Πανεπιστήμιο Πειραιώς
Σχολή Τεχνολογιών Πληροφορικής και Τηλεπικοινωνίων
Τμήμα Ψηφιακών Συστημάτων
Π.Μ.Σ. Ασφάλεια Ψηφιακών Συστημάτων

Διοίκηση Επικινδυνότητας της Κυβερνοασφάλειας στην Εφοδιαστική Αλυσίδα (supply chain)

Διπλωματική Εργασία

Γεώργιος Μακρής MTE2113

Επιβλέπων Καθηγητής: Καθ. κ. Σ. Γκρίτζαλης

Πειραιάς
2023

Ευχαριστίες

Με την ευκαιρία αυτή μέσω της διπλωματικής μου εργασίας θα ήθελα να εκφράσω την ευγνωμοσύνη μου στην οικογένειά μου για την αμέριστη υποστήριξή τους καθ' όλη τη διάρκεια των σπουδών μου. Επιπλέον, θέλω να ευχαριστήσω όλους τους συμφοιτητές μου αλλά και τους φίλους μου που με στήριξαν σε όλη τη διαδρομή μου. Τέλος, θέλω να εκφράσω τις ειλικρινείς μου ευχαριστίες στον επιβλέποντα μου Καθ. κ. Στέφανο Γκρίτζαλη για την υπομονή και τη συνεχή υποστήριξή του τόσο για τη μεταπτυχιακή μου διατριβή όσο και για το Π.Μ.Σ. «Ασφάλεια Ψηφιακών Συστημάτων».

Περίληψη

Η παρούσα διπλωματική εργασία εξετάζει τη διοίκηση επικινδυνότητας στην κυβερνοασφάλεια στην εφοδιαστική αλυσίδα. Η εφοδιαστική αλυσίδα αποτελεί ένα απαραίτητο κομμάτι της σύγχρονης επιχειρηματικής δραστηριότητας, ωστόσο η κυβερνοασφάλεια της εφοδιαστικής αλυσίδας είναι επιρρεπής σε διάφορους κινδύνους και απειλές. Με την αύξηση των κυβερνοεπιθέσεων στην εφοδιαστική αλυσίδα, η ανάγκη για μια αποτελεσματική διοίκηση επικινδυνότητας είναι πιο σημαντική από ποτέ. Η παρούσα διπλωματική εργασία εξετάζει τις βέλτιστες πρακτικές για την αντιμετώπιση αυτών των κινδύνων. Αρχικά, παρουσιάζεται μια εισαγωγή στην εφοδιαστική αλυσίδα και στην κυβερνοασφάλεια, καθώς και μια ανάλυση των κινδύνων και των απειλών που υπάρχουν σε αυτήν. Έπειτα, δίνονται παραδείγματα από περιστατικά που έχουν συμβεί τα προηγούμενα χρόνια από επιθέσεις στην εφοδιαστική αλυσίδα. Επιπλέον, η εργασία προτείνει μια ολοκληρωμένη προσέγγιση για τη διοίκηση επικινδυνότητας στην κυβερνοασφάλεια στην εφοδιαστική αλυσίδα. Η εφαρμογή αυτής της προσέγγισης μπορεί να βελτιώσει σημαντικά την ασφάλεια της εφοδιαστικής αλυσίδας από τις κυβερνοεπιθέσεις και να προστατεύσει τις επιχειρήσεις από σοβαρές επιπτώσεις.

Abstract

The present dissertation examines Cybersecurity Risk Management in the supply chain. The supply chain is an essential part of modern business. However, the cybersecurity of the supply chain is prone to various risks and threats. Considering the increase in cyber-attacks on the supply chain, it is evident that effective risk management is crucial. This dissertation reviews best practices to address these risks. The first chapter contains an introduction to the supply chain and cybersecurity and an analysis of the risks and threats. In the following chapter, there is an overview of incidents of supply chain attacks that have occurred in previous years. In addition, the paper proposes a comprehensive approach to cybersecurity risk management in the supply chain. Implementing this approach can significantly improve supply chain security from cyber attacks and protect businesses from severe impacts.

Πίνακας Περιεχομένων

Λίστα Αρκτικόλεξων

CNI	Critical National Infrastructure
AI	Artificial intelligence
PII	Personally Identifiable Information
IoT	Internet of Things
CISO	Chief Information Security Officer
CIO	Chief Information Officer
CFO	Chief Financial Officer
NIST	National Institute of Standards and Technology
APT	Advanced Persistence Threat
RA	Risk Assessment

Λίστα Εικόνων

1. Εισαγωγή

Στις μέρες μας υπάρχει μια αυξανόμενη αβεβαιότητα και αστάθεια στο περιβάλλον ασφαλείας που αντιμετωπίζουν οι περισσότεροι οργανισμοί. Κατά συνέπεια, αντιμετωπίζουν ζητήματα ασφάλειας που επηρεάζουν τους στόχους και τις επιθυμίες τους να τα αντιμετωπίζουν συστηματικά στο πλαίσιο του συστήματος διαχείρισής τους. Μια προσέγγιση στην ασφάλεια από την διοίκηση ενός οργανισμού μπορεί να συμβάλει άμεσα στην επιχειρηματική ικανότητα και αξιοπιστία του οργανισμού. Η εφοδιαστική αλυσίδα υφίσταται μια ιστορική πίεση, αλλά η πίεση στην κυβερνοασφάλεια και τη διαχείριση κινδύνου μπορεί να είναι σε ακόμη χειρότερη κατάσταση. Καθώς είμαστε στα μέσα του 2023, η παγκόσμια αλυσίδα εφοδιασμού βρίσκεται σε κατάσταση συγκρίσιμη με την κυκλοφορία των αυτοκινήτων σε ώρες αιχμής σε κακές καιρικές συνθήκες. Όλα φαίνεται να επηρεάζονται είτε λόγω ζητημάτων προσφοράς και ζήτησης, χρόνου αναμονής στα λιμάνια αποστολής ή οποιουδήποτε αριθμού άλλων καθυστερήσεων.

Εάν η αλυσίδα εφοδιασμού πρόκειται να έχει πιθανότητες ανάκαμψης στο εγγύς μέλλον, οι οργανισμοί πρέπει να αντιμετωπίσουν την ασφάλεια στον κυβερνοχώρο και τη διαχείριση κινδύνου. Αυτό οφείλεται στο γεγονός ότι η κυβερνοασφάλεια και η αποτελεσματικότητα της εφοδιαστικής αλυσίδας είναι στενά αλληλένδετες.

Το ηλεκτρονικό έγκλημα έχει προκαλέσει σημαντικά γεγονότα και σοβαρές επιπλοκές με αποτέλεσμα να έχει δημιουργηθεί κρίση της εφοδιαστικής αλυσίδας Η κυβερνοασφάλεια και η διαχείριση κινδύνων ήταν πάντα ζωτικής σημασίας για τη ροή οποιασδήποτε επιχείρησης. Ωστόσο, η τρέχουσα κατάσταση της παγκόσμιας αλυσίδας εφοδιασμού την καθιστά εξαιρετικά ευάλωτη σε σοβαρές ζημιές από μια επίθεση περισσότερο από ό,τι συνήθως. Όταν η αλυσίδα εφοδιασμού μόλις μετά βίας τα βγάζει πέρα, οι εγκληματίες είναι πιο πιθανό να υποθέσουν ότι έχουν μόχλευση στις επιχειρήσεις. Ένα ransomware μπορεί να είναι πιο θρασύ και να έχει υψηλότερες απαιτήσεις από ό,τι θα μπορούσε να είχε πριν από μερικά χρόνια.

Οι περισσότεροι άνθρωποι θυμούνται το 2020 για την παγκόσμια πανδημία COVID-19. Ένα λιγότερο εμφανές παγκόσμιο πρόβλημα συνέβαινε την ίδια στιγμή, που επηρέαζε κάθε κλάδο και εκατομμύρια ανθρώπους: η πανδημία του κυβερνοχώρου.

Όταν ο COVID-19 κατέλαβε τον κόσμο, οι εγκληματίες του κυβερνοχώρου είδαν την ευκαιρία να προκαλέσουν μαζί τον όλεθρο.

Οι εκτιμήσεις κινδύνου από την INTERPOL[1] ανέφεραν μια εκπληκτική αύξηση των κυβερνοεπιθέσεων παράλληλα με την πανδημία COVID-19. Οι δύο υψηλότερες αυξήσεις στο έγκλημα στον κυβερνοχώρο ήταν οι επιθέσεις phishing και το ransomware. Αυτό δεν είναι τυχαίο. Αυτοί οι δύο τύποι κυβερνοεπιθέσεων εκμεταλλεύονται τις πιο κοινές συνθήκες που μαστίζουν τον παγκόσμιο πληθυσμό. Οι άνθρωποι παλεύουν με τον φόβο, την αβεβαιότητα και την άνευ προηγουμένου εξάρτηση από το διαδίκτυο, δημιουργώντας περισσότερες ευκαιρίες για επιτυχημένες επιθέσεις phishing. Στην πραγματικότητα, η δημοτικότητα της εργασίας από το σπίτι έχει συνδεθεί άμεσα με την αύξηση του εγκλήματος στον κυβερνοχώρο.

Ομοίως, ορισμένες βιομηχανίες και επιχειρήσεις διατρέχουν μεγαλύτερο κίνδυνο εάν τα συστήματά τους παραβιαστούν, όπως τα ιδρύματα υγειονομικής περίθαλψης, γεγονός που ευθύνεται για την αύξηση των επιθέσεων ransomware. Ακόμη και μετά την κάπως υποχώρηση της πανδημίας COVID-19 το 2021, το έγκλημα στον κυβερνοχώρο παρέμεινε υψηλό. Αυτό περιλάμβανε επιθέσεις σε κρίσιμες εθνικές υποδομές (CNI), όπως η επίθεση ransomware Colonial Pipeline [2].

Την ίδια στιγμή που αυτή η πανδημία στον κυβερνοχώρο επικράτησε το 2020, η παγκόσμια αλυσίδα εφοδιασμού άρχισε να αντιμετωπίζει την πίεση που συνεχίζει να την επιβαρύνει μέχρι το 2023. Εκατομμύρια άνθρωποι άρχισαν να χρησιμοποιούν τις ηλεκτρονικές αγορές ως τον κύριο, ή ακόμα και τον μοναδικό, τρόπο αγοράς αγαθών. δημιουργώντας μεγαλύτερη ζήτηση για παραγγελίες μέσω του διαδικτύου. Επιπλέον, ορισμένες βιομηχανίες παρουσίασαν άνευ προηγουμένου αυξήσεις στη ζήτηση άμεσα ως απάντηση στην πανδημία του COVID-19.

Ένα κρίσιμο παράδειγμα αυτού είναι η αλυσίδα εφοδιασμού εξαρτημάτων υπολογιστών. Η προσφορά και η ζήτηση για ορισμένα εξαρτήματα δεν ήταν ποτέ μεγαλύτερη τόσο για τις επιχειρήσεις όσο και για τους καταναλωτές. Οι λάτρεις των υπολογιστών εγγράφονται σε λίστες αναμονής διάρκειας ενός έτους για να αποκτήσουν επεξεργαστές, κάρτες γραφικών, ενώ οι κατασκευαστές αυτοκινήτων αναφέρουν ζημίες εκατομμυρίων δολαρίων λόγω ελλείψεων chip. Ορισμένοι αγοραστές παίρνουν

ακόμη και τον κίνδυνο να χρησιμοποιήσουν πλαστά προϊόντα, όπως τροφοδοτικά, για να τα βγάλουν πέρα. Μεταξύ της διαδικτυακής εργασίας, της ψυχαγωγίας στο σπίτι και της ζήτησης παραγωγής, η έλλειψη chip υπολογιστών είναι από τις χειρότερες περιπτώσεις στην τρέχουσα κρίση εφοδιαστικής αλυσίδας.

Αυτοί οι παράγοντες δημιουργούν επείγουσα ανάγκη για ισχυρότερα μέτρα ασφαλείας στην αλυσίδα εφοδιασμού. Οι οργανισμοί πρέπει να ξεκινήσουν αυξάνοντας την ευαισθητοποίησή τους για τους κινδύνους. Είναι σημαντικό να θυμόμαστε ότι η κυβερνοασφάλεια πρέπει να υπερβαίνει την απλή εγκατάσταση λογισμικού προστασίας από ιούς σε υπολογιστές της εταιρείας. Πρέπει επίσης να συμβαίνει σε κάθε στάδιο της εφοδιαστικής αλυσίδας με κάθε εργαζόμενο. Στην ψηφιακή εποχή, η γραμμή μεταξύ του εγκλήματος στον πραγματικό και τον εικονικό κόσμο είναι πολύ θολή, επομένως αυτοί οι κίνδυνοι πρέπει να ληφθούν εξίσου σοβαρά με οποιοδήποτε μέτρο φυσικής ασφάλειας.

Οι βασικοί κίνδυνοι που αντιμετωπίζει η εφοδιαστική αλυσίδα εμφανίζονται σε διάφορα επίπεδα. Οι ειδικοί του κλάδου επισημαίνουν ότι μπορεί να συμβούν στον φυσικό κόσμο, όπως πρόσβαση σε server rooms, διακομιστές ή υλικό ενσωματωμένο σε κακόβουλο λογισμικό. Οι οργανισμοί πρέπει να γνωρίζουν κάθε τρίτο μέρος με το οποίο αλληλοεπιδρούν σε όλη την αλυσίδα εφοδιασμού, από εταιρείες συντήρησης με σύμβαση μέχρι προμηθευτές. Οποιοσδήποτε έχει πρόσβαση στο δίκτυο ή τα συστήματα του οργανισμού μπορεί να αποτελέσει κίνδυνο.

Η ασφάλεια όλων των προμηθευτών και συνεργατών επηρεάζει άμεσα και τον οργανισμό. Ένα εκπληκτικό 66% των κυβερνοεπιθέσεων της εφοδιαστικής αλυσίδας εκμεταλλεύτηκε την εμπιστοσύνη στην ασφάλεια των προμηθευτών. Εάν τα δεδομένα πληρωμών διακυβεύονται, οι πληροφορίες σχετικά με τους πελάτες αυτών των οργανισμών κινδυνεύουν επίσης. Οι προμηθευτές και οι οργανισμοί είναι επίσης υπεύθυνοι για τον τερματισμό των δεδομένων των καταναλωτών, κάτι που αποτελεί κοινό στόχο για κυβερνοεπιθέσεις.

Τα λογισμικά παραμένουν ένας επιτακτικός κίνδυνος για την ασφάλεια, ειδικά για οργανισμούς που λειτουργούν εξ αποστάσεως. Κάθε υπάλληλος που αλληλοεπιδρά με τα δεδομένα ή το δίκτυο της εταιρείας πρέπει να έχει εγκατεστημένο τουλάχιστον ένα

λογισμικό ασφαλείας στις συσκευές του. Οι γνώσεις ασφαλείας των εργαζομένων ενέχουν επίσης έναν κίνδυνο, ο οποίος είναι εμφανής στην προαναφερθείσα αύξηση των επιθέσεων phishing.

Πώς όμως οι οργανισμοί μπορούν να διαχειριστούν τους κινδύνους; Οι κίνδυνοι και η ευάλωτη κατάσταση της παγκόσμιας αλυσίδας εφοδιασμού μπορεί να κάνουν τρομακτική την προσέγγιση διαχείρισης κινδύνου[3]. Ωστόσο, η ασφάλεια είναι στην πραγματικότητα αρκετά απλή. Πολλοί οργανισμοί απλώς δεν γνωρίζουν το εύρος του κινδύνου και τις ενέργειες που μπορούν να λάβουν ως απάντηση. Το πρώτο βήμα είναι να ολοκληρώσουν μια ενδελεχή αξιολόγηση κινδύνου. Αυτή η ανάλυση θα πρέπει να εξετάζει κάθε επίπεδο του οργανισμού, από τη φυσική ασφάλεια έως την ατομική ασφάλεια στον κυβερνοχώρο κάθε υπαλλήλου. Επιπλέον, είναι σημαντικό να μελετηθούν τα μέτρα ασφαλείας που ισχύουν σε άλλα επίπεδα της σχετικής αλυσίδας εφοδιασμού. Πρέπει να εξεταστεί το ενδεχόμενο να επικοινωνήσει ο οργανισμός με τους προμηθευτές ή να προγραμματίσουν μια συνάντηση με εκπροσώπους για να συζητήσουν μεθόδους ασφάλειας και διαχείρισης κινδύνου, από τις οποίες θα επωφεληθούν όλοι. Η αλυσίδα εφοδιασμού είναι τόσο ισχυρή όσο ο σύνδεσμος με τις πιο αδύναμες πολιτικές κυβερνοασφάλειας και διαχείρισης κινδύνου.

Μετά τον ενδελεχή εντοπισμό των κινδύνων, το επόμενο βήμα είναι να τεθούν σε εφαρμογή ισχυρά μέτρα ασφαλείας. Η τεχνολογία μπορεί να βοηθήσει στην κάλυψη αυτού του εδάφους. Για παράδειγμα, η τεχνητή νοημοσύνη (AI) είναι ένα πολύτιμο εργαλείο για τη βελτίωση της ανθεκτικότητας στην αλυσίδα εφοδιασμού, ειδικά όταν πρόκειται για την ασφάλεια στον κυβερνοχώρο. Οι λύσεις AI λειτουργούν σαν εικονικοί φύλακες ασφαλείας 24/7. Συχνά χρησιμοποιούν αναγνώριση προτύπων και συλλογή δεδομένων για να εντοπίσουν γρήγορα οτιδήποτε ασυνήθιστο, όπως εισβολείς στον κυβερνοχώρο.

Ένα άλλο μέτρο που μπορεί να παρθεί είναι να εξεταστεί το ενδεχόμενο εφαρμογής ενός προγράμματος εκπαίδευσης για την ασφάλεια στον κυβερνοχώρο σε ολόκληρη την εταιρεία και να βεβαιωθεί ο οργανισμός ότι όλες οι προσωπικές συσκευές έχουν εγκατεστημένο ενημερωμένο, αξιόπιστο λογισμικό ασφαλείας. Πολλοί οργανισμοί έχουν ακόμη και έναν ειδικό υπεύθυνο κυβερνοασφάλειας για να επιβλέπει επαγγελματικά την εφαρμογή όλων των στρατηγικών ασφαλείας.

Οι οργανισμοί εντός της αλυσίδας εφοδιασμού πρέπει να υιοθετήσουν μια ενεργή, εστιασμένη προσέγγιση στην ασφάλεια στον κυβερνοχώρο για να αποφύγουν καθυστερήσεις που σχετίζονται με το έγκλημα, παραβιάσεις δεδομένων και οικονομικές απώλειες. Η κατάσταση μπορεί να φαίνεται τραγική, αλλά οι εταιρείες μπορούν να εμποδίσουν τους ψηφιακούς εισβολείς να χτυπήσουν την παγκόσμια αλυσίδα εφοδιασμού ενισχύοντας την άμυνά τους. Εάν το έγκλημα στον κυβερνοχώρο είναι η πανδημία, το εμβόλιο είναι η προηγμένη διαχείριση της ασφάλειας και του κινδύνου.

2. Κατανόηση της αύξησης των Επιθέσεων Ασφαλείας Εφοδιαστικής Αλυσίδας

Οι επιθέσεις στην αλυσίδα εφοδιασμού[4] απασχολούν τους εμπειρογνώμονες στον κυβερνοχώρο εδώ και πολλά χρόνια, επειδή η αλυσιδωτή αντίδραση που προκαλείται από μία επίθεση σε έναν μόνο προμηθευτή μπορεί να θέσει σε κίνδυνο ένα δίκτυο παρόχων. Το ransomware (κακόβουλο λογισμικό) είναι η τεχνική επίθεσης στην οποία καταφεύγουν οι επιτιθέμενοι στο 62% των επιθέσεων.

Εικόνα 1: ENISA report - Threat Landscape for Supply Chain Attacks

Σύμφωνα με τη νέα έκθεση ENISA - Threat Landscape for Supply Chain Attacks [5], η οποία ανέλυσε 24 πρόσφατες επιθέσεις, η ισχυρή προστασία ασφαλείας δεν είναι πλέον αρκετή για τους οργανισμούς όταν οι επιτιθέμενοι έχουν ήδη στρέψει την προσοχή τους στους προμηθευτές. Αυτό αποδεικνύεται από τον αυξανόμενο αντίκτυπο αυτών των επιθέσεων, όπως η διακοπή λειτουργίας συστημάτων, η χρηματική απώλεια και η φήμη.

Οι επιθέσεις στην εφοδιαστική αλυσίδα αναμένεται τώρα αλλά και στο μέλλον να πολλαπλασιαστούν κατά σε σύγκριση με πέρυσι. Αυτή η νέα τάση τονίζει την ανάγκη για τους υπεύθυνους χάραξης πολιτικής και την κοινότητα της κυβερνοασφάλειας να δράσουν τώρα. Αυτός είναι ο λόγος για τον οποίο πρέπει να εισαχθούν επειγόντως νέα προστατευτικά μέτρα για την πρόληψη και την αντιμετώπιση πιθανών επιθέσεων της εφοδιαστικής αλυσίδας στο μέλλον με παράλληλη άμβλυνση των επιπτώσεών τους. Ας εξηγήσουμε λοιπόν τι είναι και τι περιλαμβάνει μια εφοδιαστική αλυσίδα. Μια αλυσίδα εφοδιασμού είναι ο συνδυασμός του οικοσυστήματος των πόρων που απαιτούνται για το σχεδιασμό, την κατασκευή και τη διανομή ενός προϊόντος. Στην ασφάλεια στον κυβερνοχώρο, μια αλυσίδα εφοδιασμού περιλαμβάνει υλικό και λογισμικό, cloud ή τοπικούς server, τοπικούς storage server και διανομής. Εφόσον ένας οργανισμός έχει ένα καλό επίπεδο ασφαλείας στον κυβερνοχώρο, αυτό μπορεί να μην είναι ποτέ αρκετά καλό. Μια σωστή και σχεδιασμένη επίθεση σε έναν ή περισσότερους προμηθευτές με μεταγενέστερη επίθεση στον τελικό στόχο, δηλαδή τον πελάτη, οι επιθέσεις της εφοδιαστικής αλυσίδας μπορεί να χρειαστούν μήνες για να πετύχουν. Σε πολλές περιπτώσεις, μια τέτοια επίθεση μπορεί ακόμη και να μείνει απαρατήρητη για μεγάλο χρονικό διάστημα. Παρόμοια με τις επιθέσεις Advanced Persistence Threat (APT) [6], οι επιθέσεις της εφοδιαστικής αλυσίδας είναι συνήθως στοχευμένες, αρκετά περίπλοκες και δαπανηρές με τους επιτιθέμενους πιθανώς να τις σχεδιάζουν πολύ εκ των προτέρων. Όλες αυτές οι πτυχές αποκαλύπτουν τον βαθμό πολυπλοκότητας των αντιπάλων και την επιμονή στην προσπάθεια επιτυχίας.

Ένας οργανισμός θα μπορούσε να είναι ευάλωτος σε επίθεση της εφοδιαστικής αλυσίδας ακόμα και όταν οι δικές του άμυνες είναι αρκετά καλές. Οι επιτιθέμενοι εξερευνούν νέους πιθανούς δρόμους για να διεισδύσουν σε οργανισμούς στοχεύοντας τους προμηθευτές τους. Επιπλέον, με τις σχεδόν απεριόριστες δυνατότητες του

αντίκτυπου των επιθέσεων της εφοδιαστικής αλυσίδας σε πολλούς πελάτες, αυτοί οι τύποι επιθέσεων γίνονται όλο και πιο συνηθισμένοι.

Προκειμένου να θέσουν σε κίνδυνο τους στοχευμένους πελάτες, οι εισβολείς εστίασαν στον κώδικα των προμηθευτών στο 66% περίπου των αναφερόμενων περιστατικών. Αυτό δείχνει ότι οι οργανισμοί θα πρέπει να επικεντρώσουν τις προσπάθειές τους στην επικύρωση κώδικα και λογισμικού τρίτων, προτού τα χρησιμοποιήσουν, για να διασφαλίσουν ότι δεν έχουν παραβιαστεί ή παραποιηθεί. Για περίπου το 58% των περιστατικών της εφοδιαστικής αλυσίδας που αναλύθηκαν, τα στοχευόμενα περιουσιακά στοιχεία πελατών ήταν κυρίως δεδομένα πελατών, συμπεριλαμβανομένων δεδομένων Προσωπικής Αναγνώρισης (PII) και πνευματικής ιδιοκτησίας. Για το 66% των επιθέσεων της εφοδιαστικής αλυσίδας που αναλύθηκαν, οι προμηθευτές δεν γνώριζαν ή παρέλειψαν να αναφέρουν πώς παραβιάστηκαν. Ωστόσο, λιγότερο από το 9% των πελατών που παραβιάστηκαν μέσω επιθέσεων στην αλυσίδα εφοδιασμού δεν γνώριζαν πώς έγιναν οι επιθέσεις. Αυτό υπογραμμίζει το χάσμα όσον αφορά την ωριμότητα στην αναφορά περιστατικών κυβερνοασφάλειας μεταξύ προμηθευτών και τελικών χρηστών.

Ο αντίκτυπος των επιθέσεων στους προμηθευτές μπορεί να έχει εκτεταμένες συνέπειες λόγω των αυξημένων αλληλεξαρτήσεων και πολυπλοκότητας των τεχνικών που χρησιμοποιούνται. Πέρα από τις ζημίες σε θιγόμενους οργανισμούς και τρίτα μέρη, υπάρχει βαθύτερος λόγος ανησυχίας όταν διασπώνται διαβαθμισμένες πληροφορίες και διακυβεύεται η εθνική ασφάλεια ή όταν ενδέχεται να προκύψουν συνέπειες γεωπολιτικής φύσης. Σε αυτό το περίπλοκο περιβάλλον για τις αλυσίδες εφοδιασμού, η καθιέρωση καλών πρακτικών και η συμμετοχή σε συντονισμένες δράσεις είναι και οι δύο σημαντικές για την υποστήριξη όλων των κρατών μελών στην ανάπτυξη παρόμοιων δυνατοτήτων – για την επίτευξη κοινού επιπέδου ασφάλειας.

Σε γενικό επίπεδο θα πρέπει να γίνουν κάποια βασικά βήματα όσον αφορά τους πελάτες ενός οργανισμού.

- Να γίνει ταυτοποίηση και τεκμηρίωση προμηθευτών και παρόχων υπηρεσιών

- καθορισμός κριτηρίων κινδύνου για διαφορετικούς τύπους προμηθευτών και υπηρεσιών, όπως εξαρτήσεις προμηθευτών και πελατών, κρίσιμες εξαρτήσεις λογισμικού, μεμονωμένα σημεία αστοχίας.
- παρακολούθηση των κινδύνων και των απειλών της εφοδιαστικής αλυσίδας
- διαχείριση προμηθευτών καθ' όλη τη διάρκεια του κύκλου ζωής ενός προϊόντος ή μιας υπηρεσίας, συμπεριλαμβανομένων των διαδικασιών χειρισμού προϊόντων ή εξαρτημάτων στο τέλος του κύκλου ζωής τους
- ταξινόμηση των περιουσιακών στοιχείων και των πληροφοριών που μοιράζονται ή είναι προσβάσιμες σε προμηθευτές και ορίζει τις σχετικές διαδικασίες για την πρόσβαση και το χειρισμό τους.

Συναντάται να γίνουν ενέργειες για να διασφαλιστεί ότι η ανάπτυξη προϊόντων και υπηρεσιών συμμορφώνεται με τις πρακτικές ασφαλείας. Συνιστάται για παράδειγμα στους προμηθευτές να εφαρμόζουν καλές πρακτικές για την ευπάθεια και τη διαχείριση ενημερώσεων κώδικα.

Οι συστάσεις προς τους προμηθευτές που μπορούν να γίνουν περιλαμβάνουν:

- διασφάλιση ότι η υποδομή που χρησιμοποιείται για το σχεδιασμό, την ανάπτυξη, την κατασκευή και την παράδοση προϊόντων, εξαρτημάτων και υπηρεσιών ακολουθεί πρακτικές κυβερνοασφάλειας
- την εφαρμογή μιας διαδικασίας ανάπτυξης, συντήρησης και υποστήριξης προϊόντος που είναι συνεπής με κοινά αποδεκτές διαδικασίες ανάπτυξης προϊόντων
- παρακολούθηση των τρωτών σημείων ασφαλείας που αναφέρονται από εσωτερικές και εξωτερικές πηγές που περιλαμβάνει χρησιμοποιημένα στοιχεία τρίτων.
- τη διατήρηση απογραφής περιουσιακών στοιχείων που περιλαμβάνει πληροφορίες σχετικές με την ενημέρωση κώδικα.

3. Περιστατικά και Συνηθισμένοι κίνδυνοι

Οι τρεις πιο συνηθισμένοι κίνδυνοι που επηρεάζουν τις εταιρείες της εφοδιαστικής αλυσίδας περιλαμβάνουν διαρροές δεδομένων, παραβιάσεις της αλυσίδας εφοδιασμού και επιθέσεις κακόβουλου λογισμικού. Διαρροές δεδομένων μπορεί να συμβούν μέσω εξωτερικών και εσωτερικών εισβολέων. Οι εργαζόμενοι, οι κακόβουλοι χρήστες, οι κακόβουλοι ανταγωνιστές και οι διευθυντές μπορούν όλοι να διαρρεύσουν ευαίσθητα δεδομένα και προσωπικές πληροφορίες εκτός της επιχείρησης.

Οι παραβιάσεις ασφαλείας συμβαίνουν συνήθως όταν ένας κακόβουλος χρήστης διεισδύει σε λειτουργικό σύστημα ή δίκτυο χωρίς άδεια. Ο στόχος είναι συχνά η πρόκληση χάους μέσα στο σύστημα μέσω διαγραφής δεδομένων, αναπαραγωγής και διαφθοράς. Οι επιθέσεις κακόβουλου λογισμικού μπορούν να συμβούν μέσω ενός ransomware που κλειδώνει έναν server ή κάποια βάση δεδομένων έως ότου η επιχείρηση πληρώσει ένα χρηματικό ποσό. Οι ιοί μπορούν να μολύνουν το σύστημα ή μέσω ενός trojan μπορούν να αποκτήσουν πρόσβαση σε ευαίσθητες πληροφορίες και συστήματα.

Ένα μεμονωμένο phishing email για πληροφορίες ή που έχει έναν σύνδεσμο στον οποίο κάνει κλικ ένας υπάλληλος μπορεί να οδηγήσει σε καταστροφή και απώλεια δεδομένων. Εάν το phishing email είναι επιτυχές, ο κακόβουλος χρήστης θα μπορούσε να βρει ένα όνομα χρήστη και έναν κωδικό πρόσβασης που χρησιμοποιείται για τη συλλογή πληροφοριών εντός του συστήματος. Αυτό θα μπορούσε να οδηγήσει σε απρόβλεπτο ανταγωνισμό και σοβαρές διαρροές που μπορεί να βλάψουν ολόκληρη μια εταιρεία ή έναν οργανισμό.

Πραγματικές παραβιάσεις που έχουν πραγματοποιηθεί στην εφοδιαστική αλυσίδα, που αφορούσαν γενικά επιθέσεις ransomware και άλλες επιθέσεις κακόβουλου λογισμικού είναι μια επίθεση ransomware που κινδυνεύει να εκθέσει τα προσωπικά δεδομένα εκατομμυρίων πελατών, συμπεριλαμβανομένων των αριθμών κοινωνικής ασφάλισης και των διευθύνσεων αλληλογραφίας. Ένα τέτοιο ήταν ένα ransomware, το Ryuk[7], εμφανίστηκε το 2018 και στόχευε χρήστες μέσω κακόβουλων μηνυμάτων ηλεκτρονικού ταχυδρομείου. Όπως με τα περισσότερα ransomware, κλείδωσε τους χρήστες από τους υπολογιστές και στη συνέχεια έκλεψε τα διαπιστευτήριά τους. Τα

αρχεία έγιναν κρυπτογραφημένα και το κακόβουλο λογισμικό απαιτούσε τεράστια λύτρα για να επιστρέψει η πρόσβαση σε αυτούς τους υπολογιστές. Οι απαιτήσεις ήταν σχεδόν 300.000$ για κάθε περιστατικό. Εάν πληρωνόταν, ο κυβερνοεγκληματίας θα μπορούσε να επιτεθεί ξανά στο ίδιο σύστημα στο μέλλον. Όλοι οι τύποι επιχειρήσεων και οργανισμών δέχθηκαν επίθεση, συμπεριλαμβανομένων των επιχειρήσεων της εφοδιαστικής αλυσίδας. Ένα άλλο παράδειγμα ήταν το TrickBot[8] που ήταν ένα άλλο εργαλείο που χρησιμοποιήθηκε. Αρχικά ένα τραπεζικό trojan, το TrickBot έγινε τελικά ένα εργαλείο που οδήγησε σε εγκλήματα στον κυβερνοχώρο που αφορούσαν τη συλλογή διαπιστευτηρίων, την εξόρυξη κρυπτονομισμάτων και εισαγηγής ransomware σε κρίσιμες υποδομές. Το εργαλείο προκάλεσε επίσης διαρροή επιχειρηματικών δεδομένων σε σημείο πώλησης προς κάθε ενδιαφερόμενο. Με την εξόρυξη κρυπτονομισμάτων, ο κυβερνοεγκληματίας θα μπορούσε να αυξήσει τον προσωπικό του πλούτο. Ωστόσο, οι εισβολές ransomware είναι παρόμοιες με άλλες παραβιάσεις που συνήθως απαιτούν πληρωμή για την επιστροφή του συστήματος στον χρήστη του. Μια άλλη επίθεση στον κυβερνοχώρο αφορούσε τους BazarLoader και BazarBackdoor[9]. Το 2020, μόλυναν ορισμένα στοχευμένα συστήματα. Χρησιμοποίησαν την κοινωνική μηχανική και στόχευαν πλατφόρμες συνεργασίας όπως το Slack και το BaseCamp, στέλνοντας email σε υπαλλήλους μεγάλων οργανισμών που έλεγαν ότι προσφέρουν σημαντικές πληροφορίες σχετικά με συμβάσεις, εξυπηρέτηση πελατών, τιμολόγια ή μισθοδοσία. Αυτά τα εργαλεία εισήγαγαν επίσης ransomware που απαιτούσαν πληρωμή από την επιχείρηση.

4. Οι 10 Κορυφαίες απειλές στον Κυβερνοχώρο

4.1 Ασφάλεια στο cloud

Οι περισσότεροι οργανισμοί ανησυχούν για την ασφάλεια στο cloud. Η εσφαλμένη διαμόρφωση, η μη εξουσιοδοτημένη πρόσβαση, οι ανασφαλείς διεπαφές και η πειρατεία λογαριασμών είναι όλα πιθανά σημεία εισόδου για τους κακόβουλους χρήστες. Με περισσότερες εταιρείες να μεταμορφώνονται ψηφιακά και να αξιοποιούν εργαλεία διαδικτυακής συνεργασίας, η μετάβαση στο cloud computing έχει επίσης επιταχυνθεί. Το cloud θα συνεχίσει να διαμορφώνει τον τρόπο λειτουργίας των επιχειρήσεων, καθώς και να εκθέτει μια σειρά από προκλήσεις και απειλές για την ασφάλεια.

4.2 Μέσα κοινωνικής δικτύωσης

Τα μέσα κοινωνικής δικτύωσης είναι παντοδύναμα και συνεχίζουν να αποτελούν μέσο επιλογής για την έναρξη κυβερνοεπιθέσεων. Οι παραβιάσεις δεδομένων έχουν δείξει αδυναμίες στα κοινωνικά δίκτυα για να περάσουν από τους κακόβουλου χρήστες και η κακή τήρηση της ασφάλειας από την πλευρά των χρηστών σημαίνει ότι οι κακόβουλοι χρήστες δεν χρειάζεται καν να παραβιάσουν τις άμυνες του ιστότοπο. Τα συστήματα phishing email (email και κείμενα με αξιόπιστη εμφάνιση που προσκαλούν τον χρήστη να μοιραστεί προσωπικά δεδομένα) και οι πλαστογραφημένοι λογαριασμοί είναι μόνο δύο από τους πολλούς τρόπους εξαπάτησης των χρηστών ώστε να εγκαταλείψουν τα διαπιστευτήριά τους και αποτελούν συνεχή απειλή. Ανησυχητικά για το εμπόριο, οι επιτιθέμενοι μεταβαίνουν από τη στόχευση ατόμων στη στόχευση επιχειρήσεων μέσω των μέσων κοινωνικής δικτύωσης.

4.3 PDF

Τα αρχεία PDF είναι ένα δελεαστικό μέσο phishing, καθώς είναι cross-platform και επιτρέπουν στους εισβολείς να αλληλεπιδρούν με τους χρήστες, κάνοντας τα σχέδιά τους να φαίνονται πιο πιστευτά από ένα μήνυμα ηλεκτρονικού ταχυδρομείου που βασίζεται σε κείμενο με απλό σύνδεσμο. Σε αντίθεση με πολλές απάτες μέσω email, οι εισβολές PDF συχνά δεν σας ζητούν να ανοίξετε έναν σύνδεσμο για να δώσετε πληροφορίες. Οι απατεώνες γνωρίζουν ότι οι άνθρωποι είναι πιο πιθανό να ανοίξουν ένα PDF παρά ένα μήνυμα ηλεκτρονικού ταχυδρομείου, ειδικά αν πιστεύουν ότι είναι μια κίνηση τραπεζικού λογαριασμού. Η εταιρεία ασφαλείας Palo Alto Networks[10] λέει ότι πέρυσι σημειώθηκε αύξηση 1.160% στα κακόβουλα αρχεία PDF και ότι αυτό πρόκειται να αυξηθεί.

4.4 Βάσεις δεδομένων

Η ασφάλεια των βάσεων δεδομένων γίνεται μια μεγάλη πρόκληση ασφαλείας για τις επιχειρήσεις. Σύμφωνα με τον Αμερικανό πάροχο IT, Straight Edge Technology, ορισμένοι κακόβουλοι χρήστες χρησιμοποιούν επιθέσεις κοινωνικής μηχανικής για να κλέψουν διαπιστευτήρια σύνδεσης, ενώ άλλοι χρησιμοποιούν κακόβουλο λογισμικό για να αποκτήσουν πρόσβαση. Ένα από τα σημαντικά ζητήματα με την έκθεση μίας

βάσης δεδομένων είναι το περιεχόμενο που παρέχει για να προβληθούν που βασίζονται στο social engineering.

4.5 Τυχαία κοινή χρήση

Το ανθρώπινο λάθος είναι κάτι στο οποίο βασίζονται όλοι οι κακόβουλοι χρήστες και για καλό λόγο: είμαστε όλοι λανθασμένοι. Η τυχαία κοινή χρήση περιλαμβάνει προσωπικά ή επιχειρηματικά δεδομένα, μέσω email, μη ασφαλών φορμών ή μέσω μηνυμάτων μέσων κοινωνικής δικτύωσης. Είναι μια ιδιαίτερη απειλή για τις εταιρείες όπου μεγάλος αριθμός εργαζομένων έχουν πρόσβαση σε βάσεις δεδομένων και έχει ως αποτέλεσμα οι πληροφορίες να κοινοποιούνται ή διαρρέουν κατά λάθος.

4.6 SMS

Ενώ το phishing συμβαίνει συχνά μέσω email και περιήγησης στον Ιστό, το λεγόμενο «smishing» γίνεται μέσω μηνυμάτων κειμένου SMS στο τηλέφωνό του θύματος. Ο εισβολέας στέλνει ένα μήνυμα κειμένου SMS με έναν σύνδεσμο στον οποίο, μόλις γίνει κλικ, ξεκινά η επίθεση. Οι εγκληματίες του κυβερνοχώρου στρέφονται σε τέτοιες επιθέσεις επειδή πολλά προγράμματα ηλεκτρονικού ταχυδρομείου - το Google Mail και το Microsoft Outlook για παράδειγμα - είναι αρκετά έξυπνα για να ανιχνεύουν μηνύματα ηλεκτρονικού "ψαρέματος" (phishing).

4.7 Συσκευές IoT

Η αγορά των Internet of Things (IoT) αναμένεται να αυξηθεί σε 1,1 τρις δολάρια ΗΠΑ έως το 2026 και η ευρεία χρήση συσκευών IoT ανοίγει σοβαρές απειλές για την ασφάλεια στον κυβερνοχώρο, ειδικά στην αλυσίδα εφοδιασμού, όπου η τεχνολογία IoT είναι συνηθισμένη. Σύμφωνα με τη Symantec, οι συσκευές IoT υφίστανται κατά μέσο όρο 5.200 επιθέσεις το μήνα και με την τεχνολογία IoT να επεκτείνεται σχεδόν εκθετικά, το πεδίο δράσης και επίθεσης για τους εγκληματίες του κυβερνοχώρου είναι τεράστια.

4.8 Κακό housekeeping

Παρά την πολυπλοκότητα των λύσεων για την ασφάλεια στον κυβερνοχώρο, ένα από τα μεγαλύτερα προβλήματα παραμένει ο εφησυχασμός και η τεμπελιά των ανθρώπων σχετικά με το βασικό housekeeping στον κυβερνοχώρο. Όλοι γνωρίζουμε κάποιον που χρησιμοποιεί τους ίδιους κωδικούς πρόσβασης για τα πάντα ή που δεν μπαίνει στον κόπο να αλλάξει τους προεπιλεγμένους κωδικούς πρόσβασης από 0000 ή 1111 σε κάτι ασφαλές. Αυτός ήταν ο τρόπος με τον οποίο κατέστη δυνατό το σκάνδαλο hacking τηλεφωνικών εφημερίδων του Ηνωμένου Βασιλείου και παραμένει ένα τρανό παράδειγμα των δράσεων για τους εγκληματίες του κυβερνοχώρου σε όλο τον κόσμο.

4.9 Phishing

Το phishing email είναι όταν οι εισβολείς προσπαθούν να εξαπατήσουν τους χρήστες (συνήθως μέσω email ή μηνυμάτων κειμένου) ώστε να κάνουν κλικ σε έναν σύνδεσμο που κατεβάζει ένα κομμάτι κακόβουλου λογισμικού ή που τους κατευθύνει σε έναν κακόβουλο ιστότοπο. Οι επιθέσεις phishing ευθύνονται για περισσότερο από το 80% των αναφερόμενων περιστατικών ασφαλείας, σύμφωνα με το CSO Online, το οποίο αντιπροσωπεύει το 1 στα 4.200 email πέρυσι και πρόκειται να αυξηθεί περαιτέρω φέτος. Σύμφωνα με τη Symantec, 1 στα 13 web request οδηγεί σε επίθεση κακόβουλου λογισμικού και εκτιμάται ότι χάνονται 17.700 $ κάθε λεπτό λόγω επίθεσης phishing.

4.10 Ransomware

Οι επιθέσεις ransomware προκαλούν τεράστια ανησυχία για επιχειρήσεις στις μεγάλες αλυσίδες εφοδιασμού. Οι επιθέσεις ransomware είναι πιο συχνές σε ανεπτυγμένες χώρες με υψηλά επίπεδα χρήσης Διαδικτύου. Αντίστοιχα, οι ΗΠΑ κατατάσσονται στην υψηλότερη θέση, με το 18,2% όλων των επιθέσεων ransomware (Symantec). Η μέση πληρωμή ransomware το 2021 ήταν 111.605 $. Ένα διαβόητο παράδειγμα μιας τέτοιας επίθεσης ήταν η επίθεση ransomware Kaseya[11] τον Ιούλιο του 2021. Η Kaseya είναι διεθνής πάροχος λογισμικού με έδρα το Μαϊάμι και το Δουβλίνο. Παρέχει λύσεις πληροφορικής σε 40.000 οργανισμούς, καθώς και τεχνολογία σε διαχειριζόμενους παρόχους υπηρεσιών, οι οποίοι στη συνέχεια εξυπηρετούν άλλους οργανισμούς. Αυτό έκανε τον Kaseya έναν τόσο ελκυστικό στόχο για τους κακόβουλους χρήστες.

Η επίθεση τελικά συνδέθηκε με τη διαβόητη ρωσική ομάδα hacking REvil, η οποία εκμεταλλεύτηκε μια ευπάθεια στο εργαλείο διαχείρισης απομακρυσμένου υπολογιστή της Kaseya.

5. Βασικά μέτρα ασφαλείας

Η ποικιλία των επιλογών που έχουν στην διάθεση τους οι εγκληματίες του κυβερνοχώρου για επιθέσεις είναι μεγάλη, γι' αυτό οι επιχειρήσεις πρέπει να είναι σχολαστικές στην προσέγγισή τους στην ασφάλεια στον κυβερνοχώρο. Παρακάτω αναφέρονται βασικά μέτρα προστασίας:

5.1 Πρόληψη

Για την ασφάλεια στον κυβερνοχώρο, η πρόληψη είναι πάντα καλύτερη από τη θεραπεία. Η συμβουλή ενός εστιασμένου παρόχου υπηρεσιών κυβερνοασφάλειας που μπορεί να αναλάβει μια ισχυρή αξιολόγηση ωριμότητας στον κυβερνοχώρο θα παίξει σημαντικό ρόλο. Σχεδιάζοντας για κάθε ενδεχόμενο και αναζητώντας μελλοντικά τρωτά σημεία, οι εταιρείες μπορούν να εξοπλιστούν με γνώση και σχέδια αντιμετώπισης ενάντια σε επίδοξες επιθέσεις στον κυβερνοχώρο και ιούς.

5.2 Αξιολόγηση προϋπολογισμού

Οι περισσότερες εταιρείες αυξάνουν τις δαπάνες για την κυβερνοασφάλεια στα συμβόλαια προμήθειας τεχνολογίας, λόγω του κόστους που μπορεί να προκύψει από μια παραβίαση. Πρέπει να υπάρχουν υγιείς συζητήσεις μεταξύ των CISO και των Οικονομικών Διευθυντών σχετικά με τους προϋπολογισμούς, προκειμένου να υποστηριχθούν κατάλληλα οι απαιτήσεις κυβερνοασφάλειας και τα προληπτικά μέτρα. Κατανέμοντας πόρους εκ των προτέρων, οι εταιρείες μπορούν να εξοικονομήσουν εκατομμύρια αποτρέποντας κυβερνοεπιθέσεις.

5.3 Συμμόρφωση

Οι εταιρείες πρέπει να διασφαλίζουν ότι οι συμφωνίες προμήθειας τεχνολογίας τους περιλαμβάνουν κατάλληλες διατάξεις συμμόρφωσης με την ασφάλεια που οριοθετούν τις απαιτήσεις κυβερνοασφάλειας στις οποίες πρέπει να συμμορφώνονται οι τεχνολογικοί συνεργάτες τους.

5.4 Συνεργασία

Είναι σημαντικό για τους επαγγελματίες προμηθειών τεχνολογίας να υποστηρίζουν τους CIO στην ανταπόκριση στις προκλήσεις που παρουσιάζουν οι απειλές στον κυβερνοχώρο. Ένα από τα πιο συνήθη πράγματα είναι μια ισχυρή στρατηγική προμήθειας που ενσωματώνει την επιμέλεια γύρω από τον έλεγχο προμηθευτών ως μέρος της διαδικασίας ενσωμάτωσης. Οι συμβατικές διατάξεις πρέπει επίσης να αποτελούν μέρος των συμφωνιών, έτσι ώστε να πραγματοποιείται μετέπειτα και διαρκής παρακολούθηση του κινδύνου της εφοδιαστικής αλυσίδας.

5.5 Συνεργασίες

Το τοπίο των προμηθευτών και λύσεων της κυβερνοασφάλειας είναι γεμάτο και οι εταιρείες πρέπει να επιλέξουν συνεργάτες που μειώνουν τον κίνδυνο κυβερνοεπίθεσης στο μοναδικό τεχνολογικό τους αποτύπωμα. Αυτό απαιτεί έναν εξαντλητικό έλεγχο κυβερνοασφάλειας, για τον εντοπισμό κενών και τρωτών σημείων.

5.6 Διαχείριση κινδύνου

Οι επιχειρήσεις πρέπει να γνωρίζουν πού βρίσκονται στο φάσμα κινδύνου. Είναι σημαντικό να κατανοήσουμε τις διαφορετικές απαιτήσεις σχετικά με την ισχυρή διαχείριση και διακυβέρνηση κινδύνων στον κυβερνοχώρο. Ο τρόπος με τον οποίο οι επιχειρήσεις κυβερνούν, εντοπίζουν και ανταποκρίνονται στον κίνδυνο είναι ζωτικής σημασίας για τη διαχείριση των αναγκών στον κυβερνοχώρο.

5.7 Μείνετε ενημερωμένοι

Ο ρυθμός της αλλαγής στην τεχνολογία είναι αμείλικτος. Οι επαγγελματίες που προμηθεύονται τεχνολογικά προϊόντα πρέπει να παραμένουν ενημερωμένοι σχετικά με τις τεχνολογικές τους γνώσεις, εάν θέλουν να συμβουλεύουν σωστά τους CIO και τους CFO για τις καλύτερες επενδύσεις στον κυβερνοχώρο.

6. Καλές πρακτικές σύμφωνα με τον NIST

Σύμφωνα με τον Nist[12] (National Institute of Standards and Technology) η κυβερνοασφάλεια στην εφοδιαστική αλυσίδα δεν μπορεί να θεωρηθεί μόνο ως πρόβλημα πληροφορικής. Οι κίνδυνοι της αλυσίδας εφοδιασμού στον κυβερνοχώρο αγγίζουν την προμήθεια, τη διαχείριση προμηθευτών, τη συνέχεια και την ποιότητα της εφοδιαστικής αλυσίδας, την ασφάλεια των μεταφορών και πολλές άλλες λειτουργίες σε όλη την επιχείρηση και απαιτούν συντονισμένη προσπάθεια για την αντιμετώπισή τους.

6.1 Αρχές ασφάλειας της αλυσίδας εφοδιασμού στον κυβερνοχώρο:

1. Ανάπτυξη των άμυνων ασφαλείας με βάση την αρχή ότι τα συστήματά θα παραβιαστούν. Όταν κάποιος ξεκινά από την υπόθεση ότι μια παραβίαση είναι αναπόφευκτη, αλλάζει τη μήτρα απόφασης στα επόμενα βήματα. Το ερώτημα δεν είναι απλώς πώς μπορεί να αποτραπεί μια παραβίαση, αλλά πώς να μετριαστεί η ικανότητα ενός εισβολέα να εκμεταλλευτεί τις πληροφορίες στις οποίες έχει πρόσβαση και πώς να ανακτήσει από την παραβίαση.
2. Η κυβερνοασφάλεια δεν είναι ποτέ απλώς ένα τεχνολογικό πρόβλημα, είναι πρόβλημα ανθρώπων, διαδικασιών και γνώσης. Οι παραβιάσεις καταλήγουν να αφορούν λιγότερο μια τεχνολογική αποτυχία και περισσότερο με ανθρώπινο λάθος. Τα συστήματα ασφαλείας πληροφορικής δεν θα προστατεύουν κρίσιμες πληροφορίες και πνευματική ιδιοκτησία εκτός εάν οι εργαζόμενοι σε όλη την αλυσίδα εφοδιασμού χρησιμοποιούν ασφαλείς πρακτικές ασφάλειας στον κυβερνοχώρο.
3. Η ασφάλεια είναι ασφάλεια. Δεν πρέπει να υπάρχει χάσμα μεταξύ της φυσικής και της ασφάλειας στον κυβερνοχώρο. Μερικές φορές οι κακοί εκμεταλλεύονται τα κενά στη φυσική ασφάλεια για να εξαπολύσουν επίθεση στον κυβερνοχώρο. Με την ίδια λογική, ένας εισβολέας που αναζητά τρόπους πρόσβασης σε μια φυσική τοποθεσία μπορεί να εκμεταλλευτεί ευπάθειες στον κυβερνοχώρο για να αποκτήσει πρόσβαση.

6.2 Βασικοί κίνδυνοι της αλυσίδας εφοδιασμού στον κυβερνοχώρο

Οι κίνδυνοι της αλυσίδας εφοδιασμού στον κυβερνοχώρο καλύπτουν μεγάλο μέρος. Ορισμένες από τις ανησυχίες περιλαμβάνουν κινδύνους από:

- Third party services ή προμηθευτές από υπηρεσίες καθαριότητας έως μηχανική λογισμικού με φυσική ή εικονική πρόσβαση σε συστήματα πληροφοριών, κώδικα λογισμικού ή IP.
- Κακές πρακτικές ασφάλειας πληροφοριών από προμηθευτές κατώτερης βαθμίδας.
- Παραβιασμένο λογισμικό ή υλικό που αγοράστηκε από προμηθευτές.
- Τρωτά σημεία ασφάλειας λογισμικού στη διαχείριση της αλυσίδας εφοδιασμού ή στα συστήματα προμηθευτών.
- Πλαστό υλικό ή υλικό με ενσωματωμένο κακόβουλο λογισμικό.
- Αποθήκευση δεδομένων τρίτων

6.3 Παραδείγματα βέλτιστων πρακτικών για την αλυσίδα εφοδιασμού στον κυβερνοχώρο

Οι εταιρείες έχουν υιοθετήσει μια ποικιλία πρακτικών που τις βοηθούν να διαχειρίζονται τους κινδύνους της αλυσίδας εφοδιασμού στον κυβερνοχώρο. Αυτές οι πρακτικές περιλαμβάνουν:

- Είναι τεκμηριωμένη η διαδικασία σχεδιασμού λογισμικού/υλισμικού του προμηθευτή;
- Ο μετριασμός γνωστών τρωτών σημείων συνυπολογίζεται στο σχεδιασμό του προϊόντος (μέσω της αρχιτεκτονικής του προϊόντος, των τεχνικών προστασίας κατά το χρόνο εκτέλεσης, της αναθεώρησης κώδικα);
- Πώς μένει ενημερωμένος ο προμηθευτής σχετικά με τις αναδυόμενες ευπάθειες; Ποιες είναι οι δυνατότητες του προμηθευτή για την αντιμετώπιση νέων ευπαθειών «zero day»;
- Ποιοι έλεγχοι υπάρχουν για τη διαχείριση και την παρακολούθηση των διαδικασιών παραγωγής;
- Πώς γίνεται η διαχείριση διαμόρφωσης; Διασφάλιση ποιότητας? Πώς ελέγχεται για ποιότητα κώδικα ή τρωτά σημεία;
- Ποια επίπεδα προστασίας και ανίχνευσης κακόβουλου λογισμικού εκτελούνται;

- Ποια βήματα λαμβάνονται για τα προϊόντα tamper proof; Είναι κλειστές οι πόρτες προς τον έξω κόσμο;
- Ποια μέτρα φυσικής ασφάλειας υπάρχουν;
- Ποιοι έλεγχοι πρόσβασης υπάρχουν, τόσο στον κυβερνοχώρο όσο και στον φυσικό χώρο; Πώς τεκμηριώνονται και ελέγχονται;
- Πώς προστατεύουν και αποθηκεύουν δεδομένα πελατών;
- Πώς κρυπτογραφούνται τα δεδομένα;
- Πόσο καιρό διατηρούνται τα δεδομένα;
- Πώς καταστρέφονται τα δεδομένα όταν λυθεί η εταιρική σχέση;
- Τι είδους έλεγχοι ιστορικού των εργαζομένων διενεργούνται και πόσο συχνά;
- Ποιες προσδοκίες πρακτικών ασφαλείας έχουν τεθεί για τους προμηθευτές; Πώς αξιολογείται η τήρηση αυτών των προτύπων;
- Πόσο ασφαλής είναι η διαδικασία διανομής;
- Έχουν τεκμηριωθεί σαφώς τα εγκεκριμένα και εξουσιοδοτημένα κανάλια διανομής;
- Ποια είναι η στρατηγική κινδύνου και μετριασμού απόρριψης εξαρτημάτων;
- Πώς διασφαλίζει ο πωλητής την ασφάλεια μέσω του κύκλου ζωής του προϊόντος;

6.4 Παραδείγματα βέλτιστων πρακτικών της αλυσίδας εφοδιασμού στον κυβερνοχώρο

Οι εταιρείες έχουν υιοθετήσει μια ποικιλία πρακτικών που τις βοηθούν να διαχειριστούν τους κινδύνους της αλυσίδας εφοδιασμού στον κυβερνοχώρο. Αυτές οι πρακτικές περιλαμβάνουν:

- Οι απαιτήσεις ασφαλείας περιλαμβάνονται σε κάθε RFP και σύμβαση.
- Μόλις ένας προμηθευτής γίνει αποδεκτός στην επίσημη αλυσίδα εφοδιασμού, μια ομάδα ασφαλείας συνεργάζεται μαζί του επιτόπου για να αντιμετωπίσει τυχόν τρωτά σημεία και κενά ασφαλείας.
- Πολιτικές για παύση συνεργασίας σε σχέση με προϊόντα πωλητών που είτε είναι πλαστά είτε δεν ταιριάζουν με τις προδιαγραφές.
- Οι αγορές εξαρτημάτων ελέγχονται αυστηρά. Οι αγορές εξαρτημάτων από εγκεκριμένους προμηθευτές είναι προεπιλεγμένες. Τα ανταλλακτικά που

αγοράζονται από άλλους προμηθευτές αποσυσκευάζονται, ελέγχονται και ακτινογραφούνται πριν γίνουν αποδεκτά.

- Καθιερώνονται Προγράμματα Ανάπτυξης Κύκλου Ζωής Ασφαλούς Λογισμικού και εκπαίδευση για όλους τους μηχανικούς στον κύκλο ζωής.
- Ο πηγαίος κώδικας λαμβάνεται για όλο το λογισμικό που αγοράζουν σαν οργανισμός.
- Το λογισμικό και το υλικό έχουν handshake security. Οι διαδικασίες ασφαλούς εκκίνησης αναζητούν κωδικούς ελέγχου ταυτότητας και το σύστημα δεν θα εκκινήσει εάν οι κωδικοί δεν αναγνωρίζονται.
- Η αυτοματοποίηση των καθεστώτων κατασκευής και δοκιμών μειώνει τον κίνδυνο ανθρώπινης παρέμβασης.

7. Οδηγός Διαχείρισης – Υλοποίησης ενός σχεδίου για την αντιμετώπιση του κινδύνου στην εφοδιαστική αλυσίδα.

Μέσα από αυτή την εργασία θα καθοριστούν οι απαιτήσεις για ένα σύστημα διαχείρισης ασφάλειας, συμπεριλαμβανομένων αυτών των πτυχών ζωτικής σημασίας για τη διασφάλιση της ασφάλειας της εφοδιαστικής αλυσίδας. Ο οργανισμός μπορεί να στηριχθεί σε βασικά εργαλεία που υπάρχουν διαθέσιμα όπως αυτό που αναφέρθηκε παραπάνω (NIST), αλλά και το πρότυπο ISO 28000 Security and resilience - Security management systems – Requirements for the supply chain.[13]

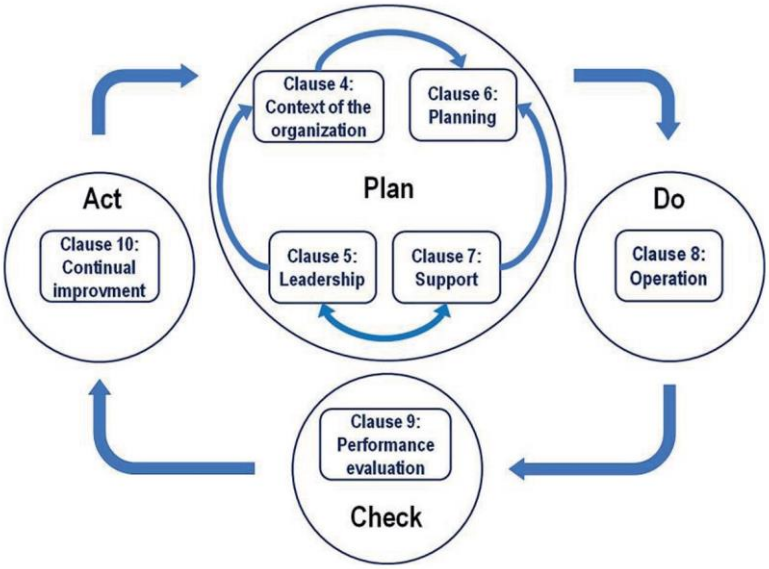
Ο οργανισμός θα πρέπει να:

- Αξιολογεί το περιβάλλον ασφαλείας στο οποίο δραστηριοποιείται συμπεριλαμβανομένης της αλυσίδας εφοδιασμού της (συμπεριλαμβανομένης εξαρτήσεις και αλληλεξαρτήσεις).
- Καθορίζει εάν υπάρχουν επαρκή μέτρα ασφαλείας για την αποτελεσματική διαχείριση των κινδύνων που σχετίζονται με την ασφάλεια.

- Διαχειρίζεται τη συμμόρφωση με νομοθετικές, ρυθμιστικές και εθελοντικές υποχρεώσεις στις οποίες ο οργανισμός είναι υποχρεωμένος, και
- Διαμορφώσει τις διαδικασίες και τους ελέγχους ασφαλείας, συμπεριλαμβανομένων των σχετικών διεργασιών και ελέγχους της εφοδιαστικής αλυσίδας για την επίτευξη των στόχων του οργανισμού.

Ο οργανισμός πρέπει να αξιολογήσει το περιβάλλον ασφαλείας στο οποίο δραστηριοποιείται και να προσδιορίσει εάν υπάρχουν επαρκή μέτρα ασφαλείας για την αποτελεσματική διαχείριση των κινδύνων που σχετίζονται με την ασφάλεια και εάν υπάρχουν ήδη κανονιστικές απαιτήσεις σχετικά με την ασφάλεια με τις οποίες συμμορφώνεται ο οργανισμός. Εάν εντοπιστούν στόχοι ασφάλειας που δεν καλύπτονται, ο οργανισμός οφείλει να εφαρμόζει ελέγχους για την επίτευξη αυτών των στόχων. Η διαχείριση της ασφάλειας συνδέεται με πολλές πτυχές της επιχειρηματικής διαχείρισης. Περιλαμβάνει όλες τις δραστηριότητες που ελέγχονται ή επηρεάζονται από οργανισμούς συμπεριλαμβανομένων, ενδεικτικά, εκείνων που επηρεάζουν την γραμμή παραγωγής. Όλες οι δραστηριότητες, λειτουργίες και διεργασίες πρέπει να λαμβάνονται υπόψη που έχουν αντίκτυπο στην διαχείριση της ασφάλειας του οργανισμού συμπεριλαμβανομένης της εφοδιαστικής αλυσίδας του. Όσον αφορά την αλυσίδα εφοδιασμού, πρέπει να ληφθεί υπόψη ότι οι αλυσίδες εφοδιασμού είναι δυναμικής φύσης. Ως εκ τούτου, ορισμένοι οργανισμοί που διαχειρίζονται πολλαπλές αλυσίδες εφοδιασμού μπορεί να αναζητήσουν βοήθεια απο τους παρόχους τους για να επιτύχουν τα σχετικά πρότυπα ασφαλείας ως προϋπόθεση για τη συμπερίληψη σε αυτήν την αλυσίδα εφοδιασμού προκειμένου να πληρούνται οι απαραίτητες απαιτήσεις για τη διαχείριση της ασφάλειας.

Ένας οργανισμός θα πρέπει να εφαρμόζει το μοντέλο «Plan-Do-Check-Act» (PDCA) στον σχεδιασμό, την εγκαθίδρυση, την εφαρμογή, τη λειτουργία, τη παρακολούθηση, την επανεξέταση, τη διατήρηση και τη συνεχής βελτίωση της αποτελεσματικότητας ενός συστήματος διαχείρισης ασφάλειας του οργανισμού.



Εικόνα 2 Plan-Do-Check-Act (PDCA)

Plan: Καθιέρωση πολιτικής ασφάλειας, στόχους, ελέγχους, διεργασίες και διαδικασίες που σχετίζονται με τη βελτίωση της ασφάλειας προκειμένου να παραχθούν αποτελέσματα που ευθυγραμμίζονται με τις γενικές πολιτικές και τους στόχους του οργανισμού.

Do: Εφαρμογή και λειτουργία της πολιτικής ασφάλειας, των ελέγχων, των διεργασιών και των διαδικασιών

Check: Παρακολούθηση και επανεξέταση της απόδοσης σε σχέση με την πολιτική και τους στόχους ασφαλείας. Αναφορές σχετικά με τα αποτελέσματα στη διοίκηση για επανεξέταση και προσδιορισμός και εξουσιοδοτημένες δράσεις αποκατάστασης και βελτίωσης.

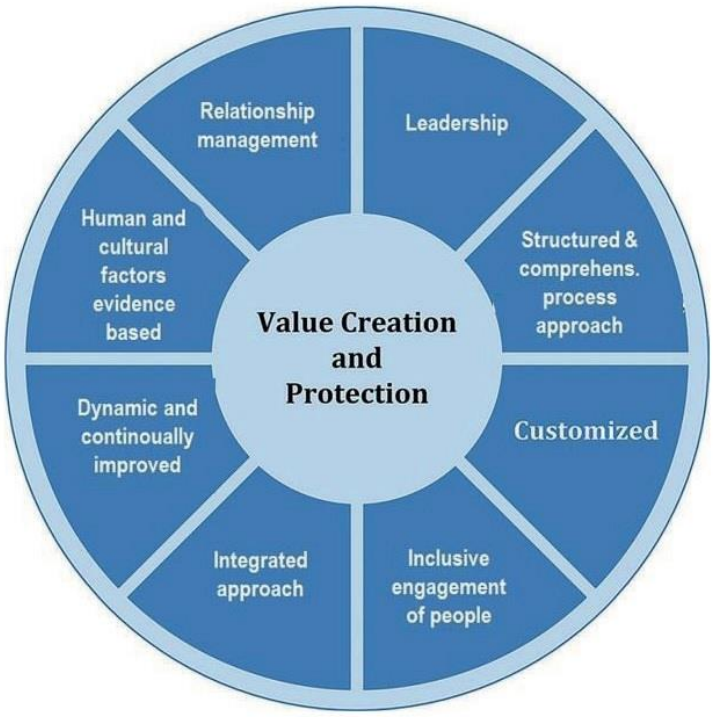
Act: Διατήρηση και βελτίωση του συστήματος διαχείρισης ασφάλειας (SMS), κάνοντας διορθωτικές κινήσεις, με βάση τα αποτελέσματα της επανεξέτασης και της επανεκτίμησης της διοίκησης στο πεδίο εφαρμογής της πολιτικής και των στόχων του SMS και της ασφάλειας.

8. Πλαίσιο Οργάνωσης ενός Οργανισμού

1) Ο οργανισμός πρέπει να έχει οργανώσει και να έχει κατανοήσει το πλαίσιο λειτουργίας του. Ο οργανισμός πρέπει να καθορίζει εξωτερικά και εσωτερικά ζητήματα που σχετίζονται με τον σκοπό του και έχει σαν αποτέλεσμα να επηρεάζει

την ικανότητα του να επιτύχει το επιδιωκόμενο αποτέλεσμα από το σύστημα που έχει υλοποιήσει διαχείρισης ασφάλειας του.

2) Ο οργανισμός πρέπει να κατανοήσει τις ανάγκες του και τις προσδοκίες του. Πρέπει να καθορίσει τα ενδιαφερόμενα μέρη που σχετίζονται με το σύστημα διαχείρισης ασφάλειας αλλά και τις σχετικές απαιτήσεις αυτών των ενδιαφερόμενων.
3) Ο οργανισμός πρέπει να εφαρμόζει όλες τις νομικές, νομοθετικές και άλλες ρυθμιστικές απαιτήσεις ασφαλείας. Για να το επιτύχει αυτό πρέπει να έχει εφαρμόζει και να διατηρεί μια διαδικασία για τον εντοπισμό, την πρόσβαση και την αξιολόγηση των εφαρμοστέων νομικών και κανονιστικών απαιτήσεων που σχετίζονται με την ασφάλεια του. Στην συνέχεια θα πρέπει να διασφαλίζει ότι αυτές οι ισχύουσες νομικές, κανονιστικές και άλλες απαιτήσεις λαμβάνονται υπόψη κατά την εφαρμογή και τη διατήρηση του συστήματος διαχείρισης ασφάλειας. Όλες αυτές οι πληροφορίες θα πρέπει να συλλέγονται να τεκμηριώνονται και είναι πάντα ενήμερες. Τέλος όλες αυτές οι πληροφορίες θα πρέπει να κοινοποιούνται στα σχετικά ενδιαφερόμενα μέρη, κατά περίπτωση.
4) Σκοπός της διαχείρισης ασφαλείας εντός του οργανισμού είναι η δημιουργία και ειδικότερα η προστασία της αξίας. Ο οργανισμός θα πρέπει να εφαρμόζει κατά κύριο λόγο τις ακόλουθες αρχές:



Εικόνα 3: Αρχές δημιουργίας αξίας και προστασία

i) Leadership: Η ηγεσία θα πρέπει σε όλα τα επίπεδα να δημιουργήσει ενότητα σκοπού και κατεύθυνσης ώστε να δημιουργήσουν συνθήκες ώστε να υλοποιηθούν οι στρατηγικές, οι διαδικασίες των πολιτικών που έχουν καθοριστεί και τους πόρους τους οργανισμού για την επίτευξη των στόχων.
ii) Structured & Comprehens process approach: Μια δομημένη και ολοκληρωμένη προσέγγιση για τη διαχείριση της ασφάλειας, συμπεριλαμβανομένης της αλυσίδας εφοδιασμού συμβάλλουν σε συνεπή και συγκρίσιμα αποτελέσματα που επιτυγχάνονται πιο αποτελεσματικά και αποδοτικά όταν οι δραστηριότητες κατανοούνται και διαχειρίζονται ως αλληλένδετες διαδικασίες που λειτουργούν ως ένα συνεκτικό σύστημα
iii) Customized: Το σύστημα διαχείρισης ασφάλειας πρέπει να είναι προσαρμοσμένο και ανάλογο με αυτό του οργανισμού και να βασίζεται στο εξωτερικό και στο εσωτερικό πλαίσιο και τις ανάγκες και να σχετίζεται με τους στόχους του οργανισμού.
iv) Inclusive engagement of people: Ο οργανισμός θα πρέπει να εμπλέξει τα ενδιαφερόμενα μέρη κατάλληλα και έγκαιρα και να εξετάσει τις γνώσεις, τις απόψεις και τις αντιλήψεις τους κατάλληλα για τη βελτίωση της ευαισθητοποίησης και τη διευκόλυνση της ενημέρωσης για τη διαχείριση ασφάλειας. Ο οργανισμός πρέπει να διασφαλίζει, ότι όλοι σε όλα τα επίπεδα σέβονται και συμμετέχουν σε οτιδήποτε μπορεί να βοηθήσει τον οργανισμό.
v) Integrated approach: Η διαχείριση της ασφάλειας αποτελεί αναπόσπαστο μέρος όλων των οργανωτικών δραστηριοτήτων. Θα πρέπει να ενσωματωθεί με όλα τα άλλα συστήματα διαχείρισης του οργανισμού. Η διαχείριση κινδύνων του οργανισμού - είτε είναι επίσημη, ανεπίσημη ή διαισθητική, θα πρέπει να ενσωματωθεί στο σύστημα διαχείρισης ασφάλειας.
vi) Dynamic and continually improved: Ο οργανισμός θα πρέπει να έχει μια συνεχή εστίαση στη βελτίωση μέσω της μάθησης και της εμπειρίας για να διατηρήσει το επίπεδο απόδοσης, να αντιδρά στις αλλαγές και να δημιουργεί νέες ευκαιρίες καθώς αλλάζει το εξωτερικό και εσωτερικό πλαίσιο του οργανισμού.
vii) Human and cultural factors evidence based: Η ανθρώπινη συμπεριφορά και η κουλτούρα επηρεάζουν σημαντικά όλες τις πτυχές της διαχείρισης της ασφάλειας και θα πρέπει να λαμβάνονται υπόψη σε κάθε επίπεδο και

στάδιο. Οι αποφάσεις θα πρέπει να βασίζονται στην ανάλυση και αξιολόγηση δεδομένων και πληροφοριών για να διασφαλίζεται ότι έχουν ως αποτέλεσμα μεγαλύτερη αντικειμενικότητα, εμπιστοσύνη στη λήψη αποφάσεων και είναι πιο πιθανό να παράγουν τα επιθυμητά αποτελέσματα. Θα πρέπει επίσης να ληφθούν υπόψη οι ατομικές αντιλήψεις.

viii) Relationship management: Για διαρκή επιτυχία, ο οργανισμός θα πρέπει να διαχειρίζεται τις σχέσεις του με όλα τα σχετικά ενδιαφερόμενα μέρη, καθώς ενδέχεται να επηρεάσουν την απόδοση του οργανισμού.

5) Ο οργανισμός πρέπει να προσδιορίσει το πεδίο εφαρμογής του συστήματος διαχείρισης ασφαλείας, να καθορίσει τα όρια και της δυνατότητα που έχει το σύστημα διαχείρισης ασφάλειας κατά την εφαρμογή του. Κατά τον καθορισμό αυτού του πεδίου εφαρμογής ο οργανισμός πρέπει να λάβει υπόψιν:
   i) Την κατανόηση του οργανισμού όπως αναφέρθηκε παραπάνω
   ii) Την κατανόηση των αναγκών και των προσδοκιών των ενδιαφερόμενων

   όπως αναφέρθηκε στις προηγούμενες παραγράφους. Το πεδίο εφαρμογής είναι διαθέσιμο ως τεκμηριωμένη πληροφορία. Όταν ένας οργανισμός επιλέγει να παράσχει εξωτερικά οποιαδήποτε διαδικασία που επηρεάζει τη συμμόρφωση με το σύστημα διαχείρισης ασφαλείας του, ο οργανισμός διασφαλίζει ότι αυτές οι διαδικασίες ελέγχονται. Οι απαραίτητοι έλεγχοι και οι αρμοδιότητες τέτοιων εξωτερικά παρεχόμενων διαδικασιών προσδιορίζονται στο πλαίσιο του συστήματος διαχείρισης ασφάλειας.

9. Ηγεσία του Οργανισμού

9.1 Ικανότητες Ηγεσίας

Η ανώτατη διοίκηση του οργανισμού πρέπει να επιδεικνύει τις ηγετικές της ικανότητες και τις δεσμεύσεις της όσον αφορά το σύστημα διαχείρισης ασφάλειας εφαρμόζοντας τα παρακάτω:

i. Να διασφαλίσει ότι η πολιτική ασφάλειας και οι στόχοι ασφάλειας έχουν καθοριστεί και είναι συμβατοί με τη στρατηγική κατεύθυνση του οργανισμού.
ii. Να διασφαλίσει ότι εντοπίζονται και παρακολουθούνται οι απαιτήσεις και οι προσδοκίες των ενδιαφερομένων μερών του οργανισμού και ότι λαμβάνονται κατάλληλα και έγκαιρα μέτρα για τη διαχείριση αυτών των προσδοκιών,

διασφαλίζοντας την ενσωμάτωση των απαιτήσεων του συστήματος διαχείρισης ασφάλειας στις επιχειρηματικές διαδικασίες του οργανισμού.

iii. Να διασφαλίσει την διαθεσιμότητα των πόρων που απαιτούνται για το σύστημα διαχείρισης ασφάλειας.

iv. Να κοινοποιήσει προς όλα τα ενδιαφερόμενα μέρη τη σημασία της αποτελεσματικής διαχείρισης της ασφάλειας και της συμμόρφωσης με τις απαιτήσεις του συστήματος διαχείρισης ασφάλειας

v. Να διασφαλίσει ότι το σύστημα διαχείρισης ασφάλειας επιτυγχάνει τα επιδιωκόμενα αποτελέσματα.

vi. Να διασφαλίσει τη βιωσιμότητα των αντικειμένων, στόχων και προγραμμάτων διαχείρισης της ασφάλειας.

vii. Να διασφαλίσει ότι τυχόν προγράμματα ασφαλείας που παράγονται από άλλα μέρη του οργανισμού, συμπληρώνουν το σύστημα διαχείρισης ασφάλειας όλου του οργανισμού.

viii. Να καθοδηγεί και να υποστηρίζει τα πρόσωπα ώστε να συμβάλουν στην αποτελεσματικότητα του συστήματος διαχείρισης της ασφάλειας.

ix. Να προωθεί τη συνεχή βελτίωση του συστήματος διαχείρισης ασφάλειας του οργανισμού.

x. Να υποστηρίζει άλλους σχετικούς διευθυντικούς ρόλους για να επιδείξουν την ηγετική τους θέση όπως ισχύει στους τομείς ευθύνης τους.

9.2 Πολιτική του Οργανισμού

Η ανώτατη διοίκηση πρέπει να θεσπίσει μια πολιτική ασφαλείας. Η πολιτική αυτή πρέπει να είναι κατάλληλη για το σκοπό του οργανισμού και να παρέχει ένα πλαίσιο για τον καθορισμό των στόχων ασφαλείας. Η πολιτική αυτή επίσης πρέπει να περιλαμβάνει την δέσμευση για την ικανοποίηση των ισχυουσών απαιτήσεων. Βασικός πυλώνας είναι και η δέσμευση της για συνεχή βελτίσωσξ του συστήματος διαχείρισης και ασφάλειας και να εξετάζει τις αρνητικές επιπτώσεις που μπορεί να έχει η πολιτική ασφαλείας, στα αντικείμενα, τους στόχους, τα προγράμματα κ.λπ. και σε άλλες πτυχές του οργανισμού.

Η πολιτική ασφαλείας που έχει λοιπόν θεσπίσει η ανώτατη διοίκηση πρέπει να έχει κάποιες σημαντικές απαιτήσεις όπως:

i) Να είναι συνεπής με άλλες οργανωτικές πολιτικές
ii) Να είναι συνεπής με τη συνολική αξιολόγηση κινδύνου ασφαλείας του οργανισμού
iii) Να προβλέπει την αναθεώρηση της σε περίπτωση εξαγοράς ή συγχώνευσης με άλλους οργανισμούς ή άλλων αλλαγών στο επιχειρηματικό πεδίο του οργανισμού που ενδέχεται να επηρεάσουν τη συνέχεια ή τη συνάφεια του συστήματος διαχείρισης ασφάλεια.
iv) Να περιγράφει και να κατανέμει την κύρια λογοδοσία και την ευθύνη για τα αποτελέσματα.
v) Να είναι διαθέσιμα ως τεκμηριωμένες πληροφορίες
vi) Να κοινοποιούνται κατάλληλα εντός του οργανισμού
vii) Να είναι στη διάθεση οποιουδήποτε ενδιαφερόμενου κατά περίπτωση.

Οι οργανισμοί μπορούν να επιλέξουν να έχουν μια λεπτομερή πολιτική διαχείρισης ασφάλειας για εσωτερική χρήση, η οποία θα παρέχει επαρκείς πληροφορίες και οδηγίες για την καθοδήγηση του συστήματος διαχείρισης ασφάλειας (τμήματα του οποίου μπορεί να είναι εμπιστευτικά) και να έχουν μια συνοπτική (μη εμπιστευτική) έκδοση που περιέχει τους γενικούς στόχους για τα ενδιαφερόμενα μέρη και σε άλλα τρίτα ενδιαφερόμενα μέρη.

9.3 Ρόλοι, ευθύνες και εξουσίες

Η ανώτατη διοίκηση θα διασφαλίζει ότι οι ευθύνες και οι αρχές για τους σχετικούς ρόλους ανατίθενται και κοινοποιούνται εντός του οργανισμού. Η ανώτατη διοίκηση θα αναθέσει την ευθύνη και την εξουσία για:

i. διασφάλιση ότι το σύστημα διαχείρισης ασφάλειας συμμορφώνεται με τις απαιτήσεις του παρόντος εγγράφου.
ii. υποβολή εκθέσεων σχετικά με την απόδοση του συστήματος διαχείρισης ασφάλειας στην ανώτατη διοίκηση.

10. Σχεδιασμός

10.1 Δράσεις για την αντιμετώπιση κινδύνων και ευκαιριών.

Κατά τον προγραμματισμό του συστήματος διαχείρισης ασφάλειας, ο οργανισμός οφείλει να εξετάσει τα ζητήματα που αναφέρονται στο οργανισμό όπως αναφέρθηκε

παραπάνω, δηλαδή την κατανόηση του σκοπού του και το πλαίσιο του οργανισμού καθώς και τις ανάγκες και τις προσδοκίες του, ώστε να καθοριστούν και να προσδιοριστούν οι κίνδυνοι που πρέπει να αντιμετωπιστούν. Ειδικότερα πρέπει να παρέχει την διαβεβαίωση ότι το σύστημα διαχείρισης ασφάλειας μπορεί να επιτύχει τα επιδιωκόμενα αποτελέσματα. Μέσω του συστήματος αυτού πρέπει να υπάρξει πρόληψη ή και μείωση των ανεπιθύμητων ενεργειών καθώς και η συνεχής βελτίωση. Ο Οργανισμός οφείλει να προγραμματίσει όλες τις απαραίτητες ενέργειες για την αντιμετώπιση των κινδύνων να ενσωματώσει και να εφαρμόσει τις ενέργειες στις διαδικασίες του συστήματος διαχείρισης ασφάλειας και να αξιολογήσει την αποτελεσματικότητα αυτών των ενεργειών. Ο σκοπός της διαχείρισης κινδύνων είναι η δημιουργία και η προστασία της αξίας κατά συνέπεια η διαχείριση του κινδύνου πρέπει να ενσωματωθεί στο σύστημα διαχείρισης ασφάλειας.

10.2 Προσδιορισμός κινδύνων για την ασφάλεια και εντοπισμός ευκαιριών.

Ο προσδιορισμός των κινδύνων για την ασφάλεια και ο εντοπισμός και η εκμετάλλευση ευκαιριών απαιτεί μια προληπτική αξιολόγηση κινδύνου, η οποία θα πρέπει να περιλαμβάνει την εξέταση, αλλά όχι να περιορίζεται σε:

i. φυσικές ή λειτουργικές αποτυχίες και κακόβουλες ή εγκληματικές πράξεις
ii. περιβαλλοντικοί, ανθρώπινοι και πολιτιστικοί παράγοντες και άλλο εσωτερικό ή εξωτερικό πλαίσιο συμπεριλαμβανομένων παραγόντων εκτός του ελέγχου του οργανισμού που επηρεάζουν την ασφάλεια του οργανισμού
iii. ο σχεδιασμός, η εγκατάσταση, η συντήρηση και η αντικατάσταση του εξοπλισμού ασφαλείας.
iv. τη διαχείριση πληροφοριών, δεδομένων, γνώσης και επικοινωνίας του οργανισμού
v. πληροφορίες που σχετίζονται με απειλές και τρωτά σημεία ασφάλειας

10.3 Αντιμετώπιση κινδύνων για την ασφάλεια και εκμετάλλευση ευκαιριών

Η αξιολόγηση του εντοπισθέντος κινδύνου ασφάλειας παρέχει στοιχεία για την συνολική διαχείριση κινδύνου του οργανισμού. Μπορεί επίσης να προσδιοριστεί ο τρόπος αντιμετώπισης του κινδύνου και ο στόχος της διαχείρισης ασφαλείας. Μέσω αυτού μπορούν να υπάρξουν συγκεκριμένες διαδικασίες διαχείρισης ασφαλείας. Μέσω του εντοπισμού ενός κινδύνου μπορεί να αξιολογηθεί ο σχεδιασμός, η προδιαγραφή και η εφαρμογή του συστήματος διαχείρισης ασφάλειας. Επίσης γίνεται προσδιορισμός των επαρκών πόρων, συμπεριλαμβανομένου του προσωπικού καθώς και ο προσδιορισμός των αναγκών κατάρτισης και του απαιτούμενου επιπέδου ικανότητας.

10.4 Στόχοι ασφαλείας και σχεδιασμός για την επίτευξή τους

Ένας οργάνισμός οφείλει να θεσπίζει στόχους ασφαλείας σε σχετικές λειτουργίες και επίπεδα. Πιο συγκεκριμένα οι στόχοι ασφαλείας πρέπει να είναι συνεπείς με την πολιτική ασφαλείας που έχει χαράξει ο οργανισμός. Πρέπει να έχουν αριθμηθεί ώστε να υπάρχει καλυτερη οργάνωση εφόσον είναι εφικτό

α) είναι συνεπείς με την πολιτική ασφαλείας

β) είναι μετρήσιμοι (εάν είναι εφικτό)

γ) λαμβάνουν υπόψη τις κατάλληλες απαιτήσεις

δ) ελέγχονται

ε) επικοινωνούνται

στ) ενημερώνονται κατά περίπτωση

Ο ογκανισμός οφείλει να διατηρεί τεκμηριωμένες πληροφορίες σχετικά με τους στόχους ασφαλείας.

Ο οργανισμός οφείλει να καθορίσει τους στόχους ασφαλείας του όταν σχεδιάζει τους τρόπους που θα τους επιτύχει. Πρέπει να καθορίσει:˝

- Τι θα γίνει
- Ποιοι πόροι θα απαιτηθούν
- Ποιος θα είναι ο υπεύθυνος
- Πότε θα έχει ολοκληρωθεί
- Πως θα αξιολογηθούν

Κατά την θέσπιση και την αναθεώρηση των στόχων ασφαλείας, ο οργανισμός πρέπει να λάβει υπόψη τις τεχνολογικές, ανθρώπινες, διοικητικές επιλογές αλλά και τις απόψεις και τις επιδράσεις με τους κατάλληλους ενδιαφερόμενους φορείς. Οι στόχοι ασφαλείας πρέπει να είναι συνεπείς με την δέσμευση της οργάνωσης για την συνεχή βελτίωση του οργανισμού. Στην περίπτωση όμως που ο οργανισμός καθορίσει την ανάγκη για αλλαγές στο σύστημα διαχείρισης ασφαλείας, αυτές πρέπει να γίνουν με συγκεκριμένο τρόπο και θα πρέπει να εξετάσει:

- Τον σκοπό των αλλαγών και τις πιθανές συνέπειες τους
- Την ακεραιότητα του συστήματος διαχείρισης ασφαλείας.
- Την διαθεσιμότητα πόρων αλλά και
- Την κατανομή των αρμοδιοτήτων και των ευθυνών.

11. Υποστήριξη

11.1 Πόροι

Ο οργανισμός καθορίζει και παρέχει τους πόρους που απαιτούνται για τη δημιουργία, την εφαρμογή, τη συντήρηση και τη συνεχή βελτίωση του συστήματος διαχείρισης ασφάλειας.

11.2 Ικανότητα

Ο οργανισμός πρέπει να προσδιορίσει την απαραίτητη ικανότητα του ή των προσώπων που εκτελούν όλες τις διεργασίες που επηρεάζουν τις επιδόσεις ασφαλείας του. Να διασφαλίζει ότι τα άτομα αυτά είναι ικανά βάσει της κατάλληλης εκπαίδευσης, κατάρτισης ή εμπειρίας και ότι έχουν λάβει την κατάλληλη άδεια ασφαλείας. Σε συγκεκριμένες περιπτώσεις να λάβουν μέτρα για την απόκτηση της απαραίτητης ικανότητας και να αξιολογήσουν την αποτελεσματικότητα των ενεργειών που έχουν ληφθεί. Και τέλος να διατηρεί τις κατάλληλες τεκμηριωμένες πληροφορίες ως αποδεικτικά στοιχεία. Οι ισχύουσες ενέργειες που εφαρμόζει ο οργανισμός μπορεί να περιλαμβάνουν την παροχή εκπαίδευσης, την καθοδήγηση ή την επανατοποθέτηση υπαλλήλων που απασχολούνται στον οργανισμό ή την πρόσληψη νέων αρμόδιων προσώπων.

11.3 Ευαισθητοποίηση

Τα άτομα που εκτελούν εργασίες υπό τον έλεγχο του οργανισμού πρέπει να γνωρίζουν την πολιτική ασφάλειας που έχει θεσπίσει ο οργανισμός καθώς και ότι η συμβουλή τους στην αποτελεσματικότητα του συστήματος διαχείρισης της ασφάλειας παίζει μεγάλο ρόλο, συμπεριλαμβανομένων των πλεονεκτημάτων της βελτιωμένης απόδοσης ασφάλειας. Επίσης πρέπει να γνωρίζουν όλες τις πιθανές συνέπειες της μη συμμόρφωσης με τις απαιτήσεις του συστήματος διαχείρισης ασφάλειας· και τους ρόλους και τις ευθύνες τους για την επίτευξη της συμμόρφωσης με την πολιτική και τις διαδικασίες διαχείρισης ασφάλειας καθώς και με τις απαιτήσεις του συστήματος διαχείρισης ασφάλειας, συμπεριλαμβανομένων των απαιτήσεων ετοιμότητας και αντίδρασης σε καταστάσεις έκτακτης ανάγκης.

11.4 Επικοινωνία

Ο οργανισμός καθορίζει τις εσωτερικές και εξωτερικές επικοινωνίες που σχετίζονται με το σύστημα διαχείρισης ασφάλειας. Συγκεκριμένα καθορίζει:

- Για το τι θα επικοινωνηθεί
- Πότε πρέπει να γίνει η επικοινωνία
- Με ποιον θα γίνει η απαραίτητη επικοινωνία
- Τον τρόπο που θα γίνει η επικοινωνία
- Την ευαισθησία των πληροφοριών πριν από τη διάδοση.

11.5 Τεκμηριωμένες πληροφορίες (Documented Information)

Το σύστημα διαχείρισης ασφάλειας του οργανισμού περιλαμβάνει σημαντικές τεκμηριωμένες πληροφορίες που απαιτούνται σε ένα έγγραφο. Οι τεκμηριωμένες πληροφορίες που προσδιορίζονται από τον οργανισμό ως απαραίτητες για την αποτελεσματικότητα του συστήματος διαχείρισης ασφάλειας. Οι τεκμηριωμένες πληροφορίες περιγράφουν τις ευθύνες και τις αρχές για την επίτευξη στόχων και στόχων διαχείρισης ασφάλειας, συμπεριλαμβανομένων των μέσων και των χρονοδιαγραμμάτων για την επίτευξη αυτών των αντικειμένων και στόχων. Η έκταση των τεκμηριωμένων πληροφοριών για ένα σύστημα διαχείρισης ασφάλειας μπορεί να διαφέρει από τον έναν οργανισμό στον άλλο λόγω κάποιων σημαντικών παραγόντων.

Ο πρώτος είναι το μέγεθος του οργανισμού και το είδος των δραστηριοτήτων, διαδικασιών, προϊόντων και υπηρεσιών του. Ο δεύτερος την πολυπλοκότητα των διαδικασιών και τις αλληλεπιδράσεις τους και ο τρίτος τις αρμοδιότητες των προσώπων. Ο οργανισμός καθορίζει την αξία των πληροφοριών, καθορίζει το απαιτούμενο επίπεδο ακεραιότητας και τους ελέγχους ασφαλείας για την αποτροπή μη εξουσιοδοτημένης πρόσβασης.

Κατά τη δημιουργία και την ενημέρωση τεκμηριωμένων πληροφοριών, ο οργανισμός διασφαλίζει τη σωστή μορφή αναγνώρισης και περιγραφής (π.χ. τίτλος, ημερομηνία, συγγραφέας ή αριθμός αναφοράς) (π.χ. γλώσσα, έκδοση λογισμικού, γραφικά) και μέσα (π.χ. έντυπα, ηλεκτρονικά). Επίσης εξετάζει και εγκρίνει την καταλληλόλητα και την επάρκεια.

Οι τεκμηριωμένες πληροφορίες που απαιτούνται από το σύστημα διαχείρισης ασφάλειας και από αυτό το έγγραφο ελέγχονται ώστε να διασφαλίζεται:

i. Να είναι διαθέσιμο και κατάλληλο για χρήση, όπου και όταν χρειάζεται
ii. Να προστατεύεται επαρκώς (π.χ. από απώλεια του απορρήτου, ακατάλληλη χρήση ή απώλεια ακεραιότητας)
iii. Να επανεξετάζεται περιοδικά και αναθεωρείται όπως απαιτείται και εγκρίνεται για την επάρκεια από εξουσιοδοτημένο προσωπικό
iv. Τα παρωχημένα έγγραφα, δεδομένα και πληροφορίες αφαιρούνται αμέσως από όλα τα σημεία έκδοσης και τα σημεία χρήσης ή διασφαλίζονται με άλλον τρόπο έναντι ακούσιας χρήσης
v. τα αρχειακά έγγραφα, τα δεδομένα και οι πληροφορίες που διατηρούνται για νομικούς ή λόγους διατήρησης γνώσεων ή και τα δύο να είναι κατάλληλα ταυτοποιημένα.

Για τον έλεγχο των τεκμηριωμένων πληροφοριών, ο οργανισμός θα ασχοληθεί με τις ακόλουθες δραστηριότητες, κατά περίπτωση:

- διανομή, πρόσβαση, ανάκτηση και χρήση·
- αποθήκευση και διατήρηση, συμπεριλαμβανομένης της διατήρησης της αναγνωσιμότητας·
- έλεγχος αλλαγών (π.χ. έλεγχος έκδοσης)

- διατήρηση και διάθεση.

Οι τεκμηριωμένες πληροφορίες εξωτερικής προέλευσης που προσδιορίζονται από τον οργανισμό ως απαραίτητες για τον σχεδιασμό και τη λειτουργία του συστήματος διαχείρισης ασφάλειας προσδιορίζονται, κατά περίπτωση, και ελέγχονται από τα αρμόδια άτομα.

12. Λειτουργία

12.1 Λειτουργικός σχεδιασμός και έλεγχος

Ο οργανισμός σχεδιάζει, εφαρμόζει και ελέγχει τις διαδικασίες που απαιτούνται για την ικανοποίηση των απαιτήσεων και για την υλοποίηση των ενεργειών που καθορίζονται κατά το καθορισμό στόχων ασφαλείας σε σχετικές λειτουργίες και επίπεδα, .όπως αναφέρθηκε παραπάνω. Συγκεκριμένα πρέπει να γίνει καθορισμός κριτηρίων για τις διαδικασίες, εφαρμογή ελέγχου των διαδικασιών σύμφωνα με τα κριτήρια και τέλος τήρηση τεκμηριωμένων πληροφοριών στο βαθμό που απαιτείται για να υπάρχει εμπιστοσύνη ότι οι διαδικασίες έχουν πραγματοποιηθεί όπως είχε προγραμματιστεί.

12.2 Προσδιορισμός διαδικασιών και δραστηριοτήτων

Ο οργανισμός προσδιορίζει εκείνες τις διαδικασίες και δραστηριότητες που είναι απαραίτητες για την επίτευξη:

i. συμμόρφωσης με την πολιτική ασφαλείας της
ii. συμμόρφωσης με νομικές, νομοθετικές και κανονιστικές απαιτήσεις ασφάλειας
iii. των στόχων διαχείρισης ασφάλειας
iv. της παράδοσης του συστήματος διαχείρισης ασφάλειας
v. το απαιτούμενο επίπεδο ασφάλειας της εφοδιαστικής αλυσίδας.

12.3 Risk assessment and treatment

Ο οργανισμός εφαρμόζει και διατηρεί διαδικασία αξιολόγησης και αντιμετώπισης κινδύνου. Ο οργανισμός θα πρέπει να προσδιορίζει τους κινδύνους ασφαλείας του, δίνοντάς τους προτεραιότητα στους πόρους που απαιτούνται για την ασφάλειά του.
Να επιλέξει και να εφαρμόσει επιλογές για την αντιμετώπιση αυτών των κινδύνων· και να προετοιμάσει και να εφαρμόσει σχέδια αντιμετώπισης κινδύνου. Οι κίνδυνοι αυτοί σχετίζονται με την ασφάλεια του οργανισμού και των ενδιαφερομένων μερών του.

12.4 Έλεγχοι

Οι διαδικασίες που αναφέρονται στο παραπάνω για τον προσδιορισμό διαδικασιών και δραστηριοτήτων θα περιλαμβάνουν ελέγχους για τη διαχείριση ανθρώπινου δυναμικού, καθώς και τον σχεδιασμό, την εγκατάσταση, τη λειτουργία, την αντικατάσταση και την τροποποίηση ειδών εξοπλισμού, οργάνων, τεχνολογίας πληροφοριών που σχετίζονται με την ασφάλεια, κατά περίπτωση. Όταν αναθεωρούνται υφιστάμενες ρυθμίσεις ή εισάγονται νέες ρυθμίσεις, οι οποίες θα μπορούσαν να έχουν αντίκτυπο στη διαχείριση της ασφάλειας, ο οργανισμός εξετάζει τους σχετικούς κινδύνους ασφαλείας πριν από την εφαρμογή τους. Οι νέες ή αναθεωρημένες ρυθμίσεις που θα εξεταστούν περιλαμβάνουν:

i. αναθεωρημένη οργανωτική δομή, ρόλοι ή αρμοδιότητες
ii. εκπαίδευση, ευαισθητοποίηση και διαχείριση ανθρώπινου δυναμικού
iii. αναθεωρημένη πολιτική διαχείρισης ασφάλειας, στόχους, διαδικασίες ή αντικείμενα εργασιών
iv. αναθεωρημένες διαδικασίες και διεργασίες
v. την εισαγωγή νέας υποδομής, εξοπλισμού ασφαλείας ή τεχνολογίας, η οποία μπορεί να περιλαμβάνει υλικό ή/και λογισμικό
vi. την εισαγωγή νέων εργολάβων, προμηθευτών ή προσωπικού, κατά περίπτωση.

Ο οργανισμός ελέγχει τις προγραμματισμένες αλλαγές και εξετάζει τις συνέπειες ακούσιων αλλαγών, λαμβάνοντας μέτρα για τον μετριασμό τυχόν δυσμενών επιπτώσεων, όπως απαιτείται. Ο οργανισμός διασφαλίζει ότι οι διαδικασίες που ανατίθενται σε εξωτερικούς συνεργάτες ελέγχονται.

12.5 Στρατηγικές, διαδικασίες, διεργασίες και αντιμετώπιση κινδύνων ασφάλειας

Ο οργανισμός θα πρέπει να εφαρμόζει και να διατηρεί συστηματικές διαδικασίες για την ανάλυση τρωτών σημείων και απειλών που σχετίζονται με την ασφάλεια. Με βάση αυτήν την ανάλυση ευπάθειας και απειλής και την επακόλουθη αξιολόγηση κινδύνου, ο οργανισμός θα πρέπει να εντοπίσει και να επιλέξει μια στρατηγική ασφάλειας που αποτελείται από μία ή περισσότερες διαδικασίες, διεργασίες και σχέδια αντιμετώπισης. Ο προσδιορισμός θα πρέπει να βασίζεται στον βαθμό στον οποίο οι στρατηγικές, οι διαδικασίες, οι διεργασίες και η αντιμετώπιση:

i. διατηρούν την ασφάλειας του οργανισμού·
ii. μειώνουν της πιθανότητας ευπαθειών ασφαλείας.
iii. μειώνουν την πιθανότητα πραγματοποίησης μιας απειλής.
iv. συντομεύουν την περίοδο τυχόν ελλείψεων στη αντιμετώπιση τρωτών σημείων ασφαλείας και να περιορίσει τον αντίκτυπό τους
v. προβλέπουν τη διαθεσιμότητα επαρκών πόρων.

Η επιλογή πρέπει να βασίζεται στον βαθμό στον οποίο οι στρατηγικές, οι διαδικασίες και τα σχέδια αντιμετώπισης πληρούν τις απαιτήσεις για την προστασία της ασφάλειας του οργανισμού, εξετάζουν το ποσό και το είδος του κινδύνου που μπορεί ή δεν μπορεί να αναλάβει ο οργανισμός και εξετάζει το σχετικό κόστος και τα οφέλη.

Ο οργανισμός θα πρέπει να καθορίσει τις απαιτήσεις πόρων για την εφαρμογή των επιλεγμένων διαδικασιών, διεργασιών και σχεδίων αντιμετώπισης περιστατικών ασφαλείας. Ο οργανισμός θα πρέπει να εφαρμόζει και να διατηρεί επιλεγμένες στρατηγικές και σχέδια αντιμετώπισης περιστατικών ασφαλείας ώστε να μπορούν να ενεργοποιούνται όταν χρειάζεται.

12.6 Σχέδια Ασφαλείας

Ο οργανισμός θα πρέπει να εφαρμόζει και να διατηρεί μια δομή απόκρισης που θα επιτρέπει την έγκαιρη και αποτελεσματική προειδοποίηση και κοινοποίηση τρωτών σημείων που σχετίζονται με την ασφάλεια και επικείμενες απειλές ασφαλείας ή συνεχιζόμενες παραβιάσεις της ασφάλειας στα σχετικά ενδιαφερόμενα μέρη. Η δομή απόκρισης θα πρέπει να παρέχει σχέδια και διαδικασίες για τη διαχείριση του

οργανισμού κατά τη διάρκεια μιας επικείμενης απειλής ασφαλείας ή μιας συνεχιζόμενης παραβίασης ασφάλειας. Τα προσδιορισμένα και τεκμηριωμένα σχέδια και διαδικασίες ασφαλείας θα πρέπει να βασίζονται στις επιλεγμένες στρατηγικές και σχεδίων αντιμετώπισης περιστατικών ασφαλείας. Επίσης θα πρέπει να εφαρμόζει και να διατηρεί μια δομή, προσδιορίζοντας ένα καθορισμένο άτομο ή μία ή περισσότερες ομάδες υπεύθυνες για την αντιμετώπιση τρωτών σημείων και απειλών που σχετίζονται με την ασφάλεια. Οι ρόλοι και οι ευθύνες για το καθορισμένο άτομο ή κάθε ομάδα και η σχέση μεταξύ του ατόμου ή των ομάδων πρέπει να προσδιορίζονται, να κοινοποιούνται και να τεκμηριώνονται με σαφήνεια. Συλλογικά, οι ομάδες θα πρέπει να είναι ικανές να:

i. να αξιολογούν τη φύση και την έκταση μιας απειλής για την ασφάλεια και τις πιθανές επιπτώσεις της
ii. να αξιολογούν τον αντίκτυπο σε σχέση με προκαθορισμένα κατώτατα όρια που δικαιολογούν την έναρξη επίσημης απάντησης
iii. να ενεργοποιηούν μια κατάλληλη απόκριση ασφαλείας
iv. σχεδιάζουν τις ενέργειες που πρέπει να αναληφθούν
v. καθορίζουν προτεραιότητες χρησιμοποιώντας την ασφάλεια ζωής ως πρώτη προτεραιότητα
vi. να παρακολουθούν τις επιπτώσεις οποιασδήποτε παραλλαγής σε τρωτά σημεία που σχετίζονται με την ασφάλεια, τις αλλαγές στην πρόθεση και ικανότητα των παραγόντων απειλής ή παραβιάσεων ασφάλειας και η αντίδραση του οργανισμού
vii. να ενεργοποιούν τα σχεδίων αντιμετώπισης περιστατικών ασφαλείας
viii. να επικοινωνούν με τα σχετικά ενδιαφερόμενα μέρη, τις αρχές και τα μέσα ενημέρωσης
ix. συνεισφέρουν στο σχέδιο επικοινωνίας με τη διαχείριση επικοινωνίας.

Για κάθε καθορισμένο άτομο ή ομάδα θα πρέπει να υπάρχει προσδιορισμένο προσωπικό συμπεριλαμβανομένων των αναπληρωματικών με την απαραίτητη ευθύνη, εξουσία και επάρκεια να εκτελούν τον καθορισμένο ρόλο τους και τεκμηριωμένες διαδικασίες για την καθοδήγηση των ενεργειών τους, συμπεριλαμβανομένων εκείνων για την ενεργοποίηση, τη λειτουργία, τον συντονισμό και επικοινωνία της απάντησης.

Ο οργανισμός πρέπει να τεκμηριώνει και να διατηρεί διαδικασίες για την επικοινωνία εσωτερικά και εξωτερικά με σχετικά ενδιαφερόμενα μέρη, συμπεριλαμβανομένου του τι, πότε, με ποιον και πώς να επικοινωνήσει. Ο οργανισμός μπορεί να τεκμηριώσει και να διατηρήσει διαδικασίες για το πώς και υπό ποιες συνθήκες, ο οργανισμός επικοινωνεί με τους υπαλλήλους και τις επαφές έκτακτης ανάγκης τους. Πρέπει να γίνεται λήψη, τεκμηρίωση και απάντηση σε ανακοινώσεις από ενδιαφερόμενα μέρη, συμπεριλαμβανομένου οποιουδήποτε εθνικού ή περιφερειακού συστήματος παροχής συμβουλών για τους κινδύνους ή ισοδύναμο. Να διασφαλίζει την διαθεσιμότητα των μέσων επικοινωνίας κατά τη διάρκεια παραβίασης, ευπάθειας ή απειλής ασφάλειας καθώς και τη διευκόλυνση της δομημένης επικοινωνίας με τους ανταποκριτές σε απειλές ή/και παραβιάσεις κατά της ασφάλειας. Εξίσου σημαντικό είναι και η παροχή λεπτομερειών για την απάντηση των μέσων ενημέρωσης του οργανισμού μετά από παραβίαση ασφαλείας, συμπεριλαμβανομένης μιας στρατηγικής επικοινωνίας και τη καταγραφή των στοιχείων της παραβίασης ασφαλείας, των ενεργειών που έγιναν και των αποφάσεων που ελήφθησαν. Όπου ισχύει και είναι δυνατό, θα πρέπει επίσης να λαμβάνονται υπόψη και να εφαρμόζονται τα ακόλουθα:

- Να γίνεται ειδοποίηση των ενδιαφερομένων μερών που ενδέχεται να επηρεαστούν από μια πραγματική ή επικείμενη παραβίαση ασφάλειας
- Να εξασφαλίζεται ο κατάλληλος συντονισμός και επικοινωνία μεταξύ πολλαπλών οργανισμών που ανταποκρίνονται. Οι διαδικασίες προειδοποίησης και επικοινωνίας θα πρέπει να ασκούνται ως μέρος του προγράμματος δοκιμών και εκπαίδευσης του οργανισμού.

Ο οργανισμός πρέπει να τεκμηριώνει και να διατηρεί σχέδια ασφαλείας. Αυτά τα σχέδια θα πρέπει να παρέχουν καθοδήγηση και πληροφορίες για να βοηθήσουν τις ομάδες να ανταποκριθούν σε μια ευπάθεια ασφαλείας, απειλή ή/και παραβίαση και να βοηθήσουν τον οργανισμό να απαντήσει και να αποκαταστήσει την ασφάλειά του.
Συλλογικά, τα σχέδια ασφαλείας θα πρέπει να περιέχουν:
α) λεπτομέρειες των ενεργειών που θα κάνουν οι ομάδες για:

1) Συνέχιση ή επαναφορά της συμφωνημένης κατάστασης ασφάλειας

2) Παρακολούθηση του αντίκτυπου των πραγματικών ή επικείμενων απειλών, τρωτών σημείων ή παραβίασης ασφάλειας και η απάντηση του οργανισμού σε αυτό

β) αναφορά στο προκαθορισμένο όριο(α) και στη διαδικασία για την ενεργοποίηση της απόκρισης

γ) διαδικασίες για την αποκατάσταση της ασφάλειας του οργανισμού

δ) λεπτομέρειες για τη διαχείριση των άμεσων συνεπειών μιας ευπάθειας και απειλής ασφαλείας ή πραγματικής ή επικείμενης παραβίασης ασφάλειας, λαμβάνοντας υπόψη:

1) την ευημερία των ατόμων

2) την αξία των περιουσιακών στοιχείων, των πληροφοριών και του προσωπικού που ενδέχεται να διακυβεύονται

3) την πρόληψη (περαιτέρω) απώλειας ή μη διαθεσιμότητας βασικών δραστηριοτήτων.

Κάθε σχέδιο πρέπει να περιλαμβάνει:

α) τον σκοπό, το πεδίο εφαρμογής και τους στόχους του

β) τους ρόλους και τις ευθύνες της ομάδας που θα εφαρμόσει το σχέδιο

γ) τις ενέργειες για την εφαρμογή των λύσεων

δ) τις πληροφορίες που απαιτούνται για την ενεργοποίηση (συμπεριλαμβανομένων των κριτηρίων ενεργοποίησης), τη λειτουργία, το συντονισμό και κοινοποιούν τις ενέργειες της ομάδας

ε) εσωτερικές και εξωτερικές αλληλεξαρτήσεις

στ) τις απαιτήσεις του σε πόρους.

ζ) τις απαιτήσεις υποβολής εκθέσεων

η) διαδικασία αποχώρησης.

Κάθε σχέδιο πρέπει να είναι χρησιμοποιήσιμο και διαθέσιμο στον χρόνο και τον τόπο στον οποίο απαιτείται.

Τέλος πολύ σημαντικό είναι και ο τρόπος ανάκτησης εφόσον έχει γίνει κάποιο περιστατικό ασφαλείας. Ο οργανισμός θα πρέπει να έχει τεκμηριωμένες διαδικασίες για την αποκατάσταση της ασφάλειας του οργανισμού από τυχόν προσωρινά μέτρα που έχουν ληφθεί πριν, κατά τη διάρκεια και μετά από παραβίαση ασφάλειας.

13. Αξιολόγηση απόδοσης

13.1 Παρακολούθηση, μέτρηση, ανάλυση και αξιολόγηση

Ο οργανισμός καθορίζει για το τι πρέπει να παρακολουθείται και να τι να μετράτε καθώς και τις μεθόδους παρακολούθησης, μέτρησης, ανάλυσης και αξιολόγησης, κατά περίπτωση, για την εξασφάλιση έγκυρων αποτελεσμάτων. Πρέπει να ορίσει και πότε θα πραγματοποιηθεί η παρακολούθηση και η μέτρηση και πότε τα αποτελέσματα από την παρακολούθηση καθώς και τις μετρήσεις που έχουν παρθεί να αναλυθούν και αξιολογηθούν. Ο οργανισμός διατηρεί κατάλληλες τεκμηριωμένες πληροφορίες ως απόδειξη των αποτελεσμάτων. Ο οργανισμός αξιολογεί την απόδοση ασφάλειας και την αποτελεσματικότητα του συστήματος διαχείρισης ασφάλειας.

13.2 Διενέργεια εσωτερικών ελέγχων

Ο οργανισμός διενεργεί εσωτερικούς ελέγχους σε προγραμματισμένα χρονικά διαστήματα για να παρέχει πληροφορίες σχετικά με το εάν το σύστημα διαχείρισης ασφάλειας:

α) συμμορφώνεται με τις απαιτήσεις του ίδιου του οργανισμού για το σύστημα διαχείρισης ασφάλειας και τις απαιτήσεις του ISO 28001

β) εφαρμόζεται και διατηρείται αποτελεσματικά.

Ο οργανισμός θα σχεδιάζει, καθιερώνει, εφαρμόζει και συντηρεί πρόγραμμα(α) ελέγχου, συμπεριλαμβανομένων της συχνότητας, των μεθόδων, των αρμοδιοτήτων, των απαιτήσεων σχεδιασμού και της υποβολής εκθέσεων, τα οποία θα λαμβάνουν υπόψη τη σημασία των σχετικών διαδικασιών και τα αποτελέσματα προηγούμενων ελέγχων

β) καθορίζει τα κριτήρια ελέγχου και το πεδίο εφαρμογής για κάθε έλεγχο

γ) επιλέγει ελεγκτές και διενεργεί ελέγχους για να διασφαλίζει την αντικειμενικότητα και την αμεροληψία της διαδικασίας ελέγχου

δ) διασφαλίζει ότι τα αποτελέσματα των ελέγχων αναφέρονται στα αρμόδια στελέχη

ε) να διατηρεί τεκμηριωμένες πληροφορίες ως αποδεικτικά στοιχεία της εφαρμογής του προγράμματος(ων) ελέγχου και των αποτελεσμάτων του ελέγχου

στ) επαληθεύστε ότι ο εξοπλισμός και το προσωπικό ασφαλείας έχουν αναπτυχθεί κατάλληλα.

Το πρόγραμμα ελέγχου, συμπεριλαμβανομένου οποιουδήποτε χρονοδιαγράμματος, θα βασίζεται στα αποτελέσματα των αξιολογήσεων κινδύνου των δραστηριοτήτων του οργανισμού και στα αποτελέσματα προηγούμενων ελέγχων. Οι διαδικασίες ελέγχου καλύπτουν το εύρος, τη συχνότητα, τις μεθοδολογίες και τις αρμοδιότητες, καθώς και τις ευθύνες και τις απαιτήσεις για τη διενέργεια ελέγχων και την αναφορά αποτελεσμάτων.

13.3 Επισκόπηση της διοίκησης

Η ανώτατη διοίκηση θα επανεξετάζει το σύστημα διαχείρισης ασφάλειας του οργανισμού, σε προγραμματισμένα χρονικά διαστήματα, για να διασφαλίζει τη συνεχή καταλληλόλητα, επάρκεια και αποτελεσματικότητά του. Η αναθεώρηση της διαχείρισης περιλαμβάνει την εξέταση:

α) την κατάσταση των ενεργειών από προηγούμενες αξιολογήσεις της διοίκησης

β) αλλαγές σε εξωτερικά και εσωτερικά ζητήματα που σχετίζονται με το σύστημα διαχείρισης ασφάλειας

γ) πληροφορίες σχετικά με τις επιδόσεις ασφαλείας, συμπεριλαμβανομένων των τάσεων σε μη συμμορφώσεις και διορθωτικές ενέργειες, αποτελέσματα παρακολούθησης και μετρήσεων, αποτελέσματα ελέγχου

δ) ευκαιρίες για συνεχή βελτίωση.

Τα αποτελέσματα της αναθεώρησης της διαχείρισης περιλαμβάνουν αποφάσεις που σχετίζονται με ευκαιρίες συνεχούς βελτίωσης και οποιαδήποτε ανάγκη για αλλαγές στο σύστημα διαχείρισης ασφάλειας. Ο οργανισμός θα διατηρεί τεκμηριωμένες πληροφορίες ως απόδειξη των αποτελεσμάτων των επισκοπήσεων της διοίκησης.

Όλο το διάστημα αυτό η διοίκηση πρέπει να αξιολογείται. Τα στοιχεία για τις αξιολογήσεις της διοίκησης περιλαμβάνουν:

α) αποτελέσματα ελέγχων και αξιολογήσεων συμμόρφωσης με τις νομικές απαιτήσεις και με άλλες απαιτήσεις στις οποίες προσυπογράφει ο οργανισμός

β) επικοινωνία(εις) από εξωτερικά ενδιαφερόμενα μέρη, συμπεριλαμβανομένων των καταγγελιών

γ) τις επιδόσεις ασφαλείας του οργανισμού

δ) ο βαθμός στον οποίο έχουν επιτευχθεί τα αντικείμενα και οι στόχοι

ε) κατάσταση των διορθωτικών ενεργειών.

στ) ενέργειες παρακολούθησης από προηγούμενες αξιολογήσεις της διοίκησης

ζ) μεταβαλλόμενες συνθήκες, συμπεριλαμβανομένων των εξελίξεων στις νομικές και άλλες απαιτήσεις που σχετίζονται με τις πτυχές της ασφάλειας

η) συστάσεις για βελτίωση.

14. Βελτίωση

Ο οργανισμός σε περίπτωση μη συμμόρφωσης οφείλει να κάνει κάποιες σημαντικές διορθωτικές ενέργειες. Ο οργανισμός οφείλει να:

α) αντιδράει στη μη συμμόρφωση και, κατά περίπτωση να λαμβάνει κατάλληλα μέτρα για τον έλεγχο και τη διόρθωσή του και να είναι σε θέση να αντιμετωπίσει τις συνέπειες.

β) να αξιολογήσει την ανάγκη δράσης για την εξάλειψη της αιτίας ή των αιτιών της μη συμμόρφωσης, προκειμένου να μην επαναληφθεί ή να εμφανιστεί αλλού, κάνοντας τρία βασικά βήματα. Τα πρώτο είναι η επανεξέταση της μη συμμόρφωσης, το δεύτερο ο προσδιορισμός των αιτιών της μη συμμόρφωσης και τέλος τον προσδιορισμό εάν υπάρχουν ή ενδέχεται να προκύψουν παρόμοιες μη συμμορφώσεις

γ) να εφαρμόσει οποιαδήποτε ενέργεια χρειάζεται

δ) επανεξετάσει την αποτελεσματικότητα οποιασδήποτε διορθωτικής δράσης που λαμβάνεται

ε) πραγματοποιήσει αλλαγές στο σύστημα διαχείρισης ασφάλειας, εάν είναι απαραίτητο.

Οι διορθωτικές ενέργειες πρέπει να είναι κατάλληλες για τις επιπτώσεις των μη συμμορφώσεων που συναντώνται. Ο οργανισμός διατηρεί τεκμηριωμένες πληροφορίες ως απόδειξη:

i. τη φύση των μη συμμορφώσεων και τυχόν μετέπειτα μέτρα που λαμβάνονται
ii. τα αποτελέσματα οποιασδήποτε διορθωτικής ενέργειας
iii. η έρευνα σχετικά με την ασφάλεια

iv. αστοχίες, συμπεριλαμβανομένων παρ' ολίγον ατυχημάτων και ψευδών συναγερμών
v. περιστατικά και καταστάσεις έκτακτης ανάγκης
vi. μη συμμορφώσεις
vii. λήψη μέτρων για τον μετριασμό τυχόν συνεπειών που προκύπτουν από τέτοιες αστοχίες, συμβάντα ή μη συμμόρφωση.

Αυτές οι διαδικασίες απαιτούν να επανεξετάζονται όλες οι προτεινόμενες διορθωτικές ενέργειες μέσω security RA (risk assessment) πριν από την εφαρμογή, εκτός εάν η άμεση εφαρμογή αποτρέπει την επικείμενη έκθεση στη ζωή ή τη δημόσια ασφάλεια. Οποιαδήποτε διορθωτική ενέργεια που λαμβάνεται για την εξάλειψη των αιτιών των πραγματικών και πιθανών μη συμμορφώσεων πρέπει να είναι κατάλληλη για το μέγεθος των προβλημάτων και ανάλογη με τους κινδύνους που σχετίζονται με τη διαχείριση της ασφάλειας που ενδέχεται να προκύψουν. Τέλος Ο οργανισμός θα βελτιώνει συνεχώς την καταλληλόλητα, την επάρκεια και την αποτελεσματικότητα του συστήματος διαχείρισης ασφάλειας.

Terminology

Απειλή	Μια πιθανή ενέργεια ή ένα γεγονός που μπορεί να προκαλέσει την απώλεια ενός ή περισσοτέρων χαρακτηριστικών ασφαλείας (Confidentiality, Integrity, Availability)
Ευπάθεια	Χαρακτηριστικό ενός πληροφοριακού συστήματος που μπορεί να επιτρέψει να συμβεί μία παραβίαση
Επιχειρησιακή Συνέχεια (Business Continuity)	Η ικανότητα ενός οργανισμού να συνεχίζει την εύρυθμη λειτουργία του μετά από ένα συμβάν που μπορεί να διαταράξει τις επιχειρησιακές του λειτουργίες
Διάθεση Ανάληψης Κινδύνου (Risk Appetite)	Ρητά καθορισμένο και καταγεγραμμένο επίπεδο κινδύνου βάσει του οποίου ο οργανισμός αποδέχεται τον κίνδυνο χωρίς την ανάγκη για υιοθέτηση περαιτέρω διορθωτικών ενεργειών
Εναπομένων Κίνδυνος	Ο κίνδυνος που απομένει ακόμα και όταν έχουν εφαρμοστεί μέτρα μείωσης του και ξεπερνά το επίπεδο διάθεσης ανάληψης κινδύνου.
Εγγενής Κίνδυνος	Ο κίνδυνος που ενυπάρχει πριν ληφθεί οποιαδήποτε διορθωτική ενέργεια για τον περιορισμό του
Αξιολόγηση Επιχειρησιακού Αντικτύπου (Business Impact Assessment)	Η διαδικασία κατά την οποία μελετώνται οι επιχειρησιακές δραστηριότητες των οργανωτικών μονάδων του Οργανισμού και διακρίνονται σε κρίσιμες και μη κρίσιμες με βάση συγκεκριμένα κριτήρια αξιολόγησης
Εμπιστευτικότητα (Confidentiality)	Η ιδιότητα που εξασφαλίζει ότι μόνο εξουσιοδοτημένες οντότητες μπορούν να έχουν πρόσβαση σε συγκεκριμένες πληροφορίες ή πληροφοριακά συστήματα
Ακεραιότητα (Integrity)	Η ιδιότητα που εξασφαλίζει την προστασία των πληροφοριών και πληροφοριακών συστημάτων από μη εξουσιοδοτημένη ή εξ αμελείας τροποποίηση
Διαθεσιμότητα (Availability)	Η ιδιότητα που εξασφαλίζει τη διαθεσιμότητα των πληροφοριών ή πληροφοριακών συστημάτων σε εξουσιοδοτημένες οντότητες
Τρίτα Μέρη ή Προμηθευτές	Πάροχοι υπηρεσιών, εταιρείες ενσωμάτωσης λύσεων πληροφορικής (integrators), προμηθευτές, τηλεπικοινωνιακοί πάροχοι, εταιρείες που παρέχουν υποστήριξη υποδομής δρώντας ως εξωτερικοί συνεργάτες. Όλοι αυτοί με τους οποίους η στενή συνεργασία είναι ζωτικής σημασίας λόγω των υπηρεσιών που παρέχονται προς αυτούς ή που λαμβάνονται από αυτούς με στόχο την υποστήριξη των επιχειρησιακών λειτουργιών του οργανισμού
Risk Assessment	Αποτίμηση της Επικινδυνότητας
Risk Treatment	Αντιμετώπιση της Επικινδυνότητας
Διοίκηση Επικινδυνότητας (Risk Management)	Αποτίμηση της Επικινδυνότητας

15. Βιβλιογραφία

1. https://www.interpol.int/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19
2. https://www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know
3. https://www.tripwire.com/state-of-security/the-supply-chain-needs-better-cybersecurity-and-risk-management
4. https://www.enisa.europa.eu/news/enisa-news/understanding-the-increase-in-supply-chain-security-attacks
5. https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks
6. https://www.imperva.com/learn/application-security/apt-advanced-persistent-threat/
7. https://www.malwarebytes.com/ryuk-ransomware
8. https://www.malwarebytes.com/trickbot
9. https://www.datto.com/blog/bazar-loader-attack-what-is-it-and-how-to-prepare
10. https://unit42.paloaltonetworks.com/phishing-trends-with-pdf-files/
11. https://www.forbes.com/sites/forbestechcouncil/2022/01/25/the2021-kaseyaattack-highlighted-the-seven-deadly-sins-of-future-ransomware-attacks/
12. https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Management/documents/briefings/Workshop-Brief-on-Cyber-Supply-Chain-Best-Practices.pdf
13. https://www.iso.org/obp/ui/#iso:std:iso:28000:en