



ΙΟΝΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ
ΣΧΟΛΗ ΕΠΙΣΤΗΜΗΣ ΤΗΣ ΠΛΗΡΟΦΟΡΙΑΣ ΚΑΙ ΠΛΗΡΟΦΟΡΙΚΗΣ
ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

Πτυχιακή Εργασία

Ζητήματα και αποκλίσεις κατά την εφαρμογή στρατηγικών
αντιμετώπισης περιστατικών ασφάλειας πληροφοριών και ο ρόλος του
ανθρώπινου παράγοντα

Πυλαρινός Διονύσης

Επιβλέπουσα Καθηγήτρια

Αγγελική Τσώχου

Χριστόφορος Νταντογιάν – Ελένη Χριστοπούλου

Σεπτέμβριος 2022

ΕΥΧΑΡΙΣΤΙΕΣ

Αρχικά, θα ήθελα να ευχαριστήσω τους γονείς μου, που ήταν πάντα δίπλα μου και έχουν συμβάλει καθοριστικά στον άνθρωπο που είμαι σήμερα.

Επίσης θέλω να ευχαριστήσω την καθηγήτρια μου κυρία Τσώχου Αγγελική για την βοήθεια και καθοδήγηση κατά τα στάδια εκπόνησης της πτυχιακής μου εργασίας.

Περίληψη

Ολοένα και περισσότεροι οργανισμοί είτε μικροί είτε μεγάλοι είτε πρόκειται για ιδιωτικές εταιρείες είτε για δημόσιους φορείς εξαρτώνται από ασφαλείς προσεγγίσεις και διαδικασίες γύρω από την ασφάλεια των πληροφοριών. Η εκρηκτική αύξηση της τεχνογνωσίας των χρηστών σχετικά με παραβιάσεις αλλά και η συντήρηση και η δημιουργία μιας υψηλού επιπέδου κουλτούρας ασφάλειας αποτελεί μια σημαντική πρόκληση για την διατήρηση της ασφάλειας στους οργανισμούς.

Είναι αξιοσημείωτο το γεγονός ότι σε πολλούς οργανισμούς σημειώνονται περιστατικά εκμετάλλευσης τρωτών σημείων, στοχεύοντας στην παραβίαση του απορρήτου όσο και στην παραβίαση της διαθεσιμότητας και της ακεραιότητας. Κατά καιρούς έχουν προταθεί πολλές εναλλακτικές και έχουν δοθεί ευέλικτες οδηγίες από αρμόδιους φορείς για τους ενδεδειγμένους τρόπους κάλυψης αναγκών ανίχνευσης, διαχείρισης, καθώς και αντιμετώπισης των περιστατικών αυτών.

Στην παρούσα εργασία, διεξήχθη έρευνα συστηματικής ανασκόπησης δύο άρθρων, σε σύνολο τεσσάρων οργανισμών. Σκοπός της έρευνας είναι η ανακάλυψη διαφόρων ζητημάτων και αποκλίσεων που ενδεχομένως προκύπτουν κατά την εφαρμογή των στρατηγικών αντιμετώπισης ασφάλειας πληροφοριών που έχουν θεσπιστεί από κάθε οργανισμό ξεχωριστά. Παράλληλα, εξετάζεται πώς ο ανθρώπινος παράγοντας και κατ' επέκταση οι υπάλληλοι του κάθε οργανισμού επηρεάζουν από την πλευρά τους την εφαρμογή των στρατηγικών ασφάλειας των εταιρικών πληροφοριών.

Τέλος, μετά την εξαγωγή των αποτελεσμάτων και των συμπερασμάτων γίνονται ορισμένες συστάσεις, σχετικά με το πώς είναι εφικτό να καταπολεμηθούν τα ζητήματα που εντοπίστηκαν αλλά και οι αποκλίσεις κατά την εφαρμογή στρατηγικών αντιμετώπισης ασφάλειας πληροφοριών.

Λέξεις Κλειδιά: Information Security Incidents, Systematic Review, Large Organizations, Human Error

Πίνακας Περιεχομένων

Πίνακας Περιεχομένων	3
Πίνακας Εικόνων	5
ΚΕΦΑΛΑΙΟ 1: Εισαγωγή.....	6
1.1 Πεδίο Εφαρμογής	6
1.2 Δήλωση Προβλήματος.....	6
1.3 Ερευνητικές ερωτήσεις	7
ΚΕΦΑΛΑΙΟ 2^ο : Ορισμοί και έννοιες σχετικά με την διαχείριση περιστατικών	
ασφάλειας πληροφοριών	8
2.1 Ορισμοί για συμβάν και περιστατικό ασφάλειας μέσα σε έναν οργανισμό	8
2.2 Διαχείριση Περιστατικού Ασφαλείας	8
2.2.1 Ο όρος της διαχείρισης περιστατικού και της διασφάλισης ασφάλειας των	
πληροφοριών.....	8
2.2.2 Τύποι ομάδων αντιμετώπισης περιστατικών ασφαλείας	9
2.2.3 Διαδικασίες αντιμετώπισης και διαχείρισης περιστατικού ασφαλείας κατά	
NIST-SP 800-61.....	10
2.2.4 Διαδικασίες αντιμετώπισης και διαχείρισης περιστατικού ασφαλείας ITIL	
.....	14
2.2.5 Το πρότυπο ISO /IEC 27001-2013	17
2.2.6 Το πρότυπο ISO / IEC 27002-2022	23
2.2.7 Το Πρότυπο ISO 27035-2016.....	24
2.2.8 Πληροφορίες που καταγράφονται σε έντυπο αναφοράς	
συμβάντος/περιστατικού.....	25
2.2.9 Πιθανές συνέπειες κακής αντιμετώπισης και τι προσφέρει μια καλή	
αντιμετώπιση/διαχείριση.....	26
2.3 Γνώσεις και αρχές που απαιτούνται από την ομάδα από τον διευθυντή της	
ομάδας και από τον οργανισμό για την διαχείριση περιστατικών	27
2.3.1 Απαιτούμενες αρχές, γνώσεις αλλά και εμπειρίες από την ομάδα	
αντιμετώπισης.....	27
2.3.2 Απαιτούμενες γνώσεις και ενέργειες για υπεύθυνο ή διευθυντή της ομάδας	
και κατάλληλες ενέργειες για εκπαίδευση των υπαλλήλων αυτής.....	28
2.3.3 Στάση οργανισμών ή κυβερνήσεων για την στήριξη της ομάδας	
αντιμετώπισης περιστατικών ασφαλείας	29
ΚΕΦΑΛΑΙΟ 3^ο: Μεθοδολογία	30
3.1 Εισαγωγή.....	30
3.2 Επιλογή Μεθοδολογίας.....	30
3.2.1 Πλεονεκτήματα	31
3.2.2 Χαρακτηριστικά και Αναζήτηση	32
3.3 Επιλογή Τύπου Ανασκόπησης.....	33
3.4 Βήματα Συστηματικής Ανασκόπησης.....	34
3.5 Αναζήτηση και Επιλογή.....	37
3.5.1 Εισαγωγή στην Αναζήτηση	37
3.5.2 Κριτήρια Αναζήτησης Μελέτης	37
3.5.3 Επιλογή Μελέτης.....	38
3.6 Έρευνα Περιπτώσεων.....	39
3.7 Αξιολόγηση ποιότητας μελετών	40

3.7.1 Περίπτωση των τριών νορβηγικών οργανισμών	41
3.7.2 Περίπτωση FinanceOrg	44
ΚΕΦΑΛΑΙΟ 4^ο: Μελέτες περιπτώσεων - Εισαγωγή.....	47
4.1 Οργανισμός Α	47
4.2 Οργανισμός Β	47
4.3 Οργανισμός Γ	48
4.4 Οργανισμός FinanceOrg.....	48
ΚΕΦΑΛΑΙΟ 5^ο: ΑΠΟΤΕΛΕΣΜΑΤΑ.....	50
5.1 Εισαγωγή.....	50
5.2 Αποτελέσματα σχετικά με την ικανότητα των οργανισμών να ανακαλύπτουν περιστατικά ασφαλείας	51
5.2.1 FinanceOrg.....	51
5.2.2 Οργανισμός Α	52
5.2.3 Οργανισμός Β	53
5.2.3 Οργανισμός Γ	54
5.3 Αποτελέσματα σχετικά με τις ρουτίνες, διαδικασίες, σχέδια και πρόβες για τον χειρισμό και την αντιμετώπιση των περιστατικών	55
5.3.1 Finance.....	55
5.3.2 Οργανισμός Α	56
5.3.3 Οργανισμός Β	58
5.3.4 Οργανισμός Γ	61
5.4 Αποτελέσματα σχετικά με τον αντίκτυπο στους οργανισμούς.....	62
5.4.1 Finance.....	62
5.4.2 Οργανισμός Α	63
5.4.3 Οργανισμός Β	63
5.4.4 Οργανισμός Γ	63
5.5 Αποτελέσματα σχετικά με την επιρροή του ανθρώπινου παράγοντα	63
5.5.1 Finance.....	63
5.5.2 Οργανισμός Α	64
5.5.3 Οργανισμός Β	65
5.5.4 Οργανισμός Γ	67
ΚΕΦΑΛΑΙΟ 6^ο : ΣΥΜΠΕΡΑΣΜΑΤΑ	69
6.1 Συμπεράσματα για το πρώτο ερευνητικό ερώτημα.....	69
6.2 Συμπεράσματα για το δεύτερο ερευνητικό ερώτημα.....	71
6.3 Συμπεράσματα για το τρίτο ερευνητικό ερώτημα.....	74
6.4 Συμπεράσματα για το τέταρτο ερευνητικό ερώτημα.....	75
ΚΕΦΑΛΑΙΟ 7^ο: Γενικά Συμπεράσματα – Προτάσεις και Μελλοντική έρευνα ..	80
7.1 Γενικά Συμπεράσματα – Προτάσεις.....	80
7.2 Μελλοντική Έρευνα.....	83
Βιβλιογραφία	84

Πίνακας Εικόνων

ΕΙΚΟΝΑ 1: ΚΥΚΛΟΣ ΖΩΗΣ ΑΠΟΚΡΙΣΗΣ ΠΕΡΙΣΤΑΤΙΚΟΥ	11
ΕΙΚΟΝΑ 2 ΒΗΜΑΤΑ ΒΙΒΛΙΟΓΡΑΦΙΚΗΣ ΣΥΣΤΗΜΑΤΙΚΗΣ ΑΝΑΣΚΟΠΗΣΗΣ	34

ΚΕΦΑΛΑΙΟ 1: Εισαγωγή

1.1 Πεδίο Εφαρμογής

Είτε πρόκειται για μικρούς είτε για μεγάλους οργανισμούς τα πληροφοριακά συστήματα είναι ζωτικής σημασίας για την λειτουργία τους. Ωστόσο, τα τελευταία χρόνια έρχονται αντιμέτωποι με μια σειρά πολλών προκλήσεων στον τομέα της ασφάλειας και πιο συγκεκριμένα έρχονται αντιμέτωποι με εξελιγμένες και οργανωμένες επιθέσεις που έχουν ως στόχο την καταστροφή υπηρεσιών και υποκλοπή δεδομένων του κυβερνοχώρου και όχι μόνο. Συνήθως, σε τέτοια περιστατικά ή συμβάντα ασφάλειας πληροφοριών χρησιμοποιούνται αρκετά εξελιγμένα εργαλεία και σύγχρονες τεχνικές μέθοδοι.

Τέτοιου είδους συμβάντα μπορεί να προέρχονται από σκόπιμες εσωτερικές ή εξωτερικές ενέργειες αλλά και από μη σκόπιμες ενέργειες, όπως σφάλματα σε υπηρεσίες. Επιπρόσθετα, είναι ευρέως αποδεκτό ότι ο ανθρώπινος παράγοντας και κατά συνέπεια το ανθρώπινο λάθος αποτελούν μεγάλο κίνδυνο για τους οργανισμούς, με αποτέλεσμα πολλοί να στρέφονται σε τεχνικές καθοδήγησης των εργαζομένων τους (Hedström, Kolkowska, Karlsson, & Allen, 2011).

Αυτά τα περιστατικά είναι απαραίτητο να αντιμετωπίζονται άμεσα για να μην θέτουν σε κίνδυνο τις αξίες των οργανισμών. Και κυρίως, όποτε συμβαίνουν είναι χρήσιμο να υπάρχει μια τυπικά συγκεκριμένη σειρά ενεργειών που θα ακολουθείται και θα τίθεται σε εφαρμογή με σκοπό τον περιορισμό και την αντιμετώπιση τους.

1.2 Δήλωση Προβλήματος

Υπάρχουν αρμόδιοι φορείς που έχουν θεσπίσει πρότυπα και θεωρίες για τον τρόπο διαχείρισης, καθώς και αντιμετώπισης ενός περιστατικού ή συμβάντος, την δήλωση του, τον περιορισμό του και στο τέλος την ολοκληρωτική αντιμετώπιση του. Αυτές οι θεωρίες είναι αδύνατο να μπορούν να καλύψουν όλο το εύρος τύπων περιστατικών και ως εκ τούτου, πολλές φορές είναι αναποτελεσματικές. Επίσης, οι λεπτομέρειες κάθε περιστατικού είναι διαφορετικές και μοναδικές, με αποτέλεσμα να καθίσταται ακόμα πιο δύσκολη η εφαρμογή αυτών των θεωριών.

Σε πολλές περιπτώσεις δεν υπάρχει γνώση μέσα στους οργανισμούς για το πως εφαρμόζονται αυτές οι θεωρίες, ακόμα και σε πολύ απλά επίπεδα, γεγονός που οδηγεί

στην έλλειψη αντίληψης του κινδύνου που κρύβουν τα περιστατικά ασφάλειας πληροφοριών.

Στην παρούσα πτυχιακή εργασία επιχειρείται η διερεύνηση των στρατηγικών που εφαρμόζουν οι οργανισμοί για την ανίχνευση, την διαχείριση και την αντιμετώπιση περιστατικών αλλά και τι ζητήματα προκύπτουν κατά την εφαρμογή τους. Παράλληλα, θα μελετηθεί ο αντίκτυπος που είχαν αυτές οι εφαρμοσμένες στρατηγικές στους οργανισμούς, με γνώμονα τον ανθρώπινο παράγοντα και κατά επέκταση τους υπάλληλους των οργανισμών, δηλαδή το πως επηρέασαν την εφαρμογή αυτών των στρατηγικών και αν ή κατά πόσο εξαρτάται η ορθή εφαρμογή από αυτούς.

Τέλος θα προταθούν κάποιες ενέργειες, οι οποίες είναι ικανές να αντιμετωπίσουν τα θέματα που εντοπίστηκαν.

1.3 Ερευνητικές ερωτήσεις

1. Έχουν οι οργανισμοί την ικανότητα να ανακαλύπτουν περιστατικά ασφαλείας;
2. Έχουν οι οργανισμοί διαδικασίες «ρουτίνας», σχέδια και πρόβες για τον χειρισμό και την αντιμετώπιση περιστατικών;
3. Τι αντίκτυπο και τι αποτέλεσμα έχουν επιφέρει οι χειρισμοί «ρουτίνας», οι διαδικασίες και η εκπαίδευση πάνω σε περιστατικά στους οργανισμούς ;
4. Πως επηρεάζει ο ανθρώπινος παράγοντας (γνώσεις, θέση, προσωπικότητα, χαρακτήρας του ανθρώπου), δηλαδή οι υπάλληλοι των οργανισμών την εφαρμογή των στρατηγικών αντιμετώπισης;

ΚΕΦΑΛΑΙΟ 2^ο: Ορισμοί και έννοιες σχετικά με την διαχείριση περιστατικών ασφάλειας πληροφοριών

2.1 Ορισμοί για συμβάν και περιστατικό ασφάλειας μέσα σε έναν οργανισμό

Οι ορισμοί για το τι είναι «συμβάν» και κατά περίπτωση «συμβάν ασφάλειας πληροφοριών» και «περιστατικό ασφάλειας πληροφοριών» δίνονται από το ISO (ISO-Technical Committee, 2016).

Συμβάν: εμφάνιση ενός προκαθορισμένου συνόλου περιστάσεων ή αλλαγή ενός συγκεκριμένου συνόλου περιστάσεων.

Συμβάν ασφάλειας πληροφοριών: αναγνωρισμένη κατάσταση ενός συστήματος, υπηρεσίας ή δικτύου που υποδεικνύει ενδεχόμενη παραβίαση της πολιτικής ασφάλειας των πληροφοριών ή αποτυχία των αντιμέτρων ή την ύπαρξη μιας άγνωστης κατάστασης που μπορεί να είναι σχετική με την ασφάλεια.

Περιστατικό Ασφάλειας Πληροφοριών: ένα ή περισσότερα ανεπιθύμητα ή μη αναμενόμενα συμβάντα ασφάλειας πληροφοριών που έχουν σημαντική πιθανότητα να υπονομεύσουν τις επιχειρηματικές λειτουργίες και να απειλήσουν την ασφάλεια των πληροφοριών.

2.2 Διαχείριση Περιστατικού Ασφαλείας

2.2.1 Ο όρος της διαχείρισης περιστατικού και της διασφάλισης ασφάλειας των πληροφοριών

Παράλληλα, σύμφωνα με το ISO δίνονται και οι σχετικοί ορισμοί, αναφορικά με τη «διαχείριση περιστατικών ασφαλείας πληροφοριών», καθώς και τη «διασφάλιση/συνέχιση της ασφάλειας πληροφοριών» (ISO-Technical Committee, 2016).

Διαχείριση περιστατικών ασφάλειας πληροφοριών: διαδικασίες ανίχνευσης, αναφοράς, αξιολόγησης, ανταπόκρισης, αντιμετώπισης και αξιοποίησης για μάθηση από συμβάντα ασφάλειας πληροφοριών.

Διασφάλιση/Συνέχιση της ασφάλειας των πληροφοριών: διαδικασίες για τη διασφάλιση συνεχιζόμενων λειτουργιών για την προστασία της ασφάλειας πληροφοριών.

2.2.2 Τύποι ομάδων αντιμετώπισης περιστατικών ασφαλείας

Ομάδα αντιμετώπισης περιστατικών ασφαλείας πληροφοριών (ISIRT): Πρόκειται για την εσωτερική ομάδα που έχει ορίσει ο οργανισμός και αποτελείται από κατάλληλα και έμπιστα μέλη του οργανισμού, υπεύθυνα για τον χειρισμό των περιστατικών ασφαλείας πληροφοριών κατά την διάρκεια του κύκλου ζωής τους (ISO-Technical Committee, 2016).

Οι οργανισμοί (Bada, Creese, Goldsmith, Mitchell, & Phillips, 2014) μπορούν να αναζητούν βοήθεια και σε εξωτερικές ομάδες ειδικών εκτός από τις δικές τους, δηλαδή ομάδες αναγνωρισμένες που προσφέρουν υπηρεσίες αντιμετώπισης περιστατικών ηλεκτρονικών υπολογιστών ή και ακόμα από την εθνική ομάδα αντιμετώπισης έκτακτης ανάγκης CERT (Computer Emergency Response Team). Υπάρχουν διάφορες συντομογραφίες για τον ίδιο όρο αλλά χρησιμοποιείται περισσότερο και το CSIRT όπως:

- CERT ή CERT/CC (Ομάδα Αντιμετώπισης Έκτακτης Ανάγκης Υπολογιστών / Κέντρο Συντονισμού)
- CSIRT (Ομάδα Αντιμετώπισης Συμβάντων Ασφάλειας Υπολογιστών)
- IRT (Ομάδα Αντιμετώπισης Συμβάντων)
- CIRT (Ομάδα Αντιμετώπισης Συμβάντων Υπολογιστή)
- SERT (Ομάδα Αντιμετώπισης Έκτακτης Ανάγκης Ασφαλείας)
- WARPs (Προειδοποιητικές συμβουλές και σημεία αναφοράς)

Η πρωταρχική αποστολή μιας Ομάδας Αντιμετώπισης Συμβάντων Ασφάλειας Υπολογιστών (CSIRT) είναι να βοηθήσει οργανισμούς να χειριστούν περιστατικά που συμβαίνουν, καθώς και να παρέχουν ένα ευρύτερο σύνολο υπηρεσιών. Εκτός από την κύρια αποστολή, οι ομάδες CSIRT πρέπει να είναι σε θέση να προσαρμόζονται σε ένα συνεχώς μεταβαλλόμενο περιβάλλον και παρόν και να έχουν την ευελιξία για την αντιμετώπιση οποιουδήποτε απροσδόκητου περιστατικού.

Τομεακές CSIRT: Ομάδα αντιμετώπισης περιστατικών ασφαλείας υπολογιστών που καλύπτει περιστατικά ασφαλείας ή και κυβερνοασφάλειας. Αφορούν ένα συγκεκριμένο τομέα, όπως η υγεία ή ο χρηματοοικονομικός τομέας ενώ αντίθετα η Εθνικές CSIRT προσφέρουν τις υπηρεσίες τους στον δημόσιο τομέα.

Οι ομάδες CSIRT (De Muynck & Portesi, 2016) παρέχουν υπηρεσίες προληπτικές, εκτός από την υποστήριξη και ανταπόκριση στα περιστατικά, όπως συνεχή ενημέρωση για μεγαλύτερη ασφάλεια αλλά και εκπαίδευση για την ενδυνάμωση της κουλτούρας της ασφάλειας των οργανισμών. Μια από τις βασικές δυνάμεις των CSIRT, ανεξαρτήτως τύπου είναι ότι έχουν τη δυνατότητα σε αρκετά μεγαλύτερο βαθμό να μετριάσουν αποτελεσματικά το συμβάν σε τεχνικό επίπεδο και σε σύντομο χρονικό διάστημα. Οι εθνικές και κυβερνητικές CSIRT ευθυγραμμίζονται με τις συστάσεις της Ευρωπαϊκής Ένωσης.

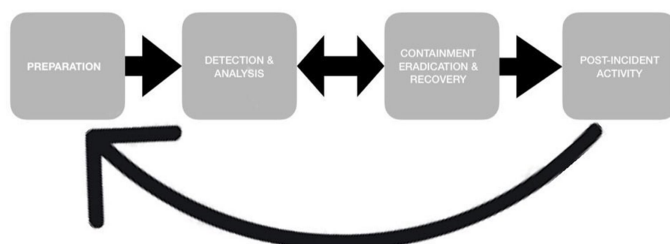
2.2.3 Διαδικασίες αντιμετώπισης και διαχείρισης περιστατικού ασφαλείας κατά NIST-SP 800-61

Σύμφωνα με τους De Muynck & Portesi (2016) η αντιμετώπιση και διαχείριση των συμβάντων ενός οργανισμού αφορά κατά βάση την προστασία των πληροφοριών, του ίδιου μέσω μιας ειδικής διαδικασίας προστασίας πληροφοριών που επιλέχθηκε να ακολουθηθεί και να εφαρμοστεί. Αυτή η διαδικασία αποτελείται από σχέδια, ρόλους, εκπαίδευση και επίβλεψη της διαχείρισης με όλα αυτά να συμβάλουν στην ταχεία ανίχνευση αλλά και στην ταχεία αντιμετώπιση της επίθεσης ώστε να εξαλειφθεί ο εισβολέας για να αποκατασταθεί η ακεραιότητα του οργανισμού. Τις περισσότερες φορές το αποτέλεσμα άλλα και ο στόχος των επιθέσεων είναι να θέτει σε κίνδυνο προσωπικά δεδομένα αλλά και επιχειρηματικά δεδομένα των οργανισμών οπότε κρίνεται υψίστης σημασίας η αποτελεσματική αντιμετώπιση στα συμβάντα ασφαλείας.

Σύμφωνα με το NIST (Cichonski, Millar, Grance, & Scarfone, 2012) στόχος των οργανισμών είναι μέσα από την κατάλληλη προετοιμασία αλλά και από τους κατάλληλους χειρισμούς να περιορίσουν τον αριθμό των περιστατικών που μπορεί να συμβούν. Η προετοιμασία αυτή και οι χειρισμοί είναι ένα αποτέλεσμα που ο κάθε οργανισμός παίρνει μέσα από τις αναλύσεις κινδύνου που πραγματοποιεί λαμβάνοντας πάντα ως δεδομένο ότι υπάρχει κάποιος υπολειπόμενος κίνδυνος που θα παραμένει ακόμα και μετά την εφαρμογή ελέγχων, ακόμα και με αυτόν τον υπολειπόμενο κίνδυνο ο εντοπισμός τυχόν παραβιάσεων που μπορεί να εξελιχθούν σε σοβαρά περιστατικά ή μη κρίνεται απαραίτητος από τους οργανισμούς. Υπάρχουν διάφορες κλίμακες σοβαρότητας που μπορεί να θεωρηθεί ένα συμβάν, αυτά τα επίπεδα διαφέρουν ως προς την αντιμετώπιση και την σοβαρότητα του συμβάντος. Με γνώμονα την σοβαρότητα ο οργανισμός μπορεί να περιορίσει τον αντίκτυπο του

συμβάντος μέχρι την ανάκαμψη του, κατά την διάρκεια της ανάκαμψης αρκετά συχνά η διαδικασία γυρνάει πίσω στην φάση της ανίχνευσης και της ανάλυσης γιατί για παράδειγμα αν έχει δεχτεί ένας οργανισμός επίθεση με κακόβουλο λογισμικό η διαδικασία θέλει να ξανά ελέγξει αν έχει μολυνθεί κάποιος επιπλέον κεντρικός υπολογιστής. Με την ολοκληρωμένη αντιμετώπιση του περιστατικού ο οργανισμός είναι υποχρεούμενος να εκδώσει αναφορά με λεπτομέρειες για τα αίτια, το κόστος αλλά και τα νέα μέτρα που θα πάρει για να αποφύγει μελλοντικά παρόμοια περιστατικά.

Η διαδικασία αντιμετώπισης του περιστατικού περνάει από μερικές φάσεις. Η πρώτη φάση αποτελείται από την ίδρυση ή επιλογή μιας ομάδας αντιμετώπισης περιστατικών ασφαλείας που θα είναι εκπαιδευμένη πάνω στα δεδομένα του συγκεκριμένου οργανισμού που εργάζονται αλλά και πλήρως εξοπλισμένη, αυτή η φάση λέγεται προετοιμασία (De Muynck & Portesi, 2016). Η δεύτερη φάση είναι της Ανίχνευσης και Ανάλυσης όπου μέσα από αυτήν την φάση ο οργανισμός εφαρμόζει διάφορα σύνολα από ελέγχους αλλά και την ταξινόμηση του συμβάντος, ανάλογα την σοβαρότητα του. Η τρίτη φάση είναι ουσιαστικά ο περιορισμός του συμβάντος και η τέταρτη, αφού αντιμετωπιστεί πλήρως και εκδοθεί η σχετική αναφορά, αντλούνται τα σχετικά νέα μέτρα και λαμβάνονται υπόψιν τα διδάγματα για μελλοντικά περιστατικά. Όλη αυτή η διαδικασία ονομάζεται κύκλος ζωής απόκρισης του περιστατικού (Incident Response Life Cycle) και δίνεται πιο αναλυτικά από το NIST (Cichonski, Millar, Grance, & Scarfone, 2012) όπου φαίνεται και στην Εικόνα 1:



Εικόνα 1: Κύκλος ζωής απόκρισης περιστατικού

Preparation (Προετοιμασία)

Η κουλτούρα της ασφάλειας αλλά και οι διαδικασίες βασίζονται σε μεγαλύτερο βαθμό στην προετοιμασία των οργανισμών, εστιάζοντας κυρίως στο να είναι όσο το δυνατόν πιο έτοιμοι στην ανταπόκριση, την αντιμετώπιση αλλά και την αποτροπή ενός περιστατικού. Απώτερος στόχος είναι η διασφάλιση ότι όλα τα αγαθά του οργανισμού δεν διατρέχουν κίνδυνο. Στο κομμάτι αυτό παίζει μεγάλο ρόλο η ομάδα αντιμετώπισης περιστατικών ασφαλείας για την καλύτερη πρόληψη.

Detection and Analysis (Ανίχνευση και Ανάλυση)

Οι οργανισμοί θα πρέπει να είναι έτοιμοι να αντιμετωπίσουν και να διαχειριστούν οποιοδήποτε περιστατικό. Γενικότερα, το εύρος των περιστατικών που μπορεί να αντιμετωπίσει ένας οργανισμός είναι τεράστιο, οπότε είναι φύση αδύνατο να υπάρξουν οδηγίες βήμα προς βήμα για τον χειρισμό τους. Ωστόσο, η οδηγία του ENISA δίνει ονομαστικά κάποια συμβάντα που έχουν κοινούς φορείς επίθεσης: External/Removable Media, Attrition, Web, Email, Impersonation, Improper Usage, Loss or Theft of Equipment. Η ανίχνευση και ανάλυση των περιστατικών αποτελεί μια αρκετά δύσκολη διαδικασία αλλά και μια διαδικασία, η οποία δεν είναι εγγυημένη. Για παράδειγμα, παρατηρούνται συχνά ενδείξεις μέσα στους οργανισμούς, που ενδέχεται να είναι λανθασμένες, όπως π.χ. παράπονα του χρήστη ότι δεν είναι διαθέσιμος ο διακομιστής ή κάποιο σύστημα ανίχνευσης εισβολής που ίσως παράγει ψευδώς θετικό αποτέλεσμα.

Όταν το περιστατικό αναλύεται κι ταξινομείται ανάλογα με την ιεραρχία τότε, σε αυτή την φάση της διαδικασίας, ειδοποιούνται τα κατάλληλα άτομα ή φορείς για να συνεισφέρουν στην αντιμετώπιση. Οι πολιτικές αντιμετώπισης συμβάντων περιλαμβάνουν μέσα στις διατάξεις τους την αναφορά των περιστατικών, δηλαδή τι πρέπει να αναφέρεται και σε ποιον.

Containment, Eradication and Recovery (Περιορισμός, Εξάλειψη και Ανάκτηση)

Για λόγους ασφαλείας κρίνεται ότι τα περιστατικά πρέπει να περιορίζονται έγκαιρα, ιδίως πριν προκαλέσουν ζημιές, οι οποίες ενδεχομένως αποτελέσουν σημαντικό κόστος για τον οργανισμό. Αναλυτικότερα, κρίνεται ότι πρέπει να περιορίζονται νωρίς συγκριτικά με το χρονικό διάστημα, όπου διαπιστώθηκε η ανίχνευση τους. Οι στρατηγικές που χρησιμοποιούνται για τον περιορισμό αυτών χρειάζεται πολλές

φορές να προσαρμόζονται ανάλογα με την κατάσταση και τις εκάστοτε κινήσεις που απαιτούνται.

Επίσης, πολύ σημαντικός παράγοντας είναι και ο χρόνος λήψης γρήγορων και ουσιαστικών αποφάσεων, όπως π.χ. η αποσύνδεση από το δίκτυο ή και αποσύνδεση ορισμένων λειτουργιών. Αυτές οι αποφάσεις είναι πιο εύκολο να ληφθούν όταν υπάρχουν ανεπτυγμένες στρατηγικές στο οργανισμό για τον περιορισμό των συμβάντων. Κάθε οργανισμός κατά την διαδικασία του περιορισμού ορίζει κάποιους κινδύνους ως αποδεκτούς και πάνω σε αυτούς στηρίζει τις στρατηγικές περιορισμού και αντιμετώπισης.

Η συλλογή διατηρούμενων αποδεικτικών στοιχείων είναι μια διαδικασία του περιορισμού του συμβάντος που βοηθάει στην αντιμετώπιση του. Η συγκεκριμένη συλλογή βασίζεται σε ειδικά νομικά πλαίσια και δεν πρέπει να χρησιμοποιούνται μέθοδοι που ενδεχομένως να παραβιάζουν οποιαδήποτε νομοθεσία, ώστε να αποτελέσει αποδεικτικό στοιχείο στο δικαστήριο. Αυτά τα αποδεικτικά στοιχεία, πέρα από ότι κρίνονται αρκετά χρήσιμα για την επίλυση του προβλήματος, δηλαδή τον περιορισμό και την αντιμετώπιση του συμβάντος λαμβάνονται υπόψη ανά πάσα στιγμή από τα άτομα της ομάδας αντιμετώπισης κατά την διαδικασία του περιορισμού.

Post-Incident Activity (Δραστηριότητα μετά το περιστατικό)

Ένα αρκετά σημαντικό κομμάτι της αντιμετώπισης των περιστατικών είναι η εκμάθηση και η βελτίωση, δηλαδή τα διδάγματα θα αφήσει το γεγονός καθαυτό στον οργανισμό και στην ομάδα αντιμετώπισης που έχει ορίσει ο οργανισμός. Για όλες τις ομάδες τέτοιου τύπου κρίνεται απαραίτητο να μπορούν να βελτιώνονται συνεχώς και να είναι σε θέση να αντιμετωπίσουν νέες απειλές κατά της ασφαλείας. Η διεξαγωγή συναντήσεων για την άντληση των παραδειγμάτων, ανεξάρτητα από την σοβαρότητα του περιστατικού, με όλα τα εμπλεκόμενα μέρη είναι εξαιρετικά χρήσιμη και στοχεύει στην αναβάθμιση των μέτρων ασφαλείας αλλά και βελτίωση της διαδικασίας χειρισμού του περιστατικού στο μέλλον. Αυτές οι συναντήσεις ποικίλλουν σε διάρκεια ανάλογα την σοβαρότητα του περιστατικού ενώ κατά τη διάρκεια τους θα πρέπει να τίθενται ερωτήματα του τύπου:

1. Τι συνέβη ακριβώς και ποιες ώρες;

2. Ποιος ήταν ο βαθμός απόδοσης τόσο του προσωπικού όσο και της διοίκησης στην αντιμετώπιση του συμβάντος;
3. Ήταν τεκμηριωμένες οι διαδικασίες που ακολουθήθηκαν; Ήταν επαρκείς;
4. Ποιες πληροφορίες χρειάζονταν νωρίτερα;
5. Ελήφθησαν μέτρα ή έγιναν ενέργειες που ενδεχομένως να εμποδίσαν την ανάκαμψη;
6. Ποιες ενέργειες του προσωπικού και της διοίκησης ίσως διαφοροποιούνταν σε μελλοντικό παρόμοιο περιστατικό;
7. Πώς θα μπορούσε να βελτιωθεί η ανταλλαγή πληροφοριών με άλλους οργανισμούς;
8. Ποιες διορθωτικές ενέργειες μπορούν να αποτρέψουν παρόμοια περιστατικά στο μέλλον;
9. Ποιοι πρόδρομοι ή δείκτες θα πρέπει να παρακολουθούνται στο μέλλον για τον εντοπισμό παρόμοιων περιστατικών;
10. Ποια πρόσθετα εργαλεία ή πόροι χρειάζονται για τον εντοπισμό, την ανάλυση και τον μετριασμό μελλοντικών συμβάντων;

Σε αρκετές περιπτώσεις, ο βαθμός επιτυχίας της ομάδας αντιμετώπισης περιστατικών που έχει ορίσει οργανισμός εξαρτάται από το εάν τα δεδομένα που συλλέγονται και διατηρούνται συνδέονται άμεσα και παίζουν καθοριστικό ρόλο στην επιτυχή αντιμετώπιση τους.

2.2.4 Διαδικασίες αντιμετώπισης και διαχείρισης περιστατικού ασφαλείας ITIL

Η βιβλιοθήκη ηλεκτρονικών υποδομών (ITIL) ουσιαστικά είναι ένα άλλο πλαίσιο για την διαχείριση υπηρεσιών που ευθυγραμμίζεται με το ISO/IEC 27000 (Brewster, Griffiths, Lawes, & Sansbury, 2012). Στην παρούσα εργασία θα ασχοληθούμε με το κομμάτι της διαχείρισης συμβάντων. Το ITIL πλαίσιο είναι αρκετά γενικό και μπορεί να ευθυγραμμιστεί με κάθε είδους οργανισμό.

Το ITIL (Brewster, Griffiths, Lawes, & Sansbury, 2012) χρησιμοποιεί τους ακόλουθους ορισμούς ως εξής:

Υπηρεσία: Μέσο παροχής αξίας που προσφέρεται σε πελάτες για να τους διευκολύνει τα αποτελέσματα που αναζητούν να πετύχουν χωρίς τη ιδιοκτησία και κατοχή δαπανών και κινδύνων.

Διαχείριση υπηρεσιών: Αποτελείται από ένα σύνολο εξειδικευμένων οργανωτικών δυνατοτήτων που προσφέρεται σε πελάτες σε μορφή υπηρεσιών.

Λειτουργία: Δραστηριότητες και διαδικασίες που πραγματοποιούνται από μια ομάδα ή μια ομάδα ανθρώπων και τα εργαλεία τους.

Διαδικασία: Είναι ένα σύνολο δομημένων δραστηριοτήτων που έχουν δημιουργηθεί για την επίτευξη συγκεκριμένων στόχων. Από τα βασικά χαρακτηριστικά της διαδικασίας είναι ότι παίρνει μία ή παραπάνω από μία εισόδους και τις μετατρέπει σε συγκεκριμένες εξόδους, καθώς και ότι περιλαμβάνει ρόλους, ευθύνες, εργαλεία και διαχειριστικούς ελέγχους που χρειάζονται για το αξιόπιστο αποτέλεσμα. Τέλος, μια διαδικασία έχει τη δυνατότητα να ορίσει πρότυπα, πολιτικές κατευθυντήριες γραμμές, δραστηριότητες αλλά και οδηγίες εργασίας, εάν κριθεί απαραίτητο.

Επίσης δίνονται ορισμοί για διαδικασίες και λειτουργίες στο πλαίσιο ITIL για την διαχείριση συμβάντων ως εξής (Brewster, Griffiths, Lawes, & Sansbury, 2012):

Διαχείριση Διαθεσιμότητας: Είναι απαραίτητη για τους οργανισμούς και αποτελεί προληπτική διαδικασία. Αυτή η διαδικασία εκτός από τις δραστηριότητες της προετοιμασίας της διατήρησης σχεδίου διαθεσιμότητας και την παρακολούθηση των επιπέδων διαθεσιμότητας αποτελεί παράλληλα και βοήθεια στη διερεύνηση και επίλυση περιστατικών που σχετίζονται με τη διαθεσιμότητα. Το τελευταίο κομμάτι της είναι ένα αντιδραστικό σκέλος που σχετίζεται με άλλες διαδικασίες, όπως της συνέχειας της υπηρεσίας πληροφορικής, της ασφάλειας πληροφοριών, της διαχείρισης συμβάντων αλλά και προβλημάτων.

Διαχείριση Συνέχειας Υπηρεσιών Πληροφορικής: Αφορά βασικά συστήματα σε περιπτώσεις αποτυχίας. Σκοπός της είναι η διασφάλιση αποκατάστασης των συστημάτων και υπηρεσιών πληροφορικής σε περίπτωση ενός συμβάντος εντός καθορισμένων χρονοδιαγραμμάτων. Η διαδικασία της Διαχείριση Συνέχειας Υπηρεσιών Πληροφορικής σχετίζεται άμεσα με την διαθεσιμότητα και τη διαχείριση ασφάλειας πληροφοριών, όπως ορίζεται στη συνέχεια:

Διαχείριση Ασφάλειας Πληροφοριών: Αφορά την επιβολή της πολιτικής ασφάλειας, κάτι το οποίο πρέπει όλα τα μέλη του οργανισμού να γνωρίζουν και να έχουν άμεση πρόσβαση. Παράλληλα, το σύστημα που υπάρχει στη συγκεκριμένη περίπτωση είναι το ISMS. Η συγκεκριμένη διαδικασία σχετίζεται με την

διαθεσιμότητα, με το πρόβλημα και τη διαχείριση της συνέχειας των υπηρεσιών πληροφορικής.

Γραφείο Εξυπηρέτησης: Πρόκειται για μια λειτουργία, στην οποία εντάσσεται μια πολύ σημαντική διαδικασία, η διαχείριση συμβάντων. Οι χρήστες IT στους οργανισμούς οφείλουν να έχουν ως μοναδικό σημείο επαφής και επικοινωνίας το γραφείο εξυπηρέτησης για την καταγραφή περιστατικών ή και την αναφορά συμβάντων. Το γραφείο εξυπηρέτησης είναι υπεύθυνο για τα περιστατικά για όλη την διάρκεια του κύκλου ζωής τους, ανεξαρτήτως των υπαλλήλων που εργάζονται πάνω στο συγκεκριμένο συμβάν για την επίλυση του. Είναι απαραίτητη η εκπαίδευση και η βελτίωση των δεξιοτήτων τους με στόχο την απόκτηση περαιτέρω γνώσεων, αναφορικά με την εκτέλεση διαχείρισης περιστατικών, ώστε να επιτυγχάνεται αποτελεσματικά και αποδοτικά η αντιμετώπιση τους.

Διαχείριση Συμβάντων: Το περιστατικό σε αυτή την περίπτωση ορίζεται ως μια μη προγραμματισμένη διακοπή ή μείωση της ποιότητας μιας υπηρεσίας πληροφορικής. Επιπρόσθετα, ενδέχεται να πρόκειται για την αποτυχία ενός στοιχείου που δεν έχει προλάβει να επηρεάσει την υπηρεσία. Η διαδικασία αφορά την αντιμετώπιση περιστατικών. Κάθε οργανισμός είναι απαραίτητο να διαθέτει μια τέτοια ομάδα, ιδιαίτερα οι μεγάλοι οργανισμοί, όπου χρειάζεται να απασχολούν αποκλειστικές ομάδες, διαθέσιμες ανά πάσα στιγμή να διαχειριστούν μεγάλα περιστατικά.

Αυτή η διαδικασία απαιτεί την κατανομή πόρων για τον μετριασμό των επιπτώσεων και τη διατήρηση της ποιότητας υπηρεσίας συμβάντων, σύμφωνα με τις επιχειρηματικές προτεραιότητες, με απώτερο στόχο την έγκαιρη αποκατάσταση των ζημιών σε υπηρεσίες και τον περιορισμό των επιπτώσεων. Μέσα από αυτήν την διαχείριση των συμβάντων μπορεί να προκύψουν διάφοροι τομείς που χρειάζονται μεγαλύτερη ασφάλεια ή ακόμα και βελτίωση σε κάποιο κομμάτι τους.

Κάθε περιστατικό που αναφέρεται πρέπει να περνάει από την συγκεκριμένη διαδικασία με την εξής σειρά: ανίχνευση, καταγραφή, κατηγοριοποίηση και ακριβής ιεράρχηση, η οποία κρίνεται εξαιρετικά σημαντική. Στην περίπτωση που ένα περιστατικό κριθεί σημαντικό, τότε η εκκινεί η διαδικασία μείζονος περιστατικού με το ενδεχόμενο να χρειαστεί εντονότερη κλιμάκωση. Η λειτουργική κλιμάκωση υφίσταται όταν το γραφείο εξυπηρέτησης δεν έχει τα μέσα, την γνώση και τις δεξιότητες για την επίλυση του περιστατικού ή δεν έχει καταφέρει να τηρήσει το

χρονοδιάγραμμα επίλυσης του. Η ιεραρχική κλιμάκωση υφίσταται όταν το προφίλ ενός περιστατικού πρέπει να αναδειχθεί εντός του οργανισμού πληροφορικής και των επιχειρηματικών περιοχών. Γενικά όλων των τύπων τα περιστατικά πρέπει να ερευνώνται και στη συνέχεια να επιλύονται. Η διαδικασία της διαχείρισης συμβάντων συνδέεται με την διαδικασία διαχείρισης προβλημάτων, όπως ορίζεται παρακάτω.

Διαχείριση Προβλημάτων: Πρόβλημα ορίζεται η αιτία ενός ή παραπάνω περιστατικών. Η συγκεκριμένη διαδικασία αναφέρεται στην ανάλυση της βασικής αιτίας αλλά ασχολείται και με την επίλυση των προβλημάτων. Είναι τόσο προληπτική όσο και αντιδραστική η συγκεκριμένη διαδικασία διαχείρισης προβλημάτων, καθώς επιδιώκει να αποτρέψει προβλήματα και περιστατικά μειώνοντας τον αντίκτυπο τους. Σε αυτές τις περιπτώσεις είναι σημαντικό να καταγράφονται όλες οι λεπτομέρειες του προβλήματος που προκύπτει και στη συνέχεια να κατηγοριοποιείται και να ιεραρχείται το ίδιο το πρόβλημα. Η ιεράρχηση του προβλήματος ακολουθεί τον ίδιο τρόπο ιεράρχησης με τον αντίστοιχο των περιστατικών. Η βασική αιτία θα πρέπει να εντοπίζεται κατά την φάση της διερεύνησης και της διάγνωσης και να επιλύεται μόλις προκύψει μια μόνιμη επιδιόρθωση. Στην περίπτωση που το πρόβλημα κριθεί μείζον ακολουθεί επανεξέταση του μείζονος προβλήματος.

Διαχείριση Γεγονότων: Ένα τυχαίο συμβάν μπορεί να έχει διάφορες μορφές όπως ενημερωτικό, προειδοποιητικό ή εξαίρεση. Αυτή η διαδικασία αναφέρεται στον χειρισμό μηνυμάτων και αντιδρά σε εξαιρέσεις. Επίσης, είναι παρόμοια με τη διαδικασία διαχείρισης περιστατικών ενώ το ιδανικό σενάριο υποδεικνύει ότι πρέπει να είναι αυτοματοποιημένη. Κατά τη διάρκεια της συγκεκριμένης διαδικασίας τα συμβάντα μπορεί να αποτελέσουν εναύσματα για τη διαδικασία διαχείρισης συμβάντων.

2.2.5 Το πρότυπο ISO /IEC 27001-2013

Το ISO/IEC 27001:2013 (ISO/IEC 27001:2013, 2013) περιέχει τις απαιτήσεις για τη δημιουργία, την εφαρμογή, τη διατήρηση και τη βελτίωση ενός συστήματος διαχείρισης ασφάλειας πληροφοριών. Παράλληλα, περιλαμβάνει και τις απαιτήσεις για την αξιολόγηση και αντιμετώπιση κινδύνων ασφάλειας πληροφοριών. Τα παραπάνω στοιχεία είναι γενικά και απευθύνονται σε όλους τους οργανισμούς, ανεξαρτήτως τύπου, μεγέθους ή φύσης.

1) Πλαίσιο του οργανισμού

1.1 Κατανόηση του οργανισμού και του πλαισίου του

Καθορίζονται εξωτερικά και εσωτερικά ζητήματα του οργανισμού, σχετικά με τον σκοπό αλλά και με την ικανότητα να πετύχουν τα αποτελέσματα που επιθυμούν, αναφορικά με το σύστημα διαχείρισης.

1.2 Κατανόηση των αναγκών και των προσδοκιών των ενδιαφερομένων

Προσδιορίζει τα ενδιαφερόμενα μέρη, καθώς και τις απαιτήσεις τους.

1.3 Προσδιορισμός του πεδίου εφαρμογής του συστήματος διαχείρισης ασφάλειας πληροφοριών

Ουσιαστικά προχωρά σε προσδιορισμό και καθορισμό των ορίων της δυνατότητας εφαρμογής του συστήματος διαχείρισης ασφάλειας πληροφοριών με σκοπό να συμπεράνει και να καθορίσει το πεδίο εφαρμογής του.

2) Ηγεσία

2.1 Ηγεσία και δέσμευση

Η διοίκηση του κάθε οργανισμού χρειάζεται τόσο να δείχνει όσο και να κατέχει ηγετικό ρόλο και να δεσμεύεται αναφορικά με το σύστημα διαχείρισης ασφάλειας πληροφοριών. Το γεγονός αυτό μπορεί να επιτευχθεί με τη διασφάλιση ότι η πολιτική της ασφάλειας πληροφοριών συμβαδίζει με τη στρατηγική κατεύθυνση του οργανισμού, με την ενσωμάτωση των απαιτήσεων του συστήματος στις διαδικασίες του οργανισμού, με την διαθεσιμότητα των πόρων που χρειάζεται το σύστημα διαχείρισης ασφάλειας πληροφοριών, καθώς και με την επίτευξη των επιδιωκόμενων αποτελεσμάτων από το σύστημα αυτό. Επίσης, διασφαλίζεται και από την καθοδήγηση και υποστήριξη προσώπων, την προώθηση της συνεχούς βελτίωσης αλλά και την υποστήριξη άλλων ηγετικών ρόλων για την επίδειξη ηγεσίας.

2.2 Πολιτική

Αναφέρεται στην ανώτατη διοίκηση, η οποία θεσπίζει την πολιτική ασφάλειας πληροφοριών.

2.3 Οργανωτική ρόλοι, αρμοδιότητες και εξουσίες

Και σε αυτό το κομμάτι, η ανώτατη διοίκηση εξασφαλίζει ότι γίνεται ανάθεση ευθυνών και αρχών για ρόλους που σχετίζονται με την ασφάλεια. Για παράδειγμα, διασφαλίζεται ότι το σύστημα διαχείρισης ασφάλειας πληροφοριών συμμορφώνεται με τις απαιτήσεις αυτού του διεθνές προτύπου

και υπάρχει υποβολή εκθέσεων, που σχετίζεται με την απόδοση του συστήματος διαχείρισης ασφάλειας πληροφοριών.

3) Προγραμματισμός

3.1 Δράσεις για την αντιμετώπιση κινδύνων ασφάλειας

3.1.1 Γενικά

Κατά την φάση του σχεδιασμού του συστήματος εξετάζονται τόσο τα ζητήματα της κατανόησης του οργανισμού και του πλαισίου του όσο και οι απαιτήσεις της ενότητας «Κατανόηση των αναγκών και των προσδοκιών των ενδιαφερομένων».

3.1.2 Αξιολόγηση κινδύνου ασφάλειας πληροφοριών

Σε αυτή τη φάση ορίζονται και εφαρμόζονται διαδικασίες αξιολόγησης του κινδύνου ασφάλειας πληροφοριών. Ουσιαστικά καθορίζονται κριτήρια κινδύνου για την ασφάλεια των πληροφοριών, διασφαλίζουν ότι η αξιολόγηση του κινδύνου παράγει έγκυρα και συγκρίσιμα αποτελέσματα, προσδιορίζει τους κινδύνους ασφάλειας πληροφοριών, τους αναλύει αλλά και τους αξιολογεί.

3.1.3 Αντιμετώπιση κινδύνου ασφάλειας πληροφοριών

Ορίζονται και εφαρμόζονται διαδικασίες αντιμετώπισης κινδύνου ασφάλειας πληροφοριών, όπως η επιλογή κατάλληλου σχεδίου αντιμετώπισης, λαμβάνοντας υπόψη τα αποτελέσματα της αξιολόγησης κινδύνου. Παράλληλα, καθορίζονται όλοι οι έλεγχοι που είναι απαραίτητοι, να γίνει σύγκριση μεταξύ τους, να γίνει σύνταξη δήλωσης που περιέχει του απαραίτητους ελέγχους, να διαμορφωθεί σχέδιο αντιμετώπισης κινδύνου και να ληφθεί ταυτόχρονα έγκριση των κατόχων κινδύνου για το σχέδιο αντιμετώπισης αλλά και του κινδύνου που θα αποδεχτούν.

3.2 Στόχοι ασφάλειας πληροφοριών και σχεδιασμός τους

Γίνεται καθορισμός των στόχων σε σχετικές λειτουργίες. Αυτοί οι στόχοι πρέπει να είναι συνεπείς, μετρήσιμοι, να έχουν ληφθεί υπόψη οι ισχύουσες απαιτήσεις και τα αποτελέσματα από την αξιολόγηση θεραπείας κίνδυνου. Στη συνέχεια, χρειάζεται να κοινοποιηθούν και να επικαιροποιηθούν. Επίσης, διατηρούνται τεκμηριωμένες και συγκεκριμένες πληροφορίες όσον αφορά τους στόχους τις ασφάλειας πληροφοριών, όπως το τι θα προκύψει

μελλοντικά, ποιοι πόροι απαιτούνται, ποιος θα είναι ο υπεύθυνος, πότε θα ολοκληρωθεί αλλά και πως θα πραγματοποιηθεί αξιολόγηση των αποτελεσμάτων.

4) Υποστήριξη

4.1 Πόροι

Παροχή των απαιτούμενων πόρων από τον οργανισμό για την δημιουργία, την εφαρμογή, τη συντήρηση και τη συνεχή βελτίωση τους.

4.2 Ικανότητα

Από τον οργανισμό καθορίζεται η αποδεδειγμένη ικανότητα των υπαλλήλων που εκτελούν την εργασία. Διασφαλίζεται ότι είναι ικανά τα άτομα έχοντας ως βάση είτε την κατάλληλη εκπαίδευση είτε εμπειρία, να λαμβάνονται μέτρα, παράλληλα, για την απόκτηση της κατάλληλης ικανότητας αξιολόγησης της αποτελεσματικότητας των ενεργειών που εκτελούνται. Επιπρόσθετα, να διατηρούνται οι κατάλληλες τεκμηριωμένες πληροφορίες ως απόδειξη.

4.3 Ευαισθητοποίηση

Τα άτομα που εκτελούν εργασίες στον οργανισμό οφείλουν να γνωρίζουν την πολιτική ασφάλειας των πληροφοριών του, καθώς και ποια είναι η συμβολή τους στην αποτελεσματικότητα του συστήματος. Ταυτόχρονα, είναι απαραίτητο να είναι γνώστες και των πλεονεκτημάτων από τη βελτιωμένη απόδοση ασφάλειας πληροφοριών αλλά και των προβλεπόμενων συνεπειών, σε περίπτωση μη συμμόρφωσης με τις απαιτήσεις.

4.4 Επικοινωνία

Καθορίζονται οι ανάγκες για εσωτερικές και εξωτερικές επικοινωνίες που σχετίζονται με το σύστημα διαχείρισης ασφάλειας πληροφοριών. Αυτές οι ανάγκες αναφέρονται περισσότερο στις πληροφορίες που πρέπει να επικοινωνήσει, πότε πρέπει να γίνει αυτή η ενέργεια, με ποιον αλλά και τι διαδικασίες χρειάζονται για να πραγματοποιηθεί αυτή η επικοινωνία.

4.5 Τεκμηριωμένες Πληροφορίες

4.5.1 Γενικά

Το σύστημα περιέχει τεκμηριωμένες πληροφορίες που απαιτούνται από το διεθνές πρότυπο αλλά και τεκμηριωμένες πληροφορίες που έχουν προσδιοριστεί ως απαραίτητες από τον οργανισμό για την αποτελεσματικότητα του συστήματος.

4.5.2 Δημιουργία και ενημέρωση

Ο οργανισμός φροντίζει κατά τη δημιουργία και την ενημέρωση τεκμηριωμένων πληροφοριών να διασφαλίζεται η ταυτότητα, η περιγραφή, η μορφή και ο έλεγχος ακαταλληλότητας.

4.5.3 Έλεγχος τεκμηριωμένων πληροφοριών

Από το διεθνές πρότυπο και από το σύστημα διαχείρισης ασφάλειας πληροφοριών απαιτούνται τεκμηριωμένες πληροφορίες, οι οποίες ελέγχονται για να διασφαλιστεί ότι το σύστημα είναι διαθέσιμο και κατάλληλο, όποτε και αν χρειάζεται και ότι προστατεύεται επαρκώς. Παράλληλα, για το έλεγχο οι δραστηριότητες περιλαμβάνουν διανομή, αποθήκευση, έλεγχος και διατήρηση.

5) Λειτουργία

5.1 Λειτουργικός σχεδιασμός και έλεγχος

Στον οργανισμό σχεδιάζονται, εφαρμόζονται και ελέγχονται οι διαδικασίες που είναι απαραίτητες για την ικανοποίηση των απαιτήσεων ασφάλειας πληροφοριών. Ακόμα εφαρμόζονται σχέδια για την επίτευξη των στόχων που έχουν τεθεί.

Επιπρόσθετα, στον οργανισμό διατηρούνται τεκμηριωμένες πληροφορίες για την επιβεβαίωση ότι οι διαδικασίες έχουν υλοποιηθεί ακριβώς έτσι όπως έχουν σχεδιαστεί. Ελέγχονται οι προγραμματισμένες αλλαγές με σκοπό τη λήψη μέτρων για τον μετριασμό των επιπτώσεων, διασφαλίζοντας παράλληλα, ότι οι διαδικασίες που έχουν ανατεθεί σε εξωτερικούς συνεργάτες καθορίζονται και ελέγχονται.

5.2 Αξιολόγηση κινδύνου για την ασφάλεια πληροφοριών

Πραγματοποιούνται αξιολογήσεις κινδύνου από τον οργανισμό για την ασφάλεια των πληροφοριών σε συγκεκριμένα χρονικά διαστήματα, όταν και όπου προτείνεται και διατηρούνται τεκμηριωμένες πληροφορίες για τα αποτελέσματα που προκύπτουν.

5.3 Αντιμετώπιση κινδύνου ασφάλειας πληροφοριών

Εφαρμόζεται το σχέδιο αντιμετώπισης κινδύνου ασφάλειας πληροφοριών και διατηρούνται τεκμηριωμένες πληροφορίες, που σχετίζονται με τα αποτελέσματα της αντιμετώπισης της.

6) Αξιολόγηση Απόδοσης

6.1 Παρακολούθηση, μέτρηση, ανάλυση και αξιολόγηση

Αξιολογούνται οι επιδόσεις ασφάλειας πληροφοριών για την αποτελεσματικότητα του συστήματος. Κατά τη διάρκεια της αξιολόγησης καθορίζεται τι πρέπει να παρακολουθείται και να μετρείται. Ως εκ τούτου, ελέγχονται και οι μέθοδοι παρακολούθησης, μέτρησης, ανάλυσης και αξιολόγησης. Επίσης, ορίζεται πότε θα πραγματοποιηθεί η παρακολούθηση και μέτρηση, ποιος θα τα αναλάβει αλλά και ποιος θα αναλύσει και θα αξιολογήσει αυτά τα αποτελέσματα. Για όλα τα παραπάνω ο οργανισμός χρησιμοποιεί τεκμηριωμένες πληροφορίες ως απόδειξη.

6.2 Εσωτερικός Έλεγχος

Διενεργούνται εσωτερικοί έλεγχοι σε συγκεκριμένα χρονικά διαστήματα για την παραγωγή πληροφοριών σχετικά με το σύστημα διαχείρισης ασφάλειας πληροφοριών. Το σύστημα πρέπει να συμμορφώνεται με τις απαιτήσεις του οργανισμού και το διεθνές πρότυπο. Ο οργανισμός πρέπει να σχεδιάζει να εφαρμόζει και να διατηρεί προγράμματα ελέγχου που θα λαμβάνουν υπόψη τη σημασία των σχετικών διαδικασιών και αποτελέσματα από προηγούμενους ελέγχους. Ακόμα στον εσωτερικό έλεγχο πρέπει να καθορίζονται σχετικά κριτήρια για κάθε πεδίο εφαρμογής, να επιλέγονται ελεγκτές και να διενεργούνται έλεγχοι που να διασφαλίζουν την ορθότητα των διαδικασιών συνολικά. Τέλος, θα πρέπει να διασφαλίζεται ότι τα αποτελέσματα των ελέγχων αναφέρονται στη διοίκηση και διατηρούνται τεκμηριωμένες πληροφορίες σαν αποδεικτικά στοιχεία.

6.3 Επισκόπηση της διοίκησης

Η ανώτατη διοίκηση πρέπει να επανελέγχει το σύστημα διαχείρισης ασφάλειας πληροφοριών ανά τακτά χρονικά διαστήματα, να διατηρεί την καταλληλότητα και την αποτελεσματικότητά του. Αυτοί οι επανέλεγχοι εξετάζουν η κατάσταση των ενεργειών, τις αλλαγές σε εξωτερικά και εσωτερικά ζητήματα, την ανατροφοδότηση σχετικά με τις αποδόσεις, τα σχόλια από τα ενδιαφερόμενα μέρη, τα αποτελέσματα της αξιολόγησης και τις ευκαιρίες για συνεχή βελτίωση. Για όλα τα παραπάνω διατηρούνται τεκμηριωμένες πληροφορίες ως απόδειξη των αποτελεσμάτων.

7) Βελτίωση

7.1 Μη συμμόρφωση και διορθωτικές ενέργειες

Στη μη συμμόρφωση ο οργανισμός αντιδρά και αξιολογεί την ανάγκη ανάληψης δράσης για να μην επαναληφθεί. Για να εφαρμοστούν οι δέουσες ενέργειες χρειάζεται επανεξέταση της αποτελεσματικότητας των διορθωτικών δράσεων και δημιουργία αλλαγών στο σύστημα. Αυτές οι ενέργειες πρέπει να συνάδουν με τις επιπτώσεις της μη συμμόρφωσης. Ταυτόχρονα, διατηρούνται και τεκμηριωμένες πληροφορίες ως απόδειξη για την φύση των μη συμμορφώσεων και των αποτελεσμάτων οποιασδήποτε διορθωτικής ενέργειας.

7.2 Συνεχής Βελτίωση

Ο οργανισμός φροντίζει για την βελτίωση της διαρκούς καταλληλότητας, επάρκειας και αποτελεσματικότητας του συστήματος.

2.2.6 Το πρότυπο ISO / IEC 27002-2022

Το ISO/IEC 27002:2022 (ISO/IEC 27002:2022, 2022) αποτελεί έναν κώδικα πρακτικής για τη διαχείριση της ασφάλειας πληροφοριών. Επίσης, θέτει κατευθυντήριες γραμμές για την έναρξη, την εφαρμογή, τη διατήρηση αλλά και τη βελτίωση της διαχείρισης της ασφάλειας πληροφοριών σε οργανισμούς. Το πρότυπο περιέχει 4 θέματα ελέγχων: τους οργανωτικούς ελέγχους, τους ελέγχους ανθρώπων, τους φυσικούς ελέγχους και τους τεχνικούς ελέγχους.

Επίσης, διαθέτει 11 στοιχεία ελέγχου παρακολούθησης, τα οποία είναι τα εξής: φυσικής ασφάλειας, ευφυΐα απειλών, διαχείριση διαμόρφωσης, διαγραφή πληροφοριών, απόκρυψη δεδομένων, πρόληψη διαρροής δεδομένων, δραστηριότητες παρακολούθησης, ασφάλεια πληροφοριών για χρήση υπηρεσιών icloud, φιλτράρισμα ιστού, ασφαλής κωδικοποίηση και ετοιμότητα της τεχνολογίας πληροφοριών και επικοινωνιών για επιχειρηματική συνέχεια. Τα συγκεκριμένα στοιχεία ελέγχου διαθέτουν 5 τύπους χαρακτηριστικών οι οποίοι είναι:

- Τύπος ελέγχου (προληπτικός, διορθωτικός)
- Ιδιότητες ασφάλειας πληροφοριών (εμπιστευτικότητα, ακεραιότητα, διαθεσιμότητα)
- Έννοιες κυβερνοασφάλειας (προσδιορισμός, προστασία, ανίχνευση, απόκριση, ανάκτηση)
- Επιχειρησιακές δυνατότητες (διακυβέρνηση, διαχείριση περιουσιακών στοιχείων)

- Τομείς ασφαλείας (διακυβέρνηση και οικοσυστήματα, προστασία, άμυνα, ανθεκτικότητα).

2.2.7 Το Πρότυπο ISO 27035-2016

Σύμφωνα με το ISO (ISO/IEC 27035-2:2016, 2016) υπάρχουν κάποιες βασικές έννοιες αλλά και φάσεις για την διαχείριση τυχών συμβάντων ασφάλειας πληροφοριών. Οι έννοιες αυτές συνδυάζονται με αρχές για να δημιουργήσουν μια αρκετά δομημένη προσέγγισή για τον εντοπισμό, την αναφορά την αξιολόγησή αλλά και την απόκριση σε συμβάντα, αποθηκεύοντας πληροφορίες για αυτά, με σκοπό την μελλοντική εφαρμογή των διδαγμάτων που εντοπίστηκαν.

Στην συνέχεια έρχεται το δεύτερο μέρος του συγκεκριμένου ISO (ISO/IEC 27035-2:2016, 2016), σύμφωνα με το οποίο αποτυπώνονται τα βήματα για την προετοιμασία και την αντιμετώπιση των περιστατικών αυτών. Οι οδηγίες αυτές διέπονται από δυο βασικά μέρη του μοντέλου «Φάσεις διαχείρισης συμβάντων ασφάλειας πληροφοριών», την φάση i) «Σχεδιασμός και προετοιμασία» και την φάση ii) «Διδάγματα που αντλήθηκαν» από το ISO/IEC 27035-1. Τα κύρια μέρη κατά το (ISO/IEC 27035-2:2016, 2016) από την φάση «Σχεδιασμός και προετοιμασία» είναι τα εξής:

Πολιτική διαχείρισης συμβάντων ασφάλειας πληροφοριών και δέσμευση της ανώτατης διοίκησης. οι πολιτικές ασφάλειας πληροφοριών, συμπεριλαμβανομένων εκείνων που σχετίζονται με τη διαχείριση κινδύνων, ενημερωμένες τόσο σε εταιρικό επίπεδο όσο και σε επίπεδο συστήματος, υπηρεσιών και δικτύου.

1. Σχέδιο διαχείρισης συμβάντων ασφάλειας πληροφοριών.
2. Ίδρυση ομάδας αντιμετώπισης περιστατικών (IRT).
3. Δημιουργία σχέσεων και συνδέσεων με εσωτερικούς και εξωτερικούς οργανισμούς.
4. Τεχνική και άλλη υποστήριξη (συμπεριλαμβανομένης της οργανωτικής και επιχειρησιακής υποστήριξης).
5. Ενημερώσεις και εκπαίδευση για τη διαχείριση συμβάντων ασφάλειας πληροφοριών.
6. Δοκιμές σχεδίου διαχείρισης συμβάντων ασφάλειας πληροφοριών.

Ενώ από την δεύτερη φάση «Διδάγματα που αντλήθηκαν»

1. Ανάλυση σχεδίου διαχείρισης.
2. Εντοπισμός και εφαρμογή βελτιώσεων.
3. Ανασκόπηση για τον βαθμό αποτελεσματικότητας της διαδικασίας στην ανταπόκριση, την αξιολόγηση αλλά και την ανάκαμψη. Επίσης, εντοπισμός βελτιώσεων στην πολιτική ασφάλειας, στις διαδικασίες, στις εφαρμογές ελέγχου, στις μορφές αναφοράς αλλά και στις αξιολογήσεις κινδύνου.
4. Το ISIRT εφαρμόζει τις βελτιώσεις σε ολόκληρο το σύστημα.

Οι αρχές που παρουσιάζει το ISO/IEC 27035-1:2016 και το ISO/IEC 27035-2:2016 είναι αρκετά γενικές και καλύπτουν όλο το εύρος των οργανισμών (συμπεριλαμβάνονται και οι οργανισμοί που παρέχουν υπηρεσίες διαχείρισης συμβάντων ασφάλειας πληροφοριών), ανεξάρτητα από τον τύπο, το μέγεθος και την φύση τους, έχοντας τη δυνατότητα να προσαρμόσουν τις οδηγίες αυτές, ανάλογα με την κλίμακα που ανήκουν και εκπροσωπούν άλλα και με την κατάσταση κινδύνου της ασφάλειας πληροφοριών που αντιμετωπίζουν.

2.2.8 Πληροφορίες που καταγράφονται σε έντυπο αναφοράς συμβάντος/περιστατικού

Πληροφορίες που καταγράφονται σε έντυπο αναφοράς συμβάντος/περιστατικού συμφωνά με το ISO (ISO/IEC 27035-2:2016, 2016) είναι οι εξής :

1. Ημερομηνία πραγματοποίησης του συμβάντος.
2. Τα στοιχεία επικοινωνίας του ατόμου που έχει αναλάβει να συμπληρώσει το συγκεκριμένο έγγραφο.
3. Στοιχεία για την περιγραφή του συμβάντος όπως: τι συνέβη, πως και πότε.
4. Ακριβής ώρα και ημερομηνία για την πραγματοποίηση, την ανίχνευση αλλά και την αναφορά του συμβάντος.
5. Την χρονική διάρκεια του συμβάντος.
6. Την κατηγορία του συμβάντος, υποθετικό ή πραγματικό.
7. Τον τύπο του συμβάντος, αν δηλαδή πρόκειται για Φυσική καταστροφή, Φυσική ζημία, Κοινωνική ανακοπή, Αποτυχία υποδομής, Τεχνική αποτυχία, Κακόβουλο λογισμικό, Τεχνική επίθεση, Παραβίαση πολιτικής, Συμβιβασμός πληροφοριών.
8. Ποια αγαθά επηρεάζονται από αυτό το συμβάν: υλικό, λογισμικό, δεδομένα, επικοινωνίες, τεκμηρίωση, διαδικασίες.

9. Επιπτώσεις από το συμβάν: παραβίαση της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας.
10. Όταν πραγματοποιηθεί η επίλυση του συμβάντος να καταγραφούν τα εξής: Ημερομηνία έναρξης διερεύνησης συμβάντος, ημερομηνία λήξης συμβάντος, ημερομηνία λήξης του αντίκτυπου του συμβάντος, ημερομηνία λήξης διερεύνησης του συμβάντος.
11. Αναφορά και τοποθεσία του εντύπου διερεύνησης.
12. Πλήρης περιγραφή του επιτιθέμενου, στην περίπτωση που αυτό είναι εφικτό.
13. Οι συγκεκριμένες ενέργειες που ακολουθήθηκαν με σκοπό την επίλυση τους συμβάντος.
14. Οι μελλοντικές ενέργειες που σχεδιάζονται για την επίλυση του συμβάντος.
15. Τα συμπεράσματα που αντλήθηκαν από το περιστατικό.
16. Άτομα και οντότητες που είτε σχετίζονται είτε όχι και πρέπει να ενημερωθούν:
 - Διαχειριστής ασφάλειας πληροφοριών.
 - Διαχειριστής ιστοσελίδας.
 - Διαχειριστής ISIRT/CSIRT.
 - Διαχειριστής πληροφοριακών συστημάτων.
 - Προϊστάμενος της Διεύθυνσης που επηρεάζεται.
 - Προϊστάμενος του ατόμου που κάνει την αναφορά.
17. Εξωτερικά άτομα ή οντότητες του οργανισμού που είτε επηρεάζονται είτε όχι και πρέπει να ενημερωθούν.

2.2.9 Πιθανές συνέπειες κακής αντιμετώπισης και τι προσφέρει μια καλή αντιμετώπιση/διαχείριση

Η τεράστια εξέλιξη των οργανωμένων επιθέσεων πάνω στην ασφάλεια στον κυβερνοχώρο και όχι μόνο, αποτελεί μια ιδιαίτερη πρόκληση για τους οργανισμούς. Οι επιτιθέμενοι τις περισσότερες φορές διαθέτουν πολύ καλή εκπαίδευση και πλήρη γνώση του τι κάνουν, έχοντας στην διάθεση τους αρκετά εξελιγμένα εργαλεία και τεχνικές που μπορούν να χρησιμοποιήσουν εναντίον των οργανισμών. Για παράδειγμα είναι σε θέση να καταστρέψουν υποδομές, να καταργήσουν την πρόσβαση των οργανισμών σε δικές τους υποδομές και υπηρεσίες, να υποκλέψουν ευαίσθητες πληροφορίες, όπως πληροφορίες πνευματικής ιδιοκτησίας, εμπορικών μυστικών και δεδομένα πελατών. Επιθέσεις σαν και αυτές έχουν αρνητικές συνέπειες

στους οργανισμούς. Συνήθως αυτές οι συνέπειες συνοψίζονται σε απώλεια ανταγωνιστικού πλεονεκτήματος και παραγωγικότητας, φήμης και εμπιστοσύνης των πελατών, νομικές κυρώσεις αλλά και άμεση οικονομική ζημία (Ahmad, et al., 2012). Η έγκαιρη και ενδεδειγμένη αντιμετώπιση προστατεύει όλα τα παραπάνω, τα οποία ενδεχομένως να διακυβεύονται, σε ένα ασφαλές πλαίσιο ενώ σε αντίθετη περίπτωση, η αναποτελεσματική τους αντιμετώπιση θέτει σε κίνδυνο είτε κάποια είτε όλα τα παραπάνω.

2.3 Γνώσεις και αρχές που απαιτούνται από την ομάδα από τον διευθυντή της ομάδας και από τον οργανισμό για την διαχείριση περιστατικών

2.3.1 Απαιτούμενες αρχές, γνώσεις αλλά και εμπειρίες από την ομάδα αντιμετώπισης

Για την δημιουργία μιας ομάδας αντιμετώπισης SCIRT και κατά επέκταση σε μια ανάλογη μικρότερη κλίμακα, για την δημιουργία μια εσωτερικής ομάδας αντιμετώπισης περιστατικών ασφάλειας πληροφοριών σε έναν οργανισμό απαιτούνται συγκεκριμένες γνώσεις και αρχές που πρέπει να διαθέτουν τα μέλη των ομάδων. Ως εκ τούτου, σύμφωνα με το πανεπιστήμιο Carnegie Mellon (Haller, Merrell, Butkovic, & Willke, 2011) οι απαιτούμενες αρχές συνοψίζονται σε τέσσερις:

Τεχνική Αριστεία: Η ομάδα CSIRT/CERT θα πρέπει να έχει την δυνατότητα να διαθέτει τους πιο ενημερωμένους πόρους, ώστε να δίνει τις πιο εξειδικευμένες και ορθές συμβουλές διατηρώντας συνέχεια και σε βάθος χρόνου αυτό το πλεονέκτημα των πόρων. Μια πιθανή συνέπεια της τεχνικής αριστείας είναι συνήθως οι περιορισμένες δυνατότητες σε αριθμό, όπως για παράδειγμα η παροχή τρίτων υπηρεσιών, οι οποίες είναι πολύ καλής ποιότητας και γενικότερα προτιμώνται σε μεγαλύτερο βαθμό από την παροχή περισσότερων και κακής ποιότητας υπηρεσιών.

Εμπιστοσύνη: Θα πρέπει να υπάρχει τυφλή εμπιστοσύνη μεταξύ των οργανισμών και των ομάδων αντιμετώπισης περιστατικών ασφαλείας, ώστε να μπορούν να μοιράζονται χωρίς ενδοιασμούς δεδομένα μεταξύ τους. Η εμπιστοσύνη είναι θεμελιώδες συστατικό της συνεργασίας των δυο για τους οργανισμούς και συνήθως απαιτείται η επιβεβαίωση ότι η ομάδα αντιμετώπισης περιστατικών ασφαλείας μπορεί να ανταπεξέλθει στον χειρισμό ευαίσθητων πληροφοριών.

Αποδοτικότητα πόρων: Οι ομάδες οφείλουν να χρησιμοποιήσουν με τον αποτελεσματικότερο τρόπο τους διαθέσιμους πόρους. Επίσης, πρέπει να είναι σε

συνεχή ενημέρωση για να μπορούν να προσαρμοστούν σε οποιαδήποτε στιγμή, αναλύοντας πιθανές νέες απειλές και τις επιπτώσεις που θα μπορούσαν να έχουν.

Συνεργασία: Είναι απαραίτητο οι ομάδες να βρίσκονται σε συνεχή συνεργασία και με άλλους φορείς είτε είναι εθνικοί είτε κάποια άλλη ομάδα του ίδιου αντικειμένου, έχοντας βασικό γνώμονα την ευαισθησία ορισμένων δεδομένων. Πρωταρχικός σκοπός των συγκεκριμένων συνεργασιών είναι ο διαμοιρασμός γνώσεων και νέων πληροφοριών μεταξύ τους.

Σύμφωνα με το NIST, τα μέλη μια ομάδας πρέπει να έχουν πολύ καλές τεχνικές δεξιότητες, που σχετίζονται με τη διαχείριση συστημάτων (system administration), τη διαχείριση δικτύων (network administration), την τεχνική υποστήριξη, την ανίχνευση εισβολών. Τέλος, πρέπει έχουν άριστες γνώσεις και δεξιότητες, αναφορικά με την επίλυση προβλημάτων και την ικανότητα κριτικής σκέψης.

2.3.2 Απαιτούμενες γνώσεις και ενέργειες για υπεύθυνο ή διευθυντή της ομάδας και κατάλληλες ενέργειες για εκπαίδευση των υπαλλήλων αυτής

Ένα από τα μέλη της ομάδας είναι ο υπεύθυνος ή διευθυντής της ομάδας αντιμετώπισης περιστατικών ασφαλείας, ο οποίος είναι επιφορτισμένος με την επίβλεψη της διαδικασίας στο σύνολο της. Συνήθως, έχει στη διάθεση του έναν ή περισσότερους αναπληρωτές. Οι διευθυντές έχουν αρκετές αρμοδιότητες, εκ των οποίων μια από τις βασικότερες είναι ότι αποτελούν σύνδεσμο επικοινωνίας με την ανώτατη διοίκηση των οργανισμών ή άλλων ομάδων.

Επιπρόσθετα, εξίσου σημαντική αρμοδιότητα του διευθυντή είναι η διαχείριση των κρίσεων και η εξασφάλιση του κατάλληλου προσωπικού και των απαραίτητων πόρων για τη διαχείριση αλλά και φυσικά η διασφάλιση ότι οι δραστηριότητες για τον περιορισμό και την αντιμετώπιση των περιστατικών εκτελούνται με τον ενδεδειγμένο τρόπο. Τα άτομα που αναλαμβάνουν αυτή την θέση πρέπει να είναι τεχνικά ικανά και να έχουν άριστες δεξιότητες επικοινωνίας.

Εκτός από τον διευθυντή πολλοί οργανισμοί ορίζουν και έναν τεχνικό υπεύθυνο, αρκετά έμπειρο, διαθέτοντας παρόμοιες γνώσεις με του διευθυντή και ταυτόχρονα μεγάλη εμπειρία στην διαχείριση και αντιμετώπιση των περιστατικών. Ο τεχνικός υπεύθυνος είναι αρμόδιος για την επίβλεψη της ομάδας και των έργων της. Παράλληλα, σε μερικές ιεραρχίες υπάρχει και η θέση του υπευθύνου περιστατικού, έχοντας την ευθύνη για τον χειρισμό του περιστατικού. Συνήθως αρκετά μεγάλες

ομάδες αντιμετώπισης περιστατικών ασφαλείας διαθέτουν αυτήν τη θέση (Cichonski, Millar, Grance, & Scarfone, 2012).

Σύμφωνα με το NIST (Cichonski, Millar, Grance, & Scarfone, 2012) έχουν θεσπιστεί συγκεκριμένες ενέργειες, οι οποίες προτείνονται με σκοπό την συνεχή βελτίωση των ομάδων αντιμετώπισης περιστατικών ασφαλείας αλλά και τη δημιουργία ενός αποτελεσματικού συνόλου, με υψηλά επίπεδα γνώσης, εμπειρίας αλλά και κουλτούρας ασφάλειας. Αναλυτικότερα, οι προτινόμενες ενέργειες είναι οι εξής:

1. Συμμετοχή προσωπικού σε συνέδρια ή παροχή κινήτρων για παρακολούθηση συνεδρίων. Αποστολή προσκλήσεων σε εξωτερικούς εμπειρογνώμονες με μεγάλη τεχνική κατάρτιση στους συγκεκριμένους τομείς.
2. Παροχή ευκαιριών στα μέλη της ομάδας για εκτέλεση διαφορετικών εργασιών από αυτές που είναι υπεύθυνοι.
3. Εναλλαγές μεταξύ ατόμων που βρίσκονται μέσα στην ομάδα και εξωτερικών μελών, ώστε να υπάρχουν και ταυτόχρονες εναλλαγές των θέσεων τους (π.χ. Διαχειριστές συστημάτων). Αυτό στοχεύει στην απόκτηση καινούργιων τεχνικών δεξιοτήτων από τα μέλη.
4. Να υπάρχει επάρκεια προσωπικού ανά πάσα στιγμή, ώστε να παρέχεται η δυνατότητα στα μέλη των ομάδων να παίρνουν τις άδειες τους, όπως ορίζεται.
5. Δημιουργία προγράμματος καθοδήγησης, ώστε να παρέχεται η δυνατότητα στο πιο έμπειρο και ανώτερα τεχνικά προσωπικό να καταρτίσει και να δίνει συμβουλές στο προσωπικό με λιγότερη εμπειρία.
6. Δημιουργία σεναρίων περιστατικών αλλά και ανάπτυξη του χειρισμού τους, με σκοπό την περαιτέρω συζήτηση γύρω από αυτά με τα μέλη της ομάδας.

2.3.3 Στάση οργανισμών ή κυβερνήσεων για την στήριξη της ομάδας αντιμετώπισης περιστατικών ασφαλείας

Ανάλογα με τους σκοπούς που έχει η ομάδα αντιμετώπισης περιστατικών ασφαλείας και ο φορέας που την χορηγεί μπορεί να είναι σε θέση να επιβάλλει συγκεκριμένες ενέργειες μετά από επιθέσεις. Μερικές φορές όμως αυτό χρειάζεται έγκριση από τον οργανισμό ή την κυβέρνηση (ανάλογα τον τύπο της ομάδας) προτού γίνει κάποια ενέργεια. Τα όρια που οφείλει να τηρεί μια ομάδα, αποτυπώνονται λεπτομερώς από τη νομοθεσία του κάθε κράτους (Bada, Creese, Goldsmith, Mitchell, & Phillips, 2014).

ΚΕΦΑΛΑΙΟ 3^ο: Μεθοδολογία

3.1 Εισαγωγή

Η επιστημονική ερευνά έχει ως στόχο την εύρεση νόμων και την δημιουργία θεωριών, οι οποίες εξηγούν διάφορα φαινόμενα. Το ενδεχόμενο η γνώση να είναι λανθασμένη, ατελής ή να υπόκεινται σε παραπάνω από μια αλήθειες είναι αρκετά πιθανό, αφού αυτές οι θεωρίες εξάγονται για την εξήγηση ενός φαινομένου που προτάθηκε από έναν επιστήμονα. Κατά συνέπεια, ενδέχεται οι εξηγήσεις και οι θεωρίες που εξάγονται να είναι αρκετά σχετικές με την πραγματικότητα ή και καθόλου. Ο δρόμος για να φτάσουμε σε ορθούς επιστημονικούς νόμους ή θεωρίες περνάει μέσα από μια διαδικασία λογικής και αποδείξεων, όπου λογική είναι η θεωρία και αποδείξεις είναι οι παρατηρήσεις. Αυτά τα δυο ουσιαστικά χαρακτηρίζονται ως οι πυλώνες της επιστημονικής γνώσης, καθώς είναι δυο αλληλένδετες έννοιες και δεν μπορούν να υπάρξουν η μια χωρίς την άλλη. Γενικότερα, οι επιστημονικές έρευνες κινούνται συνεχώς μεταξύ αυτών των εννοιών, αφού δεν θα ήταν ορθό και έγκυρο μια έρευνα να βασίζεται μονό σε παρατηρήσεις για να καταλήξει σε συμπεράσματα, αγνοώντας το μέρος της θεωρίας (Bhattacharjee, 2012).

3.2 Επιλογή Μεθοδολογίας

Στην παρούσα μελέτη χρησιμοποιείται και εφαρμόζεται η μεθοδολογία της συστηματικής ανασκόπησης σε υπάρχουσες βιβλιογραφίες, όπως ορίζεται από την Kitchenham (Kitchenham, 2004) ως εξής:

Συστηματική Ανασκόπηση: Πρόκειται για ένα εργαλείο έρευνας, το οποίο εντοπίζει, ερμηνεύει και αξιολογεί διαθέσιμες έρευνες που σχετίζονται με ένα συγκεκριμένο ερευνητικό ερώτημα, θεματικό πεδίο ή και ένα αντικείμενο ενδιαφέροντος. Πρωτογενείς μελέτες είναι οι μεμονωμένες μελέτες που συμβάλλουν στην συστηματική ανασκόπηση ενώ η συστηματική ανασκόπηση είναι ένα είδος δευτερογενούς μελέτης.

Ένας μελετητής έχει τη δυνατότητα να διενεργήσει μια έρευνα με την μέθοδο της συστηματικής ανασκόπησης για πολλούς λόγους. Συγκεκριμένα, του δίνεται η δυνατότητα να συγκεντρώσει τα σημαντικότερα επιστημονικά δεδομένα σχετικά με το γνωστικό αντικείμενο που τον ενδιαφέρει, να συνοψίσει εμπειρικά στοιχεία για τα

πλεονεκτήματα και τα μειονεκτήματα μιας μεθόδου, να εντοπίσει σε τρέχουσες έρευνες τυχόν κενά και στο τέλος να καταθέσει προτάσεις για περαιτέρω διερεύνηση του θέματος. Παράλληλα, είναι σε θέση να εξετάσει κατά πόσο κάποια εμπειρικά στοιχεία στηρίζουν θεωρητικές υποθέσεις ή και κατά πόσο ανταποκρίνονται στο να συμβάλουν σε νέες υποθέσεις και ως εκ τούτου να παρέχουν ένα πλαίσιο ή υπόβαθρο για την κατάλληλη τοποθέτηση νέων ερευνητικών δραστηριοτήτων (Kitchenham, 2004). Σε αυτό τον λόγο στηρίζεται κατά βάση και η παρούσα έρευνα.

3.2.1 Πλεονεκτήματα

Το μεγαλύτερο πλεονέκτημα των συστηματικών ανασκοπήσεων είναι ότι έχουν την δυνατότητα να προσφέρουν πληροφορίες για τις επιπτώσεις διαφόρων φαινομένων μέσα σε ένα αρκετά μεγάλο εύρος εμπορικών μεθόδων και ρυθμίσεων. Αν οι αρχικές μεμονωμένες έρευνες παρέχουν ορθά και συνεπή αποτελέσματα, τότε η συγκεκριμένη μέθοδος μπορεί να προσφέρει επαρκή δεδομένα ότι το εξεταζόμενο φαινόμενο είναι ισχυρό και μεταβιβάσιμο ενώ στην αντίθετη περίπτωση είναι εφικτό να μελετηθούν οι πηγές διακύμανσης. Ένα άλλο πλεονέκτημα των συστηματικών ανασκοπήσεων είναι ότι στην περίπτωση των ποσοτικών μελετών μπορεί να χρησιμοποιηθούν οι μετά αναλυτικές τεχνικές. Ως μειονέκτημα θα μπορούσε να χαρακτηριστεί ο εντοπισμός σχετικών προκαταλήψεων, εξαιτίας της μεγάλης ισχύς της συγκεκριμένης μεθόδου (Kitchenham, 2004). Βιβλιογραφικές συστηματικές ανασκοπήσεις εξαιρετικής ποιότητας συγκεντρώνουν έρευνες για να:

1. Καταλήξουν σε ποιοτικά και ορθά συμπεράσματα σε σχέση με τα ερευνητικά ερωτήματα και τα ζητήματα.
2. Να δοθεί εξήγηση για τη συσχέτιση των μελετών, για τα συμπεράσματα που προκύπτουν για μελλοντικές έρευνες αλλά και τη σημασία τους για την θεωρία (Siddaway, Wood, & Hedges, 2019).

Μια βιβλιογραφική συστηματική ανασκόπηση μπορεί να καθοδηγηθεί από δυο πιθανά σκέλη, την υπό εξέταση θεωρία και τις νέες ιδέες και διαδικασίες που μπορεί να εξαχθούν ως αποτέλεσμα κατά την εφαρμογή της ανασκόπησης (Siddaway, Wood, & Hedges, 2019).

3.2.2 Χαρακτηριστικά και Αναζήτηση

Τα χαρακτηριστικά που κάνουν μια συστηματική ανασκόπηση να ξεχωρίζει, σύμφωνα με την Kitchenham είναι ότι ξεκινάει με τον ορισμό συγκεκριμένου πρωτοκόλλου ανασκόπησης, με τα ερευνητικά ερωτήματα που θα αντιμετωπιστούν και τις μεθόδους που θα χρησιμοποιηθούν. Επίσης, είναι εξαιρετικής σημασίας ότι ακολουθείται καθορισμένη στρατηγική αναζήτησης, η οποία στοχεύει στον εντοπισμό μεγάλου μέρους της υπό διερεύνησης σχετικής βιβλιογραφίας.

Η τεκμηρίωση της στρατηγικής αναζήτησης πραγματοποιείται με σκοπό οποιοσδήποτε άλλος ερευνητής να έχει τη δυνατότητα να αξιολογήσει την αυστηρότητα και την πληρότητα της. Φυσικά, στα πλαίσια αποτελεσματικότερης τεκμηρίωσης, καθορίζονται συγκεκριμένα κριτήρια ένταξης και αποκλεισμού για τις πρωτογενείς μελέτες. Ακόμα καθορίζονται οι πληροφορίες που αντλούνται από τις πρωτογενείς μελέτες αλλά και τα κριτήρια ποιότητας που θα αξιολογηθούν από αυτές τις μελέτες. Η συγκεκριμένη μέθοδος της συστηματικής ανασκόπησης είναι απαραίτητη προϋπόθεση για την μετά-ανάλυση ή μετά-σύνθεση.

Αυτά δηλώνονται ρητά και με λεπτομέρεια και τηρούνται με μεγάλη συνέπεια για να είναι ξεκάθαρα στους επιστήμονες και στους ερευνητές που θα χρησιμοποιήσουν τα ίδια κριτήρια να μπορέσουν καταλήξουν στα ίδια αποτελέσματα. Μια προσέγγιση σαν την παραπάνω προσφέρει την δυνατότητα στους επιστήμονες να αξιολογήσουν το έργο με τις υποθέσεις του, τις διαδικασίες του, τα συμπεράσματα του και οτιδήποτε άλλο το διέπει, ενώ ταυτόχρονα σε άλλους ερευνητές προσφέρει την δυνατότητα για περαιτέρω έρευνα. Αν κάποιος ερευνητής διεξήγαγε ακριβώς την ίδια έρευνα αναζήτησης, αν η προηγούμενη ήταν ορθή και ακολούθησε το μοτίβο κανόνων που προϋποθέτει η συστηματική ανασκόπηση, θα έπρεπε να βγάλει στη νέα ακριβώς τα ίδια αποτελέσματα. Τα αποτελέσματα που προκύπτουν είναι επόμενο να διαφέρουν ελαφρώς ή και ακόμα να χρησιμοποιούνται διαφορετικά σε μικρότερο βαθμό (Siddaway, Wood, & Hedges, 2019).

Η μεθοδικότητα, η περιεκτικότητα, η διαφάνεια και η δυνατότητα αναπαραγωγής χαρακτηρίζουν μια συστηματική ανασκόπηση. Μια συστηματική ανασκόπηση περιέχει μία συστηματική διαδικασία αναζήτησης, που εντοπίζει όλα τα σχετικά δημοσιεύματα έγγραφα μελετών ή και μη δημοσιευμένα που σχετίζονται και υποστηρίζουν τα ερευνητικά ερωτήματα που τέθηκαν στην πρώτη φάση της έρευνας.

Επίσης, περιέχει και μια συστηματική διαδικασία παρουσίασης και σύνθεσης των δεδομένων και των αποτελεσμάτων της αναζήτησης. Μια συστηματική μεθοδολογία αλλά και μια συστηματική παρουσίαση στοχεύουν αλλά και τείνουν προς την ελαχιστοποίηση της υποκειμενικότητας της μεροληψίας (Siddaway, Wood, & Hedges, 2019).

3.3 Επιλογή Τύπου Ανασκόπησης

Η διαδικασία της συστηματικής ανασκόπησης απαιτεί και την επιλογή του τύπου ανασκόπησης. Η πρώτη αφορά της ποσοτικές πληροφορίες και ονομάζεται «ποσοτική μετά-ανάλυση» και η δεύτερη σχετίζεται με ποιοτικές πληροφορίες και ονομάζεται «ποιοτική μετά-ανάλυση». Για την πιο ενδεδειγμένη επιλογή της προσέγγισης είναι απαραίτητο να ληφθεί υπόψη η φύση και η κατάσταση της βιβλιογραφίας που έχει επιλεχθεί, τα ερευνητικά ερωτήματα που έχουν τεθεί αλλά και τα θεωρητικά και εμπειρικά ζητήματα.

Οι συστηματικές ανασκοπήσεις ποιοτικών πληροφοριών μπορούν να διεξαχθούν μέσω δυο τύπων ποιοτικής σύνθεσης έρευνας, την «αφηγηματική ανασκόπηση» και τις «μετά-συνθέσεις». Για τις μετά-συνθέσεις χρησιμοποιείται επίσης ο όρος «μετά-εθνογραφία» ή «ποιοτική μετά-ανάλυση», όπως ήδη αναφέρθηκε. Οι αφηγηματικές ανασκοπήσεις είναι κατάλληλες για την διεξαγωγή συνθέσεων αποτελεσμάτων μεμονωμένων ποσοτικών μελετών χωρίς να συμπεριλαμβάνονται αναφορές σε στατιστικά ευρήματα. Οι αφηγηματικές ανασκοπήσεις αποτελούν ισχυρό μέσο σύνδεσης μελετών για ποικίλα και διαφορετικά θέματα, για την ερμηνεία ή την διασύνδεση, με στόχο την δημιουργία ή την αξιολόγηση μιας καινούργιας θεωρίας. Τέλος, παρέχουν την δυνατότητα ιστορικής περιγραφής της ανάπτυξης της θεωρίας και της έρευνας σε ένα συγκεκριμένο θέμα.

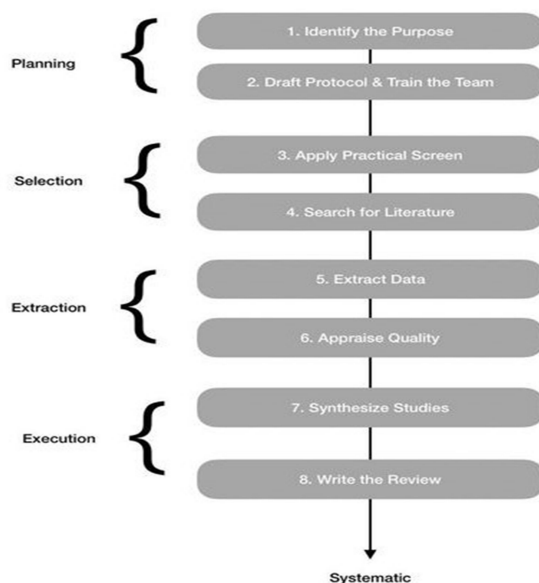
Αντίθετα, η μετά-σύνθεση ή αλλιώς ποιοτική μετά-ανάλυση χρησιμοποιείται όταν σε μια ανασκόπηση είναι αναγκαίο να ενταχθεί η ποιοτική έρευνα. Στόχος της είναι η σύνθεση ποιοτικών μελετών για τον εντοπισμό βασικών θεμάτων ή θεωριών που με την σειρά τους θα δημιουργήσουν νέες εξηγήσεις και πληροφορίες για το φαινόμενο που εξετάζεται (Siddaway, Wood, & Hedges, 2019). Η μετά-σύνθεση στις ποιοτικές έρευνες δεν αθροίζει όλα τα δεδομένα αλλά παρουσιάζει νέες προσεγγίσεις μέσω της ερμηνείας ευρημάτων (Nye, Melendez-Torres, & Bonell, 2016).

Σύμφωνα με τους Nye, Melendez-Torres & (2016) εντοπίζονται τρεις τρόποι, οι οποίοι βοηθούν την ποιοτική μετά-σύνθεση να χρησιμοποιηθεί σαν μέθοδος. Η πρώτη αφορά πτυχές από την συστηματική ανασκόπηση που απαιτούνται για την ορθή και επιτυχημένη μετά-σύνθεση, η δεύτερη περιλαμβάνει τις μεθόδους που αναλύονται οι ποιοτικές μελέτες, όπως και η χρήση των αποτελεσμάτων αυτής και τρίτον έχει να κάνει με τις λεκτικές, μεθοδολογικές αλλά και παραδειγματικές διαστάσεις της ποιοτικής μετά-σύνθεσης (Nye, Melendez-Torres, & Bonell, 2016).

Με βάση τα παραπάνω αλλά και την προηγούμενη ενότητα μετά από προσεκτική μελέτη αιτιολογείται η επιλογή της συστηματικής ανασκόπησης και στην συνέχεια της μετά-σύνθεσης των δεδομένων. Η συστηματική ανασκόπηση θεωρείται μια έγκυρη αλλά και αντικειμενική μέθοδος για δευτερογενείς έρευνες.

3.4 Βήματα Συστηματικής Ανασκόπησης

Συμφώνα με τον Okoli (2015) υπάρχουν συγκεκριμένα βήματα που πρέπει να ακολουθηθούν αυστηρά για την διεξαγωγή μια συστηματικής βιβλιογραφικής ανασκόπησης (Okoli, 2015) (βλ. Εικόνα 2).



Εικόνα 2 Βήματα βιβλιογραφικής συστηματικής ανασκόπησης

Αυτά τα βήματα ορίζονται ως εξής:

Βήμα 1: Το πρώτο βήμα αφορά τον προσδιορισμό με πλήρη σαφήνεια από τον ερευνητή του σκοπού της έρευνας αλλά και τους επιδιωκόμενους στόχους της κριτικής.

Βήμα 2: Το δεύτερο βήμα αφορά την σύνταξη πρωτοκόλλου και την εκπαίδευση της ομάδας. Το γεγονός αυτό σημαίνει ότι για τις αξιολογήσεις που απασχολούν παραπάνω από έναν κριτή, οι κριτές πρέπει να είναι σύμφωνοι και σαφείς με την σχετική διαδικασία που πρόκειται να ακολουθηθεί. Αυτό απαιτεί λεπτομερές γραπτό έγγραφο πρωτοκόλλου αλλά και εκπαίδευση για τους κριτές, αναφορικά με τον τρόπο με τον οποίο θα φέρουν εις πέρας την αξιολόγηση.

Βήμα 3: Το τρίτο βήμα αφορά την λεγόμενη εφαρμογή πρακτικής οθόνης ή αλλιώς «έλεγχος συμπερίληψης» (“Apply Practical Screen”). Σε αυτό το βήμα θα πρέπει οι κριτές να δείξουν με σαφήνεια ποιες μελέτες επέλεξαν για να εξετάσουν αλλά και ποιες αποκλειστήκαν αμέσως. Για όσες μελέτες αποκλείστηκαν θα πρέπει να αναφερθούν οι λόγοι αυτής της απόρριψης αλλά και ο τρόπος που θα μπορούσαν να φανούν χρήσιμες, λαμβάνοντας υπόψη τα κριτήρια που δεν πληρούν.

Βήμα 4: Το βήμα τέσσερα αφορά την αναζήτηση της σχετικής βιβλιογραφίας και οι κριτές οφείλουν να πραγματοποιήσουν μια ξεκάθαρη εικόνα διεξαγωγής της αναζήτησης της βιβλιογραφίας και τις λεπτομέρειες της. Επίσης, θα πρέπει να αιτιολογήσουν την βαθμό πληρότητας της αναζήτησης.

Βήμα 5: Το βήμα πέντε αφορά την εξαγωγή των δεδομένων από τις μελέτες που επιλέχθηκαν και τον συστηματικό τρόπο εξαγωγής των πληροφοριών από κάθε μελέτη.

Βήμα 6: Το βήμα έξι αφορά την αξιολόγηση της ποιότητας (ή «έλεγχος για αποκλεισμό»). Σε αυτή τη φάση οι κριτές θα πρέπει να αναφέρουν και να προσδιορίσουν τα κριτήρια που χρησιμοποίησαν για να κρίνουν τις επιλεγθείσες μελέτες ως προς την ποιότητα τους και αν κρίθηκαν κάποιες ως ανεπαρκείς. Οι κριτές θα πρέπει να εξετάσουν όλες τις μελέτες που επιλέξανε, σύμφωνα με τις ερευνητικές μεθοδολογίες που χρησιμοποίησαν για τον έλεγχο της ποιότητας τους.

Βήμα 7: Το βήμα επτά αφορά την σύνθεση μελετών και είναι επίσης γνωστό και ως «ανάλυση». Σε αυτό το βήμα γίνεται συνδυασμός των δεδομένων που εξάγονται από

όλες τις μελέτες που επιλέχθηκαν με την χρήση κατάλληλων τεχνικών είτε ποσοτικών είτε ποιοτικών είτε ακόμα και των δύο.

Βήμα 8: Το βήμα οκτώ αφορά την ανασκόπηση, όπου εκτός από τις τυπικές αρχές και τους τυπικούς κανόνες που ακολουθούνται σε τέτοιες περιπτώσεις, μια συστηματική βιβλιογραφική ανασκόπηση και γενικότερα όλη η διαδικασία πρέπει να περιγράφεται με κάθε λεπτομέρεια για να μπορούν και άλλοι ερευνητές να αναπαράγουν ανεξάρτητα τα αποτελέσματα της.

Λαμβάνοντας υπόψη τα παραπάνω βήματα και ενεργώντας με γνώμονα αυτά, τα βήματα της παρούσας μελέτης διαμορφώνονται ως εξής:

Βήμα 1: Σύμφωνα και με τον τίτλο της έρευνας θα εξετάσουμε και θα αναζητήσουμε ζητήματα και αποκλίσεις κατά την εφαρμογή στρατηγικών αντιμετώπισης περιστατικών ασφάλειας πληροφοριών αλλά και τον ρόλο του ανθρώπινου παράγοντα. Αυτό θα γίνει μέσω των ερευνητικών ερωτημάτων που θέσαμε στην Ενότητα 1.3.

Βήμα 2: Στα πλαίσια του δεύτερου βήματος η συγκεκριμένη έρευνα διεξάγεται στα πλαίσια πτυχιακής εργασίας, οπότε υπάρχει ένας ερευνητής και ένας επιβλέπων καθηγητής.

Βήμα 3 και Βήμα 4: Τα συγκεκριμένα βήματα αναλύονται διεξοδικά στην ενότητα 3.5

Βήμα 5: Για την εξαγωγή των δεδομένων χρησιμοποιήθηκε μια παραγωγική (deductive) ή αλλιώς «απαγωγική μέθοδος» κωδικοποίησης αυτών, όπου αναλύονται με περισσότερες λεπτομέρειες στο Κεφάλαιο 5.

Βήμα 6: Για το έκτο βήμα χρησιμοποιήθηκε το εργαλείο CASP για την αξιολόγηση της ποιότητας των μελετών. Περισσότερες λεπτομέρειες για το εργαλείο αλλά και για την αξιολόγηση αναφέρονται στην Ενότητα 3.7.

Βήμα 7: Για το έβδομο βήμα της συστηματικής βιβλιογραφικής ανασκόπησης χρησιμοποιήθηκε μια ποιοτική μετά-σύνθεση δεδομένων που αποτυπώνεται αναλυτικά στην εισαγωγή του Κεφαλαίου 5.

Βήμα 8: Στα πλαίσια του τελευταίου βήματος, περιγράφονται λεπτομερώς τα αποτελέσματα της έρευνας στο Κεφάλαιο 5.

3.5 Αναζήτηση και Επιλογή

3.5.1 Εισαγωγή στην Αναζήτηση

Η μελέτη της σχετικής βιβλιογραφίας αποτελείται κυρίως από άρθρα, πλαίσια, δημοσιεύσεις και άλλες σχετικές έρευνες. Καταγράφηκε ένας αρκετά μεγάλος όγκος δεδομένων κατά την αναζήτηση. Ωστόσο, εντοπίστηκαν ελάχιστα αποτελέσματα που να δίνουν αρκετές πληροφορίες για τον τρόπο που διαχειρίζονται και αντιμετωπίζουν περιστατικά οι οργανισμοί σε πρακτικό επίπεδο.

Η αναζήτηση και η μελέτη της σχετικής βιβλιογραφίας έγινε σε δημόσιες βάσεις δεδομένων, ανοικτής πρόσβασης ή σε βάσεις που είχε πρόσβαση συγκεκριμένη ομάδα ατόμων, δηλαδή φοιτητές. Με αυτό τον τρόπο, αρκετές φορές επιτεύχθηκε η πρόσβαση με το ακαδημαϊκό e-mail του Ιονίου Πανεπιστημίου. Παραδείγματα των πηγών αναζήτησης που χρησιμοποιήθηκαν είναι Science Direct, IEEE Access, Research Gate Enisa, Nist, Google Scholar.

3.5.2 Κριτήρια Αναζήτησης Μελέτης

Για να καταλήξει η έρευνα στην επιλογή της συγκεκριμένης βιβλιογραφίας έπρεπε αρχικά να τεθούν κάποια κριτήρια ένταξης και αποκλεισμού. Για να τεθούν αυτά τα κριτήρια χρησιμοποιήθηκε ως βάση μια γενική κοινή φόρμα κριτηρίων (Siddaway, Wood, & Hedges, 2019).

1. Τα ερευνητικά ερωτήματα που τέθηκαν και θα μελετηθούν (πεδίο εφαρμογής).
2. Ορισμοί και έννοιες όπως τις ορίζει ο κάθε ερευνητής.
3. Μέτρα κι μεταβλητές (μέτρηση δεδομένων και με τι προϋποθέσεις).
4. Ο σχεδιασμός της έρευνας (σε τι έρευνες θα βασιστεί η μελέτη π.χ. ποιοτικές, μελέτες περίπτωσης, κ.λπ.).
5. Συμμετέχοντες (τα άτομα που λαμβάνουν μέρος στην έρευνα π.χ. υπάλληλοι).
6. Χρονικό πλαίσιο ή όριο.
7. Δεδομένα (που μπορούν να αναφερθούν σε μετά-ανάλυση).

Με γνώμονα τα παραπάνω κριτήρια επιλογής βιβλιογραφίας, τέθηκαν και τα κριτήρια της παρούσας έρευνας και τα οποία παρουσιάζονται στη συνέχεια.

Εφόσον η έρευνα κινείται γύρω από την ανίχνευση, διαχείριση και αντιμετώπιση και πιο συγκεκριμένα μελετώνται τυχόν ζητήματα κατά την εφαρμογή στρατηγικών

αντιμετώπισης περιστατικών ασφάλειας πληροφοριών, το πρώτο κριτήριο διαμορφώνεται ως εξής:

1. Πεδίο εφαρμογής η ανίχνευση, διαχείριση και η αντιμετώπιση περιστατικών ασφάλειας.

Η διαχείριση και αντιμετώπιση περιστατικών ασφαλείας απασχολεί σε μεγάλο βαθμό τους οργανισμούς και ακόμα περισσότερο τους μεγαλύτερους, καθώς διακυβεύονται αρχές και δεδομένα μεγαλύτερης αξίας. Κατά συνέπεια, επίκεντρο της συγκεκριμένης μελέτης είναι οι μεγάλοι οργανισμοί και ο τρόπος αντιμετώπισης των περιστατικών ασφαλείας. Ως εκ τούτου, το δεύτερο κριτήριο διαμορφώθηκε ως εξής:

2. Οι έρευνες θα πρέπει να είναι μελέτες περίπτωσης μεγάλων οργανισμών.

Για να παρέχει η μελέτη σύγχρονα αποτελέσματα και απαντήσεις στα ερευνητικά ερωτήματα που τέθηκαν αλλά και για να συμβαδίζει με αρκετά πρόσφατα δεδομένα και γεγονότα, το τρίτο κριτήριο τέθηκε ως εξής:

3. Οι αρχικές μεμονωμένες έρευνες να έχουν δημοσιευτεί από το 2010 και μετά.

Το τελευταίο κριτήριο που τέθηκε ήταν οι συγκεκριμένες μελέτες περίπτωσης που θα επιλέγονταν να παρείχαν όσο το δυνατόν περισσότερα και λεπτομερή στοιχεία από τους ερευνητές και τους συγγραφείς τους, ώστε να μπορούν να στηρίζουν τις απαντήσεις στα ερωτήματα που τέθηκαν.

4. Τα δεδομένα που δίνονται να μπορούν να υποστηρίξουν απαντήσεις στα ερευνητικά ερωτήματα που τέθηκαν.

3.5.3 Επιλογή Μελέτης

Χρησιμοποιήθηκαν αρκετές λέξεις και όροι κλειδιά σε δημόσιες βάσεις δεδομένων ή σε βάσεις που επιτρεπόταν η είσοδος μέσω του Ιονίου Πανεπιστημίου. Πιο αναλυτικά χρησιμοποιήθηκε ο συνδυασμός των όρων “Information Security Incidents”, “Breach”, “Playbooks”, “Mitigation”, “Response”, “Response Lifecycle”, “Team”, “CSIRT, Management”, “Use Case”, “Case Study”.

Τα πρώτα αποτελέσματα δεν πληρούσαν αρκετά από τα κριτήρια που είχαν τεθεί ενώ άλλες φορές εμφανίζονταν αποτελέσματα εκτός πεδίου μελέτης ή διπλότυπα. Ωστόσο, με το συνδυασμό των όρων “Incident Response Team” στο Google Scholar ένα από τα αρκετά αποτελέσματα που εμφανίστηκαν ήταν η περίπτωση της

FinanceOrg (Ahmad, et al., 2012). Κατόπιν διεξοδικής μελέτης της συγκεκριμένης περίπτωσης, θεωρήθηκε ότι είναι κατάλληλη να στηρίζει την παρούσα ερευνητική εργασία.

Στην δεύτερη περίπτωση της μελέτης των τριών μεγάλων νορβηγικών οργανισμών με τον συνδυασμό των όρων “Information Security Incident Management” διαπιστώθηκε μια έρευνα συστηματικής ανασκόπησης σχετικά με τις εμπειρίες αρκετών οργανισμών στην διαχείριση συμβάντων και περιστατικών. Ο τίτλος της έρευνας είναι “Information Security Incident Management” και οι συγγραφείς της είναι οι Inger Anne Tøndel, Maria B. Line, Martin Gilje Jaatun. Μια από αυτές τις περιπτώσεις που επικεντρώθηκε η παραπάνω δημοσίευση είναι και αυτή που επιλέχθηκε βάση των κριτηρίων που έχουν τεθεί. Η αρχική έρευνα των τριών νορβηγικών οργανισμών (Hove & Tarnes, 2013) εντοπίστηκε στην βιβλιογραφία της παραπάνω μελέτης.

3.6 Έρευνα Περιπτώσεων

Η έρευνα που διεξήχθη βασίστηκε σε υλικό που εντοπίστηκε σε παλαιότερες έρευνες με συνεντεύξεις και ανάλυση εγγράφων. Στις περιπτώσεις των τριών μεγάλων νορβηγικών οργανισμών (Hove & Tarnes, 2013) που μελετήθηκαν χρησιμοποιήθηκε ποιοτική μέθοδος έρευνας με σχετικά μικρό αριθμό συνεντευζιαζόμενων. Επίσης, σε αυτή την έρευνα χρησιμοποιήθηκε μια επαγωγική ερευνητική προσέγγιση στην αγγλική γλώσσα (Inductive Research) (Bhattacharjee, 2012) ή αλλιώς μια έρευνα οικοδόμησης θεωριών με στόχο τη συγκέντρωση θεωριών από τα δεδομένα που προκύπτουν, δηλαδή, ουσιαστικά από μελέτες και παρατηρήσεις που κάνουν οι ερευνητές εξάγουν θεωρίες.

Αυτή η μέθοδος είναι η αντίθετη της απαγωγικής στην αγγλική γλώσσα Deductive Research (Bhattacharjee, 2012) όπου στόχος των ερευνητών ήταν να δοκιμάσουν θεωρίες κι πρότυπα χρησιμοποιώντας νέα εμπειρικά δεδομένα. Ενώ για την ανάλυση των δεδομένων χρησιμοποιήθηκε μια πιο «Γενική Επαγωγική Προσέγγιση» (Thomas, 2006). Μέσω της ενδελεχούς μελέτης εγγράφων των οργανισμών αλλά και πραγματοποιώντας λεπτομερείς συνεντεύξεις, δόθηκαν στους ερευνητές επαρκή στοιχεία που σχετίζονται με την λειτουργία διαχείρισης και αντιμετώπισης των περιστατικών τους.

Στην περίπτωση του τέταρτου οργανισμού FinanceOrg (Ahmad, et al., 2012) που μελετήθηκε στα πλαίσια αυτής της έρευνας χρησιμοποιήθηκε μια διερευνητική προσέγγιση πολλαπλών περιπτώσιολογικών μελετών με τη χρήση συνεντεύξεων, ως βασική μέθοδο συλλογής δεδομένων. Οι ηχογραφημένες συνεντεύξεις αλλά και οι σημειώσεις που καταχωρήθηκαν, επεξεργάστηκαν με τη χρήση ανοιχτής, αξονικής και επιλεκτικής κωδικοποίησης από εξειδικευμένο λογισμικό.

Στις μελέτες περιπτώσεων για να επαληθευτούν ή και για να αμφισβητηθούν κάποια δεδομένα χρησιμοποιήθηκε η μελέτη εγγράφων των συγκεκριμένων οργανισμών. Τα δεδομένα που επαληθεύονται ή αμφισβητούνται προκύπτουν από άλλες πηγές ή μεθόδους συλλογής δεδομένων. Η ανάλυση των ερευνών που στηρίχτηκαν πάνω στις μελέτες περιπτώσεων, όπου βασίζεται και η παρούσα έρευνα, επέτρεψε την σύγκριση μεταξύ των οργανισμών, των προτύπων πλαισίων και των τεχνικών διαχείρισης και αντιμετώπισης περιστατικών ασφαλείας.

3.7 Αξιολόγηση ποιότητας μελετών

Για την αξιολόγηση ποιότητας της μελέτης (Hove & Tarnes, 2013; Ahmad, et al., 2012) χρησιμοποιήθηκε ένα εργαλείο από την μελέτη των Majid & Vanstone (2018), όπου ουσιαστικά μέσα από ένα ερωτηματολόγιο προτείνεται το καταλληλότερο εργαλείο αξιολόγησης ποιότητας μελέτης για την κάθε περίπτωση (Majid & Vanstone, 2018).

Σύμφωνα με τα στοιχεία της παρούσας έρευνας, το εργαλείο αξιολόγησης ποιότητας μελέτης που προτάθηκε ήταν το CASP. Το CASP είναι ένα εργαλείο που χρησιμοποιείται για την αξιολόγηση των δυνατοτήτων και των περιορισμών σε μεθοδολογίες ποιοτικής έρευνας. Η υλοποίηση του πραγματοποιείται μέσα από δέκα ερωτήσεις που ουσιαστικά απαιτούν από τον ερευνητή που θέλει να αξιολογήσει την μελέτη της επιλογής του να μελετήσει και να εξετάσει προσεκτικά της μεθόδους της έρευνας αλλά και τα ευρήματα αυτής και το νόημα τους. Το CASP είναι ένα αρκετά φιλικό εργαλείο, ως προς την χρήση και είναι κατάλληλο για ερευνητές οι οποίοι είναι αρχάριοι στην αξιολόγηση ποιότητας μελετών (Long, French, & Brooks, 2020).

Στην συνέχεια καταγράφονται οι δέκα ερωτήσεις του εργαλείου CASP, ακριβώς έτσι όπως αναγράφονται και στο εργαλείο. Οι πιθανές απαντήσεις σε αυτές τις ερωτήσεις είναι «Ναι/Όχι» ή «Δεν μπορώ να πω» με μια μικρή αιτιολόγηση πάντα. Κάτω από κάθε ερώτηση υπάρχει και η απάντηση για την κάθε μελέτη με την σχετική

αιτιολόγηση. Οι ερωτήσεις χωρίζονται σε τρία σκέλη. Το πρώτο σκέλος ερωτήσεων αφορά την εγκυρότητα των αποτελεσμάτων της μελέτης, όπου περιλαμβάνει και τις ερωτήσεις από την 1-6. Το δεύτερο σκέλος εξετάζει ποια είναι τα αποτελέσματα της μελέτης, όπου και περιλαμβάνει τις ερωτήσεις 7-9. Τέλος, το τρίτο σκέλος σχετίζεται με το, αν θα βοηθήσουν τα αποτελέσματα τοπικά, όπου και περιλαμβάνει την ερώτηση 10. Στην συνέχεια των Ενοτήτων 3.7.1 και 3.7.2 καταγράφεται η απάντηση στις ερωτήσεις αξιολόγησης ποιότητας έρευνας του εργαλείου CASP και η αιτιολόγηση της από τον ερευνητή, αναφορικά με τις περιπτώσεις των τριών νορβηγικών οργανισμών και της FinanceOrg.

3.7.1 Περίπτωση των τριών νορβηγικών οργανισμών

Το πρώτο μέρος ερωτήσεων αξιολόγησης και αναφοράς αφορά την μελέτη των τριών μεγάλων νορβηγικών οργανισμών (Hove & Tarnes, 2013). Στην συνέχεια αναγράφονται οι 10 ερωτήσεις του εργαλείου CASP (Long, French, & Brooks, 2020) ακριβώς έτσι όπως αναγράφονται και στο εργαλείο και η συγκεκριμένη έρευνα απαντάει αυτά τα ερωτήματα με την σχετική αιτιολόγηση για να μπορέσει να αξιολόγηση την συγκεκριμένη μελέτη.

Ερώτηση 1: Υπάρχει σαφής δήλωση των στόχων της έρευνας;

Απάντηση: Ναι.

Αιτιολόγηση: Οι στόχοι της έρευνας διατυπώνονται με απόλυτη σαφήνεια στην Ενότητα 1.2.

Ερώτηση 2: Είναι κατάλληλη μια ποιοτική μεθοδολογία;

Απάντηση: Ναι.

Αιτιολόγηση: Η μέθοδος της συγκεκριμένης μελέτης είναι η μελέτη περίπτωσης. Οι ερευνητές αναζητούσαν πληροφορίες σε βάθος από συγκεκριμένους οργανισμούς. Η επιλογή αυτή τεκμηριώνεται και στην παρούσα εργασία στο Κεφάλαιο 2: Μέθοδος.

Ερώτηση 3: Ο σχεδιασμός της έρευνας ήταν κατάλληλος για να αντιμετωπίση τους στόχους αυτής;

Απάντηση: Ναι.

Αιτιολόγηση: Ήταν κατάλληλη και υπάρχει πλήρη αιτιολόγηση και συζήτηση της μεθοδολογίας που ακολουθήθηκε στο Κεφάλαιο 2: Μέθοδος.

Ερώτηση 4: Ήταν η στρατηγική πρόσληψης κατάλληλη για τους στόχους της έρευνας;

Απάντηση: Ναι.

Αιτιολόγηση: Σύμφωνα με το έγγραφο, επιλέχθηκε από τους ερευνητές για να εξετάσουν μεγάλους οργανισμούς και την αιτία για την μεγαλύτερη έκθεση τους σε επιθέσεις. Επίσης, αναφέρονται και άλλοι λόγοι της επιλογής αυτής στην Ενότητα 2.4. Η επιλογή των εργαζομένων για να κληθούν σε συνέντευξη τεκμηριώνεται στην Ενότητα 2.3.4 αλλά και στο Κεφάλαιο 4: Εισαγωγή Περιπτώσεων.

Ερώτηση 5: Τα δεδομένα συλλέχτηκαν με τέτοιο τρόπο ώστε να στηρίζουν το ερευνητικό ζήτημα;

Απάντηση: Ναι.

Αιτιολόγηση: Χρησιμοποιήθηκαν ημιδομημένες ποιοτικές συνέντευξης με γνώμονα συγκεκριμένο οδηγό συνέντευξης. Παράλληλα, χρησιμοποιήθηκε μελέτη εγγράφων και μια γενική επαγωγική προσέγγιση για την ανάλυση των δεδομένων. Η αιτιολόγηση για τις επιλογές αυτές αλλά και σχετικές πληροφορίες αναφέρονται αναλυτικά στις Ενότητες 2.3.2, 2.3.3, 2.3.4 και 2.3.5 της εργασίας.

Ερώτηση 6: Έχει ληφθεί επαρκώς υπόψη η σχέση μεταξύ του ερευνητή και των συμμετεχόντων;

Απάντηση: Ναι.

Αιτιολόγηση: Έχουν ληφθεί υπόψη οι προκλήσεις, αφού η μεγαλύτερη συλλογή δεδομένων προήλθε από συνεντεύξεις. Είχε εντοπιστεί ο ενδεχόμενος κίνδυνος ότι η έλλειψη εμπιστοσύνης μεταξύ ερευνητών και οργανισμών μπορεί να επηρεάσει την μελέτη, οπότε ελήφθησαν οι δέουσες προφυλάξεις για την αποφυγή μεροληπτικών απαντήσεων. Επιπρόσθετα, τέθηκε υπόψη η πιθανή μεροληψία των συνεντευξιαζόμενων αλλά και η επιλογή της επαγωγικής ποιοτικής ερευνητικής προσέγγισης, η οποία απέφερε

μικρότερη προκατάληψη στα αποτελέσματα. Περισσότερες πληροφορίες αλλά και αιτιολόγηση αυτών παρατίθενται στην Ενότητα 2.6 της εργασίας.

Ερώτηση 7: Έχουν ληφθεί υπόψη ηθικά ζητήματα;

Απάντηση: Ναι.

Αιτιολόγηση: Δόθηκαν πληροφορίες στους συνεντευξιαζόμενους σχετικά με την χρήση των δεδομένων που θα συλλέγονταν μέσα από μια δήλωση συναίνεσης. Οι πληροφορίες και οι επεξηγήσεις υπάρχουν και στο έγγραφο στην Νορβηγική γλώσσα. Τηρήθηκε η ανωνυμία κατά την διάρκεια της έρευνας, δηλαδή πληροφορία η οποία ενδεχομένως να συνδεόταν ή να «φωτογραφίζε» άτομα ή οργανισμούς αυτομάτως διαγραφόταν ή άλλαζε. Ως εκ τούτου, στην εργασία κανένα άτομο ή κανένας οργανισμός δεν είναι δυνατόν να αναγνωριστεί ενώ κατόπιν της ολοκλήρωσης της έρευνας, οι ηχογραφημένες συνεντεύξεις διαγράφηκαν. Περισσότερες πληροφορίες αλλά και αιτιολόγηση αυτών αναφέρονται στην Ενότητα 2.5 της εργασίας.

Ερώτηση 8: Ήταν η ανάλυση των δεδομένων ήταν αρκετά αυστηρή;

Απάντηση: Ναι.

Αιτιολόγηση: Όπως προαναφέρθηκε, χρησιμοποιήθηκε μια γενική επαγωγική προσέγγιση για την ανάλυση των δεδομένων. Τα βήματα που ακολουθήθηκαν από τα πρωτογενή δεδομένα στα κύρια ευρήματα αποτυπώνεται σε τέσσερα βήματα. Περισσότερες πληροφορίες αλλά και αιτιολόγηση αυτών αναφέρονται στην Ενότητα 2.3.5 της εργασίας.

Ερώτηση 9: Υπάρχει σαφής δήλωση των ευρημάτων;

Απάντηση: Ναι.

Αιτιολόγηση: Τα ευρήματα της μελέτης περιγράφονται ξεχωριστά για τον κάθε οργανισμό στο Κεφάλαιο 6: Ευρήματα. Οι πληροφορίες που αναφέρονται σε αυτό το κεφάλαιο δεν αποτελούν προϊόν επεξεργασίας από τους ερευνητές αλλά έχουν αποτυπωθεί, όπως δίνονται στις συνεντεύξεις ή στα έγγραφα.

Ερώτηση 10: Πόσο πολύτιμη είναι η έρευνα;

Αιτιολόγηση: Ήταν αρκετά πολύτιμη, αφού πέρα από το ότι παρείχε κάποιες σημαντικές συστάσεις για την προετοιμασία στην ανταπόκριση για μεγάλους οργανισμούς, πρόσφερε αρκετά λεπτομερή δεδομένα, τα οποία μπορούν να φανούν χρήσιμα και σε άλλους ερευνητές.

3.7.2 Περίπτωση FinanceOrg

Το δεύτερο μέρος ερωτήσεων αξιολόγησης και αναφοράς αφορά την μελέτη των (Ahmad, et al., 2012). Στην συνέχεια αναγράφονται οι 10 ερωτήσεις του εργαλείου CASP (Long, French, & Brooks, 2020) ακριβώς έτσι όπως αναγράφονται και στο εργαλείο και η συγκεκριμένη έρευνα απαντάει αυτά τα ερωτήματα με την σχετική αιτιολόγηση για να μπορέσει να αξιολογήσει την συγκεκριμένη μελέτη.

Ερώτηση 1: Υπάρχει σαφής δήλωση των στόχων της έρευνας;

Απάντηση: Ναι

Αιτιολόγηση: Η συγκεκριμένη μελέτη έχει ως στόχο να διερευνήσει ζητήματα που καλούνται οι ομάδες των οργανισμών να αντιμετωπίσουν. Ο στόχος δηλώνεται στο Κεφάλαιο 1: Εισαγωγή με πλήρη σαφήνεια και περισσότερες πληροφορίες.

Ερώτηση 2: Είναι κατάλληλη μια ποιοτική μεθοδολογία;

Απάντηση: Ναι.

Αιτιολόγηση: Η μέθοδος της συγκεκριμένης μελέτης είναι η μελέτη περίπτωσης.

Ερώτηση 3: Ο σχεδιασμός της έρευνας ήταν κατάλληλος για να αντιμετωπίσει τους στόχους αυτής;

Απάντηση: Ναι.

Αιτιολόγηση: Ο σχεδιασμός της έρευνας είναι ο κατάλληλος, ωστόσο δεν υπάρχει κάποια αναφορά που να το αιτιολογεί.

Ερώτηση 4: Ήταν η στρατηγική πρόσληψης κατάλληλη για τους στόχους της έρευνας;

Απάντηση: Ναι.

Αιτιολόγηση: Η επιλογή πραγματοποιήθηκε με γνώμονα τους στόχους της έρευνας. Οι ερευνητές ήθελαν να δώσουν μια συνολική εικόνα για το πως οι ομάδες του οργανισμού ενημερώνουν την ασφάλεια πληροφοριών. Έτσι οι

μισοί από του ερωτηθέντες κρίθηκε ότι θα πρέπει να τεθούν εκτός ομάδας απόκρισης περιστατικών ενώ άλλοι δυο είναι σε τμήματα του οργανισμού που θα πρέπει να ενημερώσουν την ομάδα αντιμετώπισης περιστατικών.

Ερώτηση 5: Τα δεδομένα συλλέχθηκαν με τέτοιο τρόπο ώστε να στηρίζουν το ερευνητικό ζήτημα;

Απάντηση: Ναι.

Αιτιολόγηση: Τα δεδομένα που συλλέχθηκαν από συνεντεύξεις, αποτελούν την κύρια πηγή συλλογής δεδομένων ενώ αξίζει να επισημανθεί ότι χρησιμοποιήθηκαν τεκμηριωμένα στοιχεία για την υποστήριξη των ευρημάτων.

Ερώτηση 6: Έχει ληφθεί επαρκώς υπόψη η σχέση μεταξύ του ερευνητή και των συμμετεχόντων;

Απάντηση: Δεν υπάρχει δυνατότητα απάντησης.

Αιτιολόγηση: Στο έγγραφο δεν αναγράφεται κάτι. Ωστόσο, συντάχθηκε από πολύ έμπειρους συγγραφείς, οι οποίοι διαθέτουν πλούσια αρθρογραφία πάνω στην ασφάλεια πληροφοριών. Κατά συνέπεια, θεωρείται δεδομένη η προσεκτική τακτική, με σκοπό την αποφυγή προκαταλήψεων κατά την συλλογή δεδομένων.

Ερώτηση 7: Έχουν ληφθεί υπόψη ηθικά ζητήματα;

Απάντηση: Δεν υπάρχει δυνατότητα απάντησης.

Αιτιολόγηση: Στο έγγραφο δεν αναγράφεται κάτι. Ωστόσο, συντάχθηκε από πολύ έμπειρους συγγραφείς, οι οποίοι διαθέτουν πλούσια αρθρογραφία πάνω στην ασφάλεια πληροφοριών. Κατά συνέπεια, θεωρείται δεδομένη η προσεκτική διατύπωση από πλευράς τους για την αποφυγή πρόκλησης ηθικών ζητημάτων.

Ερώτηση 8: Ήταν η ανάλυση των δεδομένων ήταν αρκετά αυστηρή;

Απάντηση: Ναι.

Αιτιολόγηση: Όπως προαναφέρθηκε, χρησιμοποιήθηκαν συνεντεύξεις ως βασική μέθοδο συλλογής δεδομένων αλλά και μελέτη σημειώσεων. Όλα τα δεδομένα που προέκυψαν επεξεργάστηκαν με ανοιχτή αξονική και επιλεκτική κωδικοποίηση από εξειδικευμένο λογισμικό που χρησιμοποιήθηκε.

Ερώτηση 9: Υπάρχει σαφής δήλωση των ευρημάτων;

Απάντηση: Ναι.

Αιτιολόγηση: Τα αποτελέσματα καταγράφονται στην Ενότητα 4.4 λεπτομερώς και με σαφήνεια. Έχουν διαχωριστεί σε πέντε διαφορετικά μέρη, ανάλογα με την κατηγορία στην οποία εντάσσονται.

Ερώτηση 10: Πόσο πολύτιμη είναι η έρευνα ;

Αιτιολόγηση: Ήταν αρκετά πολύτιμη καθώς γιατί πέρα από το ότι πρότεινε ένα μοντέλο διπλού βρόχου για εκμάθηση περιστατικών που θα βοηθούσε στην αντιμετώπιση συστημικών διορθωτικών μέτρων, πρόσφερε αρκετά λεπτομερή δεδομένα, τα οποία μπορούν να φανούν χρήσιμα και σε άλλους ερευνητές.

ΚΕΦΑΛΑΙΟ 4^ο: Μελέτες περιπτώσεων - Εισαγωγή

Για την παρούσα έρευνα χρησιμοποιήθηκαν δύο μελέτες περίπτωσης που αποτελούνταν συνολικά από τέσσερις οργανισμούς. Οι τρεις οργανισμοί προέρχονται από τη δημοσίευση των Hove & Tårnes και αφορούν τρεις μεγάλους, νορβηγικούς οργανισμούς, οι οποίοι στο πλαίσιο της ερευνητικής διαδικασίας, θα παραμείνουν ανώνυμοι (Hove & Tårnes, 2013). Επίσης, ο τέταρτος οργανισμός είναι η FinanceOrg (Ahmad, et al., 2012) με γραφεία σε τέσσερις ηπείρους. Στο συγκεκριμένο κεφάλαιο καταγράφονται ορισμένα βασικά στοιχεία και χαρακτηριστικά των υπό εξέταση οργανισμών.

4.1 Οργανισμός Α

Ο Οργανισμός Α (Hove & Tårnes, 2013) είναι ένας κρατικός οργανισμός με χιλιάδες υπάλληλους. Στα πλαίσια λειτουργίας του και ευθύνης του είναι ο αποκλειστικός χειρισμός των περισσότερων λειτουργιών πληροφορικής με ελάχιστες να ανατίθενται σε εξωτερικούς συνεργάτες. Στην έρευνα συμμετείχαν συνολικά δεκαπέντε εργαζόμενοι του οργανισμού Α ενώ ο βασικός συνεντευξιαζόμενος ήταν ο διευθυντής ασφάλειας πληροφοριών, ο οποίος είναι επιφορτισμένος με τεχνικά και διοικητικά καθήκοντα. Με βάση την χρονολογία της συνέντευξης την θέση αυτή την κατέχει δύο χρόνια.

4.2 Οργανισμός Β

Ο Οργανισμός Β (Hove & Tårnes, 2013) είναι ένας μη εμπορικός μεγάλος οργανισμός με χιλιάδες υπαλλήλους. Εξαιτίας της επεξεργασίας μεγάλων, πολύτιμων και ευαίσθητων πληροφοριών, κρίνεται υψηλή προτεραιότητα η ασφάλεια των πληροφοριών. Οι δυο κύριοι συνεντευξιαζόμενοι ήταν ο διευθυντής ασφάλειας πληροφορικής και ο διευθυντής εφοδιαστικής αλυσίδας. Και οι δυο ανήκουν στο τμήμα πληροφορικής του οργανισμού και συχνά εμπλέκονται στην διαχείριση συμβάντων. Ο οργανισμός Β σε έναν πολύ μεγάλο βαθμό έχει αναθέσει σε εσωτερικούς συνεργάτες διάφορες λειτουργίες της πληροφορικής. Στην έρευνα συμμετείχαν δεκαπέντε άτομα από τρία διαφορετικά τμήματα με υπαλλήλους που έχουν διοικητικά καθήκοντα αλλά και με υπαλλήλους που εκτελούν βασικές δραστηριότητες του οργανισμού.

4.3 Οργανισμός Γ

Ο Οργανισμός Γ (Hove & Tarnes, 2013) είναι ένα μεγάλος οργανισμός που παρέχει υπηρεσίες πληροφορικής, πέρα από την εσωτερική του λειτουργία ενώ διαθέτει χιλιάδες υπαλλήλους. Ο οργανισμός εφαρμόζει διαφορετικές πολιτικές λόγω της πληθώρας τμημάτων που την απαρτίζουν. Ο βασικός συνεντευξιαζόμενος ήταν ο επιχειρησιακός αρχηγός τμήματος, υπεύθυνος για την ασφάλεια, την ποιότητα, την συμμόρφωση αλλά και τον κίνδυνο. Επίσης, εκτός από την ευθύνη διαχείρισης συμβάντων του εταιρικού τμήματος ήταν υπεύθυνος και για την διαχείριση συμβάντων για υπηρεσίες που πρόσφεραν σε πελάτες. Γενικότερα, ο οργανισμός Γ αντιμετώπιζε συχνά περιστατικά ασφαλείας. Σε αυτή την θέση ο υπεύθυνος ήταν περίπου δύο χρόνια, με βάση την χρονολογία της συνέντευξης. Στην έρευνα συμμετείχαν έντεκα υπάλληλοι του οργανισμού που είχαν διαφορετικούς ρόλους, καθήκοντα και ευθύνες. Παράλληλα, μελετήθηκαν και αρκετά έγγραφα, όπως το εγχειρίδιο IRT, η εταιρική πολιτική ασφαλείας πληροφοριών, η περιγραφή της διαδικασίας διαχείρισης επιχειρηματικού κινδύνου, η περιγραφή της διαδικασίας διαχείρισης συμβάντων, η περιγραφή ρουτίνας σημαντικών περιστατικών και η πολιτική έκτακτης ανάγκης.

4.4 Οργανισμός FinanceOrg

Η FinanceOrg (Ahmad, et al., 2012) προσφέρει χρηματοοικονομικές υπηρεσίες και διαθέτει πάνω από είκοσι χιλιάδες υπαλλήλους και ένα εκατομμύριο πελάτες σε όλο τον κόσμο. Η ομάδα αντιμετώπισης περιστατικών του οργανισμού Δ, όπου τα περιστατικά ταξινομούνται σύμφωνα με το επίπεδο επιπτώσεων για τον οργανισμό, αποτελείται από τέσσερα άτομα, τα οποία ασχολούνται με περιστατικά χαμηλού και μεγάλου κινδύνου. Η συγκεκριμένη ομάδα διασφαλίζει ότι το κεντρικό δίκτυο του οργανισμού προστατεύεται και ταυτόχρονα, ανάλογα το περιστατικό, έχει την δυνατότητα να εντάξει στην ομάδα, με ταχύτερες διαδικασίες, δεκάδες άτομα που ανταποκρίνονται σε περιστατικά και εργάζονται στον οργανισμό.

Όταν συμβεί κάποιο περιστατικό υψηλού κινδύνου, τότε αναλαμβάνει η ομάδα αντιμετώπισης συμβάντων υψηλών επιπτώσεων. Δύο από τους συμμετέχοντες στην έρευνα εργάζονταν με ικανότητες αντιμετώπισης περιστατικών ενώ άλλοι δυο επιλέχθηκαν από τμήματα που θα έπρεπε να τους ενημερώσει η ομάδα αντιμετώπισης

περιστατικών ότι συμβαίνει κάποιο περιστατικό. Γενικότερα, οι μισοί από τους ερωτώμενους ήταν εκτός της ομάδας αντιμετώπισης περιστατικών.

ΚΕΦΑΛΑΙΟ 5^ο: ΑΠΟΤΕΛΕΣΜΑΤΑ

Για την ανάλυση των δεδομένων χρησιμοποιήθηκε η παραγωγική ή απαγωγική (deductive) μέθοδος ανάλυσης και κωδικοποίησης ποιοτικών δεδομένων ενώ για την ερμηνεία των δεδομένων χρησιμοποιήθηκε η ερμηνευτική και η κυριολεκτική προσέγγιση. Σύμφωνα με τον Jennifer (2011) στην κυριολεκτική αναγνώριση των δεδομένων ο ερευνητής επιδιώκει την ανίχνευση του εκφρασμένου νοήματος με έμφαση στον κυριολεκτικό χαρακτήρα. Η κυριολεκτική αναγνώριση συνδέεται άμεσα με την υιοθέτηση μιας οπτικής είτε ουσιολογικής είτε ρεαλιστικής, δηλώνοντας ότι ο ερευνητής προσπαθεί να τεκμηριώσει με μια κυριολεκτική εκδοχή αυτό που «υπάρχει» έξω. Σύμφωνα πάλι με τον ίδιο η ερμηνευτική ανάγνωση των δεδομένων αφορά την «ανάγνωση ανάμεσα από τα δεδομένα είτε αυτά είναι κείμενα είτε οπτικές παραστάσεις ή οτιδήποτε άλλο». Με αυτήν την ανάγνωση ο ερευνητής μπορεί να ανιχνεύσει και να διακρίνει υπονοούμενα και κανόνες με του οποίους λειτουργεί ο ερωτώμενος. Επίσης έχει την δυνατότητα να ανιχνεύσει τα είδη του θεματικού λόγου και του τρόπους που με το οποίους συγκρατούνται αλλά και την ύπαρξη μηχανισμών αιτιότητας στο πλαίσιο της κοινωνικής πράξης. Τέλος ακόμη μπορεί να εστιάσει σε ερμηνείες, αναφορές αλλά και αντιλήψεις που υποδηλώνουν το πώς τα αντικείμενα της έρευνας αντιλαμβάνονται νοηματικά και κοινωνικά φαινόμενα.

Τα αποτελέσματα που καταγράφονται στη συνέχεια έχουν αποτυπωθεί σχεδόν με τον ίδιο τρόπο με τον οποίο αντλήθηκαν από τις αρχικές έρευνες, με σκοπό την αποφυγή οποιασδήποτε παρερμηνείας. Για την κωδικοποίηση των δεδομένων και την ανάλυση τους συμβουλευτικά τα άρθρα των Skjott Linneberg & Korsgaard, (2019) και των Bandara, Furtmueller, Gorbacheva, Miskon & Beekhuyzen (2015) ενώ για την ερμηνεία τους τον Jennifer (2011) (Linneberg & Korsgaard, 2019; Bandara, Furtmueller, Gorbacheva, Miskon, & Beekhuyzen, 2015; Jennifer, 2011).

5.1 Εισαγωγή

Η Finance ακολουθεί την βιβλιογραφία και τα πλαίσια CERT, ITIL και ISO 27002.

Ο Οργανισμός Α δεν στοχεύει σε κάποια πιστοποίηση αλλά έχει εφαρμόσει το ISO/IEC 27001 και 27002. Το πρότυπο ISO/IEC 27035 δεν εφαρμόζεται στον οργανισμό. Για τη διαχείριση συμβάντων ασφαλείας εφαρμόζει το πλαίσιο ITIL. Σε γενικές γραμμές δεν έχουν θέσει σε εφαρμογή όλες τις συστάσεις από τα ISO/IEC

27001 και 27002, καθώς και το πλαίσιο ITIL. Εντούτοις, έχουν εφαρμόσει αυτές που θεωρούν ότι τους αφορούν.

Πολλές από τις διαδικασίες στον Οργανισμό Β στηρίζονται στο πλαίσιο ITIL και στο πρότυπο ISO, καταβάλλοντας προσπάθεια ώστε τα σχέδια έκτακτης ανάγκης να βασίζονται και αυτά στο ISO. Το πρότυπο ISO/IEC 27035 δεν έχει εφαρμοστεί για τη διαχείριση συμβάντων.

Ο Οργανισμός Γ και ιδιαίτερα ο διευθυντής του οργανισμού δεν φαίνεται να είναι εξοικειωμένος με το πρότυπο ISO 27035 για την αντιμετώπιση και διαχείριση συμβάντων. Για το ISO/IEC 27001 διαθέτει αρκετές πιστοποιήσεις ενώ στηρίζει πλήρως τις διαδικασίες διαχείρισης στο πλαίσιο ITIL.

5.2 Αποτελέσματα σχετικά με την ικανότητα των οργανισμών να ανακαλύπτουν περιστατικά ασφαλείας

5.2.1 FinanceOrg

Αναφορικά με τα συστήματα, στην Finance υπάρχει σύστημα για την παρακολούθηση συμβάντων αλλά και δύο διαφορετικές ομάδες αντιμετώπισης περιστατικών. Στην πρώτη ομάδα έχει ανατεθεί να προστατεύει τον οργανισμό με οποιοδήποτε τρόπο ενώ η δεύτερη έχει δημιουργηθεί για συμβάντα υψηλού αντίκτυπου και έχει τη δυνατότητα, ανάλογα με τον βαθμό χρησιμότητας να επεκταθεί σε επιπλέον ανταποκριτές. Οι δύο ομάδες μεταξύ τους λειτουργούν ανεξάρτητα αλλά δεν αποκλείει η μία την άλλη, με απώτερο στόχο την συνεργασία, όποτε αυτή κριθεί απαραίτητη.

Στον οργανισμό έχουν θεσμοθετηθεί διάφορες υψηλόβαθμες θέσεις. Μια από αυτές είναι και η θέση του διευθυντή της ομάδας αντιμετώπισης συμβάντων ασφαλείας δικτύου. Διαθέτει υψηλού επιπέδου εκπαίδευσης με δυο μεταπτυχιακά και αρκετά μεγάλη εμπειρία στον συγκεκριμένο χώρο. Μια άλλη θέση εξαιρετικής σημασίας είναι αυτή του διευθυντή της ομάδας συντονισμού αντιμετώπισης συμβάντων υψηλού αντικτύπου, όπου συντονίζει και συνεργάζεται με διάφορους εκπροσώπους επιχειρήσεων, τεχνικές ομάδες και αρκετούς άλλους μέχρι την οριστική διευθέτηση και επίλυση του προβλήματος.

Τέλος, ακόμα μία σημαντική θέση είναι του ανώτερου μέλους της ομάδας πολιτικής και διαδικασιών ασφαλείας πληροφοριών, ο οποίος διαθέτει ένα ιδιαίτερα ισχυρό

τεχνικό υπόβαθρο αλλά και πολυετή εμπειρία πάνω στην ασφάλεια. Ο ίδιος εργάζεται στην Finance, με μια ομάδα τεσσάρων ατόμων και είναι ο υπεύθυνος για την διαχείριση αλλά και την δημιουργία γενικών πολιτικών ασφάλειας πληροφοριών για τον οργανισμό της Finance.

5.2.2 Οργανισμός Α

Ο Οργανισμός Α έχει στη διάθεση και στην κατοχή του διάφορα συστήματα, εργαλεία και διαδικασίες για την ανίχνευση περιστατικών, κάτι το οποίο εξάλλου συνιστάται και από τις κατευθυντήριες γραμμές. Για την ανίχνευση ανεπιθύμητης αλληλογραφίας έχει στη διάθεσή του εργαλεία που χρησιμοποιούνται για την ανάλυση των συγκεκριμένων email. Επίσης, τα περιστατικά αρχικής ανίχνευσης μπορούν να αναφερθούν μέσω του συστήματος κατάχρησης τους. Στην κατοχή του Οργανισμού Α υπάρχει ένα νέο σύστημα διαχείρισης αποκλίσεων, το οποίο μπορεί να χρησιμοποιηθεί για την αναφορά διάφορων αποκλίσεων από την ασφάλεια των πληροφοριών. Η λειτουργία αυτού του συστήματος επεκτείνεται σαν βάση δεδομένων για τα συμβάντα που λαμβάνουν χώρα τον οργανισμό.

Ένα ακόμα εργαλείο που διαθέτει ο Οργανισμός Α σχετίζεται με την παρακολούθηση των συνδέσεων στο δίκτυο του, με την δυνατότητα ανίχνευσης περιστατικών. Οι κάτοχοι συστήματος του οργανισμού, εάν πέσει στην αντίληψη τους κάποια ευπάθεια, ειδοποιούν τον υπεύθυνο ασφαλείας IT και στη συνέχεια ο ίδιος πραγματοποιεί συγκεκριμένες ενέργειες για να αντιμετωπιστεί το συμβάν. Ο Οργανισμός Α διαθέτει έναν διευθυντή στον τομέα του Διαδικτύου του οργανισμού, ο οποίος ειδοποιεί, σε περίπτωση που διαπιστώσει παραβιασμένους κεντρικούς υπολογιστές.

Οι περισσότεροι από τους υπαλλήλους που εμπλέκονται σε συμβάντα διαθέτουν υψηλού επιπέδου εκπαίδευση και αρκετές γνώσεις πάνω στον τομέα της πληροφορικής. Οι ίδιοι ακολουθούν το πρότυπο ISO/IEC 27002, σύμφωνα με το οποίο αυτοί που αναφέρουν συμβάντα ασφαλείας πληροφοριών θα πρέπει κιόλας να ενημερώνονται για τα αποτελέσματα αυτού.

Αρκετοί από τους εργαζόμενους φάνηκε να μην έχουν τις απαιτούμενες γνώσεις και τα προσόντα για την αναγνώριση περιστατικών, γεγονός που υποδηλώνει ότι οι πόροι για την ανίχνευση περιστατικών δεν χρησιμοποιούνται στο μέγιστο τους. Από τους εργαζόμενους πάλι που συμμετείχαν στην έρευνα αυτή διαπιστώθηκε ότι δεν

γνώριζαν είτε ότι έπρεπε να αναφέρουν περιστατικά είτε με ποιο τρόπο και υπό ποιες συνθήκες έπρεπε να τα αναφέρουν. Οι περισσότεροι υπάλληλοι που συμμετείχαν στην έρευνα αυτή πίστευαν ότι είναι σε θέση να καταλάβουν εάν έπρεπε να αναφέρουν περιστατικό. Ωστόσο, από τα συμπεράσματα που προέκυψαν υπάρχει σημαντική πιθανότητα να ισχύουν για ολόκληρη την ομάδα του οργανισμού.

5.2.3 Οργανισμός B

Ο Οργανισμός B χρησιμοποιεί συστήματα και τους υπαλλήλους του για την ανίχνευση περιστατικών. Το γεγονός αυτό εναρμονίζεται με τη σύσταση των περισσότερων προτύπων και κατευθυντήριων γραμμών. Διαθέτει Antivirus, το οποίο εντοπίζει και αναφέρει πιθανούς ιούς. Επίσης, οι υπάλληλοι έχουν τη δυνατότητα να κάνουν σχετική αναφορά μόλις αντιληφθούν ότι υπάρχει κάποια δυσλειτουργία στον υπολογιστή τους. Αυτή η αναφορά γίνεται στο γραφείο εξυπηρέτησης του Supplier 1. Ακόμα μια πηγή εντοπισμού περιστατικών για τον Supplier 1 είναι το ίδιο το δίκτυο. Σε αυτή την περίπτωση έχει την ευθύνη παρακολούθησης του, καθώς οποιεσδήποτε αλλαγές στην κίνηση του, συνήθως υποδηλώνουν συμβάντα ασφαλείας. Συχνά αυτό το δίκτυο αισθητήρων ανατίθεται σε εξωτερική ομάδα ασφάλειας.

Ο Supplier 1 του οργανισμού B διαθέτει μια ομάδα, όπου λαμβάνει συχνά αυτοματοποιημένες αναφορές περιστατικών. Αυτή η ομάδα είναι διαθέσιμη ολόκληρο το 24ωρο. Ο Supplier 2 έχει και αυτός στη διάθεση του ομάδες για τη διαχείριση περιστατικών στον οργανισμό B. Η μία ομάδα είναι επιφορτισμένη με τις κρίσεις και η άλλη ομάδα με την καθημερινή διαχείριση και τη συντήρηση. Και αυτές οι ομάδες είναι διαθέσιμες όλο το 24ωρο, αναζητώντας συνεχώς βελτίωση των διαδικασιών αλλά και να σχεδιάζουν αναθεωρήσεις σχεδίων.

Ο διευθυντής δικτύου του Οργανισμού B και άλλοι συνεργάτες ενδέχεται επίσης να εντοπίσουν ένα περιστατικό ασφαλείας. Ο διευθυντής της εφοδιαστικής αλυσίδας δήλωσε ότι είναι πεπεισμένος πως υπάρχει υπό-αναφορά περιστατικών μέσα στον οργανισμό, παρόλο που δεν το βλέπει σαν πρόβλημα, αφού είναι αδύνατο να εντοπίζονται τα πάντα. Ο δυνητικά υψηλός βαθμός αυτών των υποδηλώσεων δεν σημαίνει ότι παραλείπουν τον εντοπισμό των βασικών απειλών και ότι μπορούν να συνεχίσουν να εφαρμόζουν τα σωστά μέτρα για την αποφυγή των σοβαρών περιστατικών.

Με βάση την ιστορία του Οργανισμού B ο Supplier 2 έχει χειριστεί με επιτυχία μέχρι σήμερα όλα τα κρίσιμα περιστατικά των τελευταίων ετών. Ο μεγαλύτερος φόβος και το χειρότερο περιστατικό που θα μπορούσε να αντιμετωπίσει ο οργανισμός B, σύμφωνα με τους συνεντευξιαζόμενους, ήταν οι επίορκοι υπάλληλοι, οι οποίοι διαρρέουν πληροφορίες σε τρίτους, χωρίς να γίνονται αντιληπτοί. Επίσης, κάποιοι υπάλληλοι δεν γνώριζαν με βεβαιότητα που πρέπει να αναφέρουν περιστατικά.

Ο Supplier 1 και ο Supplier 2 είναι σχετικά καινούργιοι στη θέση του διευθυντή στον οργανισμό B, κατά συνέπεια δεν έχουν αρχεία και ιστορικά προηγούμενων περιστατικών. Ωστόσο, όπως φαίνεται, έχουν αποκτήσει αρκετές επιπλέον γνώσεις, αφού χειρίζονται τις καθημερινές λειτουργίες του τομέα της πληροφορικής και της διαχείρισης εφαρμογών του οργανισμού B. Επιπλέον, έχουν θέσει ως βασική προϋπόθεση στους υπαλλήλους του γραφείου εξυπηρέτησης να είναι πιστοποιημένοι με το ITIL.

5.2.3 Οργανισμός Γ

Ο Οργανισμός Γ έχει και αυτός στην κατοχή του συστήματα παρακολούθησης για την ανίχνευση περιστατικών. Αυτό βρίσκεται σύμφωνο με τις συστάσεις ISO/IEC, NIST και ENISA. Συνιστάται στους εργαζόμενους κάθε φορά που αντιμετωπίζουν κάτι μη φυσιολογικό να το αναφέρουν στην ομάδα αντιμετώπισης περιστατικών. Χαρακτηριστικό παράδειγμα είναι η λήψη αγνώστου αποστολέα email ή συνημμένα email που δεν λειτουργούν, όπως πρέπει.

Υπάρχει ειδικό πλαίσιο κινδύνου στον οργανισμό, το οποίο παρέχει τη δυνατότητα να αναφέρονται τρωτά σημεία, με σκοπό την άμεση εφαρμογή μέτρων στη συνέχεια. Για την αρχική ανίχνευση των περιστατικών στον Οργανισμό Γ μπορεί είτε να εκτελεστεί αυτόματα από διακομιστή και να ενεργοποιηθεί συναγερμός είτε να ανακαλυφθεί χειροκίνητα. Συχνά η ανάλυση του δικτύου πρέπει να διεξάγεται χειροκίνητα για τον εντοπισμό παραβιάσεων ασφαλείας. Ο Οργανισμός Γ έχει σαν απαίτηση σε ό,τι αφορά την διαχείριση συμβάντων, να δηλώνονται όλα τα συμβάντα και να καταχωρούνται στο σύστημα τους. Ο Οργανισμός Γ κατέχει και ένα κεντρικό εργαλείο για την τεκμηρίωση περιστατικών, εκτός από τις εμπειρίες, τις πιθανές βελτιώσεις και τους εσωτερικούς ελέγχους.

5.3 Αποτελέσματα σχετικά με τις ρουτίνες, διαδικασίες, σχέδια και πρόβες για τον χειρισμό και την αντιμετώπιση των περιστατικών

5.3.1 Finance

Η Finance έχει ορίσει στις αρμοδιότητες της ομάδας αντιμετώπισης περιστατικών δικτύου να υπάρχουν προληπτικές δοκιμές ευπάθειας και διείσδυσης δικτύου αλλά και ανταπόκριση σε περιστατικά που αποτελούν απειλή για δίκτυα. Χαρακτηριστικό παράδειγμα ανάλογων περιστατικών είναι οι προσβολές από ιούς. Όσο αναφορά τα περιστατικά χαμηλού αντικτύπου η ομάδα αντιμετώπισης περιστατικών δικτύου έχει την υποχρέωση να συντάσσει πολυάριθμες επίσημες εκθέσεις για την διαχείριση, εστιάζοντας κυρίως σε τεχνικά σημεία. Ουσιαστικά πρόκειται για στατιστικά έγγραφα που περιέχουν μόνο γενικευμένες πληροφορίες εκμάθησης. Για τα συγκεκριμένα έγγραφα η ομάδα χρησιμοποιεί άτυπα κανάλια επικοινωνίας, προκειμένου να διαδώσει την γνώση των περιστατικών. Η ομάδα εστιάζει σε τεχνικές πτυχές και συλλέγει μεγάλες ποσότητες εγκληματολογικών δεδομένων ενώ ανταποκρίνεται γρήγορα για τον εντοπισμό των βασικών αιτιών του περιστατικού. Με άλλα λόγια επικεντρώνεται στην προστασία του βασικού δικτύου, με περιορισμό και κλιμάκωση, όπου κρίνεται απαραίτητο.

Στις συνεδριάσεις που πραγματοποιούνται συμβάλλουν και τεχνικά μέλη για να παραχθεί μια ολοκληρωμένη αναφορά για το συμβάν. Αυτή η αναφορά περιέχει λεπτομέρειες, καθώς και την αιτιώδη δομή του συμβάντος ενώ ακόμα αναφέρει και εντοπίζει κενά σε θέματα πολιτικής και συντήρησης. Στην συνέχεια πραγματοποιείται μια αξιολόγηση κινδύνου και ανατίθενται καθήκοντα στο αρμόδιο προσωπικό, μέσω του συστήματος παρακολούθησης συμβάντων.

Η Finance θεωρεί τον τρόπο με τον οποίο ταξινομεί τα περιστατικά της αρκετά ευαίσθητο και έχει αρκεστεί στο να κοινοποιήσει την ύπαρξη μιας σαφούς και τυποποιημένης μεθόδου για τον προσδιορισμό επιπέδου των επιπτώσεων ενός περιστατικού. Ουσιαστικά μετά την αναφορά περιστατικών και σύμφωνα με την διαδικασία υπάρχουν κάποια συστήματα HelpDesk, Email και τηλεφωνικές επαφές, όπου και ταξινομούν τα περιστατικά και ειδοποιούν την κατάλληλη ομάδα. Τόσο στα περιστατικά μεγάλης επίπτωσης όσο και στα περιστατικά χαμηλής επίπτωσης η διαφορά στην δημιουργία γνώσης είναι αισθητή και έντονη.

Στα περιστατικά όπου ο αντίκτυπος είναι υψηλός υπάρχει αυστηρά τυποποιημένη διαδικασία και πραγματοποιείται πάντα ανασκόπηση. Η διαδικασία συλλογής των πληροφοριών στα περιστατικά με μεγάλη επίπτωση είναι αρκετά ώριμη και είναι πιθανό να περιλαμβάνει μεγάλο αριθμό τεχνικού και επιχειρηματικού προσωπικού. Μάλιστα για τον λόγο αυτό, ο διευθυντής της ομάδας συντονισμού αντιμετώπισης συμβάντων υψηλού αντικτύπου αναφέρει ότι μετά από ένα τέτοιο περιστατικό πραγματοποιούνται δύο κλήσεις διάσκεψης, εκ των οποίων η μια είναι τεχνικού χαρακτήρα και η άλλη επαγγελματικού. Σε αυτές τις κλήσεις εμπλέκονται ο διευθυντής της ομάδας συντονισμού αντιμετώπισης συμβάντων υψηλού αντικτύπου και οι αντίστοιχοι επικεφαλής επιχειρήσεων που θα πρέπει να λάβουν μια λεπτομερή και επικαιροποιημένη ενημέρωση.

Το γεγονός απόκλισης του προσωπικού στις πρώτες δύο συνεδριάσεις αναφοράς περιστατικού επηρεάζει κατά πολύ την γνωστοποίηση των συμβάντων. Ο οργανισμός δεν χρησιμοποιεί όλα τα περιστατικά για εκμάθηση και δεν καταβάλλει μεγάλες προσπάθειες ως προς αυτή την κατεύθυνση. Η ομάδα αντιμετώπισης περιστατικών για την εκμάθηση από αυτά είναι πιο κοντά στο να ακολουθεί εκμάθηση ενός βρόχου, παρά διπλού βρόχου. Δηλαδή, οι εργαζόμενοι εντοπίζουν και στη συνέχεια διορθώνουν, χωρίς να υπάρχει λεπτομερής έρευνα για τα αίτια που προκάλεσαν το περιστατικό.

5.3.2 Οργανισμός Α

Ο Οργανισμός Α πραγματοποίησε ενάμιση χρόνο πριν την μελέτη περίπτωσης μια εκστρατεία ευαισθητοποίησης και μια πρόβα έκτακτης ανάγκης ενώ είχε και προγραμματισμένες για την ίδια χρονιά νέες πρόβες, εκ των οποίων μία από αυτές θα διεξαγόταν σε συνεργασία με έναν άλλον οργανισμό. Η εκστρατεία ευαισθητοποίησης ήταν σε συνεργασία με εξωτερικό παράγοντα. Ουσιαστικά, στα πλαίσια αυτής της εκστρατείας στάλθηκαν διαφάνειες στους εργαζόμενους μέσω email που περιείχαν μικρές διαλέξεις με θέματα, όπως για παράδειγμα η προστασία των κωδικών πρόσβασης. Η πρόβα έκτακτης ανάγκης που πραγματοποιήθηκε είχε ως θέμα την ασφάλεια των πληροφοριών και πραγματοποιήθηκε με τη συμμετοχή της διοίκησης ενώ αποτελούταν από επτά επίπεδα κλιμάκωσης. Η εκπαίδευση αλλά και το σχέδιο έκτακτης ανάγκης συνέβαλαν στην αύξηση της ευαισθητοποίησης σχετικά με την ασφάλεια πληροφοριών στην διοίκηση.

Ο οργανισμός για να μπορεί να προσδιορίζει κάθε φορά τα ζητήματα που πρέπει να επικεντρώνεται στις πρόβες χρησιμοποιεί τις αξιολογήσεις κινδύνου και ευπάθειας. Επίσης, χρησιμοποιεί τις πρόβες για καταστάσεις «ρουτίνας» αλλά και για καταστάσεις που δεν έχουν καμία «ρουτίνα». Οπότε, κατά τη διάρκεια μιας πρόβας δίνεται η δυνατότητα να προσδιοριστούν τα θέματα «ρουτίνας» που πρέπει να εφαρμοστούν. Ο διευθυντής ασφάλειας IT του Οργανισμού Α δήλωσε ότι οι περιπτώσεις «ρουτίνας», έχουν συνήθως ομαλή λειτουργία. Ενώ σε περιπτώσεις που δεν λειτούργησαν όπως έπρεπε, πραγματοποιήθηκε επανεξέταση.

Επίσης, ανέφερε ότι αντιμετωπίζουν πολύ συχνά περιστατικά που δεν είναι «ρουτίνας» και ότι δεν είναι δυνατόν ο οργανισμός να έχει διαδικασίες «ρουτίνας» για όλες τις περιπτώσεις. Οι πρόβες τους περιλαμβάνουν καταστάσεις που δεν χαρακτηρίζονται «ρουτίνας», με αποτέλεσμα να δίνεται η ευκαιρία στην ομάδα να μπορεί να εκπαιδευτεί πάνω στον αυτοσχεδιασμό και σε περιστατικά που δεν έχουν προκαθορισμένα σχέδια. Μια ακόμα διαδικασία που ακολουθεί ο οργανισμός αφορά την πρόσληψη καινούργιων υπαλλήλων, οι οποίοι υπόκεινται σε μια εκπαιδευτική διαδικασία, διαφορετική από αυτή που θα κληθούν να αντιμετωπίσουν όταν αναλάβουν τα νέα τους καθήκοντα.

Ο διαχειριστής ασφάλειας IT μετά από ένα περιστατικό δεν εστιάζει στην εκκίνηση της λειτουργίας των συστημάτων αλλά βεβαιώνεται πρώτα ότι το περιστατικό επιλύθηκε σωστά και ότι τα επηρεαζόμενα συστήματα δεν είναι ευάλωτα σε άλλες επιθέσεις. Υπήρξαν περιπτώσεις που ο διαχειριστής ασφάλειας IT ήθελε να πραγματοποιήσει αξιολογήσεις κινδύνου και ευπάθειας συστημάτων αλλά δεν του επιτράπη, εξαιτίας των περιορισμένων πόρων. Στον Οργανισμό Α μετά από κάθε περιστατικό ο κάτοχος του συστήματος πρέπει να προσδιορίσει ποιες πληροφορίες έχουν παραβιαστεί ή χαθεί και να κάνει μια εκτίμηση της οικονομικής ζημίας που προκλήθηκε στον Οργανισμό Α. Ανάμεσα σε αυτές τις αξίες που προσβλήθηκαν, όπως είναι η αξία των πληροφοριών είναι εξαιρετικά δύσκολο να εκτιμηθεί το μέγεθος της ζημίας.

Με την αναφορά περίπτωσης στο σύστημα κατάχρησης του Οργανισμού Α τότε αμέσως κατηγοριοποιείται και αποστέλλεται στη γραμμή αντιμετώπισης περιστατικών. Στην γραμμή αντιμετώπισης περιστατικών είτε το θέμα επιλύεται είτε αποστέλλεται με τη σειρά του σε άλλο τμήμα με καλύτερο εξοπλισμό. Ένα τέτοιο τμήμα, για παράδειγμα, είναι το Τμήμα Δικτύου του Οργανισμού Α. Επίσης, ένα

περιστατικό έχει τη δυνατότητα να επιλυθεί μέσα από την συνεργασία μεταξύ των χειριστών του περιστατικού και των εργαζομένων από άλλα τμήματα. Στην περίπτωση που ένα περιστατικό είναι ιδιαίτερα σοβαρό γίνεται αναφορά στη διοίκηση. Ο υπεύθυνος πληροφορικής του Οργανισμού Α ειδοποιείται μόνο σε περιπτώσεις μεγάλων περιστατικών και όχι σε περιπτώσεις ρουτίνας.

Ο Οργανισμός Α δεν έχει αναπτύξει ροές εργασίας που να ισχύουν για όλα τα περιστατικά αλλά αντίθετα έχει αναπτύξει ροές για συγκεκριμένα είδη περιστατικών. Υπάρχουν καταγεγραμμένα αναλυτικά τα βήματα των συγκεκριμένων κατηγοριών περιστατικών. Χαρακτηριστικό είναι το παράδειγμα ενός περιστατικού botnet. Επίσης, ο Οργανισμός Α διαθέτει σχέδιο έκτακτης ανάγκης για το τμήμα πληροφορικής του που περιλαμβάνει την περιγραφή αρκετών τύπων συμβάντων. Αυτό το σχέδιο ενεργοποιείται όταν ένα περιστατικό είναι ιδιαίτερα σοβαρό και περιλαμβάνει σενάρια που τα συστήματα δεν είναι διαθέσιμα. Αποτελείται από επικοινωνίες ρουτίνας που σχετίζονται με συμβάντα ενώ σε περίπτωση που υπάρξει περιστατικό αυτού του βαθμού σοβαρότητας εμπλέκεται και η διοίκηση.

Δεν έχει αναπτυχθεί κάποιο ολιστικό σχέδιο για τον χειρισμό των περιστατικών στον Οργανισμό Α, καθώς υπάρχει μεγάλη ποικιλία περιστατικών που το καθένα απαιτεί και μια διαφορετική λύση και αντιμετώπιση. Εντούτοις, υπάρχουν καταγεγραμμένες γενικές οδηγίες που αφορούν τον χειρισμό συμβάντων ασφαλείας. Για παράδειγμα, το phishing είναι συνηθισμένο περιστατικό για τον Οργανισμό Α και έχουν ακολουθούνται λεπτομερείς οδηγίες για την αντιμετώπιση του. Ο υπεύθυνος ασφαλείας πληροφορικής ανέφερε ότι ο Οργανισμός Α δεν διαθέτει τόσο λεπτομερείς οδηγούς, που να λαμβάνουν υπόψη όλες τις πιθανές εκδοχές περιστατικών αλλά και ότι δεν υπάρχει τέτοια φιλοδοξία στο κοντινό μέλλον.

5.3.3 Οργανισμός Β

Ο Οργανισμός Β δεν ακολουθεί συγκεκριμένη πολιτική για την αντιμετώπιση και διαχείριση των περιστατικών αλλά έχει θεσπίσει κάποιες πρακτικές ρουτίνας και υποστηρικτικά εργαλεία. Επίσης, για τη διασφάλιση της διαθεσιμότητας των υπηρεσιών εφαρμόζει πλεονάζον εξοπλισμό και άλλους μηχανισμούς. Ο Supplier 1 έχει την υποχρέωση να διασφαλίζει ότι τα συστήματα του οργανισμού δημιουργούν σε καθημερινή βάση αντίγραφα ασφαλείας. Παράλληλα, ο ίδιος πραγματοποιεί ελέγχους στα αντίγραφα για να σιγουρευτεί ότι είναι σε θέση να χρησιμοποιηθούν.

Εκτελείται συχνά σάρωση λογισμικού στους υπολογιστές του Οργανισμού Β για τον εντοπισμό τρωτών σημείων σε παλιά λογισμικά και για την αποφυγή εκμετάλλευσης τους. Τα λογισμικά που εντοπίζονται με τρύπες ασφαλείας αφαιρούνται. Πριν προχωρήσει σε αυτή την αφαίρεση ο Supplier 1, κατηγοριοποιεί και ιεραρχεί τα τρωτά σημεία για να μπορέσει να καθορίσει την αναγκαιότητα της ενημέρωσης που απαιτείται ενώ για ευπάθειες μηδενικής ημέρας που εντοπίζονται είναι πιθανό να τερματίσουν κάποιες υπηρεσίες.

Ο Supplier 1 παρακολουθεί διαρκώς τις τάσεις των συμβάντων ασφαλείας αλλά και τα εσωτερικά συστήματα του οργανισμού. Οι τάσεις που προκύπτουν, γνωστοποιούνται και στον Οργανισμό Β. Επίσης, ο ίδιος έχει στην διάθεση του ένα σύστημα διαχείρισης υποθέσεων, όπου και εκεί καταγράφονται όλες οι υποθέσεις που προκύπτουν. Χάρη σε αυτόν τον τρόπο υπάρχει και παρακολούθηση των προηγούμενων περιστατικών του Οργανισμού Β.

Όσον αφορά τις περιπτώσεις έκτακτης ανάγκης έχουν αναπτυχθεί συγκεκριμένα σχέδια έκτακτης ανάγκης σε συνεργασία με τον οργανισμό, τα οποία ελέγχονται κάθε δύο χρόνια. Στον Οργανισμό Β διεξάγονται τακτικά πρόβες με σκοπό την ευαισθητοποίηση και την καλύτερη προετοιμασία για την πρακτική αντιμετώπιση περιστατικών, ενώ συζητούν και εσωτερικές πρόβες ρουτίνας με τους υπαλλήλους. Σε αυτές τις συζητήσεις συμμετέχουν και εξωτερικά άτομα που συνδράμουν στην εκπαίδευσή τους. Στις πρόβες έκτακτης ανάγκης λαμβάνουν επίσης μέρος και οι Suppliers 1 και 2, ο διευθυντής IT, η ομάδα κρίσης, οι βασικές λειτουργίες του Οργανισμού Β και η εξυπηρέτηση πελατών από τον Διευθυντή.

Ουσιαστικά κατά τη διάρκεια της πρόβας θα τους παρουσιαστεί ένα περιστατικό, με απώτερο σκοπό τον έλεγχο των διαδικασιών ρουτίνας, καθώς και την εύρυθμη λειτουργία τους. Ταυτόχρονα, κατέστη σαφής η σημασία των προβών και ότι πρέπει να επαναλαμβάνονται συνεχώς, ώστε να επιτευχθεί η ορθή λειτουργία τους. Ο Supplier 2 πραγματοποιεί συχνά πρόβες έκτακτης ανάγκης σε χαρτί για την ομάδα κρίσης. Δεν υπάρχει καθιερωμένη λίστα στον Οργανισμό Β που πρέπει να ακολουθείται κατά την απόκριση σε περιστατικό. Ωστόσο υπάρχει λίστα ελέγχου που περιλαμβάνει το κεντρικό σχέδιο έκτακτης ανάγκης.

Ο Supplier 2 έχει δημιουργήσει ένα σχέδιο για την διαχείριση συμβάντων του Οργανισμού Β. Αυτό το σχέδιο βασίζεται στα επίπεδα επιπτώσεων του κάθε

συμβάντος και έχει να κάνει μόνο με εφαρμογές, καθώς ο ίδιος δεν είναι υπεύθυνος για δεδομένα. Στον Οργανισμό B υπάρχει μια διαδικασία για τα περιστατικά που εντοπίζει ο Supplier 1. Σε πρώτη φάση τις περισσότερες φορές ειδοποιεί τον οργανισμό με Email και στη συνέχεια ειδοποιεί μια ομάδα για την διαχείριση του περιστατικού. Εάν το περιστατικό δεν περιοριστεί έγκαιρα και εξαπλωθεί ειδοποιείται για να αναλάβει καθήκοντα η ομάδα κρίσης. Η επικοινωνία από εκείνο το σημείο και έπειτα διεξάγεται με Email, μέσω τηλεφώνου, ακόμα και μέσω προσωπικής επικοινωνίας.

Τα περισσότερα περιστατικά που καλείται να αντιμετωπίσει ο Supplier 1 είναι περιπτώσεις ρουτίνας που συνήθως χρησιμοποιούνται τυπικές διαδικασίες. Εάν όμως το περιστατικό είναι αρκετά σοβαρό, τότε είναι απαραίτητο να εμπλακεί ο συντονιστής ασφαλείας, ο οποίος και είναι αρμόδιος για την επικοινωνία μεταξύ Supplier 1 και οργανισμού. Όλα τα περιστατικά που καλείται ο Οργανισμός B να αντιμετωπίσει καταγράφονται στο ίδιο σύστημα. Στο αρχείο καταγραφής υπάρχουν πληροφορίες, όπως η βασική αιτία του συμβάντος, πιθανές παραβιάσεις SLA, οι ενέργειες που ακολουθήθηκαν καθώς και οι πιθανές λύσεις.

Ο διευθυντής IT ανέφερε ότι η εξασφάλιση μιας σταθερής συλλογής πληροφοριών κατά τη διάρκεια ενός συμβάντος, σε συνδυασμό με την λήψη ορθών αποφάσεων τις σωστές στιγμές είναι σημαντικότερα από ένα ολιστικό σχέδιο. Το σχέδιο αυτό είναι ένα από τα πιο απαιτητικά μέρη της διαχείρισης συμβάντων, καθώς τις περισσότερες φορές είναι πιθανό να συμβούν πράγματα που δεν υπάρχει προγενέστερη γνώση για τον τρόπο αντιμετώπισης τους.

Ο Supplier 1 έχει αναλάβει να χειρίζεται συμβάντα που σχετίζονται με λειτουργίες πληροφορικής και υπάρχει συγκεκριμένη ροή εργασιών για συμβάντα που δεν κλιμακώνονται ενώ είναι στη κρίση του η κατηγοριοποίηση τους. Ο Supplier 2 είναι υπεύθυνος για χειρισμό συμβάντων που σχετίζονται με εφαρμογές, όπου υπάρχει και σε αυτή την περίπτωση ακριβής διαδικασία ροής εργασιών. Για περιστατικά, τα οποία αφορούν απόρρητο εργαζομένων, είναι ορισμένη ακριβής διαδικασία, σύμφωνα με την οποία δίνεται η δέουσα προσοχή για την αποφυγή παραβίασης απορρήτου. Επιπροσθέτως, ο Supplier 2 έχει αναπτύξει ξεκάθαρες διαδικασίες ρουτίνας για την κλιμάκωση και έχει ορίσει τα άτομα επικοινωνίας. Τέλος αν κριθεί απαραίτητο, έχουν την αρμοδιότητα να καλέσουν μέχρι και ομάδα διαχείρισης κρίσεων.

Ο διευθυντής πληροφορικής του Οργανισμού Β δήλωσε ότι η εκπαίδευση από τρίτους είναι ένας σημαντικός παράγοντας για την επίτευξη των στόχων τους. Ο Supplier 2 οργανώνει συνέδρια με την ομάδα αντιμετώπισης περιστατικών για να μοιραστεί τις εμπειρίες του κατά τη διάρκεια του χειρισμού περιστατικών και να συζητήσει διάφορα θέματα για το τι συνέβη και τα περιθώρια βελτίωσης.

5.3.4 Οργανισμός Γ

Στον Οργανισμό Γ πραγματοποιούνται τακτικά συνέδρια και παρουσιάσεις αναφορικά με την ασφάλεια, με τον υπεύθυνο ασφάλειας πληροφορικής του οργανισμού να δηλώνει ότι εκτελούνται εκτεταμένες εργασίες για την ευαισθητοποίηση των εργαζομένων σε θέματα ασφάλειας. Το εγχειρίδιο ασφαλείας αναθεωρείται σε ετήσια βάση και κατά τη διάρκεια των αξιολογήσεων των εργαζομένων. Οι εργαζόμενοι από την πλευρά τους θα πρέπει να επιβεβαιώσουν εκ νέου ότι το περιεχόμενο είναι γνωστό. Το ζητούμενο είναι να αυξηθεί η συνολική ικανότητα και να διασφαλιστεί ότι οι κατευθυντήριες γραμμές ασφαλείας είναι γνωστές.

Για τους υπάλληλους που αντιμετωπίζουν συνηθισμένα περιστατικά ο Οργανισμός Γ δεν πραγματοποιεί εκπαιδευτικές δράσεις. Αυτό συμβαίνει, σύμφωνα με τον υπεύθυνο ασφάλειας πληροφορικής, επειδή τα σχέδια και οι διαδικασίες χρησιμοποιούνται τόσο συχνά, που δεν συντρέχει ιδιαίτερος λόγος να πραγματοποιηθεί και να προγραμματιστούν εκπαιδευτικά σεμινάρια που να σχετίζονται με αυτές τις περιπτώσεις. Ωστόσο, μια φορά το χρόνο ο οργανισμός διεξάγει πρόβες με σενάρια που θεωρείται από τους αρμόδιους ότι είναι απαραίτητα. Ταυτόχρονα, πραγματοποιούνται πρόβες και με τους πελάτες τους.

Ο οργανισμός έχει ένα προκαθορισμένο σχέδιο επικοινωνίας με τα ΜΜΕ κατά τη διάρκεια μεγάλων περιστατικών. Οι νέοι υπάλληλοι συμμετέχουν σε μαθήματα εξοικείωσης με το εγχειρίδιο ασφαλείας του οργανισμού ενώ είναι απαραίτητο να υπογράψουν ότι το περιεχόμενο είναι γνωστό και κατανοητό. Οι απαιτήσεις που έχει θέσει ο οργανισμός αφορούν την διαδικασία διαχείρισης συμβάντων και ουσιαστικά απαιτεί όλα τα περιστατικά και οι ενέργειες να καταγράφονται.

Ο Οργανισμός Γ προχώρησε σε ένα έργο βελτίωσης, όπου μέσα από αυτό εντόπισαν την αδύναμη ποιότητα στις περιγραφές της αλυσίδας αξίας ως πρόβλημα για την αποτελεσματική αντιμετώπιση περιστατικών. Το διαγνωστικό έργο ήταν περίπλοκο

ενώ μερικές φορές ήταν δύσκολο να εντοπιστεί τι ακριβώς συνέβη, πού συνέβη και με ποια επακόλουθα. Παρόλα αυτά, είχαν ξεκινήσει εκτεταμένες εργασίες για τον εντοπισμό κάθε μεμονωμένου σημείου αποτυχίας. Τα θετικά αποτελέσματα που προέκυψαν από την υλοποίηση του συγκεκριμένου έργου οδήγησαν στην επέκταση και σε μεγαλύτερα τμήματα του οργανισμού. Στόχος του έργου είναι ο εντοπισμός των τρωτών σημείων και τους τομείς βελτίωσης ενώ είναι ευθύνη των διαφόρων τμημάτων να εφαρμόσουν τις προτεινόμενες αλλαγές. Μέχρι στιγμής το έργο έχει οδηγήσει σε βελτιώσεις και νέες διαδικασίες ρουτίνας, ενισχύοντας την αλληλεπίδραση με τρίτα μέρη και δημιουργώντας μια συνολική θετική τάση για τα μικρά περιστατικά εντός του οργανισμού.

Ο Οργανισμός Γ διαθέτει δύο ομάδες αντιμετώπισης περιστατικών. Η πρώτη ομάδα αντιμετώπισης περιστατικών, κατά τη διάρκεια της απόκρισης συντονίζει όλα τα εμπλεκόμενα μέρη ενώ η δεύτερη που ονομάζεται ομάδα διαχείρισης κρίσιμων περιστατικών λειτουργεί συμπληρωματικά και εσωτερικά για την πρώτη ομάδα. Μια από τις βασικές απαιτήσεις του Οργανισμού Γ σχετικά με τη διαδικασία διαχείρισης περιστατικών είναι η πλήρης καταγραφή των ενεργειών που εκτελούνται από τις ομάδες, με σκοπό να παρέχεται η δυνατότητα και σε άλλους να συνεχίσουν τον χειρισμό της εργασίας, σε περίπτωση που κριθεί απαραίτητο. Ο Οργανισμός Γ διαθέτει δικό του εγχειρίδιο που αποσκοπεί στην εκμάθηση του τρόπου λειτουργίας της ομάδας αντιμετώπισης περιστατικών αλλά και στην εξήγηση τις εσωτερικών διαδικασιών ρουτίνας στα νέα μέλη της ομάδας.

Υπάρχει συγκεκριμένη ροή εργασιών για τη διαχείριση συμβάντων που βασίζεται στο πλαίσιο ITIL. Τα μεγάλα περιστατικά έχουν ξεχωριστές διαδικασίες και μια λεπτομερή ροή εργασιών, καθώς τις περισσότερες φορές έχουν υψηλό βαθμό επιρροής από τους χρήστες, με αποτέλεσμα να θεωρούνται πιο επείγοντα και με σφικτούς χρονικούς περιορισμούς για την απόκρισή τους.

5.4 Αποτελέσματα σχετικά με τον αντίκτυπο στους οργανισμούς

5.4.1 Finance

Η διαδικασία που ακολουθείται μετά την επίλυση του περιστατικού, δηλαδή η έρευνα και οι συνεδριάσεις με συμμετέχοντες και αρκετά τεχνικά μέλη για την δημιουργία μιας αναφοράς με βάθος στη λεπτομέρεια έχει επιφέρει τη δραστική μείωση των περιστατικών από περίπου 200 το μήνα σε 16 από το 2002 μέχρι την διεξαγωγή της

μελέτης περίπτωσης. Επίσης, σημαντική μείωση των περιστατικών απέφεραν τα περιστατικά με υψηλό αντίκτυπο που διέπονται από τη διαδικασία παρακολούθησης και λεπτομερούς αιτιολόγησης, με απώτερο σκοπό τη λήψη διορθωτικών μέτρων.

5.4.2 Οργανισμός Α

Οι πρόβες του Οργανισμού Α αποκάλυψαν αρκετά σημαντικά πράγματα με σημαντικότερο όλων την έλλειψη αίσθησης κινδύνου από τους υπαλλήλους του.

5.4.3 Οργανισμός Β

Ο διευθυντής εφοδιαστικής αλυσίδας του Οργανισμού β ανέφερε ότι παρατηρείται μείωση του αριθμού των περιστατικών ασφαλείας, παρά το γεγονός ότι η διαδικασία μέτρησης της επίδρασης των εκστρατειών ευαισθητοποίησης είναι ιδιαίτερα δύσκολη. Ο Supplier 2 χειρίστηκε με επιτυχία οποιοδήποτε κρίσιμο περιστατικό κλήθηκε να αντιμετωπίσει. Εξαιρετικά σημαντικός παράγοντας ως προς αυτή την κατεύθυνση ήταν η διενέργεια επαφών με τους κατάλληλους τεχνικούς πόρους την σωστή στιγμή. Επίσης, άλλο ένα βασικό στοιχείο που αποτυπώθηκε στις πρόβες του Οργανισμού Β με αποδέκτες τους υπαλλήλους είναι να μην εμπιστεύονται απόλυτα τις ηλεκτρονικές μορφές σχεδίων έκτακτης ανάγκης, τα οποία καλό είναι να υπάρχουν τόσο σε έντυπη, όσο και σε ηλεκτρονική μορφή.

5.4.4 Οργανισμός Γ

Μια πρόκληση που αποκαλύφθηκε μέσα από τις πρόβες ήταν η επικοινωνία του οργανισμού και των πελατών του σε διάφορα περιστατικά. Ο Οργανισμός Γ στα πλαίσια της διαδικασίας εκπαίδευσης ακολουθεί το πρωτόκολλο ITIL, όπου και εντοπίζονται βελτιώσεις κατά τη διαδικασία αυτή. Επίσης, η προσπάθεια βελτίωσης διαχείρισης συμβάντων έχει αποδειχθεί ιδιαίτερα αποτελεσματική, τουλάχιστον μέχρι τη στιγμή διεξαγωγής της μελέτης περίπτωσης.

5.5 Αποτελέσματα σχετικά με την επιρροή του ανθρώπινου παράγοντα

5.5.1 Finance

Στην αρκετά έμπειρη και αποτελεσματική ομάδα αντιμετώπισης περιστατικών της Finance, παρατηρείται η έλλειψη ικανότητας εκμετάλλευσης της οργανωσιακής μάθησης.

Ο οργανισμός έχει θεσπίσει ορισμένες υψηλόβαθμες θέσεις. Για παράδειγμα, ο διευθυντής ομάδας αντιμετώπισης συμβάντων ασφαλείας δικτύου έχει υψηλό επίπεδο εκπαίδευσης, με δύο μεταπτυχιακά πάνω στον τομέα της πληροφορικής και μεγάλη εμπειρία τόσο στη δικτύωση όσο και στην ασφάλεια. Ο ίδιος εργάζεται στον οργανισμό δυόμισι χρόνια από τη στιγμή διεξαγωγής της έρευνας. Ο διευθυντής της ομάδας συντονισμού αντιμετώπισης συμβάντων υψηλού αντίκτυπου διαθέτει αρκετές τεχνικές και επιχειρηματικές γνώσεις για το προσωπικό και τα πληροφοριακά συστήματα του οργανισμού. Τέλος, το ανώτερο μέλος της ομάδας πολιτικής και διαδικασιών ασφαλείας πληροφοριών διαθέτει ισχυρό τεχνικό υπόβαθρο και πολυετή εμπειρία.

Σε γενικές γραμμές, στον οργανισμό της Finance υπάρχει μια θετική κουλτούρα για την αντιμετώπιση περιστατικών, καθώς δεν τιμωρείται, όποιος αναφέρει περιστατικά.

5.5.2 Οργανισμός Α

Από τους 15 ερωτηθέντες υπαλλήλους του Οργανισμού Α, αναφορικά με την εξοικειώσή τους με την πολιτική ασφαλείας, οι 3 ήταν θετικοί, 5 ήταν αρνητικοί και 7 είχαν ακούσει λίγα πράγματα για την πολιτική ασφαλείας, χωρίς το περιεχόμενο της να είναι ιδιαίτερα άγνωστο.

Οι περισσότεροι από αυτούς δεν ανέφεραν ποτέ ύποπτο email ενώ μικρός αριθμός υπαλλήλων ανέφερε ελάχιστες περιπτώσεις. Επίσης, οι περισσότεροι είχαν λάβει ύποπτα email, με έναν από τους εργαζόμενους να κάνει λόγο για spam email και όχι στοχευμένα. Εν κατακλείδι, κανένας από τους υπαλλήλους δεν αναγνώρισε ότι άνοιξε ή ότι εκτέλεσε οδηγίες από ένα τέτοιο email.

Σε σχέση με το τι είναι ένα περιστατικό ασφαλείας πληροφοριών, λίγοι θεώρησαν ότι γνωρίζουν ενώ σχεδόν οι μισοί δεν γνώριζαν ή δεν ήταν εξοικειωμένοι με τον ορισμό, αναγνωρίζοντας την άγνοια τους. Οι υπόλοιποι να παρουσιάζονται με έλλειψη σιγουριάς. Μεγάλο ποσοστό υπαλλήλων δήλωσε ως παράδειγμα πιθανού περιστατικού ασφαλείας πληροφοριών την κοινή χρήση κωδικών πρόσβασης, τα διαπιστευτήρια σύνδεσης και τις ευαίσθητες πληροφορίες. Κατά τη διάρκεια της εργασίας τους στον οργανισμό και σε καθημερινό επίπεδο, δήλωσαν ότι ήταν αρκετά προσεκτικοί, παρόλο που αρκετοί από αυτούς δεν ήταν βέβαιοι για τον ορισμό των περιστατικών ασφαλείας πληροφοριών. Μερικοί δικαιολόγησαν την αβεβαιότητα

αυτή με το ότι δεν βρίσκονταν συχνά σε καταστάσεις όπου η ασφάλεια των πληροφοριών είναι σχετική.

Παράλληλα, ένας υπάλληλος ανέφερε ότι από την εφαρμογή του συστήματος κλειδώματος θυρών που αποσκοπούσε στη βελτίωση της ασφάλειας, οδήγησε αρκετούς υπαλλήλους στο να νιώσουν ασφάλεια, αφήνοντας πολλές φορές τους υπολογιστές ξεκλειδωτους, καθώς και τις πόρτες γραφείων μη ασφαλισμένες.

Από το σύνολο των εργαζομένων, μόνο ένας δήλωσε ότι γνωρίζει σε ποιες περιπτώσεις αλλά και σε ποιους θα έπρεπε να αναφέρει ένα περιστατικό ασφάλειας. Η πλειοψηφία των εργαζομένων δήλωσε ότι δεν ήταν σίγουρη για το ποια περιστατικά πρέπει να αναφέρονται. Εντούτοις, όπως επεσήμαναν αρκετοί υπάλληλοι η κοινή λογική καθοδηγούσε τις επιλογές τους και ότι αν κρινόταν απαραίτητο θα ειδοποιούσαν τον άμεσο προϊστάμενο τους. Σχεδόν οι μισοί από τους υπαλλήλους που συμμετείχαν στην έρευνα είχαν παρακολουθήσει διαδικτυακές διαλέξεις και παρουσιάσεις για την ασφάλεια πληροφοριών. Η πλειοψηφία όσων είχαν παρακολουθήσει τέτοιου είδους εκπαιδευτικές δράσεις δήλωσαν ότι το περιεχόμενο τους ήταν ήδη γνωστό αλλά παρόλα αυτά, το βρήκαν χρήσιμο.

5.5.3 Οργανισμός B

Από τους 15 ερωτηθέντες υπαλλήλους του Οργανισμού B, αναφορικά με την πολιτική ασφάλειας πληροφοριών, μόλις δύο από αυτούς δεν ήταν εξοικειωμένοι, οκτώ ήταν σε κάποιο βαθμό, χωρίς ωστόσο να γνωρίζουν λεπτομέρειες ενώ ένας μόνο ανέφερε ότι έχουν γίνει αρκετές αλλαγές στον οργανισμό τα τελευταία χρόνια που σχετίζονται με την πολιτική ασφάλειας. Επίσης, δήλωσε ότι πολλές φορές δεν υπήρχε η κατάλληλη ενημέρωση προς τους εργαζόμενους για τις αλλαγές αυτές.

Αρκετοί λαμβάνουν συχνά email με ανεπιθύμητο περιεχόμενο αλλά είναι σε θέση να το αναγνωρίσουν εύκολα. Μόλις ένας δήλωσε ότι δεν είχε λάβει ποτέ κανένα ύποπτο email ενώ δεν ανέφερε κανείς ότι είχε λάβει κάποιο στοχευμένο email ή ότι ακολούθησε οδηγίες από κάτι σχετικό. Υπήρχε μια εξαίρεση όμως, όπου ένας υπάλληλος δήλωσε ότι ακολούθησε τέτοιες οδηγίες εσκεμμένα και με ασφαλή τρόπο καθαρά από περιέργεια. Περισσότεροι δεν αναφέρουν τέτοιες περιπτώσεις, επειδή είναι κάτι πολύ συνηθισμένο.

Για τον ορισμό του περιστατικού ασφάλειας πληροφοριών, 6 από τους υπαλλήλους γνώριζαν τι αφορά, 5 δεν κατάφεραν να δώσουν τον ορισμό του αλλά είχαν μια ιδέα

για το περί τίνος πρόκειται ενώ οι υπόλοιποι δήλωσαν ότι δεν γνωρίζουν. Οι περισσότεροι από τους εργαζόμενους κατάφεραν να δώσουν ένα παράδειγμα για το τι είναι περιστατικό ασφάλειας πληροφοριών, καθώς και άλλα παραδείγματα σχετικά με λανθασμένες πληροφορίες, κωδικούς πρόσβασης, αποθήκευσης ευαίσθητων πληροφοριών σε μη κρυπτογραφημένα USB, χρήση άγνωστων USB και παραβίαση οδηγιών ασφαλείας ή κοινή χρήση του ίδιου υπολογιστή.

Υπήρξε μια ομάδα υπαλλήλων που δήλωσε ότι δεν γνώριζε τι είναι το περιστατικό ασφάλειας πληροφοριών. Εντούτοις, οι περισσότεροι από αυτούς ήταν ιδιαίτερα προσεκτικοί στα περιστατικά, χωρίς να γνωρίζουν τον όρο. Δηλαδή, όπως ανέφεραν χαρακτηριστικά το κλείδωμα της οθόνης του υπολογιστή τους, ότι κλειδώνουν τις πόρτες των γραφείων τους, ακόμα και ότι καταστρέφουν ευαίσθητα έγγραφα. Ένας διευθυντής τμήματος πληροφορικής επεσήμανε την προσπάθειά του για την μεταλαμπάδευση στους υπαλλήλους του της θεωρίας που αναφέρει ότι δεν θα θεωρηθούν υπεύθυνοι στην περίπτωση που προκαλέσουν ένα περιστατικό ασφάλειας.

Όσον αφορά τη δήλωση των περιστατικών, οι περισσότεροι δεν ήταν σίγουροι για το ποιες περιπτώσεις πρέπει να αναφέρουν. Επίσης, μπροστά σε ένα τέτοιο ενδεχόμενο θα είχαν αναφερθεί στον τοπικό κεντρικό διευθυντή πληροφορικής, χωρίς ωστόσο να είναι σίγουροι, αν αυτή είναι μια ενδεδειγμένη διαδικασία, με έναν από αυτούς να δηλώνει ότι θα αναφερόταν στον διευθυντή IT ή στον Supplier 1. Οι υπάλληλοι που δεν γνώριζαν τον ορισμό και την έννοια του περιστατικού ασφάλειας, εξακολουθούν να πιστεύουν ότι είναι σε θέση να αναγνωρίσουν εάν πρέπει να αναφέρουν ένα περιστατικό σε περίπτωση που συμβεί. Φυσικά υπήρξαν και αυτοί που δεν ήταν ιδιαίτερα εξοικειωμένοι με τις διαδικασίες υποβολής και αναφοράς εκθέσεων από τη στιγμή που δεν παρέσθη ανάγκη να το μάθουν.

Στον Οργανισμό B, αναφορικά με τις εκστρατείες ευαισθητοποίησης που είχαν πραγματοποιηθεί στο παρελθόν, ένας διευθυντής πληροφορικής έλαβε θετικά σχόλια από τους υπαλλήλους του και μάλιστα αυτό υποστηρίχθηκε και από αρκετούς που διάβασαν τις διαδικτυακές διαφάνειες. Δήλωσαν ότι τις βρήκαν ιδιαίτερα χρήσιμες, παρόλο που γνώριζαν το περιεχόμενό τους, με την πλειοψηφία να ζητάει επανάληψη τέτοιων ενημερωτικών και εκπαιδευτικών εκστρατειών. Δύο από αυτούς που είχαν διαβάσει τις διαδικτυακές διαφάνειες, απάντησαν πως δεν τις βρήκαν χρήσιμες ενώ ένας εκ των δύο δήλωσε ότι κάποια μέτρα ήταν τόσο αυστηρά που θα προτιμούσε να λάβει υπόψη τον κίνδυνο, παρά να τα εφαρμόσει.

Ο ρόλος του Supplier 1 είναι η στενή παρακολούθηση των τάσεων που σχετίζονται με τα περιστατικά ασφάλειας. Ταυτόχρονα είναι συμβατός ο ρόλος του και σύμφωνα με τις συστάσεις για τη φάση της προετοιμασίας από το πρότυπο ISO/IEC 27035.

Για τον Οργανισμό Β η κατανομή των πόρων για την ανάπτυξη λεπτομερών σχεδίων δεν αποτελεί ένα από τους κύριους στόχους του, αφού θεωρείται ότι η ύπαρξη έμπειρων χειριστών συμβάντων είναι αρκετά πιο χρήσιμη και σημαντικότερη για την επιτυχία των χειρισμών αυτών.

Η συμμετέχοντες υπάλληλοι στην έρευνα του Οργανισμού Β δήλωσαν ότι το χειρότερο δυνατό περιστατικό ασφάλειας και ο μεγαλύτερος φόβος που θα μπορούσαν να αντιμετωπίσουν είναι οι επίορκοι υπάλληλοι που διαρρέουν πληροφορίες σε τρίτους χωρίς να αποκαλυφθεί η ταυτότητα τους.

Ο διευθυντής της εφοδιαστικής αλυσίδας δήλωσε ότι η έλλειψη σωστής επικοινωνίας είναι πιθανόν να οδηγήσει σε περιττά προβλήματα. Η σιωπηρή γνώση των ευθυνών σε περιπτώσεις όχι τόσο σημαντικές είναι ένα παράδειγμα ρουτίνας που είναι δύσκολο να τεκμηριωθεί σωστά. Τέλος, δήλωσε ότι ενδέχεται να ανακύψουν προβλήματα ακόμη και με μικρά περιστατικά, ιδιαίτερα σε περιπτώσεις όπου δεν παίρνει κανείς την ευθύνη και υποθέτουν ότι η ευθύνη είναι κάποιου άλλου.

Στον Οργανισμό Β αναφέρθηκε ότι σε περίπτωση που τα μέτρα ασφαλείας κριθούν ιδιαίτερα περίπλοκα για τους χρήστες, θα βρουν εναλλακτικούς τρόπους για να τα παρακάμψουν, με αποτέλεσμα τα αρχικά μέτρα ασφαλείας τίθενται σε κίνδυνο. Οι 2 υπάλληλοι που αναφέρθηκαν νωρίτερα, οι οποίοι δεν βρήκαν χρήσιμες τις εκστρατείες, έχουν ένα ιστορικό στο κομμάτι της πληροφορικής, όπου σύμφωνα με την αρχική έρευνα μελέτης περίπτωσης ενδεχομένως να δηλώνει αρνητική στάση απέναντι στις δραστηριότητες ευαισθητοποίησης αλλά και μια μη ικανοποιητική κουλτούρα ασφάλειας. Αξίζει εντούτοις να σημειωθεί ότι ο αριθμός αυτών των υπαλλήλων ήταν μικρός, συγκριτικά με όσους βρήκαν χρήσιμες τις εκστρατείες ευαισθητοποίησης.

5.5.4 Οργανισμός Γ

Στον Οργανισμό Γ ο διευθυντής ασφάλειας πληροφορικής πιστεύει ότι το όριο αναφοράς περιστατικών ήταν υψηλό και ότι οι εργαζόμενοι συχνά δεν ανέφεραν τυχόν ύποπτα γεγονότα. Εν συνεχεία, δήλωσε ότι είχε υποψιαστεί την υπό-αναφορά περιστατικών μεταξύ των εργαζομένων. Ως πιθανές αιτίες θεωρεί πρωτίστως ότι οι

εργαζόμενοι δεν είναι ικανοί να αντιληφθούν τη σημασία της αναφοράς περιστατικών ή ότι δεν ήθελαν να αναγνωρίσουν πιθανά λάθη που έκαναν.

Ο οργανισμός δεν υποστηρίζει καμία λειτουργία ανώνυμης αναφοράς συμβάντων ασφαλείας για τους υπαλλήλους αλλά παρέχει τη δυνατότητα χρήσης εξωτερικής δικηγορικής εταιρείας, σε περίπτωση που επιθυμεί κάποιος να κάνει ανώνυμη αναφορά περιστατικού. Ο διευθυντής ασφάλειας IT δεν ήταν εξοικειωμένος με το πρότυπο ISO 27035 που σχετίζεται με την αντιμετώπιση με τη διαχείριση συμβάντων ασφαλείας. Η πολιτική ασφάλειας πληροφοριών του Οργανισμού Γ είναι αρκετά γνωστή στους εργαζόμενους που συμμετείχαν στην έρευνα.

Ο διευθυντής ασφάλειας IT δήλωσε ότι οι αιτήσεις αξιολόγησης των εργαζομένων ασφαλείας εντοπίζουν πάντα ένα θέμα. Οι περισσότεροι από τους εργαζόμενους έδειξαν ότι έχουν γνώσεις για το τι είναι ένα περιστατικό ασφαλείας πληροφοριών ενώ ταυτόχρονα στον οργανισμό θεωρούν ότι είναι αρκετά σημαντικό να υπάρχει ένα θετικό περιβάλλον για την ασφάλεια και κάνουν συνεχείς προσπάθειες προς αυτή την κατεύθυνση.

ΚΕΦΑΛΑΙΟ 6^ο : ΣΥΜΠΕΡΑΣΜΑΤΑ

6.1 Συμπεράσματα για το πρώτο ερευνητικό ερώτημα

Ο οργανισμός της Finance έχει στην κατοχή του συστήματα για την ανίχνευση περιστατικών αλλά και δυο ομάδες αρκετά έμπειρες. Επίσης, διαθέτει άτομα με εμπειρία και γνώσεις σε σημαντικές θέσεις. Παρόλο που δεν δίνονται ιδιαίτερα πολλές πληροφορίες για το κατά πόσο ο οργανισμός έχει την ικανότητα να αναγνωρίσει περιστατικά, με βάση την εμπειρία του οργανισμού και των ατόμων που εργάζονται σε αυτόν φαίνεται πως είναι ικανός να ανιχνεύσει περιστατικά ασφάλειας είτε αυτά είναι κρίσιμα είτε πιο απλές περιπτώσεις.

Ο Οργανισμός Α έχει διάφορα συστήματα ανίχνευσης περιστατικών που ποικίλουν ανάλογα τις περιπτώσεις, όπως ανάλυση email και παρακολούθηση δικτύου. Επιπρόσθετα, έχουν οριστεί διάφορες θέσεις μέσα στον οργανισμό, όπως ο υπεύθυνος ασφαλείας IT, στον οποίο έχουν την δυνατότητα οι υπάλληλοι να αναφέρουν αν διακρίνουν κάτι ασυνήθιστο σε αυτούς. Αναφορικά με τους υπαλλήλους αυτοί που εμπλέκονταν άμεσα με το αντικείμενο διέθεταν την δέουσα εμπειρία ενώ κάποιοι άλλοι εργαζόμενοι φάνηκε να μην είναι τόσο καταρτισμένοι. Είχαν πολύ βασικά κενά, όπως το να μην είναι σίγουροι για το τι πρέπει να αναφέρουν, σε ποιον και υπό ποιες συνθήκες. Αυτές οι διαπιστώσεις υπήρχαν στους υπαλλήλους που συμμετείχαν στις συνεντεύξεις, οπότε υπάρχει μεγάλη πιθανότητα να ισχύουν τα ίδια αποτελέσματα και για τους υπόλοιπους.

Εξαιτίας της έλλειψης επαρκών γνώσεων των υπαλλήλων, ο Οργανισμός Α είναι πιθανό να αντιμετωπίσει περιπτώσεις, όπου θα παρατηρείται καθυστέρηση στην αντίληψη του περιστατικού. Ενώ αυτά τα περιστατικά θα μπορούσαν να προέρχονται από αμέλεια ή από έλλειψη γνώσεων των υπαλλήλων του και όχι από κάποιο λάθος από τα συστήματα ανίχνευσης που έχει στη διάθεσή του, ωστόσο δεν διαφαίνεται ότι το συγκεκριμένο αποτέλεσμα μπορεί να προκαλέσει μεγάλη ζημιά στον οργανισμό. Με εξαίρεση τα παραπάνω, ο Οργανισμός Α φαίνεται πως είναι σε θέση να ανιχνεύσει περιστατικά ασφάλειας.

Ο Οργανισμός Β ανιχνεύει περιστατικά μέσω συστημάτων που έχει στη διάθεσή του αλλά και από τις αναφορές των υπαλλήλων του. Ενδιαφέρον προκαλεί το στοιχείο ότι ο Supplier 1 του οργανισμού διαθέτει μια ομάδα που λαμβάνει αυτοματοποιημένες

ειδοποιήσεις για περιστατικά κατά τη διάρκεια του 24ωρου. Αυτό δείχνει μια αρκετά υγιή διαδικασία για την ανίχνευση περιστατικών ενώ αποδεικνύει έμπρακτα και το ενδιαφέρον του οργανισμού στο να εντοπίζονται όσο το δυνατόν περισσότερα περιστατικά ή συμβάντα.

Αυτό έρχεται σε αντίθεση με το ότι πιστεύουν ότι υπάρχει υπό-αναφορά περιστατικών, χωρίς να το βλέπουν ως πρόβλημα. Ακόμα, υπήρξαν δηλώσεις από ορισμένους υπαλλήλους που ανέφεραν ότι δεν ήταν και πολύ σίγουροι για το που έπρεπε να αναφέρουν περιστατικά. Γενικότερα, όλα τα κρίσιμα περιστατικά τον τελευταίο χρόνο έχουν αντιμετωπιστεί με επιτυχία, γεγονός που αποδεικνύει ότι οτιδήποτε σημαντικό υπήρξε, ανιχνεύθηκε, χωρίς ωστόσο να γνωρίζουμε το πόσο έγκαιρη ήταν η ανίχνευση. Όπως συμπεραίνεται όμως από τα δεδομένα δεν επηρέασε τον οργανισμό το χρονικό διάστημα της ανίχνευσης. Φυσικά υπήρξαν και κάποιοι υπάλληλοι όπου δήλωσαν ότι δεν γνωρίζουν ή ότι δεν ήταν πολύ σίγουροι για το πού πρέπει να αναφέρουν περιστατικά. Αυτό ίσως αποδεικνύει ότι ο Οργανισμός Β μάλλον δεν έχει κάνει σαφείς και ξεκάθαρες τις διαδικασίες του για την ανίχνευση περιστατικών σε όλους τους εργαζόμενους.

Αξιοσημείωτη ήταν η δήλωση ότι ο μεγαλύτερος φόβος και το χειρότερο περιστατικό που θα μπορούσαν να αντιμετωπίσουν είναι οι επίορκοι υπάλληλοι που διαρρέουν πληροφορίες σε τρίτους. Αυτή και μόνο η δήλωση καταδεικνύει μια ιδιαίτερη στάση, μη εμπιστοσύνης από τον οργανισμό προς τους εργαζόμενους. Ο Οργανισμός Β φαίνεται να έχει κάποιες καλές διαδικασίες για την ανίχνευση περιστατικών, πέρα από τα συστήματα που έχει στη διάθεσή του και δείχνει ικανός στην ανίχνευση αυτών, παρόλα τα θέματα που αντιμετωπίζει με τους υπαλλήλους του.

Ο Οργανισμός Γ έχει και αυτός κάποια συστήματα για την ανίχνευση περιστατικών. Επίσης, διαθέτει ένα ειδικό πλαίσιο κινδύνου που αναφέρονται τα τρωτά σημεία. Μια ιδιαίτερη απαίτηση όμως που εντοπίστηκε ήταν ότι ζητούσε ο οργανισμός να δηλώνονται όλα τα συμβάντα και να καταχωρούνται στο σύστημά του. Αυτό για την ανίχνευση περιστατικών θα μπορούσε να σημαίνει ότι εάν υπάλληλοι ή οποιοσδήποτε άλλος παρατηρήσει κάτι μη συνηθισμένο, θα μπορεί να ανατρέξει στο αρχείο και να δει αν σχετίζεται με κάποιο περιστατικό που είχε αντιμετωπίσει στο παρελθόν. Σε γενικές γραμμές ο Οργανισμός Γ με τις διαδικασίες και τα συστήματα που διαθέτει φαίνεται ικανός να μπορεί να ανιχνεύσει και να αναγνωρίσει ένα περιστατικό ασφαλείας ή συμβάν.

Αναφορικά με το ερευνητικό ερώτημα που τέθηκε, όλοι οι οργανισμοί βρέθηκαν να έχουν συστήματα για την ανίχνευση περιστατικών. Στους Οργανισμούς Α και Β φαίνεται ότι υπήρχε θέμα με τους υπαλλήλους τους, δηλαδή ότι αρκετοί από αυτούς δεν γνώριζαν πότε και πού πρέπει να αναφέρουν περιστατικά. Αυτό βέβαια δεν φαίνεται να επηρεάζει σε σημαντικό βαθμό την ανίχνευση τους. Γενικά, όλοι οι οργανισμοί φαίνονται να έχουν τις δυνατότητες να ανιχνεύουν περιστατικά με τον καθένα από αυτούς να αντιμετωπίζει και κάποια προβλήματα πάνω σε αυτό τον τομέα, τα οποία ωστόσο δεν δείχνουν να τους επηρεάζουν σε μεγάλο βαθμό.

6.2 Συμπεράσματα για το δεύτερο ερευνητικό ερώτημα

Στον οργανισμό της Finance υπάρχουν καθημερινές δοκιμές ευπάθειας, πρόβες, συντάσσονται επίσημες εκθέσεις, συλλέγονται μεγάλες ποσότητες από εγκληματολογικά δεδομένα και πραγματοποιούνται συνεδριάσεις περιστατικών για περαιτέρω ανάλυση. Όλα τα παραπάνω δείχνουν μια ώριμη κουλτούρα προετοιμασίας για την διαχείριση και αντιμετώπιση συμβάντων με συγκεκριμένες διαδικασίες και ενδιαφέρον του οργανισμού για ευαισθητοποίηση των εργαζομένων του. Ένα ενδιαφέρον εύρημα υπάρχει στην διαδικασία για περιστατικά χαμηλού αντικτύπου. Αναλυτικότερα, για τα περιστατικά χαμηλού αντίκτυπου η ομάδα αντιμετώπισης περιστατικών δικτύου έχει την υποχρέωση να συντάσσει αρκετές επίσημες εκθέσεις με περιεχόμενο τη διαχείριση και τεχνικά σημεία.

Για την ταξινόμηση των περιστατικών ο οργανισμός έχει αναπτύξει διαδικασίες που υλοποιούνται αμέσως μετά την ανίχνευση του και οδηγούν στην ειδοποίηση των κατάλληλων ατόμων για να διαχειριστούν τις περιπτώσεις. Τα παραπάνω αποτελούν μια τυπική διαδικασία, χωρίς να διακρίνεται κάποιο πρόβλημα. Οι διαδικασίες μάθησης διαφέρουν για τα περιστατικά κρίσεων και τα πιο απλά ενώ υπάρχει μια πολύ ώριμη και συγκεκριμένη διαδικασία για τα περιστατικά κρίσης. Εντούτοις, σε πιο απλά περιστατικά φαίνεται να συμβαίνει το αντίθετο. Ο οργανισμός δείχνει να είναι πολύ προσεκτικός για τα περιστατικά κρίσης, το οποίο είναι και λογικό, ωστόσο θα μπορούσε να έχει αναπτύξει και πιο προσεκτικές διαδικασίες μάθησης για τα πιο μικρά περιστατικά, αφού πολλές φορές και αυτά με τη σειρά τους μπορούν να αποτελέσουν μια ισχυρή πηγή μάθησης ή μια υπολογίσιμη ζημιά για τον οργανισμό. Ένα ακόμα κενό που παρουσιάζεται είναι αυτό του αποκλεισμού στις πρώτες δυο συνεδριάσεις αναφοράς, με αποτέλεσμα να στερούνται γνώση και πληροφορία οι

ίδιοι υπάλληλοι τους. Συμπερασματικά, οι διαδικασίες του οργανισμού στον τομέα της μάθησης φαίνεται να χρειάζονται μεγαλύτερη προσοχή και μια καλύτερη οργάνωση.

Ο Οργανισμός Α έχει θεσπίσει αρκετές πρόβες και εκστρατείες ευαισθητοποίησης για τους εργαζόμενους του, που πραγματοποιούνται σχεδόν σε ετήσια βάση. Με αυτό τον τρόπο, ο οργανισμός δείχνει το μεγάλο του ενδιαφέρον και την κουλτούρα που έχει αναπτύξει σε θέματα εκπαίδευσης, ενημέρωσης και ευαισθητοποίησης του προσωπικού του, αναφορικά με την ασφάλεια πληροφοριών. Επιπρόσθετα, ο οργανισμός έχει αναπτύξει διαδικασίες που του επιτρέπουν να ανιχνεύει που χρειάζεται να επικεντρώνονται οι πρόβες του και ποιες διαδικασίες πρέπει να εφαρμόζονται. Παράλληλα, στις περιπτώσεις που δεν λειτούργησαν καλά οι διαδικασίες ρουτίνας, πραγματοποιήθηκε επανεξέταση. Αυτό αποτελεί άλλο ένα σημάδι του πόσο καλά και προσεγμένα έχουν αναπτυχθεί οι διαδικασίες για τις πρόβες και τις ενέργειες ρουτίνας στον οργανισμό.

Ακόμα ένα δείγμα της πολύ συγκεκριμένης και σε βάθος λεπτομερούς διαχείρισης είναι ότι για να διατηρήσει σε υψηλό επίπεδο το επίπεδο της εταιρείας σε θέματα ασφάλειας έχει επιβάλλει μια συγκεκριμένη διαδικασία στην πρόσληψη νέων υπαλλήλων, να υποβάλλονται δηλαδή σε εξειδικευμένη εκπαίδευση. Όσον αφορά τη δημιουργία γνώσης μετά τα περιστατικά, υπάρχει και εκεί μια αρκετά ώριμη αντιμετώπιση, καθώς μετά από κάθε συμβάν, βεβαιώνεται πρώτα ότι επιλύθηκε σωστά και στη συνέχεια τίθενται σε λειτουργία τα συστήματα. Ο Οργανισμός Α αναφορικά με την διαδικασία κατηγοριοποίησης περιστατικού φαίνεται ότι ακολουθεί συγκεκριμένα τυπικά βήματα, αφού μετά την ανίχνευση του από το σύστημα κατάχρησης κατηγοριοποιείται και αποστέλλεται ανάλογα με τον βαθμό κατηγοριοποίησης στο αντίστοιχο τμήμα.

Εξαιτίας της ποικίλης φύσεως των περιστατικών, ο Οργανισμός Α επέλεξε να φτιάξει κάποιες ροές εργασίας για πολύ συγκεκριμένα περιστατικά, καθώς και ένα σχέδιο έκτακτης ανάγκης. Από την ενέργεια αυτή προκύπτει η ευαισθητοποίηση του οργανισμού, που σχετίζεται με τα περιστατικά κρίσης. Αντίθετα, για πιο απλά περιστατικά ο οργανισμός δεν ενδιαφέρεται να δημιουργήσει λεπτομέρειες βημάτων σε τόσο μεγάλο χρονικό βάθος.

Στον Οργανισμό Β παρόλο που δεν υπάρχει κάποια συγκεκριμένη πολιτική για την διαχείριση και αντιμετώπιση περιστατικών, εντούτοις, έχουν θεσπιστεί κάποιες δικές του διαδικασίες ρουτίνας. Φαίνεται ότι αυτές οι διαδικασίες είναι προσαρμοσμένες ακριβώς πάνω στις ανάγκες του οργανισμού. Έχει φροντίσει παράλληλα, οι εργαζόμενοι να συμμετέχουν σε πρόβες για την καλύτερη προετοιμασία και ευαισθητοποίηση τους. Ένα εύρημα παρόμοιο με τους προηγούμενους οργανισμούς είναι ότι και σε αυτή την περίπτωση δεν υπάρχουν συγκεκριμένα βήματα για την αντιμετώπιση περιστατικών αλλά ένα σχέδιο έκτακτης ανάγκης. Όσο για τα περιστατικά κρίσης, απλά δίνεται μεγαλύτερη βαρύτητα και προσοχή. Όλο το σχέδιο αντιμετώπισης βασίζεται στην κατηγοριοποίηση που θα λάβει το περιστατικό μόλις ανιχνευθεί. Από εκεί και πέρα υπάρχει μια πολύ συγκεκριμένη διαδικασία με δυο ομάδες αντιμετώπισης. Παρόλο που υπάρχει πολύ λεπτομερής διαδικασία υψηλού επιπέδου, εντούτοις φαίνεται ότι επικοινωνία μεταξύ τους κατά την ώρα της απόκρισης δεν είναι πολύ συγκεκριμένη. Βέβαια αυτό δεν σημαίνει ότι μπορεί να αποτελεί αρνητικό στοιχείο για την όλη διαδικασία. Ο οργανισμός έχει εστιάσει σε έμπειρα πρόσωπα και όχι σε λεπτομερείς διαδικασίες με τον Supplier 2 να είναι ένα από αυτά, προσπαθώντας με την διεξαγωγή των συνεδρίων να μοιράζεται τις εμπειρίες του, δίνοντας ένα δείγμα υψηλής κουλτούρας στον οργανισμό σε θέματα ασφάλειας.

Στον Οργανισμό Γ υπάρχουν διαδικασίες και ενέργειες, όπως συνέδρια και παρουσιάσεις για την ευαισθητοποίηση των υπαλλήλων, ενώ οι ίδιοι οι υπάλληλοι ελέγχονται και κάθε χρόνο πάνω σε ένα εγχειρίδιο ασφαλείας, αποσκοπώντας στο να διαπιστώσουν τον βαθμό γνώσης του περιεχομένου του. Επίσης, οι καινούργιοι εργαζόμενοι, αμέσως μετά την πρόσληψη τους εξετάζονται πάνω σε αυτό το εγχειρίδιο. Όπως μπορεί να διαπιστώσει κανείς, μέσα από τις συγκεκριμένες πρακτικές του οργανισμού, τον ενδιαφέρει ιδιαίτερα η ευαισθητοποίηση σε θέματα ασφάλειας των εργαζομένων του, έχοντας στηρίξει αρκετές προσπάθειες πάνω σε αυτό. Επιπρόσθετα, φαίνεται και ότι έχει καταβάλει τόσο χρόνο όσο και προσπάθειες για την προετοιμασία των υπαλλήλων του στην απόκτηση της ικανότητας να ανταπεξέλθουν σε περιστατικά.

Σε αυτόν επίσης τον οργανισμό ισχύει το ίδιο και με τους παραπάνω Οργανισμούς Α και Β, ότι δηλαδή δεν υπάρχουν συγκεκριμένες διαδικασίες για περιστατικά που θα αποτελούν κρίσεις γιατί θεωρούν ότι είναι κάτι πολύ συνηθισμένο για αυτούς.

Αξιοσημείωτο είναι το έργο βελτίωσης που πραγματοποίησε ο οργανισμός, όπου μέσα από αυτό εντοπίστηκαν διαφορές αδυναμίες, αποτελώντας άλλο ένα πιθανό στοιχείο που να δηλώνει τις προσπάθειες του οργανισμού για την καλύτερη ανταπόκριση αλλά και πρόληψη. Πέρα από αυτά, το έργο αποτελεί ένα βασικό δείγμα της υψηλής κουλτούρας ασφάλειας του οργανισμού.

Όσον αφορά τις ομάδες αντιμετώπισης ο οργανισμός έχει μεριμνήσει για δυο πολύ σημαντικά θέματα. Το ένα είναι η διαδικασία, σε περίπτωση δηλαδή που χρειαστεί κάποιος άλλος να συνεχίσει τον χειρισμό του έργου ενώ το άλλο είναι το εγχειρίδιο που περιγράφει τον τρόπο που δουλεύει η ομάδα και μεριμνά και για τα νέα μέλη της ομάδας. Αυτές οι δυο ενέργειες δείχνουν την οργάνωση που επικρατεί στον οργανισμό αλλά και το ενδιαφέρον για την επίτευξη λειτουργίας της ομάδας, καθώς και της αποτελεσματικότητας της.

Σε σχέση με το ερευνητικό ερώτημα που τέθηκε παρατηρείται ότι όλοι οι οργανισμοί έχουν πρόβες και διαδικασίες και γενικότερα διάφορες ενέργειες που στοχεύουν στην πρόληψη και στην προετοιμασία των ομάδων και αντίστοιχα των οργανισμών. Σε όλους τους οργανισμούς, εκτός από τον οργανισμό της Finance υπάρχουν διαδικασίες με συγκεκριμένα βήματα για την αντιμετώπιση περιστατικών κρίσης. Η διαφορά τους με τον οργανισμό της Finance είναι ότι η ίδια διαθέτει μια συγκεκριμένη διαδικασία εκθέσεων για περιστατικά χαμηλού αντίκτυπου. Για τις διαδικασίες μάθησης μετά από περιστατικά η Finance φαίνεται να αντιμετωπίζει κάποια προβλήματα, σε αντίθεση με τον Οργανισμό Α. Για τους Οργανισμούς Β και Γ δεν δίνονται αρκετές πληροφορίες. Στις διαδικασίες κατηγοριοποίησης η Finance, ο Οργανισμός Α και Β ακολουθούν το ίδιο τυπικό μοτίβο ενώ ο Οργανισμός Γ κατηγοριοποιεί με βάση το ITIL.

6.3 Συμπεράσματα για το τρίτο ερευνητικό ερώτημα

Οι διαδικασίες της μάθησης μετά από περιστατικά φαίνεται να λειτουργούν ορθά για τον οργανισμό της Finance, καθώς έχουν βοηθήσει κατά πολύ μεγάλο βαθμό τον οργανισμό σε αυτή την κατεύθυνση. Χαρακτηριστική είναι η μείωση που καταγράφεται από 200 σε 16 το μήνα που αποτελεί ένα αξιοσέβαστο ποσοστό. Επίσης, η διαδικασία παρακολούθησης και αιτιολόγησης φαίνεται να λειτούργησε πολύ καλά και προς όφελος του οργανισμού, καθώς συντέλεσαν στη μείωση περιστατικών.

Στον Οργανισμό Α οι πρόβες που πραγματοποιεί τον βοήθησαν αρκετά στο να αποκαλυφθούν διάφορα θέματα, όπως η έλλειψη αίσθησης κινδύνου από τους υπαλλήλους, αποδεικνύοντας ότι οι κινήσεις για αυτές τις πρόβες έχουν ένα θετικό αντίκτυπο στον οργανισμό. Το ίδιο ισχύει και για την διοργάνωση των διαλέξεων που πραγματοποιούνται, αφού θεωρούνται χρήσιμες από τους υπαλλήλους.

Στον Οργανισμό Β τα περιστατικά και σε αυτή την περίπτωση δείχνουν μια τάση μείωσης και αυτό φαίνεται να είναι το αποτέλεσμα των εκστρατειών ευαισθητοποίησης. Επίσης, οι πρόβες φανέρωσαν διάφορα θέματα του οργανισμού που πρέπει να προσεχθούν μελλοντικά, δείχνοντας το πόσο καλά λειτουργούν και συνεισφέρουν στην ασφάλεια του οργανισμού αλλά και το πόσο σημαντική είναι η εύρυθμη λειτουργία. Ο Supplier 2 οποιοδήποτε περιστατικό κλήθηκε να αντιμετωπίσει είχε επιτυχημένη κατάληξη. Ωστόσο, αυτό ίσως οφείλεται περισσότερο στην εμπειρία του και όχι τόσο στην αποτελεσματικότητα των διαδικασιών.

Στον Οργανισμό Γ φαίνεται ότι οι πρόβες βοήθησαν στο να εμφανιστούν αρκετές προκλήσεις ενώ και το έργο βελτίωσης περιστατικών προσφέρει τα μέγιστα. Ταυτόχρονα, οι διαδικασίες μάθησης που στηρίζονται στο ITIL φαίνεται πως έχουν θετικό αντίκτυπο στον οργανισμό.

Σε σχέση με το ερευνητικό ερώτημα, οι πρόβες και οι ενέργειες πρόληψης έχουν αναδείξει προβλήματα που επιδέχονται περαιτέρω βελτίωσης αλλά παράλληλα έχουν μειώσει και τα περιστατικά. Το να δοθούν δεδομένα από τους οργανισμούς, τα οποία θα μπορούσαν να χρησιμοποιηθούν για να αποδείξουν το αρνητικό αντίκτυπο στην λειτουργία τους, ίσως είναι μια λεπτομέρεια που δεν θα ήθελαν να κοινοποιηθεί.

6.4 Συμπεράσματα για το τέταρτο ερευνητικό ερώτημα

Ο οργανισμός της Finance φαίνεται να έχει βάλει σε σημαντικές και καθοριστικές θέσεις έμπειρα άτομα με πολλές γνώσεις. Παρόλο που υπάρχουν αρκετές διαδικασίες για την πρόληψη τη διαχείριση και την αντιμετώπιση, εντούτοις ο οργανισμός φαίνεται να αντιμετωπίζει προβλήματα στις διαδικασίες μάθησης μετά τα περιστατικά. Αυτά τα προβλήματα είναι πιθανόν να πηγάζουν από τις ενέργειες των υψηλόβαθμων θέσεων, όπως προαναφέρθηκε, καθώς κάποιες διαδικασίες τους φαίνονται ελαττωματικές, όπως για παράδειγμα αυτή του αποκλεισμού του προσωπικού στις πρώτες συνεδριάσεις. Το ότι οι εργαζόμενοι είναι κοντά στο μοτίβο

του οργανισμού, το ότι εντοπίζουν και διορθώνουν, χωρίς να υπάρχει σε βάθος έρευνα για τα αίτια του περιστατικού είναι πιθανόν να αναγκάζει τις στρατηγικές αντιμετώπισης περιστατικών του οργανισμού να μην εφαρμόζονται στο μέγιστο τους, καθώς η μάθηση μετά από περιστατικά αποτελεί ένα πολύ σημαντικό πλεονέκτημα για την ομάδα αντιμετώπισης και τον οργανισμό.

Στον Οργανισμό Α από τους υπαλλήλους που συμμετείχαν στην αρχική έρευνα (με μεγάλη πιθανότητα να εκπροσωπούν την πλειοψηφία) φάνηκε να μην είναι ιδιαίτερα εξοικειωμένοι με την πολιτική ασφαλείας και να μην είναι ιδιαίτερα προσεκτικοί σε στοχευμένα Email και με το σημαντικότερο οι περισσότεροι από αυτούς να μην γνωρίζουν τι είναι ένα περιστατικό ασφαλείας. Το δεδομένο της έλλειψης κινδύνου από τις πύλες φαίνεται να επιβεβαιώνει και τη δήλωση ενός από τους συμμετέχοντες στην έρευνα, ότι η εφαρμογή κλειδώματος θυρών τους έκανε να νιώσουν ασφάλεια και να αμελούν διάφορες διαδικασίες που έπρεπε να πραγματοποιούνται.

Φαίνεται ότι όλα αυτά που διοργανώνει και για τα οποία μέριμνα ο Οργανισμός Α δεν έχουν τον ανάλογο αντίκτυπο στους υπαλλήλους. Αυτό μπορεί να συμβαίνει είτε γιατί δεν χρησιμοποιούνται στο μέγιστο τους είτε γιατί οι υπάλληλοι αδιαφορούν μερικώς για αυτά. Η άγνοια των υπαλλήλων και η έλλειψη αίσθησης κινδύνου επηρεάζει άμεσα τον οργανισμό και τις στρατηγικές ανίχνευσης, διαχείρισης και αντιμετώπισης περιστατικών, καθώς αποτελούν την πλειοψηφία των υπαλλήλων που εμπλέκονται σε αυτά. Είναι πιθανό να τις επηρεάζουν με τέτοιο τρόπο, ώστε να υπάρχει μια σχετική υπολειτουργία σε σχέση με την αρχική δυναμική των στρατηγικών αντιμετώπισης περιστατικών ασφαλείας πληροφοριών, καθώς δεν φαίνεται ο οργανισμός να αντιμετωπίζει κάποιο σοβαρό πρόβλημα που να προέρχεται από ανθρώπινη αμέλεια ή σφάλμα.

Επίσης, φαίνεται να έχει δημιουργηθεί ένα προβληματικό κλίμα κουλτούρας ασφαλείας με τους υπάλληλους του οργανισμού να έχουν επαναπαυτεί στις αυτόματες λειτουργίες και τα συστήματα του οργανισμού που μεριμνούν για την ασφάλεια. Ο υπεύθυνος ασφαλείας πληροφοριών με την δήλωση ότι δεν ενδιαφέρονται να αποκτήσουν μεγάλη λεπτομέρεια σε σχέση με τις διαδικασίες και τα βήματα για την αντιμετώπιση συγκεκριμένων περιστατικών στον οργανισμό είναι πιθανό να έχει δημιουργήσει μια νοοτροπία και μια λογική έλλειψης γνώσης της λεπτομέρειας σε βάθος, η οποία μπορεί κάλλιστα να μεταφερθεί και σε άλλα τμήματα και άτομα του οργανισμού.

Για το τι είναι περιστατικό στον Οργανισμό Β φαίνονται σχετικά εξοικειωμένοι με την πλειοψηφία να δείχνει ιδιαίτερα προσεκτική. Το γεγονός αυτό καταδεικνύει ότι υπάρχει μια σχετική ευαισθητοποίηση για την ασφάλεια από πλευράς του οργανισμού. Αντίθετα, μέσα στα πλαίσια της διαδικασίας σχετικά με το που και ποιες περιπτώσεις έπρεπε να αναφέρονται, παρατηρήθηκε μια σχετική ανησυχία. Σε σχέση με την πολιτική ασφάλειας οι περισσότεροι ήταν κάπως εξοικειωμένοι, παρόλο που φαίνεται ο οργανισμός να παραγκωνίζει την ενημέρωση των υπαλλήλων του κάθε φορά που αλλάζει αυτή η πολιτική.

Τα στοχευμένα Email οι περισσότεροι δήλωσαν ότι τα αναγνωρίζουν με έναν υπάλληλο να απαντάει ότι ακολούθησε εσκεμμένα και με ασφαλή τρόπο τέτοιες οδηγίες από Email. Αυτό το εύρημα προκαλεί ιδιαίτερη εντύπωση, καθώς φαίνεται ότι ο οργανισμός επιτρέπει τις αυτόβουλες ενέργειες των υπαλλήλων ή έστω να μην τους τιμωρεί για αυτές τις ενέργειες. Ακόμα, είναι φανερό ότι οι υπάλληλοι αγνοούν τις οδηγίες και τους κανόνες του οργανισμού. Προς επίρρωση αυτής της θεωρίας περιλαμβάνονται και τα αποτελέσματα του ερωτήματος ότι σε περίπτωση που χαρακτηριστούν κάποια μέτρα ασφάλειας ως ιδιαίτερα, οι χρήστες θα βρουν τον τρόπο να τα παρακάμψουν και ότι οι υπάλληλοι που δεν είχαν βρει χρήσιμες τις εκστρατείες είναι πιθανό να δηλώνουν αρνητική στάση απέναντι στις δραστηριότητες του οργανισμού ή ενδεχομένως και μια ελαττωματική κουλτούρα ασφάλειας. Το γεγονός αυτό αποτελεί δείγμα του μεγάλου βαθμού επιρροής που μπορούν να ασκήσουν οι υπάλληλοι στις στρατηγικές αντιμετώπισης περιστατικών του οργανισμού.

Όλα τα παραπάνω, επίσης, είναι πιθανό να υποδηλώνουν μια όχι ιδιαίτερα στενή σχέση εμπιστοσύνης ανάμεσα στο οργανισμό και τους υπαλλήλους. Αυτό φαίνεται να αποδεικνύεται και στο ότι το χειρότερο περιστατικό που θα μπορούσαν να αντιμετωπίσουν ήταν οι επίορκοι υπάλληλοι. Αυτό το αποτέλεσμα δείχνει επιπλέον τον βαθμό εξάρτησης της ασφάλειας του οργανισμού από τους υπαλλήλους του. Επίσης και σε αυτόν τον οργανισμό δεδομένης της ιδιαίτερης σχέσης οργανισμού και υπαλλήλων είναι πιθανό και σε αυτήν την περίπτωση να διαφαίνεται ένα είδος υπολειτουργίας, συγκριτικά με την αρχική δυναμική των στρατηγικών αντιμετώπισης περιστατικών ασφάλειας πληροφοριών. Από τις δηλώσεις του διευθυντή της εφοδιαστικής αλυσίδας προκύπτουν συμπεράσματα που δείχνουν ότι δεν υπάρχει υψηλό επίπεδο επικοινωνίας μεταξύ των εργαζομένων αλλά και ότι δεν υπάρχει

αίσθημα ευθύνης. Το γεγονός αυτό ίσως να προκαλεί συχνά προβλήματα σε περιστατικά.

Στον Οργανισμό Γ θεωρούν ότι υπάρχει υπό-αναφορά περιστατικών. Αυτό ενδεχομένως να συμβαίνει γιατί δεν είναι πρόθυμοι οι υπάλληλοι να αναγνωρίσουν λάθη τους. Άλλοι πιθανοί λόγοι είναι ότι δεν γνώριζαν που να αναφέρουν περιστατικά ή ακόμα και υπό ποιες συνθήκες έπρεπε να τα αναφέρουν. Το ότι οι υπάλληλοι δεν ήθελαν να αναγνωρίσουν το λάθος τους είναι ένα ανησυχητικό εύρημα, καθώς δείχνει την έλλειψη κουλτούρας ασφάλειας και τον κίνδυνο, στον οποίο θα ήταν ικανοί να βάλουν τον οργανισμό αψηφώντας την συγκεκριμένη διαδικασία στρατηγικής που υπάρχει στον οργανισμό για την αναφορά.

Ο διευθυντής ασφάλειας IT που κατέχει μια σημαντική θέση στον οργανισμό ,όπως προαναφέρθηκε, στα αποτελέσματα δεν ήταν εξοικειωμένος με το πρότυπο ISO 27035, γεγονός που θα μπορούσε να επηρεάσει άμεσα και αρνητικά διαδικασίες, ενέργειες και στρατηγικές, οι οποίες σχετίζονται με τη διαχείριση συμβάντων ασφάλειας. Ο Οργανισμός Γ φαίνεται να γνωρίζει την σοβαρότητα ύπαρξης κουλτούρας αλλά και τη σημασία να υπάρχει ευαισθητοποίηση για την ασφάλεια στο προσωπικό, καθώς αυτά τα δύο συντελούν στην ανίχνευση, διαχείριση και αντιμετώπιση των περιστατικών. Αυτό φαίνεται κυρίως από το ότι μεριμνά για την κατάρτιση και εκπαίδευση των νέων υπαλλήλων πάνω σε ζητήματα ασφαλείας και σχετικές κατευθυντήριες οδηγίες.

Σε σχέση με το ερευνητικό ερώτημα που τέθηκε παρατηρείται ότι ο ρόλος του ανθρώπινου παράγοντα και κατά επέκταση των υπαλλήλων και των τεσσάρων οργανισμών, σχετίζεται άμεσα και επηρεάζει τις ενέργειες και τις διαδικασίες που πραγματοποιούνται. Στις περιπτώσεις των Οργανισμών Α και Β είδαμε ότι επηρέαζαν την εφαρμογή των στρατηγικών ασφάλειας, καθώς και άλλων ενεργειών με αποτέλεσμα αυτές οι στρατηγικές να μην εφαρμόζονται ή να μην λειτουργούν στο έπακρο.

Ενώ στις περιπτώσεις των Οργανισμών Γ και Finance αποτυπώθηκε το γεγονός ότι ενώ υπάρχει μέριμνα για την ύπαρξη υψηλού επιπέδου κουλτούρας ασφάλειας, αυτό δεν λειτουργεί στον μέγιστο βαθμό, καθώς οι υπάλληλοι φαίνεται πως αντιμετωπίζουν προβλήματα σε αυτό τον τομέα. Ως εκ τούτου, το ζήτημα αυτό

επηρεάζει άμεσα και την συνολική εφαρμογή των στρατηγικών αντιμετώπισης περιστατικών ασφάλειας πληροφοριών.

ΚΕΦΑΛΑΙΟ 7^ο: Γενικά Συμπεράσματα – Προτάσεις και Μελλοντική έρευνα

7.1 Γενικά Συμπεράσματα – Προτάσεις

Αυτή η ενότητα παρέχει συζήτηση και συστάσεις γύρω από τα ευρήματα και τα συμπεράσματα που προκύπτουν από τα αποτελέσματα της έρευνας.

Υπάρχει η τάση των οργανισμών να μεριμνούν για τεχνικά θέματα και να ξεοδεύουν μεγαλύτερους πόρους σε αυτά ενώ μεριμνούν σε μικρότερο βαθμό για την εστίαση του ανθρώπινου παράγοντα όπως φαίνεται και στην βιβλιογραφία (ANDY, 2001). Οπότε δεν προκαλεί έκπληξη η παρατήρηση της έρευνας ότι στους οργανισμούς εργάζονται υπάλληλοι όπου δεν είναι εξοικειωμένοι με το τι είναι περιστατικό και ποτέ πρέπει να αναφέρεται ή να μην υπάρχουν διαδικασίες μάθησης για όλους τους τύπους των περιστατικών ενώ ταυτόχρονα υπάρχουν αρκετά εξελιγμένα συστήματα ανίχνευσης περιστατικών μέσα σε αυτούς. Η παραπάνω άγνοια των υπάλληλων υποδηλώνει ένα χαμηλό επίπεδο κουλτούρας όπου αυτό με την σειρά του μπορεί να αποτελέσει κάλλιστα πηγή περιστατικών (Da Veiga, Astakhova, Botha and Herselman, 2020). Η συγκεκριμένη αγνοία και κατά επέκταση το χαμηλό επίπεδο κουλτούρας συμπεράναμε ότι είναι πιθανό να αποτελεί μια βασική πηγή για την μη αποδοτική λειτουργία στο μέγιστο των δυνατοτήτων ενεργειών των οργανισμών που αποσκοπούνε στην πρόληψη, στην εκπαίδευση και την ενημέρωση και γενικά στην ενίσχυση των στρατηγικών αντιμετώπισης περιστατικών. Το γεγονός ότι οι εσωτερικές λειτουργίες των οργανισμών επηρεάζονται από τους εργαζόμενους και το αντίστροφο είναι αποδεκτό και από την βιβλιογραφία (Szilagyi and Wallace, 1990). Μέσα από την διάκριση διαφόρων ενεργειών όπως, ότι αν κριθούν κάποια μέτρα ασφάλειας ιδιαίτερα για τους υπαλλήλους αυτοί θα βρουν τρόπο να τα παρακάμψουν, επιβεβαιώνεται η δυσκολία υψηλής ύπαρξης κουλτούρας στους οργανισμούς αλλά και η απουσία σχέσεων σεβασμού από τους υπαλλήλους προς τους οργανισμούς. Η παραπάνω παρακάμψη κρίνεται απολύτως λογική από τον Harley (2009) από οικονομικής άποψης, καθώς η συνέπεια στα μέτρα τους προσφέρει προστασία από άμεσο κόστος των επιθέσεων αλλά παράλληλα τους επιβαρύνει με μεγάλο έμμεσο κόστος προσπάθειας.

Για την ενίσχυση του επιπέδου της κουλτούρας ασφάλειας των οργανισμών προτείνετε μια πιο ουσιαστική και προσεκτική εστίαση του οργανισμού στους υπαλλήλους της που θα επιφέρει αποτελέσματα που θα ισχύουν για μεγάλα χρονικά

διαστήματα. Με το να τεθούν σε ισχύ κάποιοι έλεγχοι και αξιολογήσεις απόδοσης στους εργαζόμενους θα αποκλειόταν ο όρος της ουσιαστικής εστίασης που προαναφέρθηκε, καθώς αντιμετωπίζει πολλά προβλήματα αξιοπιστίας και εγκυρότητας (Szilagyi and Wallace, 1990). Υπάρχουν αρκετοί παράγοντες που επηρεάζουν τα παραπάνω δυο αλλά και αρκετά εμπόδια για την ορθή επιτυχία του, η αποφυγή των ελέγχων και η εύρεση ενός άλλου τρόπου αξιολόγησης των εργαζομένων που δεν θα θυμίζει αστυνόμευση των εργαζομένων προτείνετε και από τους (Vroom and von Solms, 2004). Έτσι αυτή η έρευνα προτείνει την εστίαση από τους οργανισμούς και την πραγματοποίηση ενεργειών για την επιβράβευση των προσπαθειών των εργαζόμενων τους όταν ενεργούν με ασφάλεια κατά την ώρα εργασίας τους, ίσως με την καταβολή κάποιου τύπου χρηματικό μπόνους. Ταυτόχρονα ως προς ενίσχυση αυτής της ουσιαστικής εστίασης προτείνετε οι οργανισμοί να θέτουν τους ίδιους περιορισμούς και τις ίδιες απαιτήσεις στους εργαζόμενους τους ενισχύοντας το κλίμα ισότητας και δικαιοσύνης στα τμήματα τους. Η επιβράβευση των ενεργειών επιβεβαιώνεται και από τους (Villamarin-Salomon, R.M. and Brustoloni, J.C. (2010) ενώ η σημασία της δικαιοσύνης στους οργανισμούς από τους (Saunders and Thornhill, 2003).

Είναι σαφές από τα ευρήματα και τα συμπεράσματα της έρευνας ότι υπάρχει μια επανάπαυση των υπάλληλων γύρω από την ασφάλεια αλλά και ταυτόχρονα απουσία αίσθησης κινδύνου με κάποια από τα αίτια να είναι τα σύγχρονα και αρκετά λειτουργικά συστήματα αυτόματων διαδικασιών που μεριμνάνε για την ασφάλεια των οργανισμών επιλέγοντας να βασιστούν σε αυτά που αποτελούν μια εύκολη και γρήγορη λύση. Μέσα από τα παραπάνω ανιχνεύεται πάλι το προαναφερθέν συμπέρασμα συνήθειας των υπαλλήλων. Ενώ και ο Reason (Reason J., 1997), θεωρεί φυσική την τάση του ανθρώπου της επιλογής της σύντομης διαδρομής.

Με γνώμονα τα παραπάνω επιπροσθέτως προτείνετε η εστίαση των υπαλλήλων στην πολιτική ασφάλειας καθώς θεωρείτε επιτακτική ανάγκη οι ενέργειες που εκτελούν οι ίδιοι να είναι με υπευθυνότητα τηρώντας όλες τις πολιτικές ασφάλειας (Vroom and von Solms, 2004). Αυτό για να είναι πιο ομαλό και προσιτό στους οργανισμούς και στου εργαζόμενους τους αλλά και η εφαρμογή του να έχει όσο το δυνατόν μεγαλύτερη δυναμική προτείνετε οι οργανισμοί να προσαρμόζουν την πολιτική ασφάλειας τους σύμφωνα με τις ανάγκες τους αλλά και τις απαιτήσεις τους πράγμα που είναι σύμφωνο επίσης και από τους (Lukas Kim & Han, 2018) . Ακόμα μια σύσταση που θα βοηθούσε τους υπαλλήλους να ενεργούν με υπευθυνότητα τηρώντας

όλες τις πολιτικές ασφάλειας θα ήταν, οι εργαζόμενοι που έδειχναν μεγαλύτερη κατανόηση αυτών των πολιτικών να επισημαίνονταν, ίσως σαν υπάλληλοι του μήνα. Με στόχο να θεωρηθούν πρότυπα από τους υπολοίπους και να αντιγραφτούν οι συμπεριφορές τους. Το συγκεκριμένο πλαίσιο της επισημάνσης με στόχο την ανάδειξη προτύπων μέσα στους οργανισμούς για την παρακίνηση των υπαλλήλων προτείνεται από τους (Robinson & O'Leary-Kelly, 1998) και τους (Thomas & Griffin, 1989).

Ένα ακόμα συμπέρασμα που προέκυψε ήταν ο επηρεασμός των υπαλλήλων από άτομα τα οποία κατείχαν υψηλές θέσεις μέσα στον οργανισμό. Οι αντιλήψεις και οι συνήθειες ατόμων που βρίσκονται σε υψηλές θέσεις είναι αρκετά πιθανό να επηρεάσουν και να αποτελέσουν πρότυπα για εργαζομένους μέσα στον οργανισμό. Αυτό μπορεί να επηρεάσει είτε θετικά είτε αρνητικά τον οργανισμό και τα ίδια τα άτομα, ωστόσο θα ήταν ορθό οι εργαζόμενοι να εκτελούν εντολές που τους έχουν ανατεθεί και να επηρεάζονται από έμπειρα άτομα που έχουν ως στόχο το υψηλό επίπεδο κουλτούρας ασφάλειας και την εστίαση στις πολιτικές ασφάλειας των οργανισμών. Αυτά τα άτομα που συνήθως αποτελούν υπεύθυνοι τμημάτων των οργανισμών θα πρέπει να έχουν λάβει τις παραπάνω κατευθυντήριες γραμμές από την διοίκηση του οργανισμού που στοχεύει στην ενδυνάμωση της ασφάλειας. Επομένως πρέπει οι οργανισμοί να μπορούν να ελέγχουν ως προς την συμμόρφωση τα άτομα που θέτουν σε αυτές τις θέσεις και να συμβαίνει η ακολουθία οπου, τους εκδίδουν οδηγίες σχετικά με τους στόχους και τον επιθυμητό τρόπο λειτουργίας του οργανισμού που επιθυμούν και στην συνέχεια οι υπεύθυνοι αυτοί μεταφράζουν αυτές τις οδηγίες σε πολιτικές, πρότυπα και διαδικασίες (von Solms & (Basie) von Solms, 2006). Αυτή η σχέση μεταφοράς οδηγιών επίσης υποστηρίζεται σε πλαίσια πληροφορικής και από τους (Jensen & Meckling, 1976)

Για την επιρροή της συμπεριφοράς αρχικά των υπευθύνων των τμημάτων και στην συνέχεια των εργαζομένων από αυτούς, η σύσταση στηρίζεται στην θεωρία της αντιπροσωπείας ή αλλιώς το παράδειγμα του κύριου πράκτορα, αυτή η θεωρία ασχολείται με τον εντολέα που αναθέτει καθήκοντα σε ένα άλλο μέρος δηλαδή τον πράκτορα (M. EISENHARDT, 1989). Για τον έλεγχο αυτής της σχέσης ο εντολέας (διοίκηση του οργανισμού) μπορεί να συνάψει συμβάσεις για τα αποτελέσματα της συμπεριφοράς του πράκτορα(υπεύθυνοι τμημάτων, υπεύθυνοι ασφάλειας), ο συγκεκριμένος έλεγχος μπορεί να θεωρηθεί ορθός με την μέτρηση επιτυχίας της εργασίας τους, η οποία με την σειράς της προτρέπει τον πράκτορα να ευθυγραμμίζει τα ενδιαφέροντα του με αυτά του

εντολέα (M. EISENHARDT, 1989). Η θεωρία της αντιπροσωπίας σε θέματα πληροφορικής προτείνεται και από τους (Posthumus & von Solms, 2008).

7.2 Μελλοντική Έρευνα

Η συγκεκριμένη βιβλιογραφική ανασκόπηση 2 άρθρων εντόπισε σαν περιορισμό το βάθος της λεπτομέρειας των πληροφοριών που δίνονται στις μελέτες περιπτώσεις οργανισμών από τους ίδιους τους οργανισμούς και τους συνεντευξιαζόμενους ή τα έγγραφα που επιλέγουν να κοινοποιήσουν με αποτέλεσμα να περιορίζει αρκετά την παρούσα έρευνα. Σαν μελλοντική έρευνα συνιστάτε η μελέτη για την εύρεση τρόπων που θα κάνουν τους οργανισμούς να νιώσουν μεγαλύτερη ασφάλεια κατά την κοινοποίηση των δεδομένων τους και θα μοιραστούν περισσότερες και πιο λεπτομερές πληροφορίες. Αυτό με την σειρά του είναι πιθανό να επιφέρει μεγάλα πλεονεκτήματα και νέα δεδομένα προς μελέτη στην ερευνητική κοινότητα που μελετάει την ασφάλεια των πληροφοριών στους οργανισμούς κι όχι μόνο.

Αυτή η βιβλιογραφική ανασκόπηση αποκάλυψε ότι για την επίτευξη υψηλού επιπέδου κουλτούρας ασφάλειας στους οργανισμούς χρειάζεται μια πιο ουσιαστική εστίαση στον ανθρώπινο παράγοντα πέρα από τις κοινές πρακτικές όπως μια εκστρατεία ευαισθητοποίησης. Έτσι για μελλοντική έρευνα συνιστάτε η μελέτη νέων τρόπων ενίσχυσης της κουλτούρας ασφάλειας με επίκεντρο τον ανθρώπινο παράγοντα αλλά και τρόπους οι οποίοι θα παρακινήσουν και θα κεντρίσουν το ενδιαφέρον του εργαζόμενου ώστε να μπει σε μια διαδικασία όπου θα μεριμνάει κι θα συμμορφώνεται από μόνος του για την επίτευξη υψηλού επιπέδου ασφάλειας. Αυτοί οι νέοι τρόποι ουσιαστικά θα μεταβάλουν την συμπεριφορά του εργαζόμενου ώστε να ενεργεί με ασφάλεια και υπευθυνότητα.

Βιβλιογραφία

- Ahmad, A., Maynard, S. B., Desouza, K. C., Kotsias, J., Whitty, M. T., & Baskerville, R. L. (2012). How can organizations develop situatio“n awareness for incident response: A case study of management practice. *Computers & Security*, 101.
- Andy, A., (2001). *Information Security Industry Survey*. [online] Lfca.net. Available at: <<http://lfca.net/Reference Documents/2001 Information Security Survey.pdf>>.
- Bada, M., Creese, S., Goldsmith, M., Mitchell, C., & Phillips, E. (2014). Computer Security Incident Response Teams (CSIRTs): An Overview. *Global Cyber Security Capacity Centre*, 1-23.
- Bandara, W., Furtmueller, E., Gorbacheva, E., Miskon, S., & Beekhuyzen, J. (2015). Achieving Rigor in Literature Reviews: Insights from Qualitative Data Analysis and Tool-Support. *Communications of the Association for Information Systems*, 37.
- Bhattacharjee, A. (2012). *Social Science Research: Principles, Methods, and Practices*. Ανάκτηση από https://digitalcommons.usf.edu/cgi/viewcontent.cgi?article=1002&context=oa_textbooks
- Brewster, E., Griffiths, R., Lawes, A., & Sansbury, J. (2012). *IT Service Management: A guide for ITIL Foundation Exam candidates* (2nd εκδ.). BCS.
- Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). *Computer Security Incident Handling Guide: Recommendations of the National Institute of Standards and Technology*. Ανάκτηση από U.S. Department of Commerce: <https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf>
- De Muynck, J., & Portesi, S. (2016). *Strategies for incident response and cyber crisis cooperation* (1.1 εκδ.). ENISA.
- Da Veiga, A., Astakhova, L., Botha, A. and Herselman, M., (2020). *Defining organisational information security culture—Perspectives from academia and industry*.

Αλλαγή κωδικού πεδίου

- Haller, J., Merrell, S. A., Butkovic, M. J., & Willke, B. J. (2011). *Best Practices for National Cyber Security: Building a National Computer Security Incident Management Capability, Version 2.0.*, Ανάκτηση από https://resources.sei.cmu.edu/asset_files/TechnicalReport/2011_005_001_154_01.pdf
- Hedström, K., Kolkowska, E., Karlsson, F., & Allen, J. (2011). Value conflicts for information security management. *The Journal of Strategic Information Systems*, 20(4), 373-384.
- Herley, C., 2009. *So long, and no thanks for the externalities* | *Proceedings of the 2009 workshop on New security paradigms workshop*. [online] ACM Other conferences. Available at: <<https://dl.acm.org/doi/10.1145/1719030.1719050>>.
- Hove, C., & Tarnes, M. (2013). Information Security Incident Management: An Empirical Study of Current Practice. *Computer Science*.
- *ISO/IEC 27002:2005(E)*. (2005). Ανάκτηση από Information technology - Security techniques - Code of practice for information security management- International Organization for Standardization: <https://www.iso.org/obp/ui/-iso:std:iso-iec:27002:ed-1:v1:en>
- *ISO/IEC 27001:2013*. (2013). Information technology — Security techniques — Information security management systems — Requirements, Ανάκτηση από <https://www.iso.org/standard/54534.html>
- ISO-Technical Committee. (2016). *ISO/IEC 27035-1:2016*. Ανάκτηση από Information technology — Security techniques — Information security incident management — Part 1: Principles of incident management: <https://www.iso.org/standard/60803.html>
- ISO-Technical Committee. (2016). *ISO/IEC 27035-2:2016*. Ανάκτηση από Information technology — Security techniques — Information security incident management — Part 2: Guidelines to plan and prepare for incident response Committee : ISO/IEC JTC 1/SC 27 Information security,

Αλλαγή κωδικού πεδίου

Αλλαγή κωδικού πεδίου

Αλλαγή κωδικού πεδίου

Αλλαγή κωδικού πεδίου

cybersecurity and privacy protection ICS : 35.030 IT Security:
<https://www.iso.org/standard/62071.html>

Αλλαγή κωδικού πεδίου

- ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls, Ανάκτηση από <https://www.iso.org/standard/75652.html>
- Jakábová, M., Urdziková, J., & Mironovová, E. (2013). Standardization of Information Security Management System: ISO/IEC 27001:2005, ITIL®, CoBIT. *IJES*, 1(2).
- Jennifer, M. (2011). *Η διεξαγωγή της ποιοτικής έρευνας*. (Ν. Κυριαζή, Επιμ., & Ε. Δημητριάδου, Μεταφρ.) Αθήνα: Πεδίο.
- Jensen, M., & Meckling, W. (1976). Theory of the firm: Managerial behavior, agency costs and ownership structure. *Journal Of Financial Economics*, 3(4), 305-360. doi: 10.1016/0304-405x(76)90026-x
- Kathleen M. Eisenhardt (1989). Agency Theory: An Assessment and Review
- Kitchenham, B. (2004). *Procedures for Performing Systematic Reviews*. Ανάκτηση από https://www.researchgate.net/publication/228756057_Procedures_for_Performing_Systematic_Reviews
- Linneberg, M., & Korsgaard, S. (2019). Coding qualitative data: a synthesis guiding the novice. *Qualitative Research Journal*.
- Long, H. A., French, D. P., & Brooks, J. M. (2020). Optimising the value of the critical appraisal skills programme (CASP) tool for quality appraisal in qualitative evidence synthesis. *Research Methods in Medicine & Health Sciences*, 1(1).
- Lukas Kim, H., & Han, J. (2018). Do employees in a “good” company comply better with information security policy? A corporate social responsibility perspective. [online] <https://www.emerald.com/insight/content/doi/10.1108/ITP-09-2017-0298/full/html>

Αλλαγή κωδικού πεδίου

- Majid, U., & Vanstone, M. (2018). Appraising Qualitative Research for Evidence Syntheses: A Compendium of Quality Appraisal Tools. *Quality Health Research*, 28(13), 2115-2131.
- Nye, E., Melendez-Torres, G., & Bonell, C. (2016). Origins, methods and advances in qualitative meta-synthesis. *Review of Education*, 4(1), 57-79.
- Okoli, C. (2015). A Guide to Conducting a Standalone Systematic Literature Review. *Communications of the Association for Information Systems*, 37.
- Reason, J. (1997), Managing the Risks of Organisational Accidents, Cambridge University Press, Cambridge.
- Robinson, S., & O'Leary-Kelly, A. (1998). Monkey See, Monkey Do: The Influence of Work Groups on the Antisocial Behavior of Employees. *Academy Of Management Journal*, 41(6), 658-672. doi: 10.5465/256963
- Saunders, M. and Thornhill, A., (2003). *Organisational justice, trust and the management of change*.
- Siddaway, A. P., Wood, A. M., & Hedges, L. V. (2019). How to Do a Systematic Review: A Best Practice Guide for Conducting and Reporting Narrative Reviews, Meta-Analyses, and Meta-Syntheses. *Annual Review of Psychology*, 70, 747-770.
- Szilagyi AD, Wallace MJ. (1990). Organizational behavior and performance. 5th ed. Illinois: Scott, Foresman and Company.
- Thomas, J., & Griffin, R. (1989). The power of social information in the workplace. *Organizational Dynamics*, 18(2), 63-75. doi: 10.1016/0090-2616(89)90043-0
- Thomas, D. R. (2006). A General Inductive Approach for Analyzing Qualitative Evaluation Data. *American Journal of Evaluation*, 27(2).
- Villamarín-Salomon, R.M. and Brustoloni, J.C. (2010), "Using reinforcement to strengthen users' secure behaviors", Proceedings of the 28th International Conference on Human Factors in Computing Systems (CHI '10), ACM, New York, NY, pp. 363-72.

- von Solms, R., & von Solms, S. (2006). Information Security Governance: A model based on the Direct–Control Cycle. *Computers & Security*, 25(6), 408-412. doi: 10.1016/j.cose.2006.07.005
- Vroom, C. and Von Solms, R., (2004). *Towards information security behavioural compliance*.