμοι:
Το μητρώο υπηρεσιακών λογαριασμών (service accounts), εφόσον δεν χρησιμοποιείτε κεντρική διαχείριση λογαριασμών, μπορεί να συσταθεί σε ένα υπολογιστικό φύλλο και να αναγράφονται τουλάχιστον τα ακόλουθα στοιχεία:
υπεύθυνος τμήματος
ημερομηνία επικαιροποίησης
χρήση
Επικαιροποιήστε το μητρώο τουλάχιστον κάθε τρίμηνο.

5.6 Χρήση Κεντρικής Διαχείρισης Λογαριασμών
Συστάσεις/ Βοηθητικοί σύνδεσμοι:
https://en.wikipedia.org/wiki/Domain_controller
https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview
https://directory.fedoraproject.org/

## Control 06

6.1 Καθιερώστε Διαδικασία Παροχής Δικαιωμάτων

Αναπτύξτε και καταγράψτε πολιτική ελέγχου πρόσβασης, που θα περιγράφει το σκοπό, το πεδίο εφαρμογής, τους ρόλους και τις ευθύνες.
Διασφαλίστε ότι το προσωπικό του οοργανισμού και οι εξωτερικοί συνεργάτες που αποκτούν λογαριασμό χρήστη θα πρέπει να αναγνωρίζονται (identified) με μοναδικό τρόπο, με σκοπό τη διασφάλιση λογοδοσίας (accountability).
Ορίστε σε ποιους πόρους θα έχουν δικαιώματα οι απλοί χρήστες, πως θα επεξεργάζονται τα αιτήματα χορήγησης δικαιωμάτων σε επιπλέον πόρους και ποια διαδικασία θα τηρείται κατά την αλλαγή ρόλου ενός χρηστή μέσα στον οργανισμό.

6.2 Καθιερώστε Διαδικασία Ανάκλησης Δικαιωμάτων

6.3 Ενεργοποίηση Πολυπαραγοντικής Αυθεντικοποίησης σε Εξωτερικά (Internet Facing) συστήματα

Συστάσεις/ Βοηθητικοί σύνδεσμοι:
Για επιπλέον πληροφόρηση:
https://docs.microsoft.com/en-us/azure/security/fundamentals/identity-management-best-practices
https://support.alertlogic.com/hc/en-us/articles/360028618612-Security-Best-Practices-for-Internet-Exposed-Endpoints
https://its.uark.edu/about/policies/mfa-policy.php

6.4 Ενεργοποίηση Πολυπαραγοντικής Αυθεντικοποίησης κατά την Απομακρυσμένη Πρόσβαση από Εξωτερικό Δίκτυο.

Απαίτηση πολυπαραγοντικής αυθεντικοποίησης κατά την απομακρυσμένη πρόσβαση (Remote Control) από εξωτερικό δίκτυο.

6.5 Ενεργοποίηση Πολυπαραγοντικής Αυθεντικοποίησης σε Λογαριασμούς Διαχειριστή

Απαίτηση πολυπαραγοντικής αυθεντικοποίησης σε λογαριασμούς διαχειριστή όπου αυτό υποστηρίζεται.

6.6 Δημιουργία και Συντήρηση Μητρώου Καταγραφής Συστημάτων Αυθεντικοποίησης και Εξουσιοδότησης

Δημιουργήστε και συντηρήστε ένα μητρώο καταγραφής συστημάτων αυθεντικοποίησης και εξουσιοδότησης.

6.7 Κεντρική Διαχείρισης Ελέγχου Πρόσβασης

Αυτό το μέτρο ασφάλειας σκοπεύει να προστατεύσει της συσκευές του οργανισμού διασφαλίζοντας ότι ο έλεγχος πρόσβασης εκτελείται κεντρικά, καθιστώντας ευκολότερη την αυτοματοποίηση και την ενημέρωσή του. Οι οργανισμοί που έχουν αυξημένη λειτουργική πολυπλοκότητα, που έχουν επιβαρύνσεις συμμόρφωσης με τους κανονισμούς ή που αποθηκεύουν και επεξεργάζονται ευαίσθητα δεδομένα πελατών, θα πρέπει να εφαρμόσουν αυτήν τη διασφάλιση.

6.8 Σύσταση Διαδικασίας/Μηχανισμού Ελέγχου Πρόσβασης Βασισμένη σε Διακριτούς Πόλους

Αυτό το μέτρο ασφάλειας σκοπεύει να προστατεύσει τις συσκευές του οργανισμού διασφαλίζοντας ότι τα δικαιώματα πρόσβασης βασίζονται σε ρόλους και διατηρούνται με τυποποιημένο και αξιόπιστο τρόπο.

Οργανισμοί με περιουσιακά στοιχεία που υπόκεινται σε ρυθμιστική εποπτεία και επίβλεψη συμμόρφωσης, καθώς και αυτοί που στοχοποιούνται από εξελιγμένους αντιπάλους, όπως οι APT, θα πρέπει να εφαρμόσουν αυτήν τη Διασφάλιση.

Για παράδειγμα, όσοι υπάλληλοι εργάζονται στο λογιστήριο θα πρέπει να έχουν πρόσβαση στα ανοιχτά συστήματα…μόνο αυτοί οι εργαζόμενοι. Μπορούν να συσταθούν και υποομάδες, π.χ. συγκεκριμένοι υπάλληλοι του λογιστηρίου που θα έχουν πρόσβαση στο σύστημα της μισθοδοσίας συν την ομάδα προϊστάμενων του λογιστηρίου. όλοι οι άλλοι υπάλληλοι του λογιστηρίου θα αποκλείονται.(Nested Security Groups)

## Control 07

7.1 Καθιέρωση και Συντήρηση Διαδικασίας Διαχείρισης Ευπαθειών

Μια ευπάθεια ορίζεται στο πρότυπο ISO 27002 ως «Ευπάθεια ενός αγαθού ή ομάδας αγαθών που μπορούν να αξιοποιηθούν από μία ή περισσότερες απειλές» (Διεθνής
Οργανισμός Τυποποίησης, 2005).
Η διαχείριση ευπαθειών είναι η διαδικασία κατά την οποία εντοπίζονται και αξιολογούνται οι κίνδυνοι αυτών των τρωτών σημείων. Αυτή η αξιολόγηση οδηγεί σε διόρθωση των τρωτών σημείων και άρση του κινδύνου ή στην επίσημη αποδοχή του κινδύνου από τη διαχείριση ενός οργανισμού (π.χ. σε περίπτωση που ο αντίκτυπος μιας επίθεσης θα ήταν χαμηλός ή το κόστος της διόρθωσης δεν υπερβαίνει τις πιθανές ζημιές στον οργανισμό).
Ο όρος «διαχείριση ευπαθειών» συχνά συγχέεται με τη σάρωση ευπάθειας. Παρά το γεγονός ότι και τα δύο σχετίζονται, υπάρχει μια σημαντική διαφορά μεταξύ των δύο.
Η σάρωση ευπάθειας συνίσταται στη χρήση ενός προγράμματος υπολογιστή για τον εντοπισμό τρωτών σημείων σε δίκτυα, υποδομές υπολογιστών ή εφαρμογές. Η διαχείριση ευπάθειας είναι η διαδικασία που περιλαμβάνει τη σάρωση ευπάθειας, λαμβάνοντας επίσης υπόψη άλλες πτυχές, όπως αποδοχή κινδύνου, αποκατάσταση κ.λπ.

Κατάλληλος οδηγός:
https://sansorg.egnyte.com/dl/2IL7fioFhM

7.2 Καθιέρωση και Συντήρηση Διαδικασίας Αποκατάστασης Ευπαθειών

Η διαδικασία αποκατάστασης είναι ένα υποσύνολο της διαδικασίας διαχείρισης ευπαθειών, δίνει έμφαση στον τρόπο με τον οποίο θα διορθώσετε τα τρωτά σημεία που ανακαλύπτονται. Εδώ είναι κρίσιμο να αναπτύξετε ένα σύστημα ιεράρχησης προτεραιοτήτων που να λειτουργεί για τον οργανισμό σας και να λαμβάνει υπόψη όλα τα δεδομένα που θα μπορούσαν να θέσουν σε κίνδυνο τον οργανισμό.

7.3 Αυτοματοποίηση Διαχείρισης Ενημερώσεων Λειτουργικών Συστημάτων

Η διαχείριση ενημερώσεων του ΛΣ αποτελεί υποσύνολο της διαχείρισης ευπαθειών, είτε οι ενημερώσεις σχετίζονται με ευπάθειες είτε όχι. Η αυτοματοποίηση των ενημερώσεων του ΛΣ αποτελεί σημαντικό κομμάτι της διαχείρισης συστημάτων σε έναν οργανισμό.

7.4 Αυτοματοποίηση Διαχείρισης Ενημερώσεων Εφαρμογών

Η διαχείριση ενημερώσεων εφαρμογών αποτελεί υποσύνολο της διαχείρισης ευπαθειών, είτε οι ενημερώσεις σχετίζονται με ευπάθειες είτε όχι. Η αυτοματοποίηση των ενημερώσεων αποτελεί σημαντικό κομμάτι της διαχείρισης συστημάτων σε έναν οργανισμό.
Κάποια εργαλεία:
https://www.manageengine.com/patch-management/automated-patch-deployment.html#:~:text=The%20automated%20patch%20management%20process,missing%20patches%20on%20the%20endpoints.
https://www.solarwinds.com/patch-manager?a_aid=BIZ-PAP-CMPRTCH&a_bid=118df781&CMP=BIZ-PAP-CMPR_NMS-PatchMngmt-PM-LM
https://docs.microsoft.com/en-us/mem/configmgr/core/understand/introduction

7.5 Αυτοματοποίηση Σάρωσης Ευπαθειών για Συστήματα Εσωτερικού Δικτύου
Χρησιμοποιήστε τα κατάλληλα εργαλεία για την εφαρμογή του μέτρου:
https://www.openvas.org/
https://www.tenable.com/products/nessus

https://nmap.org/
https://govanguard.com/legion/
https://www.open-scap.org/

7.6 Αυτοματοποίηση Σάρωσης Ευπαθειών για Συστήματα Προσβάσιμα από το Παγκόσμιο Διαδίκτυο
Χρησιμοποιήστε τα κατάλληλα εργαλεία για την εφαρμογή του μέτρου:
https://www.qualys.com/
https://www.openvas.org/
https://www.tenable.com/products/nessus
https://nmap.org/
https://www.open-scap.org/
https://www.shodan.io/
https://www.maltego.com/?utm_source=paterva.com&utm_medium=referral&utm_campaign=301

7.7 Αποκατάσταση Εντοπισμένων Ευπαθειών

Η αποκατάσταση είναι μια βασική πτυχή της διαδικασίας. Η αποκατάσταση είναι τελικά αυτό που μειώνει τον κίνδυνο, είτε με επιδιόρθωση είτε με άλλο μέσο (παροπλισμός συστήματος, αποδοχή ρίσκου, ανάθεση σε 3ους κ.α.). Εάν δεν προβείτε σε αποκατάσταση ή αποτύχετε να ιεραρχήσετε σωστά τα αποτελέσματά, θέτετε ολόκληρο το πληροφοριακό σύστημα του οργανισμού σε κίνδυνο.

## Control 08

8.1 Καθιέρωση και συντήρηση διαδικασίας διαχείρισης αρχείων καταγραφής ελέγχου(Audit Logs)

Αυτό το μέτρο ασφάλειας σκοπεύει να προστατεύσει τα αγαθά(assets) του οργανισμού διασφαλίζοντας ότι τα αρχεία καταγραφής ελέγχου συλλέγονται, εξετάζονται και διατηρούνται συστηματικά. Τα αρχεία καταγραφής ελέγχου πρέπει να είναι πλήρη και ακριβή. Μπορεί να είναι απαραίτητο να προγραμματίσετε προσομοιώσεις συμβάντων για να επαληθεύσετε ότι δημιουργούνται τα επιθυμητά αρχεία καταγραφής. Ενδέχεται να απαιτούνται εργαλεία για την απορρόφηση και την αναζήτηση αρχείων καταγραφής. Τα δεδομένα καταγραφής μπορεί να χρειαστεί να κανονικοποιηθούν για να καταστεί δυνατή η γρήγορη και αποτελεσματική ανάλυση.
Η διαδικασία θα θέσει την βάση έτσι ώστε να εκτελείται ορθά η διαχείριση των αρχείων καταγραφής ελέγχου.
Συνιστάται η εφαρμογή εργαλείου Security Information and Event Management SIEM.
Κάποια SIEM:
https://www.manageengine.com/products/eventlog/?utm_source=Comparitech&utm_medium=Website-cpc&utm_campaign=ELA-SIEMTools
https://www.datadoghq.com/dg/security/siem-solution/?utm_source=advertisement&utm_medium=review-site&utm_campaign=dg-comparitech-security-ww-siem/
https://www.ossec.net/docs/docs/manual/non-technical-overview.html

8.2 Συλλογή Αρχείων Καταγραφής Ελέγχου(Audit Logs)

Αυτό το μέτρο ασφάλειας σκοπεύει να υποστηρίξει τον εντοπισμό απειλών στα αγαθά(assets) του οργανισμού. Είναι ένα από τα βασικά μέτρα ασφάλειας στον κυβερνοχώρο και θα πρέπει να εφαρμόζεται από όλους του οργανισμούς.

Διασφαλίστε ότι έχει ενεργοποιηθεί η λειτουργία της καταγραφής συμβάντων (event/audit logs) σε όλους τους σταθμούς εργασίας, τους servers και τις δικτυακές συσκευές.

https://www.strongdm.com/blog/audit-log-review-management
https://www.snaresolutions.com/basic-guide-to-collecting-system-and-audit-logs-2/
Συνιστάται η εφαρμογή εργαλείου Security Information and Event Management SIEM.
Κάποια SIEM:
https://www.manageengine.com/products/eventlog/?utm_source=Comparitech&utm_medium=Website-cpc&utm_campaign=ELA-SIEMTools
https://www.datadoghq.com/dg/security/siem-solution/?utm_source=advertisement&utm_medium=review-site&utm_campaign=dg-comparitech-security-ww-siem/
https://www.ossec.net/docs/docs/manual/non-technical-overview.html

8.3 Επιβεβαίωση Κατάλληλης Αποθήκευσης Αρχείων Καταγραφής Ελέγχου (Audit Logs)

Διασφαλίστε ότι τα αρχεία καταγραφής συμβάντων προστατεύονται επαρκώς από μη εξουσιοδοτημένη πρόσβαση, τροποποίηση και διαγραφή. Ελέγξτε επιπλέον πολίτικες συμμόρφωσης που μπορεί να έχουν τεθεί στο μετρό ασφάλειας 8.1.

8.4 Συγχρονισμός Ημερομηνίας και ‘Ωρας

8.5 Συλλογή Αναλυτικών Αρχείων Καταγραφής (Audit Logs) ανά περίπτωση

Αυτό το μέτρο ασφάλειας σκοπεύει να υποστηρίξει τον εντοπισμό παραβίασης συστημάτων/δεδομένων, διασφαλίζοντας ότι συλλέγονται αναλυτικά αρχεία καταγραφής ελέγχου, τα οποία μας επιτρέπουν να ανασυνθέσουμε τι συνέβη κατά τη διάρκεια ενός συμβάντος και να καθορίσουμε την έκταση των επηρεαζόμενων αγαθών.
Συνιστάται η εφαρμογή εργαλείου Security Information and Event Management SIEM.
Κάποια SIEM:
https://www.manageengine.com/products/eventlog/?utm_source=Comparitech&utm_medium=Website-cpc&utm_campaign=ELA-SIEMTools
https://www.datadoghq.com/dg/security/siem-solution/?utm_source=advertisement&utm_medium=review-site&utm_campaign=dg-comparitech-security-ww-siem/
https://www.ossec.net/docs/docs/manual/non-technical-overview.html
Μια πλατφόρμα αναφοράς για όλα τα events και την ερμηνεία τους:https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/default.aspx

8.6 Συλλογή DNS Query Αρχείων Καταγραφής Ελέγχου (Audit Logs)

Τα αρχεία καταγραφής DNS μπορούν να βοηθήσουν στον εντοπισμό συστημάτων που δεν έχουν ρυθμιστεί ορθά όπως και την πηγή μιας εισβολής ή επίθεσης.
Συνιστάται η εφαρμογή εργαλείου Security Information and Event Management SIEM.
Κάποια SIEM:
https://www.manageengine.com/products/eventlog/?utm_source=Comparitech&utm_medium=Website-cpc&utm_campaign=ELA-SIEMTools
https://www.datadoghq.com/dg/security/siem-solution/?utm_source=advertisement&utm_medium=review-site&utm_campaign=dg-comparitech-security-ww-siem/
https://www.ossec.net/docs/docs/manual/non-technical-overview.html
Μια πλατφόρμα αναφοράς για όλα τα events και την ερμηνεία τους:https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/default.aspx

8.7 Συλλογή URL Request Αρχείων Καταγραφής Ελέγχου (Audit Logs)

Αυτό το μέτρο ασφάλειας σκοπεύει να ανιχνεύσει απειλές και μη συνηθισμένα συμβάντα που σχετίζονται με αιτήματα URL.
Συνιστάται η εφαρμογή εργαλείου Security Information and Event Management SIEM.
Κάποια SIEM:
https://www.manageengine.com/products/eventlog/?utm_source=Comparitech&utm_medium=Website-cpc&utm_campaign=ELA-SIEMTools
https://www.datadoghq.com/dg/security/siem-solution/?utm_source=advertisement&utm_medium=review-site&utm_campaign=dg-comparitech-security-ww-siem/
https://www.ossec.net/docs/docs/manual/non-technical-overview.html
Μια πλατφόρμα αναφοράς για όλα τα events και την ερμηνεία τους:https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/default.aspx

8.8 Συλλογή Αρχείων Καταγραφής Ελέγχου από Command Line

Αυτό το μέτρο ασφάλειας σκοπεύει να εντοπίσει ασυνήθιστη ή απειλητική συμπεριφορά στις κονσόλες εντολών. Οι επιτιθέμενοι μπορούν να χρησιμοποιήσουν scripts για κάθε τεχνική παραβίασης όπως αναφέρεται στο πίνακα Mitre Att&ack https://attack.mitre.org/matrices/enterprise/
Συνιστάται η εφαρμογή εργαλείου Security Information and Event Management SIEM.
Κάποια SIEM:
https://www.manageengine.com/products/eventlog/?utm_source=Comparitech&utm_medium=Website-cpc&utm_campaign=ELA-SIEMTools
https://www.datadoghq.com/dg/security/siem-solution/?utm_source=advertisement&utm_medium=review-site&utm_campaign=dg-comparitech-security-ww-siem/
https://www.ossec.net/docs/docs/manual/non-technical-overview.html
Μια πλατφόρμα αναφοράς για όλα τα events και την ερμηνεία τους:https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/default.aspx

8.9 Κεντρικοποίηση Αρχείων Καταγραφής Ελέγχου

Αυτό το μέτρο ασφάλειας σκοπεύει να υποστηρίξει άλλα μέτρα ελέγχου και ασφάλειας εντός οργανισμών που έχουν αυξημένη λειτουργική πολυπλοκότητα. Διασφαλίστε ότι τα απαραίτητα αρχεία καταγραφής συμβάντων συγκεντρώνονται σε έναν κεντρικό διακομιστή καταγραφής (log server) για ανάλυση και επιθεώρηση. Η συγκέντρωση των αρχείων καταγραφής ελέγχου θα κάνει τη συλλογή, τη διατήρηση και την αναθεώρηση απλούστερη. Υπάρχουν εργαλεία για την συλλογή, την κανονικοποίηση και την ανάλυση αρχείων καταγραφής για αποτελεσματική αναζήτηση και ανάλυση.
Απαιτείται η εφαρμογή εργαλείου Security Information and Event Management SIEM.
Κάποια SIEM:
https://www.manageengine.com/products/eventlog/?utm_source=Comparitech&utm_medium=Website-cpc&utm_campaign=ELA-SIEMTools
https://www.datadoghq.com/dg/security/siem-solution/?utm_source=advertisement&utm_medium=review-site&utm_campaign=dg-comparitech-security-ww-siem/
https://www.ossec.net/docs/docs/manual/non-technical-overview.html
8.10 Διατήρηση Αρχείων Καταγραφής Ελέγχου
Διατήρησε τα αρχεία καταγραφής ελέγχου των συστημάτων του οργανισμού για τουλάχιστον 90 μέρες

8.11 Επιθεώρηση Αρχείων Καταγραφής Ελέγχου

Η συλλογή αρχείων καταγραφής δεν αρκεί, θα πρέπει σε τακτά χρονικά διαστήματα να γίνεται επιθεώρηση αυτών έτσι ώστε να εντοπιστούν τυχόν κυβερνοεπίθεσεις και παραβιάσεις συστημάτων.

Εγκαταστήστε εργαλείο ασφάλειας πληροφοριών και διαχείρισης συμβάντων (Security Information and Event Management - SIEM), με σκοπό τη συσχέτιση των συμβάντων και τον εντοπισμό ύποπτης δραστηριότητας.
Κάποια SIEM:
https://www.manageengine.com/products/eventlog/?utm_source=Comparitech&utm_medium=Website-cpc&utm_campaign=ELA-SIEMTools
https://www.datadoghq.com/dg/security/siem-solution/?utm_source=advertisement&utm_medium=review-site&utm_campaign=dg-comparitech-security-ww-siem/
https://www.ossec.net/docs/docs/manual/non-technical-overview.html

Μια πλατφόρμα αναφοράς για όλα τα events και την ερμηνεία τους:https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/default.aspx

8.12 Συλλογή Αρχείων Καταγραφής από Παρόχους Υπηρεσιών

SIEM/SOAR όπως Microsoft Sentinel παρέχουν modules έτσι ώστε να συνδέονται και να κατεβάζουν real-time τα αρχεία καταγραφής από το σύστημα του παρόχου. Αλλιώς η επιθεώρηση θα πρέπει να γίνει ετεροχρονισμένα και χειροκίνητα με την εξαγωγή το αρχείων καταγραφής. .
https://azure.microsoft.com/en-us/services/microsoft-sentinel/

## Control 09

9.1 Εξασφάλιση Χρήσης μόνο Υποστηριζόμενων Προγραμμάτων Περιήγησης Ιστότοπων και Ηλεκτρονικού Ταχυδρομείου

Κατά κανόνα τα προγράμματα περιήγησης όπως Google Chrome, MS Edge, Mozilla Firefox ελέγχουν κατά την εκκίνηση εάν υπάρχουν ερημώσεις και τις εγκαθιστούν αυτόματα ή ενημερώνουν τον χρήστη για επικείμενη ενημέρωση.
Ανάλογα εκτελούνται οι ενημερώσεις σε προγράμματα ηλεκτρονικού ταχυδρομείου όπως MS Outlook, Mozilla Thunderbird.
Υπάρχουν εργαλεία που ελέγχουν κεντρικά την έκδοση προγραμμάτων ή μπλοκάρουν την εκτέλεση παλιών εκδόσεων. Τέτοια συστήματα/εφαρμογές είναι:

https://docs.microsoft.com/en-us/mem/configmgr/core/understand/introduction
https://www.manageengine.com/application-control/
https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/applocker/applocker-overview
https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/hh831791(v=ws.11)#:~:text=Group%20Policy%20is%20an%20infrastructure,settings%20and%20Group%20Policy%20Preferences.&text=If%20you%20install%20the%20Remote,Group%20Policy%20are%20also%20installed.

9.2 Χρήση DNS Filtering

Το DNS filtering είναι η διαδικασία χρήσης του συστήματος DNS για τον αποκλεισμό κακόβουλων ιστότοπων και το φιλτράρισμα επιβλαβούς ή ακατάλληλου περιεχομένου. Αυτό διασφαλίζει ότι τα συστήματα, PC και τα δεδομένα του παραμένουν ασφαλή και επιτρέπει στους οργανισμούς να έχουν τον έλεγχο σε τι μπορούν να έχουν πρόσβαση οι χρήστες τους στα δίκτυα που διαχειρίζεται εκείνος. Το φιλτράρισμα DNS filtering αποτελεί συχνά μέρος μιας ευρύτερης στρατηγικής ελέγχου πρόσβασης.

Εργαλεία που υλοποιούν αυτό το μέτρο ασφάλειας :
https://www.cloudflare.com/products/zero-trust/gateway/
https://umbrella.cisco.com/

Όπως και τα συστήματα Intrusion Detection System – IDS:
https://docs.paloaltonetworks.com/dns-security.html

9.3 Λειτουργία και Διαχείριση Δικτυακού URL filtering

Συστάσεις/ Βοηθητικοί σύνδεσμοι:
Το Uniform Resource Locator (URL) είναι μια διαδικασία που επιτρέπει στους οργανισμούς να περιορίζουν τους ιστότοπους και το περιεχόμενο που μπορούν να έχουν πρόσβαση οι χρήστες. Οι χρήστες αποκλείονται από την επίσκεψη σε συγκεκριμένες τοποθεσίες και αποτρέπεται η χρήση πόρων του οργανισμού, όπως συσκευές ή εύρος ζώνης δικτύου, με τρόπο που θα μπορούσε να επηρεάσει αρνητικά τον οργανισμό.
Η διαδικασία URL filtering λειτουργεί συγκρίνοντας τη διεύθυνση URL που προσπαθεί να επισκεφτεί ένας χρήστης με μια βάση δεδομένων ή λίστα ιστότοπων που έχουν αποκλειστεί ή έχουν επιτραπεί για χρήση. Αυτό συνήθως αποτρέπει τους χρήστες από το να επισκέπτονται ιστότοπους που θα μπορούσαν να επηρεάσουν τον οργανισμό να λειτουργεί κανονικά, όπως ιστότοποι που έχουν παράνομο ή ακατάλληλο περιεχόμενο, ιστότοπους που δεν σχετίζονται με την εργασία και ιστότοπους που θα μπορούσαν να είναι υψηλού κινδύνου, κακόβουλοι ή να σχετίζονται με επιθέσεις phishing.
Το URL Filtering μπορεί να εκτελεστεί μέσω Network Firewall, IDS, EDR, ProxyServer κ.α..
Ενδεικτικά κάποιοι βοηθητικοί σύνδεσμοι:
https://campus.barracuda.com/product/cloudgenfirewall/doc/79463097/how-to-configure-url-filtering-in-the-http-proxy/
https://community.cisco.com/t5/security-documents/asa-url-filtering-without-a-websense-or-n2h2-smartfilter-server/ta-p/3116352
https://urlfiltering.paloaltonetworks.com/
https://www.fortinetguru.com/2016/06/web-filter-fortinet-fortigate/

9.4 Περιορισμός Μη Αναγκαίων ή Μη Εγκεκριμένων πρόσθετων σε Προγράμματα Περιήγησης Ιστότοπων (web broswer) και Ηλεκτρονικού Ταχυδρομείου (email client)

Η εφαρμογή αυτού του μέτρου ασφάλειας απομονώνει το κίνδυνο εγκατάστασης πρόσθετου, το οποίο εμπεριέχει κακόβουλο κώδικα. Μπορεί να υλοποιηθεί μέσω Group Policy ή και μέσω της registry. Ακολουθεί ενδεικτικά ένας οδηγός για τον web browser google chrome.
https://www.howtogeek.com/724165/how-to-prevent-people-from-installing-extensions-in-chrome/
https://www.thewindowsclub.com/prevent-users-from-installing-extensions-in-google-chrome
Ανάλογα για email clients όπως Outlook
https://www.urtech.ca/2019/08/solved-how-to-block-users-from-installing-add-ins-in-outlook-owa-on-office-365-hosted-exchange/

9.5 Εφαρμογή Πολιτικής DMARC

DKIM: Domain Keys Identified Signature, ψηφιακή υπογραφή του Domain του αποστολέα και έλεγχος ακεραιότητας . Χρησιμοποιεί ασύμμετρη κρυπτογράφηση με Public Key Infrastructure.
SPF: Sender Policy Framework, επιτρέπει την αντιστοίχιση IP διευθύνσεων σε Domains για την αποφυγή εξαπάτησης των παραληπτών.
DMARC: Πρόκειται για μια μετεξέλιξη και ενσωμάτωση των SPF και DKIM. https://datatracker.ietf.org/doc/html/rfc7489
Θα πρέπει να γίνουν οι κατάλληλες εγγραφές στον DNS Server ή και email server.

9.6 Φραγή Μη Αναγκαίων Τύπων Αρχείων ως Επισυναπτόμενα

Για την προστασία από κακόβουλο λογισμικό πρέπει να αποκλειστούν ορισμένοι τύποι επισυναπτόμενων αρχείων. Αυτό μπορεί να υλοποιηθεί ανάλογα με τον email server.Ενδεικτικά ο οδηγός για τον Exchange Online:https://docs.microsoft.com/en-us/exchange/troubleshoot/antispam-and-protection/how-to-reduce-malware-threats-via-file-attachment-blocking

9.7 Υλοποίηση και Διαχείριση Υπηρεσίας Προστασίας από Κακόβουλο Λογισμικό για Διακομιστές Ηλεκτρονικού Ταχυδρομείου (Email Server Anti-Malware Protection)

Κάποια ενδεικτικά εργαλεία:
https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/overview?view=o365-worldwide
https://docs.microsoft.com/en-us/exchange/antispam-and-antimalware/antimalware-protection/antimalware-protection?view=exchserver-2019
https://www.proofpoint.com/us/products/email-security-and-protection

## Control 10

10.1 Εγκατάσταση και Διαχείριση Λογισμικού Antivirus

Συστάσεις/ Βοηθητικοί σύνδεσμοι:
Διασφαλίστε ότι έχει εγκατασταθεί antivirus σε όλες τις συσκευές του οργανισμού που το υποστηρίζουν (PC,Server, κινητές συσκευές) όπως και την ενημέρωσή τους με τα πιο πρόσφατα definitions/signatures.

Κάποια γνωστά antivirus λογισμικά:
https://www.microsoft.com/en-us/windows/comprehensive-security
https://www.kaspersky.com/
https://www.gdatasoftware.com/
https://www.avast.com/index#pc
https://www.f-secure.com/en
http://www.clamav.net/

10.2 Ρύθμιση Αυτομάτων Ενημερώσεων για το Λογισμικό Antivirus

Ρυθμίστε το λογισμικό antivirus ώστε να λαμβάνει αυτόματα ενημερώσεις definitions/signatures για τον εντοπισμό κακόβουλου λογισμικού σε όλες τις συσκευές του οργανισμού.

10.3 Απενεργοποίηση αυτόματης εκτέλεσης αναιρουμένων μέσων αποθήκευσης USB

Απενεργοποιήστε την λειτουργία αυτόματης εκτέλεσης των αφαιρούμενων μέσων αποθήκευσης USB.

10.4 Ρύθμιση Αυτόματης Σάρωσης για Κακόβουλο Λογισμικό σε Αφαιρούμενα μέσα Αποθήκευσης USB

Ρυθμίστε τα συστήματα του οργανισμού έτσι ώστε να εκτελείται αυτόματα σάρωση για κακόβουλο λογισμικό κατά την σύνδεση αφαιρούμενου μέσου αποθήκευσης USB.

10.5 Ενεργοποίηση Δυνατοτήτων Anti-Exploitation

Η ανάπτυξη αυτού του λογισμικού είναι πολύ σημαντική για την άμυνα του οργανισμού, αλλά δεν χρησιμοποιείται πάντα στο μέγιστο των δυνατοτήτων του. Βεβαιωθείτε ότι το λογισμικό που μπορεί να

αποτρέψει ή να μειώσει τις επιθέσεις στα συστήματά σας χρησιμοποιείται όποτε είναι δυνατόν.
https://cybersecurity.yale.edu/mss/5/1/2
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/enable-exploit-protection?view=o365-worldwide

10.7 Χρήση Λογισμικού Συμπεριφοράς (Behavior-Based)

Χρησιμοποιήστε λογισμικό antivirus το οποίο λειτουργεί και προστατεύει το σύστημα με βάση την συμπεριφορά (συνδέσεις, πόρους) των προγραμμάτων.
Τα definitions/signatures έχουν ένα συγκεκριμένο πεδίο δράσης, θα υπάρχουν πάντα άγνωστα κομμάτια κακόβουλου λογισμικού που θέτουν τον οργανισμό σας σε κίνδυνο. Η εκτέλεση του antivirus που βασίζεται στη συμπεριφορά (Behavior-Based) θα διασφαλίσει ότι ακόμη και αν δεν υπάρχουν διαθέσιμα definitions/signatures, ο οργανισμός σας εξακολουθεί να έχει μια ευκαιρία έναντι του κακόβουλου λογισμικού που κυκλοφόρησε πρόσφατα.
Θα πρέπει ανά περίπτωση να ελέγξετε εάν το antivirus έχει δυνατότητα behavior-based εντοπισμού κακόβουλου λογισμικού.

## Control 11

11.1 Καθιέρωση και Διαχείριση Διαδικασίας Επαναφοράς Δεδομένων
_ Αναπτύξτε και καταγράψτε:
-πολιτική αντιγράφων ασφαλείας, που θα περιγράφει σκοπό, πεδίο εφαρμογής, ρόλους και ευθύνες
-ποια συστήματα, ποια δεδομένα, συχνότητα, τύπος (full, incremental, differential), προτεραιότητα επαναφοράς και ασφάλεια των αντιγράφων ασφαλείας

11.2 Διασφάλιση Εκτέλεσης Αυτοματοποιημένων Backup

Αυτοματοποιήστε την διαδικασία λήψης backup. Λαμβάνεται backup σε εβδομαδιαία βάση τουλάχιστον ή και πιο συχνά ανάλογα με τον βαθμό ευαισθησίας και κρισιμότητας των δεδομένων.

11.3 Προστασία των Αντιγράφων Ασφαλείας

Διασφαλίστε ότι τα ληφθέντα αντίγραφα ασφαλείας προστατεύονται με κρυπτογράφηση τόσο κατά την αποθήκευση όσο και κατά τη μεταφορά τους. Αυτό περιλαμβάνει τα απομακρυσμένα αντίγραφα, καθώς και τις αντίστοιχες υπηρεσίες cloud.

11.4 Καθιέρωση και Συντήρηση μιας Απομονωμένης Μονάδας Αντιγράφων Ασφαλείας

Διασφαλίστε ότι όλα τα αντίγραφα ασφαλείας αποθηκεύονται σε τουλάχιστον έναν (1) offline προορισμό, που δεν είναι συνδεδεμένος σε κάποιο δίκτυο.

11.5 Δοκιμή Επαναφοράς Δεδομένων

Να εκτελείτε δοκιμαστικές επαναφορές δεδομένων από τα αντίγραφα ασφάλειες σε τακτά χρονικά διαστήματα.
Διενεργήστε έλεγχο ακεραιότητας των αντιγράφων ασφαλείας σε περιοδική βάση.
Διενεργήστε δοκιμή επαναφοράς δεδομένων (restoration), ώστε να διασφαλίσετε ότι η λήψη αντιγράφων λειτουργεί με σωστό τρόπο.

## Control 12

12.1 Έλεγχος Ενημερώσεων Δικτυακής Υποδομής
**Βήματα:**
Χρησιμοποιήστε το μητρώο καταγραφής από το μέτρο ασφάλειας "1.1 Δημιουργία και διαχείριση λεπτομερούς μητρώου παγίων/συσκευών " για την καταμέτρηση το δικτυακών συσκευών.
Ενημερωθείτε για τις τελευταίες ενημερώσεις από επίσημες πήγες κατασκευαστών και προμηθευτών.
Προχωρήστε στις ενημερώσεις
Ενημερώστε καταλληλά το μητρώο καταγραφής παγίων/συσκευών(Hardware Assets)

12.2 Σχεδίαση και Συντήρηση Ασφαλούς Αρχιτεκτονικής Δικτύου

Φροντίστε να ομαδοποιήσετε και να διαχωρίσετε το δίκτυο του οργανισμού. Ανάλογα μες τις προσφερόμενες υπηρεσίες εγκαθιδρύστε μια Demilitarized Zone (DMZ)
https://www.isa.org/intech-home/2017/november-december/features/three-keys-designing-configuring-secure-networks
https://www.isa.org/intech-home/2017/november-december/features/three-keys-designing-configuring-secure-networks
https://www.hindawi.com/journals/scn/2021/6694650/
https://www.incibe-cert.es/en/blog/secure-network-architecture-things-order
https://rsmus.com/what-we-do/services/risk-advisory/the-ultra-secure-network-architecture.html

12.3 Ασφαλή Διαχείριση Δικτυακής Υποδομής

Για την ασφαλή διαμόρφωση συμβουλευτείτε
https://learn.cisecurity.org/benchmarks

12.4 Καθιέρωση και Συντήρηση Διαγράμματος Δικτύου

Σχεδιάστε και συντηρήστε ένα διάγραμμα που χαρτογραφεί όλο το δίκτυο του οργανισμού. Να το ενημερώνετε όταν γίνονται αλλαγές στο δίκτυο ή όταν γίνεται αντικατάσταση συσκευών.

12.5 Κεντρικοποίηση Δικτυακής Ταυτοποίησης, Εξουσιοδότησης και Ελέγχου (Authentication, Authorization, and Auditing)

Συγκεντρώστε σε ένα σύστημα την ταυτοποίηση, την εξουσιοδότηση και τον έλεγχο του δικτύου του οργανισμού.(Centralized AAA)
Έλεγχος ταυτοποίησης, εξουσιοδότησης και ελεγκτικής (AAA) είναι ένας μηχανισμός ελέγχου πρόσβασης σε IT πόρους του οργανισμού, την επιβολή πολιτικών, τον έλεγχο χρήσης και την παροχή των απαραίτητων δεδομένων . Αυτές οι συνδυασμένες διαδικασίες θεωρούνται σημαντικές για την αποτελεσματική διαχείριση και ασφάλεια του δικτύου.
https://www.techtarget.com/searchsecurity/definition/authentication-authorization-and-accounting
https://en.wikipedia.org/wiki/RADIUS
https://www.techtarget.com/searchsecurity/definition/RADIUS

12.6 Χρήση ασφαλούς Διαχείρισης Δικτύου και Πρωτοκόλλων

Ενεργοποιήστε ασφαλή πρωτόκολλα επικοινωνίας και διαχείρισης (π.χ., 802.1X, Wi-Fi Protected Access 2 (WPA2) Enterprise or greater).
Αυτό το μέτρο αφορά την χρήση ασφαλών πρωτοκόλλων μέσα στο δίκτυο του οργανισμού, όπως για παράδειγμα: 802.1X, Wi-Fi Protected Access, IPsec, HTTPS, SSL/TLS, SSH

12.7 Χρήση VPN Απομακρυσμένης Πρόσβασης και Σύνδεση σε Σύστημα AAA

Βεβαιωθείτε ότι οι τελικοί χρήστες συνδέονται μέσω του VPN στο δίκτυο του οργανισμού.
Ένα Virtual Private Network (VPN) επεκτείνει το εσωτερικό δίκτυο σε ένα δημόσιο δίκτυο και επιτρέπει στους χρήστες να στέλνουν και να λαμβάνουν δεδομένα σε κοινόχρηστα ή δημόσια δίκτυα σαν να ήταν απευθείας συνδεδεμένες οι υπολογιστικές τους συσκευές στο εσωτερικό δίκτυο. Τα οφέλη ενός VPN περιλαμβάνουν τις αυξήσεις στη λειτουργικότητα, την ασφάλεια και τη διαχείριση του εσωτερικού δικτύου. Παρέχει πρόσβαση σε πόρους που δεν είναι προσβάσιμοι στο δημόσιο δίκτυο και χρησιμοποιούνται συνήθως για χρήστες τηλεργασίας.
Η συνήθης υλοποίηση point-side ενός VPN για οργανισμούς απαιτεί χρήση ενός VPN Gateway, το οποίο μπορεί να είναι μια δικτυακή συσκευή ή ένα εξειδικευμένο σύστημα με ειδικό εξοπλισμό hardware.

12.8 Καθιέρωση και Συντήρηση Διαχωρισμένης Υποδομής για Διαχειριστικές Εργασίες

Διαχωρίστε την υποδομή που απαιτείται για τη διαχείριση από τον κύριο κορμό του δικτύου. Αυτή η συγκεκριμένη υποδομή θα πρέπει να είναι απομονωμένη από το παγκόσμιο διαδίκτυο.

## Control 13

13.1 Κεντρικοποίηση Ειδοποιήσεων Ασφάλειας

Το SIEM σημαίνει security information and event management και παρέχει στους οργανισμούς δυνατότητες εντοπισμού, ανάλυσης και ανταπόκρισης. Το λογισμικό SIEM συνδυάζει τη διαχείριση πληροφοριών ασφαλείας (SIEM) και τη διαχείριση συμβάντων ασφαλείας (SEM) για την ανάλυση των ειδοποιήσεων ασφαλείας που παράγονται από εφαρμογές και συσκευές του δικτύου σε πραγματικό χρόνο. Το λογισμικό SIEM αντιστοιχεί συμβάντα με κανόνες και μηχανές ανάλυσης και τα απαριθμεί για δευτερεύουσα αναζήτηση ώστε να ανιχνεύσει και να αναλύσει προηγμένες απειλές χρησιμοποιώντας παγκόσμια συλλογή πληροφοριών. Αυτό δίνει στις ομάδες ασφαλείας πληροφορίες αλλά και ιστορικό των δραστηριοτήτων στο IT περιβάλλον του οργανισμού, παρέχοντας με αυτό τον τρόπο ανάλυση δεδομένων, συσχέτιση συμβάντων, συγκέντρωση, αναφορά και διαχείριση αρχείων καταγραφής.

Ενδεικτικά κάποια εργαλεία :
https://azure.microsoft.com/en-us/services/microsoft-sentinel/#:~:text=Microsoft%20Sentinel%20is%20a%20cloud,data%20across%20an%20enterprise%E2%80%94fast.

https://www.manageengine.com/products/eventlog/?utm_source=Comparitech&utm_medium=Website-cpc&utm_campaign=ELA-SIEMTools

https://www.softwaretestinghelp.com/siem-tools

13.2 Εγκατάσταση Host-Based Instruction Detection System

Ένα Host- Based IDS (HIDS) είναι ένα σύστημα ανίχνευσης εισβολής που παρακολουθεί το σύστημα στο οποίο είναι εγκατεστημένο, αναλύοντας την κυκλοφορία και καταγράφοντας κακόβουλη συμπεριφορά. Ένα HIDS σάς δίνει σε βάθος ορατότητα σχετικά με το τι συμβαίνει στα κρίσιμα συστήματα σας. Με αυτό, μπορείτε να εντοπίσετε και να απαντήσετε σε κακόβουλες ή ανώμαλες δραστηριότητες που ανακαλύπτονται στο δίκτυο του οργανισμού σας.

Ενδεικτικά κάποια εργαλεία :
https://www.ossec.net/
https://www.splunk.com/

https://quadrantsec.com/sagan_log_analysis_engine/
https://www.snort.org/

13.3 Εγκατάσταση Network Instruction Detection System

Ένα Network IDS (NIDS) χρησιμοποιείται για την παρακολούθηση και ανάλυση της κυκλοφορίας του δικτύου και για την προστασία ενός συστήματος από απειλές που βασίζονται στο δίκτυο.
Ένα NIDS διαβάζει όλα τα εισερχόμενα πακέτα και αναζητά τυχόν ύποπτα μοτίβα. Όταν εντοπίζονται απειλές, με βάση τη σοβαρότητά τους, το σύστημα μπορεί να λάβει μέτρα, όπως να ειδοποιήσει τους διαχειριστές ή να εμποδίσει την πρόσβαση της διεύθυνσης IP προέλευσης στο δίκτυο.
https://www.comodo.com/siem/network-ids.php
Ενδεικτικά κάποια εργαλεία :
https://suricata.io/
https://www.snort.org/
https://www.splunk.com/
https://securityonionsolutions.com/
https://www.paloaltonetworks.com/cyberpedia/what-is-an-intrusion-detection-system-ids

13.4 Έλεγχος Δικτυακής Κίνησης Μεταξύ Τμημάτων του Δικτύου

Ο διαχωρισμός(τμηματοποίηση) δικτύου είναι μια αρχιτεκτονική που διαχωρίζει ένα δίκτυο σε μικρότερα τμήματα ή υποδίκτυα. Κάθε τμήμα δικτύου λειτουργεί ως το δικό του δίκτυο, το οποίο παρέχει στις ομάδες ασφαλείας αυξημένο έλεγχο της κίνησης που ρέει στα συστήματά τους.
Αυτό το μέτρο ασφάλειας απαιτεί τον έλεγχο της δικτυακής κίνησης μεταξύ των τμημάτων του δικτύου.

13.5 Διαχείριση Ελέγχου Πρόσβασης για τις Απομακρυσμένες Συσκευές του Οργανισμού

Ρυθμίστε κατάλληλα το δίκτυο ώστε να ελέγχει τις προϋποθέσεις που πρέπει να πληρούν οι απομακρυσμένες συσκευές προκειμένου να συνδεθούν σε πόρους του πληροφοριακού συστήματος του οργανισμού. Προσδιορίστε τον έλεγχο πρόσβασης με βάση: το εγκατεστημένο ενημερωμένο antivirus λογισμικό, τη συμφόρηση ρυθμίσεων σύμφωνα με τις προκαθορισμένες πολιτικές του οργανισμού και την επιβεβαίωση ότι το λειτουργικό σύστημα και οι εγκατεστημένες εφαρμογές έχουν πάρει τις τελευταίες ενημερώσεις.
Το μέτρο ασφάλειας μπορεί να υλοποιηθεί μέσω ενός VPN Gateway.

13.6 Συλλογή Αρχείων Καταγραφής Ροής Δικτύου

Συλλέξτε τα αρχεία καταγραφής ροής της κίνησης του δικτύου από τις δικτυακές συσκευές του οργανισμού

13.7 Εγκατάσταση Host-Based Intrusion Prevention System

Ένα Host-Based Intrusion Prevention System (HIPS) προστατεύει τα σύστημά σας από κακόβουλο λογισμικό και ανεπιθύμητη δραστηριότητα. Το HIPS χρησιμοποιεί προηγμένη ανάλυση συμπεριφοράς σε συνδυασμό με τις δυνατότητες ανίχνευσης του φιλτραρίσματος δικτύου για την παρακολούθηση εκτελούμενων διεργασιών, αρχείων και registry. Το HIPS είναι ξεχωριστό από την προστασία συστήματος σε πραγματικό χρόνο (Real-Time AV) και δεν είναι τείχος προστασίας (Firewall). Παρακολουθεί μόνο διαδικασίες που εκτελούνται εντός του λειτουργικού συστήματος.
Ενδεικτικά κάποια εργαλεία :
https://zeek.org/
https://www.fail2ban.org/wiki/index.php/Main_Page
https://openwips-ng.org/

https://www.ossec.net/
https://www.splunk.com/
https://www.snort.org/
EDR:
https://voodooshield.com/
https://github.com/ComodoSecurity/openedr
https://www.osarmor.com/
https://www.fortinet.com/products/endpoint-security/fortiedr

13.8 Εγκατάσταση Network Intrusion Prevention System

Ενδεικτικά κάποια εργαλεία :
https://www.datadoghq.com/dg/security/network-threat-monitoring/?utm_source=advertisement&utm_medium=review-site&utm_campaign=dg-comparitech-security-ww-ipstools/
https://www.splunk.com/
https://quadrantsec.com/sagan_log_analysis_engine/
https://www.ossec.net/
https://openwips-ng.org/
http://www.fail2ban.org/wiki/index.php/Main_Page
https://zeek.org/

13.9 Υλοποίηση Ελέγχου Πρόσβασης σε Επίπεδο θυρών Δικτύου

Τα τοπικά δίκτυα αναπτύσσονται συχνά με τρόπο που επιτρέπει σε μη εξουσιοδοτημένους υπολογιστές να συνδέονται στο δίκτυο. Επίσης, η χρήση υπηρεσιών DHCP και η μη διαμόρφωση καθιστούν την πρόσβαση σε υπηρεσίες δικτύου εύκολα διαθέσιμη. Αυτό εκθέτει το δίκτυο σε μη εξουσιοδοτημένη χρήση και κακόβουλες επιθέσεις. Ενώ η πρόσβαση στο δίκτυο θα πρέπει να είναι εύκολη, η ανεξέλεγκτη και μη εξουσιοδοτημένη πρόσβαση συνήθως δεν είναι επιθυμητή. Το 802.1X απλοποιεί τη διαχείριση ασφάλειας παρέχοντας έλεγχο πρόσβασης μαζί με τη δυνατότητα ελέγχου προφίλ χρηστών από έναν έως και τρεις διακομιστές RADIUS, ενώ επιτρέπει σε έναν συγκεκριμένο χρήστη να χρησιμοποιεί τα ίδια έγκυρα διαπιστευτήρια χρήστη για πρόσβαση από πολλά σημεία του δικτύου.
https://techhub.hpe.com/eginfolib/networking/docs/switches/WB/15-18/5998-8152_wb_2920_asg/content/ch13.html

13.10 Υλοποίηση Ελέγχου στο Επίπεδο Εφαρμογών του TCP/IP

Τα application proxy firewalls είναι η πιο έξυπνη αρχιτεκτονική τείχους προστασίας. Με τον όρο έξυπνο, εννοούμε ότι ένα τείχος προστασίας διακομιστή μεσολάβησης εφαρμογής μπορεί να εκτελέσει την πιο λεπτομερή επιθεώρηση δεδομένων πριν λάβει μια απόφαση φιλτραρίσματος. Ένα proxy firewall μεσολάβησης εφαρμογής μπορεί να αποκωδικοποιήσει και να επεξεργαστεί στο επίπεδο εφαρμογής τα δεδομένα που περιέχονται στα πακέτα. Κατά συνέπεια, τα application proxy μπορούν να φιλτράρουν με βάση το πραγματικό περιεχόμενο δεδομένων της εφαρμογής. Ενα firewall 4ου επιπέδου TCP/IP, είναι σε θέση απλώς να επιτρέπει ή να απορρίπτει την κυκλοφορία με βάση δεδομένα όπως το πρωτόκολλο IP που χρησιμοποιείται. Ωστόσο, με ένα application proxy firewall, όχι μόνο γνωρίζει εάν πρέπει να επιτρέπει ή να απορρίπτει την κυκλοφορία HTTP, αλλά μπορεί επίσης να ρυθμιστεί ώστε να φιλτράρει με βάση τον τύπο της κίνησης HTTP. Μια τέτοια διαμόρφωση επιτρέπει σε ένα τείχος application proxy firewall να διερευνά τα δεδομένα και να αναγνωρίζει κακόβουλη κυκλοφορία ιστού, όπως και να μπορεί να διακρίνει μεταξύ της κανονικής κίνησης HTTP και της κυκλοφορίας HTTP με κόκκινο κώδικα και να φιλτράρει ανάλογα. Αυτή η δυνατότητα δίνει στους διαχειριστές του firewall μια τεράστια ευελιξία και έλεγχο σχετικά με το ποια κίνηση θα επιτρέπεται και ποια δεν θα επιτρέπεται.
https://www.sciencedirect.com/topics/computer-science/application-layer-filtering#:~:text=Application%20Layer%20Filtering%20(ALF)%20is,that%20occur%20at%20this%20layer

.&text=Application%20of%20HTTP%20filtering%20to%20all%20client%20connections
https://www.jigsawacademy.com/blogs/cyber-security/proxy-firewall/
Ενδεικτικά κάποια εργαλεία :
https://www.cloudflare.com/products/cloudflare-spectrum/
https://www.f5.com/products/nginx
https://www.f5.com/products/security/advanced-waf
https://www.wallarm.com/
https://www.g2.com/products/imperva-app-protect/reviews
https://aws.amazon.com/waf/
https://www.cloudflare.com/waf/

13.11 Ρύθμιση Επιπέδου Ειδοποιήσεων για Συμβάντα Ασφάλειας

Οι κανόνες των συμβάντων ασφάλειας δεν είναι τίποτα άλλο από το, "Αυτό το πράγμα συνέβη πολλές φορές σε αυτό το χρονικό διάστημα...". ή συνδυασμός τέτοιων πραγμάτων. Οι κατάλληλες μετρήσεις και τα κατώφλια στο περιβάλλον σας είναι πολύ διαφορετικά από άλλα περιβάλλοντα. Αυτά τα όρια πρέπει να προσαρμοστούν ακριβώς μεταξύ της «κανονικής» κίνησης στο περιβάλλον σας και της μη κανονικής κίνησης. Αυτό απαιτεί τη δημιουργία ενός επιπέδου κανονικότητας δικτύου εκτελώντας το σύστημα για αρκετές εβδομάδες και αναλύοντας την κίνηση για να γνωρίζουμε τα κατάλληλα όρια για κάθε κανόνα. Λίγοι οργανισμοί αφιερώνουν χρόνο για να συντονίσουν το SIEM στο πραγματικό περιβάλλον τους.

https://blog.corserva.com/siem-optimization

## Control 14

14.1 Καθιέρωση και Συντήρηση Προγράμματος Εκπαίδευσης και Ευαισθητοποίησης σε Θέματα Κυβερνοασφάλειας

Οι εργαζόμενοι χρήστες διαδραματίζουν ιδιαίτερα κρίσιμο ρόλο για την ασφάλεια των συστημάτων πληροφορικής. Η έλλειψη εκπαίδευσης και αντίστοιχης ευθύνης για το θέμα αυτό εγκυμονεί διάφορα είδη απειλών για τους Οργανισμούς:
• Επιθέσεις κοινωνικής μηχανικής (social engineering attacks): λόγω της βελτίωσης των τεχνολογιών προστασίας τα τελευταία χρόνια, οι επιτιθέμενοι στοχεύουν πλέον στη μεγαλύτερη ευπάθεια, που είναι ο ανθρώπινος παράγοντας. Η μεγάλη πλειοψηφία των κυβερνοεπιθέσεων σήμερα ξεκινά με ένα phishing email, το οποίο περιέχει είτε ένα κακόβουλο συνημμένο αρχείο είτε ένα σύνδεσμο (link) προς μία κακόβουλη ιστοσελίδα. Εάν ο χρήστης εξαπατηθεί, τότε και στις δύο περιπτώσεις ο επιτιθέμενος μπορεί να αποκτήσει τον πλήρη έλεγχο των συστημάτων του Οργανισμού.
• Εκ των έσω απειλή (insider threat): δυσαρεστημένοι εργαζόμενοι ενδέχεται να αποκαλύψουν κρίσιμα δεδομένα του Φορέα, καθώς και να προκαλέσουν σκόπιμη διαγραφή ή άλλη ζημιά σε πόρους του.
• Φορητά μέσα αποθήκευσης και ιδιόκτητες συσκευές: η έλλειψη πολιτικής του Οργανισμού για την ορθή χρήση των φορητών μέσων αποθήκευσης και των ιδιοκτητών συσκευών, καθώς και η αντίστοιχη έλλειψη τεχνικών γνώσεων από μέρους των χρηστών μπορούν να προκαλέσουν μόλυνση με κακόβουλο λογισμικό εάν μία τέτοια συσκευή συνδεθεί στο δίκτυο του Οργανισμού.

Αναπτύξτε και καταγράψτε:
- πολιτική εκπαίδευσης χρηστών σε θέματα κυβερνοασφάλειας, που θα περιγράφει σκοπό, πεδίο εφαρμογής, ρόλους και ευθύνες,
- διαδικασίες υλοποίησης της πολιτικής και των σχετικών μέτρων προστασίας.

Οργανώστε ένα εκπαιδευτικό πρόγραμμα ευαισθητοποίησης και ενημέρωσης του προσωπικού για θέματα κυβερνοασφάλειας, που θα αφορά στο σύνολο των εργαζομένων και θα διενεργείται τουλάχιστον δύο (2) φορές το χρόνο. Η ύλη του προγράμματος θα περιλαμβάνει: α) την αλληλεπίδραση του χρήστη με

τις συσκευές και το δίκτυο με ασφαλή τρόπο, β) τη δημιουργία ισχυρών κωδικών πρόσβασης και την πολυπαραγοντική αυθεντικοποίηση, γ) την ανίχνευση διαφόρων μορφών επιθέσεων κοινωνικής μηχανικής (όπως π.χ. phishing emails, τηλεφωνικές κλήσεις πλαστοπροσωπίας κ.α.), δ) την αναγνώριση ενδείξεων παραβίασης συστημάτων και περιστατικών εκ των έσω απειλών (insider threats).

14.2 Εκπαίδευση στην Αναγνώριση Επιθέσεων Κοινωνικής Μηχανικής

Η εκπαίδευση του ανθρώπινου δυναμικού θα έχει στόχο την αναγνώριση επιθέσεων κοινωνικής μηχανικής(πχ. Phishing, pre-texting, tailgating)

14.3 Εκπαίδευση στην Εφαρμογή Καλόν Πρακτικών σε Θέματα Αυθεντικοποίησης

Η εκπαίδευση του ανθρώπινου δυναμικού θα έχει στόχο την καλύτερη διαχείριση πρακτικών αυθεντικοποίησης, π.χ. MFA οπού αυτό υποστηρίζεται, σύνθεση κωδικού, γενική διαχείριση στοιχειών πρόσβασης(credentials)

14.4 Εκπαίδευση στην Εφαρμογή Καλών Πρακτικών σε Θέματα Διαχείρισης Δεδομένων (ευαίσθητων και μη)

Η εκπαίδευση του ανθρώπινου δυναμικού θα έχει στόχο την εφαρμογή καλών πρακτικών σε θέματα διαχείρισης δεδομένων. Πιο συγκεκριμένα την σωστή αναγνώριση, αποθήκευση, μεταφορά και διαγραφή ευαίσθητων δεδομένων. Η εκπαίδευση θα εμπερικλείει και το κλείδωμα οθόνης, «καθαρό γραφείο» δηλ. να μην αφήνουν οι υπάλληλοι ευαίσθητα δεδομένα σε εκτυπωμένη μορφή ή χειρόγραφες ς στο γραφείο τους. Διαγραφή πληροφοριών σε πίνακες παρουσιάσεων. Όπως και την ορθή αποθήκευση συσκευών και δεδομένων του οργανισμού σε ασφαλισμένα ντουλάπια/συρτάρια ή άλλους ειδικούς χώρους.

14.5 Εκπαίδευση στην Αποφυγή Ακούσιας Έκθεσης Ευαίσθητων Δεδομένων

Η εκπαίδευση του ανθρώπινου δυναμικού θα έχει στόχο την αναγνώριση πιθανών αιτίων και αποφυγή ακουσίας έκθεσης ευαίσθητων δεδομένων. Παραδείγματα θεμάτων μπορεί να είναι η λανθασμένη αποστολή μέσω email, απώλεια φορητών μέσων αποθήκευσης, δημοσίευση δεδομένων σε μη κατάλληλους ισότοπους ή σε μη κατάλληλο κοινό.

14.6 Εκπαίδευση στην Αναγνώριση και Αναφορά Συμβάντων Κυβερνοασφάλειας

Εκπαιδεύεται το ανθρώπινο δυναμικό καταλληλά, έτσι ώστε να είναι σε θέση να αναγνωρίζει ένα πιθανό συμβάν κυβερνοασφάλειας και να το αναφέρει στο αρμόδιο πρόσωπο/ομάδα/αρχή.

14.7 Εκπαίδευση στην Αναγνώριση και Αναφορά Έλλειψης Ενημερώσεων Ασφάλειας

Εκπαιδεύεται το ανθρώπινο δυναμικό καταλληλά έτσι ώστε να είναι σε θέση να αναγνωρίζει την έλλειψη ή αποτυχία εγκατάστασης ενημερώσεων ασφάλειας στις συσκευές (PC & κινητά τηλεφωνά) τους. Όπως και να ερημώνεται το κατάλληλο τμήμα πληροφορικής/υποστήριξης για την επιδιόρθωση.

14.8 Εκπαίδευση στην Ασφαλή Σύνδεση στον Παγκόσμιο Ιστό

Εκπαιδεύεται το ανθρώπινο δυναμικό, που εργάζεται εξ αποστάσεως, καταλληλά έτσι ώστε να είναι σε θέση να αναγνωρίζει τους κίνδυνους σύνδεσης μέσω μη ασφαλών δικτυών. Αυτό μπορεί να συμπεριλαμβάνει δημόσια σημεία σύνδεσης Wifi (wifi public access points), την δικτυακή υποδομή στις οικίες των υπάλληλων κ.α..

14.9 Εκπαίδευση με Βάση Διακριτούς Ρόλους

Να διεξάγονται εξειδικευμένες εκπαιδεύσεις με βάση του διακριτούς ρόλους των εργαζομένων μέσα στον οργανισμό. Για παράδειγμα, κατάλληλες εκπαιδεύσεις κυβερνοασφάλειας διαχειριστών συστημάτων πληροφορικής, OWASP Top10 εκπαιδεύσεις για την αναγνώριση και αποφυγή ευπαθειών στην ανάπτυξη εφαρμογών/λογισμικού για τους προγραμματιστές, προχωρημένες εκπαιδεύσεις ενάντια σε επιθέσεις κοινωνικής μηχανικής σε πρόσωπα με περισσότερες ή πιο συγκεντρωτικές ευθύνες και γραμματειακή υποστήριξη.
Διενεργήστε, σε τακτική βάση, εκπαιδευτικά προγράμματα ευαισθητοποίησης βασισμένα σε διακριτούς ρόλους και στοχευμένα σε διαφορετικές κατηγορίες εργαζομένων με βάση το επίπεδο τεχνικής εξειδίκευσης.

## Control 15

15.1 Καθιέρωση και Συντήρηση Μητρώου Καταγραφής Παρόχων Υπηρεσιών

Το μητρώο καταγραφής πρέπει να περιλαμβάνει, τουλάχιστον, τα παρακάτω στοιχεία:
-Όνομα Παρόχου
-Υπηρεσία/Αγαθό
-Ημερομηνίες Παροχής/Συμβολαίου
-Υπεύθυνος
-Κατηγορία
-Επικοινωνία/Υποστήριξη
-Άξονες Συμφωνίας

15.2 Καθιέρωση και Συντήρηση Πολιτικής Διαχείρισης Παρόχων Υπηρεσιών

Καθιερώστε και συντηρήστε μια πολιτική διαχείρισης των παρόχων υπηρεσιών. Θα πρέπει να καθορίζει την κατηγοριοποίηση, την καταγραφή, την αξιολόγηση, την παρακολούθηση συμμόρφωσης, τον παροπλισμό των υπηρεσιών και το επίπεδο κυβερνοασφάλειας . Επιθεωρήστε και ενημερώστε την πολιτική σε ετήσια βάση ή πιο σύντομά άμα προκύψει ανάγκη για αλλαγή.

15.3 Κατηγοριοποίηση Παρόχων Υπηρεσιών

Στη σύσταση της πολιτικής για τη διαχείριση των παρόχων υπηρεσιών (15.2) καθορίστε μια κατηγοριοποίηση αυτών των παρόχων. Επιβεβαιώστε ότι εμπεριέχει μια ή περισσότερες κατηγορίες, οι οποίες θα μπορούσαν να είναι: επίπεδο ευαισθησίας δεδομένων, πλήθος δεδομένων, επίπεδο διαθεσιμότητας, εφαρμογή νομοθεσιών, μεταφερόμενο ρίσκο. Επιθεωρήστε και ενημερώστε την κατηγοριοποίηση σε ετήσια βάση ή πιο σύντομα, αν προκύψει ανάγκη για αλλαγή.

15.4 Επιβεβαίωση Απαιτήσεων Ασφάλειας σε Παρεχόμενες Υπηρεσίες

Επιβεβαιώστε ότι οι πάροχοι υπηρεσιών λαμβάνουν τα κατάλληλα μέτρα σε θέματα κυβερνοασφάλειας . Αυτή μπορεί να είναι: ελάχιστες απαιτήσεις ασφάλειας λογισμικού που χρησιμοποιείται , ενημέρωση σε περίπτωση συμβάντος κυβερνοασφάλειας και παραβίαση εμπιστευτικότητας δεδομένων, απαιτήσεις κρυπτογράφησης δεδομένων, κ.α. Αυτές οι απαιτήσεις πρέπει να συμπεριληφθούν στην πολιτική διαχείρισης παρόχων υπηρεσιών (15.2). Επιθεωρήστε και ενημερώστε την πολιτική σε ετήσια βάση ή πιο σύντομά, άμα προκύψει ανάγκη για αλλαγή

15.5 Αξιολόγηση Παρόχων Υπηρεσιών

Αξιολογήστε την συνέπεια των παρόχων υπηρεσιών σε θέματα κυβερνοασφάλειας με βάση την πολιτική διαχείρισης παρόχων υπηρεσιών (15.2). Το πεδίο εφαρμογής της αξιολόγησης μπορεί να ποικίλλει σύμφωνα με την κατηγοριοποίηση που έχει οριστεί στην πολιτική και μπορεί να περικλείει τυποποιημένες εκθέσεις αξιολόγησης όπως: Service Organization Control 2 (SOC 2), Payment Card Industry,(PCI) Attestation of Compliance (AoC), ερωτηματολόγια, ή άλλες διαδικασίες αξιολόγησης. Εκτελείτε την αξιολόγηση σε ετήσια βάση ή πιο συχνά άμα προκύψει ανάγκη.

15.6 Παρακολούθηση Παρόχων Υπηρεσιών

Παρακολούθηση των παρόχων υπηρεσιών σύμφωνα με την πολιτική διαχείρισης παρόχων υπηρεσιών (15.2) που έχει συσταθεί. Η παρακολούθηση μπορεί να γίνεται μέσω της επαναξιολόγησης συμμόρφωσης με βάση τα συμβόλαια,τον οδηγό λειτουργίας/συμβόλαιο παροχής και το dark web monitoring

15.7 Ασφαλής και Ελεγχόμενος Παροπλισμός Παρεχόμενων Υπηρεσιών

Ορίστε και διασφαλίστε διαδικασία για τον ασφαλή και ελεγχόμενο παροπλισμό των υπηρεσιών του παρόχου. Αυτή μπορεί να αφορά την απενεργοποίηση λογαριασμών χρηστών και πρόσβασης, τον τερματισμό ροών δεδομένων, την ελεγχόμενη και ασφαλή διαγραφή δεδομένων που ήταν αποθηκευμένα στην υποδομή του παρόχου.

## Control 16

16.1 Καθιέρωση και Συντήρηση Διαδικασίας Ασφαλούς Ανάπτυξης Λογισμικού

Συστάσεις/ Βοηθητικοί σύνδεσμοι:
https://owaspsamm.org/model/design/security-architecture/
https://owasp.org/www-project-secure-coding-practices-quick-reference-guide/migrated_content
https://www.gartner.com/reviews/market/vulnerability-assessment
https://csrc.nist.gov/News/2020/mitigating-risk-of-software-vulns-ssdf
https://www.bsa.org/reports/updated-bsa-framework-for-secure-software
https://safecode.org/resource-publications/cis-controls/
https://csrc.nist.gov/News/2020/mitigating-risk-of-software-vulns-ssdf
https://owasp.org/

16.2 Καθιέρωση και Συντήρηση διαδικασίας Διευθέτησης και Αποδοχής Ευπαθειών λογισμού

Καθιερώστε και συντηρήστε μια διαδικασίας διευθέτησης και πιθανής αποδοχής ευπαθειών λογισμικούσυμπεριλαμβάνοντας ένα σύστημα/μέσο/πλατφόρμα για αναφορά ευπαθειών από εξωτερικές πήγες. Η διαδικασία θα αποτελείται από: πολιτική χειρισμού ευπαθειών που προσδιορίζει την διαδικασία αναφορών, υπεύθυνη οντότητα για το χειρισμό αναφορών ευπαθειών και μια διαδικασία για την εισαγωγή, ανάθεση, αποκατάσταση και έλεγχο αποκατάστασης. Ως μέρος της διαδικασίας χρησιμοποιήστε ένα σύστημα παρακολούθησης ευπαθειών το οποίο θα συμπεριλαμβάνει ταξινόμηση βαρύτητας (severity ratings) αλλά και στοιχεία για την μέτρηση χρονικών διαστημάτων για τον εντοπισμό, την ανάλυση και την αποκατάσταση των ευπαθειών. Επιθεωρήστε και ενημερώστε την διαδικασία σε ετήσια βάση ή πιο σύντομά άμα προκύψει ανάγκη για αλλαγή.

16.3 Εφαρμογή Ανάλυσης/Εξακρίβωσης Βαθύτερων Αίτιων για Ευπάθειες Ασφάλειας σε Λογισμό

Εφαρμόστει ανάλυση βαθύτερων αιτίων ευπαθειών. Όταν αναλύεται μια ευπάθεια πρέπει να εκτελείται και έλεγχος των βαθύτερων αίτιων που οδήγησαν στην εκδήλωση μιας οι περισσοτέρων ευπαθειών σε

επίπεδο κώδικα, έτσι ώστε να υπάρχει πλήρη εικόνα της ευπάθειας και των επιπτώσεων.

16.4 Καθιέρωση και Συντήρηση Μητρώου Καταγραφής Παρεχόμενου Λογισμικού

Καθιερώστε και συντηρήστε ένα μητρώο που θα καταγράφεται λογισμικό/κώδικας που έχει αναπτυχθεί από παράγοντες εκτός οργανισμού. Θα πρέπει να αναφέρεται και μια εκτίμηση ρίσκου για κάθε εγγραφή του μητρώου. Επιθεωρήστε και ενημερώστε το μητρώο τουλάχιστον σε μηνιαία βάση ή πιο σύντομά άμα προκύψει ανάγκη για αλλαγή και αξιολογήστε εάν το λογισμικό υποστηρίζεται.

16.5 Χρήση Ενημερωμένου Λογισμικού και Προμηθευόμενο από Επίσημες και Έμπιστες Πήγες

Το λογισμικό ή ο κώδικας που χρησιμοποιείται από εξωτερικές πήγες θα πρέπει να είναι ενημερωμένο και από έμπιστες/διαπιστευμένες πήγες. Εφόσον είναι δυνατόν, χρησιμοποιήστε δοκιμασμένο λογισμικό και βιβλιοθήκες το οποίο έχει ελεγχθεί ί σε θέματα ασφάλειας. Προμηθευτείτε το λογισμικό από έμπιστες πήγες ή ελέγξτε το λογισμικό για ευπάθειες.

16.6 Καθιέρωση και Συντήρηση Συστήματος Ταξινόμηση Βαρύτητας (Severity Rating)

Συστάσεις/ Βοηθητικοί σύνδεσμοι:
https://www.synopsys.com/blogs/software-security/designing-severity-risk-ranking-systems/
https://nvd.nist.gov/vuln-metrics/cvss

16.7 Χρήση Προτύπων Βελτιστοποίησης Διαμόρφωσης Ασφάλειας για τα Συστήματα Εφαρμογών (Application Servers)
Συστάσεις/ Βοηθητική σύνδεσμοι:
CIS Benchmarks: https://www.cisecurity.org/cis-benchmarks/

16.8 Διαχωρισμός Συστημάτων Παραγωγής
Διαχωρίστε συστήματα παραγωγικά από μη παραγωγικά συστήματα

16.9 Εκπαίδευση Προγραμματιστών στις Αρχές Ασφαλούς Προγραμματισμού

Διασφαλίστε ότι όλοι οι προγραμματιστές του οργανισμού λαμβάνουν την απαραίτητη εκπαίδευση σύμφωνα με το προγραμματιστικό περιβάλλον και την θέση ευθύνης που καλύπτουν. Η εκπαίδευση μπορεί να καλύπτει γενικές αρχές κυβερνοασφάλειας και ασφάλειας λογισμικού. Επαναλάβετέ τις εκπαιδεύσεις σε ετήσια βάση και διαμορφώστε το εκπαιδευτικό πρόγραμμα έτσι ώστε να είναι σε θέση να αναπτύξει μια κουλτούρα κυβερνοασφάλειας μεταξύ της ομάδας των προγραμματιστών.

16.10 Εφαρμογή Αρχών Αρχιτεκτονικής Ασφάλειας στην Ανάπτυξη Λογισμικού

Συστάσεις/ Βοηθητικοί σύνδεσμοι:
https://blog.rsisecurity.com/what-is-the-purpose-of-cybersecurity-architecture/
https://www.sonarqube.org/features/security/owasp/?gads_campaign=ROW-2-Generic&gads_ad_group=OWASP&gads_keyword=owasp%20tool&gclid=CjwKCAiA24SPBhB0EiwAjBgkhtopBco1sVhbJa7wtbOxAM8IBUqkaQitZ6E-KQzBS62UESRMID62pRoCI08QAvD_BwE
https://owasp.org/www-project-web-security-testing-guide/
https://www.synopsys.com/blogs/software-security/attributes-of-secure-web-application-architecture/

16.11 Αξιοποίηση Γνωστών Μηχανισμών ή υπηρεσιών Ασφάλειας στο Λογισμικό που Αναπτύσσετε

Αξιοποιήστε γνωστούς μηχανισμούς ή υπηρεσίες για της ενότητες του λογισμικού που αναπτύσσετε,

όπως: identity management, κρυπτογράφηση, μητρώο ελέγχου(audit logs) και καταγραφής(logs). Η χρήση έτοιμων υλοποιήσεων από προγραμματιστικές πλατφόρμες σε κρίσιμες συναρτήσεις ασφάλειας μπορεί να μειώσει το φόρτο εργασίας των προγραμματιστών, την πιθανότητα σφαλμάτων σχεδιασμού και υλοποίησης. Σύγχρονα λειτουργικά σύστημα παρέχουν αποτελεσματικούς μηχανισμούς αναγνώρισης, ταυτοποίησης και εξουσιοδότησης και παρέχουν αυτούς τους μηχανισμούς σε εφαρμογές. Κάνετε χρήση γνωστών και ενημερωμένων προτύπων κρυπτογράφησης. Λειτουργικά συστήματα επίσης παρέχουν δυνατότητες χρήσης μητρώων καταγραφής και ελέγχου.

16.12 Εφαρμογή Ελέγχων Ασφαλείας σε Επίπεδο Κώδικα

Ενσωματώστε εργαλεία στατικής και δυναμικής ανάλυσης στο κύκλο ζωής μιας εφαρμογής για να βεβαιωθείτε ότι τηρούνται ασφαλές πρακτικές προγραμματισμού.
https://www.mitre.org/publications/systems-engineering-guide/enterprise-engineering/systems-engineering-for-mission-assurance/secure-code-review
https://www.codewetrust.com/

16.13 Διεξαγωγή Ελέγχου Εισβολής Εφαρμογών

Συστάσεις/ Βοηθητικοί σύνδεσμοι:
https://www.imperva.com/learn/application-security/penetration-testing/#:~:text=A%20penetration%20test%2C%20also%20known,web%20application%20firewall%20(WAF).
https://www.tenable.com/products/nessus
https://owasp.org/www-community/Vulnerability_Scanning_Tools

16.14 Διεξαγωγή Μοντελοποίησης Απειλών (Threat Modelling)

Το thread modelling είναι μια διαδικασία που έχει ως σκοπό τον εντοπισμό και τη διευθέτηση σφαλμάτων κατά τον σχεδιασμό ενός λογισμικού, πριν την υλοποίηση ή τη γραφή κώδικα . Εκτελείτε από ειδικά εκπαιδευμένα άτομα που αξιολογούν την αρχιτεκτονική του λογισμικού και καταγράφουν τους κινδύνους για την ασφάλεια για κάθε τρόπο επιδώσου και επιπέδου εξουσιοδότησης. Ο στόχος είναι η δομημένη καταγραφή της εφαρμογής, της αρχιτεκτονικής και της υποδομής ώστε να γίνουν κατανοητά τα μειονεκτήματα.

Συστάσεις/ Βοηθητικοί σύνδεσμοι:
https://owasp.org/www-community/Threat_Modeling
https://www.microsoft.com/en-us/download/details.aspx?id=49168
https://www.sans.org/white-papers/1646/

## Control 17

17.1 Ανάθεση Προσωπικού στην Διαχείριση Περιστατικών

Συστάσεις/ Βοηθητικοί σύνδεσμοι:
https://assets.contentstack.io/v3/assets/blt36c2e63521272fdc/blt0ad3c29a50dd218b/60d3a588bdf5ed4ae2de5b3d/Incident_Handling_-_Chain_Of_Custody_Form.pdf
https://www.sans.org/white-papers/1516/
https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf

17.2 Καθιέρωση και Συντήρηση Στοιχείων Επικοινωνίας για Αναφορά Περιστατικών Ασφάλειας

Συστάσεις/ Βοηθητικοί σύνδεσμοι:
https://assets.contentstack.io/v3/assets/blt36c2e63521272fdc/bltcb04a9ba5ca41996/60d39dda0504174

955a99fda/Incident_Handling_Forms_-_Incident_Contacts_List.pdf
https://www.sans.org/white-papers/1516/
https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf

17.3 Καθιέρωση και Συντήρηση Διαδικασίας Αναφοράς Περιστατικών για τον Οργανισμό

Συστάσεις/ Βοηθητικοί σύνδεσμοι:
https://www.sans.org/white-papers/1516/
https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf

17.4 Καθιέρωση και Συντήρηση Διαδικασίας Ανταπόκρισης σε Περιστατικό Κυβερνοασφάλειας

Συστάσεις/ Βοηθητικοί σύνδεσμοι:
https://www.sans.org/white-papers/1516/
https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf

17.5 Ανάθεση Ρόλων και Ευθυνών

Συστάσεις/ Βοηθητικοί σύνδεσμοι:https://www.sans.org/white-papers/1516/
https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf

17.6 Ορισμός Μέσων Επικοινωνίας εν μέσω Διαδικασίας Ανταπόκρισης Περιστατικού ασφάλειας

Συστάσεις/ Βοηθητικοί σύνδεσμοι:
https://www.sans.org/white-papers/1516/
https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf

17.7 Διεξαγωγή Ασκήσεων Προσομοίωσης Κυβερνοεπιθέσεων

Προγραμματίστε σε τουλάχιστον ετήσια βάση ασκήσεις που θα προσομοιώνουν κυβερνοεπιθέσεις διάφορων τύπων, με στόχο την εξάσκηση του προσωπικού που βρίσκονται σε ρόλους κλειδιά στην διαδικασία ανταπόκρισης σε περιστατικά κυβερνοασφάλειας. Στις ασκήσεις αξιολογήστε τα κανάλια επικοινωνίας, τη λήψη αποφάσεων και τις ροές καθηκόντων.
https://home.kpmg/content/dam/kpmg/ca/pdf/2017/10/cyber-incident-simulation-slipsheet-kpmg-canada.pdf

17.8 Ανασκόπηση μετά το Πέρας των Περιστατικών Ασφάλειας

Μετα το τέλος ενός περιστατικού ασφάλειας κάντε μια ανασκόπηση και μια αξιολόγηση για την καλύτερη κατανόηση της απειλής και της διαδικασίας. Εξάγετε συμπεράσματα και βρείτε κενά ή βελτιώστε τις πολιτικές /διαδικασίες/playooks ανταπόκρισης σε περιστατικά κυβερνοασφάλειας.

Συστάσεις/ Βοηθητικοί σύνδεσμοι:
https://www.sans.org/white-papers/1516/
https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf

17.9 Καθιέρωση και Συντήρηση Κλίμακας Ταξινόμησης Περιστατικών Κυβερνοασφάλειας

Καθιερώστε και συντηρήστε κλίμακες ταξινόμησης για περιστατικά ασφάλειας, κατά το ελάχιστο, διαχωρίζοντας περιστατικά από συμβάντα. Παραδείγματα μπορούν να αποτελούν: η μη κανονική δραστηριότητα, η ευπάθεια ασφάλειας, τα αδύναμα σημεία ασφάλειας, η έκθεση ευαίσθητων δεδομένων, το περιστατικό εμπιστευτικότητας κ.α. Επιθεωρήστε και ενημερώστε την ανάθεση σε ετήσια βάση ή πιο

σύντομά άμα προκύψει ανάγκη για αλλαγή.

## Control 18

18.1 Καθιερώστε και Συντηρήστε ένα Πρόγραμμα Ελέγχου Εισβολής Δικτυών και Συστημάτων
**Penetration test**
Τι είναι: Μέθοδος αξιολόγησης ασφάλειας Πληροφοριακών Συστημάτων (Η/Υ), προσομοιώνοντας κυβερνοεπίθεσεις από “κακόβουλους” χρήστες. Αφορά επίθεση για απόκτηση πρόσβασης σε υπηρεσίες, δεδομένα ή συστήματα χωρίς διαπιστευτήρια (username/password)
Σκοπός: Αύξηση / βελτίωση του επιπέδου ασφαλείας του συστήματος
Περιλαμβάνει:
- Ανάλυση συστήματος για εντοπισμό αδυναμιών/ευπαθειών (vulnerabilities)
- Εκμετάλλευση (exploitation) αδυναμιών/ευπαθειών
Θέστε του άξονες στους οποίους θα στηρίζεται το πρόγραμμα. Το πεδίο εφαρμογής, εσωτερικός/εξωτερικός έλεγχος, συχνότητα διεξαγωγής, διαδικασία και επιτήρηση επιδιόρθωσης, ανάθεση διεξαγωγής.

18.2 Περιοδική Διεξαγωγή Εξωτερικού Ελέγχου Εισβολής

Συστάσεις/ Βοηθητικοί σύνδεσμοι:
Ο έλεγχος μπορεί να ανατεθεί και σε εξωτερικούς συνεργάτες που εξειδικεύονται σε αυτό πεδίο και διαθέτουν τους κατάλληλους πόρους.

18.3 Επιδιόρθωση Ευρημάτων ελέγχου Εισβολής

Επιδιορθώστε τα ευρήματα του ελέγχου σύμφωνα με την αναφορά και τις πολικές του οργανισμού.

18.4 Επικύρωση Μέτρων Ασφάλειας

Επικυρώστε τα μέτρα ασφάλειας μετά από κάθε έλεγχο εισβολής δικτύων και συστημάτων αναλόγως με τα αποτελέσματα, τροποποιήστε κανόνες και μηχανισμούς ασφάλειας για την βέλτιστη ανταπόκριση.

18.5 Περιοδική Διεξαγωγή Εσωτερικού Ελέγχου Εισβολής

Διεξάγετε τουλάχιστον σε ετήσια βάση εσωτερικό έλεγχο εισβολής συστημάτων. Δηλαδή η ειδικευμένη ομάδα θα προσπαθήσει να εισβάλει από το εσωτερικό του δικτύου του πληροφοριακού συστήματος του οργανισμού. Διαχωρίστε σε Whitebox και Blackbox

## ΠΑΡΑΤΗΜΑ Ε' – Reverse Mapping με Οριζόντιο Άθροισμα

| CIS Safeguards ALL IG | Malware | Ransomeware | Web App Hacking | Insider and Privilege Misuse | Targeted Intrusion | Accumulated Horizontal Value |
|---|---|---|---|---|---|---|
| 1.1 | | | | | | |
| 1.2 | | | | | | |
| 1.3 | | | | | | |
| 1.4 | | | | | | |
| 1.5 | | | | | | |
| 2.1 | 3 | 3 | 1 | 2 | 3 | 12 |
| 2.2 | 3 | 3 | 1 | 2 | 3 | 12 |
| 2.3 | 30 | 31 | 22 | 18 | 18 | 119 |
| 2.4 | 3 | 3 | 1 | 2 | 3 | 12 |
| 2.5 | 35 | 40 | 30 | 21 | 26 | 152 |
| 2.6 | 2 | 7 | 10 | 2 | 7 | 28 |
| 2.7 | 12 | 28 | 19 | 9 | 17 | 85 |
| 3.1 | 3 | 6 | 2 | 11 | 6 | 28 |
| 3.2 | 3 | 5 | 1 | 8 | 4 | 21 |
| 3.3 | 13 | 23 | 9 | 28 | 24 | 97 |
| 3.4 | 3 | 1 | 1 | 3 | 2 | 10 |
| 3.5 | | | | | | |
| 3.6 | | | | | | |
| 3.7 | | | | | | |
| 3.8 | | | | | | |
| 3.9 | | | | | | |
| 3.1 | 7 | 5 | 4 | 9 | 6 | 31 |
| 3.11 | 1 | 5 | 4 | 10 | 8 | 28 |

| CIS Safeguards ALL IG | Malware | Ransomeware | Web App Hacking | Insider and Privilege Misuse | Targeted Intrusion | Accumulated Horizontal Value |
|---|---|---|---|---|---|---|
| 3.12 | 9 | 18 | 13 | 15 | 19 | 74 |
| 3.13 | | | | | | |
| 3.14 | | | | | | |
| 4.1 | 79 | 94 | 71 | 54 | 82 | 380 |

| | | | | | | |
|---|---|---|---|---|---|---|
| 4.2 | 20 | 18 | 18 | 9 | 16 | 81 |
| 4.3 | | | | | | |
| 4.4 | 20 | 20 | 16 | 11 | 19 | 86 |
| 4.5 | 6 | 7 | 6 | 2 | 6 | 27 |
| 4.6 | 1 | 1 | 2 | 1 | | 5 |
| 4.7 | 55 | 60 | 41 | 40 | 68 | 264 |
| 4.8 | 25 | 30 | 22 | 3 | 21 | 101 |
| 4.9 | 1 | | | | 1 | 2 |
| 4.1 | 3 | 2 | 4 | 4 | 2 | 15 |
| 4.11 | | | | | | |
| 4.12 | | | | | | |
| 5.1 | | 5 | 3 | 5 | 3 | 16 |
| 5.2 | 21 | 21 | 16 | 16 | 25 | 99 |
| 5.3 | 52 | 58 | 37 | 36 | 66 | 249 |
| 5.4 | 49 | 56 | 34 | 36 | 62 | 237 |
| 5.5 | 7 | 8 | 4 | 5 | 8 | 32 |
| 5.6 | | | | | | |
| 6.1 | 62 | 70 | 47 | 45 | 75 | 299 |
| 6.2 | 62 | 70 | 48 | 45 | 75 | 300 |
| 6.3 | 8 | 8 | 9 | 12 | 7 | 44 |
| 6.4 | 13 | 11 | 14 | 14 | 13 | 65 |
| 6.5 | 14 | 12 | 14 | 15 | 13 | 68 |
| 6.6 | | | | | | |
| 6.7 | | | | | | |
| 6.8 | 55 | 68 | 41 | 43 | 68 | 275 |
| 7.1 | 9 | 15 | 10 | 7 | 11 | 52 |
| 7.2 | 9 | 15 | 10 | 7 | 11 | 52 |
| 7.3 | 8 | 14 | 9 | 7 | 11 | 49 |
| 7.4 | 6 | 13 | 4 | 5 | 8 | 36 |

| CIS Safeguards ALL IG | Malware | Ransomeware | Web App Hacking | Insider and Privilege Misuse | Targeted Intrusion | Accumulated Horizontal Value |
|---|---|---|---|---|---|---|
| 7.6 | 13 | 17 | 18 | 1 | 9 | 58 |
| 7.7 | 13 | 15 | 18 | 2 | 8 | 56 |
| 8.1 | 3 | 1 | 1 | 4 | 3 | 12 |
| 8.2 | 3 | 2 | 1 | 4 | 3 | 13 |

| | | | | | | |
|---|---|---|---|---|---|---|
| 8.3 | 4 | 2 | 2 | 4 | 3 | 15 |
| 8.4 | | | | | | |
| 8.5 | | | | | 1 | 1 |
| 8.6 | | | | | | |
| 8.7 | | | | | | |
| 8.8 | | | | | | |
| 8.9 | 2 | 1 | 1 | 3 | 4 | 11 |
| 8.1 | 3 | 1 | 1 | 3 | 3 | 11 |
| 8.11 | | | | 0 | 1 | 1 |
| 8.12 | | | | | | |
| 9.1 | 1 | 1 | 1 | | | 3 |
| 9.2 | 3 | 1 | | | 3 | 7 |
| 9.3 | 16 | 13 | 6 | 6 | 10 | 51 |
| 9.4 | 2 | 2 | 1 | | | 5 |
| 9.5 | | | | | | |
| 9.6 | 7 | 9 | 3 | 3 | 5 | 27 |
| 9.7 | 4 | 4 | 1 | 3 | 4 | 16 |
| 10.1 | 6 | 7 | 2 | 4 | 6 | 25 |
| 10.2 | 6 | 7 | 2 | 4 | 6 | 25 |
| 10.3 | 1 | 1 | 1 | 4 | | 7 |
| 10.4 | | | 8 | | | 8 |
| 10.5 | 7 | 11 | | 1 | 6 | 25 |
| 10.6 | | | | | | |
| 10.7 | 5 | 7 | 2 | 4 | 6 | 24 |
| 11.1 | | 3 | | 7 | 2 | 12 |
| 11.2 | | | | 7 | 2 | 9 |
| 11.3 | 6 | 9 | 4 | 16 | 11 | 46 |
| 11.4 | 5 | 7 | 2 | 12 | 8 | 34 |
| 11.5 | | 3 | | 7 | 2 | 12 |

| CIS Safeguards ALL IG | Malware | Ransomeware | Web App Hacking | Insider and Privilege Misuse | Targeted Intrusion | Accumulated Horizontal Value |
|---|---|---|---|---|---|---|
| 12.1 | 1 | 1 | 1 | | 1 | 4 |
| 12.2 | 17 | 20 | 14 | 8 | 16 | 75 |
| 12.3 | | | | | | |
| 12.4 | | | | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| 12.5 | | | | | | |
| 12.6 | | | | | | |
| 12.7 | 3 | 4 | 3 | 2 | 2 | 14 |
| 12.8 | 18 | 18 | 11 | 13 | 17 | 77 |
| 13.1 | | | | | | |
| 13.2 | 12 | 13 | 3 | 4 | 9 | 41 |
| 13.3 | 31 | 28 | 4 | 2 | 25 | 90 |
| 13.4 | 9 | 7 | 7 | 3 | 7 | 33 |
| 13.5 | 3 | 4 | 3 | 1 | 2 | 13 |
| 13.6 | | | | | | |
| 13.7 | 12 | 13 | 4 | 4 | 9 | 42 |
| 13.8 | 31 | 28 | 6 | 2 | 25 | 92 |
| 13.9 | | | | | | |
| 13.1 | 7 | 7 | 4 | | 5 | 23 |
| 13.11 | | | | | | |
| 14.1 | 13 | 16 | 3 | 6 | 9 | 47 |
| 14.2 | 7 | 12 | 2 | 2 | 4 | 27 |
| 14.3 | 10 | 7 | 5 | 7 | 8 | 37 |
| 14.4 | 3 | 3 | 3 | 5 | 3 | 17 |
| 14.5 | | 1 | | 3 | | 4 |
| 14.6 | 7 | 12 | 2 | 2 | 4 | 27 |
| 14.7 | | | | | | |
| 14.8 | | | | | | |
| 14.9 | 2 | 2 | 1 | 3 | 2 | 10 |
| 15.1 | | | | | | |
| 15.2 | | | | | | |

| CIS Safeguards ALL IG | Malware | Ransomeware | Web App Hacking | Insider and Privilege Misuse | Targeted Intrusion | Accumulated Horizontal Value |
|---|---|---|---|---|---|---|
| 15.3 | | | | | | |
| 15.4 | | | | | | |
| 15.5 | | | | | | |
| 15.6 | | | | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| 15.7 | | 1 | 1 | 2 | | 4 |
| 16.1 | 13 | 11 | 4 | 11 | 10 | 49 |
| 16.2 | | 2 | 2 | 3 | 2 | 9 |
| 16.3 | | 2 | 3 | 3 | 2 | 10 |
| 16.4 | | 2 | 1 | 3 | 2 | 8 |
| 16.5 | | 2 | 1 | 3 | 2 | 8 |
| 16.6 | | | | | | |
| 16.7 | | | | | | |
| 16.8 | 5 | 7 | 6 | 4 | 5 | 27 |
| 16.9 | 9 | 9 | 3 | 9 | 8 | 38 |
| 16.1 | 10 | 12 | 8 | 7 | 9 | 46 |
| 16.11 | | 2 | 1 | 3 | 2 | 8 |
| 16.12 | | 2 | 1 | 3 | 2 | 8 |
| 16.13 | 4 | 5 | 6 | 1 | 6 | 22 |
| 16.14 | | | | | | |
| 17.1 | | | | | | |
| 17.2 | | | | | | |
| 17.3 | | | | | | |
| 17.4 | | | | | | |
| 17.5 | | | | | | |
| 17.6 | | | | | | |
| 17.7 | | | | | | |
| 17.8 | | | | | | |
| 17.9 | | | | | | |
| 18.1 | 2 | 2 | 1 | | 2 | 7 |
| 18.2 | 11 | 11 | 10 | 1 | 6 | 39 |
| 18.3 | 65 | 78 | 62 | 53 | 62 | 320 |
| 18.4 | | | | | | |
| 18.5 | 56 | 72 | 55 | 53 | 58 | 294 |