



Ιόνιο Πανεπιστήμιο
Τμήμα Πληροφορικής

Πτυχιακή Εργασία

***<<Μελέτη Αξιολόγησης κινδύνων για την Ασφάλεια
Πληροφοριών και διαδικασίες για τη προστασία πληροφοριών:
Μία μελέτη περίπτωσης>>***

Υποψήφιος : Παναγιώτης Πιπής Π2016080

Επιβλέπουσα : Τσώχου Αγγελική (Καθηγήτρια)

***Μελέτη Αξιολόγησης κινδύνων για την Ασφάλεια Πληροφοριών
και διαδικασίες για τη προστασία πληροφοριών μελέτης
περίπτωσης***

Η πτυχιακή εργασία εγκρίθηκε από :

Αναπληρώτρια Καθηγήτρια Τσώχου Αγγελική

Καθηγητής Εμμανουήλ Μάγκος μέλος της επιτροπής

Επίκουρος Καθηγητής Νταντογιάν Χριστόφορος μέλος της
επιτροπής

Ευχαριστίες

Ευχαριστώ τη καθηγήτρια Τσώχου Αγγελική για την καθοδήγηση που μου προσέφερε κατά τη διάρκεια των σπουδών μου και κατά τη διάρκεια της εκπόνησης της πτυχιακής μου εργασίας για την άψογη συνεργασία που είχαμε και για τις γνώσεις που απέκτησα όλο αυτό το διάστημα.

Περίληψη

Καθώς οι περισσότεροι οργανισμοί βασίζουν πλέον ένα μεγάλο μέρος της λειτουργίας τους σε πληροφοριακά συστήματα, η ανάγκη για κατάλληλη ασφάλεια αυξάνεται. Δυστυχώς, είναι δύσκολο να γίνει επιλογή των μέτρων ασφαλείας που χρειάζονται για να επιτευχθεί ικανοποιητική ασφάλεια. Αυτή η διπλωματική εργασία ασχολείται με την ανάλυση κινδύνων, μια διαδικασία που αναγνωρίζει τα προβλήματα ασφαλείας, τα ταξινομεί με βάση την σημαντικότητά τους και τέλος προτείνει λύσεις για την επίλυσή τους. Παρουσιάζονται οι διαφορετικοί τρόποι ανάλυσης κινδύνων, οι κυριότερες μέθοδοι που χρησιμοποιούνται σήμερα, τα πακέτα λογισμικού που κυκλοφορούν στην αγορά και τελικά γίνεται μια πρακτική εφαρμογή ανάλυσης κινδύνων στην επιχείρηση Εταιρεία Α.Ε. ένας εξειδικευμένος πάροχος λύσεων λογισμικού Τηλεπικοινωνιών, Ενοποιημένων Επικοινωνιών και Επιχειρήσεων μέσω Pilar.

Abstract

As most organizations now base a large part of their operations on information systems, the need for appropriate security is increasing. Unfortunately, it is difficult to select the security measures needed to achieve satisfactory security. This thesis deals with risk analysis, a process that identifies security problems, classifies them according to their importance and finally proposes solutions to solve them. It presents the different ways of risk analysis, the main methods currently used, the software packages available on the market and finally a practical application of risk analysis in the company Company A.E. a specialized provider of Telecommunications, Unified Communications and Enterprise software solutions through Pilar.

Πίνακας Περιεχομένων

1. Εισαγωγή	8
1.1. Ασφάλεια πληροφοριακών συστημάτων	8
1.2. Απαιτήσεις ασφαλείας πληροφοριακών συστημάτων	10
1.3. Παραβίαση πληροφοριακών συστημάτων	11
1.4. Αντιμετώπιση παραβιάσεων	12
2. Διαχείριση επικινδυνότητας πληροφοριακών συστημάτων	15
2.1. Επικινδυνότητα (Risk management)	15
2.2. Μείωση επικινδυνότητας	16
2.3. Έλεγχος ασφαλείας	19
3. Σχετικά Διεθνή πρότυπα ISO	20
3.1. ISO/IEC 27005: 2022	20
3.2. ISO/IEC 27001:2022	24
3.3. ISO 31000:2018	26
4. Μεθοδολογίες αξιολόγησης και διαχείρισης κινδύνου στα ΠΣ	29
4.1. Μέθοδος EAR / PILAR	29
4.2. Μέθοδος VERINICE	30
4.3. Μέθοδος SBA	31
4.4. Μέθοδος MEHARI	33
4.5. Μέθοδος EBIOS	35
4.6. Μέθοδος OCTAVE-S	37
5. Εμπειρική μελέτη	42
5.1. Το πρόγραμμα που χρησιμοποιήθηκε	43
5.2. Το case study της εργασίας	48
5.3. Το πληροφοριακό σύστημα	50
5.3.1. Υλικά του συστήματος	53
5.3.2. Λειτουργίες του Συστήματος	55
5.3.3. Το Λογισμικό και τα Δεδομένα του Συστήματος	56
5.3.4. Οι διαδικασίες και Πολιτικές του Συστήματος	57
5.3.5. Οι χρήστες του Συστήματος	68

5.4. Εισαγωγή δεδομένων στο Pilar	69
5.5. Συζήτηση αποτελεσμάτων ανάλυσης επικινδυνότητας	80
6. Συμπεράσματα	87
7. Βιβλιογραφικές Αναφορές	89
8. Παράρτημα Εργασίας	97
1. Λειτουργίες βασικού χρήστη	97
2. Λειτουργίες μέσου χρήστη	100

Πίνακας εικόνων

Εικόνα 1 : Υπηρεσίες επιχείρησης
Εικόνα 2 : Εισαγωγή Asset στο Pilar
Εικόνα 3: Valuation of domains
Εικόνα 4: Valuation of domains (2)
Εικόνα 5: Valuation of Assets
Εικόνα 6: Valuation of Assets (2)
Εικόνα 7: Threats – security domains
Εικόνα 8: Threats identification
Εικόνα 9: Threats valuation
Εικόνα 10: Threats valuation of phases
Εικόνα 11: Impact
Εικόνα 12: Risk
Εικόνα 13: Infrastructure risk
Εικόνα 14: Servers' risks
Εικόνα 15: Εφαρμογές γραφείου risk
Εικόνα 16: Technical risk
Εικόνα 17: Platform risk
Εικόνα 18: Risk per dimension

Πίνακας διαγραμμάτων

Διάγραμμα 1 - Πληροφοριακό σύστημα.....	53
---	----

Κατάλογος Πινάκων

Πίνακας 1 - Δικαιώματα χρηστών πληροφοριακού συστήματος	68
---	----

1. Εισαγωγή

Το κεφάλαιο αυτό έχει το χαρακτήρα εισαγωγής στη πτυχιακή εργασία. Στο κεφάλαιο παρατίθενται βασικές έννοιες που θα συναντήσει ο αναγνώστης στην εργασία όπως η ασφάλεια των πληροφοριακών συστημάτων, οι απαιτήσεις των συστημάτων, η προσπάθεια παραβίασης της ασφάλειας και η αντιμετώπιση από τον χρήστη.

Η εργασία πραγματεύεται την αξιολόγηση κινδύνων σε ένα πληροφοριακό σύστημα. Η μελέτη αυτή είναι σημαντική για την ασφάλεια και την προστασία των πληροφοριών μιας επιχείρησης. Για το λόγο αυτό θα γίνει πραγματική μελέτη περίπτωσης σε μια επιχείρηση η οποία χρησιμοποιεί αληθινά δεδομένα. Η επιχείρηση που επιλέχθηκε για τη μελέτη περίπτωσης είναι ένας εξειδικευμένος πάροχος λύσεων λογισμικού Τηλεπικοινωνιών, Ενοποιημένων Επικοινωνιών και Επιχειρήσεων. Η επιχείρηση δεν απευθύνεται σε ιδιώτες αλλά σε επιχειρήσεις ως πελάτες, λειτουργώντας στο business to business τμήμα της αγοράς. Σε αυτή την εργασία, εκτός από το εισαγωγικό κεφάλαιο, θα αναλυθεί η διαχείριση επικινδυνότητας των πληροφοριακών συστημάτων, τα διεθνή πρότυπα ISO, οι μεθοδολογίες αξιολόγησης και διαχείρισης κινδύνων στα πληροφοριακά συστήματα και στη συνέχεια το ερευνητικό μέρος που θα λάβει χώρο η εμπειρική μελέτη. Η διπλωματική θα κλείσει με τα συμπεράσματα.

1.1. Ασφάλεια πληροφοριακών συστημάτων

Ο όρος «Ασφάλεια» μπορεί να ερμηνευτεί με πολλούς τρόπους, κάθε ερμηνεία μπορεί να περιγράψει με ακρίβεια ποικίλες καταστάσεις. Στο λεξικό της Οξφόρδης, η ασφάλεια ορίζεται ως «η ελευθερία από τον κίνδυνο ή το φόβο». Ο όρος «Ασφάλεια» ορίζεται με τους εξής τρόπους:

- Η κατάσταση στην οποία δεν υπάρχουν κίνδυνοι, όπου δεν υπάρχει το αίσθημα της απειλής.
- Η αποτροπή κινδύνου ή απειλής, εξασφαλίζοντας σιγουριά και βεβαιότητα.
- Υπηρεσία της Αστυνομίας.
- Η λεκτική διάταξη που αποτρέπει πιθανά ατυχήματα.
- Μηχανισμός στην πόρτα αυτοκινήτου.
- Συμφωνία μεταξύ ασφαλιστικής εταιρείας και πελάτη.
- Ιατροφαρμακευτική περίθαλψη.

Από μία άποψη, η ασφάλεια ενδέχεται να συνίσταται στην επαρκή προστασία ανθρώπων και αγαθών, λαμβάνοντας ποικίλα μέτρα προστασίας από ενδεχόμενους κινδύνους. Για παράδειγμα, η φυσική ασφάλεια ενός κτιρίου συνίσταται στην αποτροπή εισόδου κακόβουλων ατόμων καθώς και στην αποτροπή ζημιών από φυσικές καταστροφές. Αντιστοίχως, η ασφάλεια των πληροφοριακών συστημάτων υφίσταται στην προστασία των δεδομένων από διαγραφή, αλλοίωση, καταστροφή ή αποκάλυψη σε μη εξουσιοδοτημένους χρήστες (Iphar, Napoli, Ray, Alincourt & Brosset, 2016).

Η επιστήμη της ασφάλειας των πληροφοριακών συστημάτων περιλαμβάνει μία πληθώρα γνωστικών αντικειμένων, θεωριών και τεχνολογιών που στοχεύουν στην πρόληψη, στην ανίχνευση και στην αντιμετώπιση μη εξουσιοδοτημένων πράξεων, οι οποίες αφορούν τη χρήση υπολογιστικών συστημάτων.

Ο ηλεκτρονικός υπολογιστής κατά την εκτέλεση των μη εξουσιοδοτημένων πράξεων συνήθως έχει δυο ιδιότητες:

- Είναι βασικό εργαλείο για την εκτέλεσή τους
- Ο ίδιος ο ηλεκτρονικός υπολογιστής, και κυρίως τα δεδομένα ή και οι πληροφορίες που περιέχονται ή δημιουργούνται σε αυτόν, αποτελεί στόχο των πράξεων αυτών.

Οι μη εξουσιοδοτημένες πράξεις, αναλόγως με τις συνέπειές τους ενδέχεται να θεωρούνται ή όχι ηλεκτρονικό έγκλημα (e-crime, computer crime). Το ηλεκτρονικό έγκλημα ορίστηκε από τους Forester και Morrison το 1994 ως : *«Μία εγκληματική πράξη κατά την εκτέλεση της οποίας ο ηλεκτρονικός υπολογιστής αποτελεί το βασικό εργαλείο»* (Abbass, Baina & Bellafkih, 2015).

Η ασφάλεια των πληροφοριακών συστημάτων αξιοποιεί τη γνώση που προέρχεται από τη μελέτη αρκετών γνωστικών χώρων, χωρίς απαραίτητως να σχετίζονται μεταξύ τους, όπως Πληροφορική, Κρυπτογραφία και Κοινωνικές Επιστήμες.

1.2. Απαιτήσεις ασφαλείας πληροφοριακών συστημάτων

Μία απαραίτητη συνθήκη ώστε να μπορεί να αποτιμηθεί η ασφάλεια είναι να υπάρχει κάποιο σύνολο απαιτήσεων, τα οποία πρέπει να αντιστοιχούν σε κάποια θεμελιώδη χαρακτηριστικά, με την έννοια ότι κανένα από αυτά δεν πρέπει να απουσιάζει ή να αγνοηθεί. Έτσι ενώ είναι δυνατόν να προσδίδεται μεγαλύτερη ή μικρότερη βαρύτητα σε κάποιο από αυτά, αναλόγως με την περίπτωση, εν τέλει όλα πρέπει να λαμβάνονται υπόψη. Τα κοινώς αποδεκτά χαρακτηριστικά είναι η εμπιστευτικότητα, η ακεραιότητα και η διαθεσιμότητα (Accerboni & Sartor, 2019).

- Εμπιστευτικότητα (confidentiality): αφορά την προστασία από το να έχουν πρόσβαση μη εξουσιοδοτημένα λογικά ή φυσικά αντικείμενα (π.χ. προγράμματα, άνθρωποι)
- Ακεραιότητα (integrity): αποτελεί την ιδιότητα των στοιχείων του συστήματος (κυρίως δεδομένων) να έχουν ακρίβεια και να αντιστοιχούν στην πραγματικότητα. Συνέπεια της ακεραιότητας είναι η κάθε αλλαγή (π.χ. του περιεχομένου των δεδομένων) η οποία είναι αποτέλεσμα εξουσιοδοτημένης ενέργειας, ενώ, ταυτόχρονα, η μη εξουσιοδοτημένη αλλαγή να μην είναι δυνατή.
- Διαθεσιμότητα (availability): είναι η ιδιότητα των πόρων του συστήματος να καθίστανται αμέσως προσπελάσιμοι από κάθε εξουσιοδοτημένο λογικό ή φυσικό αντικείμενο, που έχει την απαίτηση για παρόμοια πρόσβαση.

Δύο ακόμα σημαντικές έννοιες είναι οι εξής :

- Αυθεντικότητα (authenticity): αφορά την αποφυγή ατελειών και ανακριβειών κατά τη διάρκεια των εξουσιοδοτημένων τροποποιήσεων μιας πληροφορίας.
- Εγκυρότητα (validity): αποδίδεται ως η απόλυτη ακρίβεια και πληρότητα μιας πληροφορίας.

Η εμπιστευτικότητα, η ακεραιότητα και η διαθεσιμότητα συνιστούν τους τρεις κύριους επιδιωκόμενους στόχους στην ασφάλεια πληροφοριακών συστημάτων. Μερικές φορές υπάρχει αλληλοεπικάλυψη, ενώ άλλες φορές αποκλείονται με αμοιβαίο τρόπο. Για παράδειγμα, η ισχυρή προστασία της εμπιστευτικότητας ενδέχεται να περιορίσει σε μεγάλο βαθμό τη διαθεσιμότητα, και το αντίστροφο.

1.3. Παραβίαση πληροφοριακών συστημάτων

Οι παραβιάσεις πραγματοποιούνται αν το σύστημα απειλείται από κάτι και ταυτόχρονα παρουσιάζει κάποια αδυναμία. Ένα πληροφοριακό σύστημα μπορεί να παραβιαστεί με τέσσερις τρόπους. Οι παράμετροι τις οποίες καταργεί ο καθένας από αυτούς καθορίζουν εάν ένα σύστημα είναι ασφαλές (Τσούμα, 2007).

- Υποκλοπή (interception): μία μη εξουσιοδοτημένη οντότητα έχει αποκτήσει πρόσβαση σε κάποια πληροφορία. Η οντότητα αυτή ενδέχεται να είναι ένα άτομο, ένα πρόγραμμα ή ακόμα και ένα υπολογιστικό σύστημα. Παράδειγμα τέτοιας παραβίασης αποτελούν η παράνομη αντιγραφή προγραμμάτων ή αρχείων καθώς και η υποκλοπή δεδομένων σε δίκτυο. Είναι επομένως φανερό ότι με την παραβίαση αυτή γίνεται άμεσα κατάργηση της εμπιστευτικότητας των δεδομένων.
- Παρεμβολή (interruption): ένα στοιχείο του συστήματος χάνεται ή αχρηστεύεται. Παράδειγμα συνιστά η σκόπιμη καταστροφή μιας συσκευής hardware ή το σβήσιμο ενός προγράμματος ή αρχείου. Στην περίπτωση αυτή δεν είναι διαθέσιμες πλέον οι πληροφορίες.

- Τροποποίηση (modification): μία μη εξουσιοδοτημένη οντότητα έχει αποκτήσει πρόσβαση σε κάποια πληροφορία και την έχει αλλοιώσει. Για παράδειγμα, κάποιος μπορεί να αλλοιώσει στοιχεία μιας βάσης δεδομένων, να πραγματοποιήσει τροποποίηση ενός προγράμματος, ώστε αυτό να εκτελεί έναν επιπλέον υπολογισμό ή ακόμα και να μετατρέπει το υλικό (hardware). Κάποιες από τις παραπάνω ενέργειες είναι εμφανείς, όμως για άλλες πιο περίπλοκες δεν υπάρχει η δυνατότητα ανίχνευσης.
- Πλαστογράφιση (fabrication): είναι δυνατή η πλαστογράφιση αντικειμένων με τη βοήθεια ενός πληροφοριακού συστήματος. Αυτό μπορεί να πραγματοποιηθεί προσθέτοντας αρχεία σε μία βάση δεδομένων. Σε πολλές περιπτώσεις δεν υπάρχει η δυνατότητα να ξεχωρίσει κανείς αν το αντικείμενο είναι γνήσιο ή όχι. Με τον τρόπο αυτό παύει να υφίσταται η εμπιστευτικότητα καθώς και η εγκυρότητα των δεδομένων.

1.4. Αντιμετώπιση παραβιάσεων

Είναι γεγονός ότι η πραγματοποίηση μιας παραβίασης σε ένα πληροφοριακό σύστημα έχει εξαιρετικά βλαβερές συνέπειες. Για την αποφυγή λοιπόν των ιδιαίτερα δυσμενών επιπτώσεων που ενδέχεται να υπάρξουν, κρίνεται αναγκαίο να εφαρμοστούν μέτρα προστασίας των πληροφοριακών συστημάτων. Τα μέτρα αυτά έχουν σκοπό να προφυλάξουν τα πληροφοριακά συστήματα από τις εξωτερικές απειλές και τις απειλές που δημιουργούνται από εσωτερικούς παραγοντες αδυναμίες τους, καθώς και από κακόβουλες ενέργειες που ενδεχομένως να προκαλέσουν την παραβίαση των πληροφοριακών συστημάτων. Τα κυριότερα μέτρα προστασίας είναι τα εξής (Agrawal, 2016):

- Κρυπτογράφηση: αποτελεί το ισχυρότερο εργαλείο στην ασφάλεια των πληροφοριακών συστημάτων. Με τη μετατροπή των δεδομένων σε μη αναγνώσιμη μορφή ο κίνδυνος υποκλοπής ή αλλοίωσής τους σχεδόν εκμηδενίζεται. Ακόμη, σε μερικά πρωτόκολλα η χρήση της κρυπτογράφησης αποσκοπεί στη διάθεση πληροφοριών σε εξουσιοδοτημένους χρήστες. Δηλαδή με την κρυπτογράφηση

υπάρχει η εξασφάλιση σε μεγάλο βαθμό των τριών βασικών στόχων της ασφάλειας. Δεν πρέπει όμως να γίνεται υπερεκτίμηση της αξίας της. Πρέπει να γίνει σαφές ότι η κωδικοποίηση, εφόσον δεν εφαρμόζεται κατάλληλα, δεν ενισχύει την επίδοση του συστήματος στο θέμα της ασφάλειας. Αντιθέτως, ενδέχεται να έχει το αντίθετο αποτέλεσμα διότι δίνει μία ψευδή αίσθηση ασφάλειας χωρίς όμως να έχει τη δυνατότητα στην πράξη να εγγυηθεί κάτι τέτοιο.

- Έλεγχοι λογισμικού: οι έλεγχοι αποτελούνται από τρεις κατηγορίες. Πρώτον, ο εσωτερικός έλεγχος όπου τα τμήματα του προγράμματος βελτιώνουν την ασφάλεια του συστήματος. Τέτοιο παράδειγμα αποτελεί ο έλεγχος πρόσβασης σε ένα πρόγραμμα διαχείρισης βάσεων δεδομένων. Δεύτερον, ο έλεγχος του λειτουργικού συστήματος. Το λειτουργικό σύστημα απαιτεί ορισμένους περιορισμούς με σκοπό ο κάθε χρήστης να προστατεύεται από τους υπόλοιπους. Τέλος, οι έλεγχοι ανάπτυξης. Αυτοί ενέχουν κριτήρια ποιότητας βάση των οποίων γίνεται ο σχεδιασμός, η κωδικοποίηση, ο έλεγχος και η συντήρηση ενός προγράμματος.
- Έλεγχοι υλικού: οι έλεγχοι αυτοί είναι πολυπληθείς και ενδέχεται να περιλαμβάνουν κλειδαριές, αντικλεπτικά συστήματα, συσκευές αναγνώρισης στοιχείων χρήστη κλπ.
- Πολιτικές: η συχνή αλλαγή κωδικών πρόσβασης (passwords), η θέσπιση ηθικού κώδικα για τους επαγγελματίες των πληροφοριακών συστημάτων, η εκπαίδευση του προσωπικού αποτελούν τις συνηθέστερες πολιτικές που εφαρμόζονται για την προστασία των πληροφοριών.
- Φυσικοί έλεγχοι: αποτελούν τους πιο εύκολους, οικονομικούς αλλά και συχνά τους πιο αποτελεσματικούς ελέγχους. Περιέχουν κλειδαριές, εφεδρικά αντίγραφα ασφαλείας των σημαντικών εγγράφων και δεδομένων, φρουρούς, αλλά και σχεδιασμό αντιμετώπισης εκτάκτων περιστατικών που να προσφέρει κάλυψη στις φυσικές καταστροφές.

Η αποτελεσματικότητα των παραπάνω ελέγχων εξαρτάται από αρκετές παραμέτρους, κυριότερη των οποίων είναι η συνειδητοποίηση του προβλήματος (Alberts, Dorofee, Stevens & Woody, 2003). Πολλοί χρήστες δεν ακολουθούν τους κανόνες ασφάλειας, αφού δεν θεωρούν αναγκαία την ύπαρξη των μέτρων αυτών. Επίσης, είναι κρίσιμο οι

έλεγχοι να είναι σαφείς, προσαρμοσμένοι στο εκάστοτε σύστημα και να μην έχουν ανάγκη από πολύ χρόνο και πόρους για την εφαρμογή τους. Επιπλέον, η ταυτόχρονη διεξαγωγή διαφορετικών ελέγχων στο ίδιο σύστημα ενισχύει σε μεγάλο βαθμό την αποδοτικότητά τους συγκριτικά με τη διεξαγωγή καθενός μεμονωμένα. Αναγκαία είναι και η περιοδική αναθεώρηση των ελέγχων. Ο κύκλος ζωής τους είναι περιορισμένος, αφενός διότι το ίδιο γίνεται και στο υπό προστασία σύστημα (π.χ. γίνεται συνεχώς αναβάθμιση του λογισμικού), αφετέρου διότι οι απειλές γίνονται ολοένα και πιο έντονες (π.χ. ο ανταγωνισμός βοηθά την προσπάθεια του να παραβιάσει το σύστημα) (Alberts, Dorofee, Stevens & Woody, 2005). Τέλος, θα πρέπει τα συστήματα να σχεδιαστούν με τέτοιο τρόπο ώστε να έχουν ανεκτικότητα σε σφάλματα, δηλαδή να συντηρείται η ασφάλεια των πληροφοριακών συστημάτων παρά τις δυσλειτουργίες ορισμένων συνθετικών τους. Αυτή η ιδιότητα έχει μεγάλη συνεισφορά στην άμυνα των πληροφοριακών συστημάτων έναντι των εσωτερικών τεχνικών αδυναμιών (Al-Dhahri, Al-Sarti & Abdul, 2017).

Με την εφαρμογή των παραπάνω μέτρων προστασίας, οι εμπλεκόμενοι φορείς έχουν την υποχρέωση να διατηρήσουν την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα των πληροφοριακών συστημάτων.

2. Διαχείριση επικινδυνότητας πληροφοριακών συστημάτων

2.1. Επικινδυνότητα (Risk management)

Η ανάλυση επικινδυνότητας είναι μία «οργανοτεχνική μελέτη η οποία μελετά τις απειλές, τις ευπάθειες και τα αγαθά ενός οργανισμού και προτείνει τα μέτρα ασφάλειας που πρέπει να ληφθούν για την αντιμετώπιση των προσδιορισμένων απειλών» (Μουλίνος, 2003). Στην πράξη, ο κίνδυνος αποτελεί ένα μέτρο της πιθανότητας πραγματοποίησης ενός συγκεκριμένου ανεπιθύμητου γεγονότος και συνδέεται άμεσα με ένα ή περισσότερα στοιχεία του συστήματος. Αυτό το ενδεχόμενο εξαρτάται τόσο από την πιθανότητα πραγματοποίησης της επίθεσης όσο και από την πιθανότητα της επιτυχίας της, η οποία ακολούθως είναι εξαρτημένη από την επιτυχή εκμετάλλευση των αδυναμιών του συστήματος (Μουλίνος, 2003).

Η διαδικασία αποτίμησης του κινδύνου υπολογίζει τόσο το ενδεχόμενο πραγματοποίησης της απειλής, όσο και την επίπτωση που θα έχει στο πληροφοριακό σύστημα έτσι ώστε να γίνει εκτίμηση του βαθμού εκείνου στον οποίο ο κίνδυνος είναι αναγκαίο να μειωθεί με κατάλληλα μέτρα. Η αξία αποτίμησης βάσει του κινδύνου (risk-based reasoning) βρίσκεται στο γεγονός στο ότι προσφέρει κριτήρια αποφάσεων για τις απαιτήσεις ασφάλειας (security requirements) εν μέσω του επιχειρησιακού και κοινωνικού περιβάλλοντος (Μάγκος, 2007). Η αποτίμηση κινδύνων θεωρείται γενικά ως η μόνη βιώσιμη μέθοδος για να τεκμηριωθούν τα μέτρα ασφάλειας σε όρους κόστους – ωφέλειας, ή για να επιλεγθούν τα αποδοτικότερα αντίμετρα. Ως συνέπεια, η διαχείριση κινδύνων αποτελεί τη βάση των περισσότερων εθνικών προτύπων για διαχείριση ασφάλειας πληροφοριών π.χ. BSI-EN 2002 και βέλτιστες πρακτικές π.χ. BSI-EN 2001. Παρά την ύπαρξη ποικίλων βαθμών ελευθερίας στην εκλογή των μεθοδολογιών για την εκπόνηση μιας μελέτης ανάλυσης επικινδυνότητας, τα πρότυπα εκτελούν τα ίδια βασικά βήματα για τη διαχείριση των κινδύνων (Λέρα, 2012):

1. Ορίζεται το περιβάλλον και τα όρια του πληροφοριακού συστήματος

2. Εντοπίζονται τα αγαθά του πληροφοριακού συστήματος και οι ανεπιθύμητες καταστάσεις που πιθανώς να προκύψουν σε αυτά τα αγαθά
3. Αποτιμώνται οι κίνδυνοι κάθε απειλής για κάθε αγαθό, υπολογίζοντας τις πιθανές επιθέσεις και αδυναμίες
4. Εκλέγονται τα κατάλληλα αντίμετρα
5. Υλοποιείται, εφαρμόζεται και περιοδικά επανα-αποτιμάται το επίπεδο κινδύνου.

Οι διαφορές μεταξύ των προσεγγίσεων διαχείρισης κινδύνων περιέχουν τον τρόπο ποσοτικοποίησης των κινδύνων, το επίπεδο γνώσεων και εξειδίκευσης που απαιτείται από τον ειδικό ασφάλειας για την εφαρμογή των αντιμέτρων και τον προσανατολισμό της προσέγγισης σε αποτίμηση βασισμένη σε αγαθά (asset-based approaches) ή σε διεργασίες πληροφορικής (process-based approaches).

2.2. Μείωση επικινδυνότητας

Η μείωση των κινδύνων αποτελεί μία συστηματική μεθοδολογία που αξιοποιείται από τη διοίκηση με σκοπό να μειωθεί το επίπεδο του κινδύνου για τον οργανισμό σε αποδεκτά επίπεδα. Αποτελείται από μία σειρά ενεργειών που περιλαμβάνουν τη θέσπιση προτεραιοτήτων, την αξιολόγηση και την υλοποίηση των κατάλληλων αντιμέτρων που απορρέουν από την ανάλυση επικινδυνότητας (Μουλίνος, 2003). Με δεδομένο ότι συνήθως δεν υπάρχει η δυνατότητα να εφαρμοστεί η εξάλειψη όλων των κινδύνων, η διοίκηση και οι επικεφαλής των επιχειρησιακών μονάδων ενός οργανισμού είναι υπεύθυνοι για την υλοποίηση των καταλληλότερων αντιμέτρων και την υιοθέτηση της πιο οικονομικής λύσης με σκοπό τη μείωση του κινδύνου σε ένα αποδεκτό επίπεδο, επιδρώντας όσο το δυνατόν λιγότερο στους πόρους καθώς και με τη στρατηγική επιστολή του οργανισμού. Τα κύρια θέματα της μείωσης των κινδύνων αποτελούν :

1. οι διαθέσιμες επιλογές για να μειωθούν οι κίνδυνοι (risk mitigation options)
2. η στρατηγική που θα υιοθετήσει (risk mitigation strategy)

3. η υλοποίηση των αντιμέτρων (control implementation)
4. οι διάφορες κατηγορίες των αντιμέτρων (control categories)
5. η ανάλυση κόστους – ωφέλειας για να αιτιολογηθούν τα επιλεγμένα αντίμετρα (cost – benefit analysis)
6. ο εναπομένον κίνδυνος (residual risk).

Αυτό μπορεί να επιτευχθεί με :

- αποδοχή του κινδύνου
- αποφυγή του κινδύνου
- μείωση του κινδύνου
- κατάρτιση σχεδίου μείωσης κινδύνου
- έρευνα για τρόπους διόρθωσης της αδυναμίας που προκαλεί κίνδυνο
- μεταφορά του κινδύνου σε τρίτα μέρη.

Δεδομένου ότι οι στόχοι ενός οργανισμού ορίζουν και τη λειτουργία του, δεν είναι διαθέσιμος ένας μόνο τρόπος για να μειωθεί ο κίνδυνος. Οι βασικότερες κατηγορίες των μέτρων είναι (Azuwa, Ahmad, Sahib & Shamsuddin, 2012):

1. τεχνικά μέτρα ασφάλειας που έχουν στόχο τα τεχνικά χαρακτηριστικά των πόρων και διαχωρίζονται σε
 - υποστηρικτικά (όπως είναι η διαχείριση ασφάλειας, η ταυτοποίηση, οι βέλτιστες λειτουργικές πρακτικές, η διαχείριση κρυπτογραφικών κλειδιών),
 - προληπτικά (όπως είναι η ταυτοποίηση, η μη – αποποίηση ευθύνης, η αυθεντικοποίηση, η επιβολή ελέγχου πρόσβασης, η μυστικότητα συναλλαγής, οι προστατευμένες επικοινωνίες) και

- διαγνωστικά (όπως είναι ο έλεγχος, η ανίχνευση και η εξάλειψη ιομορφικού λογισμικού, η ακεραιότητα, η ανίχνευση και ο περιορισμός των εισβολών, τα σημεία επαναφοράς σε συστημική κατάσταση).
2. διαδικαστικά μέτρα ασφάλειας που τονίζουν την τήρηση των πολιτικών, προτύπων και διαδικασιών και διαχωρίζονται σε
- Προληπτικά (όπως είναι η ανάπτυξη σχεδίων ασφάλειας, ο καθορισμός ρόλων και υπευθυνοτήτων, η επιμόρφωση και εκπαίδευση σε θέματα ασφάλειας, οι διαδικασίες πρόσβασης και διαχείρισης αλλαγών)
 - Διαγνωστικά (όπως είναι οι περιοδικοί έλεγχοι ασφάλειας, η υλοποίηση μέτρων ασφάλειας για τους χρήστες, οι διαδικασίες διαχείρισης κινδύνων)
 - Ανάκτησης λειτουργιών (όπως η μονάδα διαχείρισης περιστατικών ασφάλειας)
3. λειτουργικά μέτρα ασφάλειας που τονίζουν την τήρηση των ελάχιστων αποδεκτών τεχνοδιαμορφώσεων μέσω της κατάρτισης αναλυτικών οδηγιών και διαδικασιών και διαχωρίζονται σε
- Προληπτικά (όπως είναι οι διαδικασίες πρόσβασης, το ιομορφικό λογισμικό)
 - Διαγνωστικά (όπως είναι η φυσική ασφάλεια).

2.3. Έλεγχος ασφαλείας

Η ανάλυση επικινδυνότητας συνιστά τον πιο σημαντικό παράγοντα στο σχεδιασμό του ελέγχου, διαμέσου του εντοπισμού κινδύνων και ευπαθειών, ο ελεγκτής έχει τη δυνατότητα να οριοθετεί τους αναγκαίους μηχανισμούς ελέγχου με σκοπό να συμβάλλει στον περιορισμό αυτών των κινδύνων σε ικανοποιητικό επίπεδο. Επίσης, ο ελεγκτής πρέπει να έχει την ικανότητα να προσδιορίζει και να διακρίνει σε επαρκή βαθμό τους διάφορους τύπους κινδύνων, καθώς και την σπουδαιότητα και την επάρκεια των αντίστοιχων μέτρων ασφαλείας (Μάγκος, 2007). Η εκτίμηση αυτή δεν πρέπει να εφαρμόζεται μόνο σε τεχνικό επίπεδο αντιμετρών αλλά και σε επίπεδο επιχειρησιακών λειτουργιών. Ο ελεγκτής μέσω της ανάλυσης επικινδυνότητας είναι σε θέση να χωρίσει σε κατηγορίες και να εντοπίσει τους πιο σημαντικούς κινδύνους για το πληροφοριακό σύστημα. Λόγω των περιορισμένων τεχνολογικών και ανθρώπινων πόρων, συχνά δεν είναι εφικτή η πραγματοποίηση ενδεδειγμένων ελέγχων για την αντιμετώπιση όλων των πιθανών κινδύνων, έτσι ο ελεγκτής καταλήγει σε μία επιλογή ελεγκτικών στόχων, τόσο ποσοτική όσο και ποιοτική. Σε αυτήν τη δύσκολη διαδικασία, η ανάλυση επικινδυνότητας προσφέρει βοήθεια στον ελεγκτή (Belsis, Kokolakis & Kiountouzis, 2005).

Από την άλλη πλευρά του ελέγχου του πληροφοριακού συστήματος, τα πλεονεκτήματα της ανάλυσης επικινδυνότητας για τον σχεδιασμό του είναι τα εξής:

1. Οι ελεγκτικοί πόροι κατανέμονται με αποτελεσματικό τρόπο.
2. Υπάρχει η διαβεβαίωση ότι μία αντιπροσωπευτική εικόνα του οργανισμού και του πληροφοριακού συστήματος είναι διαθέσιμη λαμβάνοντας πληροφορίες από όλα τα επίπεδα του οργανισμού.
3. Παρέχεται μια αφετηρία για αποτελεσματική διαχείριση του τμήματος εσωτερικού ελέγχου.
4. Συνδέεται το συγκεκριμένο αντικείμενο ελέγχου με τον οργανισμό.

3. Σχετικά Διεθνή πρότυπα ISO

3.1. ISO/IEC 27005: 2022

Σκοπός του ISO 27005 είναι να δίνει κατευθύνσεις για την Διαχείριση Κινδύνων Ασφάλειας Πληροφοριών. Το ISO 27005 παρέχει υποστήριξη για τις γενικές έννοιες που ορίζονται στο πρότυπο ISO 27001 και ο σκοπός του σχεδιασμού του είναι να προσφέρει βοήθεια για την ικανοποιητική εφαρμογή της Ασφάλειας Πληροφοριών η οποία έχει ως βάση μια προσέγγιση διαχείρισης κινδύνου (Dey, 2007). Το ISO 27005 δεν κάνει διευκρινήσεις ούτε αποτελεί οποιαδήποτε εξειδικευμένη μέθοδος ανάλυσης κινδύνου, αν και δεν κάνει προσδιορισμό μιας δομημένης, συστηματικής και αυστηρής διαδικασίας από την ανάλυση των κινδύνων με σκοπό να δημιουργήσει το σχέδιο για την αντιμετώπιση του κινδύνου.

Το ISO/IEC 27005:2022 αποτελείται από τα εξής βήματα:

1. Εγκατάσταση πλαισίου (context establishment)
2. Αξιολόγηση κινδύνου (risk assessment)
3. Αντιμετώπιση κινδύνου (risk treatment)
4. Αποδοχή κινδύνου (risk acceptance)
5. Κοινοποίηση κινδύνου (risk communication)
6. Παρακολούθηση και επανεξέταση κινδύνου (risk monitoring and review).

Η εγκατάσταση πλαισίου αποτελεί το 1ο βήμα του πλαισίου ISO/IEC 27005. Σε αυτό συμπεριλαμβάνεται η απόκτηση όλων των σχετικών πληροφοριών που αφορούν την οργάνωση και τον καθορισμό των βασικών κριτηρίων, το πεδίο εφαρμογής, τον σκοπό, τα όρια και την οργάνωση των δραστηριοτήτων για τη διαχείριση κινδύνου (Diamantopoulou, Tsohou & Karyda, 2019).

Σκοπός, συνήθως, αποτελεί η συμμόρφωση με τις νομικές απαιτήσεις καθώς και η παροχή αποδείξεων επιμέλειας που στηρίζει το ISMS που έχει τη δυνατότητα να πιστοποιηθεί.

Το πεδίο εφαρμογής ενδέχεται να είναι ένα σχέδιο αναφοράς, ένα σχέδιο επιχειρησιακής συνέχειας ή η πιστοποίηση ενός προϊόντος. Τα κριτήρια αποτελούνται από την εκτίμηση και αποδοχή του κινδύνου και τα κριτήρια αξιολόγησης των επιπτώσεων. Επίσης, κάνουν προσδιορισμό του πεδίου εφαρμογής και των ορίων του πλαισίου στον οργανισμό.

Η αξιολόγηση κινδύνου έχει ως είσοδο, την έξοδο του προηγούμενου βήματος, δηλαδή την εγκατάσταση του πλαισίου. Η έξοδος αποτελεί τη λίστα των εκτιμώμενων κινδύνων κατά προτεραιότητα, σύμφωνα με τα κριτήρια αξιολόγησης των κινδύνων. Υπάρχει η δυνατότητα αυτή η διαδικασία να χωριστεί σε:

1. Ανάλυση κινδύνου (risk analysis)
 - a. Αναγνώριση κινδύνου (risk identification)
 - b. Εκτίμηση κινδύνου (risk estimation)
2. Εκτίμηση κινδύνου (risk evaluation).

Ο κώδικας εφαρμογής του ISO/IEC 27002:2005 για τη διαχείριση ασφάλειας πληροφοριών συνιστά την εξέταση κατά τη διάρκεια της εκτίμησης του κινδύνου των εξής:

1. Την πολιτική ασφαλείας (διοικητική καθοδήγηση)
2. Την οργάνωση της ασφάλειας των πληροφοριών
3. Τη διαχείριση περιουσιακών στοιχείων (ταξινόμηση των πληροφοριακών αγαθών)
4. Τη φυσική και περιβαλλοντική ασφάλεια
5. Τη διαχείριση επικοινωνιών και λειτουργιών
6. Τον έλεγχο πρόσβασης (περιορισμός των δικαιωμάτων πρόσβασης σε δίκτυα, συστήματα, εφαρμογές και δεδομένα)
7. Την απόκτηση, την ανάπτυξη και τη συντήρηση πληροφοριακού συστήματος
8. Τη διαχείριση περιστατικών της ασφάλειας πληροφοριών
9. Τη διαχείριση επιχειρησιακής συνέχειας (προστασία, συντήρηση και ανάρρωση των ευαίσθητων επιχειρηματικών διαδικασιών και συστημάτων)

10. Τη συμμόρφωση (διασφάλιση της συμμόρφωσης με τις πολιτικές ασφαλείας, τα πρότυπα, το νόμο και τους κανονισμούς).

Με την αναγνώριση των κινδύνων είναι εφικτό να διαπιστωθεί τι ενδέχεται να προκαλέσει μία πιθανή απώλεια.

Έτσι, είναι αναγκαίο να προσδιορίζονται :

1. Τα περιουσιακά στοιχεία
 - i. Πρωτογενή (δηλαδή επιχειρηματικές διεργασίες και σχετικές πληροφορίες)
 - ii. Υποστήριξη (hardware, software, προσωπικό, τοποθεσία, οργανωτική δομή)
2. Οι απειλές
3. Τα μέτρα ασφαλείας
4. Οι ευπάθειες
5. Οι συνέπειες
6. Οι σχετιζόμενες επιχειρηματικές διαδικασίες

Η έξοδος των επιμέρους διεργασιών συνίσταται από έναν κατάλογο με τα περιουσιακά στοιχεία και τις σχετιζόμενες επιχειρηματικές διαδικασίες, που είναι υπεύθυνος για τη διαχείριση του κινδύνου, με τον ανάλογο κατάλογο απειλών και μέτρων ασφαλείας. Επιπλέον, περιέχει έναν κατάλογο με τις ευπάθειες, που δεν έχουν σχέση με τις προσδιορισμένες απειλές, καθώς και έναν κατάλογο με περιστατικά σεναρίων και τις συνέπειές τους (Diamantopoulou, Tsohou & Karyda, 2019).

Η εκτίμηση κινδύνου έχει ως είσοδο, την έξοδο της ανάλυσης του κινδύνου και αποτελείται από τα εξής βήματα :

1. Εκτίμηση των συνεπειών μέσω της αποτίμησης των περιουσιακών στοιχείων
2. Εκτίμηση της πιθανότητας του περιστατικού μέσω των απειλών και την αποτίμηση της ευπάθειας
3. Εκχώρηση τιμών στην πιθανότητα και την συνέπεια των κινδύνων.

Η έξοδος συνιστά τη λίστα των κινδύνων με τα επίπεδα αξίας που είναι ανατεθειμένα και η τεκμηρίωσή της γίνεται σε ένα μητρώο κινδύνου.

Η διαδικασία αξιολόγησης του κινδύνου έχει ως είσοδο, την έξοδο της διαδικασίας ανάλυσης κινδύνου. Γίνεται σύγκριση κάθε επιπέδου σύμφωνα με τα κριτήρια αποδοχής καθώς και με την προτεραιότητα στη λίστα αντιμετώπισης του κινδύνου.

Η τρίτη διαδικασία σύμφωνα με το πρότυπο ISO 27005 είναι η μείωση κινδύνου. Συμπεριλαμβάνει την ιεράρχηση, την αξιολόγηση και την εφαρμογή των κατάλληλων ελέγχων με σκοπό να μειωθεί ο κίνδυνος, που προτείνεται από την διαδικασία εκτίμησης κινδύνου.

Η διαδικασία αντιμετώπισης του κινδύνου στοχεύει στην επιλογή των μέτρων ασφαλείας για την μείωση, τη διατήρηση, την αποφυγή και τη μεταφορά του κινδύνου καθώς και στην παραγωγή ενός σχεδίου αντιμετώπισής του.

Η έξοδος της διαδικασίας αποτελεί το σχέδιο αντιμετώπισης με τους εναπομένοντες κινδύνους που σχετίζεται με την αποδοχή της διαχείρισης.

Η κοινοποίηση των κινδύνων συνιστά μία διαδικασία που έχει αμφίδρομη αλληλεπίδραση με όλες τις διαδικασίες της διαχείρισης των κινδύνων. Στοχεύει στην ύπαρξη μιας κοινής αντίληψης για όλες τις πτυχές του κινδύνου μεταξύ των ενδιαφερόμενων μερών του οργανισμού (Whitman, Townsend & Aalberts, 2001).

Η διαχείριση των κινδύνων αποτελεί μία συνεχή και ατέρμονη διαδικασία. Στο πλαίσιο αυτής της διαδικασίας γίνεται εφαρμογή μέτρων ασφάλειας, για τα οποία υπάρχει συχνή παρακολούθηση και γίνεται αξιολόγησή τους έτσι ώστε να διασφαλιστεί ότι η λειτουργία τους γίνεται σύμφωνα με το πρόγραμμα. Όμως, οι απαιτήσεις, οι ευπάθειες και οι απειλές ενδέχεται να προκαλέσουν αλλαγές με την πάροδο του χρόνου. Γι' αυτό είναι αναγκαίο να γίνονται τακτικά προγραμματισμένοι έλεγχοι και να η διεξαγωγή τους να γίνεται από κάποιο ανεξάρτητο άτομο, δηλαδή από κάποιον που δεν έχει ευθύνη για τις εφαρμογές ή την καθημερινή διαχείριση ISMS.

3.2. ISO/IEC 27001:2022

Το ISO/IEC 27001 ανήκει σε μία αναπτυσσόμενη οικογένεια των ISO/IEC standards ('ISO/IEC 27000 series'), συνιστά ένα πρότυπο σύστημα διαχείρισης ασφάλειας πληροφοριών (ISMS) η έκδοση του οποίου έγινε τον Οκτώβρη του 2005 από τον διεθνή οργανισμό πιστοποίησης (ISO) και την International Electrotechnical Commission (IEC). Το πλήρες του όνομα είναι ISO/IEC 27001 :2022 – Information technology – Security techniques – Information security management systems – requirements αλλά για λόγους συντομίας αναφερόμαστε σε αυτό με το “ISO 27001” (Diamantopoulou, Tsohou & Karyda, 2019).

Η χρήση του πρόκειται να γίνει συνδυαστικά με το ISO/IEC 27002, the Code of Practice for Information Security Management, το οποίο εντάσσεται εντός των σκοπών ελέγχου ασφαλείας και συγκροτεί ένα εύρος συγκεκριμένων ελέγχων ασφαλείας. Οι οργανισμοί οι οποίοι θα θέσουν σε εφαρμογή ένα ISMS σύμφωνα με την καλύτερη πρακτική συμβουλή στο ISO/IEC 27002 παρέχουν ενδεχομένως παράλληλα κάλυψη για τις απαιτήσεις του ISO/IEC 27001, αλλά η επικύρωση με το δίπλωμα είναι καθαρά προαιρετική.

Το ISO/IEC 27001:2022 εγκρίνει και εφαρμόζει το πρότυπο της διαδικασίας “Plan – Do – Check – Act” (PDCA), το οποίο χρησιμοποιείται στη δομή όλων των διαδικασιών ενός ISMS.

- Plan (καθορισμός του ISMS)

Στο στάδιο αυτό καθιερώνεται η πολιτική, οι στόχοι του ISMS, οι διεργασίες και διαδικασίες που συνδέονται με τη διαχείριση των κινδύνων, καθώς και βελτιώνεται η ασφάλεια των πληροφοριών με σκοπό την παροχή αποτελεσμάτων σε συμφωνία με τις παγκόσμιες πολιτικές και τους στόχους της οργάνωσης.

- Do (εφαρμογή και λειτουργία του ISMS)

Εδώ, τίθεται σε εφαρμογή και γίνεται χρήση της πολιτικής ISMS, των ελέγχων και των διαδικασιών.

- Check (παρακολούθηση και επανεξέταση του ISMS)

Σε αυτό το στάδιο αξιολογούνται και υπολογίζονται οι επιδόσεις των διαδικασιών ενάντια στην πολιτική, στους στόχους, στην πρακτική εμπειρία και εκτίθενται τα αποτελέσματα της διαχείρισης για επανεξέταση.

- Act (αναβάθμιση και βελτίωση του ISMS)

Σύμφωνα με τα αποτελέσματα του εσωτερικού ελέγχου του ISMS και της επανεξέτασης της διαχείρισης ή άλλων σχετικών πληροφοριών γίνονται διορθωτικές και προληπτικές ενέργειες με σκοπό την επίτευξη της συνεχούς βελτίωσης του συστήματος.

Το ISO/IEC 27001:2022 απαρτίζεται από τους εξής τομείς:

- Διαχείριση περιουσιακών στοιχείων (asset management)
- Εγγραφή περιουσιακών στοιχείων (asset register)
- Ταξινόμηση περιουσιακών στοιχείων (asset classification)
- Σήμανση περιουσιακών στοιχείων (asset labeling)
- Έλεγχος πρόσβασης (access control)
- Εγγραφή χρήστη (user registration)
- Διαχείριση κωδικών πρόσβασης (password management)
- Καθαρισμός εργασιακού περιβάλλοντος (clear work environment)
- Λειτουργικό σύστημα και έλεγχος εφαρμογής (operating system and application control)
- Ασφάλεια δικτύου (network security).

Συνήθως, η πιστοποίηση με το πρότυπο ISO/IEC 27001 ενέχει μία διαδικασία με τρία βήματα (Dubois, Heymans, Mayer & Matulevičius, 2010):

- Στο πρώτο βήμα πραγματοποιείται μία ανασκόπηση της ύπαρξης και της πληρότητας σημαντικών εγγράφων όπως, για παράδειγμα, η πολιτική ασφαλείας

του οργανισμού, Statement of Applicability (SoA) and Risk Treatment Plan (RTP).

- Στο δεύτερο βήμα υλοποιείται ένας λεπτομερής σε βάθος έλεγχος για την ύπαρξη και την αποτελεσματικότητα των ελέγχων ασφάλειας που δηλώνονται στο SoA και στο RTP καθώς επίσης και τα υποστηρικτικά τους έγγραφα.
- Στο τρίτο βήμα πραγματοποιείται μία επανεκτίμηση για να διαπιστωθεί ότι ο οργανισμός ο οποίος είναι ήδη πιστοποιημένος, παραμένει συμμορφωμένος με το πρότυπο. Η συντήρηση της πιστοποίησης περιλαμβάνει περιοδικές ανασκοπήσεις και επανεκτιμήσεις για να επιβεβαιωθεί ότι το ISMS συνεχίζει να λειτουργεί όπως έχει καθοριστεί.

3.3. ISO 31000:2018

Το ISO 31000 είναι ένα σύστημα διαχείρισης κινδύνων, το οποίο μαζί με άλλα πρότυπα που θα παρουσιαστούν στη συνέχεια, έχει σκοπό να παρέχει στις επιχειρήσεις μια βοήθεια στη στρατηγική διαχείρισης κινδύνων για τον αποτελεσματικό εντοπισμό των κινδύνων του επιχειρηματικού περιβάλλοντος. Αναπτύσσει μια κουλτούρα διαχείρισης κινδύνων στην οποία οι εργαζόμενοι και οι ενδιαφερόμενοι φορείς γνωρίζουν τη σημασία της παρακολούθησης και της διαχείρισης των κινδύνων. Το ISO 31000 παρέχει οδηγίες για τη διαχείριση του κινδύνου που αντιμετωπίζουν οι επιχειρήσεις. Η εφαρμογή αυτών των οδηγιών μπορεί να προσαρμοστεί σε οποιονδήποτε επιχειρήση και στο πλαίσιο της λειτουργίας της. Παρέχει μια κοινή προσέγγιση για τη διαχείριση οποιουδήποτε τύπου κινδύνου και δεν αφορά συγκεκριμένο κλάδο ή τομέα και μπορεί να χρησιμοποιηθεί σε όλη τη διάρκεια ζωής της επιχείρησης, με εφαρμογή σε οποιαδήποτε δραστηριότητα, συμπεριλαμβανομένης της λήψης αποφάσεων σε όλα τα επίπεδα.

Το ISO 31000 παρέχει ένα πλαίσιο διαχείρισης κινδύνου με σκοπό να βοηθήσει τον οργανισμό να ενσωματώσει τη διαχείριση κινδύνου σε σημαντικές δραστηριότητες και λειτουργίες. Η αποτελεσματικότητα της διαχείρισης κινδύνων σε μεγάλο βαθμό επηρεάζεται από την ενσωμάτωσή της στην εταιρική διακυβέρνηση, συμπεριλαμβανομένης της λήψης αποφάσεων, γεγονός που απαιτεί συνεχή υποστήριξη από τα ενδιαφερόμενα μέρη, ιδιαίτερα από την ανώτατη διοίκηση.

Λόγω της σημαντικότητας της ανώτατης διοίκησης, η ηγεσία και η δέσμευση διαδραματίζει σημαντικό ρόλο στην εφαρμογή του. Η ανώτατη διοίκηση θα πρέπει να διασφαλίζει ότι η διαχείριση κινδύνων ενσωματώνεται σε όλες τις οργανωτικές δραστηριότητες και θα πρέπει να επιδεικνύουν ηγεσία και δέσμευση με:

- προσαρμογή και εφαρμογή όλων των στοιχείων του πλαισίου που παρέχεται
- έκδοση δήλωσης ή πολιτικής που καθορίζει μια προσέγγιση διαχείρισης κινδύνου, σχέδιο ή πορεία δράσης
- διασφάλιση ότι διατίθενται οι απαραίτητοι πόροι για τη διαχείριση του κινδύνου
- ανάθεση αρμοδιοτήτων, ευθύνης και λογοδοσίας σε κατάλληλα επίπεδα εντός του οργανισμού

Παράλληλα, το ISO σημειώνει και την ανάγκη για την αρμονική ενσωμάτωση της διαχείρισης κινδύνου, η οποία βασίζεται στην κατανόηση των οργανωτικών δομών και του πλαισίου το οποίο διέπει το ISO 31000. Οι δομές διαφέρουν ανάλογα με το σκοπό, τους στόχους και την πολυπλοκότητα της κάθε επιχείρησης και έτσι η διαχείριση του κινδύνου γίνεται σε κάθε τμήμα της δομής της. Με αυτό τον τρόπο, οι εργαζόμενοι σε κάθε βαθμίδα της έχουν αναλογική ευθύνη για τη διαχείριση του κινδύνου. Η ενσωμάτωση της διαχείρισης κινδύνου είναι μια δυναμική και επαναλαμβανόμενη διαδικασία και θα πρέπει να προσαρμόζεται στις ανάγκες και την κουλτούρα των επιχειρήσεων. Η διαχείριση κινδύνων πρέπει να είναι τμήμα και όχι διαφορετική έννοια από τον σκοπό, τη διακυβέρνηση, την ηγεσία και τη δέσμευση, τη στρατηγική, τους στόχους και τις λειτουργίες.

Ακόμη ένα δομικό στοιχείο του ISO 31000 είναι η σχεδίαση μιας δομής η οποία: 1) να αντιλαμβάνεται επαρκώς την επιχείρηση και το πλαίσιο λειτουργίας της – ώστε να προβλέπει με ακρίβεια τους κινδύνους, 2) να αρθρώνει δέσμευση για τη διαχείριση του κινδύνου, 3) να μπορεί να αναθέτει οργανωτικούς ρόλους, εξουσίες, και ευθύνες, 4) να μπορεί να διανέμει επαρκώς τους πόρους (π.χ. οικονομικούς) και 5) να είναι σε θέση να εγκαταστήσει ένα δίκτυο επικοινωνίας, κατανόησης και παροχής συμβουλευτικών, οδηγιών και κατευθυντήριων για την αντιμετώπιση των κινδύνων.

Προκειμένου να αξιολογηθεί η αποτελεσματικότητα του πλαισίου διαχείρισης κινδύνου, η επιχείρηση θα πρέπει περιοδικά να μετράει την απόδοση του πλαισίου διαχείρισης κινδύνου σε σχέση με τον σκοπό, τα σχέδια εφαρμογής, τους δείκτες και την αναμενόμενη συμπεριφορά του και παράλληλα να προσδιορίζει εάν παραμένει κατάλληλο για την υποστήριξη της επίτευξης των στόχων του οργανισμού.

Τέλος, η βελτίωση είναι ακόμη ένα από τα δομικά στοιχεία κατά την οποία μια επιχείρηση θα πρέπει να αποτιμά συνεχώς την διαδικασία που εφαρμόζει και να προσαρμόζει το πλαίσιο διαχείρισης κινδύνου για την αντιμετώπιση εξωτερικών και εσωτερικών αλλαγών. Με αυτόν τον τρόπο, ο οργανισμός μπορεί να βελτιώσει την αξία του και συγκεκριμένα να είναι σε θέση να βελτιώνει συνεχώς την καταλληλότητα, την επάρκεια και την αποτελεσματικότητα του πλαισίου διαχείρισης κινδύνου και τον τρόπο με τον οποίο ενσωματώνεται η διαδικασία διαχείρισης κινδύνου.

Ως προς τη διαδικασία αξιολόγησης των κινδύνων, η ανάλυση διαχείρισης θα πρέπει να λαμβάνει υπόψη παράγοντες όπως:

- την πιθανότητα γεγονότων και συνεπειών
- τη φύση και το μέγεθος των συνεπειών
- πολυπλοκότητα και συνδεσιμότητα
- παράγοντες που σχετίζονται με το χρόνο και αστάθεια
- την αποτελεσματικότητα των υφιστάμενων ελέγχων
- επίπεδα ευαισθησίας και εμπιστοσύνης

4. Μεθοδολογίες αξιολόγησης και διαχείρισης κινδύνου στα ΠΣ

4.1. Μέθοδος EAR / PILAR

Πρόκειται για λογισμικό που υλοποιεί και επεκτείνει τη Μεθοδολογία Magerit RA/RM. Το λογισμικό έχει σχεδιαστεί με σκοπό να υποστηρίζει τη διαδικασία διαχείρισης κινδύνου για μεγάλα χρονικά διαστήματα, παρέχοντας σταδιακή ανάλυση καθώς βελτιώνονται οι διασφαλίσεις. Οι λειτουργίες του περιλαμβάνουν κυρίως: Ποσοτική και ποιοτική Ανάλυση και Διαχείριση Κινδύνων Ποσοτική και ποιοτική Ανάλυση Επιχειρηματικών Επιπτώσεων & Συνέχεια Λειτουργιών. Το εργαλείο είναι διαισθητικό, παρέχει γρήγορους υπολογισμούς και δημιουργεί μια ποσότητα κειμένου και γραφικών.

Η μέθοδος αυτή παρέχει στην επιχείρηση :

- 1) Προσδιορισμό κινδύνων που ξεκινά από την ταυτοποίηση περιουσιακών στοιχείων (assets), σχέσεις και αξία για την επιχείρηση και καταλήγει στον προσδιορισμό και εκτίμηση απειλών.
- 2) Ανάλυση κινδύνου που περιλαμβάνει τον αντίκτυπο και τον αντίστοιχο κίνδυνο από απειλές, δυνητικές και υπολειμματικές τιμές με ποιοτικά και ποσοτικά μεγέθη
- 3) Αξιολόγηση κινδύνων καθώς Τα αποτελέσματα ιεραρχούνται και παρουσιάζονται στη διοίκηση για επιχειρηματική αξιολόγηση

Η επεξεργασία των πληροφοριών γίνεται στις εξής κατηγορίες:

- Παρέχεται ένα μοντέλο αξίας (value model) με περιουσιακά στοιχεία, εξαρτήσεις και αξίες.
- Παρέχεται ένας χάρτης κινδύνων που αποτελούν απειλές για περιουσιακά στοιχεία

- Παρέχονται πολιτικές ασφαλείας - βασική γραμμή για δημιουργία.
- Παρέχεται αξιολόγηση διασφάλισης: επίπεδο ωριμότητας με την πάροδο του χρόνου.
- Διαδικασίες ασφαλείας : γραμμή βάσης για δημιουργία.
- Πρόσθετες προστασίες περιουσιακών στοιχείων : για συγκεκριμένα περιουσιακά στοιχεία
- Εκτιμάται η Κατάσταση κινδύνου : ποιοτική και ποσοτική, συσσωρευμένη και εκτροπή.
- Συμμόρφωση με την ασφάλεια: σε σχέση με τυπικά και ειδικά προφίλ χρήστη.

Αυτή τη στιγμή η μεθοδολογία υποστηρίζει 4 διαθέσιμες γλώσσες: Αγγλικά, Ισπανικά, Ιταλικά και Γαλλικά. Το πρόγραμμα είναι δωρεάν για 30 ημέρες λειτουργίας (trial version).

Συνολικά το PILAR είναι ένα αρκετά χρήσιμο εργαλείο που πραγματοποιεί πολύ γρήγορη ανάλυση κινδύνου. Το αποτέλεσμα της ανάλυσης υπόκειται σε περαιτέρω μελέτη. Οι κίνδυνοι αναλύονται σε διάφορες διαστάσεις: εμπιστευτικότητα, ακεραιότητα, διαθεσιμότητα, αυθεντικότητα και ιχνηλασιμότητα (accountability). Για την αντιμετώπιση των παραπάνω κινδύνων, προτείνονται διασφαλίσεις (ή αντίμετρα), που αναλύουν τον υπολειπόμενο κίνδυνο.

4.2. Μέθοδος VERINICE

Το Verinice είναι ένα εργαλείο για τη διαχείριση της ασφαλείας πληροφοριών και κινδύνων. Το λογισμικό διατίθεται χωρίς άδεια χρήσης για 30 ημέρες. Υποστηρίζει λειτουργίες δημιουργίας, διατήρησης και βελτίωσης ενός ISMS με βάση το ISO 27001. Επίσης παρέχει διασφάλιση συμμόρφωσης με πρότυπα όπως ISO 27002, BSI IT-Baseline Security, VDA IS-Assessments και πολλά άλλα διεξαγωγή ανάλυσης κινδύνου με βάση το ISO 27005 έλεγχος, διαχείριση εγγράφων, δημιουργία αναφορών και πολλά άλλα. Το verinice τρέχει σε Windows, Linux και Mac OS.

Όλα τα παραπάνω είτε είναι έτοιμα στο εργαλείο είτε τα νεότερα μπορούν να εισαχθούν εύκολα. Όλα τα δεδομένα αποθηκεύονται σε ένα μοντέλο που είναι προσαρμοσμένο στις απαιτήσεις ασφάλειας πληροφοριών της επιχείρησης και είναι μπορεί να επεκταθεί.

Το Verinice επιτρέπει την εκτέλεση πλήρους ανάλυσης κινδύνου των στοιχείων ενεργητικού μιας επιχείρησης και να διεξαχθεί ανάλυση.Ο χρήστης θα πρέπει να προσθέσει απειλές και τρωτά σημεία από διάφορες υπάρχουσες πηγές του περιβάλλοντος της επιχείρησης.Τα αποτελέσματα στην ανάλυση κινδύνου θα βοηθήσουν να πραγματοποιηθεί αυτόματα μια αξιολόγηση κινδύνου για όλα τα περιουσιακά στοιχεία.Είτε ο προσδιορισμός των κινδύνων διεξάγεται σύμφωνα με το ISO 27005, είτε οποιαδήποτε άλλη διαδικασία, το λογισμικό verinice μπορεί να υποστηρίξει με αποτελεσματικότητα τις ανάγκες των επιχειρήσεων.

Το λογισμικό δημιουργεί διαφορετικά σενάρια κινδύνου ως μέρος των εργαστηρίων αξιολόγησης κινδύνου – ή καταφύγετε στους κινδύνους που αναφέρονται στον κατάλογο BSI IT Baseline Protection.

Συνοπτικά, πρόκειται για ένα επαγγελματικό πρόγραμμα το οποίο μπορεί να δοκιμαστεί δωρεάν αλλά η αγορά του είναι αρκετά κοστοβόρα.Τέλος, είναι αρκετά απαιτητικό σε υπολογιστικούς πόρους.

4.3. Μέθοδος SBA

Η μέθοδος SBA (Security By Analysis) δημιουργήθηκε στις αρχές του 1980 στη Σουηδία και αξιοποιείται έκτοτε σχεδόν αποκλειστικά στις Σκανδιναβικές χώρες.Βασικό χαρακτηριστικό της μεθόδου αυτής αποτελεί το γεγονός ότι αποδέχεται πως οι άνθρωποι που λαμβάνουν μέρος στην καθημερινή λειτουργία ενός πληροφοριακού συστήματος μπορούν πιθανότατα να εντοπίσουν προβλήματα που ενδέχεται να αντιμετωπίζει και να προτείνουν λύσεις για αυτά.Έχουν δημιουργηθεί διάφορες μέθοδοι SBA με κυριότερες τις SBA Check και SBA Scenario (Gerber & Von Solms, 2008).

Η μέθοδος SBA Check αποτιμά με ταχείς ρυθμούς το επίπεδο ασφάλειας ενός πληροφοριακού συστήματος, βασίζεται σε ερωτηματολόγια και δέχεται υποστήριξη από ειδικό λογισμικό.

Η μέθοδος SBA Scenario έχει τρεις επιλογές (Standard, 2015):

- Main analysis: πραγματοποιείται πλήρης ανάλυση του πληροφοριακού συστήματος προκειμένου να προσδιοριστεί η πιθανότητα πραγματοποίησης ενός κινδύνου ασφάλειας καθώς και εκτιμά το κόστος μέσω αναλυτικών αριθμητικών μεθόδων.
- Ten analysis: αναλύει με ταχείς ρυθμούς την πιθανότητα και το κόστος ώστε να προσδιορίζονται στην κλίμακα 1:10.
- Risk window: γίνεται συνοπτική ανάλυση η οποία βασίζεται σε μία ποιοτική κλίμακα τεσσάρων βαθμίδων.

Η SBA Scenario αποτελείται από τέσσερα στάδια:

- Προετοιμασία (preparation): στο στάδιο αυτό γίνεται συγκρότηση των ομάδων ανάλυσης και διδασκαλίας της SBA. Ο ειδικός έχει περιορισμένο ρόλο, δηλαδή είναι υπεύθυνο για τη διδασκαλία της μεθόδου και για τον συντονισμό των εργασιών της ομάδας. Επίσης σχηματίζεται το χρονοδιάγραμμα, πραγματοποιείται καταγραφή, οριοθέτηση και προσδιορισμός των ρόλων της ομάδας.
- Σενάρια (scenarios): στο στάδιο αυτό εντοπίζονται τα ενδεχομενικά σενάρια, αναλύεται η επικινδυνότητα χρησιμοποιώντας την αναλυτική περιγραφή του κάθε σεναρίου, καταγράφονται όλα τα διαθέσιμα στοιχεία που σχετίζονται με το σενάριο καθώς και εκτιμάται η πιθανότητα πραγματοποίησης του κάθε σεναρίου. Επιπλέον, πραγματοποιείται η διαχείριση της επικινδυνότητας προσδιορίζοντας τις ευπάθειες που σχετίζονται με το σενάριο, γίνεται επιλογή των αντιμέτρων και η κοστολόγησή τους.
- Σύνοψη (overview): στο στάδιο αυτό γίνεται καθορισμός των προτεραιοτήτων υλοποίησης, των προτεραιοτήτων σύμφωνα με τις επιπτώσεις και των προτεραιοτήτων σύμφωνα με τη μείωση της επικινδυνότητας που είναι εφικτή με την υλοποίηση του αντιμέτρου.

- Σχέδιο δράσης (action plan): στο στάδιο αυτό σχηματίζεται ένα συνολικό σχέδιο δράσης αναφορικά με την ασφάλεια του πληροφοριακού συστήματος και γίνεται καθορισμός των υπεύθυνων για την υλοποίηση των μέτρων προστασίας.

Πλεονεκτήματα της SBA μεθόδου:

1. Γίνεται υιοθέτηση μίας ολιστικής προσέγγισης (holistic approach) του ζητήματος της ασφάλειας.
2. Η ανάλυση πραγματοποιείται από τους ίδιους ανθρώπους που κάνουν καθημερινή χρήση του συστήματος.
3. Είναι αρκετά απλή, κατανοητή από μη – ειδικούς και υπάρχει η δυνατότητα να υλοποιηθεί με μικρό κόστος
4. Υποστηρίζεται από απλό και εύχρηστο λογισμικό.

Μειονεκτήματα της SBA μεθόδου:

1. Σημείο στήριξης σε μεγάλο βαθμό αποτελούν οι ικανότητες, η φαντασία και η διάθεση για συνεισφορά των ανθρώπων που εμπλέκονται
2. Θέτει ως προϋπόθεση την ανάπτυξη ανθρωποκεντρικής και συμμετοχικής κουλτούρας
3. Δεν προσφέρει βιβλιοθήκες μέτρων προστασίας.

4.4. Μέθοδος MEHARI

Η MEHARI (Methode Harmonisee d' Analyse de Risques) αποτελεί μία μέθοδο αξιολόγησης κινδύνου η οποία δημιουργήθηκε από την CLUSIF το 1996. Αφορά κυρίως στελεχιακό δυναμικό (διευθυντές λειτουργίας, CISO, CIO, ελεγκτές, διευθυντής διαχείρισης κινδύνων) και έχει ως κεντρικό θέμα τη διαχείριση της ασφάλειας των πληροφοριών και των πόρων των πληροφοριακών συστημάτων, καθώς και τη μείωση των κινδύνων. Η MEHARI παρουσιάζει συμβατότητα με το πρότυπο διαχείρισης κινδύνου ISO/ IEC 27005 και θεωρείται κατάλληλη για τη διαδικασία ISMS που σκιαγραφείται στο πρότυπο ISO 27001. Κάνει περιγραφή μίας περίπλοκης διαδικασία

ενσωματώνοντας τα κυκλικά βήματα της διαχείρισης κινδύνων καθώς και τη δημιουργία μιας προσαρμοσμένης βάσης γνώσεων (Gillies, 2011). Μετά τη δημιουργία βάσης γνώσεων αρχίζει μία διαδικασία για να αναλυθούν οι κίνδυνοι κάθε σεναρίου. Αυτή η διαδικασία γίνεται σύμφωνα με τα παρακάτω βήματα:

1. Ταυτοποίηση μιας κατάστασης κινδύνου (είτε αξιοποιώντας τη βάση γνώσεων είτε εντοπίζοντας τις πιθανές δυσλειτουργίες)
2. Αξιολόγηση της φυσικής έκθεσης
3. Αξιολόγηση των αποτρεπτικών και προληπτικών παραγόντων
4. Αξιολόγηση της προστασίας
5. Αξιολόγηση της πιθανότητας του κινδύνου
6. Αξιολόγηση των εγγενών επιπτώσεων (πχ. συνέπειες) με την συμπλήρωση ενός πίνακα
7. Αξιολόγηση και μείωση των επιπτώσεων διαμέσου αυτοματοποιημένου υπολογισμού
8. Σφαιρική αξιολόγηση του κινδύνου
9. Απόφαση αν ο κίνδυνος είναι αποδεκτός

Πλεονεκτήματα της μεθόδου MEHARI

1. Είναι συμβατή με όλα τα πρότυπα ασφαλείας πληροφοριών ISO
2. Περιλαμβάνει εκτεταμένη βάση γνώσεων σε μορφή Microsoft Excel

Μειονεκτήματα της μεθόδου MEHARI

1. Γίνεται χρήση της μόνο σε συνδυασμό με ειδικό λογισμικό ή υπολογιστικά φύλλα
2. Το πρώτο παράδειγμα της ανάλυσης έχει την απαίτηση από μια περίπλοκη προσαρμογή στη βάση γνώσεων.

4.5. Μέθοδος EBIOS

Η μέθοδος EBIOS (Expression des Besoins et Identification des Objectifs de Securite) κάνει αξιολόγηση και θέτει σε λειτουργία τους κινδύνους αναφορικά με την ασφάλεια των πληροφοριακών συστημάτων. Η μέθοδος αυτή αναπτύχθηκε από τη Direction Centrale de la Securite des Systemes d' Information (DCSSI), ένα τμήμα του γαλλικού υπουργείου άμυνας και στοχεύει κυρίως στη γαλλική διοίκηση.

Το ANSSI και ο σύλλογος EBIOS έχει αναπτύξει μία νέα έκδοση του EBIOS η οποία λαμβάνει υπόψη την εμπειρία ανατροφοδότησης και τις κανονιστικές αλλαγές. Η νέα μέθοδος έχει πιο εύκολη χρήση, είναι πιο σαφής και περιλαμβάνει παραδείγματα και συμβουλές. Δίνει την ικανότητα να δημιουργηθούν και να παρατηρούν ένα σχέδιο δράσης αναφορικά με την ασφάλεια των πληροφοριακών συστημάτων. Επίσης, περιέχει μία μελέτη περίπτωσης για την κατανόηση της μεθόδου (Standard, 2015).

Η EBIOS συμφωνεί με τα διεθνή πρότυπα ISO/IEC 31000, ISO/IEC 27001, ISO/IEC 27005, ISO/IEC 13335, ISO/IEC 15408, ISO/IEC 17799.

Η μέθοδος EBIOS εξακολουθεί να θεωρείται ως το θεμελιώδες πακέτο εργαλείων για οποιαδήποτε συζήτηση αναφορικά με την ασφάλεια πληροφοριών.

Η EBIOS περιλαμβάνει πέντε ενότητες:

1. Μελέτη του πλαισίου
2. Μελέτη των ανεπιθύμητων ενεργειών
3. Μελέτη των σεναρίων για απειλές
4. Μελέτη της επικινδυνότητας
5. Μελέτη των μέτρων ασφάλειας

Μελέτη του πλαισίου

Αυτή η ενότητα στοχεύει στη συλλογή στοιχείων που είναι αναγκαία για τη διαχείριση κινδύνων. Προσαρμόζεται στο πλαίσιο της μελέτης και στα αποτελέσματά της με σκοπό

να γίνει χρήσης τους από τους ενδιαφερόμενους. Δίνει τη δυνατότητα να επισημοποιηθεί το πλαίσιο διαχείρισης κινδύνων στο οποίο γίνεται η μελέτη, καθώς και να εντοπιστεί, να οριοθετηθεί και να περιγραφεί το πεδίο εφαρμογής της. Μετά την ολοκλήρωση αυτής της ενότητας σκιαγραφείται το σύνολο των παραμέτρων που περιέχονται σε άλλες ενότητες.

Η ενότητα αυτή αποτελείται από τρία στάδια:

- Ορισμός του πεδίου διαχείρισης κινδύνου
- Προετοιμασία μετρήσεων
- Προσδιορισμός των αγαθών

Μελέτη των ανεπιθύμητων ενεργειών / Μελέτη των σεναρίων για απειλές

Οι ενότητες αυτές στοχεύουν στον προσδιορισμό των γενικών σεναρίων των ανεπιθύμητων ενεργειών και απειλών. Δίνουν τη δυνατότητα να αναδειχθούν όλα τα ανεπιθύμητα συμβάντα εντοπίζοντας και συνδυάζοντας κάθε ένα από τα συστατικά του. Υπάρχει η δυνατότητα εκτίμησης της σοβαρότητας και της πιθανότητας κάθε ανεπιθύμητης ενέργειας/ απειλής. Προσφέρουν βοήθεια στον εντοπισμό των ήδη υπαρχόντων μέτρων ασφάλειας και, εφόσον τεθούν σε εφαρμογή, γίνεται ο επαναυπολογισμός της επίδρασης των συμβάντων. Μετά την ολοκλήρωση κάθε ενότητας, γίνεται προσδιορισμός των επίφοβων συμβάντων και των απειλών αντιστοίχως, παρέχεται εξήγηση και τοποθετούνται σύμφωνα με τη πιθανότητα και τη σοβαρότητά τους (Gillies, 2011).

Μελέτη της επικινδυνότητας

Στόχος αυτής της ενότητας αποτελεί η απόδειξη των συστηματικών κινδύνων και η επιλογή του τρόπου επεξεργασίας υπολογίζοντας και τις ιδιαιτερότητες του πλαισίου. Συνδέοντας τα ανεπιθύμητα γεγονότα με τα σενάρια των απειλών που μπορεί να προκύψουν, αυτή η ενότητα δίνει τη δυνατότητα να προσδιοριστούν μόνο τα πραγματικά σενάρια στο πεδίο εφαρμογής της μελέτης. Επίσης, υπάρχει η δυνατότητα να δοθεί προτεραιότητα και να γίνει επιλογή της κατάλληλης θεραπείας. Μετά, την ολοκλήρωση της ενότητας, γίνεται αξιολόγηση των κινδύνων και των θεραπευτικών επιλογών.

Η ενότητα αυτή αποτελείται από δύο στάδια:

- Αξιολόγηση των κινδύνων
- Προσδιορισμός των στόχων ασφάλειας

Μελέτη των μέτρων ασφάλειας

Στόχος της ενότητας αποτελεί ο καθορισμός της αντιμετώπισης των κινδύνων και η παρακολούθηση της εφαρμογής τους. Δίνει τη δυνατότητα για την επίτευξη της συναίνεσης αναφορικά με τα μέτρα ασφάλειας που είναι σχεδιασμένα για την αντιμετώπιση του κινδύνου που έχει αναγνωριστεί προηγουμένως, αποδεικνύοντας τον σχεδιασμό, την υλοποίηση και την επικύρωση της θεραπείας. Μετά την ολοκλήρωση αυτής της ενότητας, γίνεται προσδιορισμός των μέτρων ασφάλειας. Υπάρχει ακόμη η δυνατότητα να υλοποιηθεί και η παρακολούθηση της εφαρμογής (Gritzalis, Iseppi, Mylonas & Stavrou, 2018).

Η ενότητα αυτή αποτελείται από δύο στάδια:

- Επισημοποίηση των μέτρων ασφάλειας που πρέπει να εφαρμοστούν
- Εφαρμογή των μέτρων ασφάλειας

Πλεονεκτήματα της μεθόδου EBIOS

1. Θεωρείται ως μια γενική μέθοδος που παρέχει τη δυνατότητα ρύθμισης με τα τοπικά πρότυπα, συνήθειες, πλαίσιο
2. Υπάρχει η πιθανότητα να εφαρμοστεί με τους στόχους της αξιολόγησης των διαφορών μεγεθών και πολυπλοκότητας

Μειονέκτημα της μεθόδου EBIOS είναι η πιο αναλυτική τεκμηρίωση και υποστήριξη διατίθεται μόνο στα γαλλικά

4.6. Μέθοδος OCTAVE-S

Η OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation) διατυπώνει μία στρατηγική αξιολόγησης κινδύνων των πληροφοριακών συστημάτων. Η

OCTAVE είναι αυτοκατευθυνόμενη, δηλαδή άτομα από την οργάνωση είναι υπεύθυνα για τον καθορισμό στρατηγικής για την ασφάλεια ενάντια στους κινδύνους. Η OCTAVE-S συνιστά μία παραλλαγή προσαρμοσμένη στα περιορισμένα μέσα και τους περιορισμούς των μικρών οργανώσεων (έως 100 άτομα).

Η OCTAVE-S καθοδηγείται από μία μικρή διεπιστημονική ομάδα, τρία με πέντε άτομα, από το προσωπικό του οργανισμού που συλλέγει και αναλύει τα στοιχεία και δημιουργεί στρατηγική για την προστασία και τα σχέδια μετριασμού στηριζόμενα στους λειτουργικούς κινδύνους του οργανισμού. Για την αποτελεσματική διεξαγωγή της OCTAVE-S η ομάδα είναι αναγκαίο να διαθέτει ευρεία γνώση των επιχειρηματικών δραστηριοτήτων και των διαδικασιών ασφάλειας του οργανισμού, με σκοπό να μπορεί να πραγματοποιεί όλες τις δραστηριότητες μόνη της (Harahap, 2011). Οι μικρές οργανώσεις συνήθως δεν έχουν αναπτυγμένες οργανωτικές ικανότητες για να εκτελούν και να ερμηνεύουν τα αποτελέσματα που προκύπτουν από τα εργαλεία αξιολόγησης της ευπάθειας. Έτσι, αντί να κάνουν χρήση των δεδομένων ευπάθειας με σκοπό τη βελτίωση της προβολής των τεχνικών της τρέχουσας ασφάλειας, διερευνούν τις διαδικασίες που εφαρμόζονται κατά τη διάρκεια της ρύθμισης και της διατήρησης της υπολογιστικής υποδομής τους (Sheikhpour & Modiri, 2012).

Εάν τυχόν παρουσιαστούν ελλείψεις στην οργανωτική ικανότητα, καταγράφονται και διερευνώνται κατά τη φάση 3 του OCTAVE-S όταν ο οργανισμός δημιουργήσει μια στρατηγική για την προστασία του.

Η OCTAVE-S αποτελείται από τρεις φάσεις:

Φάση 1: Δημιουργία αγαθού βασισμένο στα προφίλ των απειλών

Στη φάση 1 γίνεται αξιολόγηση των οργανωτικών πτυχών. Κατά τη διάρκεια αυτής της φάσης, καθορίζονται από την ομάδα ανάλυσης τα κριτήρια αξιολόγησης των επιπτώσεων τα οποία θα χρησιμοποιηθούν αργότερα για την αξιολόγηση των κινδύνων. Κάνει προσδιορισμό των αγαθών και αποτιμά την αξία της ασφάλειας της τρέχουσας πρακτικής του οργανισμού (Humphreys, 2016). Όλες οι εργασίες ολοκληρώνονται από την ομάδα μέσω της συλλογής επιπρόσθετων πληροφοριών μόνο όταν τις έχει ανάγκη. Στη συνέχεια κάνει επιλογή τριών με πέντε κρίσιμων περιουσιακών στοιχείων και γίνεται σε βάθος

ανάλυση σύμφωνα με την σημασία τους στον οργανισμό. Τέλος, η ομάδα καθορίζει τις απαιτήσεις ασφάλειας και ένα προφίλ απειλών για κάθε κρίσιμο αγαθό.

Αυτή η φάση αποτελείται από δύο διαδικασίες.

1. Εντοπισμός των οργανωτικών πληροφοριών

- Καθιερώνονται τα κριτήρια αξιολόγησης των επιπτώσεων
- Προσδιορίζονται τα οργανωτικά αγαθά
- Αξιολογούνται τα οργανωτικά πρακτικά ασφάλειας

2. Δημιουργία προφίλ απειλών

- Γίνεται επιλογή του κρίσιμου αγαθού
- Προσδιορίζονται οι απαιτήσεις ασφάλειας για τα κρίσιμα αγαθά
- Προσδιορίζονται οι απειλές για τα κρίσιμα αγαθά

Φάση 2: Προσδιορισμός ευπάθειας υποδομών

Κατά τη διάρκεια αυτής της φάσης, η ομάδα ανάλυσης κάνει μία ανασκόπηση υψηλού επιπέδου της υπολογιστικής υποδομής του οργανισμού. Γίνεται ανάλυση του τρόπου με τον οποίο οι άνθρωποι κάνουν χρήση της υπολογιστικής υποδομής με σκοπό να έχουν πρόσβαση σε αγαθά ζωτικής σημασίας, παρέχοντας τις κύριες κατηγορίες των συστατικών καθώς και για το ποιος ευθύνεται για τη διαμόρφωση και τη διατήρηση των εν λόγω στοιχείων (Iqbal, Horie, Goto & Cheng, 2009).

Η φάση 2 διαθέτει μία διαδικασία.

1. Εξέταση υπολογιστικής υποδομής αναφορικά με κρίσιμα αγαθά

- Εξέταση προσπέλασης
- Ανάλυση τεχνολογίας με τις σχετικές διαδικασίες

Φάση 3: Ανάπτυξη σχεδίων και στρατηγικής για την ασφάλεια

Κατά τη διάρκεια της φάσης 3, πραγματοποιείται εντοπισμός από την ομάδα ανάλυσης των κινδύνων για τα περιουσιακά στοιχεία του οργανισμού και παίρνει την απόφαση για

το τι πρέπει να κάνει. Με βάση την ανάλυση των πληροφοριών που συγκεντρώθηκαν, η ομάδα αναπτύσσει μία στρατηγική προστασίας για την οργάνωση και τα σχέδια μετριασμού των επιπτώσεων για να αντιμετωπιστούν οι κίνδυνοι στα αγαθά. Τα φύλλα εργασία OCTAVE-S που αξιοποιούνται σε αυτή τη φάση έχουν εξαιρετική δομή και συνδέονται με τον κατάλογο πρακτικών του OCTAVE, δίνοντας τη δυνατότητα στην ομάδα να αντιστοιχίσει τις συστάσεις για τη βελτίωση των πρακτικών ασφάλειας σε ένα αποδεκτό σημείο.

Αυτή η φάση αποτελείται από 2 διαδικασίες.

1. Προσδιορισμός και ανάλυση κινδύνων

- Αξιολογούνται οι επιπτώσεις των απειλών
- Καθιερώνονται τα κριτήρια αξιολόγησης πιθανοτήτων
- Αξιολογούνται οι πιθανότητες των απειλών

2. Ανάπτυξη στρατηγικής προστασίας και σχεδίων μετριασμού επιπτώσεων

- Περιγράφεται η στρατηγική της τρέχουσας προστασίας
- Γίνεται επιλογή του μετριασμού προσεγγίσεων
- Αναπτύσσονται σχέδια μετριασμού των κινδύνων
- Προσδιορίζονται οι αλλαγές στην στρατηγική προστασίας
- Προσδιορίζονται τα επόμενα βήματα

Πλεονεκτήματα της μεθόδου OCTAVE-S (Humphreys, 2016):

- 1.** Πραγματοποιείται από μικρές ομάδες των ιδίων εργαζομένων του οργανισμού
- 2.** Περιλαμβάνει ποικίλες μεθόδους προσαρμοσμένες για συγκεκριμένες οργανώσεις και πλαίσια
- 3.** Αποτελεί μία ευρέως χρησιμοποιούμενη μέθοδος με αφθονία δικαιολογητικών και συμβατών εργαλείων τρίτων κατασκευαστών

Μειονέκτημα της μεθόδου OCTAVE-S (Ionita, 2013):

- Είναι μία βαριά μέθοδος που διαθέτει πολλούς τόμους, φύλλα εργασίας και διαδικασίες.

5. Εμπειρική μελέτη

Για τη διεξαγωγή του ερευνητικού τμήματος, της υλοποίησης της πτυχιακής εργασίας χρειάστηκε να υπάρξει κατάλληλο πρόγραμμα που θα οπτικοποιεί τα δεδομένα που είναι διαθέσιμα για τη μελέτη περίπτωσης που εξετάζουμε. Για την επιλογή του κατάλληλου λογισμικού εξετάστηκε η δυνατότητα επιλογής ενός λογισμικού που θα μπορούμε να εισάγουμε τα στοιχεία της επιχείρησης και τους κινδύνους που υπάρχουν. Η βιβλιογραφική ανασκόπηση κατέληξε στην ύπαρξη τεσσάρων προγραμμάτων, τα οποία θα μπορούσαν να αποτελέσουν αξιόπιστες λύσεις για την παρουσίαση των κινδύνων :

- Το RM Studio με δωρεάν άδεια λειτουργίας για 21 μέρες
- SimpleRisk , το οποίο δεν έχει περιορισμό λειτουργίας σε Virtual Machine
- PILAR με δωρεάν άδεια λειτουργίας για 30 μέρες
- Verinice με δωρεάν άδεια λειτουργίας για 30 μέρες

Τα παραπάνω προγράμματα έχουν χρησιμοποιηθεί σε αντίστοιχες εργασίες και πτυχιακές και παρέχονται ως πρόταση από το Πανεπιστήμιο. Το πρόγραμμα που επιλέχθηκε τελικά ήταν το PILAR, γιατί ήταν διαθέσιμο για μεγαλύτερο διάστημα, για λόγους παρουσίασης και διότι θα μπορούσαμε να χρησιμοποιήσουμε περισσότερα διαγράμματα για την καλύτερη οπτικοποίηση των δεδομένων.

5.1. Το πρόγραμμα που χρησιμοποιήθηκε

Το λογισμικό PILAR αποτελεί το σύστημα που χρησιμοποιείται στην παρούσα εργασία και παρέχει ένα σύνολο εργαλείων για ανάλυση και διαχείριση κινδύνων. Το πρόγραμμα και η μεθοδολογία που χρησιμοποιεί, περιεγράφηκε στο κεφάλαιο 4.1. Το PILAR εξειδικεύεται στα Συστήματα Πληροφοριών και Επικοινωνιών και υποστηρίζει τη μεθοδολογία Magerit που παρέχεται από την Ισπανική Διοίκηση. Η επιχείρηση που θέλει να αξιολογήσει και να αναλύσει τους κινδύνους, θα πρέπει να εισάγει τα δεδομένα που υπάρχουν στο επιχειρηματικό της περιβάλλον. Τα περιουσιακά στοιχεία των επιχειρήσεων υπόκεινται σε απειλές που, όταν συμβούν, υποβαθμίζουν την αξία και τη χρήση του κάθε περιουσιακού στοιχείου. Το κόστος ενός γεγονότος ονομάζεται αντίκτυπο. Εάν είμαστε σε θέση να εκτιμήσουμε τη συχνότητα των απειλών, τότε τα εργαλεία μπορούν να εκτιμήσουν τον κίνδυνο στον οποίο υπόκειται το σύστημα. Η υποβάθμιση και η συχνότητα είναι τα μέσα για την εκτίμηση της άμυνας του συστήματος. Ο διαχειριστής συστήματος έχει την επιλογή να αναπτύξει δικλίδες ασφαλείας, είτε για να μειώσει τη συχνότητα είτε για να περιορίσει τον αντίκτυπο. Ο βαθμός αποτελεσματικότητας αυτών των διασφαλίσεων, το σύστημα υπόκειται σε υπολειπόμενο κίνδυνο. Το λογισμικό PILAR παρέχει μια τυπική βιβλιοθήκη εργαλείων για περιουσιακά στοιχεία, απειλές και μέτρα προστασίας. Επιπλέον, είναι σε θέση να εξάγει κλιμακώσεις ασφαλείας έναντι ευρέως γνωστών προτύπων ασφαλείας, όπως π.χ ISO/IEC 27002:2013 - Κώδικας πρακτικής για τη διαχείριση της ασφάλειας πληροφοριών. Το PILAR έχει χρηματοδοτηθεί εν μέρει από το Centro Criptológico Nacional (Ισπανική Υπηρεσία Εθνικής Ασφάλειας).

Οδηγίες για τη χρήση του προγράμματος παρέχονται από το Πανεπιστήμιο, οι οποίες ακολουθήθηκαν για την ορθή χρήση του και τη διεξαγωγή συμπερασμάτων.

Η εγκατάσταση του προγράμματος γίνεται σε διάφορα λειτουργικά συστήματα όπως Windows, Linux, Java, MacOS.

Για τα Windows που είναι το πιο συνηθισμένο λειτουργικό σύστημα το PILAR εγκαθίσταται με δικαιώματα διαχειριστή ή ως απλός χρήστης. Τα αρχεία μπορούν να εγκατασταθούν οπουδήποτε. Για τα δικαιώματα διαχειριστή, τα αρχεία μπορεί να πάνε

στο "Program Files" για όλους τους χρήστες και το μητρώο μπορεί να έχει μια σειρά από καταχωρήσεις για να συσχετίσει το PILAR με τις επεκτάσεις .mgr.

- Αρχικά θα πρέπει να εγκατασταθεί το πρόγραμμα που είναι της μορφής `pilar_<version>_<profile>_<lang>.exe`
- Στη συνέχεια ο χρήστης θα πρέπει να ακολουθήσει τις οδηγίες για να εγκαταστήσει στον κατάλογο της προτίμησης του (πολλές γλώσσες μπορεί να μοιράζονται τον ίδιο κατάλογο εγκατάστασης)
- όταν ολοκληρωθεί η εγκατάσταση, θα υπάρχει ένα αρχείο `pilar.exe` στο σημείο που ο χρήστης θα αποφασίσει να εγκαταστήσει το λογισμικό.

Σε ότι αφορά την άδεια χρήσης, κάνοντας δεξί κλικ στο πλαίσιο "άδεια χρήσης", παρουσιάζονται οι ακόλουθες επιλογές:

- κωδικός ενεργοποίησης (εδώ ο χρήστης μπορεί να κάνει επικόλληση αν έχει κωδικό στην κατοχή του)
- αρχείο άδειας χρήσης (εδώ ο χρήστης μπορεί να επιλέξει αν έχει στην κατοχή του ένα αρχείο LIC)
- άδεια αξιολόγησης (ο χρήστης μπορεί να δημιουργήσει αυτόματα μια προσωρινή άδεια αξιολόγησης για 30 ημέρες).
- Επαναφορά (αυτή η επιλογή επιλέγεται για να απορρίψει το PILAR την τελευταία επιλογή και να ξεκινήσει εκ νέου την επικύρωση της άδειας).

Αφού εγκατασταθεί, το υπολογιστικό σύστημα διαθέτει τρία επίπεδα χρηστών σύμφωνα με το εγχειρίδιο χρήσης του : basic user, average user και advanced user. Στο κάθε επίπεδο χρήστη αντιστοιχούν κάποιες συγκεκριμένες ενέργειες για το σύστημα.

Ο **basic user** μπορεί να ρυθμίσει τις επιλογές του προγράμματος. Οι ενέργειες που μπορεί να κάνει ο χρήστης σε αυτό το επίπεδο είναι:

- Να κάνει μια εκτίμηση για τα περιουσιακά στοιχεία + τομείς. Ουσιαστικά ο χρήστης αξιολογεί τα βασικά περιουσιακά στοιχεία που κατανέμονται σε τομείς ασφαλείας

- Να επισημάνει αυτόματα τις απειλές. Το PILAR εφαρμόζει ένα τυποποιημένο προφίλ για τις στιγμές που δέχεται επίθεση.
- Να αξιολογεί τις διάφορες φάσεις επικινδυνότητας με μια βαθμολογία η οποία αντιγράφεται στις επόμενες φάσεις, εκτός αν τροποποιηθεί.
- Να αλλάξει την πιθανότητα να συμβεί ένα ενδεχόμενο
- Να αλλάξει το ποσοστό της επίδρασης
- Να ελέγξει αν το πρόγραμμα δέχεται λογικές μετβαλητές.
- Να διασταυρώνει τις διαστάσεις και να μεταφέρει αξίες ως προς την ασφάλεια των δικλίδων σε κάθε περίπτωση.

Τα βασικά περιουσιακά στοιχεία που μπορεί να παραθέσει ο basic user εισάγονται ένα προς ένα από τον χρήστη. Στην ουσία, γίνεται η εισαγωγή περιουσιακών στοιχείων ως πληροφοριών όπως απαιτείται για να καταγραφούν όλα τα στοιχεία που αφορούν τους διαχειριστές. Εδώ μπορούν να χρησιμοποιηθούν συγκεντρωτικά στοιχεία ενεργητικού που αντιπροσωπεύουν στοιχεία πληροφοριών με την ίδια βαθμολογία και να προστεθούν επιχειρηματικές υπηρεσίες.

Το PILAR αναλαμβάνει να μεταφράσει τις απαιτήσεις ασφαλείας (επίπεδα) από βασικά σε υποστηρικτικά περιουσιακά στοιχεία- και σε αυτό το στάδιο ο χρήστης μπορεί να αναθεωρήσει και να τα βελτιώσει χειροκίνητα προσαρμόζοντας μεμονωμένα περιουσιακά στοιχεία.

Στο τέλος της κάθε διαδικασίας εισαγωγής στοιχείων δομούνται τα προφίλ ασφαλείας τα οποία είναι συλλογές αντιμέτρων, τόσο τεχνικών όσο και διαδικαστικών. Το PILAR μπορεί να φορτώσει ένα ή περισσότερα για να βοηθήσει τους χρήστες να αντιμετωπίσουν τεχνικούς κινδύνους μέσω αντιμέτρων και να συμμορφωθούν με τους φορείς διαπίστευσης. Στην οθόνη παρουσιάζεται η συμμόρφωση προς ένα συγκεκριμένο προφίλ ασφαλείας, το οποίο αποτελείται από ελέγχους ασφαλείας που μπορούν να επεκταθούν ή να χρειάζεται μέτρα διασφάλισης .

Μετά από αυτά, το PILAR μπορεί να παρέχει προτάσεις προς μέτρα ασφαλείας τα οποία είναι προς τον χρήστη για διόρθωση.

Ο **average user** έχει κάποιες παραπάνω δικαιοδοσίες και αρμοδιότητες από τον βασικό χρήστη, οι οποίες υπάρχουν σε όλα τα στάδια. Οι πρόσθετες αρμοδιότητες εκκινούν με την καταχώρηση των περιουσιακών στοιχείων τα οποία μπορούν να κατανεμηθούν σε τομείς ασφαλείας. Κάθε τομέας ασφάλειας μπορεί να έχει συγκεκριμένο προφίλ επίθεσης και συγκεκριμένα μέτρα ασφάλειας. Οι τομείς ασφαλείας αλληλοσυνδιάζονται: ένας τομέας εμφανίζεται ως τμήμα ενός άλλου τομέα. Η ένθεση χρησιμοποιείται στην αξιολόγηση των διασφαλίσεων και των προφίλ ασφαλείας.

Για την αξιολόγηση των στοιχείων αυτών, πρέπει να αξιολογηθούν τα βασικά περιουσιακά στοιχεία, και η αξία τους μεταφράζεται σε κάθε περιουσιακό στοιχείο στον ίδιο τομέα, καθώς και σε άλλους τομείς με τους οποίους συνδέεται το βασικό περιουσιακό στοιχείο.

Στη συνέχεια καθορίζονται οι φάσεις που θα εξελιχθούν οι διαδικασίες ελέγχου. Αμέσως μετά, το PILAR θα τρέξει μια διαδικασία διασφάλισης, κατά την οποία λαμβάνει υπόψη

- τις κλάσεις των περιουσιακών στοιχείων στον τομέα
- το επίπεδο ασφάλειας που απαιτείται, άμεσα ή έμμεσα, για κάθε διάσταση για κάθε περιουσιακό στοιχείο στον τομέα
- την ικανότητα κάθε μέσου διασφάλισης να προστατεύει κάθε διάσταση ασφάλειας
- την εγγενή ισχύς (δύναμη) του μέτρου διασφάλισης

Στη συνέχεια ο χρήστης επιλέγει τα μέτρα ασφαλείας για την αντιμετώπιση του κινδύνου και για τη συμμόρφωση. Για τη συλλογή μέτρων ασφαλείας της οι χρήστες έχουν τρεις επιλογές:

- μπορούν να τα αγνοήσουν εντελώς
- να τα βλέπουν, αλλά να μην τα χρησιμοποιούν για την αντιμετώπιση του κινδύνου
- να τα βλέπουν και να τα εφαρμόζουν για την αντιμετώπιση του κινδύνου

Ο **advanced user** έχει και αυτός κάποιες παραπάνω δικαιοδοσίες από τους προηγούμενους δύο. Οι αρμοδιότητες ξεκινούν με τον καθορισμό του ποιο περιουσιακό στοιχείο εξαρτάται από ποιο άλλο περιουσιακό στοιχείο (dependencies). Σε αυτό το σημείο, η εφαρμογή των απαιτήσεων ασφαλείας σε κάθε περιουσιακό στοιχείο σε έναν ενιαίο τομέα ασφαλείας είναι μια γρήγορη προσέγγιση, αλλά μερικές φορές είναι το ακριβώς αντίθετο. Για παράδειγμα, όταν κάθε πληροφορία και υπηρεσία βασίζεται μόνο σε ένα υποσύνολο του εξοπλισμού του τομέα. Κατά συνέπεια, υπάρχουν περιπτώσεις που ο χρήστης θα πρέπει ακριβώς να καθορίσει τα dependencies. Ο καθορισμός ενός σωστού και λειτουργικού συνόλου dependencies είναι χρονοβόρος και δύσκολο να διατηρηθεί, αλλά παρέχει την καλύτερη ανάλυση κινδύνου. Τα dependencies μπορούν να εντοπιστούν σε μια σειρά από λειτουργίες. Μια από αυτές είναι οι κόμβοι OR, κατά τους οποίους καθορίζονται οι εξαρτήσεις εντός τους. Οι κόμβοι OR αντιπροσωπεύουν εναλλακτική παροχή. Κάθε κλάδος πρέπει να πληροί τις απαιτήσεις ασφάλειας πληροφοριών (εμπιστευτικότητα, ακεραιότητα, ...), αλλά και τη διαθεσιμότητα. Έτσι, τα περιουσιακά στοιχεία σε έναν μόνο κλάδο δεν κληρονομούν απαιτήσεις διαθεσιμότητας επειδή υπάρχει και άλλος κλάδος. Εκτός αν υπάρχουν κοινά σημεία αποτυχίας, δηλαδή περιουσιακά στοιχεία που υποστηρίζουν και τους δύο κλάδους.

Ακόμη, ένας advanced user μπορεί να παραλείψει την αποτίμηση τομέα και να μην δημιουργήσει καμία εξάρτηση. Σε κάθε περιουσιακό στοιχείο πρέπει να εκχωρηθούν ξεχωριστά οι απαιτήσεις ασφαλείας. Αυτό είναι χρονοβόρο και δύσκολο να διατηρηθεί όταν το πληροφοριακό σύστημα αλλάζει, και οι κίνδυνοι δεν μπορούν να αξιολογηθούν.

Ως προς τις απειλές, το PILAR εφαρμόζει ένα τυποποιημένο προφίλ επιθέσεων που καθορίζει τις απειλές που είναι πιθανές για κάθε περιουσιακό στοιχείο και εκτιμά την πιθανότητα και τις συνέπειές τους. Το προφίλ είναι ένα εξωτερικό αρχείο. Οι advanced χρήστες μπορούν να επεξεργαστούν το αρχείο αυτό. Ακόμη, μπορούν να έχουν πολλά

αρχεία και να επιλέγουν ένα για κάθε τομέα ασφαλείας. Η επεξεργασία του εξωτερικού αρχείου είναι η καλύτερη προσέγγιση αφενός για την τεκμηρίωση των αλλαγών και αφετέρου για την ανάλυση ενός πληροφοριακού συστήματος υπό διαφορετικά σενάρια επίθεσης

Τέλος, ο χρήστης advanced μπορεί να απενεργοποιήσει το μηχανισμό διάδοσης που εφαρμόζεται για την ασφάλεια του συστήματος. Το PILAR αντιστοιχίζει τους ελέγχους σε δικλείδες ασφαλείας και, στη συνέχεια, οι αλλαγές στην ωριμότητα των ελέγχων μεταδίδονται στις συνδεδεμένες δικλείδες ασφαλείας και η ωριμότητα των δικλείδων ασφαλείας χρησιμοποιείται για την εκτίμηση της ωριμότητας των ελέγχων. Αυτός ο μηχανισμός διάδοσης μπορεί να απενεργοποιηθεί με παρέμβαση του χρήστη. Ο χρήστης μπορεί επίσης να μεταφέρει τη βαθμολογία ελέγχου στις διασφαλίσεις και τη βαθμολογία διασφαλίσεων στους ελέγχους, αλλά αυτό δεν είναι αυτοματοποιημένο. Έτσι, ο χρήστης advanced μπορεί να παρουσιάσει την ωριμότητα των ελέγχων για τη συμμόρφωση, ξεχωριστά από την ωριμότητα των διασφαλίσεων για την αντιμετώπιση του κινδύνου.

Για κάποιες από τις παραπάνω επιλογές και λειτουργίες του PILAR, στο παράρτημα της εργασίας παρατίθενται screenshots από το πρόγραμμα για την ευκρινέστερη αντίληψή του.

5.2. Το case study της εργασίας

Η μελέτη περίπτωσης της πτυχιακής εργασίας επικεντρώνεται σε μια επιχείρηση ως case study. Η επιχείρηση που επιλέχθηκε είναι η Εταιρεία Α.Ε. ένας εξειδικευμένος πάροχος λύσεων λογισμικού Τηλεπικοινωνιών, Ενοποιημένων Επικοινωνιών και Επιχειρήσεων. Η επιχείρηση απευθύνεται σε επιχειρήσεις (business to business) ως πελάτες. Η εταιρία ιδρύθηκε το 2001 και έκτοτε εφαρμόζει εξειδικευμένες λύσεις ICT που συνδυάζουν αναπτυγμένες εφαρμογές με καθιερωμένες λύσεις από κορυφαίους παρόχους τεχνολογίας παγκοσμίως. Η εταιρία παράγει έργα που επιτρέπουν στους πελάτες της να

αυξήσουν την παραγωγικότητά τους, να μεγιστοποιήσουν την αποτελεσματικότητά τους και τελικά να γίνουν κορυφαίες επιδόσεις στον επιχειρηματικό τους τομέα. Οι βασικές υπηρεσίες της επιχείρησης είναι τρεις: διαχείριση δεδομένων και αναλυτικών επιδόσεων της επιχείρησης, διαχείριση και συνεργασία επιχειρήσεων και ειδικές λύσεις τηλεπικοινωνιών. Συγκεκριμένα, η επιχείρηση εξυπηρετεί άλλες επιχειρήσεις για τις παρακάτω υπηρεσίες .

Εικόνα 1 : Υπηρεσίες επιχείρησης

1.	 DATA MANAGEMENT & BUSINESS ANALYTICS AI & Machine Learning - Big data	• Data Warehouse & Data Virtualization • Big Data Analytics • Reports & Forecasts
2.	 ENTERPRISE MANAGEMENT & COLLABORATION	• Digital Process & Document Management • Digital Signature • Team Collaboration / Project Management • Digital Workspace
3.	 TELECOM SPECIFIC SOLUTIONS	• Network Planning & Asset Management • Multi-Service Access Routers & EAD • Transport Systems

5.3. Το πληροφοριακό σύστημα

Σε αυτή την ενότητα της εργασίας παρατίθεται και σχολιάζεται το πληροφοριακό σύστημα που η εταιρία χρησιμοποιεί. Πρόκειται για ένα πληροφοριακό σύστημα το οποίο είναι ένα Σύστημα Αυτοματισμού και Διοίκησης. Επιτελεί λειτουργίες για τη βελτίωση της επικοινωνίας και της παραγωγικότητας εντός της επιχείρησης με την αυτοματοποίηση καθηκόντων ρουτίνας και τη βελτίωση της ροής πληροφοριών και παράλληλα συλλέγει, επεξεργάζεται και παρέχει πληροφορίες σε διαχειριστές και άλλους λήπτες αποφάσεων, διευκολύνοντας τη λήψη αποφάσεων στη διοίκηση. Το συγκεκριμένο πληροφοριακό σύστημα καλύπτει σκοπούς όπως η εύρυθμη λειτουργία της επιχείρησης, η αποτελεσματική επικοινωνία, η διοίκηση, η καταγραφή πληροφοριών.

Τα Συστήματα Αυτοματισμού Γραφείου (OAS) αναφέρονται σε ένα σύνολο εργαλείων και λογισμικού που ενισχύουν την παραγωγικότητα των εργαζομένων γραφείου αυτοματοποιώντας καθημερινές εργασίες και βελτιώνοντας τη ροή πληροφοριών μέσα σε έναν οργανισμό. Ο πρωταρχικός στόχος του OAS είναι να δώσει τη δυνατότητα στους εργαζόμενους να εκτελούν τις εργασίες τους πιο αποτελεσματικά. Αυτά τα συστήματα περιλαμβάνουν μια σειρά τεχνολογιών και λειτουργιών όπως οι κάτωθι (Laudon and Laudon, 2020; Stair and Reynolds, 2017):

- Αποθήκευση και διαχείριση δεδομένων: Το πληροφοριακό σύστημα παρέχει δυνατότητες αποθήκευσης, διαχείρισης και ανάκτησης επιχειρηματικών πληροφοριών. Αυτό περιλαμβάνει βάσεις δεδομένων, αποθήκες δεδομένων και συστήματα διαχείρισης εγγράφων. Επιτρέπουν την αποτελεσματική οργάνωση και ανάκτηση ψηφιακών εγγράφων και δεδομένων, μειώνοντας τον χρόνο που δαπανάται για χειροκίνητο χειρισμό δεδομένων.
- Επεξεργασία κειμένου: Αυτή είναι μια από τις πιο βασικές και ευρέως χρησιμοποιούμενες λειτουργίες του OAS. Οι επεξεργαστές κειμένου επιτρέπουν στους χρήστες να δημιουργούν, να επεξεργάζονται και να μορφοποιούν έγγραφα. Προσφέρουν δυνατότητες όπως ορθογραφικός έλεγχος, γραμματικός έλεγχος και διάφορες επιλογές μορφοποίησης, που έχουν αντικαταστήσει την

παραδοσιακή γραφομηχανή στα περισσότερα γραφεία. Αντίστοιχα, το λογισμικό υπολογιστικών φύλλων επιτρέπει στους χρήστες να εκτελούν σύνθετους υπολογισμούς, να δημιουργούν μοντέλα δεδομένων και να αναλύουν δεδομένα. Χρησιμοποιούνται ευρέως σε εργασίες που περιλαμβάνουν χρηματοοικονομική ανάλυση, κατάρτιση προϋπολογισμού, προβλέψεις και αναφορές.

- **Συστήματα ηλεκτρονικού ταχυδρομείου:** Το ηλεκτρονικό ταχυδρομείο είναι ένα κρίσιμο στοιχείο του OAS, παρέχοντας ένα γρήγορο και αποτελεσματικό μέσο επικοινωνίας εντός και εκτός του οργανισμού. Υποστηρίζει την ανταλλαγή μηνυμάτων, αρχείων και άλλων συνημμένων, διευκολύνοντας τη γρήγορη και αποτελεσματική επικοινωνία.
- **Desktop Publishing:** Αυτό περιλαμβάνει τη δημιουργία εγγράφων με επαγγελματική διάταξη και σχεδιασμό, όπως φυλλάδια, ενημερωτικά δελτία και υλικό μάρκετινγκ. Το λογισμικό επιτραπέζιων εκδόσεων προσφέρει προηγμένες δυνατότητες σχεδίασης γραφικών και διάταξης πέρα από αυτό που είναι διαθέσιμο σε τυπικούς επεξεργαστές κειμένου.
- **Εργαλεία Προγραμματισμού:** Αυτά τα εργαλεία βοηθούν στην οργάνωση χρονοδιαγραμμάτων, συναντήσεων, συναντήσεων και χρονοδιαγραμμάτων έργων. Οι εφαρμογές ημερολογίου και τα εργαλεία διαχείρισης έργων είναι παραδείγματα που βοηθούν στην αποτελεσματική διαχείριση χρόνου και στο συντονισμό του έργου.
- **Εργαλεία επικοινωνίας και συνεργασίας:** Περιλαμβάνει διάφορα εργαλεία που υποστηρίζουν την επικοινωνία και τη συνεργασία σε πραγματικό χρόνο, όπως η ανταλλαγή άμεσων μηνυμάτων, η τηλεδιάσκεψη και οι διαδικτυακές πλατφόρμες συνεργασίας. Επιτρέπουν στις ομάδες να συνεργάζονται αποτελεσματικά, ανεξάρτητα από τη γεωγραφική θέση.
- **Συστήματα διαχείρισης βάσεων δεδομένων:** Αυτά τα συστήματα επιτρέπουν τη δημιουργία, την ενημέρωση και τη διαχείριση βάσεων δεδομένων. Είναι απαραίτητα για την αποθήκευση μεγάλων ποσοτήτων δομημένων δεδομένων και την παροχή αποτελεσματικής πρόσβασης και δυνατοτήτων ανάκτησης.

- Διαχείριση αρχείων: Το OAS περιλαμβάνει συστήματα για τη διαχείριση αρχείων και αρχείων, διασφαλίζοντας ότι τα κρίσιμα επιχειρηματικά αρχεία ελέγχονται συστηματικά, διατηρούνται και είναι προσβάσιμα.

Σε γενικές γραμμές, τα συστήματα αυτοματισμού γραφείου έχουν εξελιχθεί σημαντικά με την πρόοδο της τεχνολογίας. Τα σύγχρονα OAS συχνά ενσωματώνονται με το cloud computing, την τεχνητή νοημοσύνη και την τεχνολογία κινητής τηλεφωνίας, ενισχύοντας την προσβασιμότητα και επιτρέποντας πιο εξελιγμένες δυνατότητες ανάλυσης δεδομένων και λήψης αποφάσεων.

Αντίστοιχα, λειτουργεί και ως Σύστημα Πληροφοριών Διαχείρισης (MIS) το οποίο παίζει έναν κρίσιμο ρόλο στις επιχειρήσεις παρέχοντας στους διευθυντές τα εργαλεία και τις πληροφορίες που είναι απαραίτητες για τη λήψη αποφάσεων. Το MIS είναι μια ηλεκτρονική βάση δεδομένων οικονομικών πληροφοριών οργανωμένη και προγραμματισμένη με τέτοιο τρόπο ώστε να παράγει τακτικές αναφορές για τις λειτουργίες για κάθε επίπεδο διοίκησης μιας εταιρείας.

Έχει σχεδιαστεί για να βοηθά στον προγραμματισμό, τον έλεγχο και τις λειτουργίες λήψης αποφάσεων των μεσαίων στελεχών. Παρακάτω, θα αναλύσω τα βασικά στοιχεία, τις λειτουργίες και τα οφέλη του MIS (Laudon and Laudon, 2020). Τα βασικά στοιχεία του MIS είναι τα υλικά, το λογισμικό, τα δεδομένα, οι διαδικασίες και οι άνθρωποι (χρήστες)

Το πληροφοριακό σύστημα παρουσιάζεται στο παρακάτω διάγραμμα.

[illegible]

Όπως φαίνεται στο παραπάνω διάγραμμα, το σύστημα διαθέτει τρία switch που χρησιμεύουν για να συνδέει στο καθένα τις συσκευές ενός δικτύου μεταξύ τους, επιτρέποντάς τους να συνομιλούν ανταλλάσσοντας πακέτα δεδομένων. Τα switch μπορεί να είναι συσκευές υλικού που διαχειρίζονται φυσικά δίκτυα ή εικονικές συσκευές που βασίζονται σε λογισμικό. Λειτουργούν στο επίπεδο σύνδεσης δεδομένων ή επίπεδο 2 του μοντέλου διασύνδεσης ανοικτών συστημάτων (OSI). Τα switch είναι συνδεδεμένα μεταξύ τους μέσω Uplink Gigabit. Το πρώτο είναι συνδεδεμένο με το δεύτερο και το δεύτερο με το τρίτο.

Το **πρώτο** switch το οποίο βρίσκεται στον 3^ο όροφο συνδέεται με τα εξής, που βρίσκονται στον 3^ο όροφο :

- 1 Access Point
- 1 κάμερα ασφαλείας για τον 3^ο όροφο
- Με 20 τερματικά , σταθερούς και φορητούς υπολογιστές της εταιρίας που βρίσκονται στον 3^ο όροφο.
- Ένα CISCO SX-10 που χρησιμοποιείται για να συνδέει το γραφείο των συναντήσεων με τον CEO.
- Ένα Tendberg EX60 που είναι στο γραφείο ενός άλλου στελέχους της επιχείρησης
- Ένα CISCO Room Kit το οποίο είναι εγκατεστημένο στο γραφείο συναντήσεων

Το **δεύτερο** switch στο Mezzani floor συνδέεται με τα εξής στοιχεία που βρίσκονται στο Mezzani floor :

- 1 Access Point
- 1 κάμερα ασφαλείας για το Mezzani floor
- Με 20 τερματικά , σταθερούς και φορητούς υπολογιστές της εταιρίας.

Το **τρίτο** switch βρίσκεται στο υπόγειο της επιχείρησης και είναι αυτό στο οποίο είναι συνδεδεμένες οι περισσότερες συσκευές. Οι συσκευές που είναι συνδεδεμένες στο πρώτο switch είναι οι εξής και βρίσκονται όλες στο υπόγειο:

- CISCO SSL VPN
- 4 SERVERS που χρησιμεύουν στην παραγωγή (production). Ο ένας από αυτούς συνδέεται απευθείας με το SIP Trunk .
- 2 SERVERS υποστηρικτικοί που είναι κλειστοί
- 1 SERVERS που είναι για την ανάπτυξη (development)
- 1 SERVERS που είναι για την ανάπτυξη & παραγωγή (development & production)

- 1 κέντρο πρόσβασης που χρησιμοποιείται για την παραγωγή (Ruckus R300 Access Point Basement Lab)
- 1 ακόμη SERVER που χρησιμεύει για την παραγωγική διαδικασία ο οποίος είναι συνδεδεμένος με ένα Firewall – IDS & VPN το οποίο είναι συνδεδεμένο με ένα Fiber 100Mb το οποίο συνδέεται με το SIP Trunk που αναφέρθηκε προηγουμένως .

Το υπολογιστικό σύστημα περιλαμβάνει επίσης διαδικτυακές συνδέσεις 2 ADSL + 2 PSTN που είναι συνδεδεμένες με το FAX της επιχείρησης και ένα συναγερμό (ALARM).

5.3.2. Λειτουργίες του Συστήματος

Οι βασικές λειτουργίες ενός MIS είναι οι εξής σύμφωνα με τους O'Brien and Marakas, (2011):

- Επεξεργασία Δεδομένων:Περιλαμβάνει τη συλλογή, αποθήκευση, επεξεργασία και ανάκτηση δεδομένων.Το MIS χειρίζεται αποτελεσματικά μεγάλο όγκο δεδομένων από διάφορες πηγές.Στο συγκεκριμένο πληροφοριακό σύστημα, τα δεδομένα επεξεργάζονται από τους 7 SERVERS της εταιρίας, τους 5 που είναι για την παραγωγή, τον 1 που είναι για την ανάπτυξη και τον 1 που είναι για παραγωγή και ανάπτυξη.
- Αποθήκευση πληροφοριών:Το MIS αποθηκεύει δεδομένα με τρόπο που είναι εύκολα ανακτήσιμο και προσβάσιμο στους χρήστες όταν απαιτείται. Σε αυτό χρησιμεύουν οι SERVERS της εταιρίας που βρίσκονται στο 3^ο switch στο υπόγειο.
- Αναφορές διαχείρισης:Το MIS παρέχει τακτικές αναφορές στη διοίκηση, οι οποίες μπορεί να είναι ημερήσιες, εβδομαδιαίες ή μηνιαίες.Αυτές οι εκθέσεις βοηθούν στη λήψη αποφάσεων και στον στρατηγικό σχεδιασμό.

- Υποστήριξη αποφάσεων:Το MIS μπορεί επίσης να παρέχει πιο σύνθετα εργαλεία ανάλυσης για να βοηθήσει τους διευθυντές να λαμβάνουν αποφάσεις. Αυτό μπορεί να περιλαμβάνει προβλέψεις, προϋπολογισμούς και άλλες οικονομικές αναλύσεις.Στο συγκεκριμένο πληροφοριακό σύστημα η υποστήριξη αποφάσεων γίνεται στον τρίτο όροφο μέσω των CISCO SX-10, Tendberg EX60 και CISCO Room Kit που είναι συνδεδεμένα στο 1^ο switch.
- Διαδραστική Επεξεργασία Ερωτημάτων:Το MIS επιτρέπει στους διαχειριστές να αλληλοεπιδρούν με το σύστημα και να ζητούν συγκεκριμένες πληροφορίες ή αναλύσεις όπως απαιτείται.Αυτό επιτυγχάνεται μέσω των Switch το οποίο διαμοιράζει τις πληροφορίες από τους χρήστες προς τη διαχείριση.

5.3.3. Το Λογισμικό και τα Δεδομένα του Συστήματος

Το πληροφοριακό σύστημα περιέχει λογισμικό και δεδομένα.Στο λογισμικό συγκαταλέγονται τα προγράμματα που χρησιμοποιούνται για τη διαχείριση και την επεξεργασία πληροφοριών.Το λογισμικό MIS μπορεί να κυμαίνεται από τυπικά εργαλεία παραγωγικότητας γραφείου έως εξειδικευμένες επιχειρηματικές εφαρμογές.Τα δεδομένα είναι το πιο κρίσιμο στοιχείο, που περιλαμβάνει τη συλλογή, αποθήκευση και διαχείριση δεδομένων από διάφορες επιχειρηματικές δραστηριότητες.

Στο λογισμικό του πληροφοριακού συστήματος συγκαταλέγονται 9 συστήματα Linux, 18 Windows Software (11,10 Pro, 10 Home & 7 Pro), 1 Oracle, 11 SQL Software, 21 MS Office Packages, 14 Eset Smart Security Business Edition.

Στο hardware του πληροφοριακού συστήματος συγκαταλέγονται 3 CentOS, 13 VMWARE, 1 Dataways i-Node Server, 24 Cisco Unified Communications Services, 22 WEBEX Cloud Services, 33 PRTG Monitoring,2 FortiSIEM Platforms, 1 Evoko Application Server, 17 Windows Servers και 4 Mac OS Servers. Επίσης, 1 Router - Firewall – IDS, 1 Access – VPN, 1 Access - ISR – Cube, 7 Ethernet Switch (εκ των

οποίων τα 2 δεν είναι σε χρήση αλλά για υποστηρικτική λειτουργία, 2 Security Camera, 4 Wifi Access Point & 1 Network Printer.

5.3.4. Οι διαδικασίες και Πολιτικές του Συστήματος

Οι διαδικασίες ενός πληροφοριακού συστήματος είναι οι μέθοδοι συλλογής, επεξεργασίας, αποθήκευσης και διάδοσης πληροφοριών σε αυτό. Οι διαδικασίες διασφαλίζουν επίσης την ακρίβεια και την ασφάλεια των δεδομένων. Σύμφωνα με το ISO (ISO 27001:2013) της εταιρίας, για τη λειτουργία του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών (ΣΔΑΠ) έχουν καθοριστεί οι ακόλουθες διαδικασίες:

- 1.** Διαδικασία εξαίρεσης από τις πολιτικές του Σ.Δ.Α.Π.
- 2.** Διαδικασία εκτίμησης αντικτύπου
- 3.** Διαδικασία επιστροφής πληροφοριακών αγαθών
- 4.** Διαδικασία ασφαλής απόρριψης φορητών μέσων αποθήκευσης
- 5.** Διαδικασία εγγραφής και διαγραφής χρηστών
- 6.** Διαδικασία εκχώρησης προνομιακού δικαιώματος
- 7.** Διαδικασία εισόδου-εξόδου από τις εγκαταστάσεις της Εταιρείας
- 8.** Διαδικασία μετακίνησης περιουσιακών στοιχείων
- 9.** Διαδικασία αντιμετώπισης περιστατικών ασφαλείας
- 10.** Διαδικασία αναφοράς συμβάντων ασφαλείας πληροφοριών
- 11.** Διαδικασία αναφοράς αδυναμιών ασφαλείας πληροφοριών
- 12.** Διαδικασία αξιολόγησης και λήψης αποφάσεων συμβάντων ασφαλείας πληροφοριών
- 13.** Διαδικασία συλλογής τεκμηριακών στοιχείων

14. Διαδικασία Διαχείρισης Δικαιωμάτων Υποκειμένων & Υποδοχής παραπόνων/καταγγελιών

15. Διαδικασία Διαχείρισης Παραβίασης Δεδομένων Προσωπικού Χαρακτήρα

Επίσης, σύμφωνα με την Πολιτική Ασφάλειας Επιχειρησιακής Λειτουργίας, εκτελούνται οι κάτωθι διαδικασίες στο Πληροφοριακό Σύστημα και περιγράφονται αναλυτικά από το αντίστοιχο έγγραφο (Operations Security Policy):

1. Διαδικασίες παραγωγικής λειτουργίας και αρμοδιότητες

Αυτές περιλαμβάνουν την τεκμηρίωση εργασιών παραγωγικής λειτουργίας συστημάτων, την διαχείριση αλλαγών (Change Management) , τη διαχείριση επιχειρησιακής ικανότητας (Capacity management) και τον διαχωρισμό των development, testing και operational περιβαλλόντων

2. Διαδικασία προστασίας από κακόβουλο λογισμικό (malware) που περιλαμβάνει τους ελέγχους έναντι κακόβουλου λογισμικού.

3. Διαδικασία Καταγραφής συμβάντων και παρακολούθησης λειτουργίας (Logging and monitoring)

Αυτή η διαδικασία περιλαμβάνει την καταγραφή συμβάντων , την προστασία των αρχείων καταγραφής, το αρχείο καταγραφής διαχειριστή και χρήστη και τον συγχρονισμό ρολογιών

4. Διαδικασία ελέγχου λειτουργικού λογισμικού που περιλαμβάνει εγκαταστάσεις λογισμικών στα επιχειρησιακά συστήματα

5. Διαδικασία διαχείρισης τεχνικών ευπαθειών

Η διαδικασία αυτή περιλαμβάνει τη διαχείριση τεχνικών ευπαθειών και τους περιορισμούς στις εγκαταστάσεις λογισμικών

6. Διαδικασία ελέγχου συστημάτων πληροφορικής

Παράλληλα με τις διαδικασίες, υπάρχουν οι ακόλουθες πολιτικές στα πλαίσια του ΣΔΑΠ, σύμφωνα με το ISO 27001:2013:

- 1.** Πολιτικές Ασφάλειας Πληροφοριών
- 2.** Πολιτική Οργάνωσης της Ασφάλειας Πληροφοριών
- 3.** Πολιτική Φορητών Συσκευών και Τηλεργασίας
- 4.** Πολιτική Ασφάλειας Ανθρώπινων Πόρων
- 5.** Πολιτική Διαχείρισης Πληροφοριακών Αγαθών
- 6.** Πολιτική Ελέγχου Πρόσβασης
- 7.** Πολιτική Κρυπτογράφησης
- 8.** Πολιτική Φυσικής και Περιβαλλοντικής Ασφάλειας
- 9.** Πολιτική Ασφάλειας Επιχειρησιακής Λειτουργίας
- 10.** Πολιτική Ασφάλειας Επικοινωνιών
- 11.** Πολιτική απόκτησης, ανάπτυξης και συντήρησης Πληροφοριακών Συστημάτων
- 12.** Πολιτική Ασφαλούς Διαχείρισης Προμηθευτών
- 13.** Πολιτική Διαχείρισης Συμβάντων Ασφαλείας
- 14.** Πολιτική ασφάλειας πληροφοριών διαχείρισης επιχειρησιακής συνέχειας
- 15.** Πολιτικές Ανάκαμψης και Επιχειρησιακής Συνέχειας
- 16.** Πολιτική Συμμόρφωσης

Σύμφωνα με τις Πολιτικές Ασφάλειας Πληροφοριών (Information Security Policies), που στοχεύουν στην οργάνωση και υποστήριξη της ασφάλειας των πληροφοριών της Εταιρείας σύμφωνα με τους ισχύοντες νόμους και κανονισμούς, περιγράφονται οι

Πολιτικές Ασφάλειας Πληροφοριών και η Ανασκόπηση των πολιτικών του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών που αποτελείται από τις εξής επιμέρους πολιτικές:

1. Information security policies (η παρούσα).
2. Organization of information security.
3. Human resource security.
4. Asset management.
5. Access control.
6. Cryptography.
7. Physical and environmental security.
8. Operations security.
9. Communications security.
10. System acquisition, development, and maintenance.
11. Supplier relationships.
12. Information security incident management.
13. Information security aspects of business continuity management.
14. Compliance.

Σύμφωνα με την Οργάνωσης της Ασφάλειας Πληροφοριών (Organization of Information Security) περιγράφονται οι αντίστοιχες πολιτικές στο συγκεκριμένο έγγραφο. Στόχος της είναι η δημιουργία ενός πλαισίου διαχείρισης για την έναρξη και τον έλεγχο της εφαρμογής και της λειτουργίας της ασφάλειας των πληροφοριών εντός της Εταιρείας. Περιλαμβάνει τους Ρόλους και αρμοδιότητες Ασφάλειας Πληροφοριών, Διαχωρισμό των καθηκόντων, Επικοινωνία με τις Αρχές, Επικοινωνία με ομάδες ειδικών ενδιαφερόντων, Ασφάλεια Πληροφοριών στη Διαχείριση Έργων.

Σύμφωνα με την Πολιτική ασφάλειας πληροφοριών διαχείρισης επιχειρησιακής συνέχειας (Information Security Aspects of Business Continuity Management Policy) καθορίζονται οι εξής πολιτικές που αναλύονται περεταίρω στο συγκεκριμένο έγγραφο.

1. Εν συνεχεία εφαρμογή της ασφάλειας των πληροφοριών

Αφορά την εν συνέχεια εφαρμογή της ασφάλειας των πληροφοριών. Στόχος της ενότητας είναι διασφαλίσει την εν συνεχεία εφαρμογή της ασφάλειας των πληροφοριών στα συστήματα διαχείρισης επιχειρησιακής συνέχειας της Εταιρείας. Αποτελείται από τον Προγραμματισμό της συνέχειας εφαρμογής ασφάλειας πληροφοριών, την Εφαρμογή της συνέχειας ασφάλειας πληροφοριών και την Επαλήθευση, εξέταση και αξιολόγηση της συνέχειας της ασφάλειας των πληροφοριών (βλ. § 6.1.3)

2. Εφεδρείες

Αφορά τον καθορισμό των μέτρων για τη διασφάλιση της συνεχούς διαθεσιμότητας εγκαταστάσεων επεξεργασίας πληροφοριών για την Εταιρεία. Περιλαμβάνει τη Διαθεσιμότητα εγκαταστάσεων επεξεργασίας πληροφοριών.

Σύμφωνα με το έγγραφο Πολιτική Φυσικής & Περιβαλλοντικής Ασφάλειας (Physical and Environmental Security Policy) υπάρχουν οι κάτωθι πολιτικές που περιγράφονται αναλυτικά στο συγκεκριμένο έγγραφο.

1. Φυσική και Περιβαλλοντική Ασφάλεια

Αυτή η πολιτική περιλαμβάνει τον έλεγχο της περιμέτρου φυσικής ασφάλειας, τους ελέγχους φυσικών εισόδων, τη Διασφάλιση χώρων εργασίας και εγκαταστάσεων, την Προστασία από εξωτερικές και περιβαλλοντικές απειλές, την Εργασία σε χώρους αυξημένης ασφάλειας και την ασφάλεια στους χώρους παραλαβής και φόρτωσης.

2. Εξοπλισμός

Περιλαμβάνει τον έλεγχο της θέσης και προστασία του εξοπλισμού, την υποστήριξη βοηθητικών υποδομών, την Ασφάλεια Καλωδίωσης, τη Συντήρηση εξοπλισμού, την Κατάργηση περιουσιακών στοιχείων, την Ασφάλεια εξοπλισμού και περιουσιακών στοιχείων εκτός εγκαταστάσεων, την Ασφαλής απόρριψη ή επαναχρησιμοποίηση

εξοπλισμού, τον εξοπλισμό μη επιτηρούμενων χρηστών και την πολιτική clear desk και clear screen

Επίσης, σύμφωνα με την Πολιτική Ασφάλειας Επιχειρησιακής Λειτουργίας, υπάρχει η πολιτική Backup πληροφοριών στο Πληροφοριακό Σύστημα και περιγράφεται αναλυτικά από το αντίστοιχο έγγραφο (Operations Security Policy).

Σύμφωνα με το έγγραφο Πολιτικής Κρυπτογράφησης (Encryption Policy) εκτελούνται κρυπτογραφικοί έλεγχοι που αφορά την ορθή και αποτελεσματική χρήση της κρυπτογραφίας για την προστασία της εμπιστευτικότητας, της αυθεντικότητας και / ή της ακεραιότητας των πληροφοριών. Οι πολιτικές περιλαμβάνουν την πολιτική χρήσης κρυπτογραφικών ελέγχων και τη διαχείριση κρυπτογραφικών κλειδιών. Οι αναλυτικές περιγραφές αυτών των πολιτικών αναφέρονται στο συγκεκριμένο έγγραφο.

Ακόμη, σύμφωνα με την Οργάνωση της Ασφάλειας Πληροφοριών (Organization of Information Security) περιγράφεται η Πολιτική Οργάνωσης Ασφάλειας Πληροφοριών με στόχο τη δημιουργία ενός πλαισίου διαχείρισης για την έναρξη και τον έλεγχο της εφαρμογής και της λειτουργίας της ασφάλειας των πληροφοριών εντός της Εταιρείας. Η πολιτική αυτή αποτελείται από την Πολιτική ρόλων και αρμοδιοτήτων Ασφάλειας Πληροφοριών, από τον Διαχωρισμό των καθηκόντων, την Επικοινωνία με τις Αρχές, την Επικοινωνία με ομάδες ειδικών ενδιαφερόντων και την Ασφάλεια Πληροφοριών στη Διαχείριση Έργων.

Σύμφωνα με την Πολιτική απόκτησης, ανάπτυξης και συντήρησης Πληροφοριακών Συστημάτων (System Acquisition, Development & Maintenance Policy), υπάρχουν οι κάτωθι πολιτικές που αναλύονται εκτενώς στο αντίστοιχο έγγραφο.

1. Απαιτήσεις ασφαλείας για τα πληροφοριακά συστήματα

Αφορά τον καθορισμό των απαιτήσεων ασφαλείας για τα πληροφοριακά συστήματα. Στόχος της ενότητας είναι να διασφαλιστεί ότι η ασφάλεια των πληροφοριών αποτελεί αναπόσπαστο μέρος των πληροφοριακών συστημάτων της Εταιρείας καθ' όλη τη διάρκεια του κύκλου ζωής τους. Περιλαμβάνει την ανάλυση και Προδιαγραφές Απαιτήσεων Ασφάλειας Πληροφοριών, τη διασφάλιση Υπηρεσιών & Εφαρμογών σε Δημόσια Δίκτυα και την Προστασία ηλεκτρονικών συναλλαγών

2. Ασφάλεια στις διαδικασίες ανάπτυξης και υποστήριξης πληροφοριακών συστημάτων

Αφορά τον καθορισμό των μέτρων για τη διασφάλιση των πληροφοριών στο στάδιο της ανάπτυξης πληροφοριακών συστημάτων της Εταιρείας. Περιλαμβάνει την πολιτική ασφαλούς ανάπτυξης πληροφοριακών συστημάτων, τις διαδικασίες ελέγχου αλλαγών συστήματος, την τεχνική επισκόπηση εφαρμογών μετά από αλλαγές στα λειτουργικά συστήματα τους περιορισμούς στις αλλαγές πακέτων λογισμικού, τις αρχές μηχανικής ασφαλούς συστήματος, την Πολιτική για Ασφαλές περιβάλλον ανάπτυξης, την Πολιτική για Ανάπτυξη συστημάτων μέσω τρίτων, την Πολιτική Δοκιμής ασφαλείας συστήματος και τη Δοκιμή αποδοχής συστήματος.

Σύμφωνα με την Πολιτική Συμμόρφωσης (Compliance Policy), περιγράφονται οι ακόλουθες πολιτικές που αναλύονται περεταίρω στο αντίστοιχο έγγραφο

1. Τήρηση των νομικών και συμβατικών υποχρεώσεων

Αφορά την τήρηση των νομικών και συμβατικών υποχρεώσεων της Εταιρείας. Στόχος της ενότητας είναι διασφαλίσει την αποφυγή παραβιάσεων και παρεκκλίσεων από τις νομικές, θεσμικές, κανονιστικές και συμβατικές υποχρεώσεις της που σχετίζονται με την ασφάλεια των πληροφοριών και λοιπών απαιτήσεων ασφαλείας. Περιλαμβάνει τον προσδιορισμό της εφαρμοστέας νομοθεσίας και συμβατικών υποχρεώσεων, τα δικαιώματα πνευματικής ιδιοκτησίας, την Προστασία αρχείων, την Ιδιωτικότητα και προστασία προσωπικών δεδομένων και τις Ρυθμίσεις κρυπτογραφικών ελέγχων.

2. Αναθεωρήσεις ασφαλείας πληροφοριών

Αφορά τον καθορισμό των μέτρων για τη διασφάλιση της εφαρμογής της ασφαλείας πληροφοριών σύμφωνα με τις πολιτικές και τις οργανωτικές διαδικασίες της Εταιρείας. Περιλαμβάνει τις Ανεξάρτητες αναφορές ασφαλείας πληροφοριών, τη Συμμόρφωση με τις πολιτικές και τα πρότυπα ασφαλείας και την Επισκόπηση τεχνικής συμμόρφωσης

Σύμφωνα με την πολιτική Ελέγχου Πρόσβασης (Access Control Policy) περιγράφονται οι παρακάτω πολιτικές που αναλύονται περαιτέρω στο συγκεκριμένο έγγραφο.

1. Βασικές αρχές ελέγχου πρόσβασης

Αφορά τις επιχειρησιακές απαιτήσεις ελέγχου πρόσβασης. Στόχος της ενότητας είναι ο καθορισμός των πολιτικών και των διαδικασιών που εξασφαλίζουν τον έλεγχο και τον περιορισμό της πρόσβασης σε πληροφορίες και εγκαταστάσεις επεξεργασίας πληροφοριών. Αποτελείται από την Πολιτική ελέγχου πρόσβασης και την Πρόσβαση σε δίκτυα και δικτυακές Υπηρεσίες.

2. Διαχείριση πρόσβασης χρηστών

Αφορά τη διαχείριση πρόσβασης των χρηστών. Στόχος της ενότητας είναι η εξασφάλιση ότι οι χρήστες έχουν εξουσιοδότηση πρόσβασης σε συστήματα και υπηρεσίες καθώς και η πρόληψη μη εξουσιοδοτημένης πρόσβασης. Αποτελείται από τις πολιτικές Εγγραφής και διαγραφής χρηστών, τα Δικαιώματα και περιορισμούς πρόσβασης χρηστών, την Πολιτική Διαχείρισης Δικαιωμάτων Χρηστών, τη Διαχείριση Συνθηματικών εισόδου χρηστών, την Επισκόπηση Δικαιωμάτων χρηστών και την Αφαίρεση & μεταβολή δικαιωμάτων Χρηστών.

3. Διαχείριση Συνθηματικών χρηστών

Αυτή αφορά τις ευθύνες των χρηστών. Στόχος της ενότητας είναι να καταστούν οι χρήστες υπεύθυνοι για τη διαφύλαξη των στοιχείων ελέγχου ταυτότητας. Συνδέεται με την Πολιτική Human Resource Security και περιλαμβάνει τη χρήση των απόρρητων στοιχείων επαλήθευσης ταυτότητας.

4. Έλεγχος της πρόσβασης στα συστήματα και τις εφαρμογές

Αφορά τον έλεγχο της πρόσβασης σε συστήματα και εφαρμογές. Στόχος της ενότητας είναι η αποτροπή της μη εξουσιοδοτημένης πρόσβασης σε συστήματα και εφαρμογές.

Περιλαμβάνει τον Περιορισμό πληροφοριακών αγαθών, την Ασφάλιση διαδικασιών εισόδου στα συστήματα, τη Διαχείριση Συστημάτων Αποθήκευσης Κωδικών, τη Χρήση εργαλείων με υψηλά δικαιώματα και τον Έλεγχο πρόσβασης σε πηγαίο κώδικα (βλ. § **Error! Reference source not found.**)

Σύμφωνα με την πολιτική φορητών συσκευών & τηλεργασίας (Mobile Device & Teleworking Policy) περιγράφεται ένα πλαίσιο διαχείρισης για τη διασφάλιση της ασφάλειας της τηλεργασίας και της χρήσης φορητών συσκευών. Αποτελείται από την Πολιτική Ασφάλειας Φορητών Συσκευών και από τα δικαιώματα πνευματικής ιδιοκτησίας. Η πολιτική των φορητών συσκευών μεριμνά για την εγγραφή και διαχείριση των συσκευών, για θέματα φυσικής προστασίας, για περιορισμούς της εγκατάστασης λογισμικών, για ενημερώσεις λειτουργικών συστημάτων και εφαρμογών, για περιορισμούς σύνδεσης, για ελέγχους – περιορισμούς πρόσβασης, για την προστασία από κακόβουλα λογισμικά, για αντίγραφα ασφαλείας και αποθήκευση και για τις συνθήκες πρόσβασης χρηστών με πρακτικές BYOD.

Σύμφωνα με την Πολιτική Ασφάλειας Ανθρώπινων Πόρων (Human Resource Security Policy) προβλέπονται πολιτικές πριν, κατά τη διάρκεια και κατά περίπτωση μεταβολής της απασχόλησης. Αυτά περιλαμβάνουν τα εξής και περιγράφονται αναλυτικά στο αντίστοιχο έγγραφο:

1. Πριν την απασχόληση

Αυτή η πολιτική αναπτύσσει τα θέματα που αφορούν στη διαχείριση ανθρώπινων πόρων πριν από την απασχόληση. Στόχος της είναι να εξασφαλίσει ότι οι εργαζόμενοι και οι υπεργολάβοι κατανοούν τις ευθύνες τους και ότι είναι κατάλληλοι για τους ρόλους τους οποίους λαμβάνονται υπόψη. Επίσης, καλύπτει το τι συμβαίνει όταν τα άτομα αυτά αφήνουν ή αλλάζουν ρόλους. Περιλαμβάνει τις Ενέργειες πριν την πρόσληψη ή την ανάθεση έργου και τους Όρους και προϋποθέσεις απασχόλησης

2. Κατά τη διάρκεια της απασχόλησης

Διασφαλίζει ότι οι εργαζόμενοι και οι υπεργολάβοι γνωρίζουν και εκπληρώνουν τις ευθύνες τους όσον αφορά την ασφάλεια των πληροφοριών κατά τη διάρκεια της

απασχόλησης. Η ενότητα αυτή αποτελείται από τις Αρμοδιότητες και ευθύνες διοίκησης, την Ενημέρωση, εκπαίδευση και κατάρτιση και την Πειθαρχική αντιμετώπιση.

3. Διακοπή ή μεταβολή απασχόλησης

Αφορά τον τερματισμό και την αλλαγή καθηκόντων της απασχόλησης. Στόχος της είναι η προστασία των συμφερόντων της εταιρείας ως μέρος της διαδικασίας αλλαγής ή τερματισμού της απασχόλησης. Περιλαμβάνει τον τερματισμό ή αλλαγή των ευθυνών απασχόλησης

Σύμφωνα με την Πολιτική Ασφάλειας Επικοινωνιών (Communications Security Policy) καταγράφονται οι κάτωθι πολιτικές, οι οποίες αναλύονται στο αντίστοιχο έγγραφο.

1. Πολιτική διαχείρισης ασφάλειας δικτύου (Network security management)

Σκοπός αυτής της ενότητας είναι η διασφάλιση της προστασίας των πληροφοριών κατά τη διακίνηση μέσω των δικτύων και των υποστηρικτικών εγκαταστάσεων επεξεργασίας πληροφοριών της Εταιρείας. Αποτελείται από την Διαχείριση δικτύων , την Ασφάλεια δικτύων και δικτυακών υπηρεσιών και τον Διαχωρισμό δικτύων.

2. Πολιτικές Μεταφοράς πληροφορίας

Σκοπός αυτής της ενότητας είναι η διατήρηση της ασφάλειας των πληροφοριών που μεταφέρονται εντός της Εταιρείας ή εκτός αυτής σε τρίτους, π.χ. πελάτης, προμηθευτής ή άλλο ενδιαφερόμενο μέρος. Περιλαμβάνει τις Πολιτικές και διαδικασίες μεταφοράς πληροφοριών, τις Συμβάσεις για τη μεταφορά πληροφοριών, την Ηλεκτρονική αλληλογραφία και τις Συμβάσεις εμπιστευτικότητας ή μη αποκάλυψης.

Σύμφωνα με την Πολιτική Διαχείρισης Πληροφοριών υπάρχουν οι ακόλουθες πολιτικές που αναλύονται στο αντίστοιχο έγγραφο.

1. Ευθύνες και αρμοδιότητες για τα πληροφοριακά αγαθά

Αφορά την ευθύνη για τα πληροφοριακά αγαθά. Στόχος της ενότητας είναι ο προσδιορισμός των περιουσιακών στοιχείων της εταιρείας (assets) που εμπίπτουν στο

πεδίο εφαρμογής του συστήματος διαχείρισης και ο καθορισμός των κατάλληλων αρμοδιοτήτων προστασίας. Περιλαμβάνει το Ευρετήριο Πληροφοριακών Αγαθών, την Ιδιοκτησία Πληροφοριακών Αγαθών, την Αποδεκτή Χρήση Πληροφοριακών Αγαθών και την Επιστροφή των Πληροφοριακών Αγαθών.

2. Διαβάθμιση της πληροφορίας

Η ενότητα αυτή αφορά τη διαβάθμιση των πληροφοριών. Στόχος της είναι να εξασφαλίσει ότι οι πληροφορίες λαμβάνουν το κατάλληλο επίπεδο προστασίας, ανάλογα με τη σημασία που έχουν για την Εταιρεία και τα ενδιαφερόμενα μέρη όπως για παράδειγμα οι πελάτες. Περιλαμβάνει τη Διαβάθμιση & Ταξινόμηση της Πληροφορίας, τη Σήμανση της Εμπιστευτικότητας της Πληροφορίας, τον Χειρισμό των Πληροφοριακών Αγαθών και τη Διαβάθμιση & Ταξινόμηση της Πληροφορίας

3. Πολιτική χειρισμού των Φορητών Μέσων Αποθήκευσης

Η ενότητα αυτή αφορά το χειρισμό των μέσων. Στόχος της είναι να αποτρέψει την άνευ αδείας αποκάλυψη, τροποποίηση, αφαίρεση ή καταστροφή των πληροφοριών που αποθηκεύονται στα μέσα. Περιλαμβάνει την πολιτική διαχείρισης των αποθηκευτικών μέσων, την ασφαλής απόρριψη φορητών μέσων αποθήκευσης και τη φυσική μεταφορά φορητών μέσων αποθήκευσης.

Τέλος, σύμφωνα με την Πολιτική Διαχείρισης Συμβάντων Ασφάλειας (Security Incident Management Policy), περιγράφονται οι ακόλουθες πολιτικές που αναλύονται στο συγκεκριμένο έγγραφο. Σκοπός της ενότητας είναι να περιγράψει την πολιτική, τους κανόνες και τις κατευθυντήριες γραμμές που υιοθετεί και εφαρμόζει η Εταιρεία για τη διαχείριση των περιστατικών ασφάλειας. Οι πολιτικές που περιλαμβάνονται σε αυτό το σημείο είναι τα καθήκοντα και Διαδικασίες, η Πρόσβαση σε δίκτυα και δικτυακές Υπηρεσίες, η Αναφορά συμβάντων ασφάλειας πληροφοριών, η Αναφορά αδυναμιών ασφάλειας πληροφοριών, η Αξιολόγηση και λήψη αποφάσεων σχετικά με τα συμβάντα ασφάλειας, η Αντιμετώπιση συμβάντων ασφάλειας πληροφοριών και η Συλλογή τεκμηριωτικών (αποδεικτικών) στοιχείων.

5.3.5. Οι χρήστες του Συστήματος

Σε αυτό το τμήμα περιλαμβάνονται οι άνθρωποι της επιχείρησης, δηλαδή οι εργαζόμενοι που έχουν πρόσβαση στο πληροφοριακό σύστημα. Αυτοί οι χρήστες είναι το κλειδί για κάθε MIS. Περιλαμβάνουν όλους, από τη διοίκηση που χρησιμοποιεί τις πληροφορίες που λαμβάνονται έως τους επαγγελματίες πληροφορικής που βοηθούν στη διαχείριση και τη διατήρηση των δεδομένων και του συστήματος.

Το ΣΔΑΠ αναφέρει ότι οι υπεύθυνοι υλοποίησης είναι ο IT administrator και λοιπό τεχνικό προσωπικό IT (εσωτερικό ή εξωτερικό συνεργάτη), ο Διευθύνοντας Σύμβουλος και ο υπεύθυνος ασφάλειας πληροφοριών. Το Πληροφοριακό Σύστημα διακρίνει τέσσερις κατηγορίες χρηστών external, basic, advanced και super user. Ο External user αφορά το προσωπικό που προσλαμβάνεται για αποκλειστική απασχόληση – εκχώρηση σε πελάτη. Οι εργαζόμενοι της επιχείρησης είναι στη βαθμίδα Basic user. Οι διευθυντές της επιχείρησης είναι στη βαθμίδα advanced user και ο Διευθύνων Σύμβουλος της επιχείρησης (CEO) είναι στη βαθμίδα Super user. Το πλαίσιο αρμοδιοτήτων του κάθε χρήστη περιγράφεται στον πίνακα που ακολουθεί, παρακάτω. Όπως δείχνει ο πίνακας, ο κάθε χρήστης έχει διαφορετικές αρμοδιότητες και δικαιώματα ανάλογα με το επίπεδό του. Ο πίνακας ξεκινάει από το χαμηλότερο επίπεδο χρηστών. Το ανώτατο επίπεδο χρήστη, ο Διευθύνων Σύμβουλος της επιχείρησης (CEO) έχει πλήρη πρόσβαση σε όλα τα τμήματα του πληροφοριακού συστήματος, όπως αναφέρει το ΣΔΑΠ.

Πίνακας 1 - Δικαιώματα χρηστών πληροφοριακού συστήματος

User Profile	Assets	Δικαιώματα
External User	OneDrive	Προβολή
	CRM	Πρόσβαση
	Monday	Πρόσβαση
	ERP SoftOne	Χωρίς Πρόσβαση
	email account	Πρόσβαση
	Laptops	Πρόσβαση
	LAN	Πρόσβαση
	VPN	Πρόσβαση
	Wireless network	Πρόσβαση

	Central printers	Πρόσβαση
Basic user	One Drive	Προβολή και Επεξεργασία σε συγκεκριμένα projects
	CRM	Προβολή και Επεξεργασία σε συγκεκριμένα projects
	Monday	Προβολή και Επεξεργασία σε συγκεκριμένα projects
	ERP SoftOne	Χωρίς Πρόσβαση
	email account	Πρόσβαση
	Laptops	Πρόσβαση
	LAN	Πρόσβαση
	VPN	Πρόσβαση
	Wireless network	Πρόσβαση
	Central printers	Πρόσβαση
Advanced user	OneDrive	Προβολή και Επεξεργασία
	CRM	Προβολή και Επεξεργασία
	Monday	Προβολή και Επεξεργασία
	ERP SoftOne	Πρόσβαση
	email account	Πρόσβαση
	Laptops	Πρόσβαση
	LAN	Πρόσβαση
	VPN	Πρόσβαση
	Wireless network	Πρόσβαση
	Central printers	Πρόσβαση
Super users	All systems for administration reason	Πλήρη Πρόσβαση

5.4. Εισαγωγή δεδομένων στο Pilar

Μόλις το πρόγραμμα εγκαταστάθηκε, οι βασικές ρυθμίσεις του ακολούθησαν τις οδηγίες που έχουν δοθεί από το Πανεπιστήμιο.

Το πρώτο βήμα που θα έπρεπε να κάνουμε ήταν να εισάγουμε τα Assets της επιχείρησης. Η επιχείρηση μας παρέχει λίστα από τα Asset, το Hardware and Software Inventory, το οποίο περιέχει τις ακόλουθες πληροφορίες που αξιοποιήθηκαν για την εισαγωγή των Asset. Έτσι, ως Asset εισάγονται τα παρακάτω στοιχεία στα αντίστοιχα group και με την αντίστοιχη καταμέτρηση :

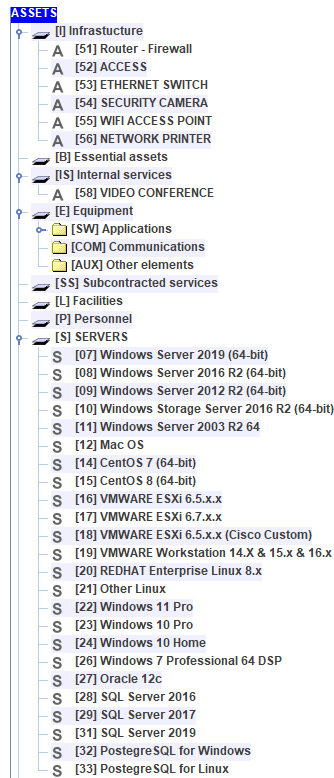
Πίνακας 2 - ASSETS της επιχείρησης

Asset Group	Asset Name	#
-------------	------------	---

Platform	Dataways i-Node Server 1.8.0.b	1
	Cisco Unified Communications Services	24
	WEBEX Cloud Services	22
	PRTG Monitoring	33
	FortiSIEM Platform	2
	Evoko Application Server	1
Servers	Windows Server 2019 (64-bit)	2
	Windows Server 2016 R2 (64-bit)	13
	Windows Server 2012 R2 (64-bit)	1
	Windows Storage Server 2016 R2 (64-bit)	1
	Mac OS	4
	CentOS 7 (64-bit)	2
	CentOS 8 (64-bit)	1
	VMWARE ESXi 6.7.x.x	2
	VMWARE ESXi 6.5.x.x (Cisco Custom)	2
	VMWARE Workstation 14.X & 15.x & 16.x	9
	REDHAT Enterprise Linux 8.x	1
	Other Linux	8
	Windows 11 Pro	2
	Windows 10 Pro	14
	Windows 10 Home	1
	Windows 7 Professional 64 DSP	1
	Oracle 12c	1
	SQL Server 2016	2
	SQL Server 2017	6
	SQL Server 2019	1
	PostgreSQL for Windows	1
	PostgreSQL for Linux	1
Εφαρμογές Γραφείου	MS-Office 365 E3 (Installed Apps)	19
	MS-Office 2016 (installed Apps)	2
	Eset Smart Security Business Edition 9.x	14
	Microsoft Product Key ID	
Τεχνικά Στοιχεία	CPU	
	RAM	
	Mouse	
	HDD Drives	
	External / Portable Disks	
Infrastructure	Router – Firewall ACCESS	

	Ethernet Switch Security camera Wifi Access Point Network Printer	
Internal Services	Video conference	

Εικόνα 2 : Εισαγωγή Asset στο Pilar



Τα πρώτα assets που εισάγονται στο σύστημα είναι οι πλατφόρμες, οι οποίες είναι στο σύνολο 81 και περιλαμβάνουν τις εξής: 24 Cisco Unified Communications Services, 22 WEBEX Cloud Services, 33 PRTG Monitorin και 2 FortiSIEM Platforms.

Σε ότι αφορά τους servers, η εταιρία κατέχει συνολικά 30 servers, και συγκεκριμένα αυτοί περιλαμβάνουν: 1 Evoko Application Server, 1 Server Dataways i-Node 1.8.0.b, 2 Windows Server 2019 (64-bit), 13 Windows Server 2016 R2 (64-bit), 1 Windows Server 2012 R2 (64-bit), 1 Windows Storage Server 2016 R2 (64-bit), 2 SQL Server 2016, 6 SQL Server 2017, 1 SQL Server 2019, 1 PostgreSQL for Windows, 1 PostgreSQL for Linux. Έχει επίσης στην κατοχή της το εξής λογισμικό: 4 Mac OS, 2 CentOS 7 (64-bit), 1 CentOS 8 (64-bit), VMWARE ESXi 6.7.x.x, VMWARE ESXi 6.5.x.x (Cisco Custom), 9 VMWARE Workstation 14.X & 15.x & 16.x, 1 REDHAT

Enterprise Linux 8.x, 8 Other Linux, 2 Windows 11 Pro, Windows 10 Pro, 1 Windows 10 Home, 1 Windows 7 Professional 64 DSP , 1 Oracle 12c.

Τέλος, σε ότι αφορά εφαρμογές γραφείου, η εταιρία έχει στην κατοχή της τα εξής assets: 19 MS-Office 365 E3 (Installed Apps), 2 MS-Office 2016 (installed Apps), 14 Eset Smart Security Business Edition 9.x

Στη συνέχεια ορίζονται οι τιμές στο valuation of domains & valuation of assets, σύμφωνα με τις πληροφορίες που λαμβάνουμε από την επιχείρηση.

Εικόνα 3: Valuation of domains

The image shows a screenshot of a web-based form titled "criteria for valuation". The form is organized into a tree structure with expandable sections. The sections and their contents are as follows:

- ☐ Recovery Time Objective:
- ☐ Personal Information:
- ☐ Legal and Regulatory Obligations:
- ☒ Security:
 - ☐ [10] is likely to lead to an exceptionally serious breach of security, or prejudice the investigation of an exceptionally serious security incident
 - ☐ [9] is likely to lead to a serious breach of security, or prejudice the investigation of a serious security incident
 - ☒ [7] is likely to lead to a major breach of security, or prejudice the investigation of a major security incident
 - ☐ [3] is likely to lead to a breach of security, or prejudice the investigation of a security incident
 - ☐ [1] could lead to a breach of security, or prejudice the investigation of a security incident
- ☐ Commercial and Economic Interests:
- ☒ Disruption of Activities:
 - ☐ [9] Is likely to cause exceptionally serious disruption of activities within an organisation and with serious impact on other organizations
 - ☐ [9] Is likely to cause a serious impact on other organizations
 - ☒ [7] Is likely to cause major disruption to activities within an organisation and with major impact on other organisations
 - ☐ [7] Is likely to impact other organizations
 - ☐ [5] Is likely to cause disruption to activities within an organisation and with some impact on other organisations
 - ☐ [5] Is likely to have some impact to other organizations
 - ☐ [3] Is likely to cause disruption to activities within an organisation
 - ☐ [1] Could cause disruption to activities within an organisation
- ☐ Public Order:
- ☐ Operations / Logistics Mission:
- ☒ Administration & Management:
 - ☐ [9] is likely to seriously impede the efficient operation of the entire organisation, or shut down the organisation
 - ☒ [7] is likely to impede the efficient operation of the entire organisation
 - ☐ [5] is likely to lead to the inefficient operation of more than one part of an organisation
 - ☐ [3] is likely to lead to the inefficient operation of one part of an organisation
 - ☐ [1] could lead to the inefficient operation of one part of an organisation
- ☐ Loss of Goodwill:
- ☐ Crime Prosecution:
- ☐ personal safety
- ☐ Classified Information:

Εικόνα 4: Valuation of domains (2)

[005] Risk Assessment								
[essential] Essential assets								
➤ A [58] VIDEO CONFERENCE	12M	13M	12M	6.7M	6.5M			6.7M
➤ S [07] Windows Server 2019 (64-bit)	10K	215K	21K	10K	2.1K	n.a.		10K
➤ S [08] Windows Server 2016 R2 (64-bit)	215K	215K	215K	10K	2.1K	n.a.		10K
➤ S [09] Windows Server 2012 R2 (64-bit)	215K	215K	215K	10K	2.1K	n.a.		10K
➤ S [10] Windows Storage Server 2016 R2 (64-bit)	215K	215K	215K	10K	2.1K	n.a.		10K
➤ S [11] Windows Server 2003 R2 64	215K	215K	215K	10K	2.1K	n.a.		10K
➤ S [12] Mac OS	215K	215K	215K	10K	2.1K	n.a.		10K
➤ S [14] CentOS 7 (64-bit)	215K	1M	215K	10K	2.1K	n.a.		10K
➤ S [15] CentOS 8 (64-bit)	215K	215K	215K	10K	2.1K	n.a.		10K
➤ S [16] VMWARE ESXi 6.5.x.x	215K	215K	215K	10K	2.1K	n.a.		10K
➤ S [17] VMWARE ESXi 6.7.x.x	215K	215K	215K	10K	2.1K	n.a.		10K
➤ S [18] VMWARE ESXi 6.5.x.x (Cisco Custom)	215K	215K	215K	10K	2.1K	n.a.		10K
➤ S [19] VMWARE Workstation 14.X & 15.x & 16.x	215K	215K	215K	10K	2.1K	n.a.		10K
➤ S [20] REDHAT Enterprise Linux 8.x	215K	215K	215K	10K	2.1K	n.a.		10K
➤ S [21] Other Linux	215K	215K	215K	10K	2.1K	n.a.		10K
➤ S [22] Windows 11 Pro	215K	215K	215K	10K	2.1K	n.a.		10K
➤ S [23] Windows 10 Pro	215K	215K	215K	10K	2.1K	n.a.		10K
➤ S [24] Windows 10 Home	215K	215K	215K	10K	2.1K	n.a.		10K
➤ S [26] Windows 7 Professional 64 DSP	215K	215K	215K	10K	2.1K	n.a.		10K
➤ S [27] Oracle 12c	215K	215K	215K	10K	2.1K	n.a.		10K
➤ S [28] SQL Server 2016	215K	215K	215K	10K	2.1K	n.a.		10K
➤ S [29] SQL Server 2017	215K	215K	215K	10K	2.1K	n.a.		10K
➤ S [31] SQL Server 2019	215K	215K	215K	10K	2.1K	n.a.		10K
➤ S [32] PostgreSQL for Windows	215K	215K	215K	10K	2.1K	n.a.		10K
➤ S [33] PostgreSQL for Linux	215K	215K	215K	10K	2.1K	n.a.		10K
➤ S [44] CPU	2.1M	2.1M	2.1M	2.1M	2.1M	n.a.		2.1M
➤ S [46] RAM	2.1M	2.1M	2.1M	2.1M	2.1M	n.a.		2.1M
➤ A [57] IP PHONE	2.1M	2.1M	2.1M	2.1M	2.1M	n.a.		2.1M
Security domains								
➤ [base] MAIN	12M	13M	12M	6.7M	6.5M			6.7M
➤ [001] CASE STUDY								

Εικόνα 5: Valuation of Assets

criteria for valuation

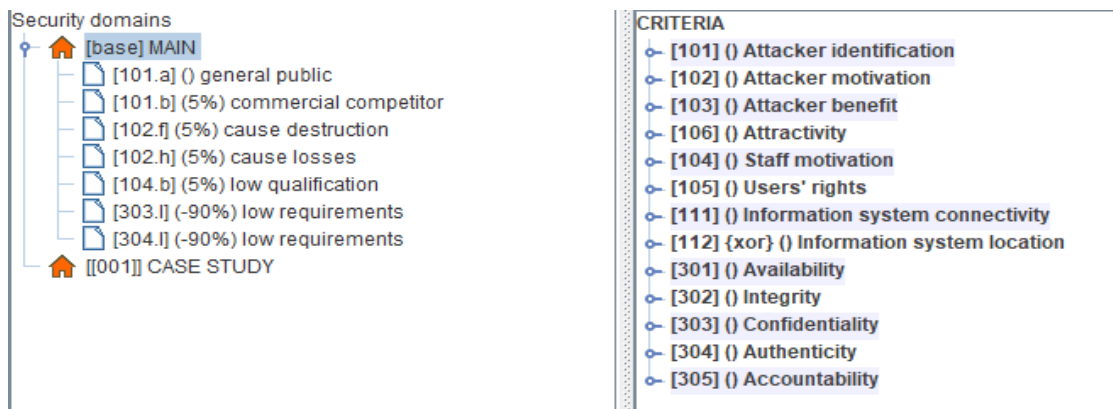
- ☐ Recovery Time Objective:
- ☐ Personal Information:
- ☐ Legal and Regulatory Obligations:
- ☒ Security:
 - ☐ [10] is likely to lead to an exceptionally serious breach of security, or prejudice the investigation of an exceptionally serious security incident
 - ☐ [9] is likely to lead to a serious breach of security, or prejudice the investigation of a serious security incident
 - ☒ [7] is likely to lead to a major breach of security, or prejudice the investigation of a major security incident
 - ☐ [3] is likely to lead to a breach of security, or prejudice the investigation of a security incident
 - ☐ [1] could lead to a breach of security, or prejudice the investigation of a security incident
- ☐ Commercial and Economic Interests:
- ☒ Disruption of Activities:
 - ☐ [9] is likely to cause exceptionally serious disruption of activities within an organisation and with serious impact on other organizations
 - ☐ [9] is likely to cause a serious impact on other organizations
 - ☒ [7] is likely to cause major disruption to activities within an organisation and with major impact on other organisations
 - ☐ [7] is likely to impact other organizations
 - ☐ [5] is likely to cause disruption to activities within an organisation and with some impact on other organisations
 - ☐ [5] is likely to have some impact to other organizations
 - ☐ [3] is likely to cause disruption to activities within an organisation
 - ☐ [1] Could cause disruption to activities within an organisation
- ☐ Public Order:
- ☐ Operations / Logistics Mission:
- ☒ Administration & Management:
 - ☐ [9] is likely to seriously impede the efficient operation of the entire organisation, or shut down the organisation
 - ☒ [7] is likely to impede the efficient operation of the entire organisation
 - ☐ [5] is likely to lead to the inefficient operation of more than one part of an organisation
 - ☐ [3] is likely to lead to the inefficient operation of one part of an organisation
 - ☐ [1] could lead to the inefficient operation of one part of an organisation
- ☐ Loss of Goodwill:
- ☐ Crime Prosecution:
- ☐ personal safety
- ☐ Classified Information:

Εικόνα 6: Valuation of Assets (2)

asset	[A]	[I]	[C]	[Auth]	
ASSETS					
[-] Infrastructure					
A [51] Router - Firewall	2.1M	215K	2.1M	2.1M	
A [52] ACCESS	215K	215K	215K	215K	
A [53] ETHERNET SWITCH	10K	10K	2.1K	10K	
A [54] SECURITY CAMERA	10K	215K	2.1K	2.1K	
A [55] WIFI ACCESS POINT	10K	10K	2.1K	10K	
A [56] NETWORK PRINTER	10K	10K	2.1K	10K	
[-] Essential assets					
[-] Internal services					
A [58] VIDEO CONFERENCE	10K	215K	2.1K	10K	
[-] Equipment					
[-] [SW] Applications					
[-] [HW] Hardware					
[-] [COM] Communications					
[-] [AUX] Other elements					
[-] [SS] Subcontracted services					
[-] [L] Facilities					
[-] [P] Personnel					
[-] [S] SERVERS					
S [07] Windows Server 2019 (64-bit)	215K	215K	215K	10K	
S [08] Windows Server 2016 R2 (64-bit)	215K	215K	215K	10K	
S [09] Windows Server 2012 R2 (64-bit)	215K	215K	215K	10K	
S [10] Windows Storage Server 2016 R2 (64-bit)	215K	215K	215K	10K	
S [11] Windows Server 2003 R2 64	215K	215K	215K	10K	
S [12] Mac OS	215K	215K	215K	10K	
S [14] CentOS 7 (64-bit)	215K	1M	215K	10K	
S [15] CentOS 8 (64-bit)	215K	215K	215K	10K	
S [16] VMWARE ESXi 6.5.x.x	215K	215K	215K	10K	
S [17] VMWARE ESXi 6.7.x.x	215K	215K	215K	10K	
S [18] VMWARE ESXi 6.5.x.x (Cisco Custom)	215K	215K	215K	10K	
S [19] VMWARE Workstation 14.X & 15.x & 16.x	215K	215K	215K	10K	
S [20] REDHAT Enterprise Linux 8.x	215K	215K	215K	10K	
S [21] Other Linux	215K	215K	215K	10K	
S [22] Windows 11 Pro	215K	215K	215K	10K	
S [23] Windows 10 Pro	215K	215K	215K	10K	
S [24] Windows 10 Home	215K	215K	215K	10K	
S [26] Windows 7 Professional 64 DSP	215K	215K	215K	10K	
S [27] Oracle 12c	215K	215K	215K	10K	
S [28] SQL Server 2016	215K	215K	215K	10K	
S [29] SQL Server 2017	215K	215K	215K	10K	
S [31] SQL Server 2019	215K	215K	215K	10K	
S [32] PostgreSQL for Windows	215K	215K	215K	10K	
S [33] PostgreSQL for Linux	215K	215K	215K	10K	
[-] [EF] Εφαρμογές - Grafeioi					
A [37] MS-Office 365 E3 (Installed Apps)	215K	215K	215K	10K	
A [38] MS-Office 2016 (Installed Apps)	215K	215K	215K	10K	
A [42] Eset Smart Security Business Edition 9.x	215K	215K	215K	10K	
A [43] Microsoft Product Key ID	215K	215K	215K	10K	
[-] [T] Technical					
Id: 1AAT1CD11	2.1M	2.1M	2.1M	2.1M	

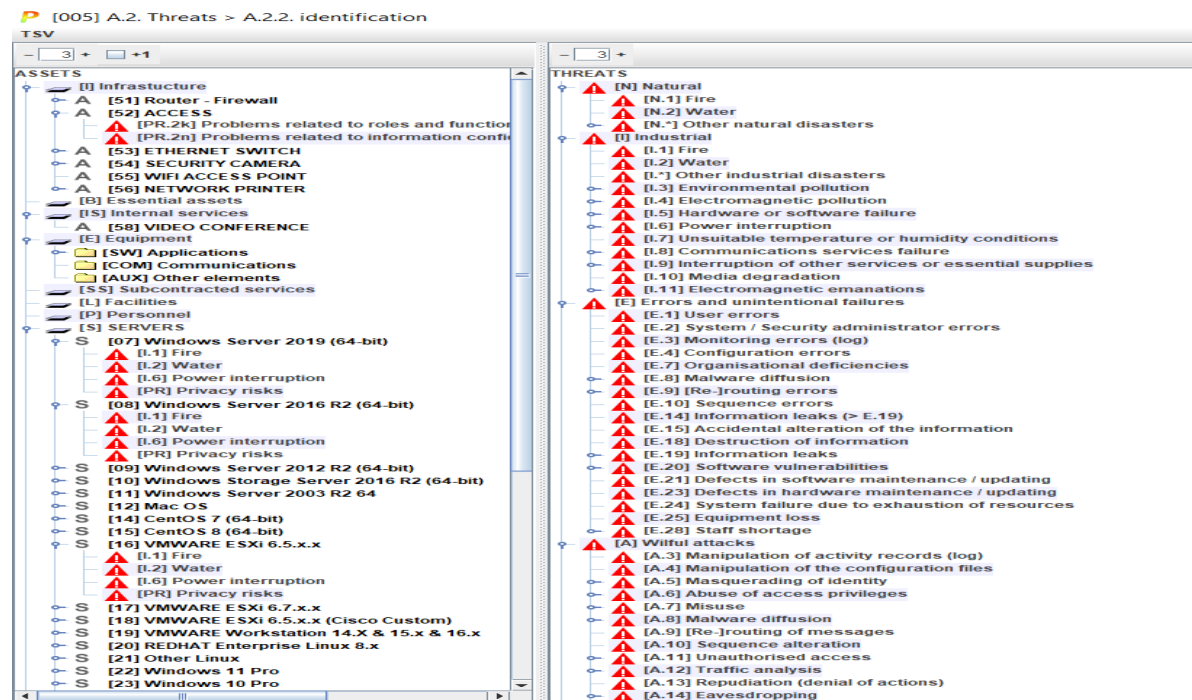
Στη συνέχεια εισάγονται οι πιθανές κατηγορίες των απειλών που δέχεται το σύστημα, που προκύπτουν από την ανάλυση των πιθανών κινδύνων (Risk Assessment) που μας έχει δοθεί. Αυτό γίνεται από την κατηγορία threats, ακολουθώντας τις οδηγίες του Πανεπιστημίου.

Εικόνα 7: Threats – security domains



Στη συνέχεια εισάγονται λεπτομερώς, οι απειλές που δέχονται αυτά τα assets, αξιοποιώντας με λεπτομέρειες τις πληροφορίες που έχει δώσει η επιχείρηση. Η παρακάτω εικόνα περιέχει μονάχα κάποια παραδείγματα από τις απειλές.

Εικόνα 8: Threats identification



Στη συνέχεια προχωράμε στον ορισμό του valuation, για αυτές τις απειλές ως πιθανότητα σύμφωνα με τις πληροφορίες που μας παρέχονται από την επιχείρηση. Ο υπολογισμός του επιπέδου του εκάστοτε κινδύνου, υπολογίζεται με πολλαπλασιασμό της πιθανότητας – probability (P) να συμβεί, με την σοβαρότητα – significance (S) των επιπτώσεων, στη λειτουργία της.

Εικόνα 9: Threats valuation

[005] A.2. Threats > A.2.3. valuation

Edit Export Import TSV

	asset	co...	frequency	[A]	[I]	[C]	[Auth]
ASSETS							
Infrastructure							
A [51] Router - Firewall				10%	10%	10%	10%
▲ [PR.2k] Problems related to roles and functions of the organization's person	(*)	1	10%	10%	10%	10%	10%
▲ [PR.2n] Problems related to information confidentiality	(*)	1	10%	10%	10%	10%	10%
A [52] ACCESS				10%	10%	10%	10%
▲ [PR.2k] Problems related to roles and functions of the organization's person	(*)	1	10%	10%	10%	10%	10%
▲ [PR.2n] Problems related to information confidentiality	(*)	1	10%	10%	10%	10%	10%
A [53] ETHERNET SWITCH				10%	10%	10%	10%
▲ [PR.2k] Problems related to roles and functions of the organization's person	(*)	1	10%	10%	10%	10%	10%
▲ [PR.2n] Problems related to information confidentiality	(*)	1	10%	10%	10%	10%	10%
A [54] SECURITY CAMERA				10%	10%	10%	10%
▲ [PR.2k] Problems related to roles and functions of the organization's person	(*)	1	10%	10%	10%	10%	10%
▲ [PR.2n] Problems related to information confidentiality	(*)	1	10%	10%	10%	10%	10%
A [55] WIFI ACCESS POINT				10%	10%	10%	10%
▲ [PR.2k] Problems related to roles and functions of the organization's person	(*)	1	10%	10%	10%	10%	10%
▲ [PR.2n] Problems related to information confidentiality	(*)	1	10%	10%	10%	10%	10%
A [56] NETWORK PRINTER				10%	10%	10%	10%
▲ [PR.2k] Problems related to roles and functions of the organization's person	(*)	1	10%	10%	10%	10%	10%
▲ [PR.2n] Problems related to information confidentiality	(*)	1	10%	10%	10%	10%	10%
[B] Essential assets							
[I5] Internal services							
A [58] VIDEO CONFERENCE							
[E] Equipment							
[SW] Applications							
[COM] Communications							
[AUX] Other elements							
[S5] Subcontracted services							
[I1] Facilities							
[P] Personnel							
[S] SERVERS							
S [07] Windows Server 2019 (64-bit)				50%	50%	50%	50%
▲ [L1] Fire	(*)	0.5	1%	1%	1%	1%	1%
▲ [L2] Water	(*)	0.5	1%	1%	1%	1%	1%
▲ [L6] Power interruption	(*)	1	10%	10%	10%	10%	10%
▲ [PR] Privacy risks	(*)	1	50%	50%	50%	50%	50%
S [08] Windows Server 2016 R2 (64-bit)				50%	50%	50%	50%
▲ [L1] Fire	(*)	0.5	1%	1%	1%	1%	1%
▲ [L2] Water	(*)	0.5	1%	1%	1%	1%	1%
▲ [L6] Power interruption	(*)	1	10%	10%	10%	10%	10%
▲ [PR] Privacy risks	(*)	1	50%	50%	50%	50%	50%
S [09] Windows Server 2012 R2 (64-bit)				50%	50%	50%	50%
▲ [L1] Fire	(*)	0.5	1%	1%	1%	1%	1%
▲ [L2] Water	(*)	0.5	1%	1%	1%	1%	1%
▲ [L6] Power interruption	(*)	1	10%	10%	10%	10%	10%
▲ [PR] Privacy risks	(*)	1	50%	50%	50%	50%	50%
S [10] Windows Storage Server 2016 R2 (64-bit)				50%	50%	50%	50%
▲ [L1] Fire	(*)	0.5	1%	1%	1%	1%	1%
▲ [L2] Water	(*)	0.5	1%	1%	1%	1%	1%
▲ [L6] Power interruption	(*)	1	10%	10%	10%	10%	10%
▲ [PR] Privacy risks	(*)	1	50%	50%	50%	50%	50%
S [11] Windows Server 2003 R2 64				50%	50%	50%	50%
▲ [L1] Fire	(*)	0.5	1%	1%	1%	1%	1%

Στη συνέχεια αξιολογούνται οι φάσεις των απειλών από την επιλογή A.3.1. Valuation of phases, η οποία παρουσιάζεται στον Πίνακα 10 που ακολουθεί.

Εικόνα 10: Threats valuation of phases

[005] A.3. Technical and organi ... > A.3.1. valuation (phases)

Edit Expand View Export Import Statistics

base MAIN				Information sources							
	aspect	top	recommend...	safeguard	doubts	source	applies	comment	current	target	PLAR
				SAFEGUARDS					L1	L4	L2-L4
	M	EL		▲ [IA] Identification and authentication	2				L1	L4	n.a.
	T	EL		▲ [AC] Logical access control					L1	L4	n.a.
	M	PR	6	▲ [D] Protection of Data / Information					L1	L4	L2-L4
	M	EL		▲ [K] Protecting cryptographic keys					L1	L4	n.a.
	M	PR	3	▲ [S] Protection of Services					L1	L4	L3
	M	PR	6	▲ [SW] Protection of Software					L1	L4	L2-L4
	M	PR	5	▲ [HW] Protection of Hardware					L1	L4	L2-L3
	M	PR		▲ [COM] Protection of Communications					L1	L4	n.a.
	M	PR		▲ [IP] Logical border protection system					L1	L4	n.a.
	M	PR	6	▲ [MP] Protection of Media					L1	L4	L2-L4
	M	PR	5	▲ [AUX] Auxiliary Means					L1	L4	L2-L3
	PHY	EL	6	▲ [PPE] Physical protection of equipment					L1	L4	L3-L4
	PHY	PR		▲ [LI] Protection of the installations					L1	L4	n.a.
	PHY	EL		▲ [PPS] Physical Perimeter Protection					L1	L4	n.a.
	PER	PR		▲ [PS] Personnel					L1	L4	n.a.
	M	PR		▲ [PDS] Potentially dangerous services					L1	L4	n.a.
	M	CR	6	▲ [IRM] Incident management (ICT)					L1	L4	L2-L4
	T	PR	7	▲ [tools] Security tools					L1	L4	L3-L4
	M	CR		▲ [V] Vulnerability management					L1	L4	n.a.
	T	MN		▲ [A] Logging and audit					L1	L4	n.a.
	M	RC	5	▲ [BC] Business continuity (contingency)					L1	L4	L2-L3
	M	AD	5	▲ [G] Organisation					L1	L4	L2-L3
	M	AD		▲ [E] External Relations					L1	L4	n.a.

Τέλος, εισάγεται το αντίκτυπο – impact στη λειτουργία της επιχείρησης και τα αντίστοιχα risks.

Εικόνα 11: Impact

[005] A.5.1. Accumulated values > A.5.1.1. impact									
View Export									
potential		current	target	PILAR					
asset					[A]	[I]	[C]	[Auth]	[Acc]
ASSETS									
[B] Infrastructure					1.2E7	1.26E7	1.2E7	7190000.0	0.0
[A] [51] Router - Firewall					12M	13M	7.2M	0.0	0.0
[A] [52] ACCESS					2.8M	2.6M	2.8M	1.8M	0.0
[A] [53] ETHERNET SWITCH					2.4M	2.6M	2.4M	1.4M	0.0
[A] [54] SECURITY CAMERA					2.3M	2.5M	2.3M	1.3M	0.0
[A] [56] NETWORK PRINTER					2.3M	2.6M	2.3M	1.3M	0.0
[B] Essential assets					2.3M	2.5M	2.3M	1.3M	0.0
[B5] Internal services									
[E] Equipment									
[S5] Subcontracted services									
[U3] facilities									
[P] Personnel									
[S] SERVERS					171M	179M	171M	101M	0.0
[S] [07] Windows Server 2019 (64-bit)					7.2M	7.8M	7.2M	4.2M	0.0
[S] [08] Windows Server 2016 R2 (64-bit)					7.2M	7.8M	7.2M	4.2M	0.0
[S] [09] Windows Server 2012 R2 (64-bit)					7.2M	7.8M	7.2M	4.2M	0.0
[S] [10] Windows Storage Server 2016 R2 (64-bit)					7.2M	7.8M	7.2M	4.2M	0.0
[S] [11] Windows Server 2003 R2 64					7.2M	7.8M	7.2M	4.2M	0.0
[S] [12] Mac OS					7.2M	7.8M	7.2M	4.2M	0.0
[S] [14] CentOS 7 (64-bit)					7.2M	7.8M	7.2M	4.2M	0.0
[S] [15] CentOS 8 (64-bit)					7.2M	7.8M	7.2M	4.2M	0.0
[S] [16] VMWARE ESXi 6.5.x.x					7.2M	7.8M	7.2M	4.2M	0.0
[S] [17] VMWARE ESXi 6.7.x.x					7.2M	7.8M	7.2M	4.2M	0.0
[S] [18] VMWARE ESXi 6.5.x.x (Cisco Custom)					7.2M	7.8M	7.2M	4.2M	0.0
[S] [19] VMWARE Workstation 14.X & 15.x & 16.x					7.2M	7.8M	7.2M	4.2M	0.0
[S] [20] REDHAT Enterprise Linux 8.x					7.2M	7.8M	7.2M	4.2M	0.0
[S] [21] Other Linux					7.2M	7.8M	7.2M	4.2M	0.0
[S] [22] Windows 11 Pro					7.2M	7.8M	7.2M	4.2M	0.0
[S] [23] Windows 10 Pro					7.2M	7.8M	7.2M	4.2M	0.0
[S] [24] Windows 10 Home					7.2M	7.8M	7.2M	4.2M	0.0
[S] [26] Windows 7 Professional 64 DSP					7.2M	7.8M	7.2M	4.2M	0.0
[S] [27] Oracle 12c					7.2M	7.8M	7.2M	4.2M	0.0
[S] [28] SQL Server 2016					7.2M	7.8M	7.2M	4.2M	0.0
[S] [29] SQL Server 2017					7.2M	7.8M	7.2M	4.2M	0

Εικόνα 12: Risk

P [005] A.5.1. Accumulated values > A.5.1.2. risk

ViewExport

potential	current	target	PILAR						
				asset	[A]	[I]	[C]	[Auth]	
				ASSETS	1.2E7	1.26E7	1.2E7	7190000.0	
				[I] Infrastructure	12M	13M	12M	7.2M	
				[A] [51] Router - Firewall	2.8M	2.6M	2.8M	1.8M	
				⚠ [PR.2k] Problems related to roles and functions of the organization's personnel	1.4M	1.3M	1.4M	885K	
				⚠ [PR.2n] Problems related to information confidentiality	1.4M	1.3M	1.4M	885K	
				[A] [52] ACCESS	2.4M	2.6M	2.4M	1.4M	
				⚠ [PR.2k] Problems related to roles and functions of the organization's personnel	1.2M	1.3M	1.2M	692K	
				⚠ [PR.2n] Problems related to information confidentiality	1.2M	1.3M	1.2M	692K	
				[A] [53] ETHERNET SWITCH	2.3M	2.5M	2.3M	1.3M	
				⚠ [PR.2k] Problems related to roles and functions of the organization's personnel	1.2M	1.3M	1.2M	671K	
				⚠ [PR.2n] Problems related to information confidentiality	1.2M	1.3M	1.2M	671K	
				[A] [54] SECURITY CAMERA	2.3M	2.6M	2.3M	1.3M	
				⚠ [PR.2k] Problems related to roles and functions of the organization's personnel	1.2M	1.3M	1.2M	671K	
				⚠ [PR.2n] Problems related to information confidentiality	1.2M	1.3M	1.2M	671K	
				[A] [56] NETWORK PRINTER	2.3M	2.5M	2.3M	1.3M	
				⚠ [PR.2k] Problems related to roles and functions of the organization's personnel	1.2M	1.3M	1.2M	671K	
				⚠ [PR.2n] Problems related to information confidentiality	1.2M	1.3M	1.2M	671K	
				[B] Essential assets					
				[IS] Internal services					
				[E] Equipment					
				[SS] Subcontracted services					
				[L] Facilities					
				[P] Personnel					
				[S] SERVERS	169M	179M	169M	98M	
				[S] [07] Windows Server 2019 (64-bit)	7.1M	7.7M	7.1M	4.1M	
				⚠ [I.1] Fire	58K	63K	58K	34K	
				⚠ [I.2] Water	58K	63K	58K	34K	
				⚠ [I.6] Power interruption	1.2M	1.3M	1.2M	671K	
				⚠ [PR] Privacy risks	5.8M	6.3M	5.8M	3.4M	
				[S] [08] Windows Server 2016 R2 (64-bit)	7.1M	7.7M	7.1M	4.1M	
				⚠ [I.1] Fire	58K	63K	58K	34K	
				⚠ [I.2] Water	58K	63K	58K	34K	
				⚠ [I.6] Power interruption	1.2M	1.3M	1.2M	671K	
				⚠ [PR] Privacy risks	5.8M	6.3M	5.8M	3.4M	
				[S] [09] Windows Server 2012 R2 (64-bit)	7.1M	7.7M	7.1M	4.1M	
				⚠ [I.1] Fire	58K	63K	58K	34K	
				⚠ [I.2] Water	58K	63K	58K	34K	
				⚠ [I.6] Power interruption	1.2M	1.3M	1.2M	671K	
				⚠ [PR] Privacy risks	5.8M	6.3M	5.8M	3.4M	
				[S] [10] Windows Storage Server 2016 R2 (64-bit)	7.1M	7.7M	7.1M	4.1M	
				⚠ [I.1] Fire	58K	63K	58K	34K	
				⚠ [I.2] Water	58K	63K	58K	34K	
				⚠ [I.6] Power interruption	1.2M	1.3M	1.2M	671K	
				⚠ [PR] Privacy risks	5.8M	6.3M	5.8M	3.4M	
				[S] [11] Windows Server 2003 R2 64	7.1M	7.7M	7.1M	4.1M	
				⚠ [I.1] Fire	58K	63K	58K	34K	
				⚠ [I.2] Water	58K	63K	58K	34K	
				⚠ [I.6] Power interruption	1.2M	1.3M	1.2M	671K	
				⚠ [PR] Privacy risks	5.8M	6.3M	5.8M	3.4M	
				[S] [12] Mac OS	7.1M	7.7M	7.1M	4.1M	
				⚠ [I.1] Fire	58K	63K	58K	34K	
				⚠ [I.2] Water	58K	63K	58K	34K	
				⚠ [I.6] Power interruption	1.2M	1.3M	1.2M	671K	
				⚠ [PR] Privacy risks	5.8M	6.3M	5.8M	3.4M	

Οι κίνδυνοι που προκύπτουν είναι αυτοί που σχετίζονται με το δίκτυο, την ασφάλεια και οι λοιποί κίνδυνοι. Οι σχετιζόμενοι με το δίκτυο είναι η αυξημένη κίνηση σε καθημερινή βάση 6-8 το απόγευμα, ο αυξημένος κίνδυνος (alarm) στις 2 ΜΜ και αυξημένο φόρτο εργασίας στις 10-12 ΠΜ. Ακόμη σημαντικός κίνδυνος είναι η Επιτρεπόμενη επισκεψιμότητα από τη λίστα IP Malware του FortiGuard, η σύνδεση μέσω VPN εκτός της χώρας και η αντιγραφή σημαντικού όγκου δεδομένων εκτός της χώρας.

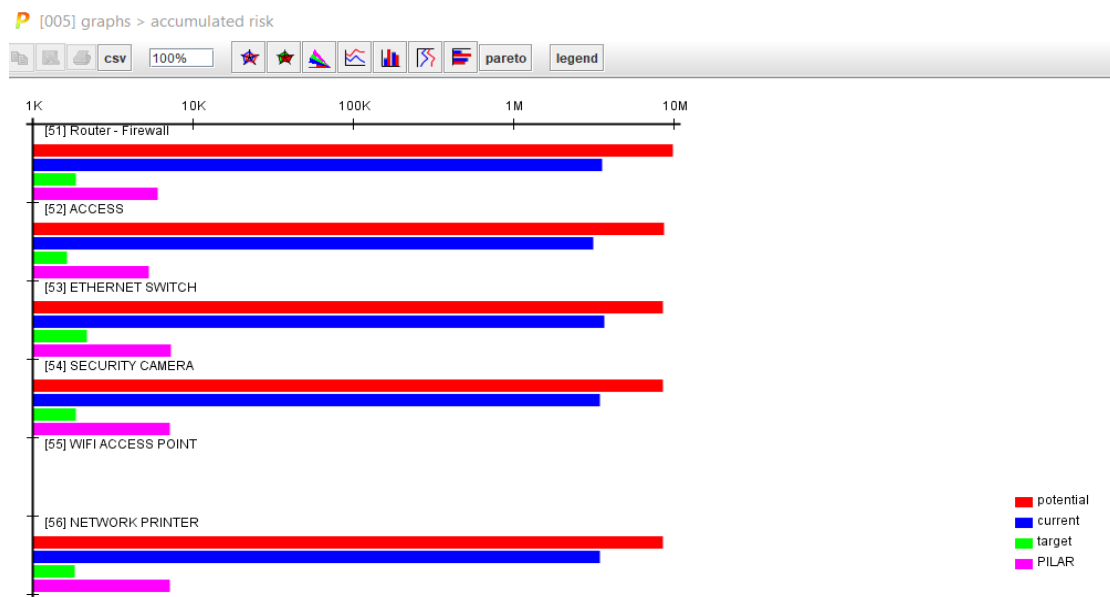
Οι κίνδυνοι σχετικά με την ασφάλεια, κίνδυνο αποτελεί η προσωρινή αποθήκευση των κωδικών πρόσβασης, η μη κοινοποίηση των οδηγιών χρήσης mobile devices στους εργαζομένους, η μη συστηματική χρήση VPN από εργαζομένους όταν εισέρχονται στο δίκτυο, η μη καταστροφή εγγράφων, η εμπιστευτικότητα των πληροφοριών, ο διαμοιρασμός και διαρροή κωδικών πρόσβασης οι ανεπαρκείς έλεγχοι για φυσική ασφάλεια και η διατήρηση πληροφοριών μετά την αποσύνδεση χρηστών. Επίσης ορισμένος εξοπλισμός χρίζει αντικατάστασης γιατί δημιουργούνται προβλήματα.

Σε ότι αφορά τους λοιπούς κινδύνους, με πιο χαμηλή πιθανότητα να συμβούν, περιλαμβάνεται ο κίνδυνος πλημμύρας και ο κίνδυνος πυρκαγιάς και η έλλειψη σε εναλλακτικά μέσα παροχής ενέργειας.

5.5. Συζήτηση αποτελεσμάτων ανάλυσης επικινδυνότητας

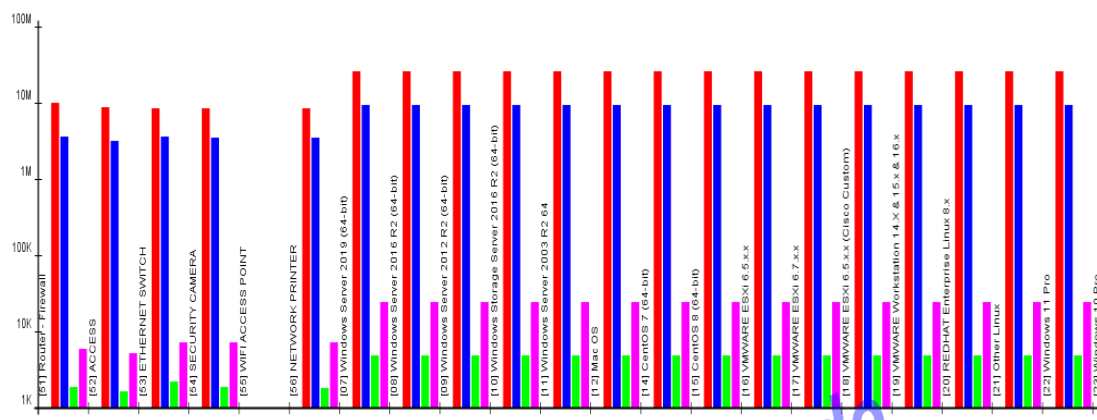
Σε αυτό το τμήμα της υλοποίησης παρουσιάζονται τα αποτελέσματα του Pilar. Αρχικά παρουσιάζονται τα ρίσκα και στη συνέχεια οι απειλές. Στην πρώτη εικόνα παρατηρούνται τα ρίσκα για το asset group -> infrastructure.

Εικόνα 13: Infrastructure risk

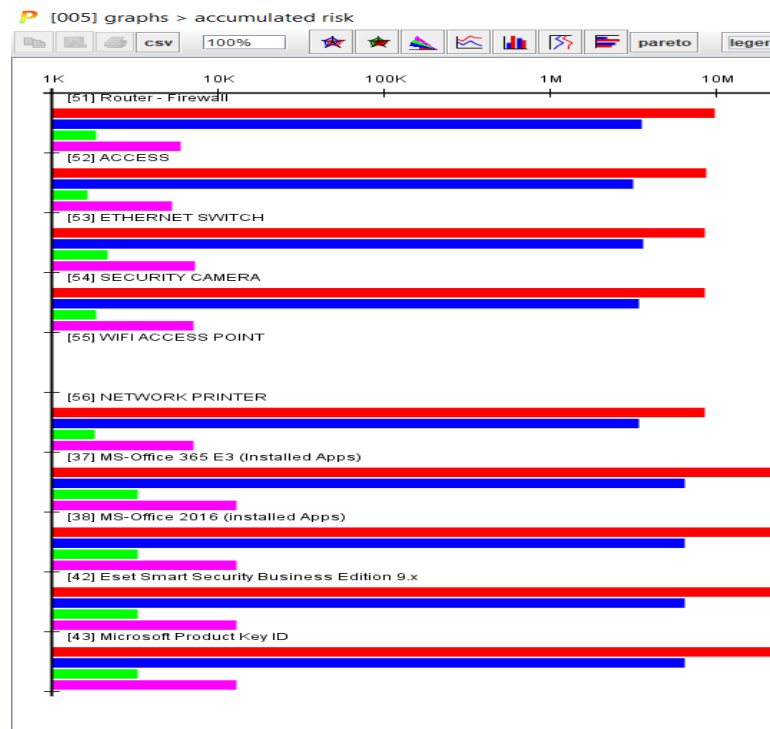


Στη συνέχεια παρουσιάζεται η ανάλυση για τους Servers, για τις εφαρμογές γραφείου, για το τεχνικό κομμάτι (technical) και για τις platforms που παρουσιάζονται στους πίνακες που ακολουθούν. Στο τέλος διενεργείται ανάλυση για το συνολικό ρίσκο ανά διάσταση

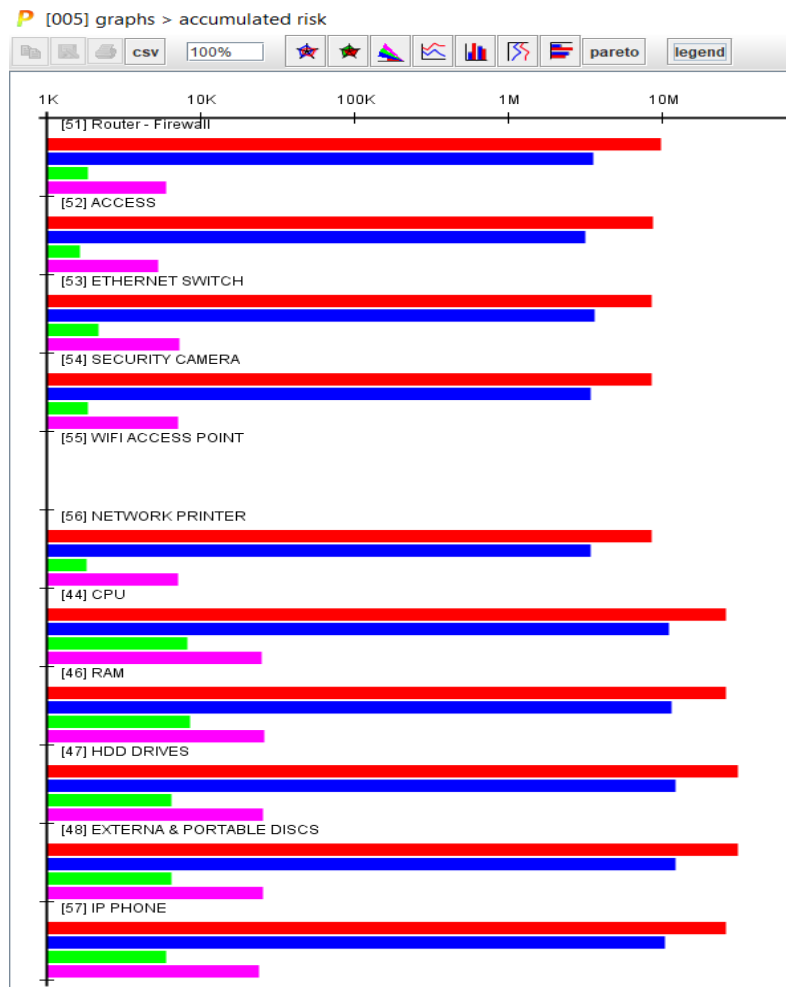
Εικόνα 14: Servers' risks



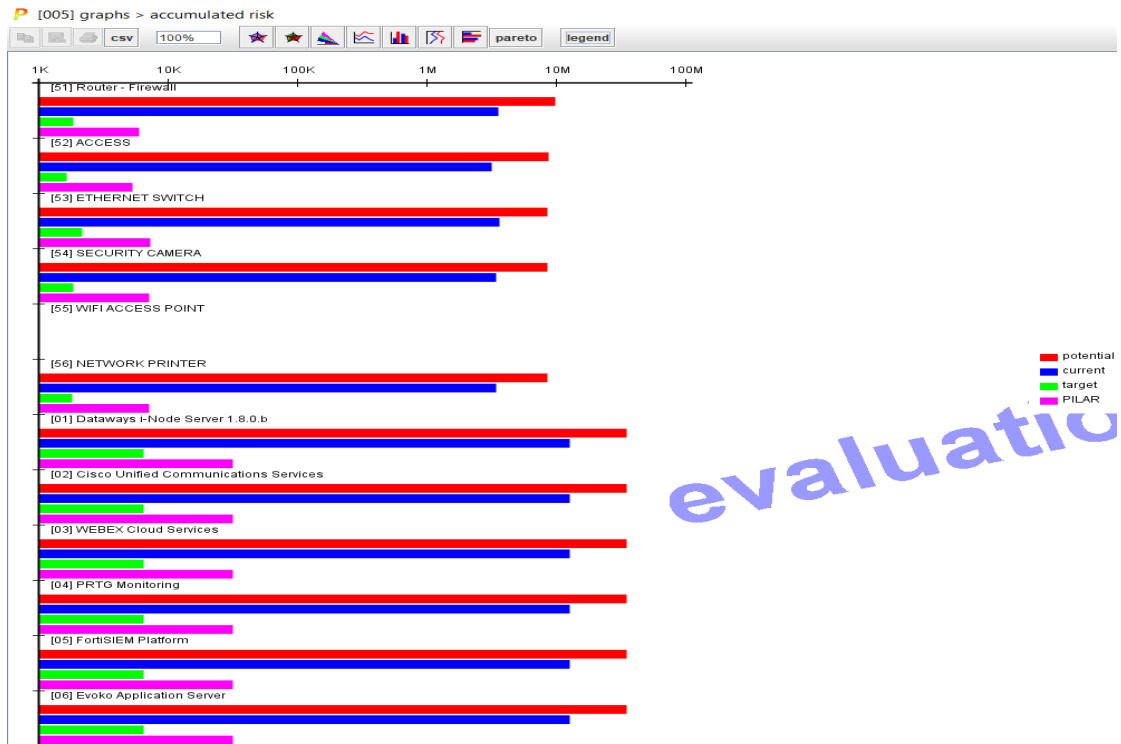
Εικόνα 15: Εφαρμογές γραφείου risk



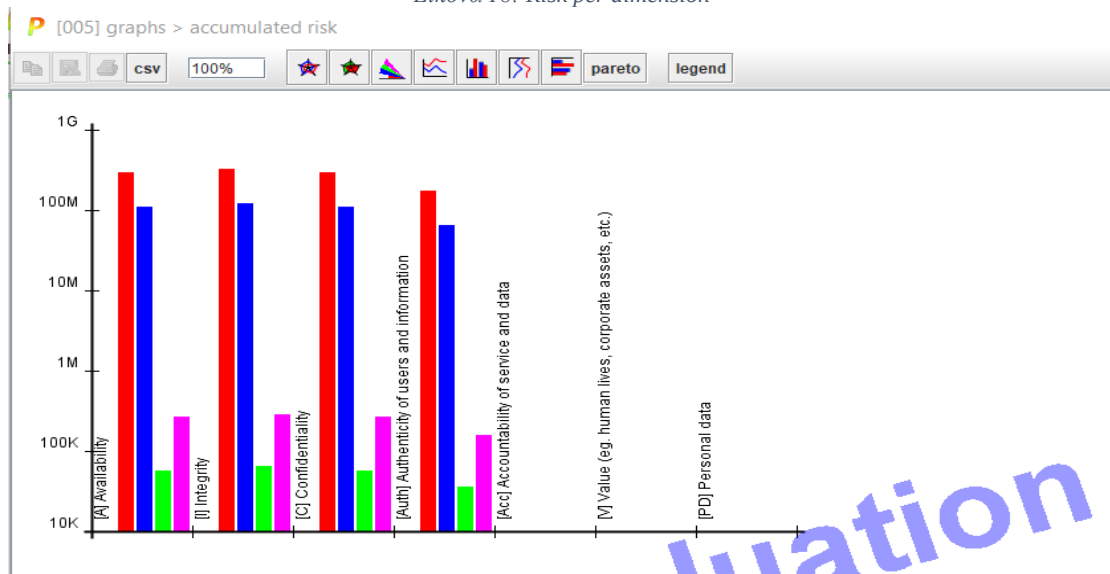
Εικόνα 16: Technical risk



Εικόνα 17: Platform risk



Εικόνα 18: Risk per dimension



Τα ευρήματα δείχνουν ότι υπάρχουν τρεις βασικές κατηγορίες κινδύνων. Οι εξωτερικοί που σχετίζονται με το δίκτυο, οι σχετιζόμενοι με την ασφάλεια ως εσωτερικοί που προκύπτουν από λανθασμένες κινήσεις και τέλος οι λοιποί κίνδυνοι.

Αναφορικά με τους πρώτους, η ανάλυση δείχνει ότι προκύπτει αυξημένη κίνηση σε καθημερινή βάση 6-8 το απόγευμα. Ακόμη, υπάρχει αυξημένος κίνδυνος (alarm) στις 2

MM και αυξημένο φόρτο εργασίας στις 10-12 ΠΜ. Ως εκ τούτου προκύπτει και μειωμένη χωρητικότητα στη μνήμη στις 12ΠΜ και αυξημένη κίνηση στο δίκτυο την ίδια ώρα. Η μελέτη δείχνει ακόμη ότι σημαντικός κίνδυνος είναι και η Επιτρεπόμενη επισκεψιμότητα από τη λίστα IP Malware του FortiGuard, το οποίο θα πρέπει να προσεχτεί δεόντως. Τα στοιχεία που μας δόθηκαν έδειξαν ότι υπήρξε επιτυχής σύνδεση μέσω VPN εκτός της χώρας και παράλληλα υπήρξε αντιγραφή σημαντικού όγκου δεδομένων εκτός της χώρας. Το τείχος προστασίας (firewall) σταμάτησε κάποιες τέτοιες προσπάθειες εισόδου. Σε μια περίπτωση τα αιτήματα σύνδεσης ήταν αυξημένα και το τείχος προστασίας αναγκάστηκε να λειτουργήσει σε μεγάλο βαθμό. Καταλήγοντας, το δίκτυο σε κάποιο βαθμό παραμένει χωρίς προστασία ενώ παράλληλα υπάρχουν σημεία χωρίς έλεγχο του δικτύου. Η γενική διαπίστωση είναι ότι υπάρχει σημαντικός φόρτος εργασίας για συγκεκριμένες ώρες που χρίζει προσοχής.

Σε σχέση με το προσωπικό και τις εσωτερικές λειτουργίες παρουσιάστηκαν ακόμη κάποιοι κίνδυνοι που χρίζουν άμεσων ενεργειών. Διαπιστώθηκε ότι σε κάποιες περιπτώσεις συμβαίνει προσωρινή αποθήκευση των κωδικών πρόσβασης, ενώ τα υπεύθυνα για την ασφάλεια στελέχη δεν κοινοποιούν τις οδηγίες χρήσης mobile devices στους εργαζομένους. Το VPN δεν χρησιμοποιείται πάντοτε από τους εργαζόμενους όταν εισέρχονται στο δίκτυο. Σε σχέση με την καταστροφή εγγράφων, υπάρχουν ακόμη κάποια έγγραφα σε γραφεία χωρίς να έχουν καταστραφεί. Το firewall δε λειτουργεί στην εντέλεια και υπάρχουν θέματα με τη λήψη κακόβουλου λογισμικού. Θέματα υπάρχουν ακόμη για την εμπιστευτικότητα των πληροφοριών, για τη χρήση του ηλεκτρονικού συστήματος επικοινωνίας και τη διαρροή εμπιστευτικών πληροφοριών. Διαπιστώθηκε ακόμη διαμοιρασμός και διαρροή κωδικών πρόσβασης ανάμεσα σε εργαζόμενους διαφορετικών βαθμίδων. Το σύστημα δεν διαθέτει ισχυρό έλεγχο ταυτότητας του χρήστη που εισέρχεται στο σύστημα, σύστημα αναγνώρισης και πιστοποίησης ταυτότητας. Συνεπώς, διαπιστώνονται ανεπαρκείς διαδικασίες και τεχνολογίες για την αποτροπή αντιγραφής ευαίσθητων δεδομένων. Ακόμη, δεν παρέχονται προστασίες για κινητό εξοπλισμό, δεν υπάρχουν επαρκείς έλεγχοι για φυσική ασφάλεια και δεν αφαιρούνται τα δικαιώματα πρόσβασης κατά τη λήξη της απασχόλησης των εργαζομένων, στο σχόλασμά τους. Συνεπώς κάποιος μπορεί να εισέλθει από άλλη τοποθεσία. Το δίκτυο δεν ελέγχεται καλά, δεν υπάρχουν οι σωστές διαδικασίες ταυτοποίησης, αλλά το πρόβλημα διογκώνεται διότι το προσωπικό δεν λαμβάνει

εκπαίδευση ευαισθητοποίησης σχετικά με την ασφάλεια. Τέλος, χρειάζεται ορισμένη αντικατάσταση εξοπλισμού που πλέον αδυνατεί να ανταπεξέλθει στο σκοπό του και εγκατάσταση νέου και σύγχρονου εξοπλισμού που θα ανταποκρίνεται πληρέστερα.

Η τρίτη κατηγορία κινδύνων περιλαμβάνει κινδύνους που δεν υπάρχει μεγάλο επίπεδο πιθανότητας να συμβούν και άρα η επικινδυνότητά τους είναι περιορισμένη. Αυτοί είναι ο κίνδυνος πλημμύρας και ο κίνδυνος πυρκαγιάς, ο οποίος είναι ελαφρώς αυξημένος σε σχέση με τον προηγούμενο καθώς διαπιστώνεται σχετική έλλειψη μέσων πυρόσβεσης. Ακόμη, διαπιστώνεται έλλειψη σε εναλλακτικά μέσα παροχής ενέργειας (π.χ. γεννήτρια) που θα μπορούσε να προβλέψει διάφορες δυσλειτουργίες σε περίπτωση διακοπής ηλεκτρικού ρεύματος.

Για τους παραπάνω κινδύνους που προκύπτουν από την ανάλυση και παρουσιάστηκαν στα συμπεράσματα, προτείνονται και συγκεκριμένα μέτρα αντιμετώπισης. Για τους πιο υψηλούς κινδύνους, που ήταν η προτεραιότητα της επιχείρησης, υπάρχει αυξημένος κίνδυνος λόγω φόρτου εργασίας σε συγκεκριμένες ώρες (10.00 - 12.00, 14.00 - 15.00 και 18.00 - 20.00). Για την αντιμετώπιση αυτών των κινδύνων ενεργοποιήθηκε πρόσθετο τείχος προστασίας (firewall). Επιπλέον έγινε παρέμβαση έτσι ώστε το σύστημα να μην αποθηκεύει προσωρινά οι κωδικοί πρόσβασης των χρηστών. Τέλος, έγινε ειδική ενημέρωση στα υπεύθυνα για την ασφάλεια στελέχη να κοινοποιούν τις οδηγίες χρήσης mobile devices στους εργαζόμενους ενώ έγινε και ειδική εκπαιδευτική παρουσίαση στους εργαζόμενους για την ασφάλεια του συστήματος. Αυτή η ενημέρωση έγινε με στόχο την εμπιστευτικότητα των πληροφοριών, για τη χρήση του ηλεκτρονικού συστήματος επικοινωνίας χωρίς να διαρρέουν οι εμπιστευτικές πληροφορίες.

Για τους δεύτερους σε ιεραρχία κινδύνους, προστέθηκε ισχυρό σύστημα που ελέγχει την ταυτότητα των χρηστών πριν εισέλθουν στο σύστημα, για την πιο αποτελεσματική αναγνώρισή τους. Για την πιο ασφαλή διαχείριση, το σύστημα απενεργοποιεί την είσοδο του χρήστη και δεν αποθηκεύει τις πληροφορίες εισόδου, μετά από 8 λεπτά αδράνειας στο σύστημα.

Τέλος, για τους λιγότερο πιθανούς κινδύνους, η επιχείρηση ενισχύθηκε με προηγμένα συστήματα πυρόσβεσης και αντιμετώπισης πλημμυρών που ενδέχεται να

αντιμετωπίσουν οι εγκαταστάσεις.Επίσης, έγινε ειδική μέριμνα για εναλλακτικά μέσα παροχής ενέργειας.Στα συστήματα της επιχείρησης προστέθηκαν γεννήτριες για κάθε κρίσιμο για την λειτουργία της σύστημα.Παράλληλα, έγιναν επενδύσεις σε εναλλακτικές μορφές ενέργειας.Συγκεκριμένα τοποθετήθηκαν ηλιακά πάνελ που αξιοποιούν την Ηλιακή Ενέργεια, για να μπορέσει να αποθηκεύει τέτοια ενέργεια αφενός για την εξοικονόμηση ενέργειας και αφετέρου να υπάρχει ασφάλεια σε περίπτωση κινδύνου όπως μια πτώση του ρεύματος.

6. Συμπεράσματα

Τα συμπεράσματα της εργασίας έρχονται στο τέλος αυτής, ως ο επίλογος της μετά το ερευνητικό τμήμα και την υλοποίηση. Στο τμήμα αυτό, στοιχειοθετούμε πως έχει καταλήξει η πτυχιακή εργασία μετά την επεξεργασία των δεδομένων που μας παρείχε η επιχείρηση. Η χρησιμότητα του κεφαλαίου αυτού είναι να εντοπιστούν οι κίνδυνοι που προκύπτουν από την παραπάνω ανάλυση, να εκτιμηθεί η σημαντικότητα τους και να προβλεφθούν μέθοδοι αντιμετώπισής τους. Οι τρεις βασικές κατηγορίες κινδύνων που περιεγράφηκαν είναι οι εξωτερικοί, οι εσωτερικοί και οι λοιποί κίνδυνοι. Αναφορικά με τους πρώτους, η γενική διαπίστωση είναι ότι υπάρχει σημαντικός φόρτος εργασίας για συγκεκριμένες ώρες που χρίζει προσοχής. Σε αυτή την κατηγορία θα πρέπει να τηρούνται όλες οι διαδικασίες και τα πρωτόκολλα ασφαλείας. Οι παρεμβάσεις που έγιναν ήταν η ενεργοποίηση πρόσθετου τείχους προστασίας και έγινε ειδική ενημέρωση στο προσωπικό.

Αναφορικά με τους δεύτερους, διαπιστώθηκε ότι το δίκτυο χρίζει περισσότερων ελέγχων και απαιτούνται οι κατάλληλες διαδικασίες ταυτοποίησης. Επίσης διαπιστώθηκε ότι η αντικατάσταση εξοπλισμού είναι αναγκαία. Σε αυτή τη βάση, προστέθηκαν πιο αναβαθμισμένα πρωτόκολλα ταυτοποίησης και αντικαταστάθηκε ο εξοπλισμός.

Ως προς την τρίτη κατηγορία κινδύνων χρειάζεται μέριμνα για μέσα πυρόσβεσης, αντιμετώπισης πλημμύρας και αντιμετώπισης διακοπών ηλεκτρικού ρεύματος. Η επιχείρηση μερίμνησε για αυτά με μέσα πυρόσβεσης και εναλλακτικές μορφές ενέργειας.

Η συνεισφορά της εργασίας είναι πολύπλευρη, δίνοντας αξία τόσο σε θεωρητική όσο και σε πρακτική διάσταση.

Αρχικά, μια πλευρά της συνεισφοράς είναι η ακαδημαϊκή συμβολή της έρευνας. Αυτό έγκειται στη θεωρητική διάσταση. Αυτή μπορεί να διαπιστωθεί ως προς τη διαδικασία που ακολούθησε η εργασία για την αξιολόγηση κινδύνου στον τομέα της προστασίας πληροφοριών και ως προς τα αποτελέσματα που εμπλουτίζουν τα γενικότερα ευρήματα στο αντικείμενο, για τους ερευνητές του μέλλοντος.

Επίσης, σε πρακτικό επίπεδο, τα αποτελέσματα της εργασίας μπορεί να είναι πολλαπλά χρήσιμα. Τα ευρήματα μπορούν να μεταφραστούν απευθείας σε συστάσεις πολιτικής για οργανισμούς και επιχειρήσεις του κλάδου, βοηθώντας στη βελτίωση των τρεχουσών διαδικασιών προστασίας πληροφοριών τους. Ακόμη, μπορούν να συνεισφέρουν στη δημιουργία ενός «οδικού χάρτη» βέλτιστων πρακτικών στην αξιολόγηση κινδύνου που θα θέτει σημεία αναφοράς για άλλους οργανισμούς στον κλάδο. Ακόμη μπορούν να χρησιμεύσουν σε στρατηγικές μετριασμού κινδύνου, καθώς θεωρητικά μπορεί να εισάγει καινοτόμες στρατηγικές για τον μετριασμό του κινδύνου, ενισχύοντας έτσι την αποτελεσματικότητα των υφιστάμενων συστημάτων. Τα αποτελέσματα θα μπορούσαν ακόμη να χρησιμοποιηθούν για την ανάπτυξη εκπαιδευτικών ενοτήτων για επαγγελματίες στον τομέα της ασφάλειας πληροφοριών, συμβάλλοντας στην ανάπτυξη δεξιοτήτων και στην ευαισθητοποίηση. Τέλος, η έρευνα μπορεί ακόμη και να καταλήγει στην ανάπτυξη εργαλείων λογισμικού ή αλγορίθμων που αυτοματοποιούν ή βελτιώνουν τη διαδικασία αξιολόγησης κινδύνου.

7. Βιβλιογραφικές Αναφορές

1. Abbass, W., Baina, A., & Bellafkih, M. (2015, December). Using EBIOS for risk management in critical information infrastructure. In *2015 5th World Congress on Information and Communication Technologies (WICT)* (pp. 107-112). IEEE.
2. Accerboni, F., & Sartor, M. (2019). ISO/IEC 27001. In *Quality Management: Tools, Methods, and Standards*. Emerald Publishing Limited.
3. Agrawal, V. (2016). Towards the Ontology of ISO/IEC 27005: 2011 Risk Management Standard. In *HAISA* (pp. 101-111).
4. Alberts, C., Dorofee, A., Stevens, J., & Woody, C. (2003). *Introduction to the OCTAVE Approach*. Carnegie-Mellon Univ Pittsburgh Pa Software Engineering Inst.
5. Alberts, C., Dorofee, A., Stevens, J., & Woody, C. (2005). OCTAVE-S implementation guide, Version 1.0. *Manuel électronique*. Pittsburg, PA,: Software Engineering Institute, Carbegie Mellon university.
6. Al-Dhahri, S., Al-Sarti, M., & Abdul, A. (2017). Information security management system. *International Journal of Computer Applications*, 158(7), 29-33.
7. Ashoor, A. S., & Gore, S. (2011). Importance of intrusion detection system (IDS). *International Journal of Scientific and Engineering Research*, 2(1), 1-4.
8. Azuwa, M., Ahmad, R., Sahib, S., & Shamsuddin, S. (2012). Technical security metrics model in compliance with ISO/IEC 27001 standard. *International Journal of Cyber-Security and Digital Forensics*, 1(4), 280-288.
9. Ballagas, R., Rohs, M., Sheridan, J. G., & Borchers, J. (2004, September). Byod: Bring your own device. In *Proceedings of the Workshop on Ubiquitous Display Environments, Ubicomp* (Vol. 2004).

10. Belsis, P., Kokolakis, S., & Kiountouzis, E. (2005). Information systems security from a knowledge management perspective. *Information Management & Computer Security*.
11. Bertino, E., & Sandhu, R. (2005). Database security-concepts, approaches, and challenges. *IEEE Transactions on Dependable and secure computing*, 2(1), 2-19.
12. Bertino, E., Jajodia, S., & Samarati, P. (1995). Database security: Research and practice. *Information systems*, 20(7), 537-556.
13. Bouganim, L., & Guo, Y. (2009). Database encryption.
14. Carminati, B., Ferrari, E., Heatherly, R., Kantarcioglu, M., & Thuraisingham, B. (2009, June). A semantic web based framework for social network access control. In *Proceedings of the 14th ACM symposium on Access control models and technologies* (pp. 177-186).
15. Chandel, S., Yu, S., Yitian, T., Zhili, Z., & Yusheng, H. (2019, October). Endpoint protection: Measuring the effectiveness of remediation technologies and methodologies for insider threat. In *2019 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC)* (pp. 81-89). IEEE.
16. Chonka, A., Zhou, W., Knapp, K., & Xiang, Y. (2008, July). Protecting information systems from ddos attack using multicore methodology. In *2008 IEEE 8th International Conference on Computer and Information Technology Workshops* (pp. 270-275). IEEE.
17. Dey, M. (2007, September). Information security management-a practical approach. In *AFRICON 2007* (pp. 1-6). IEEE.
18. Diamantopoulou, V., Tsohou, A., & Karyda, M. (2019, August). General Data Protection Regulation and ISO/IEC 27001: 2013: Synergies of activities towards organisations' compliance. In *International Conference on Trust and Privacy in Digital Business* (pp. 94-109). Springer, Cham.

19. Disterer, G., & Kleiner, C. (2013). BYOD bring your own device. *Procedia Technology*, 9, 43-53.
20. Dubois, É., Heymans, P., Mayer, N., & Matulevičius, R. (2010). A systematic approach to define the domain of information system security risk management. In *Intentional Perspectives on Information Systems Engineering* (pp. 289-306). Springer, Berlin, Heidelberg.
21. Eloff, J. H., & Eloff, M. (2003, September). Information security management: a new paradigm. In *Proceedings of the 2003 annual research conference of the South African institute of computer scientists and information technologists on Enablement through technology* (pp. 130-136).
22. Eloff, J. H., Labuschagne, L., & Badenhorst, K. P. (1993). A comparative framework for risk analysis methods. *Computers & Security*, 12(6), 597-603.
23. Ertoz, L., Lazarevic, A., Eilertson, E., Tan, P. N., Dokas, P., Kumar, V., & Srivastava, J. (2003). Protecting against cyber threats in networked information systems. *Battlespace Digitization and Network-Centric Systems III*, 5101, 51-56.
24. Fenz, S., Goluch, G., Ekelhart, A., Riedl, B., & Weippl, E. (2007, December). Information security fortification by ontological mapping of the ISO/IEC 27001 standard. In *13th Pacific Rim International Symposium on Dependable Computing (PRDC 2007)* (pp. 381-388). IEEE.
25. Fomin, V. V., Vries, H., & Barlette, Y. (2008, September). ISO/IEC 27001 information systems security management standard: Exploring the reasons for low adoption. In *Euromot 2008 conference, nice, france*.
26. Forester, T., & Morrison, P. (1994). *Computer ethics: Cautionary tales and ethical dilemmas in computing*. Mit Press.
27. Gerber, M., & Von Solms, R. (2008). Information security requirements—interpreting the legal aspects. *Computers & Security*, 27(5-6), 124-135.

28. Gillies, A. (2011). Improving the quality of information security management systems with ISO27000. *The TQM Journal*.
29. Gritzalis, D., Iseppi, G., Mylonas, A., & Stavrou, V. (2018). Exiting the risk assessment maze: A meta-survey. *ACM Computing Surveys (CSUR)*, 51(1), 1-30.
30. Haber, M. J. (2020). Privileged Access Management. In *Privileged Attack Vectors* (pp. 151-171). Apress, Berkeley, CA.
31. Harahap, R. M. (2011). Information Technology Risk Measurement: Octave-S Method. *CommIT (Communication and Information Technology) Journal*, 5(1), 27-29.
32. Heer, T., Gotz, S., Weingartner, E., & Wehrle, K. (2008, June). Secure Wi-Fi sharing at global scales. In *2008 International Conference on Telecommunications* (pp. 1-7). IEEE.
33. Humphreys, E. (2016). *Implementing the ISO/IEC 27001: 2013 ISMS Standard*. Artech House.
34. Ioannidis, S., Keromytis, A. D., Bellovin, S. M., & Smith, J. M. (2000, November). Implementing a distributed firewall. In *Proceedings of the 7th ACM conference on Computer and communications security* (pp. 190-199).
35. Ionita, D. (2013). *Current established risk assessment methodologies and tools* (Master's thesis, University of Twente).
36. Iphar, C., Napoli, A., Ray, C., Alincourt, E., & Brosset, D. (2016, September). Risk Analysis of falsified Automatic Identification System for the improvement of maritime traffic safety. In *Proceedings of ESREL* (pp. 606-613).
37. Iqbal, A., Horie, D., Goto, Y., & Cheng, J. (2009, December). A database system for effective utilization of ISO/IEC 27002. In *2009 Fourth International Conference on Frontier of Computer Science and Technology* (pp. 607-612). IEEE.

38. Jahchan, G. J. (2011). Privileged User Management. *Information Security Management Handbook*, 5, 37.
39. Khati, L., Mouha, N., & Vergnaud, D. (2017, February). Full disk encryption: bridging theory and practice. In *Cryptographers' Track at the RSA Conference* (pp. 241-257). Springer, Cham.
40. Laudon, K. C., & Laudon, J. P. (2020). *Management Information Systems: Managing the Digital Firm* (15th ed.). Pearson Education.
41. Li, Q., & Clark, G. (2013). Mobile security: A look ahead. *IEEE Security & Privacy*, 11(1), 78-81.
42. Liu, S., & Kuhn, R. (2010). Data loss prevention. *IT professional*, 12(2), 10-13.
43. Mavridis, I. (2016). Information and Security Systems Laboratory.
44. O'Brien, J. A., & Marakas, G. M. (2011). *Management Information Systems* (10th ed.). McGraw-Hill/Irwin.
45. Om, K. (2017, August). Secure email gateway. In *2017 IEEE International Conference on Smart Technologies and Management for Computing, Communication, Controls, Energy and Materials (ICSTM)* (pp. 49-53). IEEE.
46. Razzaq, A., Hur, A., Shahbaz, S., Masood, M., & Ahmad, H. F. (2013, March). Critical analysis on web application firewall solutions. In *2013 IEEE Eleventh International Symposium on Autonomous Decentralized Systems (ISADS)* (pp. 1-6). IEEE.
47. Scott, D., & Sharp, R. (2002). Developing secure web applications. *IEEE internet Computing*, 6(6), 38-45.
48. Sesay, S., Yang, Z., Chen, J., & Xu, D. (2005, January). A secure database encryption scheme. In *Second IEEE Consumer Communications and Networking Conference, 2005. CCNC. 2005* (pp. 49-53). IEEE.

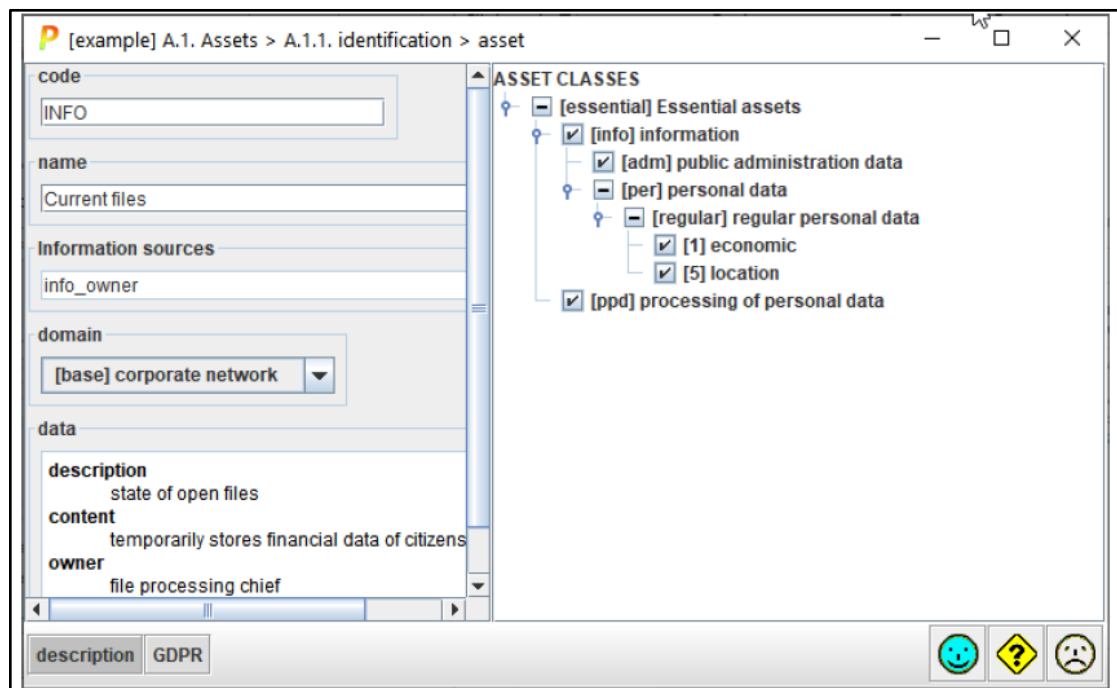
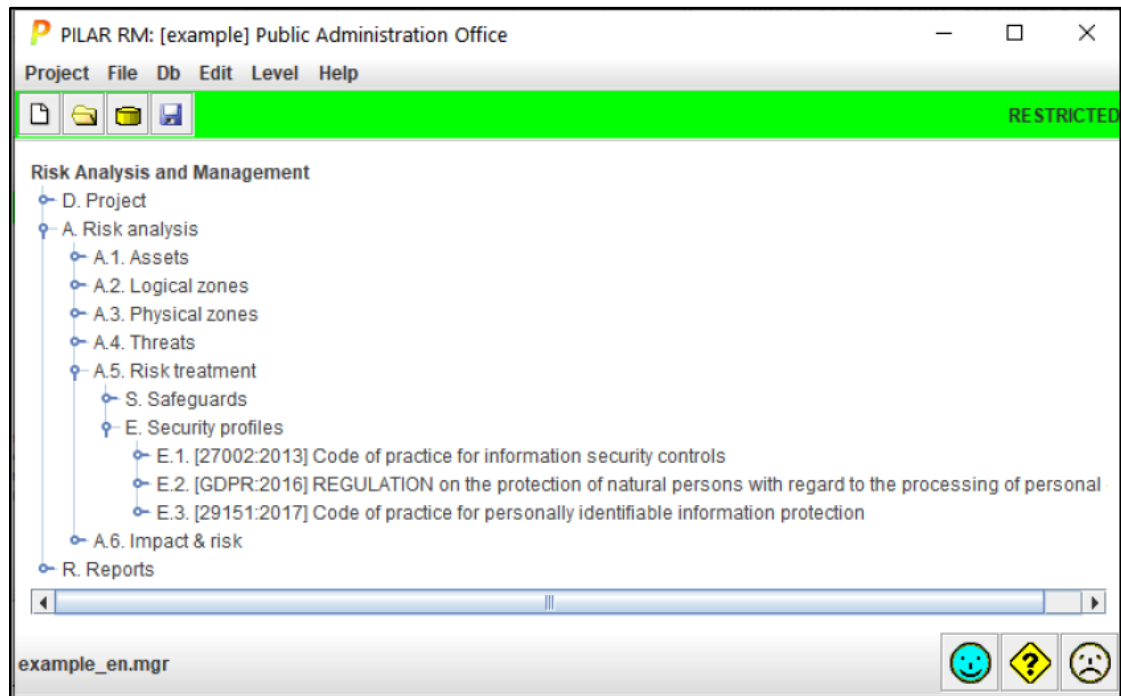
49. Sheikhpour, R., & Modiri, N. (2012). A best practice approach for integration of ITIL and ISO/IEC 27001 services for information security management. *Indian journal of science and technology*, 5(2), 2170-2176.
50. Sindiren, E., & Ciylan, B. (2018). Privileged account management approach for preventing insider attacks. *International Journal of Computer Science and Network Security*, 18(1), 33-42.
51. Singh, P., & Kaur, K. (2015, February). Database security using encryption. In *2015 International Conference on Futuristic Trends on Computational Analysis and Knowledge Management (ABLAZE)* (pp. 353-358). IEEE.
52. Smith, R. E. (1994, December). A secure Email gateway (building an RCAS external interface). In *Tenth Annual Computer Security Applications Conference* (pp. 202-211). IEEE.
53. Stair, R., & Reynolds, G. (2017). **Principles of Information Systems** (13th ed.). Cengage Learning.
54. Standard, A. (2015). ISO/IEC27002. In *Informationtechnology-security techniques-code of practice for information security controls,(AS ISO/IEC 27002: 2015)*.
55. Tariq, M. I., & Santarcangelo, V. (2016, February). Analysis of ISO 27001: 2013 controls effectiveness for cloud computing. In *International Conference on Information Systems Security and Privacy* (Vol. 2, pp. 201-208). SciTePress.
56. Țigănoaia, B. (2015). Some aspects regarding the information security management system within organizations–adopting the ISO/IEC 27001: 2013 standard. *Studies in Informatics and Control*, 24(2), 201-210.
57. Trèek, D. (2003). An integral framework for information systems security management. *Computers & Security*, 22(4), 337-360.

58. Tsohou, A., Kokolakis, S., Lambrinoudakis, C., & Gritzalis, S. (2009, September). Information systems security management: a review and a classification of the ISO standards. In *International Conference on e-Democracy* (pp. 220-235). Springer, Berlin, Heidelberg.
59. Velasco, J., Ullauri, R., Pilicita, L., Jácome, B., Saa, P., & Moscoso-Zea, O. (2018, November). Benefits of implementing an ISMS according to the ISO 27001 standard in the ecuadorian manufacturing industry. In *2018 International Conference on Information Systems and Computer Science (INCISCOS)* (pp. 294-300). IEEE.
60. Verma, S., & Singh, A. (2012, December). Data theft prevention & endpoint protection from unauthorized USB devices—Implementation. In *2012 Fourth International Conference on Advanced Computing (ICoAC)* (pp. 1-4). IEEE.
61. Von Solms, R. (1996). Information security management: The second generation. *Computers & Security*, 15(4), 281-288.
62. Von Solms, R. (1998). Information security management (3): the code of practice for information security management (BS 7799). *Information Management & Computer Security*.
63. Whitman, M. E., Townsend, A. M., & Aalberts, R. J. (2001). Information systems security and the need for policy. In *Information security management: Global challenges in the new millennium* (pp. 9-18). IGI Global.
64. Wüchner, T., & Pretschner, A. (2012, November). Data loss prevention based on data-driven usage control. In *2012 IEEE 23rd International Symposium on Software Reliability Engineering* (pp. 151-160). IEEE.
65. Yeh, J. (2017). *Key factors in building a Secure Web Gateway* (Doctoral dissertation, University of Waikato).

66. Λέρα, Μ. (2012). Μελέτη ασφάλειας πληροφοριών και Πληροφοριακών Συστημάτων. *Διπλωματική Εργασία, Τμήμα Μηχανικών Πληροφορικής και Τηλεπικοινωνιών, Πανεπιστήμιο Δυτικής Μακεδονίας.*
67. Μάγκος, Ε. (2007). Ασφάλεια Υπολογιστών και Προστασία Δεδομένων.
68. Μουλίνος, Κ. (2003). *Τεχνολογική υποδομή προστασίας δεδομένων στο διαδίκτυο* (Doctoral dissertation, Οικονομικό Πανεπιστήμιο Αθηνών. Τμήμα Πληροφορικής).
69. Τσούμα, Β. (2007). *Διαχείριση ασφάλειας πληροφοριακών συστημάτων με οντολογίες*. Διατριβή, Τμήμα Πληροφορικής, Οικονομικό Πανεπιστήμιο Αθηνών.

8. Παράρτημα Εργασίας

1. Λειτουργίες βασικού χρήστη



[example] A.1. Assets > A.1.1. identification > asset

code
mission

name
business unit x

Information sources

domain
[base] corporate network

data

description GDPR

ASSET CLASSES

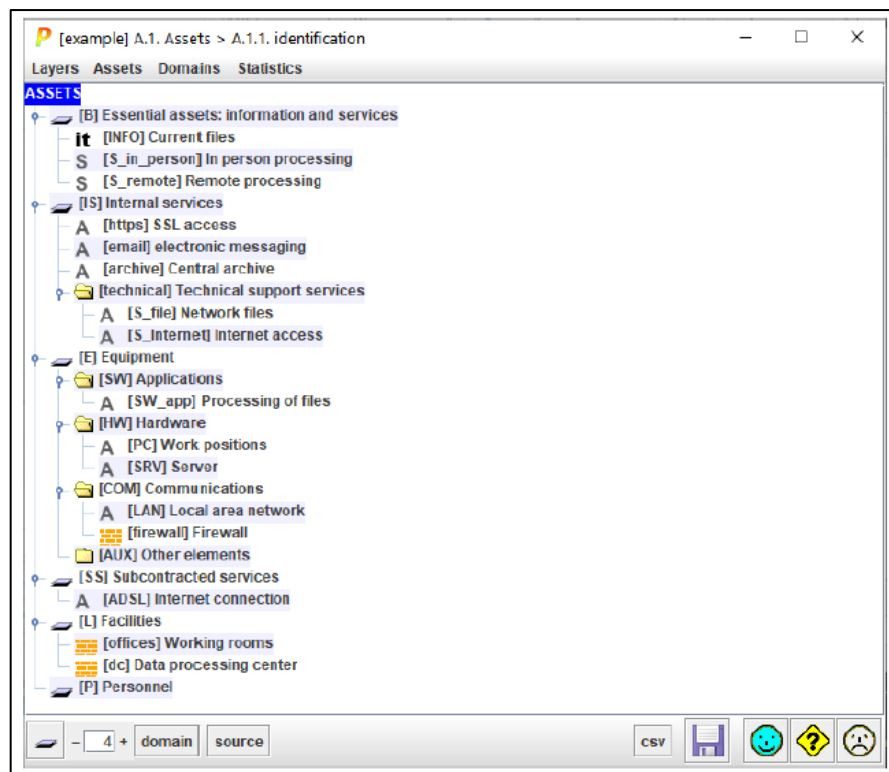
- [essential] Essential assets
 - [info] information
 - ☒ [biz] business data
 - ☐ [com] commercial data
 - ☐ [adm] public administration data
 - ☐ [vr] vital records (organizational r
 - ☐ [per] personal data
 - ☐ [normal] normal personal data
 - ☒ [regular] regular personal data
 - ☐ [pseudonymous] pseudonymo
 - ☐ [sensitive] sensitive personal
 - ☐ [children] children
 - ☐ [criminal] criminal law (art. 10
 - ☐ [classified] classified information
 - [service] service
 - ☒ [operations] operations
 - ☐ [logistics] logistics
 - ☐ [intelligence] intelligence

[example] risk analysis > assets > valuation of domains

Edit Export Import

asset / security domain	[A]	[I]	[C]	[Auth]	[Acc]	[V]	[PD]
[example] Public Administration Office							
[-] [essential] Essential assets	[4]	[4]	[7]	[7]	[7]		[1]
[-] it [INFO] Current files		[4]	[7]	[4]	[4]		[1]
[-] S [S_in_person] In person processing	[4]			[7]	[7]		
[-] S [S_remote] Remote processing	[1]			[7]	[7]		
[-] Security domains							
[-] [base] corporate network	[4]	[4]		[7]	[7]		[1]
[-] [bps] Internet connection	[1]			[7]	[7]		

associate dissociate



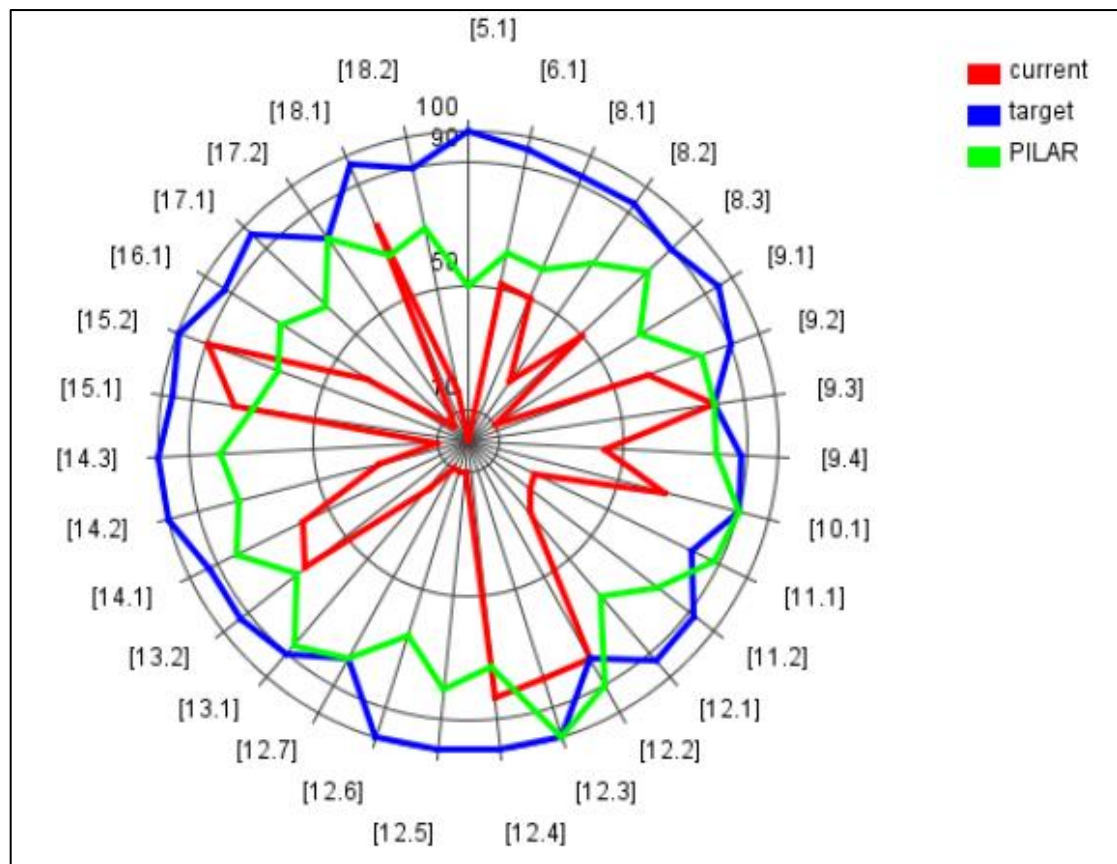
[example] 27002:2013 > valuation

Edit Expand View Export Import Statistics Select Graphs

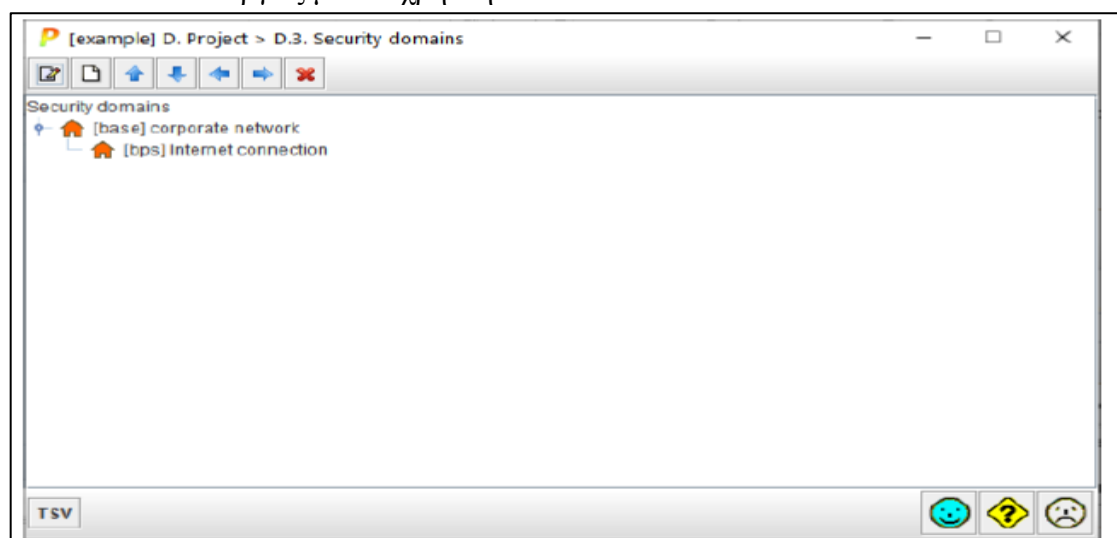
(base) corporate network Information sources

	rec.	level	control	do...	so...	ap...	co...	current	target	PII AR
☐			[27002:2013] Code of practice for information security cont					L0-L5 ...	L3-L5 ...	L2-L5
☐	2		✓ [5] INFORMATION SECURITY POLICIES					L0	L5	L2
☐	2		✓ [5.1] MANAGEMENT DIRECTION FOR INFORMA					L0	L5	L2
☐	4		✓ [6] ORGANIZATION OF INFORMATION SECURITY			...		L0-L5 ...	L4-L5	L2-L3
☐	4		✓ [6.1] INTERNAL ORGANIZATION					L0-L5 ...	L4-L5	L2-L3
☐			✓ [6.2] MOBILE DEVICES AND TELEMWORKING			n.a.				
☐			✓ [7] HUMAN RESOURCE SECURITY			n.a.				
☐			✓ [7.1] PRIOR TO EMPLOYMENT			n.a.				
☐			✓ [7.2] DURING EMPLOYMENT			n.a.				
☐			✓ [7.3] TERMINATION AND CHANGE OF EMPLOYM			n.a.				
☐	5		✓ [8] ASSET MANAGEMENT			...		L1-L2 ...	L4-L5 ...	L2-L3
☐	4		✓ [8.1] RESPONSIBILITY FOR ASSETS			...		L2 (L0...	L4-L5 ...	L2-L3
☐	5		✓ [8.2] INFORMATION CLASSIFICATION					L1-L2	L4-L5	L2-L3
☐	5		✓ [8.3] MEDIA HANDLING					L2 (L1...	L4 (L3...	L3 (L2...
☐	5		✓ [9] ACCESS CONTROL					L0-L4 ...	L3-L5 ...	L2-L3
☐	3		✓ [9.1] BUSINESS REQUIREMENTS FOR ACCESS					L1 (L1...	L4-L5	L2-L3
☐	5		✓ [9.2] USER ACCESS MANAGEMENT					L1-L4 ...	L3-L5 ...	L3 (L2...

- 1 + +1 domains [Icons] suggest



2. Λειτουργίες μέσω χρήστη



[example] A.1. Assets > A.1.5. valuation of domains

Edit Export Import

asset / security domain	[A]	[I]	[C]	[Auth]	[Acc]	[V]	[PD]
[example] Public Administration Office							
[-] [essential] Essential assets	[4]	[4]	[7]	[7]	[7]		[1]
[-] [INFO] Current files		[4]	[7]	[4]	[4]		[1]
[-] [S_in_person] In person processing	[4]			[7]	[7]		
[-] [S_remote] Remote processing	[1]			[7]	[7]		
Security domains							
[-] [base] corporate network	[4]	[4]	[7]	[7]	[7]		[1]
[-] [bps] Internet connection	[1]			[7]	[7]		

associate dissociate

[example] S. Safeguards > S.2. valuation (phases)

Edit Expand View Export Import Statistics

[base] corporate network										Information sources		
	as...	top	re...	level	safeguard	dou...	sou...	app...	com...	curr...	target	PILAR
☐					SAFEGUARDS					L0-L5	L0-L5	L2-L5
☐	M	EL	8		[-] [A] Identification and authentication					L0-L4	L1-L4	L2-L4
☐	T	EL	6		[-] [AC] Logical access control			...		L0-L5	L1-L5	L2-L4
☐	M	PR	8		[-] [D] Protection of Data / Information			...		L0-L5	L1-L5	L2-L4
☐	M	EL	8		[-] [K] Protecting cryptographic keys [SC-12]			...		L3	L4	L2-L5
☐	M	PR	5		[-] [S] Protection of Services			...		L0-L5	L1-L5	L2-L3
☐	M	PR	5		[-] [SW] Protection of Software			...		L0-L5	L1-L5	L2-L3
☐	M	PR	5		[-] [HW] Protection of Hardware	..?		...		L0-L3	L0-L5	L2-L3
☐	M	PR	9		[-] [COM] Protection of Communications			...		L0-L3	L1-L5	L2-L5
☐	M	PR	5		[-] [M] Protection of Media			...		L1-L2	L3-L5	L2-L3
☐	M	PR	5		[-] [AUX] Auxiliary Means		phy...			L0-L2	L3-L5	L2-L3
☐	PHY	EL	5		[-] [PPE] Physical protection of equipment			...		L2	L4-L5	L2-L3
☐	PHY	PR	4		[-] [L] Protection of the installations		phy...	...		L0-L5	L3-L5	L2-L3
☐	PER	PR			[-] [P] Personnel			n.a.		n.a.	n.a.	n.a.
☐	M	CR	5		[-] [IM] Incident management (ICT)			...		L0-L5	L1-L5	L2-L3
☐	T	PR	7		[-] [tools] Security tools			...		L0-L2	L1-L5	L2-L4
☐	M	CR	3		[-] [V] Vulnerability management					L0	L5	L2-L3

- 1 + sources operation suggest find >>

[example] S. Safeguards > S.2. valuation (phases)

Edit Expand View Export Import Statistics

[base] corporate network Information sources

	as...	top	re...	level	safeguard	dou...	sou...	app...	com...	curr...	target	PILAR
☐	T	EL	9		[COM.SC] Secure configuration baseline is applied [CM-6]					L0-L2	L4-L5	L3-L5
☐	T	PR	4		[COM.SC.1] Communication options are reduced to the minimum required					L0	L5	L3
☐	T	EL	5		[COM.SC.2] User accounts included by default in the products are removed or modified					L0	L5	L3
☐	T	EL	9		[COM.SC.3] Administrator accounts included by default in the products are removed or modified [IA-5(5)]					L0	L5	L5

28.4 :: [COM.SC.3] Administrator accounts included by default in the products are removed or modified [IA-5(5)]

26.9 :: [IAb] IDENTIFICATION AND AUTHENTICATION [IA, IAb]

20.2 :: [tools.CM.1.2] Application of security patches

20.2 :: [ACb] ACCESS CONTROL [AC, ACb]

20.2 :: [COM.SC.5] Enabled services are configured securely

18.1 :: [IA.8.3] {xor} AAL3: provides very high confidence

1 sources operation suggest find >>

Risk treatment

PILAR - Own safeguards

☒ visible ☒ apply

NIST SP800-53 - Security and Privacy Controls for Information Systems and Organizations

☒ visible ☐ apply

[27002:2013] Code of practice for information security controls

☒ visible ☒ propagate

[GDPR:2016] REGULATION on the protection of natural persons with regard to the processing of personal data

☒ visible ☒ propagate ☒ apply

[29151:2017] Code of practice for personally identifiable information protection

☒ visible ☒ propagate