ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ
ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ
ΤΟΜΕΑΣ ΗΛΕΚΤΡΙΚΩΝ ΒΙΟΜΗΧΑΝΙΚΩΝ
ΔΙΑΤΑΞΕΩΝ ΚΑΙ ΣΥΣΤΗΜΑΤΩΝ ΑΠΟΦΑΣΕΩΝ

Διαχείριση της Ασφάλειας Πληροφοριών και Μεγάλων Καταστροφών

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Φώτιος Γ. Σιουτάρης

Επιβλέπων: Δημήτριος Ασκούνης
Καθηγητής Ε.Μ.Π.

Αθήνα, Ιούλιος 2021

ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ
ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ
ΤΟΜΕΑΣ ΗΛΕΚΤΡΙΚΩΝ ΒΙΟΜΗΧΑΝΙΚΩΝ
ΔΙΑΤΑΞΕΩΝ ΚΑΙ ΣΥΣΤΗΜΑΤΩΝ ΑΠΟΦΑΣΕΩΝ

Διαχείριση της Ασφάλειας Πληροφοριών και Μεγάλων Καταστροφών

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Φώτιος Γ. Σιουτάρης

Επιβλέπων: Δημήτριος Ασκούνης
Καθηγητής Ε.Μ.Π.

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την 16η Ιουλίου 2021.

…….	……..……	……..……
Δημήτριος Ασκούνης	Ιωάννης Ψαρράς	Χρυσόστομος Δούκας
Καθηγητής Ε.Μ.Π.	Καθηγητής Ε.Μ.Π.	Επίκουρος Καθηγητής Ε.Μ.Π.

Αθήνα, Ιούλιος 2021

……..……

Φώτιος Γ. Σιουτάρης
Διπλωματούχος Ηλεκτρολόγος Μηχανικός και Μηχανικός Υπολογιστών Ε.Μ.Π.

Περίληψη:

Η παρούσα διπλωματική αναφέρεται στα συστήματα διαχείρισης της ασφάλειας των πληροφοριών και τις διαδικασίες διαχείρισης μεγάλων καταστροφών στα πλαίσια οργανισμών. Αρχικά, παρουσιάζονται τα προβλήματα των παραβιάσεων ασφαλείας και το αντίκτυπο των φυσικών καταστροφών. Έπειτα, εισάγονται και αναλύονται οι βασικές έννοιες της ασφάλειας των πληροφοριών, της προστασίας της και δομημένες προσεγγίσεις και συστήματα διαχείρισης της τελευταίας για οργανισμούς. Ακολούθως, αναλύονται διαδεδομένα διεθνή πρότυπα διαχείρισης της ασφάλειας των πληροφοριών και αναλύονται οι διαδικασίες αντιμετώπισης των κινδύνων της πληροφορίας και των καταστροφικών γεγονότων, με εστίαση στις διαδικασίες ανάλυσης επιχειρηματικού αντίκτυπου, διαχείρισης ρίσκου, τα πλάνα επιχειρηματικής συνέχισης και αποκατάστασης καταστροφών, τις διαδικασίες αξιολόγησης και διαχείρισης συμβάντων στα πλαίσια του οργανισμού και ενδεικτικά αντίμετρα. Στη συνέχεια, παρουσιάζονται συνήθεις καταστροφές και αντίστοιχοι τρόποι αντιμετώπισης και καταληκτικά, αναφέρονται γενικά συμπεράσματα και δυνατότητες μελλοντικής επέκτασης.

Λέξεις Κλειδιά:

Ασφάλεια πληροφοριών, μεγάλες καταστροφές, συμβάντα ασφαλείας, συστήματα διαχείρισης, οργανισμοί, διεθνή πρότυπα, διαχείριση ρίσκου, ανάλυση επιχειρηματικού αντίκτυπου, πλάνο επιχειρηματικής συνέχισης, πλάνο αποκατάστασης καταστροφών

Abstract:

This thesis refers to information security management systems and disaster management processes, in the context of organizations. Initially, the issues of security breaches and the impact of natural disasters are presented. Afterwards, basic concepts of information security and structured approaches and systems to manage it are introduced and analysed. Subsequently, renown international information management system standards are analysed, as well as information risk processes, focusing on business impact assessment, risk management processes, business continuity and disaster mitigation planning, incident management, testing and recommended countermeasures. Additionally, management practices of common disasters are presented and the thesis is concluded with notes and opportunities for future expansion

Keywords:

Information security, disasters, security incidents, management systems, organizations, international standards, risk management, business impact assessment, business continuity planning, disaster recovery planning

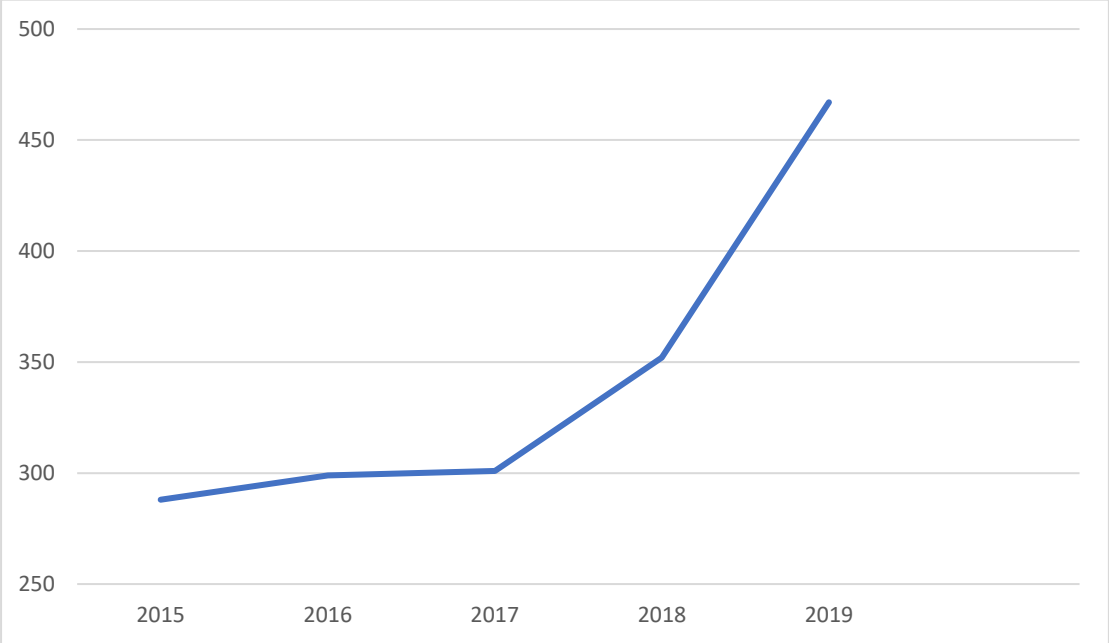
Περιεχόμενα:

Πίνακας Διαγραμμάτων:

Κεφάλαιο 1: Εισαγωγή

Οργανισμοί όλων των τύπων και μεγεθών συλλέγουν, επεξεργάζονται, αποθηκεύουν και μεταδίδουν πληροφορία, αναγνωρίζοντας ότι τα δεδομένα και οι σχετιζόμενες διαδικασίες, συστήματα, δίκτυα και ομάδες συντελούν δραματικά στην επίτευξη των στόχων τους.

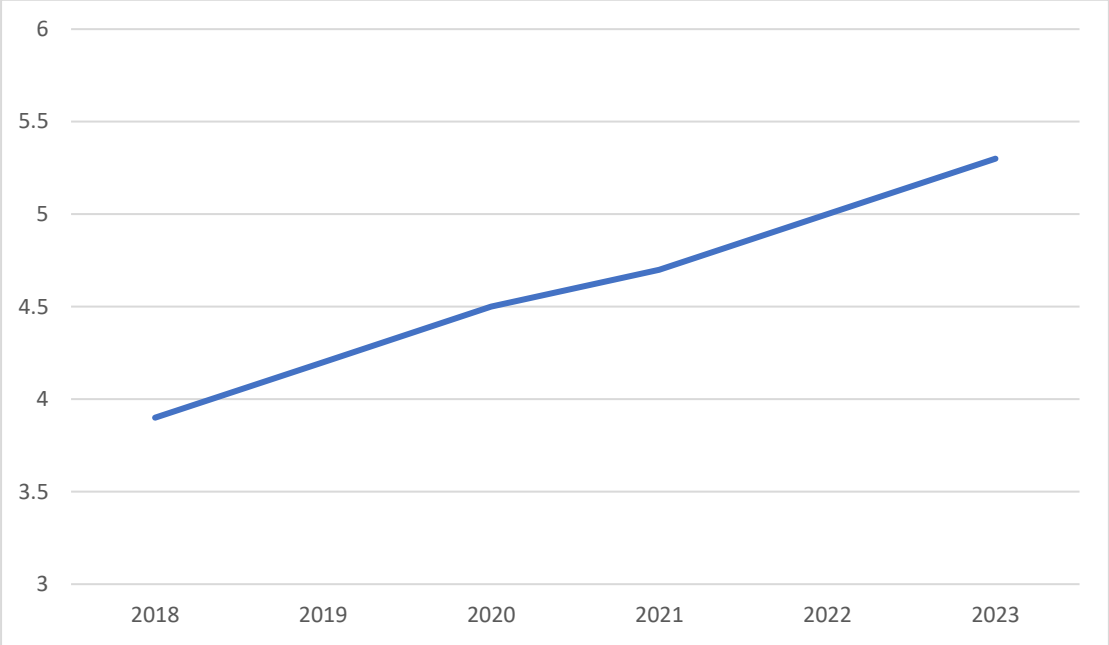
Σε έναν διασυνδεδεμένο κόσμο, τα συστήματα, οι διαδικασίες και τα δίκτυα πληροφοριών είναι δυνητικά ευάλωτα σε πλήθος κινδύνων ασφαλείας, ανεξαρτήτως του τομέα δραστηριοτήτων του οργανισμού. Η διασύνδεση δημοσίων και ιδιωτικών δικτύων και η συνεχής επικοινωνία αυξάνουν τη δυσκολία ελέγχου της πρόσβασης και της διαχείρισης. Ως αποτέλεσμα, η πληροφορία, συχνά, γίνεται αντικείμενο επιθέσεων, λαθών και καταστροφών, με σημαντικές οικονομικές επιπτώσεις και πλήγματα της βιωσιμότητας των οργανισμών.



Διάγραμμα 1 - Ο αριθμός των καταγγελιών που ελήφθησαν από το Κέντρο Καταγγελιών Ηλεκτρονικού Εγκλήματος, την περίοδο 2015-2019, σε χιλιάδες

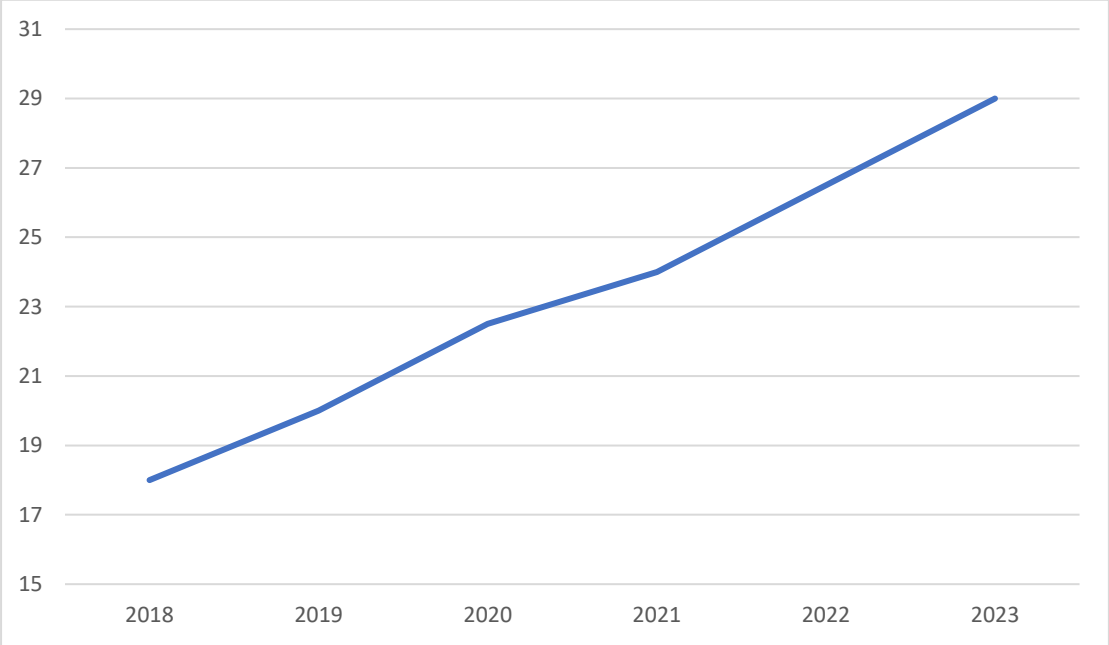
Ενδεικτικά, από τα μεγαλύτερης έκτασης δημοσιοποιημένα συμβάντα, αναφέρεται ότι το 2013, από την αμερικανική εταιρία υπηρεσιών διαδικτύου Yahoo υπεκλάπησαν τα προσωπικά δεδομένα των 3 δισεκατομμυρίων - τότε - χρηστών της, με αποτέλεσμα την μείωση της τιμής εξαγοράς της κατά 350 εκατομμύρια δολάρια (Stempel & Finkle, 2017). Πλέον πρόσφατα, στις αρχές του 2021 απεκαλύφθει ότι, αξιοποιώντας κενά ασφαλείας του αμερικανικού προμηθευτή λογισμικού SolarWinds και με χρονικό ορίζοντα 1,5 χρόνου, επιτιθέμενοι απέκτησαν πρόσβαση σε δίκτυα πληροφοριών τουλάχιστον 250 οργανισμών, συμπεριλαμβανομένων ομοσπονδιακών υπηρεσιών των ΗΠΑ, από τους περίπου 18 χιλιάδες οργανισμούς, στους οποίους είχαν πρόσβαση (Sanger, et al., 2021). Ακόμη, το Μάρτιο του 2021, λόγω ευπαθειών στην υποδομή της εταιρίας λογισμικού Microsoft, ανακαλύφθηκε παραβίαση των λογαριασμών τουλάχιστον 30 χιλιάδων πελατών τους, η οποία στόχευε σε μηνύματα ηλεκτρονικού ταχυδρομείου, ψηφιακά ημερολόγια και συστήματα (Conger & Frenkel, 2021). Για τις τελευταίες δύο αναφορές, η ανάλυση του αντίκτυπου στα δεδομένα και τις υποδομές των προσβεβλημένων οντοτήτων συνεχίζεται.

Παράλληλα, η παγκόσμια αύξηση της συνδεσιμότητας, η επικράτηση νέων τεχνολογιών δικτύωσης, όπως τα δίκτυα 5G και οι εφαρμογές του διαδικτύου των αντικειμένων (internet of things – IOT) που υποστηρίζουν και ο ψηφιακός μετασχηματισμός των οργανισμών, αναμένεται να επιδεινώσουν σημαντικά την κατάσταση.



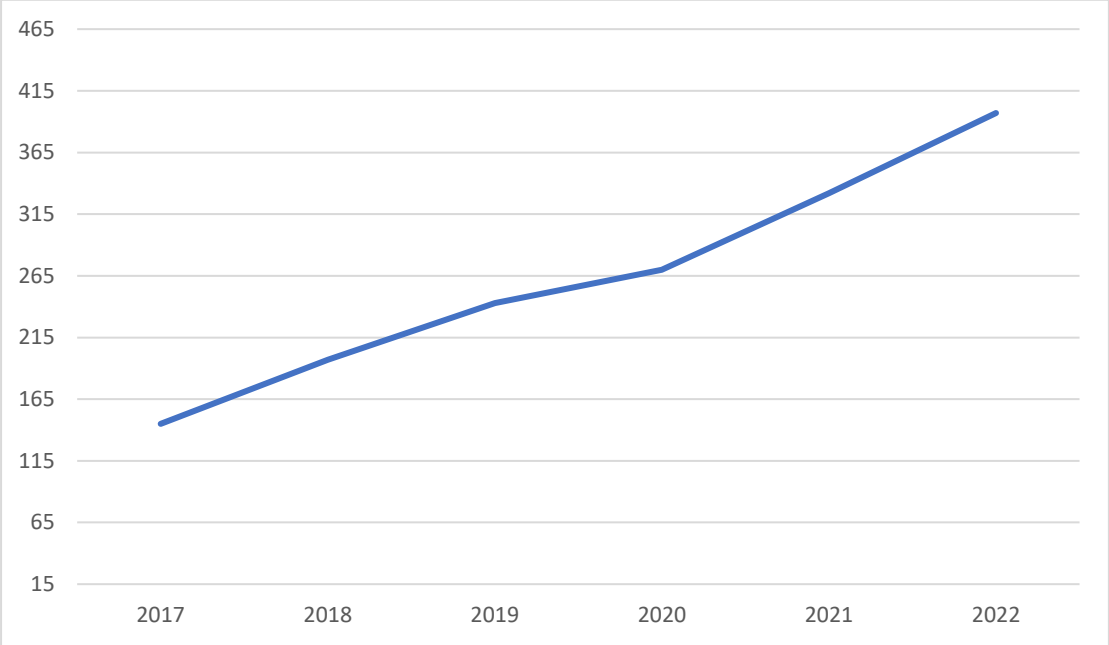
Διάγραμμα 2 - Εκτίμηση του αριθμού των παγκόσμιων χρηστών του διαδικτύου για το διάστημα 2018-2023, σε δισεκατομμύρια (CISCO)

Σε σύγκριση με το 2018, το 2023 αναμένεται οι χρήστες του διαδικτύου να έχουν αυξηθεί από τα 3,9 στα 5,3 δισεκατομμύρια και οι διασυνδεδεμένες συσκευές από τα από τα 18 στα 29 δισεκατομμύρια (Cisco, 2020).



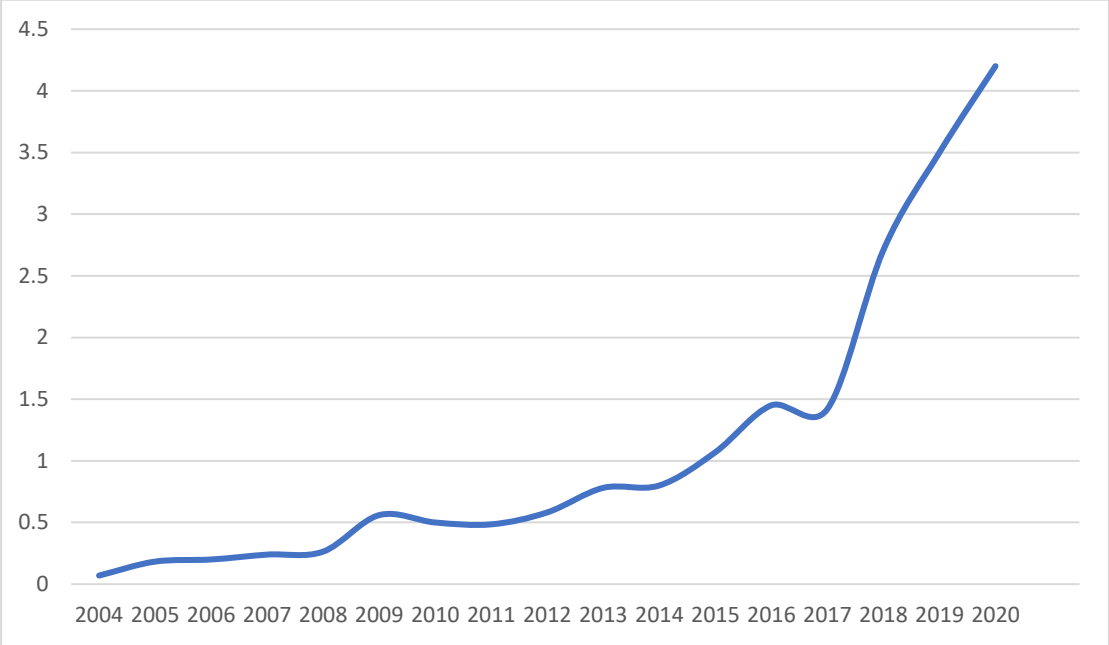
Διάγραμμα 3 - Εκτίμηση του αριθμού των διασυνδεδεμένων συσκευών για το διάστημα 2018-2023, σε δισεκατομμύρια (CISCO)

Ταυτόχρονα, το 90% των παγκόσμιων επιχειρήσεων αναμένεται να αξιοποιεί υβριδικές λύσεις τεχνολογιών συννέφου μέχρι το 2022 (International Data Corporation, 2020), ενώ το μέγεθος της αγοράς παροχής υπηρεσιών δημόσιου συννέφου εκτιμάται ότι θα προσεγγίσει τα 400 δισεκατομμύρια δολάρια το 2022 (Statista, 2021).



Διάγραμμα 4 - Εκτίμηση του μεγέθους της αγοράς παροχής υπηρεσιών δημόσιου συννέφου για το διάστημα 2017-2022, σε δισεκατομμύρια δολάρια (Statista)

Επακόλουθα, οι συνολικές οικονομικές επιπτώσεις των παραβιάσεων ασφαλείας αναμένεται να προσεγγίσουν τα 6 τρισεκατομμύρια δολάρια το 2021 (World Economic Forum, 2020) και τα 10,5 το 2025 (Morgan, 2020). Οι ετήσιες απώλειες λόγω κυβερνοεγκλημάτων που αναφέρθηκαν στην αρμόδια υπηρεσία των Ηνωμένων Πολιτειών ήταν 4,2 δισεκατομμύρια δολάρια το 2020, έναντι περίπου 0,5 δισεκατομμυρίων το 2010 και 0,18 δισεκατομμυρίων το 2005 (Statista, 2021). Αξιοσημείωτα, εκτιμάται ότι το συνολικό κόστος του κυβερνοεγκλήματος, συμπεριλαμβανομένου του κόστους αποκατάστασης, ξεπέρασε τα 450 δισεκατομμύρια δολάρια το 2014 (McAfee, 2014).

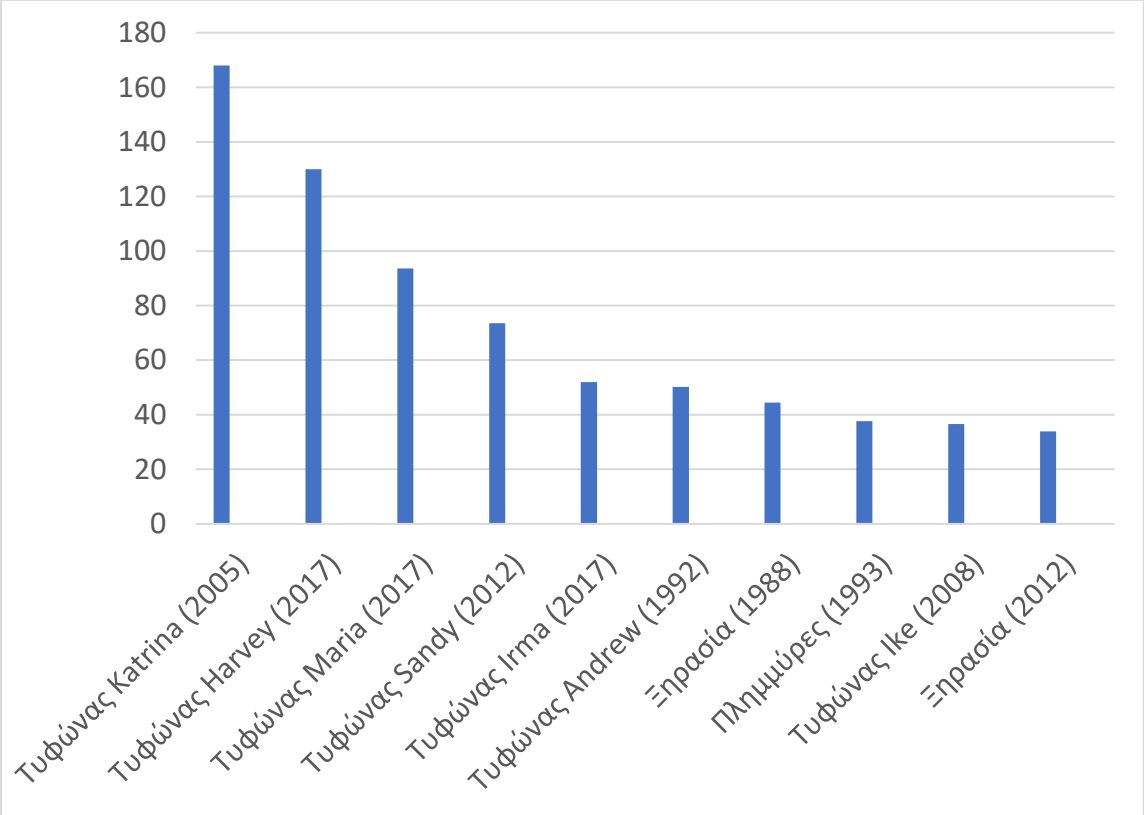


Διάγραμμα 5 - Ετήσιες απώλειες λόγω κυβερνοεγκλημάτων που αναφέρθηκαν στην αρμόδια υπηρεσία των Ηνωμένων Πολιτειών, το διάστημα 2000-2020, σε δισεκατομμύρια δολάρια (Statista)

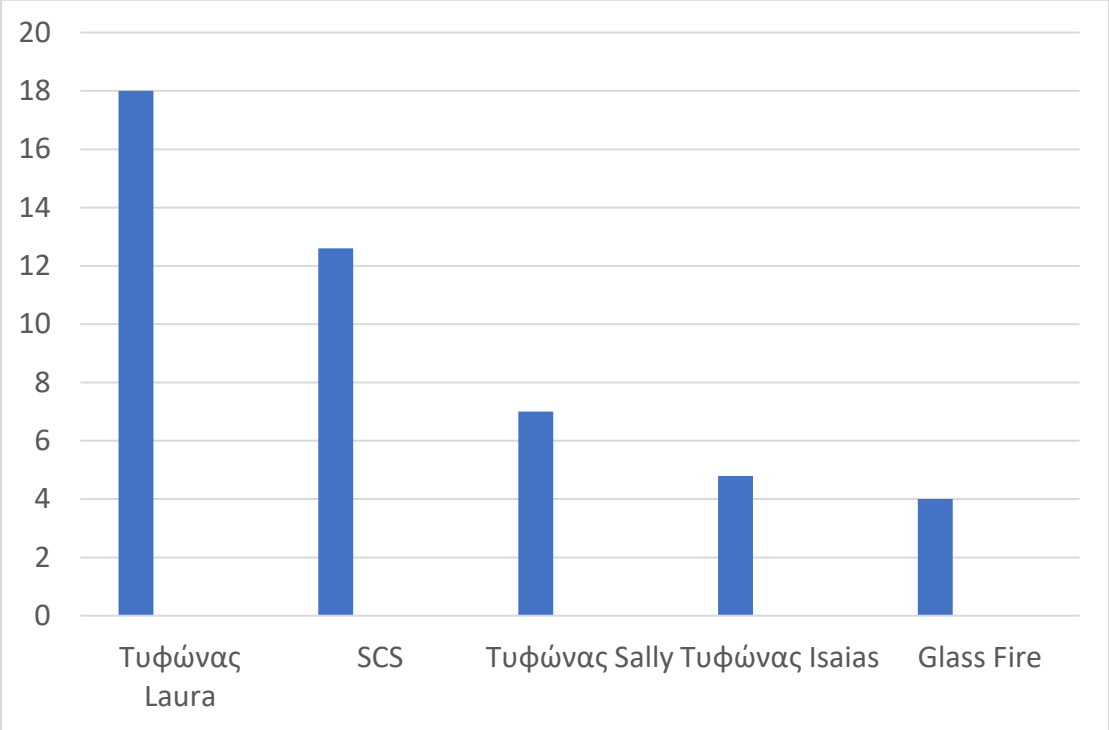
Εκτός από τις κυβερνοεπιθέσεις, διαταραχές και φυσικές καταστροφές επηρεάζουν άμεσα τις υποδομές και το ανθρώπινο δυναμικό των οργανισμών, με δραματικές συνέπειες και οικονομικό αντίκτυπο.

Αναφορικά, το Φεβρουάριο του 2021, η πολιτεία του Τέξας, ΗΠΑ, επλήγη από ακραίες χιονοπτώσεις και πολικό ψύχος, με αποτέλεσμα πολυήμερες διακοπές ρεύματος και ύδρευσης και ζημιές στις υποδομές που εκτιμώνται στα 20 δισεκατομμύρια δολάρια (SECHLER & HAWKINS, 2021). Επίσης, κατά τη θερινή περίοδο του 2020, πυρκαγιές στην Αυστραλία προκάλεσαν οικονομικές απώλειες που υπολογίζονται στα 100 δισεκατομμύρια δολάρια (Read & Denniss, 2020). Όσον αφορά την πανδημία του COVID-19, οι συνολικές επιπτώσεις είναι ιδιαίτερα δύσκολα προσεγγίσιμες, ωστόσο αξίζει να σημειωθεί ότι, λαμβάνοντας υπόψη τη συρρίκνωση του παγκόσμιου ΑΕΠ το 2020 και την υποβάθμιση των προβλέψεων ανάπτυξης - αποκλειστικά - για το 2021, οι εκτιμώμενες απώλειες ανέρχονται στα 10,3 τρισεκατομμύρια δολάρια (The Economist, 2021). Σε αυτό το μέγεθος δεν συμπεριλαμβάνονται πολύχρονες

οικονομικές επιδράσεις, ούτε ποσοτικοποιούνται οι επιπτώσεις της αύξησης της ανεργίας, του μειωμένου εμπορίου και η διαφοροποίηση των εξόδων και επενδύσεων που αναγκαία πραγματοποιήθηκαν για τον περιορισμό της κρίσης, σε σχέση με τις προηγούμενες προβλέψεις.



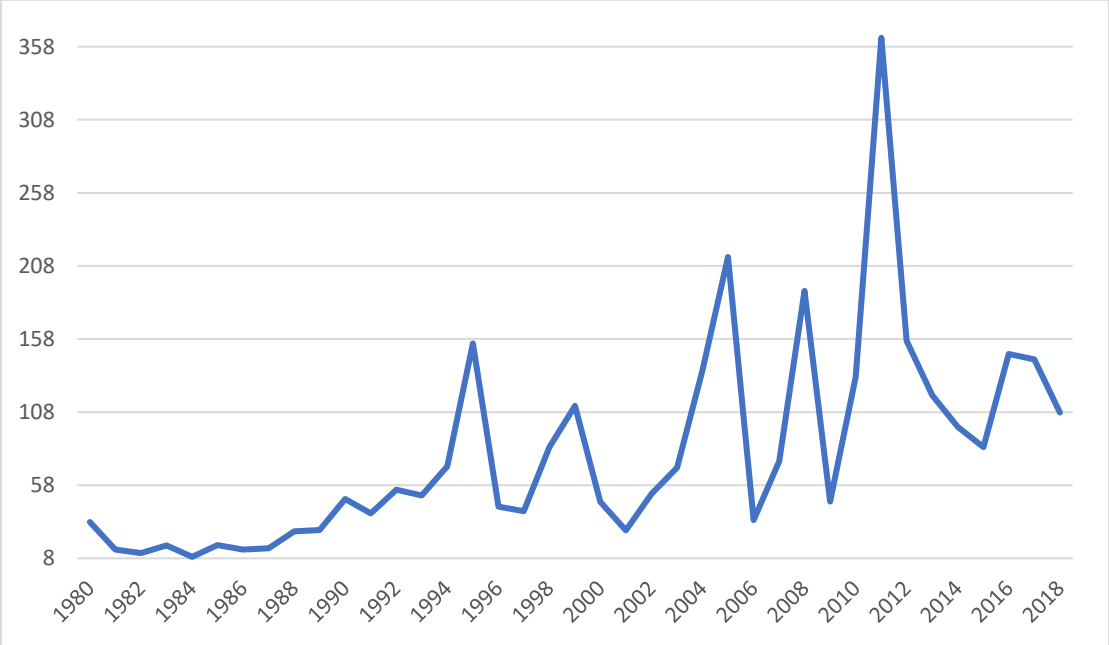
Διάγραμμα 6 - Κατάταξη και οικονομικές απώλειες, σε δισεκατομμύρια δολάρια, των 10 σημαντικότερων καταστροφών στις ΗΠΑ, το διάστημα 1980-2019 (NOAA National Centers for Environmental Information (NCEI), 2021)



Διάγραμμα 7 - Απώλειες, σε δισεκατομμύρια δολάρια, των σημαντικότερων καταστροφών στις ΗΠΑ, το 2020

Παράλληλα, λόγω της κλιματικής αλλαγής, η συχνότητα και ένταση των ακραίων καιρικών φαινομένων και καταστροφών που προκαλούν παρουσιάζει σημαντική αυξητική τάση (Coronese, et al., 2019).

Ενδεικτικά, τη δεκαετία του 1980-1989 στις ΗΠΑ, καταγράφηκαν 19 καταστροφές με οικονομικό αντίκτυπο περίπου 180 δισεκατομμυρίων δολαρίων, σε σύγκριση με τις 119 καταστροφές υλικών απωλειών περίπου 811 δισεκατομμυρίων δολαρίων, τη δεκαετία του 2010-2019 (NOAA National Centers for Environmental Information (NCEI), 2021). Παγκοσμίως, ο αριθμός των φυσικών καταστροφών έχει δεκαπλασιαστεί το διάστημα 1960-2019 (Institute for Economics & Peace, 2019). Αντίστοιχα, το συνολικό κόστος των φυσικών καταστροφών ανήλθε στα 108 δισεκατομμύρια δολάρια το 2018, σε σύγκριση με 47 δισεκατομμύρια δολάρια το 2000 (CRED, D. Guha-Sapir, n.d.).



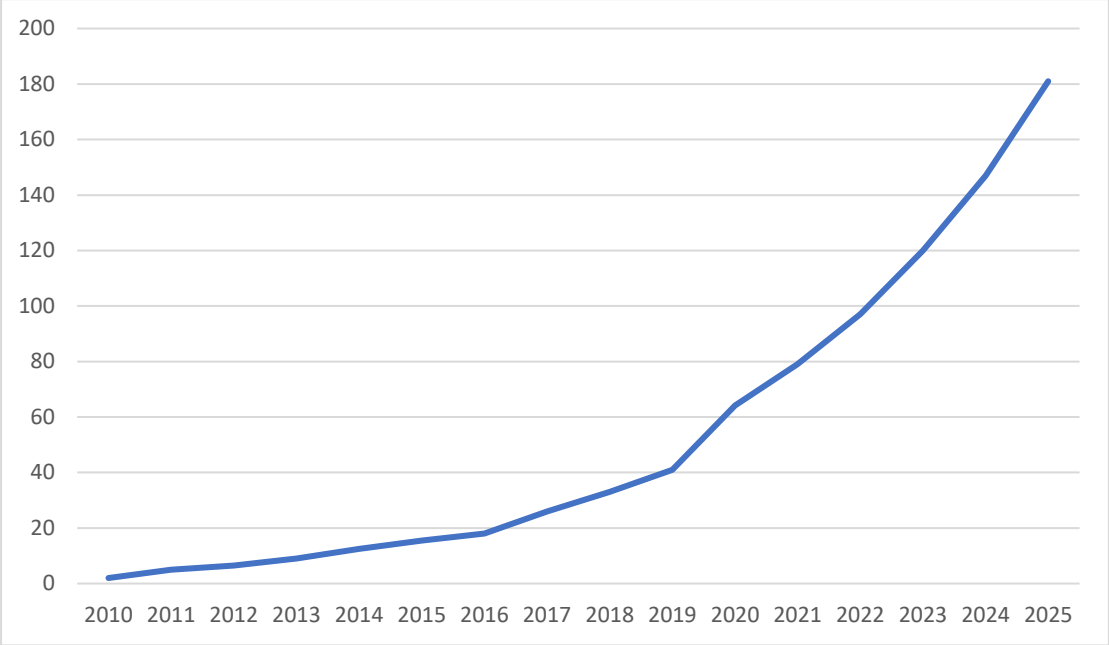
Διάγραμμα 8 - Συνολικό ετήσιο κόστος των φυσικών καταστροφών στις Ηνωμένες Πολιτείες, σε δισεκατομμύρια δολάρια, το διάστημα 1980-2018 (CRED)

Συνεπώς, καθίσταται σαφές ότι συντονισμένες ενέργειες προσδιορισμού, υλοποίησης, συντήρησης και βελτίωσης της ασφάλειας των πληροφοριών και των σχεδίων αντιμετώπισης καταστροφών αποτελούν κρίσιμο μέρος της διαχείρισης κάθε οργανωτικής οντότητας.

Κεφάλαιο 2: Ασφάλεια των πληροφοριών

2.1: Η πληροφορία για τους οργανισμούς

Η πληροφορία μπορεί να αποθηκευτεί σε πολλές μορφές, υλικές ή άυλες, αναλογικές ή ψηφιακές και να μεταδοθεί με διάφορους τρόπους και μέσω ποικιλίας διαύλων. Ακριβής και πλήρης πληροφορία, διαθέσιμη έγκαιρα σε όσους έχουν εξουσιοδοτηθεί, υποστηρίζει μέγιστα κάθε οργανισμό.



Διάγραμμα 9 - Εκτίμηση του μεγέθους της πληροφορίας που παράγεται, καταγράφεται, αντιγράφεται και καταναλώνεται παγκοσμίως, σε zettabytes, το διάστημα 2010-2025

Καθ' όλο το διάστημα ζωής της, η πληροφορία επηρεάζεται από ένα σύνολο ρίσκων, ο περιορισμός των οποίων κρίνεται καταλυτικής σημασίας για τη λειτουργία των οργανισμών. Δεδομένων των μεταβλητών συγκυριών, οι οργανισμοί πρέπει να παρακολουθούν και αξιολογούν την απόδοση των εφαρμοσμένων μέτρων προστασίας και διαδικασιών, να ταυτοποιούν έγκαιρα τα ρίσκα προς αντιμετώπιση και να επιλέγουν, υλοποιούν και βελτιώνουν τους

απαραίτητους ελέγχους. Οι πολιτικές και στόχοι ασφάλειας των πληροφοριών επιτρέπουν την αποτελεσματική επίτευξη της ζητούμενης ασφάλειας.

2.2: Η προστασία της πληροφορίας

Τα περιουσιακά στοιχεία τα οποία κάθε οργανισμός καλείται να ασφαλίσει είναι διαφορετικά, ανάλογα με τον τομέα δραστηριοτήτων, το επιχειρηματικό πλάνο και τις μεθόδους που χρησιμοποιούνται, διαθέτουν, ωστόσο, αρκετά σημαντική αξία ώστε να χρήζουν προστασίας. Αντίστοιχα, οι πολύτιμες πληροφορίες μπορεί να αφορούν τα δεδομένα των πελατών, τη δικτυακή υποδομή και τα πληροφοριακά συστήματα, πνευματική ιδιοκτησία, οικονομικά δεδομένα και δεδομένα για τις εσωτερικές διαδικασίες, τη διαθεσιμότητα και παραγωγικότητα της υπηρεσίας ή τη φήμη του οργανισμού.

Η προστασία της πληροφορίας αναφέρεται στη διατήρηση της ακεραιότητας, διαθεσιμότητας και εμπιστευτικότητας των δεδομένων, μέσω της εφαρμογής και διαχείρισης των κατάλληλων ελέγχων, λαμβάνοντας υπόψη τις πιθανές απειλές. Περιορίζοντας τις αρνητικές επιπτώσεις των συμβάντων ασφαλείας, προωθείται η επιτυχία των δραστηριοτήτων κάθε οντότητας. Η επίτευξη της ασφάλειας των πληροφοριών απαιτεί τη διαχείριση του ρίσκου φυσικού ανθρώπινου και τεχνολογικού που σχετίζεται με όλες τις μορφές πληροφορίας οι οποίες χρησιμοποιούνται από τον οργανισμό.

Ένα πληροφοριακό σύστημα επιτρέπει τη συλλογή, επεξεργασία και αποθήκευση δεδομένων σε άτομα και οργανισμούς. Αντίστοιχα, η ασφάλεια των πληροφοριακών συστημάτων αναφέρεται στη συλλογή των ενεργειών που προστατεύουν αυτά τα συστήματα και τα δεδομένα τους. Στην πλειονότητα των περιπτώσεων, η προστασία της πληροφορίας βασίζεται σε τεχνολογίες που υποστηρίζουν τη δημιουργία, επεξεργασία, αποθήκευση, μετάδοση, διατήρηση και καταστροφή της. Συχνά, κατά τη σχεδίαση και ανάπτυξη πληροφοριακών συστημάτων, η ασφάλεια τους δεν λαμβάνεται εξ αρχής υπόψη. Επίσης, η συνηθισμένη θεώρηση της επίτευξης της ασφάλειας των πληροφοριών με την

αποκλειστική χρήση τεχνικών μέσων είναι επικίνδυνη και ελλιπής, χωρίς αντίστοιχη υποστήριξη από τις υπόλοιπες διαδικασίες του οργανισμού.

Για να χαρακτηριστεί η πληροφορία ασφαλής, πρέπει να είναι εμπιστευτική, ακέραια και διαθέσιμη. Η εμπιστευτικότητα της πληροφορίας αναφέρεται στην διαφύλαξή της από όλους όσους δεν έχουν δικαίωμα να την δουν. Χαρακτηριστικά παραδείγματα εμπιστευτικών πληροφοριών αποτελούν τα προσωπικά δεδομένα των ατόμων, η πνευματική ιδιοκτησία των οργανισμών και τα δεδομένα εθνικής ασφάλειας των κρατών. Η προστασία της εμπιστευτικότητας επιτυγχάνεται μέσω ελέγχων ασφαλείας, με στόχο τον περιορισμό του ρίσκου ασφαλείας. Κοινοί έλεγχοι περιλαμβάνουν εκπαιδεύσεις εργαζομένων, εφαρμογή πλαισίων πολιτικών ασφάλειας πληροφοριών, πολυεπίπεδα συστήματα προστασίας πληροφοριακών συστημάτων, περιοδικές αναλύσεις ρίσκου, παρακολούθηση συμβάντων ασφαλείας, αυστηρούς ελέγχους ταυτότητας και χρήση κρυπτογραφίας.

Η ακεραιότητα της πληροφορίας ασχολείται με τη διατήρηση της εγκυρότητας και ακρίβειας των δεδομένων, ώστε να έχουν λειτουργική αξία, αποτρέποντας μη εξουσιοδοτημένες αλλαγές.

Η διαθεσιμότητα της πληροφορίας αναφέρεται στο διάστημα κατά το οποίο η υπηρεσία, το σύστημα και τα δεδομένα ενδιαφέροντος μπορούν να χρησιμοποιηθούν από τους χρήστες. Προσεγγίζεται αριθμητικά από το λόγο του χρόνου κατά τον οποίο είναι διαθέσιμη προς το συνολικό χρονικό διάστημα που εξετάζεται. Άλλα χρήσιμα μεγέθη αφορούν το μέσο χρόνο μεταξύ πραγματικών ή προβλεπόμενων αποτυχιών του συστήματος και το μέσο χρόνο επιδιόρθωσης των προβλημάτων και αποκατάστασης της λειτουργίας. Το κόστος ευκαιρίας αναφέρεται στο οικονομικό αντίκτυπο της έλλειψης διαθεσιμότητας, προσεγγίζεται ως απώλεια παραγωγικότητας και μπορεί να έχει δραματικές συνέπειες. Σε πολλούς τομείς, οι οργανισμοί υπογράφουν συμφωνίες επιπέδου παρεχόμενων υπηρεσιών (service-level agreements - SLAs), με συγκεκριμένη ελάχιστη αποδεκτή διαθεσιμότητα.

2.3: Παραβιάσεις της ασφάλειας των πληροφοριών

Ως απειλή ορίζεται κάθε πράξη που μπορεί να προκαλέσει ζημιές σε ένα περιουσιακό στοιχείο, φυσική ή ανθρώπινη και προερχόμενη από το περιβάλλον, άτομα ή οργανισμούς. Στόχος των διαδικασιών ασφαλείας των συστημάτων είναι η παροχή πληροφοριών, μεθοδολογιών και τεχνικών για την αντιμετώπιση των απειλών. Ανάλογα με τη σημασία και το δυνητικό τους αντίκτυπο, οι απειλές μπορούν να ταυτοποιηθούν και ταξινομηθούν ως προς τις οικονομικές απώλειες, το πλήγμα της φήμης του οργανισμού, των νομικών συνεπειών τους ή της συχνότητας με την οποία μπορούν να παρουσιαστούν. Ενδεικτικά, περιλαμβάνουν κακόβουλο λογισμικό, αποτυχία υλικού ή λογισμικού, εσωτερικούς ή εξωτερικούς επιτιθέμενους, κλοπή περιουσιακών στοιχείων, βιομηχανική κατασκοπεία, φυσικές καταστροφές και τρομοκρατικές επιθέσεις. Για την αποτελεσματικότερη προστασία απαιτείται συνεχής παρακολούθηση όλων των πιθανών απειλών.

Κάθε ένα από τα χαρακτηριστικά της ασφαλούς πληροφορίας πλήττεται από διαφορετική κατηγορία απειλών. Οι απειλές γνωστοποίησης αφορούν μη εξουσιοδοτημένη πρόσβαση σε ιδιωτική η εμπιστευτική πληροφορία, αποθηκευμένη ή κατά τη μετάβασή της μεταξύ κόμβων. Συνήθως, παρουσιάζονται ως υποκλοπή ή κατασκοπεία και το μέγεθος του αντίκτυπου εμφανίζουν τις καθιστά από τις πιο μελετημένες.

Οι απειλές μεταβολής παραβιάζουν την ακεραιότητα της πληροφορίας, πραγματοποιώντας επιτηδευμένα η τυχαία μη εξουσιοδοτημένες αλλαγές δεδομένων σε ένα σύστημα. Οι επιτηδευμένες απειλές μεταβολής είναι ως επί το πλείστον κακόβουλες, εκδηλώνονται συχνά ως δολιοφθορές και μπορούν να πλήξουν σημαντικά έναν οργανισμό, ιδιαίτερα αν επηρεάσουν κρίσιμα δεδομένα. Προηγούμενη προετοιμασία μειώνει σημαντικά τον κίνδυνο των συγκεκριμένων απειλών, καθώς συστήματα διαχείρισης αλλαγών περιορίζουν και καταγραφούν την πρόσβαση και τις μεταβολές των δεδομένων, ενώ στην ύστατη περίπτωση μπορεί να γίνει επαναφορά διαθέσιμων αντίγραφων ασφαλείας.

Οι απειλές άρνησης ή καταστροφής καθιστούν πληροφορία μη διαθέσιμη η άχρηστη, παραβιάζοντας τη διαθεσιμότητα της και αποτρέποντας εξουσιοδοτημένους χρήστες προσωρινά η μόνιμα από τη χρήση της. Το αντίκτυπο των συγκεκριμένων απειλών εξαρτάται άμεσα από την σημασία του πόρου ο οποίος παραβιάζεται.

Τρωτά σημεία

Τα τρωτά σημεία επιτρέπουν σε κάποια απειλή να επηρεάσει κάποιο στοιχείο του οργανισμού, με αρνητικές συνέπειες. Η ύπαρξη τρωτών σημείων σε ένα σύστημα συνδέεται άμεσα με την πιθανότητα εμφάνισης κάποιας απειλής. Οι τελευταίες, δεν μπορούν να εξαλειφθούν, αλλά τα τρωτά σημεία δύναται να καλυφθούν, με αποτέλεσμα η ύπαρξη της απειλής να μην επηρεάζει τη λειτουργία του οργανισμού. Για την αποτελεσματική προστασία των περιουσιακών στοιχείων του οργανισμού, απαιτείται εξάλειψη όσον το δυνατόν περισσότερων τρωτών σημείων, με τη χρήση των κατάλληλων πολιτικών ασφαλείας.

Η παρουσίαση κάθε απειλής συνδέεται με την εμφάνιση του αντίστοιχου γεγονότος ή συμβάντος. Στην πρώτη περίπτωση αναφερόμαστε σε κάποιο μετρήσιμο αντίκτυπο στη λειτουργία του οργανισμού, Στη δεύτερη, η σημασία του συμβάντος είναι σημαντικά μεγαλύτερη και παραβιάζεται άμεσα ή απειλείται τουλάχιστον μία πολιτική ασφαλείας.

Επιθέσεις

Οι επιθέσεις σε ένα σύστημα αναφέρονται στις κακόβουλες ενέργειες αξιοποίησης κάποιου τρωτού σημείου, με στόχο την παραβίαση της ασφάλειας των πληροφοριών. Διακρίνονται σε τεχνάσματα, οι οποίες επιχειρούν να εξαπατήσουν τους χρήστες, παρεμβολές, οι οποίες υποκλέπτουν και προωθούν δεδομένα, διακοπές, οι οποίες διακόπτουν τη λειτουργία κάποιου διαύλου επικοινωνίας και μετατροπής, οι οποίες αλλάζουν την πληροφορία που

μεταδίδεται ή βρίσκεται αποθηκευμένη σε κάποιον πόρο, ενώ εμφανίζονται και συνδυασμοί των παραπάνω. Στα διάφορα είδη επιθέσεων εντοπίζονται οι επιθέσεις κωδικών - ωμής βίας ή λεξικών, η πλαστογράφηση διευθύνσεων, οι επιθέσεις μεταμφίεσης, το ηλεκτρονικό «ψάρεμα», οι επιθέσεις «ανθρώπου-στη-μέση» και η κοινωνική μηχανική.

Παραβιάσεις ασφαλείας

Κάθε γεγονός που οδηγεί σε παραβίαση της εμπιστευτικότητας, ακεραιότητας ή διαθεσιμότητας των δεδομένων αποτελεί παραβίαση ασφαλείας. Τα μέτρα κατά των απειλών πρέπει να είναι σε θέση να ανιχνεύσουν τρωτά σημεία, να προλάβουν επιθέσεις και να ανταποκριθούν με ταχύτητα στις επιπτώσεις επιτυχημένων επιθέσεων.

Σημειώνεται ότι σημαντικό μέρος των παραβιάσεων ασφαλείας δεν ανιχνεύονται ή ανιχνεύονται με πολυετή καθυστέρηση. Επίσης, ανάλογα με το ισχύον νομικό πλαίσιο και τις διαδικασίες κάθε χώρας, είναι πιθανό τα θύματα κάποιας παραβίασης προσωπικών τους δεδομένων να μην ενημερώνονται, λόγω νομικών κωλυμάτων (Davidoff, 2020).

Οι κύριοι παράγοντες των δεδομένων ενός οργανισμού που συντελούν στην αύξηση του ρίσκου των παραβιάσεων ασφαλείας είναι:

- Η διατήρηση, δηλαδή ο χρόνος ύπαρξής τους

- Η διάδοση, δηλαδή ο αριθμός των αντιγράφων τους

- Η πρόσβαση, δηλαδή ο αριθμός των ατόμων που έχουν δικαίωμα πρόσβασης και ο χρόνος και οι τρόποι επίτευξής της

- Η ρευστότητα, δηλαδή ο χρόνος απόκτησης πρόσβασης, μεταφοράς και επεξεργασίας τους

- Η αξία τους, αναφερόμενη στο αντίστοιχο οικονομικό μέγεθος

Στις ενέργειες που μπορούν να προκαλέσουν μία παραβίαση ασφαλείας περιλαμβάνονται:

- Οι επιθέσεις άρνησης υπηρεσιών, οι οποίες εμποδίζουν τη λειτουργία ή την πρόσβαση σε μία υπηρεσία του οργανισμού, διαθέσιμη διαδικτυακά. Διακρίνονται σε λογικές, οι οποίες εκμεταλλεύονται προγραμματιστικά λάθη για να καταστήσουν την υπηρεσία μη λειτουργική, «πλημμύρας» (flooding), οι οποίες κατακλύζουν το σύστημα με άχρηστες αιτήσεις και κατανεμημένες, αν συμμετέχουν συνεργατικά στην επίθεση σημαντικοί αριθμοί παραβιασμένων συστημάτων.

- Η μη αποδεκτή χρήση λογισμικού, όπως απόπειρες πρόσβασης σε μη εξουσιοδοτημένη πληροφορία και επίσκεψη απαγορευμένων ιστοσελίδων μέσω περιηγητών διαδικτύου σε συστήματα του οργανισμού.

- Οι υποκλοπές πληροφοριών από διαύλους επικοινωνίας του οργανισμού. Διακρίνονται σε ενεργές, αν επηρεάζουν τον δίαυλο και τα μηνύματα και παθητικές, αν η επικοινωνία κατασκοπεύεται χωρίς αλλοίωση. Επίσης, Οι ενεργές υποκλοπές μπορεί να πραγματοποιούνται «μεταξύ-των-γραμμών», αν δεν τροποποιούνται τα μηνύματα αλλά εισάγονται νέα ή «επί-της-ράχεως-εισόδου», αν τα αρχικά μηνύματα υποκλέπτονται, τροποποιούνται και επαναπροωθούνται στον παραλήπτη.

- Οι παράνομη είσοδος σε συστήματα, μέσω κρυφών μεθόδων πρόσβασης, σχεδιασμένες από τους προγραμματιστές του λογισμικού

για υποστήριξη ή χρησιμοποιώντας εγκατεστημένο κακόβουλο λογισμικό.

- Οι τροποποιήσεις πληροφοριών, είτε λόγω ατυχήματος, το οποίο δεν επέτρεψε την ολοκληρωμένη αποθήκευση κάποιων δεδομένων, είτε λόγω λανθασμένης αρχιτεκτονικής συστήματος, για παράδειγμα η οποία δε λειτουργεί ορθά υπό συνθήκες παράλληλης επεξεργασίας και αποθήκευσης δεδομένων από πολλαπλά συστήματα, είτε λόγω προγραμματιστικής αμέλειας και αστοχιών.

Οι απαιτήσεις ασφάλειας των πληροφοριών ταυτοποιούνται κατανοώντας την αξία της πληροφορίας, τις επιχειρηματικές ανάγκες για επεξεργασία, αποθήκευση και επικοινωνία, τις νομικές απαιτήσεις και τις συμφωνίες με ενδιαφερόμενα μέρη. Η μέθοδος αξιολόγησης περιλαμβάνει την ανάλυση των απειλών των τρωτών σημείων, της πιθανότητας της απειλής να παρουσιαστεί και του πιθανού αντίκτυπου των σχετικών συμβάντων ασφαλείας. Οι πόροι που αφιερώνονται σε κάθε διαδικασία ελέγχου είναι ανάλογοι των επιπτώσεων και της πιθανότητας εμφάνισης του κινδύνου που καλούνται να αντιμετωπίσουν.

2.4: Τα πλαίσια ενεργειών ασφαλείας του οργανισμού

Κάθε οργανισμός καλείται να λειτουργήσει σε ένα σύνθετο πλαίσιο νόμων, κανονισμών, απαιτήσεων, ανταγωνιστών και συνεργατών. Για την ομαλή του λειτουργία σε αυτό το περιβάλλον, είναι απαραίτητη η συμμόρφωση με διευθύνσεις ασφαλείας, μέσω της διαμόρφωσης πολιτικών, προτύπων, διαδικασιών και κατευθυντήριων και βασικών γραμμών.

Οι πολιτικές ασφαλείας καταγράφουν τους στόχους της διοίκησης του οργανισμού, εξηγούν τις ανάγκες του και προωθούν τη δέσμευση για την κάλυψη τους. Αποτελούν σύντομες περιλήψεις βασικών στοιχείων, χωρίς υπερβολική πολυπλοκότητα, ώστε να είναι κατανοητές και ακολουθήσιμες.

Στοχεύουν στον περιορισμό του ρίσκου και βοηθούν τον οργανισμό να αξιολογήσει τη συμμόρφωσή του με τους νόμους, κανονισμούς και πρότυπα που απαιτούνται. Εν κενώ, οι πολιτικές δεν έχουν αξία και απαιτείται να διαμορφώνονται, διατίθενται, επιβάλλονται και ενημερώνονται με βάση τις αλλαγές του περιβάλλοντος. Βασιζόμενο στις πολιτικές, το ανθρώπινο δυναμικό μπορεί να κατανοήσει καλύτερα τα περιουσιακά στοιχεία και τις οργανωτικές αρχές του οργανισμού. Οι λειτουργικές πολιτικές ασφαλείας, οι οποίες προωθούν ασφαλείς συμπεριφορές σε συγκεκριμένους λειτουργικούς τομείς του οργανισμού, πρέπει να διαμορφώνονται σε συνεργασία με τα τμήματα που αφορούν και να γνωστοποιούνται σε όλα τα μέρη που επηρεάζουν. Σε κάθε περίπτωση, η χρήση ισχυρού λεξιλογίου – “πρέπει” αντί για “μπορεί” – είναι απαραίτητη, δεδομένου του υποχρεωτικού και όχι συμβουλευτικού τους χαρακτήρα.

Τα πρότυπα περιγράφουν απαιτήσεις που πρέπει να καλυφθούν για την αντιμετώπιση του ρίσκου σε έναν οργανισμό. Μπορούν να είναι συγκεκριμένα ή γενικά και δηλώνουν μια ή περισσότερες επιλογές του οργανισμού για την επίτευξη κάποιων στόχων ασφαλείας, παρέχοντας κοινή βάση για όλα τα τμήματα και ομάδες. Αναπτύσσονται από τον ίδιο τον οργανισμό ή υιοθετούνται από εξωτερικούς φορείς, οι οποίο συχνά προσφέρουν δωρεάν εκπαίδευση ή δυνατότητα μαζικών αγορών μέσων. Πριν οποιαδήποτε επιλογή, απαιτείται προσεκτική ανάλυση των εναλλακτικών, δεδομένου του κόστους που τις συνοδεύει αλλά και του σημαντικού αντίκτυπου ασφάλειας – κάποιο τρωτό σημείο σε ένα πρότυπο που έχει επιλεγεί, επηρεάζει αυτόματα το σύνολο του οργανισμού ή και συνεργάτες.

Οι οργανισμοί καλούνται να συντονίσουν αποδοτικά και αποτελεσματικά πλήθος δραστηριοτήτων για την ορθή λειτουργία τους. Οι διαδικασίες αναφέρονται σε οποιαδήποτε ενέργεια αξιοποιεί πόρους και επιτρέπει τη μετατροπή εισόδων σε εξόδους, υπό προβλεπόμενες και ελεγχόμενες συνθήκες. Οι διαδικασίες ασφάλειας αποτελούν συστηματικές δράσεις για την κάλυψη κάποια ανάγκης ασφάλειας, σε διακριτά και κατανοητά βήματα.

Οι βασικές γραμμές αναφέρονται στις πρότυπες, κανονικές διαμορφώσεις βάσης, που εξασφαλίζουν την ύπαρξη ενός ελάχιστου απαιτούμενου επιπέδου ασφάλειας στα πλαίσια του συνόλου του οργανισμού. Αναφέρονται στις αρχικές ρυθμίσεις των μέσων που χρησιμοποιούνται και επιτρέπουν συγκρίσεις βασικής κάλυψης των αναγκών ασφαλείας.

Οι κατευθυντήριες γραμμές παρέχουν δομή σε ένα πρόγραμμα ασφάλειας, προτείνοντας αποδέκτες ενέργειες και καλές πρακτικές αξιοποίησης ενός πόρου. Σε αντίθεση με τις πολιτικές, προτείνεται η χρήση αδύναμου λεξιλογίου για να είναι σαφής ο προαιρετικός χαρακτήρας τους.

2.5: Τα συστήματα διαχείρισης της ασφάλειας των πληροφοριών

Η διαχείριση, γενικότερα, αναφέρεται στις ενέργειες διεύθυνσης, ελέγχου και βελτίωσης του οργανισμού, στα πλαίσια των κατάλληλων δομών. Περιλαμβάνει ενέργειες, μεθόδους και πρακτικές οργάνωσης, επίβλεψης, διαχείρισης και ελέγχου δομών και εμπλέκει ένα ή περισσότερα άτομα και ομάδες, ανάλογα με το μέγεθος του οργανισμού. Στα πλαίσια της διαχείρισης της ασφάλειας των πληροφοριών, ο όρος περιλαμβάνει την επίβλεψη και λήψη αποφάσεων προς επίτευξη των στόχων του οργανισμού, μέσα από την προστασία της πληροφορίας του.

Ένα σύστημα διαχείρισης της ασφάλειας των πληροφοριών αποτελεί συστηματική προσέγγιση της εφαρμογής, λειτουργίας, παρακολούθησης, ανάλυσης, συντήρησης και βελτίωσης των συστημάτων, βασιζόμενη στα αποτελέσματα αναλύσεων ρίσκου και στην ανοχή κάθε οργανισμού σε αυτό. Περιλαμβάνει πολιτικές, διαδικασίες, οργανωτικές δομές, ενέργειες σχεδίασης, ευθύνες, κανονισμούς και πόρους διαχειριζόμενους από έναν οργανισμό με στόχο την προστασία της πληροφορίας του, τη βελτίωση των πλάνων και δραστηριοτήτων του, τη συμμόρφωση με τους κανονισμούς και νομοθεσίες του τομέα και τη προσαρμογή στις αλλαγές του περιβάλλοντος.

Η επιτυχημένη εφαρμογή σχετικού συστήματος απαιτεί ανάλυση των απαιτήσεων προστασίας και ρίσκων, σχεδίαση και εφαρμογή κατάλληλων ελέγχων, σύμφωνα με τις ανάγκες του οργανισμού, δέσμευση της διοίκησης όσον αφορά την προώθηση κουλτούρας ασφαλείας για την προστασία των συμφερόντων των ενδιαφερόμενων μερών, ενσωμάτωση της ασφάλειας ως αναπόσπαστο μέρος των συστημάτων και δικτύων πληροφορίας, διεξοδικότητα στη διαχείριση της ασφάλειας, συνεχιζόμενη αξιολόγηση του επιπέδου προστασίας του οργανισμού και εντοπισμό των απαραίτητων αλλαγών.

Ένα ορθά λειτουργικό σύστημα ασφαλείας εξασφαλίζει τη συνεχιζόμενη προστασία της πληροφορίας, συντηρεί ένα δομημένο και διεξοδικό πλαίσιο ταυτοποίησης και αξιολόγησης των κινδύνων, επιλογής και εφαρμογής των κατάλληλων ελέγχων και μέτρησης της απόδοσης τους, βελτιώνει συνεχώς το περιβάλλον ασφάλειας και επιτυγχάνει αποδοτικά συμμόρφωση με τους απαραίτητους νόμους και κανονισμούς.

Η στρατηγική απόφαση της υιοθέτησης ενός συστήματος διαχείρισης της ασφάλειας των πληροφοριών εξαρτάται από τις ανάγκες, του στόχους, τις επιχειρηματικές διαδικασίες, το μέγεθος και τη δομή του οργανισμού. Είναι σημαντικό κατά τη σχεδίαση και λειτουργία του συστήματος να ληφθούν υπόψη τα ενδιαφέροντα και οι απαιτήσεις όλων των ενδιαφερόμενων μερών, πελατών, προμηθευτών και συνεργατών, σε τακτικές επαναλήψεις.

Η αξιολόγηση και βελτίωση της απόδοσης του συστήματος απαιτεί επαναλαμβανόμενες αναλύσεις και συγκρίσεις με τις πολιτικές και στόχους του οργανισμού και αναφορά των αποτελεσμάτων στην ηγεσία. Οι αξιολογήσεις αυτές βεβαιώνουν ότι περιλαμβάνονται οι απαραίτητοι έλεγχοι στα πλαίσια του συστήματος και υποστηρίζονται οι ενέργειες διόρθωσης, πρόληψης και βελτίωσης. Με στόχο τη συνεχιζόμενη βελτίωση του συστήματος και επακόλουθη αύξηση της πιθανότητας επίτευξης των στόχων, γύρω από τη διατήρηση της εμπιστευτικότητας, διαθεσιμότητας και ακεραιότητας της

πληροφορίας, απαιτείται εντοπισμός των ευκαιριών και απόρριψη της στασιμότητας. Στις ενέργειες για βελτίωση περιλαμβάνονται αναλύσεις και εκτιμήσεις της υπάρχουσας κατάστασης, καθορισμός ενεργειών για βελτίωση, αναζήτηση πιθανών λύσεων σε εντοπιζόμενα προβλήματα, αξιολόγηση, επιλογή και εφαρμογή τους και μέτρηση των αποτελεσμάτων τους.

Στους κρισιμότερους παράγοντες επιτυχίας ενός συστήματος διαχείρισης της ασφάλειας των πληροφοριών εντοπίζονται η ευθυγράμμιση των πολιτικών στόχων και ενεργειών ασφαλείας με τους γενικότερους στόχους του οργανισμού, η επιλογή προσεγγίσεων και πλαισίων σχεδιασμού υλοποίησης, παρακολούθησης, συντήρησης και βελτίωσης του συστήματος συμβατές με την κουλτούρα του οργανισμού και η υποστήριξη από όλα τα επίπεδα της διοίκησης. Ακόμη, η κατανόηση των απαιτήσεων ασφαλείας που προκύπτουν από τις αντίστοιχες αναλύσεις ρίσκου, η ύπαρξη προγράμματος εκπαίδευσης και ενημέρωσης των μελών του οργανισμού γύρω από την ασφάλεια των πληροφοριών, η ύπαρξη αποτελεσματικής διαδικασίας διαχείρισης των συμβάντων ασφαλείας και διαδικασίας συνέχισης της παροχής των υπηρεσιών, η συνεχιζόμενη αξιολόγηση της απόδοσης του συστήματος και η συγκέντρωση αναπληροφόρησης επιδρούν καταλυτικά.

2.6: Έλεγχοι ασφαλείας

Οι έλεγχοι ασφαλείας περιορίζουν δραστηριότητες που μπορεί να βλάψουν την ασφάλεια του οργανισμού, η οποία απαιτεί συνεχείς αξιολογήσεις για να παραμένει σύγχρονη και αποτελεσματική. Περιλαμβάνουν τις διασφαλίσεις και τα αντίμετρα που αξιοποιούνται από έναν οργανισμό για την αντιμετώπιση του ρίσκου. Κατηγοριοποιούνται σε διοικητικούς ελέγχους, οι οποίοι ελέγχουν τη συμπεριφορά του ανθρώπινου δυναμικού και εξασφαλίζουν τη συμμόρφωση με τις πολιτικές και διαδικασίες του οργανισμού και σε τεχνικούς ελέγχους, οι οποίοι αναφέρονται σε πληροφοριακά συστήματα. Κάθε έλεγχος πρέπει να έχει λόγο ύπαρξης και να δίνει λύση σε συγκεκριμένο πρόβλημα. Ανάλογα με το

σημείο του κύκλου ζωής της διαδικασίας που στοχεύουν, διακρίνονται, επίσης, σε:

- Ελέγχους εντοπισμού, οι οποίοι αναγνωρίζουν την είσοδο κάποιας απειλής στο σύστημα

- Ελέγχους πρόληψης, οι οποίοι επιχειρούν να αποτρέψουν την εκμετάλλευση κάποιου τρωτού σημείου από απειλές

- Ελέγχους επιδιόρθωσης, οι οποίοι περιορίζουν το αντίκτυπο κάποιας απειλής

- Ελέγχους αποτροπής, οι οποίοι παρεμποδίζουν δραστηριότητες που υποβοηθούν παραβιάσεις ασφαλείας. Σε αντίθεση με τους ελέγχους πρόληψης, δίνουν τη δυνατότητα σε εξειδικευμένους χρήστες να τους παρακάμψουν, λαμβάνοντας συνειδητά το σχετικό ρίσκο.

- Ελέγχους αντιστάθμισης, οι οποίοι επιλέγονται στη θέση ελέγχων με υπερβολικό κόστος ή πολυπλοκότητα εφαρμογής

Σημειώνεται ότι οι έλεγχοι περιορίζουν τη συμπεριφορά, ενώ οι διασφαλίσεις και τα αντίμετρα αναφέρονται σε ενέργειες, οι μεν προληπτικά και τα δε ως αντίδραση σε κάποια ζημιά. Είναι σημαντικό να προσδιορίζονται, παρακολουθούνται, αξιολογούνται και βελτιώνονται συνεχώς, ώστε να επιτυγχάνεται η ασφάλεια της πληροφορίας και η επίτευξη των στόχων του οργανισμού. Η ταυτοποίηση των ελέγχων που υπάρχουν και απαιτούνται για την επίτευξη της ασφάλειας απαιτούν προσεκτικό σχεδιασμό, ο όποιος να συνδυάζει τεχνικά, φυσικά και διαχειριστικά μέσα, για τη διασφάλιση της εξουσιοδοτημένης και περιορισμένης πρόσβασης στην πληροφορία του οργανισμού, ανάλογα με τις ανάγκες.

2.7: Η ομάδα διαχείρισης της ασφάλειας

Η ομάδα διαχείρισης της ασφάλειας κάθε οργανισμού αποτελείται από άτομα υπεύθυνα για το σχεδιασμό, την εφαρμογή και την παρακολούθηση του σχεδίου ασφαλείας. Είναι επιφορτισμένη με τις αρμοδιότητες ελέγχου κάθε περιουσιακού στοιχείου και καθορίζει τη σημασία τους και την αντίστοιχη αναγκαιότητα προστασίας τους. Στις βασικότερες αρμοδιότητες της ομάδας περιλαμβάνεται ο έλεγχος της πρόσβασης σε συστήματα και πόρους, μέσω των διαδικασιών τις ταυτοποίησης και αυθεντικοποίησης των χρηστών, ελέγχου της εξουσιοδότησης και καταγραφής των ενεργειών τους.

Πλήθος εγγράφων τεκμηρίωσης είναι απαραίτητα για τη λήψη ορθότερων αποφάσεων από την ομάδα ασφαλείας. Στα πιο σημαντικά εντοπίζονται οι λίστες ευαίσθητων στοιχείων, οι διαδικασίες ασφάλειας του οργανισμού, οι εξουσιοδοτήσεις των υπευθύνων, οι πολιτικές, διαδικασίες και κατευθυντήριες γραμμές που έχουν υιοθετηθεί.

Ένας οργανισμός πρέπει να συμμορφώνεται τόσο νομικά, με τους νόμους και τους κυβερνητικούς κανονισμούς, όσο και οργανωτικά, με τις εσωτερικές πολιτικές, αρχές, την κουλτούρα και τα πρότυπα που έχουν επιλεγεί. Βασική αρμοδιότητα της ομάδας ασφαλείας είναι η παρακολούθηση και επιβεβαίωση της συμμόρφωσης με όλα τα παραπάνω. Για αυτό το σκοπό αξιοποιούνται οι καταγραφές συμβάντων, ο ρόλος του συνδέσμου συμμόρφωσης και οι διαδικασίες αποκατάστασης.

Οι καταγραφές συμβάντων περιλαμβάνουν ενέργειες που ακολουθήθηκαν και γενικότερες πληροφορίες πρόσβασης και αξιοποίησης πόρων και συστημάτων κατά τη διάρκεια του χρονικού διαστήματος ενδιαφέροντος. Μετά από παραβιάσεις ασφαλείας, χρησιμοποιούνται κατά την έρευνα του προβλήματος και τις προσπάθειες εντοπισμού του τρωτού σημείου. Είναι σημαντικό να συμπεριλαμβάνεται στις καταγραφές όλη η πληροφορία που μπορεί μελλοντικά να χρειαστεί, λαμβάνοντας πάντα υπόψη ότι μεγαλύτερος όγκος δεδομένων συνεπάγεται υψηλότερες ανάγκες αποθήκευσης και πιο αργά συστήματα, αλλά

και η σημασία της ύπαρξης αυστηρά ελεγχόμενης πρόσβασης, για τη διασφάλιση της ακεραιότητας της πληροφορίας.

Ο σύνδεσμος συμμόρφωσης διασφαλίζει ότι το προσωπικό, ανεξαρτήτως τμήματος και επιμέρους αναγκών ασφαλείας, γνωρίζει και συμμορφώνεται με τις πολιτικές του οργανισμού. Πρόκειται για διαδικασία με σημαντική δυσκολία, ανάλογη με το μέγεθος και την πολυπλοκότητα του οργανισμού. Στις αρμοδιότητες του ρόλου περιλαμβάνεται η διασφάλιση της ευθυγράμμισης κάθε μέρους του οργανισμού με το πλαίσιο ασφαλείας, η υποστήριξη της ενσωμάτωσης διαδικασιών ασφαλείας στις καθημερινές δραστηριότητες των τμημάτων και η εξέταση των δεσμεύσεων εξωτερικής ανάθεσης και της τήρησης των συμφωνιών από τα ενδιαφερόμενα μέλη.

Η πρόληψη των κινδύνων έχει υψηλότερη προτεραιότητα, αναμενόμενα, ωστόσο, κάποιοι θα παρουσιαστούν. Συνεπώς, απαιτούνται πλάνα αντιμετώπισης και ομάδες αντίδρασης σε συμβάντα ασφαλείας. Οι διαδικασίες αποκατάστασης περιλαμβάνουν τόσο την πρόληψη της εμφάνισης τρωτών σημείων, όσο και την επιδιόρθωση όσων εντοπιστούν, ανάλογα με την προτεραιότητά τους. Οι αρμοδιότητες της ομάδας διαχείρισης της ασφάλειας περιλαμβάνουν ενέργειες αντίδρασης σε κάθε συμβάν – διακοπή ή καταστροφή - που πλήττει τον οργανισμό. Στα πλαίσια αυτής της αντίδρασης, σχηματίζονται ομάδες υπεύθυνες για την έρευνα και αντιμετώπιση τυχόν παραβιάσεων ασφαλείας, αλλά και ομάδες έκτακτης λειτουργίας, οι οποίες αναλαμβάνουν την προστασία των ευαίσθητων πληροφοριών κατά τη διάρκεια των έκτακτων αναγκών, με ταχύτητα και αποδοτικότητα.

Επίσης, η σημασία της προώθησης της επαγγελματικής ηθικής και των αντίστοιχων κανόνων συμπεριφοράς κρίνεται καταλυτική. Όλοι οι κανόνες καλούνται να ακολουθηθούν από ανθρώπους, το οποίο απαιτεί την αντίστοιχη εμπιστοσύνη και σεβασμό προς το πρόσωπο αυτών που τους ορίζουν, ενώ οι πιστοποιήσεις ασφαλείας απαιτούν από τους υποψηφίους να συμμορφώνονται με έναν συγκεκριμένο κώδικα δεοντολογίας προτού προκριθούν. Προς αυτή την κατεύθυνση, βοηθάει σημαντικά η επίδειξη ισχυρών ηθικών αρχών στις

καθημερινές δραστηριότητες της ομάδας ασφαλείας, η προώθηση των ηθικών οδηγιών και προτύπων που κρίνονται σημαντικά και συνεχείς προσπάθειες ενημέρωσης εκπαίδευσης σχετικά με την ασφάλεια για όλους τους εργαζομένους.

Κεφάλαιο 3: Πρότυπα διαχείρισης της ασφάλειας των πληροφοριών

Τα πρότυπα διαχείρισης της ασφάλειας των πληροφοριών βοηθούν τους οργανισμούς να υλοποιήσουν τις κατάλληλες διαδικασίες και ελέγχους προς περιορισμό των απειλών, παρέχοντας τις βάσεις για αποδοτικά συστήματα διαχείρισης της ασφάλειας των πληροφοριών και περιγράφοντας απαιτήσεις, διαδικασίες, πολιτικές ή και καλές πρακτικές.

Σημειώνεται ότι η πλειονότητα των προτύπων προβλέπει τη δυνατότητα πιστοποίησης της εφαρμογής τους σε συγκεκριμένους φορείς. Ένας οργανισμός με πιστοποιημένη συμμόρφωση με δημοφιλή πρότυπα μπορεί να αποδείξει και επιδείξει σε πελάτες και συνεργάτες του το επίπεδο ασφάλειας των πληροφοριών του, ενώ οι επαναλαμβανόμενες διαδικασίες πιστοποίησης οδηγούν συνεχή βελτίωση και ενημέρωση των διαδικασιών του, με βάση τις εξελίξεις του περιβάλλοντος.

Στα πιο διαδεδομένα εντοπίζονται η οικογένεια προτύπων ISO/IEC 27000, το πλαίσιο ITIL, το πλαίσιο COBIT και το πλαίσιο O-ISM3. Παρά σχετικές βιβλιογραφικές αναφορές, ακριβή, πρόσφατα δεδομένα για την παγκόσμια υιοθέτησή τους είναι διαθέσιμα μόνο για την πρώτη οικογένεια προτύπων, με περίπου 37 χιλιάδες ενεργές πιστοποιήσεις οργανισμών το 2019 (International Organization for Standardization, 2020).

Η έλλειψη σχετικών δεδομένων υποδεικνύει τη συγκριτικά μικρή σημασία, ακόμη, για την πλειονότητα των οργανισμών, όσον αφορά τη συμμόρφωση με διεθνή πρότυπα ασφάλειας πληροφοριών. Στην Ιταλία, μόλις το 22% των οργανισμών είχε ολική ή εν μέρει πιστοποίηση συμμόρφωσης με τα πρότυπα ISO/IEC 27000 το 2016, σε σύγκριση με το 63% των οργανισμών με καμία συμμόρφωση (Statista, 2016). Το 2012, μόλις το 15% των ερωτηθέντων οργανισμών παγκοσμίως ακολουθούσε επίσημα πρότυπα ασφαλείας (Statista, 2012), ενώ στο Ηνωμένο Βασίλειο, το 2017, μόνο το 20% των μικρών και 38%

των μεσαίων επιχειρήσεων γνώριζε την ύπαρξη της οικογένειας προτύπων ISO/IEC 27000.

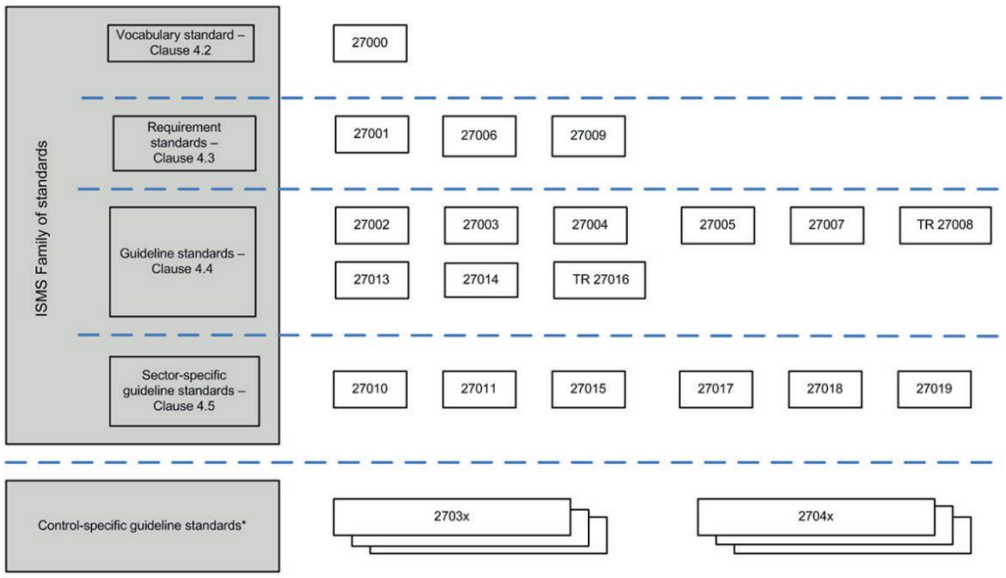
Σημειώνεται ότι η υιοθέτησή τους δεν απαιτεί μονολιθική επιλογή, η οποία αποκλείει την εφαρμογή των υπολοίπων. Οι διαφορετικές τους προσεγγίσεις τα καθιστά σε σημαντικό βαθμό συμβατά.

Παρακάτω, αναλύονται τα κύρια σημεία τους, τα οποία σχετίζονται με τη διαχείριση των πληροφοριακών συστημάτων και της ασφάλειάς τους.

3.1: Η οικογένεια προτύπων ISO/IEC 27000

Η οικογένεια προτύπων ISMS ή σειρά ISO/IEC 27000 (International Organization for Standardization, 2018) αποτελείται από πλήθος προτύπων ασφάλειας πληροφοριών, τα οποία προωθούν συμβουλές και καλές πρακτικές για την αποτελεσματικότερη διαχείριση των ρίσκων πληροφορίας, με τη χρήση των κατάλληλων ελέγχων. Είναι επιτηδευμένα ευρεία, ώστε να ανταποκρίνονται στις ανάγκες πλήθους διαφορετικών οργανισμών και ενθαρρύνουν τους τελευταίους να τα παραμετροποιούν, ανάλογα με τις ανάγκες τους, βασιζόμενοι σε συνεχή ανάδραση και ενέργειες βελτίωσης, για να είναι σε θέση να ανταποκρίνονται στη δυναμική φύση των προβλημάτων που καλούνται να αντιμετωπίσουν.

Τα αλληλοσυνδεμένα πρότυπα της οικογένειας επικεντρώνονται στην θέση της ασφάλειας πληροφοριών υπό το συνολικό διαχειριστικό έλεγχο της διοίκησης του οργανισμού. Κατηγοριοποιούνται σε πρότυπα τα οποία περιγράφουν απαιτήσεις των συστημάτων διαχείρισης της ασφάλειας των πληροφοριών, πρότυπα με προϋποθέσεις για τους φορείς πιστοποίησης της τήρησής τους΄, κατευθυντήριες γραμμές και πρόσθετα έγγραφα με επιπλέον πληροφορίες για την εφαρμογή των προτύπων σε συγκεκριμένους τομείς.



Διάγραμμα 10 - Η οικογένεια προτύπων ISMS (International Organization for Standardization, 2018)

Σύμφωνα με τα αυτά, ένας οργανισμός ευθυγραμμισμένος με τη συγκεκριμένη οικογένεια προτύπων επωφελείται από ένα δομημένο πλαίσιο διαμόρφωσης των διαδικασιών ενός αποδοτικού συστήματος διαχείρισης της ασφάλειας των πληροφοριών, την υποστήριξη της υπεύθυνης διαχείρισης του συστήματος με ολιστικό τρόπο, την προώθηση κοινώς αποδεκτών καλών πρακτικών, προσαρμόσιμων στις ανάγκες του οργανισμού, τους κοινούς και πιστοποιήσιμους σχετικούς ελέγχους, που αυξάνουν την αυτοπεποίθηση και εμπιστοσύνη των συνεργατών, την κάλυψη κοινωνικών αναγκών και την αποδοτικότερη οικονομική διαχείριση των επενδύσεων σε συστήματα ασφαλείας. Τονίζεται ότι οι σχετικοί κανονισμοί πρέπει να είναι καταγεγραμμένοι, επικοινωνήσιμοι και διαθέσιμοι σε όλα τα ενδιαφερόμενα μέρη.

Το πρότυπο ISO/IEC 27001

Το πρότυπο ISO/IEC 27001 (International Organization for Standardization, 2013) περιγράφει απαιτήσεις για την ανάπτυξη και λειτουργία ενός συστήματος

διαχείρισης της ασφαλείας των πληροφοριών και των σχετικών ελέγχων, προς περιορισμό των ρίσκων, τα οποία ο οργανισμός κρίνει σημαντικά.

Στα πλαίσια του συγκεκριμένου προτύπου περιλαμβάνονται 8 υποχρεωτικές κατηγορίες ελέγχων και 148 επιμέρους σημεία, τα οποία πρέπει να καλύπτονται, γύρω από την οργάνωση, ηγεσία του οργανισμού, τις διαδικασίες σχεδίασης, υποστήριξης, λειτουργίας, αξιολόγησης και βελτίωσης.

Διάγραμμα 11 - Απεικόνιση των βασικών κατηγοριών ελέγχων του προτύπου ISO/IEC 27001

Σχεδίαση του συστήματος διαχείρισης της ασφάλειας των πληροφοριών

Σύμφωνα με το πρότυπο, ο οργανισμός πρέπει να προσδιορίσει εξωτερικά και εσωτερικά προβλήματα, σχετικά με το σκοπό του, που επηρεάζουν τη δυνατότητά του να επιτύχει τα επιθυμητά αποτελέσματα, στα πλαίσια της διαχείρισης της ασφάλειας των πληροφοριών. Επίσης, πρέπει να προσδιοριστούν οι ομάδες σχετικές με το συγκεκριμένο σύστημα , οι απαιτήσεις των τελευταίων και η αλληλεπίδραση των ενεργειών του οργανισμού και των

συνεργατών του, καταλήγοντας στα όρια και τη λειτουργία του συστήματος. Σημειώνεται η αναγκαιότητα του προσδιορισμού υλοποίησης, συντήρησης και συνεχούς βελτίωσης του συστήματος, με βάση τα πρότυπα που ακολουθούνται.

Κατά τη σχεδίαση του συστήματος, ο οργανισμός πρέπει να λάβει υπόψη του τις προαναφερθείσες απαιτήσεις, τους κινδύνους και τις ευκαιρίες που σχετίζονται με την επίτευξη των επιθυμητών αποτελεσμάτων από το σύστημα ασφαλείας, την πρόληψη ή μείωση των ανεπιθύμητων επιδράσεων, την επίτευξη συνεχούς βελτίωσης, την ενσωμάτωση του συστήματος ασφαλείας στις διαδικασίες και την αξιολόγηση της απόδοσης των τελευταίων.

Ανάλυση και αντιμετώπιση ρίσκου

Στα πλαίσια του προτύπου, είναι απαραίτητος ο προσδιορισμός και η εφαρμογή διαδικασίας αξιολόγησης του ρίσκου ασφαλείας πληροφοριών, με βάση συγκεκριμένα κριτήρια αποδοχής και η διασφάλιση ότι οι αναλύσεις ρίσκου παράγουν συνεχή, επιβεβαιωμένα και συγκρίσιμα αποτελέσματα. Οι τελευταίες, απαιτείται να είναι σε θέση να εντοπίσουν κινδύνους που αφορούν την ακεραιότητα, διαθεσιμότητα και εμπιστευτικότητα της πληροφορίας και πιθανές συνέπειες και τους ταξινομούν, ανάλογα με την προτεραιότητα τους.

Ο οργανισμός πρέπει να διαμορφώσει και εφαρμόσει μια διαδικασία αντιμετώπισης των ρίσκων ασφάλειας πληροφοριών, λαμβάνοντας υπόψη τις διαθέσιμες επιλογές για το προφίλ ρίσκου του οργανισμού, τα αποτελέσματα των αναλύσεων και τους απαραίτητους ελέγχους ασφαλείας, να είναι σε θέση να δικαιολογήσει αυτές τις επιλογές και να τις εντάξει σε ένα συνολικότερο πλάνο, το οποίο να λαμβάνει την έγκριση των υπευθύνων διαχείρισης της συγκεκριμένης κατηγορίας ρίσκων.

Η στοχοθεσία ασφάλειας πληροφοριών πρέπει να είναι συμβατή με τις πολιτικές ασφαλείας, μετρήσιμη, κατανοητή, να λαμβάνει υπόψη της τα αποτελέσματα των αναλύσεων και να ανανεώνεται τακτικά. Είναι σημαντικό τα

διαθέσιμα έγγραφα να προσδιορίζουν με ακρίβεια το τι, από ποιον, με ποιον τρόπο και μέχρι πότε θα πραγματοποιηθεί, αλλά και τον τρόπο επαλήθευσης των αποτελεσμάτων.

Στα πλαίσια του προτύπου, ο οργανισμός καλείται να σχεδιάσει, υλοποιήσει και ελέγχει τις απαραίτητες διαδικασίες για την κάλυψη των απαιτήσεων ασφαλείας και να πραγματοποιεί τακτικές αναλύσεις ρίσκου, διατηρώντας τα κατάλληλα αρχεία προς επιβεβαίωση των ενεργειών και αποφυγή και εξάλειψη των αρνητικών επιπτώσεων, ιδιαίτερα πριν και μετά από σημαντικές αλλαγές.

Εκπαίδευση, επικοινωνία και καταγραφή πληροφορίας

Ο οργανισμός πρέπει να καθορίσει τις απαραίτητες ικανότητες, εκπαίδευση και προσόντα των ατόμων που επηρεάζουν την απόδοση του συστήματος ασφάλειας των πληροφοριών, να αναλάβει δράση για την επίτευξη και αξιολόγηση της τελευταίας και να διατηρήσει τα απαραίτητα αρχεία πληροφοριών ως αποδείξεις. Τα συγκεκριμένα άτομα πρέπει να γνωρίζουν τις πολιτικές ασφαλείας, τη συμμετοχή τους στην αποτελεσματικότητά των πολιτικών, τα πλεονεκτήματα της ορθής τους εφαρμογής και τους κινδύνους σχετικών παραλείψεων.

Όσον αφορά την επικοινωνία των ομάδων του οργανισμού, απαιτείται σαφής προσδιορισμός των αναγκών για εσωτερικές και εξωτερικές επαφές, αλλά και του αντικειμένου, των συμμετεχόντων, του τρόπου και χρόνου της επικοινωνίας και των διαδικασιών που επηρεάζονται.

Η καταγεγραμμένη πληροφορία πρέπει να περιλαμβάνει ό,τι απαιτείται από τα εφαρμοζόμενα πρότυπα και χρειάζεται για την αποτελεσματικότερη λειτουργία του συστήματος ασφαλείας των πληροφοριών. Η καταγραφή και ανανέωση της πληροφορίας πρέπει να έχει σαφή περιγραφή και τρόπο ταυτοποίησης, μορφή και επάρκεια για το στόχο της συγκεκριμένης επικοινωνίας και η διαθεσιμότητα και προστασία της πρέπει να ελέγχεται συνεχώς. Σαφείς δε κανόνες πρέπει να διέπουν τον διαμοιρασμό και τη διάθεση της πληροφορίας, τον τρόπο

πρόσβασης και ανάκτησης, αποθήκευσης και διατήρησης της εγκυρότητας και τον έλεγχο των αλλαγών.

Αξιολόγηση του συστήματος

Ο οργανισμός πρέπει να αξιολογεί την απόδοση του συστήματος διαχείρισης της ασφάλειας των πληροφοριών, προσδιορίζοντας τί πρέπει να παρακολουθείται και μετρείται, τις μεθόδους επιβεβαίωσης και τον τρόπο διατήρησης των αποτελεσμάτων, το χρόνο και τρόπο ανάλυσης των τελευταίων και τον υπεύθυνο αυτών των ενεργειών. Η ύπαρξη εσωτερικών ελέγχων, ανά τακτικά διαστήματα, κρίνεται απαραίτητη για τη διασφάλιση της συμμόρφωσης του συστήματος με τις απαιτήσεις του οργανισμού και τα πρότυπα που ακολουθούνται. Τα σχετικά προγράμματα ελέγχων πρέπει να σχεδιαστούν διεξοδικά και να εφαρμόζονται με συνέπεια, με σαφή συχνότητα, μεθόδους, ευθύνες, αναφορές, κριτήρια και υπεύθυνα μέρη, με αντικειμενικότητα, διατήρηση λεπτομερών εγγράφων και τακτικές ενημερώσεις της ηγεσίας. Η τελευταία, πρέπει να λαμβάνει υπόψη της προηγούμενα αποτελέσματα, αλλαγές σε εσωτερικά και εξωτερικά ζητήματα που επηρεάζουν το περιβάλλον ασφαλείας του οργανισμού, αναπληροφόρηση γύρω από σχετικά μεγέθη, αστοχίες και ενέργειες αντιμετώπισης, αναλύσεις ρίσκου, ελέγχους ασφαλείας και ευκαιρίες για βελτίωση για την ορθότερη λήψη αποφάσεων.

Όταν εντοπίζεται κάποια αστοχία, ο οργανισμός πρέπει να είναι σε θέση να αντιδράσει άμεσα, να διορθώσει το πρόβλημα, να αντιμετωπίσει τις συνέπειες και να αξιολογήσει την ανάγκη για εξάλειψη των αιτιών της αστοχίας, αναλύοντας την περίσταση, άλλες παρόμοιες αστοχίες και την απόδοση των διορθωτικών ενεργειών, διατηρώντας το κατάλληλο αρχείο ενεργειών και αποτελεσμάτων. Επίσης, κρίνεται σημαντική η συνεχής βελτίωση της επάρκειας και αποτελεσματικότητας του συστήματος ασφάλειας πληροφοριών.

Ο ρόλος της ηγεσίας

Σε αυτά τα πλαίσια, η ηγεσία καλείται να δεσμευθεί για την προώθηση πολιτικών, οι οποίες αφορούν τη διασφάλιση της στοχοθεσίας του συστήματος ασφαλείας των πληροφοριών, τη συμβατότητα του με το στρατηγικό όραμα του οργανισμού, την ενσωμάτωση των απαιτήσεων του συστήματος στις διαδικασίες του οργανισμού, την εξασφάλιση των απαραίτητων πόρων και τη προώθηση της συμμόρφωσης με τις απαιτήσεις ασφαλείας. Ακόμη, αναφέρεται η σημασία της ενίσχυσης και υποστήριξης των ατόμων που συμμετέχουν στις διαδικασίες προστασίας, της προώθησης της συνεχούς βελτίωσης και της υποστήριξης των διαχειριστικών ρόλων ασφαλείας. Επίσης, η ηγεσία πρέπει να δεσμευθεί για τον σαφή προσδιορισμό και κάλυψη των ευθυνών και ρολών, γύρω από τη διασφάλιση της κάλυψης των απαιτήσεων του προτύπου και για τακτικές ενημερώσεις, σχετικά με την απόδοση του συστήματος ασφάλειας των πληροφοριών.

3.2: Το πλαίσιο ITIL

Το πλαίσιο ITIL (Information Technology Infrastructure Library) αποτελεί μια συλλογή εννοιών, πολιτικών και καλών πρακτικών αποτελεσματικής διαχείρισης υποδομής και υπηρεσιών πληροφορικής, προωθώντας την ευθυγράμμιση των τελευταίων με τις ανάγκες της επιχείρησης (AXELOS, 2019). Περιγράφει διαδικασίες, καθήκοντα και λίστες ελέγχου, ανεξαρτήτως του τομέα δραστηριοτήτων του οργανισμού ή τεχνολογιών που χρησιμοποιούνται, προσανατολισμένες με την εταιρική στρατηγική, την παράδοση ανώτερης αξίας και τη διατήρηση ενός κατώτατου επιπέδου εταιρικής επάρκειας. Αποτελεί μια βάση για τον οργανισμό, η οποία υποβοηθεί τη σχεδίαση, υλοποίηση και μέτρηση της βελτίωσης.

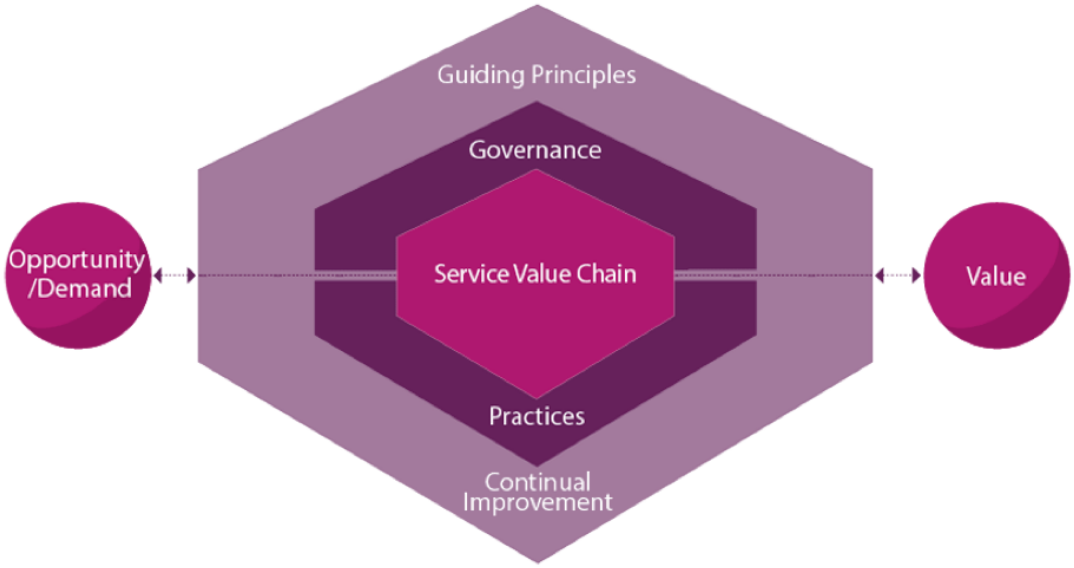
Ο φορέας που αρχικά ανέπτυξε το συγκεκριμένο πλαίσιο ήταν μέρος του Υπουργείου Οικονομικών του Ηνωμένου Βασιλείου, ωστόσο πλέον έχει απορροφηθεί από την κυβέρνηση. Δεν υπάρχει επίσημη, ανεξάρτητη αρχή

πιστοποίησης της συμμόρφωσης με το πλαίσιο σε εταιρικό επίπεδο, παρά μόνο σε ατομικό.

Τα κύρια σημεία του πλαισίου αποτελούνται από το σύστημα αξίας υπηρεσιών (service value system – SVS) και το μοντέλο των τεσσάρων διαστάσεων (four dimensions model).

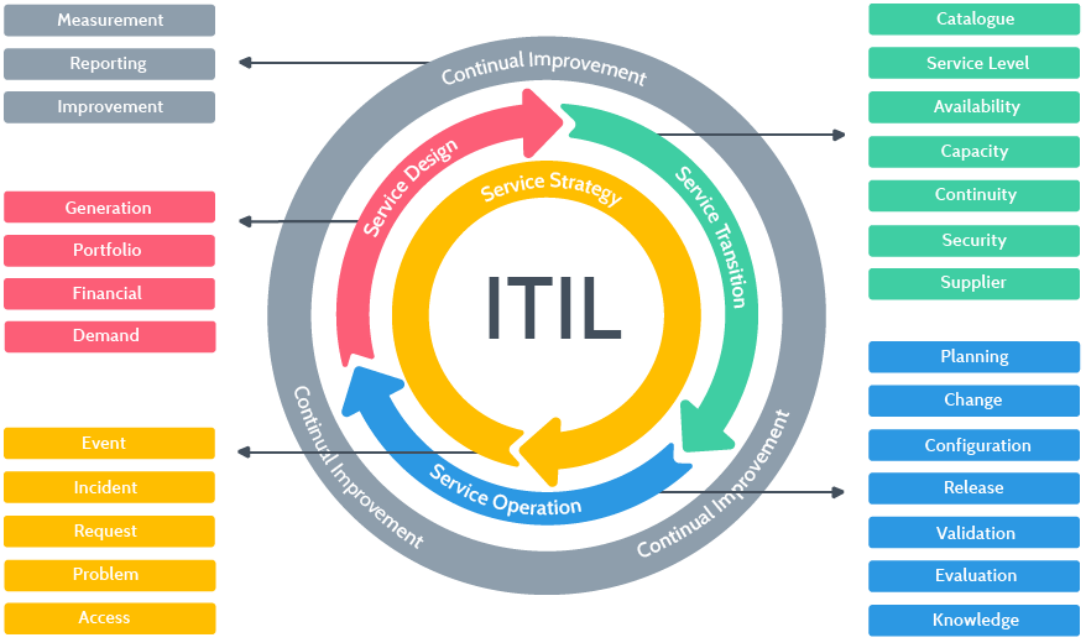
Το σύστημα αξίας υπηρεσιών

Η παρουσίαση της αλληλεπίδρασης των διαφορετικών δραστηριοτήτων και τμημάτων του οργανισμού, υποστηριζόμενων από τεχνολογίες πληροφορικής, γίνεται μέσω του συστήματος αξίας υπηρεσιών. Το σύστημα διευκολύνει την ευέλικτη διασύνδεση και συντονισμό των παραπάνω και εστιάζει τις προσπάθειες του οργανισμού στην παραγωγή αξίας. Κύρια μέρη του είναι η αλυσίδα αξίας υπηρεσιών, οι πρακτικές, οι κατευθυντήριες αρχές, η διακυβέρνηση και η συνεχής βελτίωση.



Διάγραμμα 12 - Απεικόνιση του συστήματος αξίας υπηρεσιών του πλαισίου ITIL (AXELOS, 2019)

Η αλυσίδα αξίας υπηρεσιών αποτελεί ένα ευέλικτο λειτουργικό μοντέλο για τη δημιουργία, παράδοση και συνεχή βελτίωση των υπηρεσιών. Ορίζει έξι διακριτές δραστηριότητες, οι προσαρμόσιμοι συνδυασμοί των οποίων δημιουργούν πολλαπλές ροές αξίας, για τις ανάγκες της αποδοτικής, αποτελεσματικής και πολυτροπικής διαχείρισης υπηρεσιών, στα σύγχρονα περιβάλλοντα μεταβαλλόμενων απαιτήσεων. Οι δραστηριότητες αυτές αναφέρονται στη σχεδίαση, τη βελτίωση, την ενεργοποίηση, τη μετατροπή, την απόκτηση ή δημιουργία και την παράδοση και υποστήριξη. Αξιοποιώντας πρακτικές, πόρους, διαδικασίες και ικανότητες, οι δραστηριότητες μετατρέπουν εισόδους σε εξόδους και δημιουργούν ροές αξίας.



Διάγραμμα 13 - Απεικόνιση των κύριων διαδικασιών του πλαισίου ITIL (Gallia, 2020)

Οι κατευθυντήριες αρχές βοηθούν τη διαδικασία λήψης αποφάσεων, ανάληψης δράσεων και την κοινή προσέγγιση στη διαχείριση υπηρεσιών, προσφέροντας παράλληλα μια βάση για τη διαμόρφωση υγειούς κουλτούρας στα πλαίσια του οργανισμού.

Οι δραστηριότητες διακυβέρνησης που παρουσιάζονται αφορούν τη συνεχή ευθυγράμμιση του στρατηγικού οράματος της διοίκησης του οργανισμού με τις καθημερινές λειτουργίες.

Οι πρακτικές προσφέρουν ευέλικτα εργαλεία για την υποστήριξη πολλαπλών δραστηριοτήτων αλυσίδων αξίας υπηρεσιών.

Η συνεχής βελτίωση υποστηρίζει όλα τα υπόλοιπα μέρη του συστήματος αξίας υπηρεσιών, παρέχοντας ένα πρακτικό μοντέλο βελτίωσης, για τη διατήρηση της ανθεκτικότητας και της ευελιξίας σε δυναμικά περιβάλλοντα.

Το μοντέλο των τεσσάρων διαστάσεων

Σύμφωνα με το μοντέλο των τεσσάρων διαστάσεων, στα πλαίσια της ολιστικής προσέγγισης της διαχείρισης υπηρεσιών, περιγράφονται οι τέσσερεις διαστάσεις της τελευταίας, οι οποίες αναφέρονται στα άτομα και στους οργανισμούς, στην τεχνολογία και την πληροφορία, στους προμηθευτές και στους συνεργάτες και στις ροές και διαδικασίες αξίας. Με την κατάλληλη αντιμετώπιση κάθε μίας από τις προαναφερθείσες διαστάσεις, το σύστημα αξίας υπηρεσιών παραμένει ισορροπημένο και αποδοτικό.

Το σύστημα αξίας υπηρεσιών περιλαμβάνει πλήθος από γενικές διοικητικές πρακτικές, πρακτικές διαχείρισης υπηρεσιών και τεχνικές πρακτικές διαχείρισης. Στα πλαίσια της συγκεκριμένης εργασίας, θα αναλυθούν οι πρακτικές διαχείρισης ασφάλειας πληροφοριών, διαχείρισης συμβάντων και συνέχισης της υπηρεσίας (service continuity).

Πρακτικές διαχείρισης ασφάλειας πληροφοριών

Οι πρακτικές διαχείρισης ασφάλειας πληροφοριών επιχειρούν να προστατεύσουν τις πληροφορίες που χρειάζεται ο οργανισμός για τη λειτουργία του και περιλαμβάνουν την κατανόηση και διαχείριση ρίσκων για την

εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα της πληροφορίας, την πιστοποίηση ταυτότητας και την απόδοση ευθύνης (non-repudiation).

Η απαιτούμενη ασφάλεια ρυθμίζεται μέσω πολιτικών, διαδικασιών, διαχείρισης ρίσκων, ελέγχων και συμπεριφορών, οι οποίες εξασφαλίζουν πρόληψη, εντοπισμό και διόρθωση των προβλημάτων που προκύπτουν από συμβάντα ασφαλείας.

Τονίζεται, παράλληλα, η σημασία της ισορροπίας μεταξύ της προστασίας του οργανισμού και της ενθάρρυνσης της καινοτομίας. Υπερβολικά περιοριστικοί έλεγχοι ασφαλείας μπορούν να αποβούν επιβλαβείς ή να παρακαμφθούν από άτομα που προσπαθούν να εργαστούν με μεγαλύτερη ευκολία. Κρίνεται αναγκαίο οι έλεγχοι ασφάλειας να λαμβάνουν υπόψη τους τους τρόπους αλληλεπίδρασης των πρακτικών διαχείρισης ασφάλειας πληροφοριών με όλους τους τομείς του οργανισμού, μέσω της ένταξης ελέγχων στις διαδικασίες σχεδιασμού των εργασιών. Η κουλτούρα της διαχείρισης ασφάλειας πληροφοριών πρέπει να προωθηθεί από τα υψηλότερα ιεραρχικά κλιμάκια του οργανισμού και να βασίζεται σε κατανοητές διοικητικές απαιτήσεις και οργανωτικές πολιτικές.

Για τις ανάγκες των περισσότερων οργανισμών απαιτείται διακριτή ομάδα ασφάλειας πληροφοριών, η οποία διεξάγει αναλύσεις ρίσκου και προσδιορίζει πολιτικές, διαδικασίες και ελέγχους. Σε περιβάλλοντα υψηλής ταχύτητας η διαχείριση ασφάλειας πληροφοριών πρέπει να είναι ενσωματωμένη στις καθημερινές εργασίες ανάπτυξης και λειτουργίας, μετατοπίζοντας τη σημασία από τον έλεγχο των διαδικασιών στην επαλήθευση των προϋποθέσεων που απαιτούνται, δεδομένης της κρίσιμης εξάρτησης της ασφάλειας πληροφοριών από τις συμπεριφορές των ατόμων στον οργανισμό. Υπάλληλοι οι οποίοι έχουν εκπαιδευτεί σωστά και προσέχουν τις πολιτικές και τους ελέγχους ασφάλειας πληροφοριών μπορούν να συνεισφέρουν στη ανίχνευση, πρόληψη και διόρθωση των συμβάντων ασφάλειας πληροφοριών, Αντίθετα, υπάλληλοι με ελλιπή εκπαίδευση ή παρακίνηση αποτελούν σημαντικό κίνδυνο ασφάλειας

Στις σημαντικότερες διαδικασίες υποστήριξης της ασφάλειας πληροφοριών περιλαμβάνονται διαδικασίες διαχείρισης συμβάντων ασφάλειας πληροφοριών, διαχείρισης ρίσκου, επανεξέτασης και ελέγχου, διαχείρισης ταυτότητας και πρόσβασης, διαχείρισης συμβάντων, δοκιμών διείσδυσης (penetration testing) και διαχείρισης αλλαγών. Σε αυτά τα πλαίσια, η ασφάλεια πληροφοριών πρέπει να ενσωματώνεται σε όλες τις πρακτικές και υπηρεσίες του οργανισμού και να λαμβάνεται υπόψη κατά τις ενέργειες βελτίωσης της αλυσίδας αξίας ώστε να αποφεύγεται η εισαγωγή ευπαθειών.

Διαχείριση συμβάντων

Στόχος των πρακτικών διαχείρισης συμβάντων είναι ο περιορισμός των αρνητικών επιδράσεων των συμβάντων και η επαναφορά της κανονικής λειτουργίας το συντομότερο δυνατόν. Η διαχείριση των συμβάντων μπορεί να έχει σημαντικότατη επίπτωση στην ικανοποίηση των χρηστών και των πελατών και στην εικόνα του οργανισμού. Κάθε συμβάν πρέπει να καταγράφεται και διαχειρίζεται για τη διασφάλιση της έγκαιρης επίλυσης του με βάση τις συγκεκριμένες προσδοκίες. Οι χρόνοι επίλυσης είναι συμφωνημένοι, καταγεγραμμένοι και γνωστοποιημένοι προς επίτευξη ρεαλιστικών προσδοκιών. Τα συμβάντα κατηγοριοποιούνται με βάση την προτεραιότητα τους, ανάλογα με το επιχειρηματικό τους αντίκτυπο.

Ο σχεδιασμός των πρακτικών διαχείρισης συμβάντων πρέπει να λαμβάνει υπόψη του τις διαφορετικές προτεραιότητες στη δίκαιη κατανομή των πόρων, ώστε συμβάντα με μικρή επίπτωση να διαχειρίζονται αποδοτικά, χωρίς αξιοσημείωτη κατανάλωση, τη στιγμή που σημαντικότερα συμβάντα θα απαιτούν περισσοτέρους πόρους και συνθέτη διαχείριση. Προτείνεται η ύπαρξη διαφορετικών διαδικασιών για σημαντικά συμβάντα και για συμβάντα ασφαλείας πληροφοριών. Πληροφορίες για τα συμβάντα πρέπει να αποθηκεύονται σε αρχεία περιστατικών, με τη χρήση κατάλληλων εργαλείων, τα οποία παρέχουν δυνατότητες αποδοτικής διάγνωσης και επίλυσης. Σύγχρονα σχετικά εργαλεία παρέχουν αυτοματοποιημένη αντιστοίχιση

συμβάντων με ήδη γνωστά προβλήματα και παρέχουν έξυπνους τρόπους ανάλυσης των δεδομένων προς υποβοήθηση του προσωπικού.

Είναι σημαντικό τα άτομα τα οποία ασχολούνται με την επίλυση συμβάντων να παρέχουν συχνά ενημερώσεις και πληροφορίες, για καλύτερη συνεργασία και συνέχιση των εργασιών. Προτείνεται, επίσης, η χρήση εργαλείων συνεργασίας, καθώς πολλά περιστατικά αφορούν και αντιμετωπίζονται από άτομα σε διαφορετικές ομάδες του οργανισμού, τα οποία καλούνται να συνεργαστούν αποδοτικά, ειδικά για πιο σύνθετα και σημαντικές καταστάσεις. Όλοι οι συμμετέχοντες πρέπει να γνωρίζουν τις διαδικασίες αντιμετώπισης και την συμμετοχή τους σε αυτή.

Τα πιο σύνθετα και κρίσιμα συμβάντα απαιτούν προσωρινές ομάδες, οι οποίες καλούνται να συνεργαστούν με όλους τους ενδιαφερόμενους, ενώ, σε ακραίες περιπτώσεις, πλάνα αντιμετώπισης καταστροφών αξιοποιούνται για την επίλυση των προβλημάτων και τη συνέχιση της παροχής της υπηρεσίας, με τη συνεργασία του γραφείου εξυπηρέτησης, τμημάτων τεχνικής υποστήριξης και εξωτερικών συνεργατών.

Τα προϊόντα και υπηρεσίες που χρησιμοποιούνται από τον οργανισμό απαιτούν την ύπαρξη συμφωνιών υποστήριξης γύρω από τις υποχρεώσεις του προμηθευτή ως προς τον οργανισμό και του οργανισμού ως προς τους πελάτες του. Συνεπώς, απαιτείται συχνή επικοινωνία μεταξύ του οργανισμού και των προμηθευτών στα πλαίσια των πρακτικών διαχείρισης συμβάντων. Ανάλογα με τις συμφωνίες, ο προμηθευτής καλείται συχνά να αντικαταστήσει ή συμπληρώσει τη δράση αντίστοιχων τμημάτων του οργανισμού και να συνεργαστεί με ειδικούς, εφόσον αυτό απαιτηθεί.

Ακόμη, κρίνεται απαραίτητο να υπάρχουν επίσημες διαδικασίες καταγραφής και διαχείρισης των συμβάντων, χωρίς απαραίτητα λεπτομέρειες ανά περίπτωση, οι οποίες παρέχουν τεχνικές για πιο αποδοτική διάγνωση και αντιμετώπιση. Οι συγκεκριμένες διαδικασίες αφορούν κάθε τμήμα της αλυσίδας αξίας, συχνά ωστόσο επικεντρώνονται στις επιχειρησιακές λειτουργίες.

Διαχείριση συνέχισης των υπηρεσιών

Στόχος των πρακτικών συνέχισης των υπηρεσιών είναι η διασφάλιση της διαθεσιμότητας και της απόδοσης της υπηρεσίας σε ικανοποιητικά επίπεδα σε περίπτωση κρίσεων. Παρέχουν ένα πλαίσιο για την ενσωμάτωση ελαστικότητας στις διαδικασίες του οργανισμού και παροχής ικανοποιητικής αντίδρασης η οποία προστατεύει τα συμφέροντα των ενδιαφερομένων και την εικόνα του οργανισμού σε περιπτώσεις καταστροφών.

Η διαχείριση της συνέχισης των υπηρεσιών υποστηρίζει γενικότερα τις διαδικασίες σχεδιασμού, διασφαλίζοντας ότι οι υπηρεσίες μπορούν να συνεχιστούν μέσα στο απαιτούμενο και προσυμφωνημένο χρονοδιάγραμμα μετά από κάποια σημαντική καταστροφή η κρίση. Ενεργοποιείται όταν η διακοπή μιας υπηρεσίας ή ένα οργανωτικό ρίσκο είναι σημαντικότερο από την ικανότητα του οργανισμού να το αντιμετωπίσει με τις συνηθισμένες πρακτικές της διαχείρισης συμβάντων. Ένα τέτοιο συμβάν χαρακτηρίζεται ως καταστροφή, με βάση το πλαίσιο λειτουργίας του κάθε οργανισμού, τόσο συνολικά όσο και ανά υπηρεσία, σύμφωνα με προηγούμενη ανάλυση επιχειρηματικών επιπτώσεων.

Οι αιτίες ενεργοποίησης του συγκεκριμένου μηχανισμού, όπως, επίσης, ο αριθμός των εμπλεκομένων ατόμων και ομάδων και ο βαθμός των επιπτώσεων είναι διαφορετικός ανά οργανισμό. Σε κάθε, όμως, περίπτωση, οι συγκεκριμένες πρακτικές πρέπει να είναι διεξοδικές, προσεκτικά σχεδιασμένες και δοκιμασμένες, δεδομένης της κρισιμότητας των καταστάσεων που αφορούν.

Στα σημαντικά μεγέθη που οι εταιρείες πρέπει να προσδιορίσουν περιλαμβάνονται ο στόχος χρόνου αποκατάστασης (recovery time objective) - το μέγιστο αποδεκτό χρονικό διάστημα μετά την διακοπή μιας υπηρεσίας, μέχρι αυτή η διακοπή να επηρεάσει σημαντικά τον οργανισμό - και ο στόχος σημείου αποκατάστασης (recovery point objective) - το σημείο στο οποίο η πληροφορία

μιας ενέργειας πρέπει να αποκατασταθεί, ώστε να συνεχιστεί ομαλά η επιχειρηματική διαδικασία. Σημειώνεται η κρισιμότητα της ανάλυσης επιχειρηματικών επιπτώσεων, δηλαδή του εντοπισμού ζωτικών επιχειρηματικών λειτουργιών και των εξαρτήσεων τους.

Συγκριτικά με την διαχείριση συμβάντων, η διαχείριση συνέχισης των υπηρεσιών επικεντρώνεται σε γεγονότα, τα οποία ο οργανισμός θεωρεί αρκετά σημαντικά ώστε να χαρακτηριστούν καταστροφές, αφήνοντας γεγονότα μικρότερης κρισιμότητας να τα διαχειριστούν οι διαδικασίες αντιμετώπισης συμβάντων. Για την ομαλή λειτουργία και συνύπαρξη των συγκεκριμένων διαδικασιών κρίνεται αναγκαίο να προσδιοριστούν και προσυμφωνηθούν με ακρίβεια τα όρια ενεργοποίησης του κάθε μηχανισμού, ώστε να εξαλειφθούν προβλήματα, καθυστερήσεις και κίνδυνοι.

Δεδομένης της όλο και σημαντικότερης τεχνολογικής εξάρτησης των οργανισμών, λύσεις υψηλής διαθεσιμότητας κρίνονται κρίσιμες για την ανταγωνιστικότητα του οργανισμού και απαιτούν προσεκτικό συνδυασμό επιχειρηματικού σχεδιασμού, τεχνικών αρχιτεκτονικών ανοχής και διαδικασιών διαχείρισης συμβάντων και προβλημάτων.

3.3: Το πλαίσιο COBIT

Το πλαίσιο COBIT (Control Objectives for Information and Related Technologies) αποτελεί μια διαδεδομένη επιλογή για την διοίκηση πληροφοριακών συστημάτων (ISACA, 2018). Προσδιορίζει γενικές διαδικασίες διοίκησης και διαχείρισης, με συγκεκριμένες εισόδους και εξόδους, κύριες ενέργειες, στόχους, μεγέθη μέτρησης της απόδοσης και ένα μοντέλο ωριμότητας. Αποδέχεται ότι τα πληροφοριακά συστήματα υποβοηθούν όλους τους τομείς και ότι η πληροφορία επηρεάζει το σύνολο του οργανισμού και τη λειτουργία του.

Το συγκεκριμένο πλαίσιο δημιουργήθηκε και συντηρείται από τον διεθνή επαγγελματικό συνεταιρισμό ISACA.

Το πρότυπο προωθεί ακριβή διάκριση της διοίκησης από τη διαχείριση. Η πρώτη διασφαλίζει ότι αξιολογούνται οι ανάγκες, συνθήκες και επιλογές των ενδιαφερόμενων μερών, ότι η κατεύθυνση του οργανισμού ορίζεται μέσα από τις διαδικασίες θέσης προτεραιοτήτων και λήψης αποφάσεων και ότι η απόδοση και συμμόρφωση επιτηρούνται με βάση συμφωνημένους στόχους. Η δεύτερη σχεδιάζει, διαμορφώνει, πραγματοποιεί και επιτηρεί ενέργειες που ευθυγραμμίζονται με την κατεύθυνση της διοίκησης προς επίτευξη των επιχειρηματικών στόχων. Για τη συνεισφορά της τεχνολογίας και της πληροφορίας στην επίτευξη των στόχων του οργανισμού, απαιτείται η ταυτόχρονη επίτευξη συγκεκριμένων στόχων διοίκησης και διαχείρισης.

Αρχές διοίκησης

Ως απαραίτητα στοιχεία ενός συστήματος διοίκησης προσδιορίζονται οι διαδικασίες, οι οργανωτικές δομές, οι πολιτικές, η ροή της πληροφορίας, η κουλτούρα και οι συμπεριφορές, οι ικανότητες και οι υποδομές. Οι κύριες αρχές του συγκεκριμένου προτύπου κατηγοριοποιούνται στις αρχές που περιγράφουν τις τεχνολογικές και πληροφοριακές απαιτήσεις του συστήματος διοίκησης και στις αρχές του πλαισίου διοίκησης που χρησιμοποιούνται για τη δημιουργία του συστήματος αυτού.

Διάγραμμα 14 - Οι αρχές ενός συστήματος διοίκησης, κατά το πρότυπο COBIT (ISACA, 2018)

Οι έξη αρχές ενός συστήματος διοίκησης, με βάση το πρότυπο, είναι οι εξής:

- Κάθε οργανισμός χρειάζεται ένα σύστημα διοίκησης και στρατηγική για να ικανοποιεί τις ανάγκες των ενδιαφερόμενων μερών και να παράγει αξία από τη χρήση πληροφοριακών συστημάτων, η οποία αναφέρεται στην ισορροπία μεταξύ οφελών, ρίσκου και πόρων

- Ένα σύστημα διοίκησης για πληροφοριακά συστήματα αποτελείται από διακριτά τμήματα διαφορετικών τύπων, τα οποία συνεργάζονται ολιστικά

- Ένα σύστημα διοίκησης πρέπει να είναι δυναμικό και να μελετάται το αντίκτυπο κάθε αλλαγής, με στόχο τη βιωσιμότητα του συστήματος

- Ένα σύστημα διοίκησης πρέπει να διακρίνει ξεκάθαρα μεταξύ διοικητικών και οργανωτικών ενεργειών και δομών

- Ένα σύστημα διοίκησης πρέπει να ανταποκρίνεται στις ανάγκες του οργανισμού, χρησιμοποιώντας κάποιους σχεδιαστικούς παράγοντες ως βάση για τη παραμετροποίηση των τμημάτων του

- Ένα σύστημα διοίκησης πρέπει να καλύπτει ολοκληρωτικά τον οργανισμό και όλη την επεξεργασία που πληροφορίας που πραγματοποιείται για την επίτευξη τον στόχων του, ανεξαρτήτως του που συμβαίνει αυτό.

Οι τρεις αρχές ενός πλαισίου διοίκησης, με βάση το πρότυπο, είναι οι εξής:

- Ένα πλαίσιο διοίκησης πρέπει να βασίζεται σε ένα εννοιολογικό μοντέλο των κύριων τμημάτων του και της αλληλεπίδρασής τους, με στόχο τη μεγιστοποίηση της συνέπειας και την προώθηση της αυτοματοποίησης

- Ένα πλαίσιο διοίκησης πρέπει να είναι ανοιχτό και ευέλικτο, επιτρέποντας την πρόσθεση νέου περιεχομένου και την επίλυση νέων προβλημάτων, παραμένοντας ακέραιο και συνεπές

- Ένα πλαίσιο διοίκησης πρέπει να συμβαδίζει με σημαντικά σχετικά πρότυπα, πλαίσια και κανονισμούς

Στόχοι

Με βάση το πρότυπο, οι στόχοι διοίκησης ομαδοποιούνται στο πεδίο της αξιολόγησης, διεύθυνσης και επιτήρησης, το οποίο ασχολείται με τη σύγκριση των διαθέσιμων στρατηγικών επιλογών, την κατεύθυνση της ηγεσίας και την επιτυχία της κάθε στρατηγικής.

Οι στόχοι διαχείρισης κατηγοριοποιούνται σε τέσσερα πεδία. Αυτά, περιλαμβάνουν το πεδίο ευθυγράμμισης, σχεδίασης και οργάνωσης, το οποίο αναφέρεται στο συνολικότερο οργανισμό και τη στρατηγική και υποστήριξη των τεχνολογιών πληροφορικής, το πεδίο δημιουργίας, απόκτησης και εφαρμογής, το οποίο απασχολείται με τις επιμέρους λύσεις πληροφορικής και την ενσωμάτωσή τους στις διαδικασίες, το πεδίο παράδοσης, υπηρεσιών και υποστήριξης, το οποίο υποβοηθά τις υπηρεσίες πληροφορικής και το πεδίο επίβλεψης και αξιολόγησης, το οποίο παρακολουθεί την απόδοση των διαδικασιών και τη συμμόρφωση με τους στόχους και τις εξωτερικές απαιτήσεις.

Οι ανάγκες των ενδιαφερόμενων μερών πρέπει να μετασχηματιστούν σε στρατηγική και η αλληλουχία στόχων συνδέει την προτεραιότητα των διαχειριστικών στόχων με τους γενικότερους στόχους του οργανισμού. Ξεκινώντας από τα ενδιαφερόμενα μέλη και τις ανάγκες τους, συναντώνται οι στόχοι του οργανισμού, η στόχοι ευθυγράμμισης και τέλος, οι επιμέρους στόχοι διοίκησης και διαχείρισης.

Οι στόχοι που περιλαμβάνονται στο συγκεκριμένο μοντέλο χαρακτηρίζονται ως ίσης προτεραιότητας και σημειώνεται ότι οι σχεδιαστικοί παράγοντες, οι οποίοι επηρεάζουν πρακτικά τη σημασία τους και τους αντίστοιχους στόχους επιπέδων δυνατοτήτων, είναι διαφορετικοί σε κάθε οργανισμό.

Πλαίσια ενεργειών

Παράλληλα, σημειώνεται η σημασία των επιμέρους μερών, τα οποία αλληλοεπιδρούν και ατομικά και συλλογικά συντελούν στην ορθή λειτουργία

του συστήματος διοίκησης. Οι διαδικασίες περιγράφουν οργανωμένες πρακτικές και δραστηριότητες προς επίτευξη συγκεκριμένων στόχων και παραγωγή επιθυμεί των εξόδων προς υποστήριξη των πληροφοριακών συστημάτων. Οι οργανωτικές δομές αναφέρονται σε συγκρίσιμες οντότητες λήψης αποφάσεων στο εσωτερικό του οργανισμού. Οι αρχές, πολιτικές και τα πλαίσια αφορούν πρακτικές οδηγίες για την καθημερινή διαχείριση.

Η κουλτούρα και η συμπεριφορά των ατόμων συντελεί σημαντικά στην επιτυχία των ενεργειών διοίκησης και διαχείρισης. Τα άτομα και οι ικανότητές τους είναι απαραίτητα για τη λήψη ορθών αποφάσεων, την εκτέλεση διορθωτικών ενεργειών και την επιτυχημένη ολοκλήρωση των δραστηριοτήτων. Υπηρεσίες, υποδομές και εφαρμογές παρέχουν στον οργανισμό το σύστημα διοίκησης και επεξεργασίας πληροφοριών.

Οι παράγοντες σχεδιασμού, ο οποίοι επηρεάζουν την σχεδίαση και την επιτυχία του συστήματος διοίκησης, περιλαμβάνουν τη στρατηγική του οργανισμού, τους στόχους που την υποστηρίζουν, το δεδομένο προφίλ ρίσκου, ζητήματα πληροφοριακών συστημάτων, το περιβάλλον απειλών, τις απαιτήσεις συμμόρφωσης, το μοντέλο και ρόλο της τεχνολογίας, την στρατηγική υιοθέτησης τεχνολογιών και το μέγεθος του οργανισμού.

Διαχείριση της απόδοσης

Η διαχείριση της απόδοσης και κρίνεται σημαντικό μέρος του συστήματος διοίκησης και διαχείρισης. Αναφέρεται στη λειτουργία των συστημάτων αυτών και των μερών τους και στη βελτίωση τους για την επίτευξη των επιθυμητών αποτελεσμάτων. Οι ενέργειες αυτές πρέπει να είναι απλές, κατανοητές και συνεπείς, να επιτρέπουν τη διαχείριση της απόδοσης όλων των μερών των συστημάτων, να παρεξηγούν βάσιμες επαναλαμβανόμενες και σχετικές μετρήσεις και να υποστηρίζουν διαφορετικές απαιτήσεις, προτεραιότητες και είδη αξιολογήσεων.

Με βάση το μοντέλο που προωθείται από το πρότυπο, οι ενέργειες των διαδικασιών σχετίζονται με συγκεκριμένα επίπεδα δυνατοτήτων και επίπεδα ωριμότητας ανάλογα με τους τομείς στους οποίους επικεντρώνονται. Το επίπεδο δυνατοτήτων εκφράζει την ποιότητα της εφαρμογής και λειτουργίας της διαδικασίας. Αντίστοιχα, το επίπεδο ωριμότητας σχετίζεται με την απόδοση σε ολόκληρους τομείς και ομάδες διαδικασιών, οι οποίες λειτουργούν σε συγκεκριμένο επίπεδο δυνατοτήτων.

Εφαρμογή

Στην εφαρμογή του προτύπου διακρίνονται επτά φάσεις:

- Ταυτοποίηση των οδηγών αλλαγής και σκιαγράφηση της επιθυμίας της ηγεσίας για αλλαγές, στα πλαίσια της κάθε περίστασης. Ως οδηγοί αλλαγής χαρακτηρίζονται εσωτερικά και εξωτερικά γεγονότα, καταστάσεις και προβλήματα, τα οποία δημιουργούν την ανάγκη για αλλαγή. Τα σχετικά ρίσκα πρέπει να εντοπίζονται και διαχειρίζονται σε όλη τη διάρκεια του κύκλου ζωής, ενώ η προετοιμασία, διατήρηση και παρακολούθηση της κάθε περίπτωσης είναι απαραίτητες για τη δικαιολόγηση, υποστήριξη και επιτυχημένη έκβαση κάθε πρωτοβουλίας.

- Ευθυγράμμιση στόχων πληροφορικής με τις στρατηγικές και το ρίσκο του οργανισμού, με βάση την προτεραιότητα της κάθε περίπτωσης. Ο οργανισμός πρέπει να ταυτοποιήσει κρίσιμους στόχους και διαδικασίες με αρκετές δυνατότητες ώστε να εξασφαλίσουν επιτυχημένα αποτελέσματα, αναγνωρίζοντας τυχόν ελλείψεις, αξιοποιώντας αναλύσεις δυνατοτήτων των διαδικασιών.

- Θέση στόχων βελτίωσης και διεξαγωγή αναλύσεων για τον εντοπισμό πιθανών λύσεων, διαμερισμένων σε διαχειρίσιμα τμήματα, με προτεραιότητα στις ευκολότερες και αποτελεσματικότερες ενέργειες.

- Σχεδιασμός εφικτών και πρακτικών λύσεων δικαιολογώντας τα πλάνα και τις αλλαγές.

- Εφαρμογή των προτεινόμενων λύσεων μέσω καθημερινών πρακτικών και εφαρμογή μέτρων και συστημάτων παρακολούθησης για την εξασφάλιση της επιχειρηματικής ευθυγράμμισης και μέτρηση της απόδοσης. Προώθηση της ενασχόλησης επικοινωνίας κατανοήσεις και ιδιοκτησίας των διαδικασιών από τους υπεύθυνους.

- Βιώσιμη ενσωμάτωση και μετάβαση από τις βελτιωμένες πρακτικές διοίκησης και διαχείρισης σε φυσιολογικές επιχειρηματικές λειτουργίες. Αξιοποίηση μετρήσεων απόδοσης για τον προσδιορισμό της επιτυχίας και των οφελών.

- Αξιολόγηση της συνολικότερης επιτυχίας του εγχειρήματος ταυτοποίηση περαιτέρω απαιτήσεων και συνεχής βελτίωση.

3.4: Το μοντέλο O-ISM3

Το μοντέλο O-ISM3 (Open Information Security Maturity Model) αποτελεί ένα διαδεδομένο πλαίσιο διαχείρισης της ασφάλειας πληροφοριών, το οποίο προωθεί την ύπαρξη κατάλληλων διαδικασιών ασφαλείας σε έναν οργανισμό, οι οποίες εξασφαλίζουν ένα σταθερό επίπεδο κάλυψης των επιχειρηματικών του αναγκών (The Open Group, 2017). Επικεντρώνεται στην θεσμοθέτηση ελέγχων ασφαλείας στα πλαίσια κάθε επιχειρηματικής διαδικασίας ως αναπόσπαστο μέρος τους, με σημαντικό θετικό αντίκτυπο για τις περιστάσεις της πλειονότητας των οργανισμών, αλλά διαχειρίσιμο αριθμό. Λαμβάνοντας υπόψη τις διαφορετικές ανάγκες και ανοχή ρίσκου κάθε οργανισμού, τονίζεται ο ιδιαίτερα σημαντικός ρόλος του υπεύθυνου διαχείρισης ασφάλειας πληροφοριών, στην αξιολόγηση του ρίσκου του περιβάλλοντος και στο

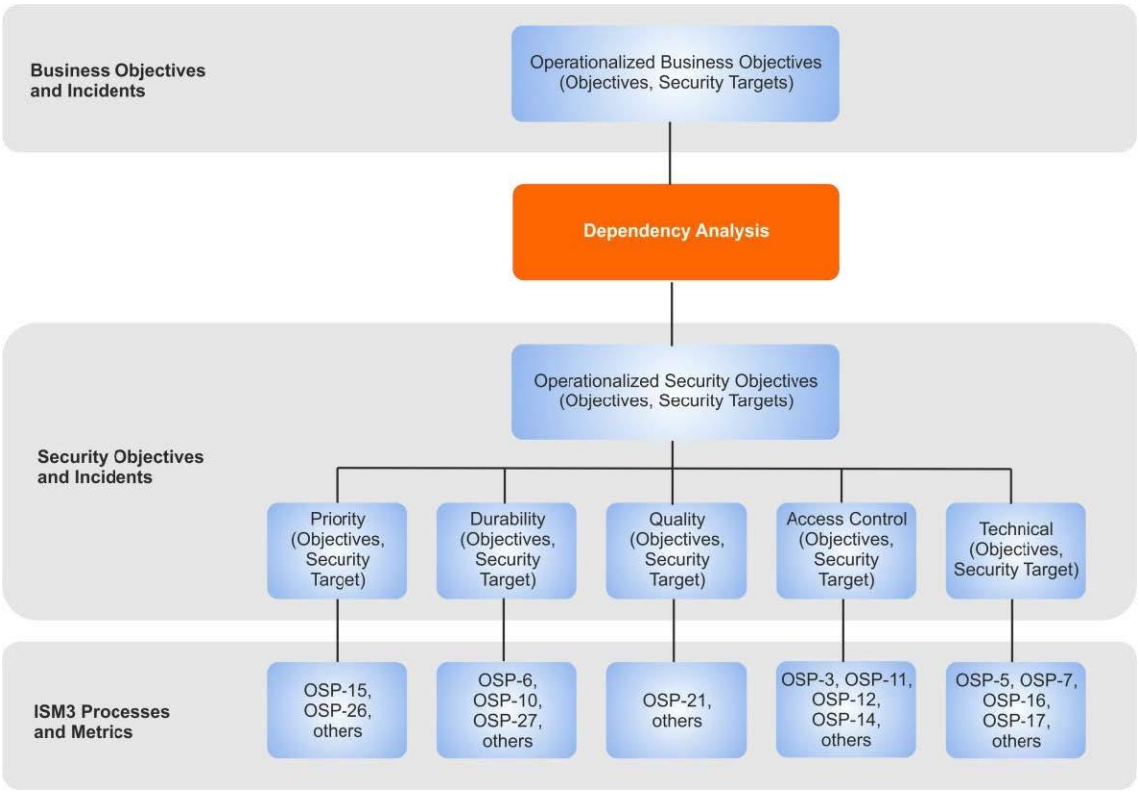
σχεδιασμό των διαδικασιών με συνεπή και οικονομικά αποδοτικό τρόπο. Στο μοντέλο περιλαμβάνονται πλήθος από παραδείγματα ανά κατηγορία περιστάσεων με ενδεικτικές εφαρμογές.

Το πρότυπο απαιτεί οι διαδικασίες ασφαλείας του οργανισμού να είναι σαφείς, καταγεγραμμένες, μετρήσιμες και διαχειρίσιμες και οι στόχοι ασφαλείας να εξάγονται με βάση την επιχειρηματική στοχοθεσία. Παράλληλα, επισημαίνει τη σημασία της χρήσης κατάλληλων λειτουργικών μετρήσεων και της αποδεκτής τους μεταβλητότητας, για την ορθότερη εξαγωγή συμπερασμάτων και λήψη επιχειρηματικών αποφάσεων, ιδιαίτερα γύρω από την κατανομή πόρων ασφαλείας, την απόδοση κάθε διαδικασίας και την αντίδραση στις αλλαγές του περιβάλλοντος. Ως απώτερος στόχος ορίζεται η μείωση του ρίσκου και η βελτιστοποίηση της απόδοσης των επενδύσεων. Στα πλαίσια του μοντέλου, χρησιμοποιούνται υποβοηθητικά οι έννοιες της ωριμότητας της λειτουργίας των κρίσιμων διαδικασιών ασφαλείας και των δυνατοτήτων της κάθε διαδικασίας.

Ο φορέας που διαμορφώνει και επιβλέπει το πλαίσιο είναι η κοινοπραξία The Open Group.

Η λειτουργική προσέγγιση του μοντέλου

Με τη χρήση μεταβλητών, λειτουργικών προσδιορισμών στη θέση εννοιολογικών όρων γύρω από την ασφάλεια των πληροφοριών, προωθείται η κατανόηση και συμφωνία μεταξύ της διοίκησης και των υπεύθυνων ασφαλείας των σχετικών στόχων, των μετρήσεών τους και της εύρεσης και ανακοίνωσης των αποτυχιών. Με βάση αυτή τη λειτουργική προσέγγιση, ως συμβάν ορίζεται η αποτυχία επίτευξης ενός ή περισσότερων επιχειρηματικών στόχων και στόχων ασφαλείας. Αντίθετα, ως ασφάλεια ορίζεται το αποτέλεσμα της συνεχούς κάλυψης ή υπέρβασης των στόχων αυτών και η επίτευξή της αναφέρεται στη συνεπή λειτουργία, παρά τα πιθανά ατυχήματα, επιθέσεις ή λάθη.



Διάγραμμα 15 - Το μοντέλο ασφάλειας που προωθείται από το πρότυπο O-ISM3 (The Open Group, 2017)

Στοχοθεσία

Στα πλαίσια του προτύπου, η σημασία της ασφάλειας των πληροφοριών στην επίτευξη των επιχειρηματικών στόχων παρουσιάζεται μέσω μιας ανάλυσης εξαρτήσεων, η οποία παράγει μια λίστα από στόχους ασφαλείας, στους οποίους βασίζεται το σύστημα. Οι στόχοι ασφαλείας κατηγοριοποιούνται σε στόχους προτεραιότητας, οι οποίοι προσδιορίζουν την έννοια της διαθεσιμότητας για τον εκάστοτε οργανισμό, στόχους αντοχής, οι οποίοι αναφέρονται στην ακεραιότητα, διατήρηση και καταστροφή της πληροφορίας, με βάση τις πολιτικές και τη στοχοθεσία, στόχους ποιότητας πληροφοριών, οι οποίοι περιλαμβάνουν την ακρίβεια, τη σχετικότητα, την πληρότητα και συνέπεια των αποθετηρίων, στόχους ελέγχου της πρόσβασης, οι οποίοι ασχολούνται με την εμπιστευτικότητα της προστατευόμενης πληροφορίας και τεχνικούς στόχους ασφαλείας, οι οποίοι αναφέρονται στην αρχιτεκτονική των πληροφοριακών συστημάτων.

Παράλληλα με τους στόχους, ορίζονται αποδεκτές αποκλίσεις από το επιθυμητό αποτέλεσμα, πριν την ενεργοποίηση των μηχανισμών αποκατάστασης, ανάλογα με την κρισιμότητα του κάθε στόχου, προσδιορίζονται από τη μέγιστη συχνότητα και το οριακό τους κόστος και συντελούν στην όρεξη ρίσκου του οργανισμού. Τα τελευταία αλλάζουν, ανάλογα με τον τομέα, την τοποθεσία, τις συγκεκριμένες απαιτήσεις ασφαλείας, τις δομές κόστους και τη χρήση της τεχνολογίας από τον κάθε οργανισμό.

Χαρακτηρισμός διαδικασιών

Το επίπεδο δυνατοτήτων μιας διαδικασίας ορίζεται ως ιδιότητα του τρόπου διαχείρισής της. Υψηλό επίπεδο δυνατοτήτων συνεπάγεται μεγαλύτερο πλήθος εφαρμόσιμων πρακτικών διαχείρισης, μεγαλύτερη σταθερότητα, διαφάνεια και δυνατότητα αυτο-διόρθωσης της διαδικασίας.

Ως επίπεδο ωριμότητας ορίζεται ένας δεδομένος συνδυασμός διαδικασιών σε δεδομένα επίπεδα δυνατοτήτων. Περισσότερες διαδικασίες σε υψηλότερα επίπεδα δυνατοτήτων συνεπάγονται υψηλότερο επίπεδο ωριμότητας. Ανάλογα με το μέγεθος, τους πόρους, τις απειλές, τις επιπτώσεις, την ανοχή ρίσκου και τον τομέα των δραστηριοτήτων ενός οργανισμού απαιτείται και διαφορετικό επίπεδο ωριμότητας.

Ιεραρχικά επίπεδα διαδικασιών

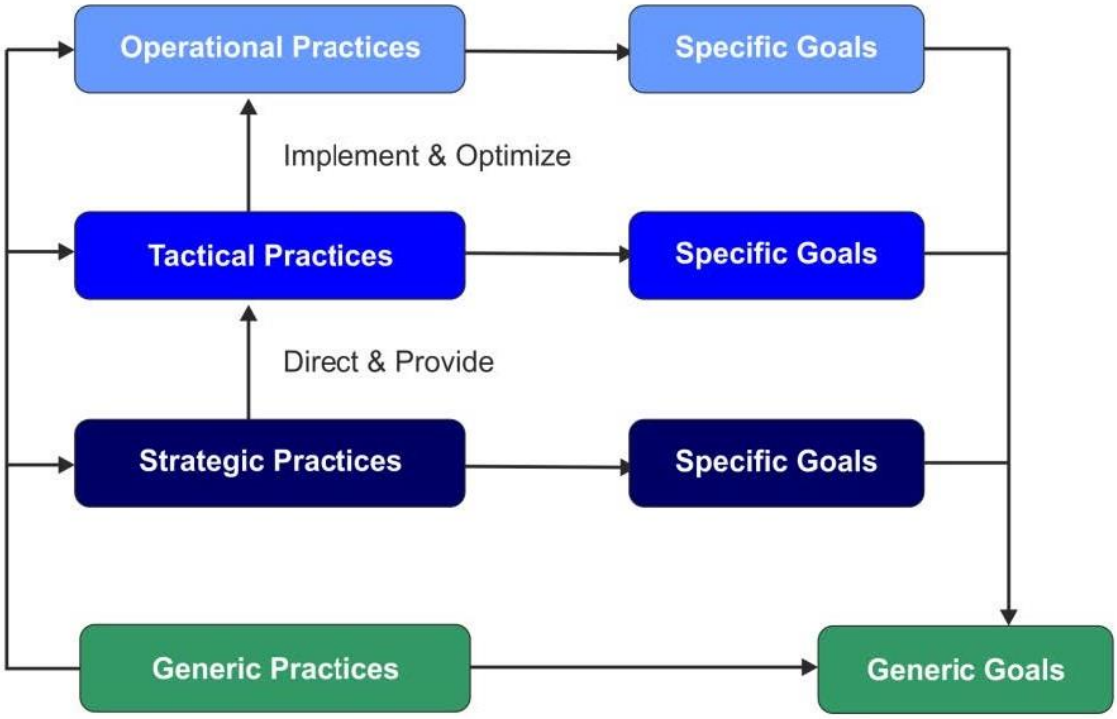
Το μοντέλο ορίζει διαφορετικά ιεραρχικά επίπεδα και διαδικασίες διαχείρισης ασφαλείας. Από τα υψηλότερα ιεραρχικά επίπεδα, διακρίνονται το στρατηγικό επίπεδο, το οποίο αναφέρεται σε γενικότερους στόχους, στον συντονισμό και στην κατανομή των πόρων, το τακτικό επίπεδο, το οποίο αναφέρεται στο σχεδιασμό και στην υλοποίηση του συστήματος διαχείρισης της ασφάλειας πληροφοριών και συγκεκριμένους στόχους του, το λειτουργικό επίπεδο, το οποίο ασχολείται με την επίτευξη των στόχων μέσω τεχνικών διαδικασιών και το γενικό επίπεδο, για γενικότερες διαδικασίες διαχείρισης.

Αντίστοιχα, οι στρατηγικές διαδικασίες αναφέρονται στην επιλογή και σχεδίαση υπηρεσιών, οι οποίες παρέχουν αξία στα δεδομένα πλαίσια κόστους και ρίσκου. Η στρατηγική διαχείριση είναι υπεύθυνη για την αξιοποίηση των πόρων μέσω συμφωνιών διακυβέρνησης και αναφέρεται σε ενδιαφερόμενα μέρη στο εσωτερικό και εξωτερικό του οργανισμού. Διαδραματίζει συντονιστικό ρόλο στη φυσική ασφάλεια, την ασφάλεια της πληροφορίας και στην αλληλεπίδραση των οργανωτικών μονάδων, επαληθεύει, βελτιώνει και κατανέμει πόρους στο σύστημα διαχείρισης της ασφάλειας των πληροφοριών, προσδιορίζει τις σχέσεις με άλλους συνεργάτες και τις αναθέσεις εργασιών και ορίζει στόχους ασφαλείας.

Οι γενικές διαδικασίες προσφέρουν απαραίτητα μέσα για την υλοποίηση, αξιολόγηση και βελτίωση των διαδικασιών του συστήματος, αποτελούμενες από τη διαχείριση γνώσης για τη συγκέντρωση και διαμοιρασμό πληροφορίας διαχείρισης της ασφάλειας, τους ελέγχους συμμόρφωσης με τις πολιτικές και τους κανονισμούς και το σχεδιασμό και εξέλιξη των διαδικασιών για καλύτερη επίτευξη των στόχων που έχουν τεθεί.

Οι τακτικές διαδικασίες ασχολούνται με την γενικότερη απόδοση του συστήματος. Συντελούν στη παροχή αναπληροφόρησης στη στρατηγική διοίκηση, στη διαχείριση των διαθέσιμων πόρων και στον προσδιορισμό του περιβάλλοντος για την λειτουργική διοίκηση.

Οι λειτουργικές διαδικασίες σκοπεύουν στη παροχή αναπληροφόρησης στη τακτική διοίκηση, γύρω από αναφορές συμβάντων και μετρήσεων, προμηθεύονται και εφαρμόζουν αποδοτικά τους πόρους που τους έχουν ανατεθεί, ταυτοποιούν, προστατεύουν και υποστηρίζουν τα σημαντικά στοιχεία των πληροφοριακών συστημάτων, διαχειρίζονται την πρόσβαση και τους περιβαλλοντικούς ελέγχους των χρηστών και των υπηρεσιών, τη διαθεσιμότητα, τον έλεγχο και την επίβλεψη των μέτρων ασφαλείας και ασχολούνται με την πρόληψη, εντοπισμό και μετρίαση των συμβάντων ασφαλείας.



Διάγραμμα 16 - Τα ιεραρχικά επίπεδα των διαδικασιών, σύμφωνα με το πρότυπο O-ISM3 (The Open Group, 2017)

Αξιολόγηση διαδικασιών

Οι διαδικασίες που πρέπει να επιλέξει ένας οργανισμός κατά την εφαρμογή του προτύπου, η συχνότητα και η δυνατότητές τους εξαρτώνται από τις πολιτικές ασφαλείας που έχουν οριστεί, τους διαθέσιμους πόρους, το περιβάλλον στο οποίο λειτουργεί και τους επιχειρηματικούς στόχους. Χαρακτηριστικά μεγέθη ανά διαδικασία είναι το υπεύθυνο επίπεδο του οργανισμού, η προστιθέμενη αξία που παρέχει και οι πρωταρχικές και δευτερεύουσες είσοδοι και έξοδοί της. Κάθε διαδικασία απαιτείται να έχει σαφώς ορισμένο υπεύθυνο για τη λειτουργία και συντήρησή της και μετρούμενα μεγέθη για την αξιολόγηση της επιτυχίας και απόδοσής της. Ο υπεύθυνος πρέπει να είναι προσωπικά επενδυμένος στην επιτυχία της, ικανός, κινητοποιημένος και εξουσιοδοτημένος. Στην κατανομή των καθηκόντων πρέπει να υπάρχει διαφάνεια, δίκαιη διαμέριση, επίβλεψη,

εναλλαγή και διαχωρισμός δραστηριοτήτων προς αποφυγή συγκρούσεων συμφερόντων και συγκάλυψης μη εξουσιοδοτημένης συμπεριφοράς.

Για την αύξηση της προστιθέμενης αξίας μίας διαδικασίας είναι χρήσιμη η συγκέντρωση, ερμηνεία και σύγκριση μετρήσεων ενδιαφέροντος γύρω από τη συνέπεια, απόδοση και κόστος των τελευταίων, καθώς βελτίωσή τους συνεπάγεται αύξηση και της προστιθέμενης αξίας. Η διοίκηση πρέπει να προσδιορίσει ποιες μετρήσεις έχει νόημα να πραγματοποιηθούν, δεδομένου του κόστους κάθε πληροφορίας.

Με βάση το πρότυπο, οι μετρήσεις ενεργειών ορίζονται ως ο αριθμός των παραδοτέων εισόδων και εξόδων μιας διαδικασίας στη μονάδα του χρόνου - ανάλογα με τη διαδικασία, αύξηση του αριθμού των ενεργειών, της συχνότητας ή της ταχύτητας της διαδικασίας οδηγεί σε αυξημένη αξία. Οι μετρήσεις πεδίου αφορούν τον αριθμό των παραδοτέων εισόδων της διαδικασίας ως προς όλες τις δυνατές εισόδους – αύξηση της ευρύτητας μιας διαδικασίας μπορεί να επηρεάσει ανάλογα και την αξία της. Οι μετρήσεις αποτελεσματικότητας συγκρίνουν τον αριθμό των παραδοτέων εισόδων ως προς τις εξόδους – περισσότερες έξοδοι ανά είσοδο υποδεικνύουν δυνητική αύξηση της αξίας της διαδικασίας. Οι μετρήσεις φορτίου αναφέρονται στους πόρους που αποδίδονται σε κάθε διαδικασία σε σχέση με αυτούς που πραγματικά χρησιμοποιούνται – χαμηλό φορτίο σημαίνει ότι πόροι μπορούν να διατεθούν αλλού. Τέλος, οι μετρήσεις αποδοτικότητας συγκρίνουν τις εξόδους τις διαδικασίας με τους πόρους που τις έχουν διατεθεί σε ένα δεδομένο χρονικό διάστημα - υψηλή αξιοποίηση των πόρων υποδηλώνει και υψηλή αξία. Οι προαναφερθείσες μετρήσεις μπορούν να χαρακτηριστούν ως μετρήσεις ποιότητας, αν συγκρίνουν την καταλληλότητα της κάθε διαδικασίας για το δεδομένο στόχο της.

Σημειώνεται ότι υπάρχουν πρακτικά όρια στη βελτίωση των μετρήσεων, όπως, επίσης, ότι οι μετρήσεις δεν έχουν νόημα ή αξία εν κενώ, αλλά στα πλαίσια των απαιτήσεων κάθε μίας και με βάση τις συμφωνίες των ενδιαφερόμενων μερών, οι οποίες προτείνεται να υπάρχουν. Η φύση, ακρίβεια και συχνότητα των

μετρήσεων κρίνεται στα πλαίσια του κάθε οργανισμού, ενώ η χρήση τους περιλαμβάνει τα στάδια της πραγματοποίησης, της συγκέντρωσης, της ερμηνείας, της έρευνας, της απεικόνισης, της αποθήκευσης και της δράσης που ενεργοποιούν.

Προσεγγίσεις εφαρμογής του προτύπου

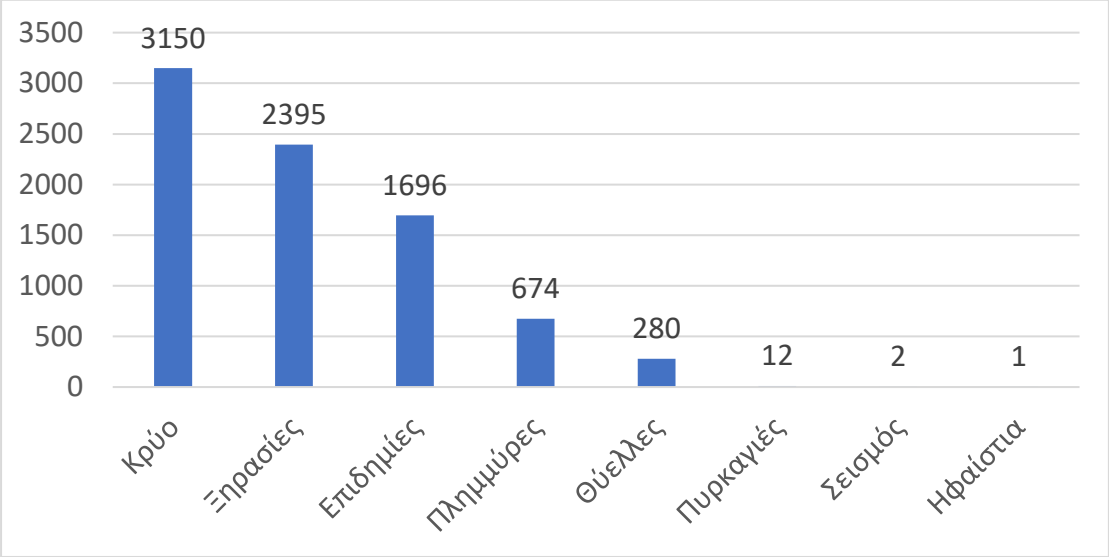
Όσον αφορά την εφαρμογή του προτύπου, εντοπίζονται οι δύο αντίθετες προσεγγίσεις της από-πάνω-προς-τα-κάτω και από-κάτω-προς-τα-πάνω εφαρμογής. Στην πρώτη περίπτωση, τα ανώτερα επίπεδα διοίκησης αποφασίζουν την εφαρμογή του προτύπου και διανέμουν τους απαραίτητους πόρους, αναθέτοντας στους υπεύθυνους ασφάλειας πληροφοριών την επίτευξη των στόχων ασφαλείας που ζητούνται και με την μεταξύ τους συνεργασία. Στην δεύτερη περίπτωση, κάποιοι υπεύθυνοι ασφάλειας πληροφοριών αποφασίζουν να αξιοποιήσουν υπάρχοντες πόρους για την πιλοτική εφαρμογή του προτύπου, στοχεύοντας στη καλύτερη διαχείριση της ασφάλειας των πληροφοριών και στην αύξηση της απόδοσης των επενδύσεων πόρων του τομέα τους, επιδεικνύοντας την αξία της συγκεκριμένης εφαρμογής.

Κεφάλαιο 4: Σοβαρές καταστροφές και αντιμετώπιση

Στοχεύοντας στην προστασία από τις επιπτώσεις κάθε ρίσκου που τους επηρεάζει, οι οργανισμοί πραγματοποιούν τακτικά αναλύσεις, οι οποίες ταυτοποιούν, ταξινομούν ανά προτεραιότητα και προετοιμάζουν την αντίδραση στους εντοπιζόμενους κινδύνους, ανάλογα με τις περιστάσεις, την πιθανότητά τους να παρουσιαστούν και το δυνητικό τους αντίκτυπο. Καταστροφές, όπως οι προαναφερθείσες, παρουσιάζουν μέγιστες επιπτώσεις αλλά χαμηλή πιθανότητα εμφάνισης, με αποτέλεσμα να αμελούνται από την πλειονότητα των οργανισμών.

Λόγω της κρισιμότητας συναφών καταστάσεων, η συγκεκριμένη προσέγγιση χαρακτηρίζεται λανθασμένη - η μη απίθανη περίπτωση της πλήξης κάποιου παγκόσμιου οικονομικού κέντρου θα είχε άμεσες, παγκόσμιες συνέπειες. Παράλληλα, στις περισσότερες αναλύσεις ρίσκου, η πιθανότητα σημαντικών καταστροφών υποτιμάται. Υποστηρίζεται ότι, αναφορικά με την πιθανότητα των καταστροφικών γεγονότων, δεν ακολουθείται κανονική κατανομή, αλλά στατιστικές κατανομές με «χοντρές ουρές» (fat tails) και με σημαντικά μικρότερους ρυθμούς μείωσης των πιθανοτήτων εμφάνισης ακραίων περιπτώσεων και μεγάλο αθροιστικά αντίκτυπο (Etkin, et al., 2018).

Ακόμη, καταστροφικά γεγονότα λαμβάνουν λιγότερη δημοσιότητα από το αναμενόμενο, με αποτέλεσμα την υποτίμηση των επιπτώσεών τους από μεγάλο μέρος της κοινής γνώμης (Eisensee & Strömberg, 2002).



Διάγραμμα 17 – Αριθμός θανάτων που απαιτούνται ανά κατηγορία καταστροφών για να καλυφθεί κάποιο καταστροφικό γεγονός δημοσιογραφικά (Eisensee & Strömberg).

Σύμφωνα με έρευνες, το 75% των οργανισμών δεν διαθέτουν επίσημο σχέδιο αντιμετώπισης συμβάντων ασφαλείας (ROBERTS & LASHINSKY, 2017). Αντίστοιχα, το 51% των επιχειρήσεων παγκοσμίως (MERCER, 2020) και το 75% των μικρομεσαίων επιχειρήσεων δε διαθέτουν σχέδια επιχειρηματικής συνέχισης και αντιμετώπισης καταστροφών (Dushie, 2014). Ως αποτέλεσμα, τουλάχιστον 2 στις 3 πληττόμενες μικρές επιχειρήσεις δεν ξαναλειτουργούν ή αποτυγχάνουν μέσα στον πρώτο χρόνο επαναλειτουργίας (MCKAY, 2018).

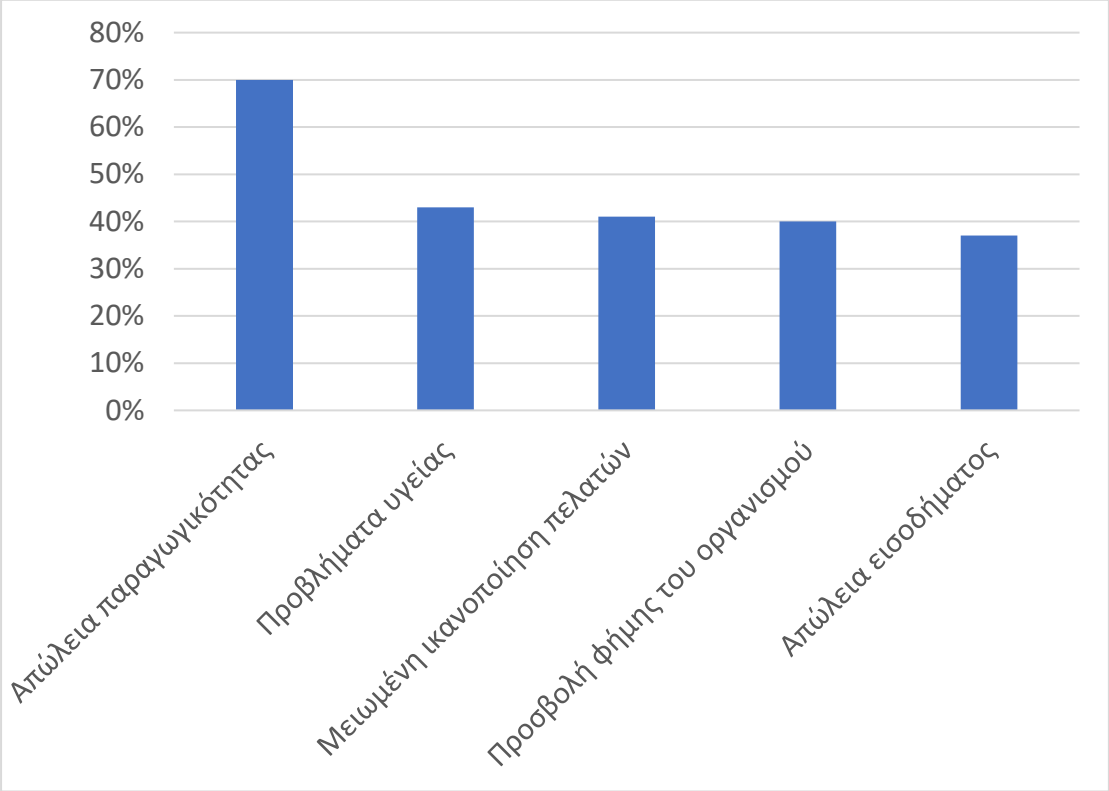
Η πολυπλοκότητα του σύγχρονου επιχειρηματικού περιβάλλοντος καθιστούν όλο και σημαντικότερη την ανάγκη ύπαρξης σχεδίων αντιμετώπισης καταστροφών, ιδιαίτερα λαμβάνοντας υπόψη τη μηδενική ή ελλιπή προετοιμασία των περισσότερων οργανισμών.

Ο τρόπος αντίδρασης ενός οργανισμού στα συμβάντα που επηρεάζουν τη λειτουργία του πιθανότατα θα καθορίσουν τη βιωσιμότητά του. Ελλιπής σχεδιασμός αυξάνει το ρίσκο στο οποίο εκτίθεται και μπορεί να οδηγήσει σε αδυναμία κατάλληλης αντιμετώπισης των προβλημάτων και επαναφοράς στην κανονική του λειτουργία.

Διακοπές

Ως διακοπές ορίζονται ξαφνικά, μη προγραμματισμένα γεγονότα, τα οποία περιορίζουν τη λειτουργία κρίσιμων επιχειρηματικών δραστηριοτήτων του οργανισμού και προκαλούν ζημιές ή απώλειες ανάλογες της έντασής τους. Περιλαμβάνουν ακραία καιρικά φαινόμενα, φυσικές καταστροφές – σεισμούς, παλιρροϊκά κύματα και τυφώνες, εγκληματική δραστηριότητα, πολιτικές αναταραχές, τρομοκρατικές ενέργειες, λειτουργικές διακοπές και αποτυχία πόρων. Η διακοπή της υπηρεσίας μπορεί να είναι επιτηδευμένη ή τυχαία, κακόβουλη η άτυχη, αλλά σε κάθε περίπτωση επηρεάζει τη δυνατότητα του οργανισμού να συνεχίσει τη λειτουργία του και την αξιοπιστία του.

Σύμφωνα με έρευνες, στις πέντε πιο διαδεδομένες επιπτώσεις των διακοπών εντοπίζονται η απώλεια παραγωγικότητας (70%), επιπτώσεις στην υγεία του ανθρώπινου δυναμικού (43%), μειωμένη ικανοποίηση πελατών (41%), προσβολή της φήμης του οργανισμού (40%) και απώλεια εισοδήματος (37%) (bci, 2020).



Διάγραμμα 18 – Οι πιο διαδεδομένες αναφερόμενες επιπτώσεις των διακοπών στη λειτουργία των οργανισμών (bci)

Η προετοιμασία για πιθανές διακοπές εντάσσεται στο γενικότερο πλαίσιο της διαχείρισης επιχειρηματικής συνέχισης, με στόχο την μετρίαση των συμβάντων και τη διατήρηση της κανονικής λειτουργίας. Οι ενέργειες της διαδικασίας περιλαμβάνουν τη διεξαγωγή αναλύσεων επιχειρηματικού αντίκτυπου, τη διαχείριση ρίσκου, τη διαμόρφωση και ενημέρωση του πλάνου επιχειρηματικής συνέχισης και του πλάνου αποκατάστασης καταστροφών, την αξιολόγηση και δοκιμή των σχεδίων και τη διαχείριση της αντίδρασης σε συμβάντα.

Σημειώνεται ότι η γενικότερη διαχείριση των συμβάντων αναφέρεται σε μικρότερης σημασίας και χρονικής διάρκειας διακοπές, ενώ το πλάνο αποκατάστασης καταστροφών επικεντρώνεται σε γεγονότα μεγάλης σημασίας, διάρκειας και αντίκτυπου, που επηρεάζουν πολλές διαδικασίες του οργανισμού.

4.1: Ανάλυση επιχειρηματικού αντίκτυπου

Η ανάλυση επιχειρηματικού αντίκτυπου αποτελεί επίσημη ανάλυση των λειτουργιών και δραστηριοτήτων του οργανισμού με στόχο την κατηγοριοποίηση τους σε κρίσιμες, οι όποιες απαιτούνται και η διακοπή των οποίων προκαλεί μία αποδεκτή ζημιά, και μη κρίσιμες οι οποίες μπορεί να είναι σημαντικές, αλλά δεν αποτρέπουν την λειτουργία του οργανισμού. Η εκτίμηση των επιπτώσεων σε ανθρώπινο δυναμικό, συστήματα, πληροφορίες και περιουσιακά στοιχεία επιτρέπει στους οργανισμούς να αναγνωρίσουν τη σειρά προτεραιότητας με την οποία πρέπει να επιχειρηθεί η αποκατάσταση κάθε λειτουργίας σε περίπτωση σημαντικής διακοπής. Παράλληλα, προσδιορίζονται οι προϋποθέσεις της επιτυχημένης αποκατάστασης, συνεισφέροντας στις διαδικασίες διαχείρισης ρίσκου και αντιμετώπισης συμβάντων.

Στα πλαίσια της διαδικασίας, κάθε κρίσιμη λειτουργία περιγράφεται πλήρως, με τις απαιτήσεις λειτουργίας της και εκφέρονται χρήσιμα μεγέθη, όπως ο στόχος σημείου αποκατάστασης, ο οποίος αναφέρεται στην μεγίστη αποδεκτή απώλεια δεδομένων, ο στόχος χρόνου αποκατάστασης, ο οποίος αναφέρεται στο μέγιστο επιτρεπτό χρονικό διάστημα αποκατάστασης της λειτουργίας, στις επιχειρηματικές απαιτήσεις αποκατάστασης, οι οποίες ταυτοποιούν άλλες επιχειρηματικές δραστηριότητες που απαιτούνται ώστε να αποκατασταθεί η περιγραφόμενη λειτουργία και στις τεχνικές απαιτήσεις αποκατάστασης, οι οποίες προσδιορίζουν τεχνικές προϋποθέσεις, απαραίτητες για την υποστήριξη της συγκεκριμένης κρίσιμης επιχειρηματικής διαδικασίας. Στις τελευταίες, περιλαμβάνονται εγκαταστάσεις, εξοπλισμός, άτομα, προμηθευτές και συνεργάτες, δίαυλοι επικοινωνίας και οργανωτικές δομές. Η εξασφάλιση της συνέχισης της λειτουργίας κρίσιμων λειτουργιών του οργανισμού είναι απαραίτητες για την επιβίωση του. Ακόμη, στα πλαίσια της συγκεκριμένης ανάλυσης ταυτοποιούνται οι απαιτήσεις πόρων για και μέχρι την επιστροφή στην κανονική λειτουργία. Απαιτείται διεξοδικότητα, για τον εντοπισμό λιγότερο εμφανών επιπτώσεων και αναγνώριση των καταστάσεων που επιδεινώνονται με την πάροδο του χρόνου, είτε λόγω αθροιστικών αλλοιώσεων σε βάθος χρόνου, είτε λόγω εποχικότητας.

4.2: Διαχείριση ρίσκου

Το ρίσκο αναφέρεται στη πιθανότητα εμφάνισης κάποιου αντίκτυπου σε ένα περιουσιακό στοιχείο του οργανισμού, από την έκθεσή του σε κάποιο γεγονός. Παρά τη συχνότερη αρνητική του σημασία, τονίζεται ότι μπορεί να έχει είτε θετική είτε αρνητική έννοια. Στα πλαίσια της αποτελεσματικής διαχείρισης έργων, επιχειρείται η ελαχιστοποίηση των αρνητικών ρίσκων και η μεγιστοποίηση των θετικών (Project Management Institute, 2017).

Η διαχείριση του ρίσκου αναφέρεται στη συνεχή διαδικασία ταυτοποίησης, αξιολόγησης, ανάλυσης προτεραιοτήτων και αντιμετώπισης του ρίσκου, η οποία διασφαλίζει ότι λαμβάνονται υπόψη οι κίνδυνοι που είναι πιθανότερο να επηρεάσουν τον οργανισμό και ότι υπάρχουν τα κατάλληλα πλάνα αντιμετώπισης πριν χρειαστούν. Η μεθοδολογία ρίσκου περιγράφει τον τρόπο διαχείρισης και περιλαμβάνει την προσέγγιση, δηλαδή τον τρόπο με τον οποίο ακολουθούνται τα βήματα της διαδικασίας, τις απαραίτητες πληροφορίες και τις τεχνικές που απαιτούνται.

Τα βήματα της διαδικασίας διαχείρισης ρίσκου περιλαμβάνουν την ταυτοποίηση των κινδύνων, την αξιολόγησή τους, τη σχεδίαση και υλοποίηση της αντίδρασης σε αυτά και την παρακολούθηση και αξιολόγηση της λειτουργίας των διαδικασιών αντιμετώπισης.

4.2.1: Ταυτοποίηση ρίσκου

Διαφορετικές μέθοδοι προσεγγίζουν με διαφορετικό τρόπο το πρόβλημα της ταυτοποίησης των περισσότερων δυνατών ρίσκων, αξιοποιώντας πλήθος πηγών. Σε αυτές περιλαμβάνονται:

- Ο «καταιγισμός ιδεών», ο οποίος αναφέρεται στη λήψη αδόμητων πληροφοριών από τα άτομα μιας ομάδας στα πλαίσια μιας συνάντησης, με απόλυτη ελευθερία έκφρασης και σε ασφαλές περιβάλλον.

- Τα ερωτηματολόγια, τα οποία αποτελούν λίστες προετοιμασμένων ερωτήσεων και για ορθότερα αποτελέσματα απαιτούν ανωνυμία και διαφορετικότητα συμμετεχόντων.

- Οι συνεντεύξεις, οι οποίες επιτρέπουν την λεπτομερέστερη καταγραφή των απόψεων των συμμετεχόντων.

- Οι ομάδες εργασίας, οι οποίες επιτρέπουν την αποτελεσματικότερη προσέγγιση ενός συγκεκριμένου τομέα, στον οποίο δραστηριοποιούνται οι συμμετέχοντες.

- Οι υπάρχουσες λίστες που αξιοποιούνται στα πλαίσια του οργανισμού και αναφέρονται στα βήματα συγκεκριμένων διαδικασιών.

- Ιστορικές πληροφορίες πάνω στα αντικείμενα ενδιαφέροντος που πιθανώς να διατηρούνται από τον οργανισμό.

Συνδυασμός αυτών των μεθόδων και ποικιλία πηγών οδηγεί στα καλύτερα δυνατά αποτελέσματα. Έξοδος αυτής της διαδικασίας είναι η λίστα ταυτοποιημένων κινδύνων ή μητρώο κινδύνων (Project Management Institute, 2017), με διαφορετικά είδη πληροφοριών, στις οποίες περιλαμβάνονται η περιγραφή του κάθε ρίσκου και στο οποίο προστίθενται μετέπειτα λεπτομέρειες για το αναμενόμενο αντίκτυπο σε περίπτωση που παρουσιαστεί, η πιθανότητα εμφάνισης, τα βήματα πρόληψης και αντιμετώπισης και η προτεραιότητα του ρίσκου. Η διαδικασία ταυτοποίησης πρέπει να λαμβάνει υπόψη της νέες και ανερχόμενες απειλές, οι οποίες μπορεί να προέρχονται από νέες τεχνολογίες, αλλαγές στην κουλτούρα του οργανισμού, στο περιβάλλον ή στις επιχειρηματικές πρακτικές και αντικανονικές ενέργειες. Ιδιαίτερη προσοχή απαιτείται κατά την αξιολόγηση του στατικού περιβάλλοντος, το οποίο

αναφέρεται σε συστήματα που δεν αλλάζουν συχνά ή και καθόλου μετά την αρχική τοποθέτηση και συχνά παραλείπονται.

4.2.2: Αξιολόγηση ρίσκου

Η αξιολόγηση του ρίσκου αφορά τον προσδιορισμό των πιο σοβαρών κινδύνων, που θα μπορούσαν να εμποδίσουν τη λειτουργία του οργανισμού, και παρέχει τα απαραίτητα δεδομένα για τη βέλτιστη επιλογή απόκρισης. Εντοπίζονται δύο προσεγγίσεις στην αξιολόγηση του ρίσκου, η ποσοτική και η ποιοτική. Συχνά, απαιτείται συνδυασμός και των δύο προσεγγίσεων, καθώς η ποιοτική ανάλυση υποστηρίζει συνολικότερες και πιο κατανοητές και επικοινωνήσιμες εκτιμήσεις κινδύνου, αλλά δυσκολεύει τη δικαιολόγηση του κόστους των ελέγχων αντιμετώπισης.

Ποσοτική αξιολόγηση κινδύνου

Η ποσοτική εκτίμηση ρίσκου επιχειρεί να περιγράψει τον κίνδυνο σε χρηματοοικονομικούς όρους και να αντιστοιχίσει μια οικονομική αξία, με επακόλουθα μεγαλύτερη αντικειμενικότητα, αλλά και δυσκολία ποσοτικοποίησης μεγεθών, όπως η φήμη του οργανισμού, η εμπιστοσύνη των πελατών και η επίδραση μελλοντικών γεγονότων. Παράλληλα, σημειώνεται ότι επιδέχεται μεγαλύτερης αυτοματοποίησης.

Ο υπολογισμός του ποσοτικοποιημένου κινδύνου περιλαμβάνει τον προσδιορισμό της αξίας ενός περιουσιακού στοιχείου και της πιθανότητας να υποστεί ζημιά, καταλήγοντας στο μέγεθος του προσδόκιμου απώλειας. Η διαδικασία περιλαμβάνει τα εξής βήματα:

- Υπολογισμός της αξίας του περιουσιακού στοιχείου, κατά τον οποίο εκτιμάται η συνεισφορά κάθε στοιχείου, υλικού ή άυλου, στην ικανότητα του οργανισμού να ανταποκριθεί στην αποστολή του και η αξία αντικατάστασης, σε περίπτωση απώλειας.

- Υπολογισμός του συντελεστή έκθεσης, ο οποίος αναφέρεται στο ποσοστό της αξίας του περιουσιακού στοιχείου που θα χαθεί λόγω κάποιου συμβάντος. Λόγω της πολυπλοκότητας και ιδιαιτερότητας κάθε κατάστασης, μεμονωμένοι υπολογισμοί σπανίως είναι σωστοί, αλλά η ομαδοποίηση παρόμοιων συμβάντων επιτρέπει ικανοποιητικές προσεγγίσεις.

- Υπολογισμός του προσδόκιμου μεμονωμένης απώλειας, το οποίο αποτελεί το γινόμενο των δύο προηγούμενων παραγόντων.

- Προσδιορισμός της πιθανότητας ετήσιας απώλειας ή πιθανότητας κινδύνου, η οποία αποτελεί εκτίμηση του μέσου όρου των ετησίων περιστάσεων εκδήλωσης. Αποτελεί ιδιαίτερα δύσκολη και ανακριβή διαδικασία, δεδομένου ότι κάθε μέγεθος επηρεάζεται από εσωτερικούς και εξωτερικούς παράγοντες και ότι τα ιστορικά δεδομένα δεν συντελούν απαραίτητα σε ορθές προβλέψεις.

- Υπολογισμός του ετήσιου προσδόκιμου απώλειας, το οποίο αποτελεί το γινόμενο του προσδόκιμου μεμονωμένης απώλειας και της πιθανότητας κινδύνου, εκτιμά το ετήσιο οικονομικό αντίκτυπο ενός ρίσκου και επιτρέπει την σύγκριση της οικονομικής αποδοτικότητας των σχετικών ελέγχων.

Ποιοτική αξιολόγηση κινδύνου

Η ποιοτική εκτίμηση επικινδυνότητας κατατάσσει τους κινδύνους με βάση την πιθανότητα εμφάνισης και το αντίκτυπό τους στις επιχειρηματικές δραστηριότητες, το οποίο αναφέρεται στο βαθμό αποτελεσματικότητας μιας εντοπισμένης απειλής. Οι επιπτώσεις ποικίλουν από ασήμαντες έως καταστροφικές, με την ανάλογη αύξηση της τιμής που τις περιγράφει. Είναι

σημαντικά υποκειμενικές, αλλά συνεισφέρουν στον προσδιορισμό των πιο κρίσιμων κινδύνων, πραγματοποιώντας μεταξύ τους συγκρίσεις. Κατά τη διαδικασία αυτή, ρίσκα με υψηλή αποτελεσματικότητα, δηλαδή ταυτόχρονα σημαντική πιθανότητα και αντίκτυπο χρίζουν και υψηλότερης προτεραιότητας, ακολουθούμενα από όσα εμφανίζουν υψηλό μόνο έναν από τους δύο δείκτες.

4.2.3: Σχεδιασμός απόκρισης κινδύνου

Η ανάπτυξη σχεδίου αντιμετώπισης ενός ρίσκου βασίζεται σε ένα σύνολο πιθανών ενεργειών. Στην περίπτωση αρνητικού ρίσκου, οι πιθανές δράσεις περιλαμβάνουν τις παρακάτω:

- Μείωση ρίσκου, η οποία αξιοποιεί τους κατάλληλους ελέγχους, διοικητικούς, φυσικούς ή τεχνικούς, προς μετρίαση των κινδύνων

- Μετάθεση ρίσκου, η οποία επιτρέπει την μεταφορά του κινδύνου σε κάποια άλλη οντότητα, συνήθως ασφαλιστική.

- Αποδοχή ρίσκου, η οποία αναφέρεται στη συνειδητή επιλογή του οργανισμού να μην εφαρμόσει κάποιον έλεγχο ασφαλείας, διότι δε συμφέρει οικονομικά, ανάλογα με τα αποτελέσματα σχετικής οικονομικής ανάλυσης και την όρεξη κινδύνου του οργανισμού

- Αποφυγή ρίσκου, κατά την οποία επιλέγεται να μην πραγματοποιηθεί κάποια δραστηριότητα, διότι συνδέεται με κίνδυνο η αντιμετώπιση του οποίου δε συμφέρει οικονομικά.

Ο συνολικός κίνδυνος αναφέρεται στο συνδυασμένο κίνδυνο για όλα τα περιουσιακά στοιχεία της επιχείρησης και ο υπολειπόμενος στο ρίσκο που απομένει μετά την εφαρμογή αντιμέτρων και ελέγχων. Στην πλειονότητα των

περιπτώσεων η εξάλειψη του ρίσκου δεν είναι εφικτή ή δεν συμφέρει οικονομικά. Υπερβολικό κόστος διαχείρισης κάποιου ρίσκου απαιτεί εναλλακτικά αντίμετρα ή αποφυγή κάποιας δραστηριότητας. Το αποδεκτό εύρος κινδύνων επηρεάζει άμεσα τις δραστηριότητες του οργανισμού και τις επιλογές των αντίμετρων. Κατά τη διαδικασία διαχείρισης ρίσκων επιχειρείται παραμονή εντός του διαστήματος, το οποίο ορίζεται μεταξύ του μέγιστο αντίκτυπου κάποιου ρίσκου που αντέχει να διαχειριστεί οικονομικά ο οργανισμός και του συνολικού κόστους των αντίμετρων προς διαχείριση του υπολειπόμενου ρίσκου.

Στην περίπτωση θετικού ρίσκου, οι οργανισμοί επιλέγουν από τις παρακάτω ενέργειες:

- Εκμετάλλευση ρίσκου, η οποία περιλαμβάνει την άδραξη της ευκαιρίας που παρουσιάζεται κατά την ανταπόκριση στο δεδομένο κίνδυνο.

- Επιμοιρασμός ρίσκου, κατά την οποία αξιοποιείται η συνεργασία με τρίτο μέρος για την από κοινού εκμετάλλευση κάποιας ευκαιρίας

- Ενίσχυση ρίσκου, η οποία αναφέρεται στη μεγιστοποίηση της πιθανότητας ή των θετικών επιδράσεων κάποιου θετικού ρίσκου.

- Αποδοχή ρίσκου, η οποία, ανάλογα με την αντίστοιχη αρνητική περίπτωση, αναφέρεται στη μη λήψη μέτρων ή πραγματοποίηση ενεργειών που σχετίζονται με το δεδομένο ρίσκο, καθώς η πιθανή του εμφάνιση μπορεί να λειτουργήσει μόνο θετικά.

4.2.4: Εφαρμογή σχεδίου απόκρισης

Η εφαρμογή του σχεδίου αντιμετώπισης του ρίσκου αναφέρεται στην υλοποίηση των κατάλληλων ελέγχων ασφαλείας, ανάλογα με τις προσεγγίσεις που επελέγησαν και τους διαθέσιμους πόρους. Κατά την επιλογή των ελέγχων πρέπει να λαμβάνονται υπόψη πλήθος παραγόντων, όπως το κόστος του προϊόντος ή υπηρεσίας, το κόστος της υλοποίησης, το κόστος συμβατότητας με τις λοιπές δομές και διαδικασίες, το περιβαλλοντικό κόστος, το κόστος δοκιμών - χρόνου, χρημάτων και δυνητικών διακοπών λειτουργίας - και το κόστος της χαμένης παραγωγικότητας.

Κάθε έλεγχος πρέπει να προστατεύει από τουλάχιστον μία συγκεκριμένη απειλή, διαφορετικά αποτελεί αδικαιολόγητη επιβάρυνση. Συγκρίνοντας το κόστος κάθε ελέγχου με το αναμενόμενο κόστος και πιθανότητα του ρίσκου το οποίο καλείται να διαχειριστεί, εντοπίζονται πιθανές σπατάλες πόρων προς εξάλειψη. Κατά τη διαμόρφωση των ελέγχων, πρέπει να λαμβάνεται υπόψη κάθε αποδεικτή και μη αποδεκτή δραστηριότητα, στα πλαίσια των πολιτικών ασφαλείας που έχουν επιλεγεί.

4.2.5: Παρακολούθηση και έλεγχος απόκρισης κινδύνου

Η επιβεβαίωση της ορθής λειτουργίας και επιδιωκόμενου οφέλους κάποιου ελέγχου είναι καταλυτικής σημασίας για την επιβεβαίωση της αξίας του. Σημειώνεται η αναγκαιότητα πιστοποίησης του προγράμματος ασφαλείας, τήρησης των καλών πρακτικών του τομέα και επιμελούς ανάλυσης νέων κινδύνων που μπορεί να εισάγονται, λόγω λανθασμένης αίσθησης ασφάλειας.

Προς αυτή την κατεύθυνση, οι αξιολογήσεις ασφάλειας επιβεβαιώνουν την ορθή λειτουργία των συστημάτων και ελέγχων ασφαλείας. Η ύπαρξή τους είναι κρίσιμη για την επιβεβαίωση της αρτιότητας και καταλληλότητας των πολιτικών ασφαλείας για τη δεδομένη επιχειρηματική δραστηριότητα, της συμβατότητας

των ελέγχων ασφαλείας και των πολιτικών και της αποτελεσματικής υλοποίησης και συντήρησης των παραπάνω.

4.3: Πλάνο επιχειρηματικής συνέχισης

Η επιχειρηματική συνέχιση αναφέρεται στη διεξοδική διαχειριστική προσπάθεια κατάταξης των επιχειρηματικών διαδικασιών ανά προτεραιότητα, αναγνώρισης των σημαντικότερων απειλών για την κανονική λειτουργία του οργανισμού και προετοιμασίας σχεδίων αντιμετώπισης κρίσεων (Dushie, 2014). Αντίστοιχα, το πλάνο επιχειρηματικής συνέχισης περιγράφει δομημένα τρόπους αντίδρασης σε οποιοδήποτε συμβάν οδηγεί σε διακοπή κρίσιμων επιχειρηματικών δραστηριοτήτων του οργανισμό.

Βασίζεται στα αποτελέσματα των αναλύσεων επιχειρηματικού αντίκτυπου και αποκλειστικά σε κρίσιμους πόρους, εντοπίζοντας τις διαδικασίες, τα περιουσιακά στοιχεία και τον εξοπλισμό, τα οποία χρειάζονται για κρίσιμες επιχειρηματικές δραστηριότητες, όταν μία διακοπή επηρεάζει τη βιωσιμότητα του οργανισμού. Βασικό τμήμα της ανάλυσης είναι η θέση προτεραιοτήτων – επισημαίνεται ότι η ασφάλεια του ανθρώπινου δυναμικού έχει απόλυτη προτεραιότητα και ακολουθείται από τις κρίσιμες διαδικασίες και έπειτα, τις υποδομές πληροφορικής. Η ιεράρχηση αυτή είναι απαραίτητο να λαμβάνεται υπόψη κατά το σχεδιασμό των δραστηριοτήτων αποκατάστασης.

Ανάλογα με το περιβάλλον δραστηριοτήτων του οργανισμού, η ύπαρξη πλάνου επιχειρηματική συνέχισης είναι πιθανό να επιβάλλεται από τους κανονισμούς και τα ισχύοντα νομικά πλαίσια. Παράλληλα, κρίνεται απαραίτητη η διεξοδική και ολιστική προσέγγιση των συστημάτων κατά τη δημιουργία του συγκεκριμένου σχεδίου, καθώς με αυτό τον τρόπο αντιμετωπίζονται οι κίνδυνοι για το συνολικό οργανισμό και δεν επιδιορθώνεται απλά ένας μεμονωμένος πόρος. Το πλάνο πρέπει να προσδιορίζει πολιτικές, πρότυπα, διαδικασίες και κατευθυντήριες γραμμές, απαραίτητα για την αποκατάσταση, να διασαφηνίζει τους ρόλους και αρμοδιότητες των ομάδων και των μελών τους και να

προβλέπει έκτακτες διαδικασίες προστασίας της ζωής και των υποδομών. Ακόμη, τονίζεται η σημασία των αναλύσεων κατάστασης και του προσδιορισμού εναλλακτικών εγκαταστάσεων, για βραχυπρόθεσμη και μακροπρόθεσμη έκτακτη λειτουργία και επιχειρηματική ανάκαμψη.

4.4: Πλάνο αποκατάστασης καταστροφών

Το πλάνο αποκατάστασης καταστροφών διευθύνει τις απαραίτητες δραστηριότητες, για την αποκατάσταση μετά από καταστροφή. Είναι τμήμα του πλάνου επιχειρηματικής συνέχισης και διασφαλίζει ότι είναι διαθέσιμοι οι απαιτούμενοι πόροι για τις δραστηριότητες συνέχισης. Στα πλαίσια του πλάνου αυτού ταυτοποιούνται γεγονότα που μπορεί να προκαλέσουν ζημιά σε κρίσιμους πόρους και τι ακριβώς μπορεί να τους συμβεί. Επίσης, οι ενέργειες του σχεδίου δεν αναφέρονται μόνο στην εκ των υστέρων αντιμετώπιση της καταστροφής, αλλά και σε πρόληψη των επιπτώσεων. Όταν ακολουθείται, το πλάνο αποκατάστασης καταστροφών μεγιστοποιεί τις πιθανότητες λήψης ορθών αποφάσεων και επιτυχημένης αντίδρασης, με αντίστοιχα σημαντικό οικονομικό κόστος δημιουργίας και επαλήθευσης.

Η ανάλυση των δυνητικών απειλών εντοπίζει και καταγράφει τους κινδύνους και πιθανές καταστροφές που επηρεάζουν κρίσιμες διαδικασίες, όπως τυφώνες, ασθένειες, σεισμούς, κυβερνοεπιθέσεις, δολιοφθορές, διακοπές ρεύματος και τρομοκρατικές επιθέσεις. Οι ασθένειες πλήττουν άμεσα το εργατικό δυναμικό, με ιδιαίτερα κρίσιμη την περίπτωση πλήξης των ομάδων που καλούνται να εκτελέσουν τις ίδιες τις διαδικασίες αποκατάστασης, ενώ οι υπόλοιπες απειλές προκαλούν καταστροφές στην υλικοτεχνική υποδομή του οργανισμού. Είναι σημαντικό να μελετώνται λογικοί συνδυασμοί των απειλών, όπως σεισμοί ή τυφώνες που προκαλούν πυρκαγιές, για καλύτερη προετοιμασία. Με βάση τα αποτελέσματα αυτής της ανάλυσης, έπεται καταγραφή των σεναρίων επιπτώσεων, λαμβάνοντας υπόψη τις πιο ευρείες καταστροφές, ώστε να μεγιστοποιηθεί η αξία του πλάνου και οι ευκαιρίες διευρυμένων στρατηγικών. Διεξοδικά πλάνα αποκατάστασης καταστροφών

συμπεριλαμβάνουν τόσο γενικότερα, όσο και πιο συγκεκριμένα σενάρια για αποτελεσματικότερη διαχείριση μεμονωμένων περιστατικών.

Τα έγγραφα απαιτήσεων αποκατάστασης καλούνται να καταγράφουν τις επιχειρηματικές και τεχνικές απαιτήσεις για την έναρξη της φάσης εφαρμογής. Περιλαμβάνουν πληροφορίες για κάθε περιουσιακό στοιχείο και τη διαθεσιμότητά του σε περίπτωση καταστροφής, με λεπτομέρειες για τις υποδομές, τον πληροφοριακό εξοπλισμό, εναλλακτικές εγκαταστάσεις, και στοιχεία επικοινωνίας με συνεργάτες και σημαντικά τρίτα μέρη και τα μέλη των ομάδων αποκατάστασης. Ακόμη, περιγράφουν κρίσιμες επιχειρηματικές και λειτουργικές διαδικασίες και την απαιτούμενη υποδομή πληροφορικής, πληροφορίες για την ανάκτηση και τη χρήση των αποθηκευμένων δεδομένων, πληροφορίες για την αποκατάσταση των συστημάτων, εφαρμογών και υπηρεσιών που απαιτούνται για τις διαδικασίες επαναφοράς και εναλλακτικές, τους στόχος χρόνου αποκατάστασης και τα βήματα που απαιτούνται για την επίτευξη τους.

Στα πλαίσια της διαδικασίας αποκατάστασης, αρχικά, επιχειρείται επαναφορά των επιχειρησιακών λειτουργιών και έπειτα επιστροφή στην κανονική κατάσταση λειτουργίας. Ακολουθώντας το πλάνο αποκατάστασης καταστροφών, στην πρώτη φάση αξιοποιούνται οι εφεδρικές εγκαταστάσεις, εξοπλισμός και πόροι. Στη δεύτερη φάση, πραγματοποιείται διάσωση των περιουσιακών στοιχείων, επισκευή και επιστροφή στις αρχικές εγκαταστάσεις.

Η εκπαίδευση του προσωπικού για την αντιμετώπιση καταστροφικών καταστάσεων κρίνεται ιδιαίτερα σημαντική, ώστε πρώτιστα να διασφαλιστεί η ασφάλεια του. Επακόλουθα, πριν οποιοδήποτε βήμα αποκατάστασης, πρέπει να αντιμετωπιστεί και περιοριστεί το ίδιο το γεγονός της καταστροφής και μετέπειτα, να ξεκινήσουν οι εργασίες αποκατάστασης.

Στα πλαίσια του σχεδίου αποκατάστασης καταστροφών, καθορίζεται , επίσης, το κέντρο επιχειρήσεων έκτακτης ανάγκης, από όπου συντονίζονται οι δραστηριότητες αποκατάστασης και εργάζονται οι σχετικές ομάδες.

Περιορισμένη λειτουργία

Σε αντίθεση με τις κανονικές συνθήκες λειτουργίας, σε περιστάσεις ανάγκης ενδεχομένως δεν είναι διαθέσιμες διαδικασίες και έλεγχοι. Η ορθή προετοιμασία και επίδειξη προσαρμοστικότητας και ευελιξίας είναι απαραίτητες για τη διατήρηση της ασφάλειας των πληροφοριών και της λειτουργίας των κρίσιμων διαδικασιών του οργανισμού.

Με βάση τα πλάνα αντίδρασης, η αναστολή κανονικών διαδικασιών και ελέγχων και η ενεργοποίηση νέων μπορεί να συνεισφέρει σημαντικά στη διαδικασία αποκατάστασης. Η προσωρινή περεταίρω εξουσιοδότηση και διεύρυνση των ρόλων των ομάδων αποκατάστασης, η διάθεση αυξημένων πόρων στις διαδικασίες τεχνικής υποστήριξης και καθοδήγησης και ο προσωρινός συνδυασμός συμβατών συστημάτων μπορεί να μειώσει σημαντικά το χρόνο που απαιτείται για την επαναφορά της δραστηριότητας. Είναι σημαντική, ωστόσο, η κανονική συνέχιση των δραστηριοτήτων υποστήριξης της ασφάλειας των πληροφοριών, ώστε να είναι έτοιμη η αντίδραση σε κάποιον νέο, ταυτόχρονο κίνδυνο και να περιοριστούν οι επιπτώσεις κάποιας αποτυχίας των ενεργειών αποκατάστασης.

Διατήρηση πληροφορίας συστημάτων

Κρίσιμης σημασίας στα πλαίσια της αποκατάστασης καταστροφών είναι οι ενέργειες αντικατάστασης των κατεστραμμένων συστημάτων. Η διατήρηση άμεσα διαθέσιμης και ενημερωμένης πληροφορίας για τα συστήματα, τις συνδεσμολογίες, τα αποθέματα υλικού, τις ρυθμίσεις του λογισμικού και τα εφεδρικά αρχεία του οργανισμού είναι απαραίτητη για τις διαδικασίες επαναφοράς. Δεν πρέπει να παραλείπεται ο έλεγχος της πρόσβασης στην πληροφορία αυτή και η έγκαιρη εξουσιοδότηση όλων των χρηστών που απαιτείται για την αποφυγή καθυστερήσεων. Επίσης, κατά τις διαδικασίες επιστροφής στην κανονική λειτουργία, είναι χρήσιμη η αξιοποίηση της ευκαιρίας για την ενημέρωση ή αναβάθμιση των πόρων.

4.5: Αξιολόγηση και δοκιμές

Η επαλήθευση του κάθε πλάνου και η αξιολόγηση της απόδοσης, πληρότητας και ακρίβειάς του, ανά τακτικά χρονικά διαστήματα, είναι απαραίτητη για τον εντοπισμό παραλείψεων και λαθών και την προσαρμογή του σε νέα δεδομένα, ανάλογα με τις ανάγκες και το προφίλ ρίσκου κάθε οργανισμού. Ακόμη, θεωρείται απαραίτητη η ενεργοποίηση αυτής της διαδικασίας μετά από σημαντικές μεταβολές, στα πλαίσια των διαδικασιών διαχείρισης αλλαγών.

Η αποδοχή οποιουδήποτε πλάνου πρέπει να έχει ως προϋπόθεση τις επιτυχημένες δοκιμές κάθε σταδίου και την επιβεβαίωση της ύπαρξης των απαραίτητων πόρων για την υλοποίησή του και την αντιμετώπιση του συμβάντος ενδιαφέροντος.

Στις δοκιμές των πλάνων περιλαμβάνονται οι παρακάτω:

- Δοκιμές λιστών ελέγχου, όπου επαληθεύεται με απλό τρόπο η κάλυψη των αναγκών και των προτεραιοτήτων του οργανισμού και επιβεβαιώνεται η συμβατότητα κάθε τμήματος του πλάνου με αλλαγές που συνέβησαν ή έπονται, από κάθε άτομο που εμπλέκεται σε αυτό.

- Δομημένες επιδείξεις, οι οποίες αναφέρονται στην παρουσίαση του πλάνου από εκπρόσωπο κάθε τμήματος, με στόχο την αξιολόγηση των στόχων, των δομών, των απαιτήσεων και των υποθέσεων στα πλαίσιά του, τον εντοπισμό παραλείψεων και επικαλύψεων και τον έλεγχο της προετοιμασίας των μελών κάθε ομάδας.

- Δοκιμές προσομοίωσης, στις οποίες συμμετέχει το σύνολο των ατόμων που εμπλέκονται στις διαδικασίες, αξιοποιούνται αποκλειστικά τα προβλεπόμενα από το πλάνο μέτρα, μετρούνται οι χρόνοι αντίδρασης

και καταγράφονται ελλείψεις και τρωτά σημεία. Οι συγκεκριμένες δοκιμές συνεχίζονται μέχρι τέλους ή μέχρι την παρουσίαση κρίσιμου προβλήματος, το οποίο δεν μπορεί να αντιμετωπιστεί επί τόπου με σύντομη διακοπή της δοκιμής.

- Δοκιμές πλήρους διακοπής, όπου μιμείται το αντίκτυπο καταστροφής η οποία αχρηστεύει τις κύριες εγκαταστάσεις και χρησιμοποιούνται αποκλειστικά οι εναλλακτικές. Λόγω της σοβαρότητας των διακοπών, τέτοιου είδους δοκιμές πραγματοποιούνται από ελάχιστους οργανισμούς.

- Παράλληλες δοκιμές, όπου, παρόμοια με τις δοκιμές πλήρους διακοπής, χρησιμοποιούνται οι εναλλακτικές δομές, χωρίς όμως τη ταυτόχρονη διακοπή της λειτουργίας των κύριων εγκαταστάσεων.

Σημειώνεται ότι το κόστος των παράλληλων δοκιμών και πλήρους διακοπής είναι το πλέον σημαντικό, αλλά αποδίδουν τα πιο ακριβή αποτελέσματα.

4.6: Διαχείριση συμβάντων

Η διαδικασία διαχείρισης συμβάντων περιλαμβάνει τις ενέργειες απόκρισης σε σοβαρά γεγονότα, τα οποία περιορίζουν τη λειτουργία του οργανισμού. Διακρίνονται τα εξής στάδια:

- Προετοιμασίας, όπου εντάσσεται η κρίσιμη διαδικασία της σχεδίασης της απόκρισης και η δημιουργία της ομάδας αντιμετώπισης συμβάντων, αποτελούμενης από άτομα με την κατάλληλη εκπαίδευση και εξουσιοδότηση για το χειρισμό των αναμενόμενων καταστάσεων.

- Ταυτοποίησης, όπου κάποιο γεγονός αναλύεται και ανάλογα με τη σοβαρότητά του χαρακτηρίζεται συμβάν που χρίζει αντιμετώπισης, με βάση τα υπάρχοντα πλάνα και διαδικασίες.

- Ειδοποίησης, όπου ένα ταυτοποιημένο συμβάν προωθείται στις ομάδες που είναι υπεύθυνες για τη διαχείρισή του, μαζί με τις συγκεντρωμένες πληροφορίες. Σημειώνεται η σημασία αναγνώρισης των λανθασμένα χαρακτηρισμένων γεγονότων ως συμβάντα, προσεκτικής αντιμετώπισης της κατάστασης, ώστε να μην επιδεινωθεί και εντοπισμού μοτίβων σε φαινομενικά μεμονωμένα γεγονότα, τα οποία συλλογικά απαιτούν διαχείριση και χειρισμό ως ενιαίο συμβάν.

- Απόκρισης, όπου αντιμετωπίζονται οι επιπτώσεις του εντοπισμένου γεγονότος, με βάση τα σχέδια του οργανισμού. Προτεραιότητα δίνεται στον περιορισμό των περιστατικών, ώστε να αποφευχθεί διάδοση του κινδύνου σε άλλα συστήματα, τοποθεσίες ή ενδιαφέροντα μέρη και στον εντοπισμό της πηγής, για ουσιαστική αντιμετώπιση της απειλής. Τα πλάνα επιχειρηματικής συνέχειας και αποκατάστασης καταστροφών, αποτελέσματα προσεκτικών και διεξοδικών υπό άνεση χρόνου, περιγράφουν τα απαραίτητα βήματα αντιμετώπισης με τη μέγιστη αποτελεσματικότητα.

- Αποκατάστασης, κατά το οποίο, κατόπιν περιορισμού του αντίκτυπου του συμβάντος, αντιμετωπίζεται το τρωτό σημείο και ενεργοποιούνται οι διαδικασίες επαναφοράς στην κανονική λειτουργία, με βάση τα σχέδια του οργανισμού.

- Καταγραφής, αξιολόγησης και ανατροφοδότησης, το οποίο αναφέρεται συγκέντρωση, αποθήκευση και ανάλυση των πληροφοριών που περισυλλέγησαν κατά την αντιμετώπιση του συμβάντος για μελλοντική χρήση, προσαρμόζοντας και δημιουργώντας νέες διαδικασίες και

ελέγχους, με στόχο την ενίσχυση του οργανισμού. Αξιολόγηση των βημάτων και του αντίκτυπου κάθε διαδικασίας απόκρισης μπορούν να βελτιώσουν σημαντικά τις διαδικασίες, τους ελέγχους και τα υπάρχοντα σχέδια και να βοηθήσουν στην ανίχνευση αδυναμιών και τρωτών σημείων.

4.7: Μέτρα αντιμετώπισης και πρόληψης

Δεδομένου του αντίκτυπου των καταστροφών στη λειτουργία κάθε οργανισμού, κρίνεται απαραίτητη η λήψη μέτρων πρόληψης και ταχείας αντιμετώπισης των σημαντικότερων συνεπειών τους.

4.7.1: Μέτρα προστασίας πληροφορίας

Δημιουργία αντιγράφων ασφαλείας δεδομένων και εφαρμογών

Η ύπαρξη αντιγράφων ασφαλείας, δηλαδή επιπλέον αντιγράφων σημαντικών πληροφοριών, πόρων και εξοπλισμού, είναι απαραίτητη για την επιτυχημένη ανάκτηση χαμένης πληροφορίας. Τα πλάνα αντιμετώπισης ρίσκων πρέπει να λαμβάνουν υπόψη τους τόσο τις ανάγκες διατήρησης, ενημέρωσης, πρόσβασης, μεταφοράς και επαναφοράς των αντιγράφων, για τις περιπτώσεις που ζητηθεί. Σημαντικό κριτήριο κατά την επιλογή πολιτικής και τεχνολογιών αντιγραφής είναι ο χρόνος παραγωγής και αποκατάστασης και ο διαθέσιμος χώρος αποθήκευσης.

Τα διαφορετικά είδη αντιγράφων ασφαλείας πληροφοριών κατηγοριοποιούνται ως εξής:

- Πλήρη αντίγραφα ασφαλείας, τα οποία περιλαμβάνουν το σύνολο της πληροφορίας. Το μέγεθος των συγκεκριμένων αντιγράφων είναι πάντοτε το μέγιστο.

- Διαφορικά αντίγραφα ασφαλείας, τα οποία βασίζονται σε ένα τακτικά λαμβανόμενο πλήρες αντίγραφο ασφαλείας, και ένα σύνολο από αντίγραφα αποκλειστικά των αλλαγών που πραγματοποιήθηκαν από την πλέον πρόσφατη πλήρη αντιγραφή. Το μέγεθος των διαφορικών αντιγράφων συνεχώς αυξάνεται και μηδενίζεται κατά την τακτική πλήρη αντιγραφή.

- Σταδιακά αντίγραφα ασφαλείας, τα οποία, παρόμοια με τα διαφορικά, βασίζονται σε ένα τακτικά λαμβανόμενο πλήρες αντίγραφο ασφαλείας, και ένα σύνολο από αντίγραφα αποκλειστικά των αλλαγών που πραγματοποιήθηκαν από την προηγούμενη σταδιακή καταγραφή. Το μέγεθος των σταδιακών αντιγράφων παραμένει σχετικά σταθερό.

Σημειώνεται ότι κατά τη διαδικασία επαναφοράς των διαφορικών αντιγράφων, απαιτείται η επαναφορά του πιο πρόσφατου πλήρους αντιγράφου και μετέπειτα του πιο πρόσφατου διαφορικού. Στην αντίστοιχη περίπτωση των σταδιακών αντιγράφων, μετά την επαναφορά του πιο πρόσφατου πλήρους αντίγραφου, απαιτείται η επαναφορά όλων των διαθέσιμων σταδιακών. Επίσης, η πολιτική απομακρυσμένης καταγραφής (remote journaling) επιτρέπει την ταυτόχρονη αποθήκευση δεδομένων σε πάνω από μία τοποθεσίες, ώστε να υπάρχει οποιαδήποτε στιγμή τουλάχιστον ένα πλήρως ενημερωμένο και διαθέσιμο αντίγραφο.

Κρυπτογράφηση δεδομένων

Η χρήση ελέγχων κρυπτογράφησης των δεδομένων, τόσο κατά την μεταφορά τους μέσω διαύλων, στα πλαίσια της επικοινωνίας, όσο και κατά την παραμονή τους στα συστήματα του οργανισμού, αποτελεί τον αποτελεσματικότερο τρόπο διασφάλισης της εμπιστευτικότητας της πληροφορίας. Βασισμένες σε αρχές κρυπτογραφίας, η αξιοποίηση των ψηφιακών υπογραφών επιτρέπει επιβεβαίωση της ακεραιότητας και αυθεντικότητας των δεδομένων. Παράλληλα, μπορούν να χρησιμοποιηθούν ψηφιακά πιστοποιητικά από τις υπηρεσίες απόδοσης ευθύνης, οι οποίες επιβεβαιώνουν την πραγματοποίηση των δραστηριοτήτων και τη συνεισφορά των καταγεγραμμένων ατόμων.

Η επιλογή του επιπέδου προστασίας και των πληροφοριών προς κρυπτογράφηση εξαρτάται από τις ανάγκες και πολιτικές του οργανισμού, λαμβάνοντας υπόψη την αύξηση των απαιτήσεων πόρων και χρόνου επεξεργασίας ανάλογα με την ασφάλεια. Σημειώνεται ότι οι ρόλοι και ευθύνες κάθε ομάδας πρέπει να είναι με ακρίβεια ορισμένοι και κατανοητοί, ώστε να αποφευχθούν παρανοήσεις. Επίσης, δεν πρέπει να αμεληθεί η ανάγκη ύπαρξης αντιγράφων και προσεκτικής διαχείρισης των κρυπτογραφικών κλειδιών, ώστε να ελαχιστοποιηθούν οι κίνδυνοι μη εξουσιοδοτημένης πρόσβασης και απώλειας πληροφοριών.

Ακόμη, αξίζει ιδιαίτερη αναφορά στις νέες τεχνολογίες ομομορφικής κρυπτογράφησης, οι οποίες επιτρέπουν την εκτέλεση υπολογισμών σε κρυπτογραφημένα δεδομένα, χωρίς την αποκρυπτογράφησή τους, θεωρητικά εξαλείφοντας πλήθος κινδύνων ασφάλειας των αποθηκευμένων δεδομένων.

4.7.2: Μέτρα εξασφάλισης πόρων

Εναλλακτικές εγκαταστάσεις

Οι εναλλακτικές εγκαταστάσεις μπορεί να αφορούν εγκαταστάσεις του ίδιου του οργανισμού, ενοικίαση χώρου από κάποιο τρίτο μέρος ή χώρους διαθέσιμους λόγω συνεργασίας με άλλους οργανισμούς. Είναι σημαντικό να διασφαλίζεται ότι οι εναλλακτικές εγκαταστάσεις διαθέτουν τους απαραίτητους πόρους, την υποδομή, τον εξοπλισμό και την πληροφορία που απαιτείται για την ομαλή λειτουργία του οργανισμού, στο βαθμό που επιτρέπει η προσέγγιση προετοιμασίας που επιλέγεται. Πιο συγκεκριμένα, οι εγκαταστάσεις χαρακτηρίζονται:

- «Καυτές» ή γρήγορης επαναφοράς, αν διαθέτουν ό,τι χρειάζεται για να αντικαταστήσουν τις κύριες εγκαταστάσεις. Πρόκειται για την πιο ακριβή προσέγγιση, από άποψη κατανάλωσης πόρων, καθώς διατηρούνται διπλές διαδικασίες, εγκαταστάσεις και δεδομένα. Η καθυστέρηση μέχρι την πλήρη λειτουργικότητα είναι πολύ μικρή ή μηδενική, αν διατηρούνται συγχρονισμένες πληροφορίες ή λειτουργούν και υπό κανονικές συνθήκες.

- «Ζεστές» ή ενδιάμεσης επαναφοράς, αν διαθέτουν ένα μέρος της υποδομής, αλλά λείπει εξοπλισμός και δεδομένα. Το κόστος διατήρησης είναι σημαντικά μικρότερο, αλλά υπάρχει κόστος για εξόπλιση και ο χρόνος για πλήρη λειτουργία είναι σημαντικός, σε σχέση με τις «καυτές» εγκαταστάσεις.

- «Κρύες» ή σταδιακής επαναφοράς, αν διαθέτουν αποκλειστικά τα απαραίτητα, όπως τροφοδοσία ρεύματος. Εμφανίζουν το μικρότερο κόστος διατήρησης, αλλά το μεγαλύτερο κόστος εξόπλισης και χρονικό διάστημα για να προετοιμαστούν για λειτουργία. Συχνά,

χρησιμοποιούνται συμπληρωματικά, με ταυτόχρονη αξιοποίηση εγκαταστάσεων με μεγαλύτερο βαθμό προετοιμασίας.

Στα πλαίσια της επιλογής υποδομής, η πρόβλεψη χώρων ξεκούρασης, υγιεινής και διαδικασιών σίτισης του προσωπικού είναι απαραίτητη για τη συνέχιση της ομαλής λειτουργίας του οργανισμού σε περιπτώσεις αποκλεισμού. Εξωτερικοί συνεργάτες μπορούν να συνεισφέρουν σε αυτό, λαμβάνοντας πάντα υπόψη την πιθανότητα να μην είναι δυνατή η λειτουργία τους λόγω της καταστροφής.

Εξασφάλιση σημαντικών πόρων

Η διατήρηση λειτουργικών, συντηρημένων και ικανοποιητικής ισχύος γεννητριών και καυσίμων είναι απαραίτητη για τη διασφάλιση της ηλεκτροδότησης των εγκαταστάσεων του οργανισμού μετά από κάποια καταστροφή. Χωρίς ρεύμα, τόσο οι διαδικασίες αποκατάστασης, όσο και η κρίσιμες λειτουργίες του οργανισμού είναι απίθανο να μπορούν να συνεχίσουν. Παράλληλα, εξοπλισμός προστασίας από υπερτάσεις και υποτάσεις μπορεί να προστατεύσει ευαίσθητο εξοπλισμό από βλάβες του δικτύου. Επίσης, δεξαμενές νερού και αποθηκευμένη ξηρά τροφή μπορούν να αποβούν απαραίτητες σε περίπτωση ανάγκης, εφόσον καταρρεύσουν αναγκαίες υποδομές και αποκλειστεί η πρόσβαση στις εγκαταστάσεις. Αντίστοιχα, είναι χρήσιμη η πρόβλεψη εναλλακτικών μεθόδων θέρμανσης και ψύξης, είτε βασιζόμενες σε ηλεκτρικό ρεύμα, είτε στην καύση χημικών καυσίμων.

Συνεργασία με άλλους οργανισμούς

Δεδομένου του κόστους και της σημασίας των δραστηριοτήτων των πλάνων αποκατάστασης καταστροφών, η σύναψη συμφωνιών με άλλους οργανισμούς παρόμοιων τεχνολογιών και μεγέθους, συντελούν σε επιμερισμό του ρίσκου και οικονομικού αντίκτυπου της προετοιμασίας και της αντιμετώπισης σοβαρών γεγονότων. Ανάλογα με την ευρύτητά τους, σημειώνονται οι παρακάτω κατηγορίες:

Συμφωνίες αμοιβαίας βοήθειας

Οι συμφωνίες αμοιβαίας βοήθειας αποτελούν την ευρύτερη και πιο ευέλικτη επιλογή συνεργασίας μεταξύ οργανισμών. Στα πλαίσια τους, δύο ή περισσότεροι οργανισμοί, οπότε αναφερόμαστε σε κοινοπραξία οργανισμών, με παρόμοιες διαδικασίες και χρήση συμβατών τεχνολογιών συμφωνούν στην αλληλοϋποστήριξη και παροχή πόρων σε περίπτωση σοβαρού συμβάντος. Σημειώνεται η σημασία προσεκτικής ανάλυσης των όρων της συμφωνίας και εξασφάλισης και επιβεβαίωσης της δυνατότητας χρήσης των συμφωνηθέντων στοιχείων, χωρίς διακοπή των κύριων δραστηριοτήτων των οργανισμών που συμμετέχουν. Η αξιολόγηση των δυνατοτήτων υποστήριξης αυξημένου φόρτου από την υποδομή, τον εξοπλισμό και τις διαδικασίες των οργανισμών είναι καταλυτικής σημασίας για την επιτυχημένη αντιμετώπιση των κρίσεων και απαιτούνται τακτικές δοκιμές προς επιβεβαίωση της συμβατότητας και επιδιόρθωσης των προβλημάτων που εντοπίζονται και εξασφάλιση της προστασίας των δεδομένων κάθε οργανισμού κατά τη διάρκεια της από κοινού χρήσης των πόρων, λαμβάνοντας υπόψη τους νομικούς και λοιπούς περιβαλλοντικούς περιορισμούς. Ακόμη, απαιτείται να τεθούν όρια ελάχιστης και μέγιστης απόστασης μεταξύ των εγκαταστάσεων, προς περιορισμό, αντίστοιχα, της πιθανότητας να επηρεαστούν από τις ίδιες καταστροφές και του χρόνου μεταφοράς.

Συμφωνίες επεξεργασίας

Ούσες πιο περιορισμένες από τις συμφωνίες αμοιβαίας υποστήριξης, οι συμφωνίες επεξεργασίας αναφέρονται στην συνεργασία στα πλαίσια παρόμοιων τεχνολογιών και υποδομών πληροφορικής, με στόχο τη συνέχιση των διαδικασιών επεξεργασίας δεδομένων ενός οργανισμού που επλήγη από κάποια καταστροφή. Παρόμοια με τις προαναφερθείσες, είναι σημαντική η συμβατότητα των συστημάτων και η επιβεβαίωση των δυνατοτήτων διαχείρισης αυξημένου φόρτου.

Αμοιβαία κέντρα

Παρόμοια με τις προαναφερθείσες συμφωνίες, η διατήρηση αμοιβαίων κέντρων αναφέρεται στην από κοινού αξιοποίηση εγκαταστάσεων, εφόσον κριθεί απαραίτητο. Η σύναψή τους αφορά μη άμεσους ανταγωνιστές και οργανισμούς από διαφορετικούς κλάδους, με συμβατές ανάγκες υποδομών.

Εφεδρικά πλάνα προμηθειών

Για την κάλυψη του ενδεχόμενου αποτυχίας κάποιου συνεργάτη ή της εφοδιαστικής αλυσίδας του οργανισμού, υπάρχει η δυνατότητα σύναψης συμφωνιών για εναλλακτική τροφοδοσία. Σημειώνεται ότι το παθητικό κόστος εν αναμονή του συμβάντος είναι συχνά μη αμελητέο και ότι παρουσιάζεται καθυστέρηση πριν την ενεργοποίηση της συνεργασίας, η οποία πρέπει να ληφθεί υπόψη. Ακόμη, είναι σημαντικό να επιβεβαιώνεται ότι οι κύριοι και εναλλακτικοί συνεργάτες και προμηθευτές δεν επηρεάζονται από τις ίδιες περιστάσεις και σημεία αποτυχίας.

Εναλλακτικοί πάροχοι υπηρεσιών

Κατόπιν συμφωνιών, ο οργανισμός μπορεί να συνεργαστεί με εναλλακτικούς παρόχους υπηρεσιών, όπως γραφεία εξυπηρέτησης, τα οποία αναλαμβάνουν την κάλυψη των αναγκών επικοινωνίας σχετικά με τις υπηρεσίες πληροφορικής. Πρόκειται για τρίτα μέρη, τα οποία παρέχουν τις υπηρεσίες τους σε περίπτωση ανάγκης, είτε συνεισφέροντας στη διαδικασία αποκατάστασης, είτε υποστηρίζοντας τις εφεδρικές διαδικασίες λειτουργίας. Παρόμοια με τις συμφωνίες επιμερισμού ρίσκου, το τρίτο μέρος έχει περίσσεια χωρητικότητα την οποία διαθέτει στον οργανισμό ή επεκτείνει τη λειτουργία του.

Χρήση τεχνολογιών συννέφου

Οι τεχνολογίες συννέφου συνεισφέρουν δραματικά στις διαδικασίες αποκατάστασης. Οι πάροχοι των πόρων παρέχουν εγγυήσεις διαθεσιμότητας

και εξασφαλίζουν επιμερισμό και οριακά εξάλειψη ρίσκων που σχετίζονται με τον εξοπλισμό πληροφορικής που διαθέτουν. Παράλληλα, αξιοποιώντας τεχνολογίες εικονοποίησης, η αποκατάσταση των υπηρεσιών γίνεται με σημαντικά μεγαλύτερη ταχύτητα και μικρότερο κόστος, χρησιμοποιώντας προετοιμασμένες και ρυθμισμένες εικονικές μηχανές. Η υποδομή που επιλέγεται να διατηρείται στο σύννεφο στα πλαίσια των διαδικασιών αποκατάστασης καταστροφών μπορεί να βασίζεται σε «κρύους», «ζεστούς» ή «καυτούς» πόρους. Ανάλογα με τους διαθέσιμους πόρους, η διατήρηση αντιγράφων ασφαλείας στο σύννεφο είναι πιθανή επιλογή, με υψηλότερο όμως οικονομικό κόστος και χρόνο επαναφοράς από εναλλακτικές. Παράλληλα, η εικονοποίηση παρέχει απομονωμένα περιβάλλοντα για δοκιμές με υψηλότερη ασφάλεια.

Σημειώνεται ότι οι ανερχόμενες τεχνολογίες υβριδικού συννέφου προσφέρουν ευκολότερη διαχείριση και μεγαλύτερη ευελιξία στη συνδυαστική χρήση διαφορετικών παρόχων και ευκολότερη συμμόρφωση με τα εκάστοτε νομικά πλαίσια προστασίας δεδομένων, λόγω της δυνατότητας αξιοποίησης τόσο δημόσιων, όσο και ιδιωτικών πόρων. Ακόμη, περιορίζουν σημαντικά το ρίσκο αποτυχίας του εξοπλισμού κάποιου προμηθευτή, αλλά και το κόστος τεχνολογικής εξάρτησης από ένα συγκεκριμένο οργανισμό.

Τηλε-εργασία

Αξιοποιώντας τις σύγχρονες τεχνολογίες και υπηρεσίες επικοινωνίας, η εξ αποστάσεως εργασία αποτελεί ελκυστική επιλογή για τους εργαζομένους και απαραίτητη προϋπόθεση για την επιβίωση των οργανισμών κατά τη διάρκεια κρίσεων, οι οποίες δεν επιτρέπουν την παρουσία και εργασία του ανθρώπινου δυναμικού στις κύριες εγκαταστάσεις. Με τη χρήση λογισμικού ασύγχρονης και σύγχρονης επικοινωνίας, τηλε-διασκέψεων και υπηρεσιών συντονισμού του έργου, των ομάδων και των διαδικασιών οργάνωσης των ανθρώπινων πόρων, η πλειονότητα των οργανισμών μπορεί να λειτουργήσει ικανοποιητικά, χωρίς φυσική παρουσία του προσωπικού.

Η τηλε-εργασία παρουσιάζει ιδιαίτερες δυσκολίες, οι οποίες είναι σημαντικό να ληφθούν υπόψη. Παρά τις δυνατότητες ασύγχρονης και σύγχρονης επικοινωνίας, λόγω της αυξημένης πολυπλοκότητας, συχνά, η απόδοση. επικοινωνία και συνεργασία των ομάδων υποβαθμίζονται. Ανάλογα με την περίπτωση, η ισορροπία εργασίας και προσωπικής ζωής μπορεί να επιδεινωθεί, με αρνητικές συνέπειες στους υπαλλήλους. Επίσης, η φυσική απομόνωση των υπαλλήλων μπορεί να επιδράσει αρνητικά τη ψυχολογία τους και την προσωπική τους εξέλιξη. Παράλληλα, η διαχείριση των ομάδων εξ αποστάσεως εμφανίζει μεγαλύτερη δυσκολία και απαιτεί περισσότερο χρόνο από τους υπεύθυνους (Donnelly & Proctor-Thomson, 2015).

Εναλλακτικοί δίαυλοι επικοινωνίας

Δεδομένων των συχνών πλήξεων της υποδομής επικοινωνιών κατά τη διάρκεια καταστροφικών γεγονότων και της κρισιμότητά της, η ύπαρξη εναλλακτικών για τη διασφάλιση απρόσκοπτης επικοινωνίας κρίνεται καθοριστική για τη συνέχιση της λειτουργίας του οργανισμού. ΄Υπαρξη εναλλακτικού παρόχου υπηρεσιών διαδικτύου, εφεδρικής καλωδίωσης και η αξιοποίηση ασύρματων τηλεφωνικών δικτύων και τεχνολογιών διασύνδεσης 4G και 5G ή ακόμη και δορυφορικών συνδέσεων για κρίσιμες ανταλλαγές πληροφορίας μπορεί να επιτρέψει την ομαλή ανταλλαγή πληροφοριών.

Προστασία πόρων εκ των προτέρων

Ειδικά σε περιοχές με εποχιακές καταστροφές, αλλά και στην περίπτωση έγκαιρης ειδοποίησης για επερχόμενη ή πιθανή καταστροφή, όπως τυφώνες ή ακραίες βροχοπτώσεις με σημαντική πιθανότητα πλημμύρας, διαδικασίες προστασίας του εξοπλισμού μπορούν να συνεισφέρουν σημαντικά στην αποκατάσταση και να εξοικονομήσουν χρόνο και κόστος επαναφοράς.

Ανάλογα με τη φύση της καταστροφής, η μεταφορά κρίσιμου εξοπλισμού σε ασφαλείς εγκαταστάσεις κρίνεται σημαντική. Επίσης, στην προστασία από το νερό συνεισφέρει η απομάκρυνσή του ηλεκτρονικού εξοπλισμού από το

έδαφος, η μεταφορά του σε δωμάτια χωρίς παράθυρα, η κατασκευή προσωρινών παραπετασμάτων ή περιτύλιξή του με πλαστικά υλικά και η χρήση αδιάβροχων δοχείων.

Σαφείς αρμοδιότητες και ιεραρχία διαδοχής κρίσιμων ρόλων

Κατά τις διαδικασίες αποκατάστασης, οι υπάλληλοι του οργανισμού διαδραματίζουν σημαντικό ρόλο και η αποδοτικότητα της επικοινωνίας επηρεάζει σημαντικά το χρόνο ολοκλήρωσης των διαδικασιών. Είναι απαραίτητο για την ομαλή επαναφορά των συνθηκών κανονικής λειτουργίας το κάθε μέρος του συνόλου να γνωρίζει και επιτελέσει τους ρόλους που του έχουν ανατεθεί, αλλά και την αλυσίδα ευθύνης και αναφοράς, τα άτομα δηλαδή στα οποία θα μπορεί να απευθύνεται για κάθε περίσταση.

Ακόμη, είναι σημαντική η ύπαρξη σαφούς ιεραρχίας διαδοχής κρίσιμων ρόλων, ώστε βασικές αρμοδιότητες διοίκησης και διαχείρισης να μπορούν να καλυφθούν και χρήσιμες γνώσεις και εμπειρία να είναι διαθέσιμες από το επόμενο άτομο, σε περίπτωση που λόγω της ίδιας της καταστροφής, κάποιου ατυχήματος ή προσωπικής συγκυρίας δεν είναι μέρος του προσωπικού διαθέσιμο.

4.7.3: Περιορισμός οικονομικού αντίκτυπου

Διαφοροποίηση

Η διαφοροποίηση αποτελεί την πιο διαδεδομένη πρακτική περιορισμού του ρίσκου. Μπορεί να εφαρμοστεί σε διάφορους τομείς με διαφορετικά αποτελέσματα.

Γεωγραφική διαφοροποίηση των δραστηριοτήτων του οργανισμού επιτρέπει τη συνεχιζόμενη λειτουργία του, ακόμη και αν κάποια περιοχή στην οποία δραστηριοποιείται πληγεί από τοπικές καταστροφές, με αποτέλεσμα

παρατεταμένη διακοπή εργασιών. Η οικονομική διαφοροποίηση των δραστηριοτήτων του οργανισμού επιτρέπει μεγαλύτερη ανοχή οικονομικών ταραχών και μεγαλύτερης κλίμακας καταστροφών, οι οποίες ανατρέπουν το επιχειρηματικό πλάνο του ή αποτρέπουν την ομαλή λειτουργία σε μεγαλύτερες γεωγραφικά περιοχές.

Ασφάλιση

Η συνεργασία με κάποιον ασφαλιστικό φορέα αποτελεί επίσης, συνηθισμένη τακτική περιορισμού του ρίσκου κάποιας δραστηριότητας. Κατόπιν κατάλληλης τεχνοοικονομικής μελέτης, η οποία δικαιολογεί το αυξημένο κόστος, σε περίπτωση κάποιας καταστροφής περιορίζεται σημαντικά το οικονομικό της αντίκτυπο, με την παροχή κεφαλαίων για την επιδιόρθωση ή αντικατάσταση των εγκαταστάσεων και των πόρων που απαιτούνται για τη λειτουργία του οργανισμού.

Διάδοση λύσεων αποκατάστασης καταστροφών

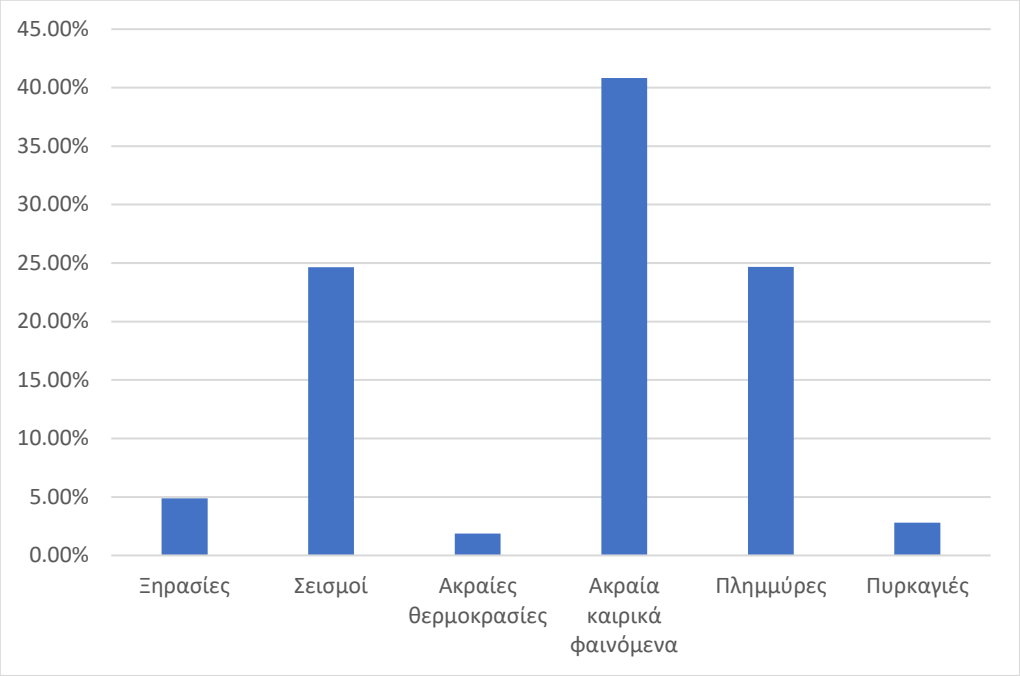
Τα στοιχεία γύρω από την εφαρμογή των λύσεων πρόληψης και αποκατάστασης καταστροφών κρίνονται ελλιπή. Το 2016, οι μεσαίες και μεγάλες επιχειρήσεις στις Ηνωμένες Πολιτείες είχαν επιλέξει τα αντίγραφα δεδομένων σε εναλλακτικές εγκαταστάσεις (40%), τη χρήση αντιγράφων ασφαλείας στο σύννεφο (13%), τη χρήση εναλλακτικής υποδομής στο σύννεφο (25%) και τη διατήρηση εναλλακτικών εγκαταστάσεων άμεσης (16%) και καθυστερημένης επαναφοράς (15%) (Statista, 2016). Αντίστοιχα, οι οργανισμοί χωρίς λύσεις εναλλακτικών εγκαταστάσεων ή υποδομών το απέφευγαν λόγω κόστους (52%), έλλειψης πληροφοριακών πόρων (29%) ή δεν γνώριζαν την ύπαρξη των σχετικών διαδικασιών ή τις θεωρούσαν ήσσονος σημασίας (55%) (Statista, 2016).

4.8: Συνήθεις καταστροφές

Απρόοπτες φυσικές καταστροφές μπορούν να πλήξουν άμεσα τις εγκαταστάσεις, τους πόρους και τα οικονομικά του οργανισμού. Επίσης, η συχνότητα των κυβερνοεπιθέσεων αυξάνεται συνεχώς, με δραματικές επιπτώσεις στα οικονομικά των οργανισμών και στη λειτουργίας τους γενικότερα. Κατάλληλη προετοιμασία μπορεί να περιορίσει σημαντικά το αντίκτυπο των καταστροφών και γνώση εκ των προτέρων των πιθανότερων προβλημάτων που προκύπτουν αυξάνουν την αποτελεσματικότητα, ταχύτητα και απόδοση των λύσεων.

Στις πιο συνηθισμένες φυσικές καταστροφές εντοπίζονται οι πλημμύρες και τα ακραία ατμοσφαιρικά φαινόμενα (ανεμοστρόβιλοι, τυφώνες και θύελλες), αποτελώντας το 42% και 30%, αντίστοιχα, των συνολικών φυσικών καταστροφών, το διάστημα 1990-2019 (Institute for Economics & Peace, 2019).

Το οικονομικό αντίκτυπο ανά κατηγορία καταστροφών ποικίλει. Αξιοσημείωτα, το διάστημα 1990-2019, το οικονομικό αντίκτυπο των ακραίων καιρικών φαινομένων ανήλθε στο 40,8% των συνολικών απωλειών, έναντι του 24,7% από πλημμύρες, 24,7% από σεισμούς. Επίσης, σημειώνεται ότι κατά μέσο όρο, στο διάστημα 2016-2019, οι ετήσιες οικονομικές απώλειες από φυσικές καταστροφές ανήλθαν στα 125 δισεκατομμύρια δολάρια.



Διάγραμμα 19 - Ποσοστό συνολικών οικονομικών απωλειών ανά κατηγορία μεγάλων καταστροφών, το διάστημα 1990-2019

Σεισμοί

Οι σεισμοί αποτελούν από τις συχνότερα εμφανιζόμενες καταστροφές, ειδικά σε σεισμογενείς περιοχές. Λόγω των πολύ περιορισμένων δυνατοτήτων πρόβλεψης και έγκαιρης προειδοποίησης, έχουν σημαντικές επιπτώσεις, ανάλογες της ισχύος και τοποθεσίας τους. Στις συχνότερες συμπεριλαμβάνονται η απώλεια ανθρώπινων ζωών, η καταστροφή εγκαταστάσεων και εξοπλισμού, και η καταστροφή υποδομών ηλεκτροδότησης, ύδρευσης, μετακίνησης και επικοινωνιών.

Πλημμύρες

Οι πλημμύρες αποτελούν συχνά επακόλουθο σημαντικών βροχοπτώσεων και άτακτης δόμησης, με αποτέλεσμα την υπερχείλιση ποταμών και την αποτυχία – εφόσον υπάρχουν – των υποδομών απορροής και διαχείρισης όμβριων υδάτων. Στις συχνότερες επιπτώσεις τους συμπεριλαμβάνονται η καταστροφή του δικτύου ύδρευσης, η διάδοση μολυσμένων υδάτων, η καταστροφή

εγκαταστάσεων, ο αποκλεισμός ή σημαντικός περιορισμός των δυνατοτήτων μετακίνησης, η καταστροφή των υποδομών μετακίνησης και τα επακόλουθα προβλήματα στις αλυσίδες μεταφοράς. Λόγω της φύσης της καταστροφής, η απομάκρυνση του νερού είναι απαραίτητη πριν από οποιαδήποτε διαδικασία αποκατάστασης.

Πυρκαγιές

Πυρκαγιές προκαλούνται συχνά από βλάβη εξοπλισμού, ανθρώπινο λάθος και ακραίες καιρικές συνθήκες. Ανάλογα με την έκταση της φωτιάς, στις συχνότερες επιπτώσεις των πυρκαγιών περιλαμβάνονται η απώλεια ανθρώπινων ζωών, η σημαντική υποβάθμιση της ποιότητας του αέρα, η καταστροφή εγκαταστάσεων και εξοπλισμού – τόσο από την ίδια την φωτιά, όσο και από την πυρόσβεση - και ο αποκλεισμός ή οι δυσκολίες μετακίνησης. Αντίστοιχα με παραπάνω, εκτός από συντρίμμια, συχνά ή στάχτη και τα καμένα υλικά απαιτούν απομάκρυνση πριν τις λοιπές διαδικασίες αποκατάστασης.

Ανεμοστρόβιλοι και τυφώνες

Οι ανεμοστρόβιλοι, αντίστοιχα με τους σεισμούς, δεν επιδέχονται πρόβλεψης, αλλά ούτε και έγκαιρης προειδοποίησης, με δραματικές συνέπειες. Αντίθετα, οι τυφώνες εντοπίζονται γρήγορα και παρακολουθούνται συνεχώς, αλλά παρουσιάζουν σημαντικά μεγαλύτερη ένταση.

Στις συχνότερες επιπτώσεις εντοπίζονται η καταστροφή των υποδομών ηλεκτροδότησης, ύδρευσης, μετακίνησης και επικοινωνιών, η καταστροφή εγκαταστάσεων και εξοπλισμού, η μόλυνση των δεξαμενών ύδρευσης και σημαντικά συντρίμμια σε μεγάλες εκτάσεις.

Σημαντικές χιονοπτώσεις και παγετός

Χειμερινές καιρικές συνθήκες υψηλής έντασης δημιουργούν όλο και συχνότερα προβλήματα, στα οποία περιλαμβάνονται η καταστροφή του δικτύου ύδρευσης

και ηλεκτροδότησης, η καταστροφή εγκαταστάσεων από επακόλουθες πλημμύρες και ο αποκλεισμός ή σημαντικές δυσκολίες μετακίνησης. Αντίστοιχα με παραπάνω, πριν τις λοιπές διαδικασίες αποκατάστασης απαιτείται η αφαίρεση του χιονιού, ιδιαίτερα από ανοιχτές, εκτεθειμένες εκτάσεις.

Κακόβουλο λογισμικό

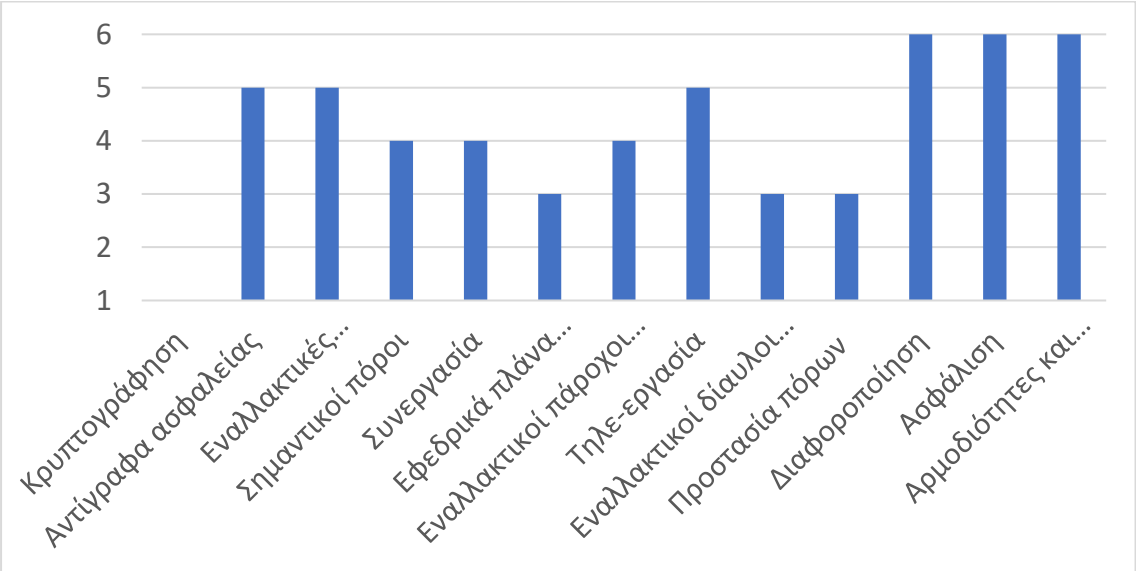
Όλο και συχνότερα, λόγω της επικράτησης τεχνολογικών μέσων που επηρεάζουν το συνολικό της λειτουργίας του οργανισμού, τα πληροφοριακά συστήματα γίνονται συχνά στόχος κακόβουλων παραγόντων. Οι τελευταίοι, στοχεύοντας συνήθως σε οικονομικές απολαβές, εισβάλουν στο δίκτυο του οργανισμού, εκμεταλλευόμενοι κενά ασφαλείας συστημάτων και συμπεριφορές υπαλλήλων, συνεργατών και προμηθευτών. Μετέπειτα, με υποκλοπή δεδομένων ή κρυπτογράφηση των υπαρχόντων, εκβιάζουν τον οργανισμό με το ενδεχόμενο διαρροής ή απώλειας των πληροφοριών. Με τη χρήση κρυπτογράφησης στα στάσιμα δεδομένα και τις επικοινωνίες του οργανισμού εξαλείφεται ο κίνδυνος υποκλοπής, ενώ τακτικά αντίγραφα ασφαλείας καθιστούν άνευ ουσίας την απειλή της κακόβουλης κρυπτογράφησης.

Παρακάτω, παρουσιάζονται σχεδιαγραμματικά τα κυριότερα αντίμετρα ανά συνήθη καταστροφή.

Συμβάν	Αντίμετρα				
	Εναλλακτικές εγκαταστάσεις	Σημαντικοί πόροι	Συνεργασία	Εφεδρικά πλάνα προμηθειών	Εναλλακτικοί πάροχοι υπηρεσιών
Σεισμοί	X	X	X	X	X
Πλημμύρες	X	X	X		X
Πυρκαγιές	X		X		X
Ανεμοστρόβιλοι και τυφώνες	X	X	X	X	X
Χιονοπτώσεις και παγετός	X	X		X	
Κακόβουλο λογισμικό					

Συμβάν	Αντίμετρα				
	Τηλε-εργασία	Εναλλακτικοί δίαυλοι επικοινωνίας	Προστασία πόρων εκ των προτέρων	Κρυπτογράφηση	Αντίγραφα ασφαλείας
Σεισμοί	X	X			X
Πλημμύρες	X		X		X
Πυρκαγιές	X				X
Ανεμοστρόβιλοι και τυφώνες	X	X	X		X
Χιονοπτώσεις και παγετός	X	X	X		
Κακόβουλο λογισμικό				X	X

Σημειώνεται ότι τα οικονομικά αντίμετρα της διαφοροποίησης και ασφάλισης αναφέρονται σε οποιοδήποτε οικονομικό πλήγμα, και συνδυαστικά με τον προσδιορισμό σαφών αρμοδιοτήτων και ιεραρχίας διαδοχής, αναφέρονται σε όλες τις πιθανές καταστροφές.



Διάγραμμα 20 - Αριθμός καταστροφών που μετριάζονται ανά αντίμετρο

Κεφάλαιο 5: Συμπεράσματα

Η συχνότητα και το αντίκτυπο των παραβιάσεων ασφαλείας και των καταστροφικών γεγονότων κρίνονται ιδιαίτερα σημαντικά μεγέθη και χρίζουν κατάλληλης προετοιμασίας και διαχείρισης από κάθε οργανισμό. Η αυξητικές τάσεις, δε, των παραπάνω προοικονομούν τη μεγαλύτερη σημασία που αποκτά η ορθή προετοιμασία για την αντιμετώπιση των προκλήσεων του παρόντος και του μέλλοντος.

Η ύπαρξη δομημένων προσεγγίσεων και οργανωτικών συστημάτων διευκολύνει σημαντικά τη θέση και λειτουργία διαδικασιών και πόρων προς αποτελεσματικότερη διαχείριση των κρίσεων που προκύπτουν από κυβερνοεπιθέσεις και φυσικές και ανθρώπινες καταστροφές.

Ολοκληρωμένες λύσεις διαχείρισης της ασφάλειας των πληροφοριών και διεθνή πρότυπα παρέχουν πλήθος πλαισίων και συγκεκριμένων προτάσεων, με στόχο την εξοικονόμηση πόρων και την υψηλότερη απόδοση των διαδικασιών ασφαλείας. Η πιστοποίηση της ορθής εφαρμογής των τελευταίων από φορείς πιστοποίησης με εξειδίκευση στις απαιτούμενες διαδικασίες συνεισφέρει τόσο στην επιβεβαίωση, επιδιόρθωση και βελτίωση των διαδικασιών αντιμετώπισης, όσο και στην υπόληψη του οργανισμού, από το μέρος των πελατών, των συνεργατών και των προμηθευτών.

Η ύπαρξη πλάνων επιχειρηματικής συνέχισης και αποκατάστασης καταστροφών μπορεί να αποβεί καθοριστική για τη βιωσιμότητα του οργανισμού, στην περίπτωση κάποιας αρνητικής συγκυρίας. Αξιοποιώντας τα πορίσματα των αναλύσεων επιχειρηματικού αντίκτυπου, με αποτελεσματική διαχείριση του ρίσκου, και συνεχή αξιολόγηση και βελτίωση των σχεδίων αντιμετώπισης των απειλών του οργανισμού, καθιστάται δυνατή η αποτελεσματική διαχείριση των συμβάντων, ο περιορισμών των αρνητικών τους επιπτώσεων και ενδεχομένως, η αξιοποίηση απρόσμενων ευκαιριών του περιβάλλοντος.

5.1: Προτάσεις για το Μέλλον

Η θεωρητική ανάλυση των ζητημάτων των κυβερνοαπειλών και των καταστροφών αποτελεί μια εποπτική παρουσίαση των βασικών εννοιών και απαραίτητων διαδικασιών. Δεδομένης της πολυπλοκότητας του σύγχρονου περιβάλλοντος, οι τομείς μπορούν να εξεταστούν σε διακριτές αναλύσεις για περεταίρω εμβάθυνση.

Τονίζεται ότι ιδιαίτερα το ζήτημα της κυβερνοασφάλειας, δεδομένου του αντίκτυπου και της αυξανόμενης συχνότητας σχετικών επιθέσεων τη σύγχρονη εποχή, αποτελεί αξιοσημείωτο πεδίο που χρήζει ξεχωριστής ανάλυσης και αντιμετώπισης.

Ακόμη, η ταχύτητα της τεχνολογικής εξέλιξης και νέες οικονομίες κλίμακας καθιστούν, σε μικρότατα χρονικά διαστήματα, κάθε αναφορά στην αξιοποίηση τεχνολογικών μέσων της εποχής παρωχημένη. Λαμβάνοντας υπόψη τις εμπορικά διαθέσιμες δυνατότητες κάθε περιόδου, τακτική ανανέωση των συγκεκριμένων προτάσεων κρίνεται αναγκαία.

Παράλληλα, η έλλειψη ευρέως διαθέσιμων λεπτομερών δεδομένων σχετικά με τις χρησιμοποιούμενες διαδικασίες συνέχισης των υπηρεσιών και διαχείρισης καταστροφών, λόγω του κόστους σχεδίασης και εφαρμογής, αλλά και ιδιωτικότητας των λεπτομερειών λειτουργίας των οργανισμών καθιστούν δύσκολη τη ποιοτική αξιολόγηση των εφαρμοσμένων προτύπων και υιοθετημένων διαδικασιών. Ταυτόχρονα, η έλλειψη δεδομένων σχετικά με την πρακτική απόδοση των οργανωτικών συστημάτων σε περιπτώσεις καταστροφών, λόγω ιδιωτικότητας, έλλειψης ουσιαστικού σχεδιασμού και της - ακόμη - μικρής συχνότητας των καταστροφικών γεγονότων εμποδίζει την ποσοτική σύγκριση των εφαρμοσμένων λύσεων. Η αυξανόμενη σημασία που αρχίζει να επιδίδεται στις προαναφερθείσες διαδικασίες και η σύγχρονες ευκαιρίες μαζικής συγκέντρωσης και ανάλυσης δεδομένων μπορούν μελλοντικά να επιτρέψουν ενδιαφέρουσες ποσοτικές αναλύσεις.

Στα παραπάνω, αλλά και στην εξ αρχής δημιουργία ενός πρότυπου οργανωτικού συστήματος και πλάνων διαχείρισης καταστροφών και επιχειρηματικής συνέχισης μπορεί να συνεισφέρει σημαντικά η συνεργασία με κάποια εταιρία, η οποία θα διαθέσει πληροφορίες για τις επιμέρους διαδικασίες, πόρους και συστήματα που αξιοποιεί, στόχους, ανάγκες και λειτουργία, ώστε να ληφθούν υπόψη κατά τις διαδικασίες επιχειρηματικού αντίκτυπου και διαχείρισης ρίσκου και την ενδεικτική σχεδίαση των διαδικασιών διαχείρισης συμβάντων.

Βιβλιογραφία

Institute for Economics & Peace, 2019. *Global number of natural disasters increases ten times.* s.l.: Institute for Economics & Peace.

International Organization for Standardization, 2018. *ISO/IEC 27000:2018 Information technology — Security techniques — Information security management systems — Overview and vocabulary.* s.l.:s.n.

AXELOS, 2019. *ITIL Foundation ITIL 4 Edition.* s.l.:s.n.

bci, 2020. *BCI Horizon Scan Report 2020,* s.l.: s.n.

Blokdijk, G., Brewster, J. & Menken, I., 2008. *Disaster Recovery and Business Continuity IT Planning, Implementation, Management and Testing of Solutions and Services Workbook.* s.l.:s.n.

Calder, A. & Watkins, S., 2015. *IT governance : an international guide to data security and ISO27001/ISO27002.* s.l.:s.n.

Cisco, 2020. *Annual Internet Report (2018–2023),* s.l.: s.n.

Conger, K. & Frenkel, S., 2021. *Thousands of Microsoft Customers May Have Been Victims of Hack Tied to China.* s.l.:The New York Times.

Coronese, M. και συν., 2019. Evidence for sharp increase in the economic damages of extreme natural disasters. *PNAS,* 116(43).

CRED, D. Guha-Sapir, χ.χ. *EM-DAT: The Emergency Events Database.* Brussels: Université catholique de Louvain (UCL).

Davidoff, S., 2020. *Data Breaches Crisis and Opportunity.* s.l.:s.n.

Disaster recovery: reasons lacking an on-demand failover solution among U.S. companies, as of 2016, 2016. *Disaster recovery: reasons lacking an on-demand failover solution among U.S. companies, as of 2016.* [Ηλεκτρονικό] Available at: https://www.statista.com/statistics/642898/worldwide-disaster-recovery-no-on-demand-solution-reasons/

Donnelly, N. & Proctor-Thomson, S. B., 2015. Disrupted work: home-based teleworking (HbTW) in the aftermath of a natural disaster. *New Technology, Work and Employment.*

Dushie, D. Y., 2014. Business Continuity Planning: An Empirical Study of Factors that Hinder Effective Disaster Preparedness of Businesses. *Journal of Economics and Sustainable Development,* 5(27).

Eisensee & Strömberg, 2002. *Equal coverage casualties ratio.* s.l.:Eisensee; Strömberg.

Etkin, D. A., Mamuji, A. A. & Clarke, L., 2018. Disaster Risk Analysis Part 1: The Importance of Including Rare Events. *Journal of Homeland Security and Emergency Management.*

Gallia, A., 2020. *8 ITIL Processes for First-Class IT Service Management,* s.l.: process.st.

International Data Corporation, 2020. *IDC Expects 2021 to Be the Year of Multi-Cloud as Global COVID-19 Pandemic Reaffirms Critical Need for Business Agility.* s.l.:International Data Corporation.

International Organization for Standardization, 2013. *ISO/IEC 27001:2013 Information technology - Security techniques - Information security management systems - Requirements.* s.l.:s.n.

International Organization for Standardization, 2020. *THE ISO SURVEY OF MANAGEMENT SYSTEM STANDARD CERTIFICATIONS – 2019 –,* s.l.: s.n.

ISACA, 2018. *COBIT® 2019 FRAMEWORK: INTRODUCTION & METHODOLOGY.* s.l.:s.n.

Kenyon, B. & Humphreys, E., 2014. *Guide to the Implementation and Auditing of ISMS Controls based on ISO/IEC 27001.* s.l.:s.n.

Kim, D. & Solomon, M. G., 2018. *Fundamentals of information systems security.* s.l.:s.n.

McAfee, 2014. *Net Losses: Estimating the Global Cost of Cybercrime - Economic impact of cybercrime II.* s.l.:McAfee.

MCKAY, J., 2018. *Small Businesses Are a Vital Part of Community Resiliency but Often Overlook Vulnerabilities.* s.l.:government technology.

MERCER, 2020. *Business responses to the COVID-19 outbreak survey findings,* s.l.: s.n.

Morgan, S., 2020. *Cybercrime To Cost The World $10.5 Trillion Annually By 2025.* s.l.:Cybersecurity Ventures.

NOAA National Centers for Environmental Information (NCEI), 2021. *U.S. Billion-Dollar Weather and Climate Disasters.* s.l.:s.n.

Ozdemir, Y., Basligil, H., Alcan, P. & Kandemirli, B. M., 2014. EVALUATION AND COMPARISON OF COBIT, ITIL AND ISO27K1/2 STANDARDS WITHIN

THE FRAMEWORK OF INFORMATION SECURITY. *International Journal of Technical Research and Applications.*

Project Management Institute, 2017. *A guide to the project management body of knowledge (PMBOK guide).* s.l.:s.n.

Read, P. & Denniss, R., 2020. *With costs approaching $100 billion, the fires are Australia's costliest natural disaster.* s.l.:THE CONVERSATION.

ROBERTS, J. J. & LASHINSKY, A., 2017. *Hacked: How Business Is Fighting Back Against the Explosion in Cybercrime.* s.l.:FORTUNE.

Sanger, D. E., Perlroth, N. & Barnes, J. E., 2021. *As Understanding of Russian Hacking Grows, So Does Alarm.* s.l.:The New York Times.

SECHLER, B. & HAWKINS, L., 2021. *Winter storm damage may rival Hurricane Harvey1s price tag, experts say.* s.l.:Austin American-Statesman.

Statista, 2012. *How does your organization assess the efficiency and effectiveness of information security?.* [Ηλεκτρονικό] Available at: https://www.statista.com/statistics/259215/aassessment-of-efficiency-and-effectiveness-of-information-security-policies/

Statista, 2016. *Disaster recovery: reasons lacking an on-demand failover solution among U.S. companies, as of 2016.* [Ηλεκτρονικό] Available at: https://www.statista.com/statistics/642898/worldwide-disaster-recovery-no-on-demand-solution-reasons/

Statista, 2016. *Leading disaster recovery solutions employed by U.S. companies, as of 2016.* [Ηλεκτρονικό] Available at: https://www.statista.com/statistics/642884/worldwide-disaster-recovery-current-solutions-in-use/

Statista, 2016. *Share of companies and public administration which adopted the ISO 27000 requirements in Italy in 2016.* [Ηλεκτρονικό] Available at: https://www.statista.com/statistics/621203/adhesion-to-iso-27000-standards-in-italy/

Statista, 2021. *Amount of monetary damage caused by reported cyber crime to the IC3 from 2001 to 2020.* [Ηλεκτρονικό] Available at: https://www.statista.com/statistics/267132/total-damage-caused-by-by-cyber-crime-in-the-us/

Statista, 2021. *Public cloud services end-user spending worldwide from 2017 to 2022.* [Ηλεκτρονικό] Available at: https://www.statista.com/statistics/273818/global-revenue-generated-with-cloud-computing-since-2009/

Stempel, J. & Finkle, J., 2017. *Yahoo says all three billion accounts hacked in 2013 data theft.* s.l.:Reuters.

Terroza, A. K. S., 2015. *Information Security Management System (ISMS) Overview.* s.l.:s.n.

The Economist, 2021. *What is the economic cost of covid-19?.* s.l.:The Economist.

The Open Group, 2017. *Open Information Security Management Maturity Model (O-ISM3), Version 2.0.* s.l.:s.n.

World Economic Forum, 2020. *The Global Risks Report 2020,* s.l.: s.n.