Πανεπιστήμιο Πειραιώς
Σχολή Τεχνολογιών Πληροφορικής και Τηλεπικοινωνιών
Τμήμα Ψηφιακών Συστημάτων

Επίπεδο: Μεταπτυχιακό Πρόγραμμα Σπουδών
Κυβερνοασφάλεια και Τεχνολογίες Τεχνητής Νοημοσύνης

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Συνδυάζοντας τα ρυθμιστικά και τα εθελοντικά πλαίσια κυβερνοασφάλειας – Μια συγκριτική μελέτη μεταξύ των προτύπων EU NIS2 και US SOC2

Επιβλέπον Καθηγητής: Σ. Γκρίτζαλης

Ονοματεπώνυμο	E-mail	Α.Μ.
Ιορδανίδης Πέτρος	petros_iordanidis@ssl-unipi.gr	mte24012

Πειραιάς
Ιούνιος 2026

Περίληψη

Η συνεχής αύξηση των κυβερνοαπειλών και η αυξανόμενη εξάρτηση οργανισμών και επιχειρήσεων από ψηφιακές υποδομές έχουν καταστήσει την κυβερνοασφάλεια και την κανονιστική συμμόρφωση κρίσιμους παράγοντες για τη διασφάλιση της επιχειρησιακής συνέχειας και της προστασίας πληροφοριών. Στο πλαίσιο αυτό, η παρούσα διατριβή εξετάζει συγκριτικά δύο σημαντικά πλαίσια κυβερνοασφάλειας και συμμόρφωσης: την Οδηγία NIS2 της Ευρωπαϊκής Ένωσης και το πλαίσιο SOC 2 του American Institute of Certified Public Accountants (AICPA).

Αρχικά, παρουσιάζεται το σύγχρονο περιβάλλον κυβερνοαπειλών και η σημασία της κανονιστικής συμμόρφωσης για τους οργανισμούς. Στη συνέχεια, αναλύονται τα βασικά χαρακτηριστικά της NIS2, συμπεριλαμβανομένων των απαιτήσεων διαχείρισης κινδύνων, των υποχρεώσεων αναφοράς περιστατικών, των μηχανισμών διακυβέρνησης και των κυρώσεων μη συμμόρφωσης. Παράλληλα, εξετάζεται το πλαίσιο SOC 2, τα Trust Services Criteria και η διαδικασία αξιολόγησης και ελέγχου συμμόρφωσης.

Η εργασία προχωρά σε αναλυτική σύγκριση των δύο πλαισίων ως προς τον σκοπό, το πεδίο εφαρμογής, τις απαιτήσεις ασφάλειας, τις διαδικασίες συμμόρφωσης και τους μηχανισμούς επιβολής. Επιπλέον, παρουσιάζονται τεχνολογικά εργαλεία και λύσεις που υποστηρίζουν την εφαρμογή απαιτήσεων κυβερνοασφάλειας και κανονιστικής συμμόρφωσης, όπως GRC πλατφόρμες, εργαλεία διαχείρισης κινδύνων και συστήματα παρακολούθησης περιστατικών ασφαλείας.

Τα αποτελέσματα της έρευνας δείχνουν ότι, παρά τις διαφορές τους, η NIS2 και το SOC 2 συγκλίνουν ως προς την ανάγκη εφαρμογής αποτελεσματικών μηχανισμών διαχείρισης κινδύνων, εσωτερικών ελέγχων και οργανωτικής διακυβέρνησης. Επιπλέον, αναδεικνύεται ότι η συμμόρφωση δεν αποτελεί μόνο κανονιστική υποχρέωση αλλά και στρατηγικό εργαλείο ενίσχυσης της κυβερνοανθεκτικότητας, της αξιοπιστίας και της εμπιστοσύνης των ενδιαφερόμενων μερών.

Τέλος, η διατριβή εξετάζει μελλοντικές τάσεις στον τομέα της κυβερνοασφάλειας, δίνοντας έμφαση σε νέες ευρωπαϊκές πρωτοβουλίες όπως το DORA και το CSRD, καθώς και στον ρόλο της τεχνητής νοημοσύνης και του αυτοματισμού στη διαχείριση κανονιστικής συμμόρφωσης και κυβερνοκινδύνων.

Λέξεις-κλειδιά: Κυβερνοασφάλεια, NIS2, SOC 2, Κανονιστική Συμμόρφωση, Διαχείριση Κινδύνων, GRC, Trust Services Criteria, Κυβερνοανθεκτικότητα.

Πίνακας Περιεχομένων

Πίνακας εικόνων

1. Εισαγωγή

1.1 Υπόβαθρο και κίνητρα της έρευνας

Η αυξανόμενη συχνότητα και σοβαρότητα των κυβερνοεπιθέσεων έχει οδηγήσει κυβερνήσεις, ρυθμιστικές αρχές και επιχειρήσεις στην ανάγκη δημιουργίας αυστηρότερων πλαισίων κυβερνοασφάλειας. Οι οργανισμοί καλούνται πλέον να αντιμετωπίσουν όχι μόνο τεχνικές απειλές, αλλά και σύνθετες απαιτήσεις συμμόρφωσης που σχετίζονται με την προστασία δεδομένων, τη διαχείριση κινδύνων και την επιχειρησιακή ανθεκτικότητα.

Η Ευρωπαϊκή Ένωση, μέσω της Οδηγίας NIS2, επιδιώκει την ενίσχυση της κυβερνοανθεκτικότητας κρίσιμων οργανισμών και την εναρμόνιση των απαιτήσεων κυβερνοασφάλειας μεταξύ των κρατών-μελών. Ταυτόχρονα, στο διεθνές επιχειρησιακό περιβάλλον, πλαίσια όπως το SOC 2 έχουν αποκτήσει ιδιαίτερη σημασία ως μηχανισμοί απόδειξης αξιοπιστίας και ασφάλειας προς πελάτες και συνεργάτες.

Το βασικό κίνητρο της παρούσας έρευνας είναι η κατανόηση του τρόπου με τον οποίο διαφορετικά πλαίσια συμμόρφωσης και διασφάλισης αλληλεπιδρούν στο σύγχρονο οικοσύστημα κυβερνοασφάλειας. Παράλληλα, η έρευνα στοχεύει στην ανάδειξη των προκλήσεων που αντιμετωπίζουν οι οργανισμοί κατά την εφαρμογή των απαιτήσεων αυτών, καθώς και των πρακτικών εργαλείων που μπορούν να υποστηρίξουν τη διαδικασία συμμόρφωσης.

1.2 Συντομεύσεις και ακρωνύμια

NIS 2	Network and Information Security 2
SOC 2	System and Organization Controls 2
EU	European Union
AICPA	American Institute of Certified Public Accountants
GRC	Governance – Risk – Compliance
AI	Artificial intelligence

2. Επισκόπηση του Ρυθμιστικού Πλαισίου Κυβερνοασφάλειας

2.1 Τι είναι η κυβερνοασφάλεια;

Η κυβερνοασφάλεια είναι η πρακτική προστασίας ανθρώπων, συστημάτων και δεδομένων από κυβερνοεπιθέσεις, μέσω της χρήσης τεχνολογιών, διαδικασιών και πολιτικών ασφαλείας.

Σε επίπεδο οργανισμών και επιχειρήσεων, η κυβερνοασφάλεια αποτελεί βασικό μέρος της συνολικής στρατηγικής διαχείρισης κινδύνων. Οι πιο συνηθισμένες κυβερνοαπειλές περιλαμβάνουν επιθέσεις ransomware, κακόβουλο λογισμικό (malware), επιθέσεις phishing, κλοπή δεδομένων και, πιο πρόσφατα, επιθέσεις που αξιοποιούν τεχνολογίες τεχνητής νοημοσύνης (AI).

Καθώς οι κυβερνοαπειλές γίνονται όλο και πιο συχνές και πιο σύνθετες, οι οργανισμοί αυξάνουν τις επενδύσεις τους σε μέτρα πρόληψης και αντιμετώπισης περιστατικών ασφαλείας. Σύμφωνα με προβλέψεις της International Data Corporation (IDC), οι παγκόσμιες δαπάνες για την ασφάλεια πληροφοριών αναμένεται να φτάσουν τα 377 δισεκατομμύρια δολάρια έως το 2028.[1]

Εικόνα 2.1 : *Κυβερνοασφάλεια*

2.2 Το παγκόσμιο περιβάλλον κυβερνοαπειλών

Οι κυβερνοεπιθέσεις που αξιοποιούν την τεχνητή νοημοσύνη αποτελούν μια σημαντική πρόκληση στον τομέα της κυβερνοασφάλειας. Οι κυβερνοεγκληματίες χρησιμοποιούν AI για να αυξήσουν την πολυπλοκότητα και τον αντίκτυπο των επιθέσεών τους, καθιστώντας τες πιο δύσκολες στον εντοπισμό.

Αυτές οι απειλές που βασίζονται στην AI μπορούν:

- να αυτοματοποιούν την αναγνώριση ευπαθειών,
- να δημιουργούν πειστικά phishing μηνύματα,
- ακόμη και να προσαρμόζονται σε πραγματικό χρόνο ώστε να παρακάμπτουν τα μέτρα ασφαλείας.

Η δυναμική φύση του AI σημαίνει ότι οι παραδοσιακές άμυνες ίσως να μην επαρκούν πλέον. Αυτό απαιτεί μια προληπτική και καινοτόμα προσέγγιση στην κυβερνοασφάλεια. Οι οργανισμοί πρέπει να επενδύσουν σε λύσεις ασφαλείας που βασίζονται στην AI και να βελτιώνουν συνεχώς τις στρατηγικές τους για να παραμένουν μπροστά από αυτές τις ταχέως εξελισσόμενες απειλές.

Τεχνολογία Deepfake

Η τεχνολογία deepfake χρησιμοποιεί τεχνητή νοημοσύνη για να δημιουργεί ρεαλιστικά ψεύτικα βίντεο, εικόνες ή ήχο που μιμούνται πραγματικά πρόσωπα, συχνά καθιστώντας δύσκολο να διακριθούν από αυθεντικό περιεχόμενο. Αποτελεί πλέον ισχυρό εργαλείο για κυβερνοεγκληματίες, με σχεδόν τα δύο τρίτα των οργανισμών να έχουν δεχθεί επίθεση deepfake μέσα σε περίοδο 12 ετών.

Παραδείγματα χρήσης deepfake:

- χιουμοριστικές αλλαγές προσώπου στα social media,
- ψεύτικες επιχειρηματικές επικοινωνίες που δημιουργούνται με AI,
- χειραγωγημένα πολιτικά βίντεο,
- σατιρικό ή καλλιτεχνικό περιεχόμενο που δημιουργείται με AI.

Απειλές Κακόβουλου Λογισμικού (Malware)

Το malware, δηλαδή το κακόβουλο λογισμικό, υπάρχει από τη δεκαετία του 1960 και παραμένει μια σημαντική απειλή για την παγκόσμια κυβερνοασφάλεια.

Σήμερα:

- υπάρχουν πάνω από 1 δισεκατομμύριο προγράμματα malware παγκοσμίως
- περίπου 560.000 νέες απειλές εντοπίζονται κάθε ημέρα.

Ransomware

Η τελευταία ανάλυση του Financial Crimes Enforcement Network δείχνει ότι καταγράφηκαν πάνω από 2,1 δισεκατομμύρια δολάρια σε πληρωμές ransomware μεταξύ 2022–2024.

- Το 2023 ήταν η κορύφωση με 1.512 περιστατικά και 1,1 δισ. δολάρια σε πληρωμές (αύξηση 77% από το 2022).
- Το 2024 μειώθηκαν σε 1.476 περιστατικά και 734 εκατ. δολάρια, μετά από σημαντικές παρεμβάσεις των αρχών.

Οι μέσες απαιτήσεις λύτρων κυμάνθηκαν από 124.000 έως 175.000 δολάρια. Οι τομείς που στοχοποιήθηκαν περισσότερο:

- μεταποίηση,
- χρηματοοικονομικές υπηρεσίες,
- υγειονομική περίθαλψη.

Μαζί αντιπροσώπευαν σχεδόν 1 δισεκατομμύριο δολάρια σε απώλειες.

Cryptojacking

Το cryptojacking είναι μια κρυφή απειλή που παραμένει συχνά απαρατήρητη. Οι επιτιθέμενοι καταλαμβάνουν τους πόρους ενός υπολογιστή για να εξορύξουν κρυπτονομίσματα. Σε αντίθεση με άλλες μορφές malware:

- δεν στοχεύει άμεσα στην κλοπή δεδομένων,
- αλλά στη δημιουργία κέρδους μέσω χρήσης υπολογιστικής ισχύος.

Παρότι λιγότερο εμφανές, προκαλεί σημαντική ζημιά μέσω υπερκατανάλωσης πόρων.

Επιθέσεις Social Engineering

Το Social Engineering είναι από τους πιο ύπουλους τύπους κυβερνοαπειλών επειδή εκμεταλλεύεται την ανθρώπινη ψυχολογία αντί για τεχνολογικές ευπάθειες. Οι επιθέσεις αυτές πείθουν άτομα να παραβιάσουν κανονικές διαδικασίες ασφαλείας, οδηγώντας συχνά σε:

- μεγάλες διαρροές δεδομένων
- οικονομικές απώλειες.

Business Email Compromise (BEC)

Το BEC είναι μια διαδεδομένη και εξελιγμένη απειλή που χρησιμοποιεί απάτες μέσω email για να εξαπατήσει εταιρείες ώστε να μεταφέρουν χρήματα ή ευαίσθητα δεδομένα.

Οι απατεώνες:

- κάνουν εκτεταμένη έρευνα για να μιμηθούν εσωτερικές επικοινωνίες,
- στέλνουν email που φαίνονται νόμιμα.

Παράδειγμα:
Επιτιθέμενοι χρησιμοποιούν παραβιασμένους λογαριασμούς email για να ζητήσουν τραπεζικά εμβάσματα με πρόσχημα επείγουσες και εμπιστευτικές επιχειρηματικές συμφωνίες. Συχνά η απάτη γίνεται αντιληπτή μόνο αφού ολοκληρωθεί η μεταφορά χρημάτων, προκαλώντας μεγάλες οικονομικές απώλειες.

Επιθέσεις Δικτύου και Εφαρμογών

Καθώς οι κυβερνοαπειλές εξελίσσονται, οι επιθέσεις σε δίκτυα και εφαρμογές γίνονται πιο σύνθετες, στοχεύοντας τη βασική υποδομή IT των οργανισμών.

Επιθέσεις Distributed Denial of Service (DDoS)

Οι επιθέσεις DDoS υπερφορτώνουν:

- δίκτυα
- servers
- ιστοσελίδες

με τεράστιο όγκο κίνησης, εξαντλώντας τους πόρους και το bandwidth ώστε οι υπηρεσίες να γίνουν μη διαθέσιμες στους νόμιμους χρήστες. Τα amplification attacks επιδεινώνουν το πρόβλημα χρησιμοποιώντας δημόσιους servers όπως:

- DNS (Domain Name System)
- NTP (Network Time Protocol)
- SNMP (Simple Network Management Protocol)

για να ενισχύσουν την επίθεση και να καταρρεύσουν συστήματα μέσα σε λίγα λεπτά.

Επιθέσεις Man-in-the-Middle (MitM)

Οι επιθέσεις MitM συμβαίνουν όταν ένας επιτιθέμενος παρεμβάλλεται στην επικοινωνία μεταξύ δύο μερών χωρίς να το γνωρίζουν. Με την αύξηση της κρυπτογραφημένης κίνησης μέσω HTTPS, αυτές οι επιθέσεις έχουν γίνει πιο πολύπλοκες.

Οι επιτιθέμενοι συχνά:

- εκμεταλλεύονται αδυναμίες στα πρωτόκολλα SSL/TLS
- χρησιμοποιούν κλεμμένα πιστοποιητικά για αποκρυπτογράφηση και αλλοίωση επικοινωνιών.

Injection Attacks

Οι injection attacks είναι συχνές σε πολλές πλατφόρμες, ειδικά σε web εφαρμογές. Συμβαίνουν όταν ένας επιτιθέμενος στέλνει μη αξιόπιστα δεδομένα σε έναν interpreter ως μέρος μιας εντολής ή ερωτήματος.

Ο interpreter εκτελεί τότε:

- μη προβλεπόμενες εντολές
- ή αποκτά πρόσβαση σε δεδομένα χωρίς εξουσιοδότηση.

Απειλές Ψηφιακής Υποδομής

Με την εξέλιξη της τεχνολογίας εμφανίζονται νέες προκλήσεις κυβερνοασφάλειας, ιδιαίτερα στους τομείς:

- Internet of Things (IoT)

- εφοδιαστικές αλυσίδες
- cloud computing.

Οι τομείς αυτοί αποτελούν βασικό κομμάτι της λειτουργίας των οργανισμών και συνεπώς γίνονται κύριοι στόχοι επιθέσεων.

Επιθέσεις στο Internet of Things (IoT)

Το IoT περιλαμβάνει τεράστιο αριθμό συσκευών, από οικιακές συσκευές μέχρι βιομηχανικό εξοπλισμό, που είναι συνδεδεμένες στο διαδίκτυο.

Πολλές από αυτές:

- δεν διαθέτουν ισχυρά μέτρα ασφαλείας
- έχουν ευπάθειες όπως:
    - μη ασφαλές firmware
    - αδύναμα πρωτόκολλα πιστοποίησης
    - μη προστατευμένες υπηρεσίες δικτύου.

Η Statista προβλέπει ότι οι IoT συσκευές θα αυξηθούν από 19,8 δισ. το 2025 σε πάνω από 40,6 δισ. μέχρι το 2045. Οι συσκευές IoT μπορούν να παραβιαστούν ώστε να δημιουργήσουν botnets για τεράστιες επιθέσεις DDoS.

Επιθέσεις στην Εφοδιαστική Αλυσίδα (Supply Chain)

Οι επιθέσεις supply chain εκμεταλλεύονται τις διασυνδεδεμένες υποδομές οργανισμών και τις σχέσεις εμπιστοσύνης μεταξύ εταιρειών. Με μία μόνο επίθεση μπορούν να παραβιάσουν πολλαπλούς οργανισμούς ταυτόχρονα. Έρευνα δείχνει ότι 1 στις 3 εταιρείες είδε αύξηση κυβερνοεπιθέσεων που στόχευαν την εφοδιαστική της αλυσίδα τους τελευταίους 6 μήνες.

Ασφάλεια Cloud

Καθώς οι επιχειρήσεις βασίζονται όλο και περισσότερο στο cloud computing, οι ευπάθειες στις cloud υποδομές γίνονται πιο εμφανείς.

Τα πιο συνηθισμένα προβλήματα είναι:

- λανθασμένες ρυθμίσεις (misconfigurations)

- ανεπαρκής έλεγχος πρόσβασης.

Παράδειγμα:
Λανθασμένα ρυθμισμένα S3 buckets στο AWS έχουν οδηγήσει σε μεγάλες διαρροές δεδομένων ακόμη και σε μεγάλες εταιρείες.

Κρατικές και Εσωτερικές Απειλές

Καθώς το κυβερνοχώρο γίνεται όλο και πιο γεωπολιτικά ανταγωνιστικός, οι κρατικά υποστηριζόμενες επιθέσεις και οι εσωτερικές απειλές αυξάνονται.

Κυβερνοδραστηριότητες Κρατών (Nation-State Cyber Activities)

Οι κυβερνοεπιχειρήσεις κρατών στοχεύουν σε:

- κατασκοπεία
- σαμποτάζ
- επηρεασμό πολιτικών εξελίξεων.

Αυτές οι επιχειρήσεις χαρακτηρίζονται από:

- υψηλή τεχνική πολυπλοκότητα
- σημαντικούς κρατικούς πόρους
- μακροπρόθεσμους στρατηγικούς στόχους.

Εσωτερικές Απειλές (Insider Threats)

Οι εσωτερικές απειλές προέρχονται από άτομα μέσα σε έναν οργανισμό που κάνουν κατάχρηση της πρόσβασής τους σε συστήματα και δεδομένα, είτε:

- κακόβουλα
- είτε λόγω αμέλειας.

Μεγάλες Παραβιάσεις Δεδομένων

Τα τελευταία χρόνια αρκετές μεγάλες παραβιάσεις δεδομένων αποκάλυψαν τις αδυναμίες των συστημάτων κυβερνοασφάλειας και ανέδειξαν την ανάγκη για αυστηρότερα μέτρα προστασίας.

Advanced Persistent Threats (APTs)

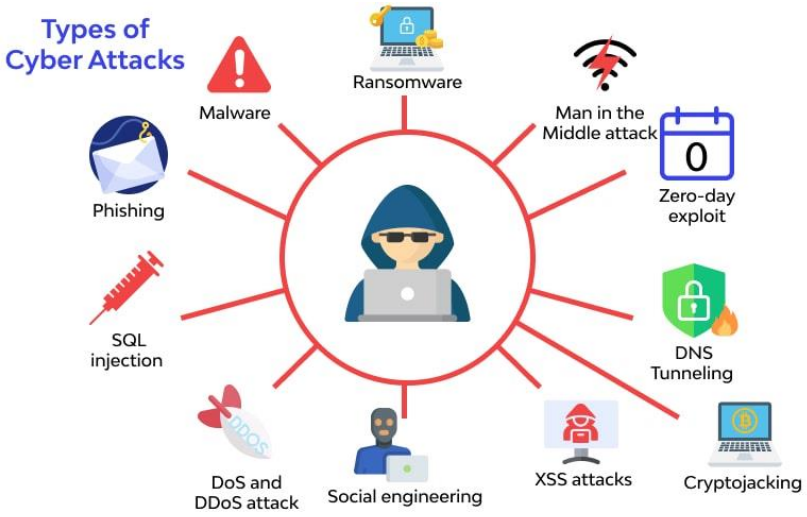
Τα APTs είναι πολύπλοκες κυβερνοεπιθέσεις που στοχεύουν κυρίως:

- στην κλοπή πληροφοριών
- ή στην υπονόμευση λειτουργιών.

Συχνά στοχεύουν:

- εθνικές κυβερνήσεις
- κρίσιμες υποδομές
- μεγάλες εταιρείες.

Αυτές οι επιθέσεις πραγματοποιούνται **σε μεγάλο χρονικό διάστημα**, γεγονός που τις καθιστά δύσκολες στον εντοπισμό και ιδιαίτερα επικίνδυνες λόγω του στρατηγικού σχεδιασμού που τις συνοδεύει.[2]



Εικόνα 2.2 : *Τύποι κυβερνοεπιθέσεων*

2.3 Η σημασία της κανονιστικής συμμόρφωσης

Οι κανονισμοί αποτελούν κανόνες που θεσπίζονται και επιβάλλονται από κρατικούς ή ρυθμιστικούς φορείς. Η σημασία τους έγκειται στο γεγονός ότι καθορίζουν τα πρότυπα που προσδιορίζουν τι επιτρέπεται και τι δεν επιτρέπεται στις επιχειρηματικές δραστηριότητες.

Μέσω των κανονισμών διασφαλίζεται ότι όλοι οι οργανισμοί λειτουργούν με βάση το ίδιο πλαίσιο κανόνων, ενώ παράλληλα προστατεύονται τα δικαιώματα και τα συμφέροντα των πολιτών. Ένα χαρακτηριστικό παράδειγμα αποτελεί ο General Data Protection Regulation (GDPR) στην Ευρώπη. Ο συγκεκριμένος κανονισμός προστασίας δεδομένων καθορίζει τα δικαιώματα των ατόμων σχετικά με τα προσωπικά τους δεδομένα και θέτει περιορισμούς στις επιχειρήσεις σχετικά με τον τρόπο συλλογής, επεξεργασίας και χρήσης αυτών των πληροφοριών. Η συμμόρφωση με τους κανονισμούς που ισχύουν για κάθε κλάδο δραστηριότητας θεωρείται απαραίτητη. Ο βαθμός συμμόρφωσης σχετίζεται με την προσέγγιση διαχείρισης κινδύνων που εφαρμόζει κάθε οργανισμός. Ο κανονισμός ορίζει ότι τα μέτρα αυτά πρέπει να είναι ανάλογα με το επίπεδο κινδύνου που ενδέχεται να προκύψει. Για τον λόγο αυτό, κάθε οργανισμός που επεξεργάζεται προσωπικά δεδομένα οφείλει να πραγματοποιεί αξιολόγηση κινδύνου. Με βάση τα αποτελέσματα της αξιολόγησης κινδύνου και την ανοχή κινδύνου του οργανισμού, καθορίζονται και εφαρμόζονται τα κατάλληλα μέτρα ασφάλειας.

2.3.1 Συνέπειες μη συμμόρφωσης με κανονισμούς

Η μη συμμόρφωση με τους ισχύοντες κανονισμούς μπορεί να οδηγήσει στην επιβολή σημαντικών οικονομικών προστίμων, τα οποία πρέπει να λαμβάνονται υπόψη στο πλαίσιο της διαχείρισης κινδύνων ενός οργανισμού. Παράλληλα, πέρα από τις οικονομικές κυρώσεις, υπάρχει και ο κίνδυνος σημαντικής βλάβης της φήμης μιας επιχείρησης. Η αρνητική δημοσιότητα που μπορεί να προκύψει από την παραβίαση κανονισμών ενδέχεται να επηρεάσει την εμπιστοσύνη πελατών και συνεργατών.

2.3.2 Πρώτα βήματα για τη διασφάλιση συμμόρφωσης

Το πρώτο και σημαντικότερο βήμα για τη διασφάλιση της συμμόρφωσης είναι η πλήρης κατανόηση των νόμων και των κανονισμών που εφαρμόζονται σε έναν οργανισμό. Οι απαιτήσεις αυτές διαφέρουν ανάλογα με τον κλάδο δραστηριότητας. Ορισμένοι κανονισμοί εφαρμόζονται σε όλους τους οργανισμούς, ενώ άλλοι είναι ειδικοί για συγκεκριμένους τομείς. Επιπλέον, οι εταιρείες που είναι εισηγμένες σε χρηματιστήρια ενδέχεται να υπόκεινται σε επιπλέον κανονιστικές απαιτήσεις. Αφού προσδιοριστούν οι ισχύοντες κανονισμοί, πραγματοποιούνται αξιολογήσεις κινδύνου. Τα αποτελέσματα αυτών των

αξιολογήσεων συμβάλλουν στη διαμόρφωση του πλαισίου διακυβέρνησης του οργανισμού, το οποίο περιλαμβάνει πολιτικές, διαδικασίες και μηχανισμούς ελέγχου. Μέσω αυτού του πλαισίου τεκμηριώνεται και αποδεικνύεται η συμμόρφωση με τις κανονιστικές απαιτήσεις.

2.3.3 Η σημασία της ασφάλειας πληροφοριών σε σχέση με τους κανονισμούς

Στη σύγχρονη ψηφιακή κοινωνία, όπου η λειτουργία των οργανισμών εξαρτάται σε μεγάλο βαθμό από δεδομένα και πληροφοριακά συστήματα, πολλοί κανονισμοί περιλαμβάνουν υποχρεωτικές απαιτήσεις σχετικά με την ασφάλεια πληροφοριών. Η απώλεια δεδομένων, όπως πληροφοριών πιστωτικών καρτών ή ιατρικών αρχείων, μπορεί να έχει σοβαρές συνέπειες τόσο για τα άτομα όσο και για τους οργανισμούς.

Η ασφάλεια πληροφοριών δεν θα πρέπει να εφαρμόζεται αποκλειστικά για την κάλυψη κανονιστικών απαιτήσεων, αλλά κυρίως για την προστασία των περιουσιακών στοιχείων ενός οργανισμού. Στη σύγχρονη οικονομία, τα δεδομένα αποτελούν ένα από τα πιο πολύτιμα περιουσιακά στοιχεία. Καθώς μεγάλο μέρος των επιχειρηματικών πόρων είναι πλέον ψηφιακό, η προστασία τους αποτελεί βασικό στοιχείο ορθής επιχειρηματικής πρακτικής. Ένας κανονισμός μπορεί, για παράδειγμα, να απαιτεί την εφαρμογή προγραμμάτων ευαισθητοποίησης σχετικά με την ασφάλεια πληροφοριών. Η απλή αποστολή μιας ετήσιας ενημέρωσης προς τους εργαζομένους ενδέχεται να καλύπτει τυπικά την απαίτηση συμμόρφωσης. Ωστόσο, για την ουσιαστική προστασία ενός οργανισμού απαιτείται ουσιαστική εκπαίδευση των εργαζομένων σχετικά με απειλές όπως το phishing και η κοινωνική μηχανική, ώστε να μπορούν να αναγνωρίζουν και να αποτρέπουν πιθανούς κινδύνους ασφάλειας.[3]

2.4 Τι σημαίνει Κανονιστική Συμμόρφωση (Regulatory Compliance) στην Κυβερνοασφάλεια;

Η κανονιστική συμμόρφωση στην κυβερνοασφάλεια αναφέρεται στην υποχρέωση ενός οργανισμού να τηρεί συγκεκριμένα νομικά, κανονιστικά και κλαδικά πρότυπα ασφάλειας πληροφοριών που καθορίζουν τον τρόπο προστασίας των δεδομένων και την εφαρμογή μέτρων ασφαλείας. Τα πρότυπα αυτά ορίζουν το βασικό επίπεδο ασφάλειας που πρέπει να διατηρούν οι επιχειρήσεις, προκειμένου να προστατεύουν ευαίσθητες πληροφορίες, να

διασφαλίζουν την ακεραιότητα των συστημάτων και να μειώνουν την έκθεση σε κυβερνοαπειλές.

Στον πυρήνα της, η συμμόρφωση με κανονισμούς προστασίας δεδομένων σημαίνει την εφαρμογή κατάλληλων μέτρων ελέγχου για την προστασία της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των δεδομένων, ιδιαίτερα όταν πρόκειται για ευαίσθητα ή ρυθμιζόμενα δεδομένα. Μέσω αυτής της διαδικασίας διασφαλίζεται ότι οι πρακτικές κυβερνοασφάλειας ενός οργανισμού ευθυγραμμίζονται με τους κανόνες που έχουν θεσπιστεί από κυβερνήσεις, επαγγελματικούς φορείς ή συμβατικές υποχρεώσεις.

Μια συχνή παρανόηση αφορά τη σύγχυση μεταξύ εσωτερικών πολιτικών κυβερνοασφάλειας και εξωτερικών κανονιστικών απαιτήσεων. Οι εσωτερικές πολιτικές αποτελούν κατευθυντήριες γραμμές που διαμορφώνονται από τον ίδιο τον οργανισμό και ρυθμίζουν ζητήματα όπως η συμπεριφορά των εργαζομένων, η χρήση των δεδομένων και η λειτουργία των πληροφοριακών συστημάτων. Οι πολιτικές αυτές μπορούν να προσαρμόζονται στις ανάγκες της επιχείρησης. Αντίθετα, οι εξωτερικές κανονιστικές απαιτήσεις αποτελούν επίσημες υποχρεώσεις που επιβάλλονται από εξωτερικούς φορείς και η μη συμμόρφωση με αυτές μπορεί να οδηγήσει σε σοβαρές οικονομικές κυρώσεις, νομικές συνέπειες ή βλάβη της φήμης του οργανισμού.

Για παράδειγμα, ένας οργανισμός υγειονομικής περίθαλψης μπορεί να διαθέτει εσωτερικές πολιτικές που καθορίζουν τον τρόπο με τον οποίο το προσωπικό διαχειρίζεται τα αρχεία ασθενών. Ωστόσο, η συμμόρφωση με τον Health Insurance Portability and Accountability Act (HIPAA) επιβάλλει συγκεκριμένες νομικές απαιτήσεις για την προστασία αυτών των δεδομένων. Αντίστοιχα, ένας πάροχος υπηρεσιών λογισμικού (SaaS) μπορεί να εφαρμόζει εσωτερικούς μηχανισμούς ελέγχου πρόσβασης, όμως πρότυπα όπως το SOC 2 απαιτούν αποδεικτικά στοιχεία για την αποτελεσματική εφαρμογή των μέτρων προστασίας δεδομένων πελατών.

Η μη συμμόρφωση δεν αποτελεί απλώς τυπική παράλειψη, αλλά εκθέτει τις επιχειρήσεις σε σημαντικούς οικονομικούς, νομικούς και λειτουργικούς κινδύνους. Οι ρυθμιστικές αρχές επιβάλλουν συχνά υψηλά πρόστιμα σε περιπτώσεις παραβίασης δεδομένων ή μη τήρησης κανονιστικών απαιτήσεων. Επιπλέον, η απώλεια εμπιστοσύνης των πελατών, η διατάραξη της λειτουργίας των οργανισμών και η αδυναμία σύναψης νέων συνεργασιών αποτελούν μακροπρόθεσμες συνέπειες.

Στο σύγχρονο ψηφιακό περιβάλλον, η κανονιστική συμμόρφωση αποτελεί κρίσιμο στοιχείο της κυβερνοασφάλειας, όχι μόνο για την ικανοποίηση εξωτερικών απαιτήσεων, αλλά και για την ενίσχυση της ανθεκτικότητας των οργανισμών, την προστασία των ενδιαφερόμενων μερών και τη διατήρηση της ανταγωνιστικότητας στην αγορά.

2.4.1 Κανονισμοί και βέλτιστες πρακτικές κυβερνοασφάλειας

Πλαίσια κυβερνοασφάλειας όπως το NIST Cybersecurity Framework, το ISO/IEC 27001 και το SOC 2 δεν αποτελούν αυθαίρετους κανόνες. Αντίθετα, έχουν προκύψει από δεκαετίες έρευνας στον τομέα της κυβερνοασφάλειας, από ανάλυση απειλών και από εμπειρίες πραγματικών κυβερνοεπιθέσεων. Οι κανονισμοί ενσωματώνουν αυτή τη γνώση σε δεσμευτικά πρότυπα με στόχο τη μείωση των κινδύνων και την αποτροπή παραβιάσεων ασφάλειας.

Συνήθως τα πρότυπα αυτά απαιτούν από τους οργανισμούς να:

- πραγματοποιούν τακτικές αξιολογήσεις κινδύνου
- εφαρμόζουν μηχανισμούς πολυπαραγοντικής ταυτοποίησης (MFA)
- κρυπτογραφούν ευαίσθητα δεδομένα
- παρακολουθούν τα πληροφοριακά συστήματα για πιθανές απειλές
- αναπτύσσουν και δοκιμάζουν σχέδια αντιμετώπισης περιστατικών ασφαλείας

Τα μέτρα αυτά αποτελούν καθιερωμένες βέλτιστες πρακτικές που συμβάλλουν στη μείωση της πιθανότητας και των επιπτώσεων κυβερνοεπιθέσεων.

Για παράδειγμα, ο General Data Protection Regulation (GDPR) απαιτεί την αρχή της ελαχιστοποίησης δεδομένων, δηλαδή τη συλλογή μόνο των απολύτως απαραίτητων πληροφοριών. Αντίστοιχα, το πρότυπο PCI DSS επιβάλλει αυστηρή κρυπτογράφηση των δεδομένων πληρωμών. Και στις δύο περιπτώσεις μειώνεται σημαντικά η πιθανότητα και η έκταση μιας πιθανής παραβίασης δεδομένων.

Ακόμη στη σύγχρονη αγορά, ιδιαίτερα σε ρυθμιζόμενους κλάδους όπως η χρηματοοικονομική, η υγεία και οι υπηρεσίες λογισμικού, οι πελάτες απαιτούν αποδείξεις συμμόρφωσης με κανονιστικά πρότυπα. Πιστοποιήσεις όπως το SOC 2 ή η συμμόρφωση με τον Health Insurance Portability and Accountability Act (HIPAA) αποτελούν συχνά προϋπόθεση για τη σύναψη συνεργασιών.

Η συμμόρφωση αποδεικνύει ότι ένας οργανισμός δεσμεύεται για την προστασία των δεδομένων των πελατών και ότι οι υπηρεσίες του πληρούν τα καθιερωμένα πρότυπα ασφάλειας. Συνολικά, το κόστος εφαρμογής μέτρων συμμόρφωσης είναι σημαντικά μικρότερο σε σύγκριση με τις συνέπειες μιας παραβίασης ασφάλειας ή κανονιστικών απαιτήσεων.[4]

2.5 Πλαίσια κυβερνοασφάλειας

Τα πλαίσια κυβερνοασφάλειας (cybersecurity frameworks) περιγράφουν τα πρότυπα και τις κατευθυντήριες γραμμές που πρέπει να ακολουθούν οι οργανισμοί προκειμένου να διαχειρίζονται διαφορετικούς κινδύνους κυβερνοασφάλειας, να εντοπίζουν ευπάθειες και να ενισχύουν την ψηφιακή τους άμυνα. Τα κενά στην προστασία της επιφάνειας επίθεσης (attack surface) καταδεικνύουν ότι οι επιχειρήσεις οφείλουν να ενισχύσουν την κυβερνοανθεκτικότητά τους.

Τα ψηφιακά αποτυπώματα των οργανισμών αυξάνονται ραγδαία, γεγονός που οδηγεί σε έκθεση των εταιρειών σε ένα ευρύ φάσμα νέων ευπαθειών. Οι κυβερνοεπιθέσεις συχνά στοχεύουν τόσο τεχνολογικά εργαλεία όσο και ανθρώπινους παράγοντες. Αφού αποκτήσουν πρόσβαση σε ένα δίκτυο, οι επιτιθέμενοι μπορούν να κινηθούν πλευρικά μέσα στο σύστημα και να επεκτείνουν την επίθεση σε άλλα σημεία της υποδομής. Επιπλέον, επιθέσεις μπορούν να πραγματοποιηθούν ακόμη και κατά τη διάρκεια περιόδων μειωμένης επιχειρησιακής δραστηριότητας, ενώ σε πολλές περιπτώσεις παρατηρείται έλλειψη ολοκληρωμένων αξιολογήσεων κινδύνου στον κλάδο.

Η απουσία ενός οργανωμένου πλαισίου κυβερνοασφάλειας μπορεί να δημιουργήσει ζητήματα λογοδοσίας σε επίπεδο διοίκησης. Παράλληλα, ενδέχεται να προκύψουν κανονιστικά και νομικά ζητήματα, τα οποία μπορεί να έχουν ευρύτερες επιπτώσεις για τη λειτουργία και τη φήμη μιας επιχείρησης.

Ένα αποτελεσματικό πλαίσιο κυβερνοασφάλειας μπορεί να βοηθήσει έναν οργανισμό να ανταποκριθεί στις διαφορετικές απαιτήσεις ασφάλειας που αντιμετωπίζει. Παράλληλα, παρέχει την απαραίτητη δομή για την υιοθέτηση κατάλληλων τεχνολογικών λύσεων και την εφαρμογή προστατευτικών μέτρων με στόχο τη διασφάλιση των κρίσιμων ψηφιακών πόρων.

2.5.1 Βασικά στοιχεία ενός πλαισίου κυβερνοασφάλειας

Ένα πλαίσιο κυβερνοασφάλειας περιλαμβάνει πέντε βασικά στοιχεία, τα οποία παρουσιάζονται παρακάτω.

1. Αναγνώριση (Identification)

Η διαδικασία αναγνώρισης περιλαμβάνει την κατανόηση των λογισμικών, συσκευών και πληροφοριακών συστημάτων που πρέπει να προστατευθούν. Σε αυτά περιλαμβάνονται

συσκευές όπως tablets, smartphones, φορητοί υπολογιστές και συστήματα σημείων πώλησης (POS).

Παράλληλα, πραγματοποιείται εντοπισμός των πιο ευάλωτων περιουσιακών στοιχείων του οργανισμού, καθώς και των εσωτερικών και εξωτερικών απειλών που ενδέχεται να τα επηρεάσουν. Μέσω αυτής της διαδικασίας, οι οργανισμοί αποκτούν σαφή εικόνα των περιοχών που απαιτούν μεγαλύτερη προσοχή και των αλλαγών που πρέπει να υλοποιηθούν.

2. Προστασία (Protection)

Η προστασία περιλαμβάνει τη λήψη μέτρων για τη διασφάλιση των δεδομένων και των πληροφοριακών συστημάτων. Εκτός από τη δημιουργία τακτικών αντιγράφων ασφαλείας (backups) και τη χρήση λογισμικού ασφάλειας, περιλαμβάνει επίσης:

Έλεγχος πρόσβασης (Access Control):
Διασφάλιση ότι μόνο εξουσιοδοτημένοι χρήστες έχουν πρόσβαση σε κρίσιμες πληροφορίες και πληροφοριακά συστήματα, καθώς και έλεγχο της πρόσβασης στο εταιρικό δίκτυο.

Ασφάλεια δεδομένων (Data Security):
Κρυπτογράφηση ευαίσθητων δεδομένων και εφαρμογή μηχανισμών προστασίας που διασφαλίζουν την εμπιστευτικότητα και την ακεραιότητα των πληροφοριών.

Εκπαίδευση και ευαισθητοποίηση (Training and Awareness):
Εκπαίδευση των εργαζομένων σχετικά με τους κινδύνους κυβερνοασφάλειας και τις κατάλληλες πρακτικές ασφάλειας, με στόχο τη μείωση ανθρώπινων λαθών που μπορεί να οδηγήσουν σε περιστατικά ασφαλείας.

3. Ανίχνευση (Detection)

Η ανίχνευση αφορά τον εντοπισμό ανωμαλιών και την προληπτική παρακολούθηση των πληροφοριακών συστημάτων και δικτύων, με στόχο την έγκαιρη αναγνώριση περιστατικών ασφάλειας. Μέσω διαδικασιών συνεχούς παρακολούθησης μπορούν να εντοπιστούν απειλές όπως μη εξουσιοδοτημένη πρόσβαση σε συστήματα ή ύποπτες δραστηριότητες εντός του δικτύου. Η έγκαιρη ανίχνευση επιτρέπει την ταχύτερη αντίδραση σε περιστατικά κυβερνοασφάλειας και περιορίζει τις πιθανές επιπτώσεις τους.

4. Αντιμετώπιση (Response)

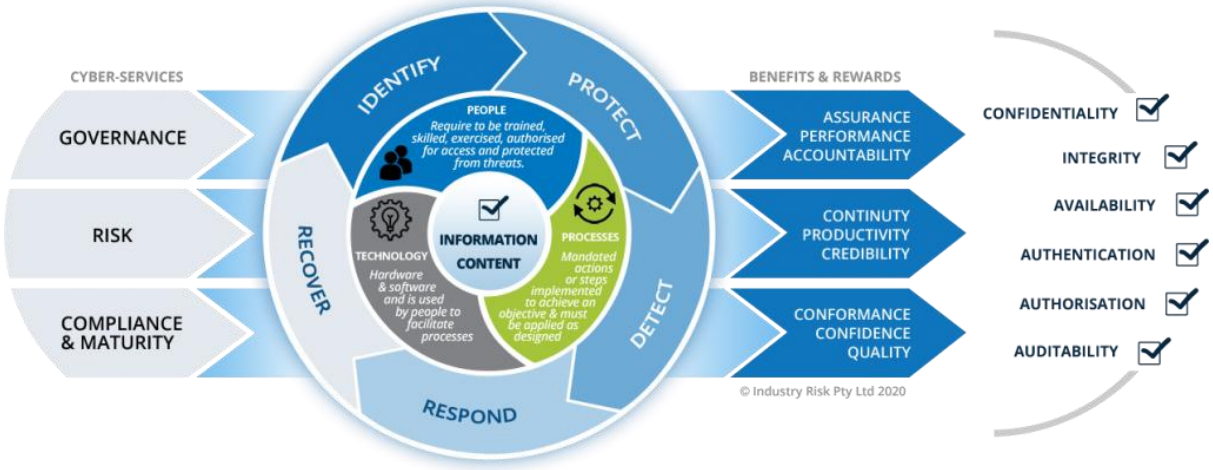
Η κατάλληλη αντιμετώπιση των κυβερνοαπειλών αποτελεί βασικό στοιχείο για την προστασία των πληροφοριακών συστημάτων ενός οργανισμού. Η διαδικασία αυτή περιλαμβάνει την ενημέρωση των ενδιαφερόμενων μερών, όπως διοίκηση, εργαζομένους και πελάτες, σε περιπτώσεις όπου υπάρχει κίνδυνος έκθεσης δεδομένων.

Παράλληλα, απαιτείται η ύπαρξη ενός σαφούς σχεδίου αντιμετώπισης περιστατικών ασφάλειας (incident response plan), το οποίο καθορίζει τις ενέργειες που πρέπει να ακολουθηθούν για τον περιορισμό της απειλής και τη μείωση των επιπτώσεων από ένα περιστατικό κυβερνοασφάλειας.

5. Ανάκαμψη (Recovery)

Η ανάκαμψη αναφέρεται στις ενέργειες που πραγματοποιούνται μετά από ένα περιστατικό κυβερνοασφάλειας, με στόχο την αποκατάσταση των συστημάτων και των υπηρεσιών ενός οργανισμού. Ένα βασικό στοιχείο της διαδικασίας ανάκαμψης είναι η ύπαρξη σχεδίων αποκατάστασης που επιτρέπουν την επαναφορά των λειτουργιών και τη διασφάλιση της επιχειρησιακής συνέχειας.

Επιπλέον, η διαδικασία αυτή περιλαμβάνει την αξιολόγηση των υφιστάμενων στρατηγικών ασφάλειας, την αναγνώριση πιθανών αδυναμιών και την αναθεώρηση των διαδικασιών, με στόχο τη βελτίωση της συνολικής στρατηγικής κυβερνοασφάλειας.



Εικόνα 2.3 : *Υπηρεσίες Κυβερνοασφάλειας*

2.6 Τύποι πλαισίων κυβερνοασφάλειας

Τα πλαίσια κυβερνοασφάλειας μπορούν να κατηγοριοποιηθούν σε τρεις βασικές κατηγορίες.

2.6.1. Πλαίσια ελέγχου (Control Frameworks)

Τα πλαίσια ελέγχου παρέχουν μια βασική στρατηγική για την εφαρμογή πρακτικών κυβερνοασφάλειας σε έναν οργανισμό. Στόχος τους είναι η μείωση των κινδύνων ασφάλειας μέσω της ιεράρχησης και της εφαρμογής κατάλληλων μηχανισμών ελέγχου ασφάλειας (security controls).

2.6.2. Πλαίσια προγραμμάτων (Program Frameworks)

Τα πλαίσια προγραμμάτων αξιολογούν την αποτελεσματικότητα του συνολικού προγράμματος κυβερνοασφάλειας ενός οργανισμού. Παράλληλα, συμβάλλουν στη βελτίωση της επικοινωνίας μεταξύ της ομάδας κυβερνοασφάλειας και της διοίκησης, διευκολύνοντας τη λήψη αποφάσεων και τον στρατηγικό σχεδιασμό στον τομέα της ασφάλειας πληροφοριών.

2.6.3. Πλαίσια διαχείρισης κινδύνου (Risk Frameworks)

Τα πλαίσια διαχείρισης κινδύνου επικεντρώνονται στον εντοπισμό και την αξιολόγηση των κινδύνων που αντιμετωπίζει ένας οργανισμός. Μέσω αυτής της διαδικασίας καθορίζονται οι κατάλληλες προτεραιότητες για την εφαρμογή μέτρων ασφάλειας, με στόχο τον περιορισμό των κινδύνων και την αποτελεσματική προστασία των πληροφοριακών συστημάτων.

2.7 Πλαίσια Κυβερνοασφάλειας

2.7.1. NIST Cybersecurity Framework

Το πλαίσιο κυβερνοασφάλειας του National Institute of Standards and Technology (NIST) αναπτύχθηκε αρχικά για την προστασία κρίσιμων υποδομών, όπως σταθμών παραγωγής ενέργειας, από κυβερνοεπιθέσεις. Το πλαίσιο αυτό αποτελείται από τρία βασικά στοιχεία: Core, Tiers και Profiles.

Το Core περιλαμβάνει έξι βασικές λειτουργίες:

- Identify (Αναγνώριση)
- Protect (Προστασία)
- Detect (Ανίχνευση)
- Respond (Αντιμετώπιση)
- Recover (Ανάκαμψη)
- Govern (Διακυβέρνηση)

Κάθε λειτουργία περιλαμβάνει επιμέρους κατηγορίες και υποκατηγορίες. Οι κατηγορίες αναφέρονται στις δραστηριότητες που συνθέτουν τη λειτουργία, ενώ οι υποκατηγορίες περιγράφουν τα επιθυμητά αποτελέσματα κάθε δραστηριότητας.

Τα Tiers χρησιμοποιούνται για την αξιολόγηση του επιπέδου ωριμότητας των πρακτικών κυβερνοασφάλειας ενός οργανισμού. Τα τέσσερα επίπεδα είναι:

- Partial: Οργανισμοί με ελάχιστα ή καθόλου μέτρα ασφάλειας και περιορισμένη κατανόηση των κινδύνων κυβερνοασφάλειας.
- Risk-Informed: Οργανισμοί που γνωρίζουν τους κινδύνους κυβερνοασφάλειας αλλά δεν διαθέτουν ολοκληρωμένες στρατηγικές αντιμετώπισης.
- Repeatable: Οργανισμοί που εφαρμόζουν βέλτιστες πρακτικές ασφάλειας και διαθέτουν αποτελεσματικές στρατηγικές διαχείρισης κινδύνου.
- Adaptive: Οργανισμοί με υψηλό επίπεδο κυβερνοανθεκτικότητας, οι οποίοι χρησιμοποιούν προγνωστικούς δείκτες για την πρόληψη επιθέσεων.

Τα Profiles περιγράφουν την τρέχουσα κατάσταση ασφάλειας ενός οργανισμού καθώς και το επιθυμητό επίπεδο ασφάλειας στο οποίο στοχεύει. Με αυτόν τον τρόπο διευκολύνεται η ιεράρχηση των απαραίτητων ενεργειών κυβερνοασφάλειας.

2.7.2. ISO/IEC 27001

Το πρότυπο ISO/IEC 27001 αναπτύχθηκε από τον International Organization for Standardization (ISO) και την International Electrotechnical Commission (IEC) και παρέχει

μια συστηματική προσέγγιση για την αξιολόγηση κινδύνων και την επιλογή κατάλληλων μέτρων ελέγχου ασφάλειας.Το πρότυπο περιλαμβάνει 114 ελέγχους ασφαλείας, οι οποίοι κατανέμονται σε 14 κατηγορίες, και προσφέρει ένα ολοκληρωμένο πλαίσιο για τη διαχείριση κινδύνων ασφάλειας πληροφοριών.Για την επίτευξη συμμόρφωσης με το πρότυπο ISO 27001 απαιτείται η υλοποίηση ενός Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών (Information Security Management System – ISMS). Οι βασικές προϋποθέσεις περιλαμβάνουν:

Κατανόηση του οργανωτικού πλαισίου

Η εφαρμογή ενός ISMS απαιτεί την κατανόηση του εσωτερικού και εξωτερικού περιβάλλοντος του οργανισμού, των ενδιαφερόμενων μερών και των κανονιστικών απαιτήσεων. Η διαδικασία αυτή συμβάλλει στον καθορισμό του πεδίου εφαρμογής του συστήματος ασφάλειας πληροφοριών.

Ηγεσία και διακυβέρνηση

Η δέσμευση της διοίκησης αποτελεί κρίσιμο παράγοντα για την επιτυχή εφαρμογή του ISMS. Η διοίκηση είναι υπεύθυνη για τον καθορισμό στόχων ασφάλειας πληροφοριών, την παροχή των απαραίτητων πόρων και τη διαμόρφωση σχετικών πολιτικών ασφάλειας.

Σχεδιασμός

Η διαδικασία σχεδιασμού περιλαμβάνει την αξιολόγηση κινδύνων, τον εντοπισμό ευκαιριών βελτίωσης και την ανάπτυξη σχεδίων αντιμετώπισης κινδύνων που ευθυγραμμίζονται με τους στρατηγικούς στόχους του οργανισμού.

2.7.3 PCI DSS

Το πρότυπο PCI-DSS - Payment Card Industry Data Security Standard σχεδιάστηκε για την προστασία δεδομένων πιστωτικών καρτών και την αποτροπή μη εξουσιοδοτημένης πρόσβασης σε οικονομικές πληροφορίες πελατών. Το πλαίσιο περιλαμβάνει 12 βασικές απαιτήσεις, οι οποίες αναλύονται σε 277 επιμέρους απαιτήσεις.

Οι απαιτήσεις αυτές καλύπτουν τομείς όπως:

- ασφάλεια δικτύου
- προστασία και αποθήκευση δεδομένων πληρωμών
- έλεγχος πρόσβασης
- παρακολούθηση και δοκιμή συστημάτων ασφάλειας

Το πρότυπο εφαρμόζεται σε όλους τους οργανισμούς που αποθηκεύουν, επεξεργάζονται ή μεταδίδουν δεδομένα καρτών πληρωμών. Παράλληλα, περιλαμβάνει τεχνικές όπως tokenization και κρυπτογράφηση για την προστασία των δεδομένων καρτών.

2.7.4. Health Insurance Portability and Accountability Act (HIPAA)

Το πλαίσιο HIPAA εφαρμόζεται κυρίως στον τομέα της υγειονομικής περίθαλψης και απαιτεί από οργανισμούς υγείας να εφαρμόζουν μέτρα προστασίας για τη διασφάλιση εμπιστευτικών ιατρικών δεδομένων.

Ο κανονισμός προστατεύει τα ηλεκτρονικά δεδομένα υγείας και είναι ιδιαίτερα σημαντικός για ασφαλιστικές εταιρείες, νοσοκομεία και παρόχους υπηρεσιών υγείας.

Εκτός από την εκπαίδευση των εργαζομένων σε θέματα κυβερνοασφάλειας, το HIPAA απαιτεί από τους οργανισμούς υγείας να πραγματοποιούν τακτικές αξιολογήσεις κινδύνου με στόχο τον εντοπισμό πιθανών απειλών και ευπαθειών.

2.7.5. General Data Protection Regulation (GDPR)

Ο κανονισμός GDPR εισήχθη με στόχο την ενίσχυση της προστασίας προσωπικών δεδομένων των πολιτών της Ευρωπαϊκής Ένωσης. Εφαρμόζεται τόσο σε εταιρείες που δραστηριοποιούνται εντός της Ευρωπαϊκής Ένωσης όσο και σε οργανισμούς που επεξεργάζονται δεδομένα πολιτών της ΕΕ.

Ο κανονισμός περιλαμβάνει 99 άρθρα που καθορίζουν τις υποχρεώσεις των οργανισμών σχετικά με:

- την προστασία προσωπικών δεδομένων
- τα δικαιώματα πρόσβασης των υποκειμένων των δεδομένων

- τη διαφάνεια στην επεξεργασία δεδομένων

Ιδιαίτερη έμφαση δίνεται στην αρχή της ελαχιστοποίησης δεδομένων, στα δικαιώματα των υποκειμένων των δεδομένων και στη διαφάνεια των διαδικασιών επεξεργασίας πληροφοριών. Σε περιπτώσεις μη συμμόρφωσης προβλέπονται σημαντικές οικονομικές κυρώσεις.[5]

3. Η Οδηγία NIS2

3.1 Ιστορική εξέλιξη: από την NIS στην NIS2

Η NIS2 αποτελεί επέκταση και ενίσχυση της προγενέστερης Οδηγίας NIS (2016) και συνιστά μια σημαντική αναθεώρηση του κανονιστικού πλαισίου κυβερνοασφάλειας της Ευρωπαϊκής Ένωσης. Στόχος της είναι η ενίσχυση του συνολικού επιπέδου κυβερνοανθεκτικότητας(cyber resilience) μεταξύ των κρατών-μελών καθώς και των οργανισμών που δραστηριοποιούνται επιχειρηματικά σε αυτά.

Η NIS2 διευρύνει το πεδίο εφαρμογής της αρχικής οδηγίας, επεκτείνοντας το εύρος των τομέων και των τύπων οργανισμών που υπάγονται στη ρύθμισή της. Σε αυτούς περιλαμβάνονται οργανισμοί που θεωρείται ότι διαδραματίζουν «ουσιώδη» ή «σημαντικό» ρόλο στην εσωτερική αγορά της Ευρωπαϊκής Ένωσης.

Για τους οργανισμούς αυτούς, η NIS2 σηματοδοτεί αυστηρότερες απαιτήσεις συμμόρφωσης σε θέματα ασφάλειας. Πολλοί οργανισμοί είτε θα ενταχθούν για πρώτη φορά στο κανονιστικό πεδίο εφαρμογής είτε θα υποχρεωθούν να τηρούν σημαντικά υψηλότερα πρότυπα και αυστηρότερες κυρώσεις σε σύγκριση με την προηγούμενη οδηγία.

Η NIS2 εισάγει επίσης αυξημένες υποχρεώσεις, απαιτώντας από τους οργανισμούς να υιοθετήσουν ολοκληρωμένους μηχανισμούς αναφοράς περιστατικών, ισχυρές πρακτικές διαχείρισης κινδύνων, μέτρα εταιρικής λογοδοσίας και αποτελεσματικές στρατηγικές επιχειρησιακής συνέχειας. Παράλληλα, η οδηγία προβλέπει σημαντικές συνέπειες σε περιπτώσεις μη συμμόρφωσης, όπως υψηλά πρόστιμα και πιθανές νομικές διαδικασίες.

Ως οδηγία της Ευρωπαϊκής Ένωσης, η NIS2 θα εφαρμοστεί με διαφοροποιήσεις από τα κράτη-μέλη, γεγονός που ενδέχεται να προσθέσει επιπλέον πολυπλοκότητα για επιχειρήσεις που δραστηριοποιούνται διασυνοριακά εντός της ΕΕ. Ωστόσο, το μήνυμα είναι σαφές: η προετοιμασία είναι απαραίτητη. Οι οργανισμοί σε όλη την Ευρωπαϊκή Ένωση οφείλουν να λάβουν προληπτικά μέτρα ώστε να κατανοήσουν τον κανονισμό, να αξιολογήσουν τις επιπτώσεις του στις δραστηριότητές τους και να αναπτύξουν ένα σχέδιο δράσης για τη διασφάλιση της συμμόρφωσης.[6]

Εικόνα 3.1 : *Από το NIS στο NIS2*

3.2 Βασικές αρχές και απαιτήσεις

Ο νέος κανονισμός κυβερνοασφάλειας NIS2 αυξάνει σημαντικά τις απαιτήσεις για τους οργανισμούς σε ολόκληρη την Ευρωπαϊκή Ένωση. Η οδηγία θέτει αυστηρούς κανόνες σε τέσσερις βασικούς τομείς υποχρεώσεων: τη διαχείριση κινδύνων, την εταιρική λογοδοσία, τις υποχρεώσεις αναφοράς περιστατικών και την επιχειρησιακή συνέχεια(business continuity), ενώ προβλέπει αυστηρές κυρώσεις σε περιπτώσεις μη συμμόρφωσης. Εάν ένας οργανισμός εμπίπτει στο πεδίο εφαρμογής της NIS2, είναι απαραίτητο να ξεκινήσει άμεσα τις

διαδικασίες συμμόρφωσης, καθώς η συμμόρφωση απαιτεί χρόνο και οι έλεγχοι εφαρμογής της οδηγίας πλησιάζουν.

3.2.1 Διαδικασίες συμμόρφωσης

1. Απαιτήσεις διαχείρισης κινδύνων: ενίσχυση της κυβερνοανθεκτικότητας

Η NIS2 απαιτεί από τους οργανισμούς να εφαρμόζουν ισχυρά μέτρα ασφάλειας προκειμένου να μειωθούν οι κυβερνοκίνδυνοι. Τα μέτρα αυτά περιλαμβάνουν:

- Ισχυρότερο έλεγχο πρόσβασης: Η πολυπαραγοντική ταυτοποίηση (Multi-Factor Authentication – MFA) είναι υποχρεωτική, ενώ όπου δεν είναι εφικτή πρέπει να εφαρμόζονται εναλλακτικές μέθοδοι ταυτοποίησης.
- Κρυπτογράφηση δεδομένων και ασφαλή αντίγραφα ασφαλείας: Τα ευαίσθητα δεδομένα πρέπει να κρυπτογραφούνται τόσο κατά την αποθήκευση όσο και κατά τη μεταφορά τους, ενώ απαιτούνται τακτικά ελεγχόμενα αντίγραφα ασφαλείας ώστε να διασφαλίζεται η γρήγορη αποκατάσταση σε περίπτωση παραβίασης.
- Ενισχυμένη ασφάλεια δικτύου: Firewalls και συστήματα ανίχνευσης και πρόληψης εισβολών (IDS/IPS) πρέπει να παρακολουθούν και να προστατεύουν τα δίκτυα από μη εξουσιοδοτημένη πρόσβαση.
- Διαχείριση περιστατικών: Οι οργανισμοί οφείλουν να αναπτύξουν σαφείς διαδικασίες αντιμετώπισης περιστατικών ασφάλειας και να πραγματοποιούν ασκήσεις προσομοίωσης για την αξιολόγηση της αποτελεσματικότητάς τους.
- Ασφάλεια τρίτων συνεργατών: Οι επιχειρήσεις πρέπει να αξιολογούν το επίπεδο κυβερνοασφάλειας προμηθευτών και συνεργατών, διασφαλίζοντας ότι συμμορφώνονται με τα πρότυπα της NIS2.

2. Απαιτήσεις εταιρικής λογοδοσίας: η κυβερνοασφάλεια ως ευθύνη της διοίκησης

Σύμφωνα με τη NIS2, η ανώτερη διοίκηση φέρει άμεση ευθύνη για τη συμμόρφωση σε θέματα κυβερνοασφάλειας. Οι διοικητικές ομάδες οφείλουν να:

- Επιβλέπουν και να εγκρίνουν τις στρατηγικές κυβερνοασφάλειας, διασφαλίζοντας ότι ευθυγραμμίζονται με τις απαιτήσεις της NIS2
- Συμμετέχουν σε εκπαιδεύσεις κυβερνοασφάλειας ώστε να παραμένουν ενημερωμένες σχετικά με τις απειλές και τις υποχρεώσεις συμμόρφωσης

- Αναλαμβάνουν ευθύνη για αποτυχίες στον τομέα της κυβερνοασφάλειας, οι οποίες μπορεί να οδηγήσουν ακόμη και σε προσωρινή απαγόρευση άσκησης διοικητικών καθηκόντων σε σοβαρές περιπτώσεις μη συμμόρφωσης.

3. Υποχρεώσεις αναφοράς: αυστηρά χρονικά όρια για την αναφορά περιστατικών

Οι οργανισμοί υποχρεούνται να αναφέρουν άμεσα περιστατικά κυβερνοασφάλειας στις αρμόδιες εθνικές αρχές:

- Ειδοποίηση προειδοποίησης εντός 24 ωρών για σημαντικά περιστατικά
- Πλήρης αναφορά εντός 72 ωρών, η οποία περιγράφει λεπτομερώς την παραβίαση και τα μέτρα αντιμετώπισης
- Τελική αναφορά εντός ενός μήνα, η οποία παρουσιάζει τις ενέργειες αποκατάστασης και τις μακροπρόθεσμες βελτιώσεις.

Η μη έγκαιρη αναφορά περιστατικών μπορεί να οδηγήσει σε πρόστιμα και αυξημένο έλεγχο από τις ρυθμιστικές αρχές.

4. Απαιτήσεις επιχειρησιακής συνέχειας: διασφάλιση ανθεκτικότητας κατά τη διάρκεια κυβερνοεπιθέσεων

Οι οργανισμοί πρέπει να είναι προετοιμασμένοι για σοβαρά περιστατικά κυβερνοασφάλειας μέσω ενός ολοκληρωμένου σχεδίου επιχειρησιακής συνέχειας που περιλαμβάνει:

- Διαδικασίες αποκατάστασης συστημάτων και μέτρα έκτακτης ανάγκης για τη μείωση του χρόνου διακοπής λειτουργίας
- Ομάδες διαχείρισης κρίσεων εκπαιδευμένες στην αντιμετώπιση περιστατικών κυβερνοασφάλειας
- Ενημερωμένα αντίγραφα ασφαλείας ώστε να διασφαλίζεται η ακεραιότητα των δεδομένων και η συνέχεια των λειτουργιών.

3.2.2 Λίστα μέτρων ασφάλειας NIS2

1. **Αξιολόγηση κινδύνων και πολιτικές ασφάλειας:** Οι οργανισμοί πρέπει να αξιολογούν τακτικά τους κυβερνοκινδύνους και να εφαρμόζουν κατάλληλους μηχανισμούς ασφάλειας για την αντιμετώπισή τους.

2. **Διαδικασίες μέτρησης της αποτελεσματικότητας της ασφάλειας:** Απαιτούνται έλεγχοι ασφάλειας, δοκιμές διείσδυσης (penetration testing) και συνεχείς αξιολογήσεις.
3. **Πολιτικές κρυπτογράφησης:** Τα ευαίσθητα δεδομένα πρέπει να κρυπτογραφούνται τόσο κατά την αποθήκευση όσο και κατά τη μεταφορά τους.
4. **Πλαίσιο διαχείρισης περιστατικών:** Πρέπει να υπάρχει οργανωμένο σχέδιο αντιμετώπισης περιστατικών για τον εντοπισμό, τη διαχείριση και την αποκατάσταση παραβιάσεων ασφάλειας.
5. **Ασφαλείς πολιτικές προμηθειών και λειτουργίας συστημάτων:** Οι οργανισμοί οφείλουν να εφαρμόζουν βέλτιστες πρακτικές ασφάλειας κατά την ανάπτυξη συστημάτων, τις προμήθειες και τη συντήρηση των πληροφοριακών συστημάτων.
6. **Εκπαίδευση κυβερνοασφάλειας και ψηφιακή υγιεινή:** Οι εργαζόμενοι πρέπει να λαμβάνουν τακτική εκπαίδευση για τη μείωση κινδύνων που σχετίζονται με ανθρώπινα λάθη.
7. **Έλεγχος πρόσβασης και διαχείριση περιουσιακών στοιχείων:** Απαιτούνται ισχυρές πολιτικές ελέγχου πρόσβασης και πλήρης καταγραφή των κρίσιμων πληροφοριακών πόρων.
8. **Σχεδιασμός επιχειρησιακής συνέχειας:** Οι οργανισμοί πρέπει να διατηρούν ενημερωμένα αντίγραφα ασφαλείας και στρατηγικές αποκατάστασης συστημάτων.
9. **Προηγμένες μέθοδοι αυθεντικοποίησης και ασφαλής επικοινωνία:** Πρέπει να χρησιμοποιούνται μέθοδοι όπως πολυπαραγοντική ταυτοποίηση (MFA), κρυπτογραφημένη επικοινωνία και συνεχής ταυτοποίηση.
10. **Πολιτικές ασφάλειας για τρίτους συνεργάτες:** Οι οργανισμοί πρέπει να αξιολογούν την κυβερνοασφάλεια των προμηθευτών τους και να εφαρμόζουν μέτρα για την προστασία της εφοδιαστικής αλυσίδας.

Με την εφαρμογή αυτών των μέτρων, οι οργανισμοί ενισχύουν την κυβερνοασφάλειά τους και παράλληλα κάνουν ένα σημαντικό βήμα προς τη συμμόρφωση με τη NIS2, μειώνοντας τους κινδύνους, ενισχύοντας την ανθεκτικότητα και ανταποκρινόμενοι στις κανονιστικές απαιτήσεις.

3.2.3 Ικανοποίηση απαιτήσεων NIS2

Η κατανόηση και εφαρμογή των απαιτήσεων της NIS2 μπορεί αρχικά να φαίνεται περίπλοκη. Ωστόσο, η διαδικασία γίνεται πιο διαχειρίσιμη όταν χωρίζεται σε σαφή και πρακτικά βήματα. Η παρακάτω λίστα παρουσιάζει τις βασικές ενέργειες που πρέπει να ακολουθήσουν οι οργανισμοί για να επιτύχουν συμμόρφωση με την NIS2, από την αξιολόγηση κινδύνων έως την προετοιμασία για ελέγχους.

1. Προσδιορισμός αν ο οργανισμός εμπίπτει στο πεδίο εφαρμογής

Το πρώτο βήμα είναι να επιβεβαιωθεί εάν η οδηγία NIS2 εφαρμόζεται στον οργανισμό. Η οδηγία καλύπτει ουσιώδεις και σημαντικές οντότητες σε διάφορους τομείς, όπως η ενέργεια, η υγεία, οι χρηματοπιστωτικές υπηρεσίες, οι ψηφιακές υπηρεσίες και η βιομηχανική παραγωγή. Επιπλέον, εάν ένας οργανισμός λειτουργεί ως προμηθευτής ή συνεργάτης σε αυτούς τους τομείς, ενδέχεται επίσης να απαιτείται συμμόρφωση.

2. Διενέργεια ανάλυσης κενών (NIS2 Gap Analysis)

Για την επίτευξη συμμόρφωσης με την NIS2, είναι απαραίτητη η πραγματοποίηση μιας ανάλυσης κενών, προκειμένου να εντοπιστούν αδυναμίες στο υπάρχον πλαίσιο κυβερνοασφάλειας.

Οι οργανισμοί πρέπει να αξιολογήσουν την ετοιμότητά τους σε θέματα διαχείρισης κινδύνων και αντιμετώπισης περιστατικών. Είναι σημαντικό να εξεταστεί εάν υπάρχουν σαφείς διαδικασίες για τον εντοπισμό και την αναφορά κυβερνοαπειλών. Παράλληλα, πρέπει να ελεγχθούν οι μηχανισμοί ελέγχου πρόσβασης και η κρυπτογράφηση, ώστε να διασφαλίζεται η προστασία των ευαίσθητων δεδομένων και η χρήση πολυπαραγοντικής ταυτοποίησης (MFA).

Επιπλέον, πρέπει να αξιολογηθεί η ασφάλεια τρίτων συνεργατών και προμηθευτών, καθώς και να ενισχυθούν τα σχέδια επιχειρησιακής συνέχειας για την ταχεία αποκατάσταση σε περίπτωση διαταραχών. Τέλος, είναι σημαντικό να διασφαλιστεί ότι η τεκμηρίωση συμμόρφωσης και οι διαδικασίες αναφοράς είναι ενημερωμένες και ανταποκρίνονται στις αυστηρές προθεσμίες της NIS2.

3. Ανάπτυξη στρατηγικής διαχείρισης κυβερνοκινδύνων

Μια ισχυρή στρατηγική διαχείρισης κινδύνων κυβερνοασφάλειας αποτελεί βασικό στοιχείο για τη συμμόρφωση με την NIS2.

Οι οργανισμοί πρέπει να πραγματοποιούν τακτικές αξιολογήσεις κινδύνου ώστε να εντοπίζουν ευπάθειες πριν τις εκμεταλλευτούν πιθανοί επιτιθέμενοι. Παράλληλα, πρέπει να ενισχύσουν τους μηχανισμούς ελέγχου πρόσβασης και να εφαρμόσουν πολυπαραγοντική ταυτοποίηση (MFA) για την αποτροπή μη εξουσιοδοτημένης πρόσβασης.

Επιπλέον, είναι απαραίτητη η εφαρμογή πολιτικών κρυπτογράφησης για την προστασία ευαίσθητων δεδομένων τόσο κατά την αποθήκευση όσο και κατά τη μεταφορά τους. Η διαχείριση ευπαθειών, μέσω τακτικών ενημερώσεων λογισμικού και δοκιμών διείσδυσης (penetration testing), συμβάλλει επίσης στη μείωση των κινδύνων.

4. Ενίσχυση της εταιρικής διακυβέρνησης και λογοδοσίας

Σύμφωνα με τη NIS2, η κυβερνοασφάλεια αποτελεί ευθύνη της διοίκησης. Η ανώτερη διοίκηση πρέπει να επιβλέπει και να εγκρίνει τις πολιτικές ασφάλειας, διασφαλίζοντας ότι η συμμόρφωση δεν αποτελεί αποκλειστικά ζήτημα των τμημάτων πληροφορικής.

Τα διοικητικά στελέχη πρέπει να λαμβάνουν κατάλληλη εκπαίδευση σε θέματα κυβερνοασφάλειας, ώστε να κατανοούν τους κινδύνους και τις ευθύνες τους στη διαδικασία λήψης αποφάσεων. Παράλληλα, η ύπαρξη ενός υπεύθυνου ασφάλειας πληροφοριών (π.χ. CISO) μπορεί να συμβάλει στον συντονισμό των ενεργειών συμμόρφωσης. Η τακτική αναθεώρηση των πλαισίων ασφάλειας και των σχεδίων αντιμετώπισης περιστατικών διασφαλίζει ότι τα μέτρα προστασίας παραμένουν ενημερωμένα.

5. Δημιουργία διαδικασίας αντιμετώπισης και αναφοράς περιστατικών

Η NIS2 επιβάλλει αυστηρές προθεσμίες αναφοράς για σημαντικά περιστατικά κυβερνοασφάλειας. Οι οργανισμοί πρέπει να αποστέλλουν αρχική ειδοποίηση εντός 24 ωρών, αναλυτική αναφορά εντός 72 ωρών και τελική έκθεση αποκατάστασης εντός ενός μήνα.

Η ύπαρξη ενός σαφούς και καλά τεκμηριωμένου σχεδίου αντιμετώπισης περιστατικών διασφαλίζει την άμεση αντίδραση σε περίπτωση επίθεσης, μειώνοντας τις ζημιές και τους κανονιστικούς κινδύνους. Η κατάλληλη προετοιμασία επιτρέπει ταχύτερη απομόνωση της απειλής, συμμόρφωση με τις κανονιστικές απαιτήσεις και αποτελεσματική αποκατάσταση των συστημάτων.

6. Ασφάλεια της εφοδιαστικής αλυσίδας

Στο πλαίσιο της NIS2, οι κίνδυνοι που προέρχονται από τρίτους συνεργάτες δεν μπορούν να αγνοηθούν. Οι οργανισμοί πρέπει να αξιολογούν το επίπεδο κυβερνοασφάλειας των προμηθευτών τους και να διασφαλίζουν ότι αυτοί πληρούν τα απαιτούμενα πρότυπα συμμόρφωσης.

Οι συμβάσεις με προμηθευτές θα πρέπει να περιλαμβάνουν συγκεκριμένες υποχρεώσεις κυβερνοασφάλειας, ώστε η ασφάλεια να αποτελεί κοινή ευθύνη. Επιπλέον, η εφαρμογή συστημάτων παρακολούθησης κινδύνων συμβάλλει στον εντοπισμό πιθανών ευπαθειών πριν εξελιχθούν σε απειλές.

7. Προετοιμασία για ελέγχους και κανονιστικές αξιολογήσεις

Η NIS2 απαιτεί από τους οργανισμούς να αποδεικνύουν τη συμμόρφωσή τους με τις απαιτήσεις της οδηγίας. Οι ρυθμιστικές αρχές μπορούν να πραγματοποιούν ελέγχους, επομένως οι οργανισμοί πρέπει να είναι σε θέση να παρουσιάσουν τα μέτρα κυβερνοασφάλειας που εφαρμόζουν.

Είναι απαραίτητη η διατήρηση ολοκληρωμένης τεκμηρίωσης σχετικά με τις αξιολογήσεις κινδύνων, τις πολιτικές ασφάλειας και τους μηχανισμούς προστασίας. Η πραγματοποίηση τακτικών εσωτερικών ελέγχων συμβάλλει στον έγκαιρο εντοπισμό αδυναμιών πριν από έναν εξωτερικό έλεγχο. Παράλληλα, η συνεχής εκπαίδευση του προσωπικού σε θέματα κυβερνοασφάλειας διασφαλίζει ότι όλοι οι εργαζόμενοι είναι κατάλληλα προετοιμασμένοι.

Μια συστηματική και οργανωμένη προσέγγιση συμβάλλει στη μείωση των κινδύνων, στην ενίσχυση της κυβερνοανθεκτικότητας και στη διατήρηση της ετοιμότητας του οργανισμού για ελέγχους συμμόρφωσης.

3.3 Τομείς και οντότητες που καλύπτονται

Η NIS2 δεν αφορά πλέον μόνο τις κρίσιμες υποδομές. Διευρύνει σημαντικά το κανονιστικό της πεδίο, καλύπτοντας περισσότερους κλάδους και οργανισμούς σε σχέση με το παρελθόν. Εάν ένας οργανισμός παρέχει βασικές ψηφιακές ή φυσικές υπηρεσίες στην Ευρωπαϊκή Ένωση ή διαδραματίζει σημαντικό ρόλο στην εφοδιαστική αλυσίδα, είναι πιθανό να εμπίπτει στο πεδίο εφαρμογής της οδηγίας.

Η οδηγία κατατάσσει τους οργανισμούς σε δύο βασικές κατηγορίες:

- **Ουσιαστικές οντότητες (Essential entities):** όπως οργανισμοί ενέργειας, υγείας, τραπεζικών υπηρεσιών και μεταφορών, οι οποίοι υπόκεινται σε αυστηρότερη εποπτεία και έλεγχο.
- **Σημαντικές οντότητες (Important entities):** όπως υπηρεσίες πληροφορικής, ψηφιακές υποδομές και βιομηχανικές επιχειρήσεις, οι οποίες επίσης πρέπει να συμμορφώνονται, αλλά με ελαφρώς μικρότερο βαθμό κανονιστικού ελέγχου.

3.3.1 Ουσιαστικές οντότητες (Essential entities)

Οι οργανισμοί αυτοί αντιμετωπίζουν τις αυστηρότερες απαιτήσεις συμμόρφωσης, λόγω του κρίσιμου ρόλου τους στην οικονομία και τη δημόσια ασφάλεια:

- **Ενέργεια:** ηλεκτρική ενέργεια, φυσικό αέριο, πετρέλαιο, συστήματα θέρμανσης και ψύξης, προμήθεια υδρογόνου, υποδομές φόρτισης ηλεκτρικών οχημάτων.
- **Μεταφορές και logistics:** αεροπορικές, σιδηροδρομικές, οδικές και θαλάσσιες μεταφορές, συμπεριλαμβανομένων ναυτιλιακών εταιρειών και διαχειριστών λιμένων.
- **Χρηματοπιστωτικές υπηρεσίες:** τραπεζικές υπηρεσίες, χρηματοοικονομικές συναλλαγές, υποδομές χρηματοπιστωτικών αγορών και ασφαλιστικές εταιρείες.
- **Υγεία:** νοσοκομεία, ερευνητικά ιατρικά εργαστήρια, φαρμακευτικές εταιρείες και κατασκευαστές ιατρικού εξοπλισμού.
- **Υδροδότηση:** διαχείριση πόσιμου νερού και επεξεργασία λυμάτων.
- **Ψηφιακές υποδομές:** πάροχοι DNS και μητρώα domain ανώτατου επιπέδου (top-level domain registries).
- **Δημόσια διοίκηση:** κυβερνητικοί οργανισμοί και άλλοι δημόσιοι φορείς.
- **Διαστημική βιομηχανία:** φορείς που διαχειρίζονται επίγειες διαστημικές υποδομές.

3.3.2 Σημαντικές οντότητες (Important entities)

Παρόλο που οι παρακάτω τομείς δεν θεωρούνται κρίσιμες υποδομές, εξακολουθούν να έχουν υποχρεώσεις συμμόρφωσης σύμφωνα με την NIS2:

- Παραγωγή τροφίμων
- Ταχυδρομικές και ταχυμεταφορικές υπηρεσίες
- Χημική βιομηχανία
- Βιομηχανική παραγωγή
- Ψηφιακές υπηρεσίες
- Ερευνητικά ιδρύματα
- Διαχείριση αποβλήτων

Εάν μια επιχείρηση ανήκει σε έναν από αυτούς τους τομείς ή παρέχει κρίσιμες υπηρεσίες σε ουσιαστικές οντότητες, τότε υποχρεούται να εφαρμόζει μέτρα διαχείρισης κινδύνων κυβερνοασφάλειας, να αναφέρει περιστατικά ασφάλειας και να διασφαλίζει τη συμμόρφωσή της με τις απαιτήσεις της οδηγίας. Εάν δεν είναι σαφές εάν η NIS2 εφαρμόζεται σε έναν οργανισμό, είναι σημαντικό να εξεταστεί εάν διαχειρίζεται κρίσιμα δεδομένα, παρέχει βασικές υπηρεσίες ή βασίζεται σε δικτυωμένα πληροφοριακά συστήματα. Σε τέτοιες περιπτώσεις, είναι απαραίτητο να ελεγχθούν οι σχετικές υποχρεώσεις, καθώς η μη συμμόρφωση μπορεί να επιφέρει σημαντικές συνέπειες.[7]

Εικόνα 3.2 : *Μέτρα NIS2*

3.4 Ρόλοι και αρμοδιότητες (Κράτη Μέλη,CSIRTs, Οργανισμοί)

Η Οδηγία NIS2 απαιτεί από τους οργανισμούς να υιοθετήσουν μια ολοκληρωμένη και δομημένη προσέγγιση στην κυβερνοασφάλεια, αναθέτοντας ένα σύνολο ευθυνών τόσο στις ουσιαστικές όσο και στις σημαντικές οντότητες. Ακολουθεί μια συνοπτική παρουσίαση των βασικών οργανωτικών ευθυνών:

3.4.1 Βασικές οργανωτικές ευθύνες

1. Διαχείριση κινδύνων κυβερνοασφάλειας

Αξιολόγηση κινδύνων: Οι οργανισμοί πρέπει να πραγματοποιούν τακτικές αξιολογήσεις κινδύνων κυβερνοασφάλειας, ώστε να εντοπίζουν και να διαχειρίζονται απειλές που αφορούν τόσο τον οργανισμό όσο και την εφοδιαστική του αλυσίδα.

Πολιτικές ασφάλειας: Απαιτείται η εφαρμογή ολοκληρωμένων πολιτικών κυβερνοασφάλειας που καλύπτουν όλες τις λειτουργίες του οργανισμού.

2. Εφαρμογή μέτρων ασφάλειας

Ασφάλεια δικτύου: Διασφάλιση της προστασίας των δικτύων και των πληροφοριακών συστημάτων, συμπεριλαμβανομένης της φυσικής και περιβαλλοντικής ασφάλειας.

Έλεγχος πρόσβασης: Εφαρμογή συστημάτων διαχείρισης ταυτότητας και πρόσβασης για τον περιορισμό της μη εξουσιοδοτημένης πρόσβασης.

Αντιμετώπιση περιστατικών: Ανάπτυξη και διατήρηση αποτελεσματικών σχεδίων αντιμετώπισης περιστατικών και διαχείρισης κρίσεων.

Παρακολούθηση συστημάτων: Συνεχής παρακολούθηση δικτύων και συστημάτων για τον εντοπισμό περιστατικών κυβερνοασφάλειας.

3. Αναφορά περιστατικών

Αρχική ειδοποίηση: Αναφορά σημαντικών περιστατικών κυβερνοασφάλειας στην αρμόδια εθνική αρχή εντός 24 ωρών από την ανίχνευσή τους.

Αναλυτική αναφορά: Παροχή πιο ολοκληρωμένης αναφοράς περιστατικού εντός 72 ωρών.

Τελική αναφορά: Υποβολή τελικής έκθεσης μετά την επίλυση του περιστατικού, η οποία περιλαμβάνει την αιτία του συμβάντος και τις ενέργειες αποκατάστασης που πραγματοποιήθηκαν.

4. Ασφάλεια εφοδιαστικής αλυσίδας

Διαχείριση κινδύνων προμηθευτών: Αξιολόγηση του επιπέδου κυβερνοασφάλειας προμηθευτών και παρόχων υπηρεσιών τρίτων.

Συμβατικές υποχρεώσεις: Συμπερίληψη απαιτήσεων κυβερνοασφάλειας στις συμβάσεις με προμηθευτές ώστε να διασφαλίζεται η συμμόρφωση.

5. Διακυβέρνηση και λογοδοσία

Εποπτεία διοίκησης: Διασφάλιση ότι η ανώτερη διοίκηση συμμετέχει ενεργά στην εποπτεία της διαχείρισης κινδύνων κυβερνοασφάλειας.

Προσωπική ευθύνη: Η ανώτερη διοίκηση ενδέχεται να φέρει προσωπική ευθύνη σε περιπτώσεις μη συμμόρφωσης με τις απαιτήσεις της οδηγίας.

Εκπαίδευση και ευαισθητοποίηση: Παροχή εκπαιδεύσεων κυβερνοασφάλειας στους εργαζομένους και τακτική ενημέρωση των δεξιοτήτων τους.

6. Συνεργασία και ανταλλαγή πληροφοριών

Ανταλλαγή πληροφοριών: Συμμετοχή σε δίκτυα ανταλλαγής πληροφοριών και κοινοποίηση σχετικών πληροφοριών απειλών σε άλλους οργανισμούς του ίδιου κλάδου και στις αρμόδιες αρχές.

Συνεργασία με CSIRTs: Συνεργασία με τις Ομάδες Αντιμετώπισης Περιστατικών Ασφάλειας Υπολογιστών (Computer Security Incident Response Teams – CSIRTs) και άλλες αρμόδιες εθνικές αρχές.

7. Διαχείριση κρίσεων και ανθεκτικότητα

Σχεδιασμός επιχειρησιακής συνέχειας: Ανάπτυξη και διατήρηση σχεδίων επιχειρησιακής συνέχειας και ανάκαμψης από καταστροφές.

Δοκιμές ανθεκτικότητας: Πραγματοποίηση τακτικών ασκήσεων και δοκιμών για τη διασφάλιση της ανθεκτικότητας των συστημάτων.

8. Τεκμηρίωση και έλεγχοι

Τήρηση αρχείων: Διατήρηση τεκμηρίωσης σχετικά με πολιτικές κυβερνοασφάλειας, αξιολογήσεις κινδύνων και αναφορές περιστατικών.

Συμμόρφωση σε ελέγχους: Ετοιμότητα για ελέγχους από τις εθνικές αρχές και παροχή αποδεικτικών στοιχείων συμμόρφωσης.

9. Μέτρα ειδικά για κάθε τομέα

Τομεακές απαιτήσεις: Εφαρμογή πρόσθετων μέτρων που σχετίζονται με τον συγκεκριμένο κλάδο δραστηριότητας του οργανισμού, όπως προβλέπεται από την οδηγία.

Η NIS2 επιβάλλει μια ολιστική προσέγγιση στην κυβερνοασφάλεια, απαιτώντας από τους οργανισμούς όχι μόνο να προστατεύουν τα δικά τους δίκτυα και συστήματα, αλλά και να αντιμετωπίζουν κινδύνους που προκύπτουν από την εφοδιαστική αλυσίδα και τον ευρύτερο κλάδο δραστηριότητάς τους. Η συμμόρφωση προϋποθέτει συνεχή βελτίωση των στρατηγικών κυβερνοασφάλειας, της εταιρικής διακυβέρνησης και των μηχανισμών αναφοράς.

Παρόλο που οι γενικές απαιτήσεις παρέχουν έναν σαφή προσανατολισμό για το πώς οι οργανισμοί πρέπει να οργανώσουν το ανθρώπινο δυναμικό, τις διαδικασίες και τις τεχνολογίες τους ώστε να προετοιμαστούν για τη NIS2, όπως συμβαίνει με κάθε κανονιστικό πλαίσιο, η ουσία βρίσκεται στις λεπτομέρειες. Για τον λόγο αυτό, είναι σημαντική η πλήρης μελέτη της οδηγίας ή η συνεργασία με εξειδικευμένους συμβούλους που γνωρίζουν σε βάθος τις απαιτήσεις της.

Ιδιαίτερα σημαντική πρόκληση αποτελεί η παρακολούθηση των διαφοροποιήσεων στην εφαρμογή της οδηγίας μεταξύ των κρατών-μελών, γεγονός που είναι καθοριστικό για τη διασφάλιση της συμμόρφωσης, ιδίως για επιχειρήσεις που δραστηριοποιούνται σε περισσότερες από μία χώρες.[6]

3.5 Κυρώσεις και μηχανισμοί επιβολής

3.5.1 Περίπτωση μη συμμόρφωσης με τις απαιτήσεις της NIS2

Η μη συμμόρφωση με τις απαιτήσεις της NIS2 αποτελεί σοβαρό κανονιστικό ζήτημα και μπορεί να θέσει έναν οργανισμό αντιμέτωπο με σημαντικά πρόστιμα και κυρώσεις. Με την αυστηροποίηση της εφαρμογής της οδηγίας από το 2025, η μη συμμόρφωση μπορεί να οδηγήσει σε σοβαρές οικονομικές και λειτουργικές επιπτώσεις για τις επιχειρήσεις.

Τα πρόστιμα και οι κυρώσεις είναι ιδιαίτερα αυστηρά. Οι ουσιαστικές οντότητες (essential entities) μπορούν να αντιμετωπίσουν πρόστιμα έως 10 εκατομμύρια ευρώ ή έως 2% του παγκόσμιου ετήσιου κύκλου εργασιών τους. Αντίστοιχα, οι σημαντικές οντότητες (important entities) μπορεί να τιμωρηθούν με πρόστιμα έως 7 εκατομμύρια ευρώ ή έως 1,4% του παγκόσμιου κύκλου εργασιών τους. Παράλληλα, οι ρυθμιστικές αρχές έχουν τη δυνατότητα να ενισχύσουν την εποπτεία των οργανισμών, να επιβάλουν πρόσθετες απαιτήσεις ασφάλειας και να πραγματοποιούν ελέγχους για τη διασφάλιση της συμμόρφωσης.

Επιπλέον, τα διοικητικά στελέχη μπορεί να φέρουν προσωπική ευθύνη. Η οδηγία NIS2 αποδίδει άμεση ευθύνη στην ανώτερη διοίκηση για την εφαρμογή των κατάλληλων μέτρων κυβερνοασφάλειας. Σε περιπτώσεις αποτυχίας εφαρμογής των απαιτούμενων μέτρων, τα στελέχη μπορεί να αντιμετωπίσουν πρόστιμα, νομικές διαδικασίες ή ακόμη και προσωρινή απαγόρευση άσκησης διοικητικών καθηκόντων.

Οι αποτυχίες στον τομέα της κυβερνοασφάλειας έχουν επίσης σημαντικές πρακτικές συνέπειες. Οργανισμοί που δεν επενδύουν επαρκώς στην ασφάλεια έχουν υποστεί σοβαρές επιθέσεις ransomware, παραβιάσεις στην εφοδιαστική αλυσίδα και εκτεταμένες διαρροές δεδομένων. Τα περιστατικά αυτά συχνά οδηγούν σε οικονομικές απώλειες, διακοπή λειτουργίας των υπηρεσιών και σημαντική βλάβη στη φήμη του οργανισμού.

Οι απαιτήσεις της NIS2 έχουν σχεδιαστεί ακριβώς για την αποτροπή αυτών των κινδύνων, μέσω της επιβολής αυστηρότερων μέτρων ασφάλειας και μηχανισμών λογοδοσίας. Επομένως, η μη συμμόρφωση δεν συνεπάγεται μόνο κανονιστικές κυρώσεις, αλλά μπορεί επίσης να απειλήσει τη συνέχεια των επιχειρηματικών δραστηριοτήτων, να υπονομεύσει την εμπιστοσύνη των πελατών και να αφήσει τον οργανισμό εκτεθειμένο σε σοβαρές διαταραχές.

3.5.2 Βήματα προετοιμασίας για συμμόρφωση με NIS2

Οι οργανισμοί πρέπει να προετοιμαστούν προληπτικά καθώς η Οδηγία NIS2 τίθεται σε εφαρμογή σε ολόκληρη την Ευρωπαϊκή Ένωση. Η ενότητα αυτή παρουσιάζει τα βασικά βήματα που πρέπει να ακολουθήσει ένας οργανισμός για να προετοιμαστεί για τη συμμόρφωση με την οδηγία.

Κατανόηση της οδηγίας

Όπως συμβαίνει με τα περισσότερα έργα που αφορούν ολόκληρο τον οργανισμό, η διαδικασία πρέπει να ξεκινά με έναν ολοκληρωμένο σχεδιασμό και με αξιολόγηση της υφιστάμενης κατάστασης, προκειμένου να προσδιοριστεί τι υπάρχει ήδη σε εφαρμογή και ποιοι στόχοι πρέπει να επιτευχθούν.

1. Κατανόηση του πεδίου εφαρμογής

Προσδιορισμός εφαρμογής: Καθορισμός του εάν ο οργανισμός ανήκει στην κατηγορία των «ουσιαστικών» ή των «σημαντικών» οντοτήτων.

Καταγραφή κρίσιμων υπηρεσιών: Εντοπισμός όλων των κρίσιμων υπηρεσιών και των ψηφιακών υποδομών που ενδέχεται να επηρεάζονται από την οδηγία.

2. Διενέργεια ανάλυσης κενών (Gap Analysis)

Αξιολόγηση βάσει της NIS2: Σύγκριση των υφιστάμενων πρακτικών κυβερνοασφάλειας με τις απαιτήσεις της οδηγίας.

Εντοπισμός ελλείψεων: Αναγνώριση κενών σε πολιτικές, διαδικασίες και τεχνικά μέτρα που πρέπει να αντιμετωπιστούν.

3. Ανάπτυξη οδικού χάρτη συμμόρφωσης

Ιεράρχηση ενεργειών: Καθορισμός προτεραιοτήτων για τις ενέργειες που απαιτούνται ώστε να καλυφθούν τα εντοπισμένα κενά.

Χρονοδιάγραμμα: Δημιουργία χρονοδιαγράμματος για την επίτευξη της συμμόρφωσης, με συγκεκριμένα ορόσημα και καθορισμένες ομάδες υπευθύνων.

4. Ενίσχυση της διακυβέρνησης κυβερνοασφάλειας

Ανάθεση ευθυνών: Ορισμός ενός Υπεύθυνου Ασφάλειας Πληροφοριών (Chief Information Security Officer – CISO) ή αντίστοιχου ρόλου.

Εποπτεία διοίκησης: Διασφάλιση ότι η ανώτερη διοίκηση συμμετέχει ενεργά στη στρατηγική και τη διακυβέρνηση της κυβερνοασφάλειας.

Τα τμήματα ασφάλειας, πληροφορικής και συμμόρφωσης δεν μπορούν να ανταποκριθούν στις απαιτήσεις της NIS2 από μόνα τους. Απαιτείται συνεργασία σε ολόκληρο τον οργανισμό. Από τα αρχικά στάδια σχεδιασμού έως τη συνεχή αξιολόγηση και συντήρηση των μέτρων, είναι σημαντικό να συμμετέχουν όλα τα εμπλεκόμενα μέρη. Η εφαρμογή των απαιτούμενων μέτρων ασφάλειας προϋποθέτει συνεργασία μεταξύ διαφορετικών ομάδων και τη δέσμευση όλων των επιπέδων του οργανισμού. Η υποστήριξη της διοίκησης είναι κρίσιμη για την υλοποίηση των αλλαγών, καθώς η NIS2 καθιστά τη διοίκηση υπεύθυνη για την κυβερνοασφάλεια. Παράλληλα, τα τμήματα πληροφορικής, ασφάλειας και λειτουργιών πρέπει να συνεργάζονται για την αποτελεσματική εφαρμογή μέτρων προστασίας, αντιγράφων ασφαλείας και κρυπτογράφησης.

5. Εφαρμογή πλαισίου διαχείρισης κυβερνοκινδύνων

Αξιολόγηση κινδύνων: Πραγματοποίηση τακτικών αξιολογήσεων κινδύνου για κρίσιμα περιουσιακά στοιχεία και την εφοδιαστική αλυσίδα.

Μέτρα μετριασμού: Ανάπτυξη και εφαρμογή μέτρων για τη μείωση των κινδύνων βάσει των αποτελεσμάτων των αξιολογήσεων.

6. Βελτίωση δυνατοτήτων αντιμετώπισης περιστατικών

Σχέδιο αντιμετώπισης περιστατικών: Ενημέρωση ή δημιουργία σχεδίου διαχείρισης περιστατικών και κρίσεων.

Μηχανισμοί αναφοράς: Εφαρμογή διαδικασιών για την αναφορά περιστατικών στις αρμόδιες αρχές εντός των προβλεπόμενων χρονικών προθεσμιών.

Η NIS2 απαιτεί την ύπαρξη ολοκληρωμένου σχεδίου διαχείρισης περιστατικών που να διασφαλίζει τη διατήρηση της λειτουργίας του οργανισμού κατά τη διάρκεια και μετά από

ένα περιστατικό. Για τον λόγο αυτό, οι επιχειρήσεις πρέπει να δημιουργήσουν ειδικές ομάδες αντιμετώπισης περιστατικών, με συμμετοχή στελεχών από διαφορετικές επιχειρησιακές μονάδες.

Ανίχνευση απειλών: Η έγκαιρη ανίχνευση περιστατικών, όπως επιθέσεις ransomware που μπορεί να παραβιάζουν συστήματα για μεγάλο χρονικό διάστημα πριν εντοπιστούν, είναι κρίσιμη. Οι οργανισμοί πρέπει να επενδύσουν σε τεχνολογίες ανίχνευσης απειλών, παρακολούθησης, ειδοποιήσεων και ανίχνευσης κακόβουλου λογισμικού.

Στρατηγική αντιγράφων ασφαλείας: Είναι απαραίτητη η ύπαρξη ενημερωμένων αντιγράφων ασφαλείας για κρίσιμα δεδομένα. Συνιστάται η εφαρμογή του κανόνα αντιγράφων ασφαλείας 3-2-1-1-0, σύμφωνα με τον οποίο πρέπει να υπάρχουν τρία αντίγραφα δεδομένων σε δύο διαφορετικά μέσα αποθήκευσης, με ένα αντίγραφο εκτός εγκαταστάσεων και ένα απομονωμένο ή μη τροποποιήσιμο, με στόχο μηδενικά σφάλματα στη διαδικασία επαλήθευσης αντιγράφων ασφαλείας και αποκατάστασης.

Αντίδραση και αποκατάσταση: Πρέπει να αναπτυχθούν διαδικασίες επικοινωνίας και αναφοράς κατά τη διάρκεια ενός περιστατικού. Επιπλέον, πρέπει να υπάρχουν διαδικασίες ανάκαμψης από καταστροφή (disaster recovery) ώστε να διασφαλίζεται η επιχειρησιακή συνέχεια.

Στρατηγικός σχεδιασμός περιβάλλοντος ανάκαμψης: Συχνά δεν είναι δυνατόν να πραγματοποιηθεί αποκατάσταση στο ίδιο περιβάλλον όπου συνέβη το περιστατικό. Για τον λόγο αυτό, είναι σημαντικό να υπάρχει εκ των προτέρων σχεδιασμός για ένα ξεχωριστό και ασφαλές περιβάλλον αποκατάστασης.

7. Ενίσχυση της ασφάλειας της εφοδιαστικής αλυσίδας

Διαχείριση κινδύνων προμηθευτών: Αξιολόγηση και συνεχής παρακολούθηση των πρακτικών κυβερνοασφάλειας προμηθευτών και συνεργατών.

Συμβατικές ρήτρες: Ενσωμάτωση απαιτήσεων κυβερνοασφάλειας στις συμβάσεις με προμηθευτές.

8. Βελτίωση της παρακολούθησης και των δοκιμών ασφάλειας

Συνεχής παρακολούθηση: Εφαρμογή εργαλείων παρακολούθησης δικτύων και συστημάτων.

Δοκιμές ασφάλειας: Πραγματοποίηση τακτικών δοκιμών διείσδυσης, αξιολογήσεων ευπαθειών και προσομοιώσεων επιθέσεων phishing.

9. Ενίσχυση της εκπαίδευσης και ευαισθητοποίησης εργαζομένων

Προγράμματα εκπαίδευσης: Παροχή τακτικής εκπαίδευσης κυβερνοασφάλειας στους εργαζομένους, προσαρμοσμένης στα καθήκοντά τους.

Προσομοιώσεις: Διοργάνωση εκστρατειών ευαισθητοποίησης και προσομοιώσεων επιθέσεων phishing.

Η εκπαίδευση αποτελεί μια συνεχή διαδικασία που διατηρεί την ευαισθητοποίηση των εργαζομένων, εξελίσσεται με την πάροδο του χρόνου και ενσωματώνει αποτελεσματικά νέους εργαζομένους.

10. Προετοιμασία για ελέγχους και τεκμηρίωση

Τήρηση αρχείων: Τεκμηρίωση όλων των μέτρων κυβερνοασφάλειας, των αναφορών περιστατικών και των αξιολογήσεων κινδύνων.

Ετοιμότητα για ελέγχους: Πραγματοποίηση εσωτερικών ελέγχων για τη διασφάλιση της συμμόρφωσης και τον εντοπισμό σημείων βελτίωσης.

11. Συμμετοχή σε δίκτυα ανταλλαγής πληροφοριών

Δίκτυα ανταλλαγής πληροφοριών: Συμμετοχή σε σχετικά δίκτυα ανταλλαγής πληροφοριών του κλάδου.

Συνεργασία με CSIRTs: Ανάπτυξη συνεργασίας με ομάδες αντιμετώπισης περιστατικών ασφάλειας υπολογιστών (CSIRTs) για συντονισμένη αντιμετώπιση περιστατικών.

12. Παρακολούθηση τομεακών κατευθυντήριων οδηγιών

Εθνικές οδηγίες: Παρακολούθηση οδηγιών και βέλτιστων πρακτικών που εκδίδονται από τις αρμόδιες εθνικές αρχές.

Πρότυπα κλάδου: Εφαρμογή πρόσθετων μέτρων που σχετίζονται με τον συγκεκριμένο τομέα δραστηριότητας του οργανισμού.

Συμπέρασμα:

Εκ κατακλείδι μπορούμε να συμπεράνουμε πως η συμμόρφωση με τη οδηγία NIS2 αποτελεί μια σημαντικότατη και πολύ απαιτητική διαδικασία ωστόσο απολύτως απαραίτητη .

4. Το Πλαίσιο SOC 2

4.1 Προέλευση και σκοπός του SOC 2

Το **SOC 2 (Service Organization Control 2)** είναι ένας όρος που χρησιμοποιείται για να περιγράψει τρία βασικά στοιχεία: μια αναφορά (report) που παρέχεται σε τρίτους για την απόδειξη ενός ισχυρού περιβάλλοντος ελέγχων, έναν έλεγχο (audit) που πραγματοποιείται από ανεξάρτητο ελεγκτή (CPA) για την έκδοση αυτής της αναφοράς, καθώς και το σύνολο των ελέγχων και του πλαισίου που απαιτούνται ώστε ένας οργανισμός να αποκτήσει τη σχετική πιστοποίηση.

Πιο συγκεκριμένα, το SOC 2 αποτελεί μια «αναφορά σχετικά με τους ελέγχους σε έναν οργανισμό υπηρεσιών που σχετίζονται με την ασφάλεια, τη διαθεσιμότητα, την ακεραιότητα επεξεργασίας, την εμπιστευτικότητα και την ιδιωτικότητα», σύμφωνα με το AICPA. Το πλαίσιο SOC 2 έχει αναπτυχθεί από το American Institute of Certified Public Accountants (AICPA) και αποτελεί μια εθελοντική διαδικασία πιστοποίησης κυβερνοασφάλειας, η οποία χρησιμοποιείται κυρίως από οργανισμούς που παρέχουν υπηρεσίες και συνεργάζονται με πελάτες και εταίρους, κυρίως στις Ηνωμένες Πολιτείες.

Για να αποκτήσει ένας οργανισμός μια αναφορά SOC 2, πρέπει να περάσει από έλεγχο τρίτου μέρους, κατά τον οποίο αξιολογούνται τα συστήματα και οι εσωτερικοί έλεγχοι του. Ο οργανισμός οφείλει να παρέχει αποδεικτικά στοιχεία και τεκμηρίωση, ώστε να αποδείξει ότι οι εσωτερικοί έλεγχοι εφαρμόζονται σωστά και ανταποκρίνονται στις δηλώσεις της διοίκησης. Με απλά λόγια, οι εξωτερικοί ελεγκτές επιβεβαιώνουν ότι ο οργανισμός εφαρμόζει στην πράξη τα μέτρα ασφάλειας που ισχυρίζεται.

Για την προετοιμασία ενός ελέγχου SOC 2, ένας οργανισμός πρέπει να υλοποιήσει κατάλληλες πολιτικές, διαδικασίες και μηχανισμούς ελέγχου που να πληρούν τα κριτήρια του πλαισίου. Παρόλο που το AICPA δεν διενεργεί τους ίδιους τους ελέγχους, παρέχει κατευθυντήριες γραμμές στα μέλη του σχετικά με τα κριτήρια συμμόρφωσης. Κατά τη φάση υλοποίησης, ο οργανισμός μπορεί να χρειαστεί να αναπτύξει μηχανισμούς ελέγχου πρόσβασης, μέτρα προστασίας δεδομένων και να πραγματοποιήσει εσωτερικούς ελέγχους ή αξιολόγηση ετοιμότητας πριν τον εξωτερικό έλεγχο.

Τα οφέλη από την απόκτηση μιας επιτυχούς (χωρίς επιφυλάξεις) αναφοράς SOC 2 περιλαμβάνουν:

- Απλοποίηση διαδικασιών ελέγχου (due diligence), καθώς οι πελάτες και συνεργάτες προτιμούν την αξιολόγηση μέσω SOC 2 αντί για εκτενή ερωτηματολόγια ασφάλειας

- Ενίσχυση της αξιοπιστίας προς υποψήφιους πελάτες και ευθυγράμμιση με τα πρότυπά τους, γεγονός που μπορεί να αυξήσει τις πωλήσεις
- Βελτίωση της εμπιστοσύνης μεταξύ πελατών, συνεργατών και λοιπών ενδιαφερόμενων μερών
- Απόδειξη ισχυρού σχεδιασμού και αποτελεσματικής λειτουργίας των εσωτερικών ελέγχων

Το πρότυπο ISO 27001, το οποίο παρουσιάζει σημαντικές ομοιότητες με το SOC 2, είναι ιδιαίτερα διαδεδομένο σε διεθνές επίπεδο και έχει αναπτυχθεί από τον International Organization for Standardization (ISO) για παρόμοιο σκοπό. Ωστόσο, ενώ το ISO 27001 ακολουθεί μια «top-down» προσέγγιση στην εφαρμογή του, το SOC 2 βασίζεται σε μια προσέγγιση ελέγχων (control-based), εστιασμένη στα κριτήρια των Trust Services Criteria (TSC).[8]

4.2 Trust Services Criteria

Το SOC 2 βασίζεται σε πέντε βασικά κριτήρια, γνωστά ως Trust Services Criteria (TSC): Ασφάλεια (Security), Διαθεσιμότητα (Availability), Ακεραιότητα Επεξεργασίας (Processing Integrity), Εμπιστευτικότητα (Confidentiality) και Ιδιωτικότητα (Privacy).

Κάθε αναφορά SOC 2 περιλαμβάνει υποχρεωτικά το κριτήριο της Ασφάλειας (Security) ως βασική γραμμή (baseline). Οι οργανισμοί μπορούν να επιλέξουν να συμπεριλάβουν επιπλέον ένα ή περισσότερα από τα υπόλοιπα τέσσερα κριτήρια, ανάλογα με τη φύση της δραστηριότητάς τους, τους στόχους τους, το είδος των δεδομένων που διαχειρίζονται ή τις απαιτήσεις πελατών και συνεργατών.

Ακολουθεί ανάλυση των πέντε κριτηρίων:

4.2.1 Ασφάλεια (Security – Common Criteria)

Τα πληροφοριακά συστήματα και τα δεδομένα προστατεύονται από μη εξουσιοδοτημένη πρόσβαση, αποκάλυψη ή καταστροφή, ώστε να διασφαλίζεται η διαθεσιμότητα, η ακεραιότητα, η εμπιστευτικότητα και η ιδιωτικότητα.

Η ασφάλεια αποτελεί τη βάση κάθε SOC 2 αναφοράς και περιλαμβάνεται υποχρεωτικά. Ένας οργανισμός μπορεί να αξιολογηθεί μόνο με βάση αυτό το κριτήριο.

Ενδεικτικά μέτρα που περιλαμβάνονται:

- Δομή και οργάνωση του οργανισμού
- Ασφάλεια τερματικών συσκευών (endpoint security)
- Εκπαίδευση χρηστών σε θέματα ασφάλειας
- Διαχείριση firewall και ρυθμίσεων
- Διαχείριση προμηθευτών
- Διαχείριση ταυτότητας, πρόσβασης και αυθεντικοποίησης
- Διαχείριση κινδύνων
- Μέτρα ασφάλειας δεδομένων και data centers (όπου εφαρμόζεται)

4.2.2 Διαθεσιμότητα (Availability)

Τα πληροφοριακά συστήματα και οι υπηρεσίες είναι διαθέσιμα για χρήση, σύμφωνα με τους στόχους του οργανισμού.

Το κριτήριο αυτό επικεντρώνεται σε:

- Σχέδια ανάκαμψης από καταστροφή (disaster recovery)
- Συμφωνίες επιπέδου υπηρεσιών (SLAs)
- Σχεδιασμό χωρητικότητας (capacity planning)

4.2.3 Ακεραιότητα Επεξεργασίας (Processing Integrity)

Η επεξεργασία των δεδομένων είναι πλήρης, έγκυρη, ακριβής, έγκαιρη και εξουσιοδοτημένη.

Εστιάζει κυρίως σε:

- Εισαγωγή και εξαγωγή δεδομένων
- Ποιότητα δεδομένων

- Χρονισμό επεξεργασίας
- Αξιοπιστία αναφορών

4.2.4 Εμπιστευτικότητα (Confidentiality)

Οι πληροφορίες που χαρακτηρίζονται ως εμπιστευτικές προστατεύονται κατάλληλα.

Το κριτήριο αυτό εξετάζει:

- Την προστασία δεδομένων κατά τη μεταφορά και αποθήκευση
- Τη σωστή διαχείριση και καταστροφή δεδομένων
- Δεδομένα όπως στοιχεία πελατών, ευαίσθητες πληροφορίες, πνευματική ιδιοκτησία και συμβάσεις

4.2.5 Ιδιωτικότητα (Privacy)

Τα προσωπικά δεδομένα συλλέγονται, χρησιμοποιούνται, αποθηκεύονται και διαγράφονται σύμφωνα με τους στόχους και τις πολιτικές του οργανισμού.

Το κριτήριο αυτό αφορά άμεσα δεδομένα φυσικών προσώπων, όπως:

- Προσωπικά αναγνωρίσιμες πληροφορίες (PII)
- Ιατρικά δεδομένα (PHI)
- Άλλες ευαίσθητες πληροφορίες

Παρουσιάζει σημαντική επικάλυψη με πλαίσια όπως το HIPAA και άλλες κανονιστικές απαιτήσεις προστασίας προσωπικών δεδομένων. Επιπλέον, απαιτεί την ύπαρξη ελέγχων για τη διαχείριση περιστατικών παραβίασης δεδομένων και τη γνωστοποίησή τους.

Συνολικά, τα Trust Services Criteria αποτελούν τη βάση για την αξιολόγηση της αποτελεσματικότητας των ελέγχων ενός οργανισμού στο πλαίσιο του SOC 2 και συμβάλλουν στη διασφάλιση υψηλού επιπέδου κυβερνοασφάλειας και προστασίας δεδομένων.

Εικόνα 4.1 : *Συμμόρφωση SOC 2*

4.3 SOC 2 Type I vs SOC 2 Type II

Υπάρχουν δύο βασικοί τύποι αναφορών SOC 2, οι οποίοι διαφέρουν ως προς το εύρος και το βάθος της αξιολόγησης:

4.3.1 SOC 2 Type 1

Η αναφορά SOC 2 Type 1 περιγράφει τους ελέγχους ασφάλειας ενός οργανισμού σε μια συγκεκριμένη χρονική στιγμή, δηλαδή κατά την ημερομηνία του ελέγχου.

Ο συγκεκριμένος τύπος επιβεβαιώνει ότι οι απαραίτητοι έλεγχοι έχουν τεθεί σε εφαρμογή, χωρίς όμως να αξιολογεί την αποτελεσματικότητά τους σε βάθος χρόνου.

Η SOC 2 Type 1:

- Ολοκληρώνεται συνήθως πιο γρήγορα
- Είναι πιο οικονομική σε σχέση με την Type 2

- Έχει μικρότερη αξία για μεγαλύτερους οργανισμούς ή απαιτητικούς πελάτες, καθώς δεν αποδεικνύει τη συνεχή αποτελεσματικότητα των ελέγχων

4.3.2 SOC 2 Type 2

Η αναφορά SOC 2 Type 2 αξιολογεί τους ελέγχους ασφάλειας σε βάθος χρόνου και εξετάζει την αποτελεσματικότητά τους.

Ο οργανισμός επιλέγει τη διάρκεια της περιόδου αξιολόγησης, η οποία συνήθως κυμαίνεται από 3 έως 12 μήνες.

Η SOC 2 Type 2:

- Ελέγχει αν οι έλεγχοι λειτουργούν σωστά σε συνεχή βάση
- Παρέχει πιο ολοκληρωμένη εικόνα της ασφάλειας του οργανισμού
- Προσφέρει μεγαλύτερη εμπιστοσύνη σε πελάτες, συνεργάτες και λοιπούς ενδιαφερόμενους

Συνολικά, ενώ η SOC 2 Type 1 αποτελεί ένα αρχικό βήμα για τη συμμόρφωση, η SOC 2 Type 2 θεωρείται πιο ουσιαστική, καθώς αποδεικνύει την πραγματική και διαχρονική αποτελεσματικότητα των μέτρων ασφάλειας.[9]

Εικόνα 4.2 : *Διαφορές μεταξύ SOC 2 Type I & SOC 2 Type II*

4.4 Διαδικασία ελέγχου και ρόλος των ελεγκτών (AICPA)

4.4.1 Εκτέλεση του Πλαισίου SOC 2

Για την επιτυχή εφαρμογή ενός προγράμματος SOC 2, οι οργανισμοί οφείλουν να υλοποιούν συνεχείς βασικές δραστηριότητες ελέγχου, ώστε να ευθυγραμμίζονται με τα **Trust Services Criteria (TSC)**. Οι απαιτούμενες ενέργειες εξαρτώνται κυρίως από το πεδίο εφαρμογής (scope) του SOC 2 κάθε οργανισμού, καθώς κάθε κατηγορία κριτηρίων καθορίζει συγκεκριμένες απαιτήσεις συμμόρφωσης.

Ακολουθούν βασικές δραστηριότητες ελέγχου που απαιτούνται συνήθως, καθώς και η συχνότητα εφαρμογής τους:

- **Καθιέρωση Προγράμματος Ασφάλειας Πληροφοριών** – Αναθεώρηση/ενημέρωση τουλάχιστον ετησίως
- **Δημιουργία και συντήρηση πολιτικών και διαδικασιών** – Αναθεώρηση τουλάχιστον ετησίως
- **Διατήρηση οργανωτικής δομής** – Αναθεώρηση ετησίως ή σε περίπτωση αλλαγών
- **Αξιολόγηση κινδύνων τρίτων (προμηθευτών)** – Σύμφωνα με πολιτικές, τουλάχιστον ετησίως
- **Αξιολόγηση κινδύνων για το περιβάλλον εφαρμογής** – Τουλάχιστον ετησίως
- **Μετριασμός εντοπισμένων κινδύνων** – Τεκμηριωμένα σχέδια και εφαρμογή τους
- **Πρόγραμμα αξιολόγησης συμμόρφωσης** – Τουλάχιστον ετησίως
- **Τεκμηρίωση και ενημέρωση ελέγχων** – Τουλάχιστον ετησίως
- **Εκπαίδευση ευαισθητοποίησης ασφάλειας** – Τουλάχιστον ετησίως
- **Πρόγραμμα διαχείρισης πρόσβασης** – Σύμφωνα με πολιτικές, τουλάχιστον ετησίως
- **Καταγραφή περιουσιακών στοιχείων πληροφορίας** – Τουλάχιστον ετησίως
- **Κατηγοριοποίηση δεδομένων** – Τουλάχιστον ετησίως
- **Πρότυπα ρυθμίσεων συστημάτων** – Τουλάχιστον ετησίως
- **Έλεγχοι ευπαθειών και δοκιμές διείσδυσης** – Τουλάχιστον ετησίως
- **Σχέδιο απόκρισης σε περιστατικά** – Ετήσια δοκιμή και επικαιροποίηση

- **Καταγραφή και παρακολούθηση συστημάτων** – Σύμφωνα με πολιτικές
- **Διαχείριση αλλαγών** – Τεκμηρίωση όλων των αλλαγών

Σημαντικό είναι ότι το SOC 2 απαιτεί πλήρη τεκμηρίωση όλων των δραστηριοτήτων ελέγχου, καθώς και αποδείξεις ότι αυτές λειτουργούν αποτελεσματικά σε βάθος χρόνου (ιδίως για SOC 2 Type II). Κατά τον εξωτερικό έλεγχο απαιτείται η παροχή σχετικών αποδεικτικών στοιχείων.

4.4.2 Διαδικασία Ελέγχου και Αξιολόγησης (Audit Process)

Εσωτερικές αξιολογήσεις (Internal / Self-Assessments)

Κάθε οργανισμός μπορεί να αξιολογήσει εσωτερικά τη συμμόρφωσή του με τα κριτήρια SOC 2. Συνιστάται:

- Ετήσια αξιολόγηση όλων των ελέγχων
- Εστίαση σε ελέγχους υψηλού κινδύνου ή με συχνότερη εφαρμογή (π.χ. μηνιαία/τριμηνιαία)
- Χρήση των Trust Services Criteria ως βάση αξιολόγησης

Εξωτερικοί έλεγχοι (External Audits)

Σύμφωνα με το AICPA, μόνο πιστοποιημένοι ελεγκτικοί οργανισμοί (CPA) μπορούν να διενεργούν SOC 2 audits και να εκδίδουν σχετικές αναφορές.

Υπάρχουν δύο τύποι:

- **Type I:** Αξιολόγηση σχεδιασμού ελέγχων σε συγκεκριμένη χρονική στιγμή
- **Type II:** Αξιολόγηση σχεδιασμού και αποτελεσματικότητας ελέγχων σε βάθος χρόνου

Χρήση τρίτων (Sub-service organizations)

Οργανισμοί που χρησιμοποιούν τρίτους παρόχους μπορούν να εφαρμόσουν τη μέθοδο "carve-out", δηλαδή να βασιστούν στους ελέγχους των τρίτων για τη συμμόρφωση. Οι εξαιρέσεις αυτές πρέπει να αναφέρονται ρητά στην τελική αναφορά.

Επιπλέον, οργανισμοί χωρίς εσωτερική ομάδα ασφάλειας μπορούν να συνεργαστούν με εξωτερικούς συμβούλους για προετοιμασία ή εσωτερικούς ελέγχους. Οι εξωτερικοί έλεγχοι SOC 2 συνεπάγονται σχετικό κόστος.

Διατήρηση συνεχούς συμμόρφωσης SOC 2

Η διατήρηση της συμμόρφωσης ακολουθεί παρόμοιες αρχές με άλλα πλαίσια κυβερνοασφάλειας, με ιδιαίτερη έμφαση στα SOC 2 Type II reports.

Για την αποφυγή αποκλίσεων:

- Οι οργανισμοί πρέπει να παρέχουν αποδείξεις ότι οι έλεγχοι λειτουργούσαν αποτελεσματικά καθ' όλη τη διάρκεια της περιόδου αξιολόγησης
- Οι έλεγχοι πρέπει να εκτελούνται σύμφωνα με τις καθορισμένες πολιτικές και διαδικασίες
- Πρέπει να συλλέγονται αποδεικτικά στοιχεία με τη σωστή συχνότητα (π.χ. τριμηνιαίες αξιολογήσεις πρόσβασης)

Οποιαδήποτε απόκλιση καταγράφεται από τον ελεγκτή, μαζί με:

- Τη συχνότητα εμφάνισης
- Τον αντίκτυπο
- Τις ενέργειες αποκατάστασης

Συνολικά, η επιτυχής εφαρμογή και διατήρηση του SOC 2 απαιτεί συνεχή παρακολούθηση, τεκμηρίωση και βελτίωση των διαδικασιών ασφάλειας, με στόχο την απόδειξη της αποτελεσματικότητας των ελέγχων σε βάθος χρόνου.

4.4.3 Ροή Συμμόρφωσης με το Πλαίσιο SOC 2

Η συμμόρφωση με το SOC 2 δεν χρειάζεται να είναι ιδιαίτερα περίπλοκη. Η διαδικασία μπορεί να οργανωθεί σε διακριτά στάδια που καλύπτουν την αρχική προετοιμασία, τον εξωτερικό έλεγχο και τη διατήρηση της συμμόρφωσης.

Αρχική Προετοιμασία / Ετοιμότητα για Έλεγχο

1. **Καθορισμός πεδίου εφαρμογής (Scope Framework)**
   Επιλογή των κατηγοριών (Trust Services Criteria) που θα συμπεριληφθούν και καθορισμός των σχετικών απαιτήσεων.
2. **Εντοπισμός και τεκμηρίωση ελέγχων**
   Καταγραφή των υφιστάμενων ελέγχων και εντοπισμός κενών όπου δεν υπάρχουν επαρκή μέτρα.
3. **Εφαρμογή ελέγχων για την κάλυψη κενών**
   Υλοποίηση νέων ελέγχων για τις απαιτήσεις που δεν καλύπτονται από το υπάρχον σύστημα.
4. **Εκτέλεση πλαισίου (Framework Execution)**
   Διασφάλιση ότι οι βασικές δραστηριότητες ελέγχου εφαρμόζονται πριν από τη φάση των δοκιμών.
5. **Συλλογή αποδεικτικών στοιχείων για εσωτερικό έλεγχο**
   Συγκέντρωση στοιχείων που αποδεικνύουν ότι οι έλεγχοι εφαρμόζονται στην πράξη.
6. **Εσωτερική αξιολόγηση (Self-Assessment)**
   Καθορισμός σχεδίων ελέγχου, εκτέλεση δοκιμών και εντοπισμός αδυναμιών στη λειτουργία των ελέγχων.
7. **Διαχείριση και αποκατάσταση προβλημάτων**
   Διόρθωση των αδυναμιών και επανέλεγχος μέχρι την επιτυχή λειτουργία των ελέγχων.

Διαδικασία Εξωτερικού Ελέγχου

1. **Λήψη αιτημάτων αποδεικτικών στοιχείων**
   Παραλαβή λίστας απαιτούμενων στοιχείων από τον ελεγκτή και ανάθεσή τους στους υπεύθυνους.

2. **Έλεγχος και υποβολή στοιχείων**
   Επαλήθευση της ορθότητας και υποβολή των αποδεικτικών στοιχείων στον ελεγκτή.

3. **Δοκιμές και αξιολόγηση από τον ελεγκτή**
   Διενέργεια ελέγχων και διαδικασιών επιβεβαίωσης (walkthroughs).

4. **Σύνταξη αναφοράς**
   Προετοιμασία της έκθεσης ελέγχου και διαδικασία ποιοτικού ελέγχου, με συμμετοχή και του οργανισμού.

5. **Έκδοση τελικής αναφοράς**
   Παράδοση της τελικής έκθεσης SOC 2.

Διατήρηση Συνεχούς Συμμόρφωσης

1. **Καθορισμός προγράμματος εσωτερικών ελέγχων**
   Προσδιορισμός των επαναλαμβανόμενων ελέγχων και δημιουργία κύκλου αξιολόγησης.

2. **Συλλογή αποδεικτικών στοιχείων**
   Συνεχής συγκέντρωση στοιχείων που αποδεικνύουν την εφαρμογή των ελέγχων.

3. **Εσωτερικές αξιολογήσεις**
   Εκτέλεση ελέγχων και εντοπισμός πιθανών αδυναμιών.

4. **Αποκατάσταση προβλημάτων**
   Διόρθωση των προβλημάτων που εντοπίζονται.

5. **Επαναληπτικοί έλεγχοι (Retesting Cycle)**
   Επανέλεγχος μετά τη διόρθωση, έως ότου όλα τα ζητήματα επιλυθούν πλήρως.

Συνολικά, η συμμόρφωση με το SOC 2 αποτελεί μια συνεχόμενη διαδικασία που απαιτεί συστηματική εφαρμογή ελέγχων, τεκμηρίωση και συνεχή βελτίωση, με στόχο τη διασφάλιση της αποτελεσματικότητας των μέτρων ασφάλειας σε βάθος χρόνου.

5. Αναλυτική Σύγκριση: NIS2 vs SOC 2

5.1 Σκοπός & Πεδίο Εφαρμογής

5.1.1 Κανονιστικό vs Εθελοντικό πλαίσιο

Η NIS2 δεν αποτελεί απλή σύσταση — είναι ευρωπαϊκή νομοθεσία. Αντίθετα, το SOC 2 είναι ένα πλαίσιο που βασίζεται στις απαιτήσεις της αγοράς και δεν έχει άμεση νομική ισχύ.

Νομική υπόσταση:

- **NIS2:** Δεσμευτική νομοθεσία της ΕΕ (Οδηγία 2022/2555), υποχρεωτική για τους οργανισμούς που εμπίπτουν στο πεδίο εφαρμογής.
- **SOC 2:** Εθελοντικό πλαίσιο διασφάλισης από το AICPA· δεν είναι νομικά υποχρεωτικό, αλλά απαιτείται ευρέως από την αγορά.

5.1.2 Γεωγραφικό και κλαδικό πεδίο

Η NIS2 έχει ευρωπαϊκή βάση, αλλά μπορεί να επηρεάζει και οργανισμούς εκτός ΕΕ που παρέχουν κρίσιμες υπηρεσίες εντός αυτής. Το SOC 2, αν και προέρχεται από τις ΗΠΑ, έχει εξελιχθεί σε παγκόσμιο πρότυπο, κυρίως για B2B υπηρεσίες.

Γεωγραφία:

- **NIS2:** Εφαρμόζεται σε περίπου 30 χώρες του ΕΟΧ(Ευρωπαϊκός Οικονομικός Χώρος) και επεκτείνεται και σε μη ευρωπαϊκούς παρόχους που εξυπηρετούν κρίσιμους τομείς.
- **SOC 2:** Προέλευση από ΗΠΑ, αλλά χρησιμοποιείται διεθνώς, κυρίως σε cloud, SaaS και fintech.

5.2 Βασικές Αρχές και Απαιτήσεις

5.2.1 Διαχείριση κινδύνου vs πιστοποίηση ελέγχων

Η NIS2 ορίζει σαφώς ποιες οντότητες θεωρούνται «ουσιώδεις» και «σημαντικές» σε κρίσιμους τομείς (ενέργεια, υγεία, υποδομές). Το SOC 2, αντίθετα, λειτουργεί ως «σήμα εμπιστοσύνης» για επιχειρήσεις που θέλουν να αποδείξουν την ασφάλεια των δεδομένων τους.

- **NIS2:** Αφορά οργανισμούς σε 18 τομείς με ≥50 εργαζόμενους ή ≥10 εκατ. € κύκλο εργασιών.
- **SOC 2:** Αφορά οποιονδήποτε οργανισμό υπηρεσιών που επιθυμεί πιστοποίηση (κυρίως SaaS, data centers, MSPs).

Για πολυεθνικές εταιρείες, αυτή η διαφοροποίηση δημιουργεί συχνά σύγκρουση μεταξύ νομικών υποχρεώσεων και εμπορικών απαιτήσεων.

5.3 Διαδικασία Συμμόρφωσης

5.3.1 Έλεγχοι και αποδεικτικά στοιχεία

Τα δύο πλαίσια διαφέρουν σημαντικά στον τρόπο που προσεγγίζουν τους ελέγχους:

Εστίαση:

- **NIS2:** Διαχείριση κυβερνοκινδύνων, απόκριση σε περιστατικά, διακυβέρνηση και ασφάλεια εφοδιαστικής αλυσίδας (Άρθρο 21).
- **SOC 2:** Κριτήρια Trust Services — ασφάλεια, διαθεσιμότητα, ακεραιότητα επεξεργασίας, εμπιστευτικότητα, ιδιωτικότητα.

Απόδειξη συμμόρφωσης:

- **NIS2:** Έλεγχοι, επιθεωρήσεις και υποχρεωτική αναφορά περιστατικών εντός 24 ωρών στις αρχές.
- **SOC 2:** Αναφορές από ανεξάρτητους ελεγκτές (CPA):
    - Type I (σχεδιασμός ελέγχων)

- Type II (σχεδιασμός + αποτελεσματικότητα σε βάθος χρόνου)

Η βασική διαφορά είναι νοοτροπίας:

- Η NIS2 απαιτεί άμεση συμμόρφωση προς τις ρυθμιστικές αρχές.
- Το SOC 2 επικεντρώνεται στη διατήρηση εμπιστοσύνης στην αγορά.

Χρονοδιαγράμματα

Τα χρονικά πλαίσια διαφέρουν σημαντικά:

- **NIS2:**
  - Υιοθέτηση: 16 Ιανουαρίου 2023
  - Ενσωμάτωση από κράτη μέλη: έως 17 Οκτωβρίου 2024
- **SOC 2:**
  - Type I: μία φορά
  - Type II: συνήθως ετήσια επανάληψη για διατήρηση ισχύος

Οι οργανισμοί που εφαρμόζουν και τα δύο καλούνται να ισορροπήσουν μεταξύ νομικών προθεσμιών και απαιτήσεων της αγοράς.

5.4 Επιβολή & Κυρώσεις

Οι διαφορές εδώ είναι ιδιαίτερα έντονες:

- **NIS2:**
  - Πρόστιμα έως 10 εκατ. € ή 2% του παγκόσμιου κύκλου εργασιών
  - Πιθανή προσωπική ευθύνη διοίκησης
- **SOC 2:**
  - Δεν υπάρχουν νομικά πρόστιμα
  - Πιθανές εμπορικές συνέπειες:
    - απώλεια πελατών ή συμβολαίων

- ζημιά στη φήμη
- αυξημένο κόστος ασφάλισης

Συνοπτικά

Η NIS2 είναι ένα υποχρεωτικό κανονιστικό πλαίσιο με νομικές συνέπειες, ενώ το SOC 2 αποτελεί ένα εθελοντικό αλλά εμπορικά κρίσιμο πρότυπο εμπιστοσύνης.

Για τους οργανισμούς, η ιδανική προσέγγιση είναι ένας συνδυασμός και των δύο, μέσω μιας ενοποιημένης στρατηγικής συμμόρφωσης που καλύπτει τόσο τις νομικές απαιτήσεις όσο και τις ανάγκες της αγοράς.[10]

6 Εργαλεία Υλοποίησης και Υποστήριξης Συμμόρφωσης

6.1 Κατηγορίες εργαλείων κυβερνοασφάλειας

Τα εργαλεία κυβερνοασφάλειας που επιλέγει ένας οργανισμός διαφέρουν ανάλογα με τον σχεδιασμό και τη δομή του δικτύου του. Ωστόσο, ανεξάρτητα από τον τρόπο με τον οποίο έχει διαμορφωθεί η ψηφιακή υποδομή μιας επιχείρησης, υπάρχουν πολλές διαθέσιμες λύσεις για την προστασία της. Το πρώτο βήμα είναι ο εντοπισμός των πιο σημαντικών ψηφιακών πόρων, καθώς και των σημείων στα οποία το δίκτυο εμφανίζει τις μεγαλύτερες ευπάθειες.

Για πολλές σύγχρονες επιχειρήσεις, οι σημαντικότερες αδυναμίες εντοπίζονται κυρίως στα τερματικά σημεία (endpoints) που συνδέονται στο δίκτυο και όχι στα εσωτερικά του στοιχεία. Η ανάλυση του ποιοι και ποιες συσκευές συνδέονται στο δίκτυο, καθώς και του τρόπου με τον οποίο διακινούνται τα δεδομένα, διευκολύνει τη βελτιστοποίηση της προστασίας. Ακολουθούν ορισμένα βασικά εργαλεία που μπορούν να χρησιμοποιηθούν για την προστασία μιας επιχείρησης από επιθέσεις ransomware, phishing, κακόβουλους χρήστες και άλλες κυβερνοαπειλές.

Endpoint Detection and Response (EDR)

Οι λύσεις Endpoint Detection and Response (EDR) επιτρέπουν τον εύκολο εντοπισμό των συσκευών που συνδέονται στο δίκτυο και την άμεση απόκριση σε απειλές που αναγνωρίζει το σύστημα.

Για παράδειγμα, εάν μια συσκευή συνδεθεί στο δίκτυο με κακόβουλη πρόθεση, το σύστημα EDR μπορεί να παρέχει αναλυτικές πληροφορίες σχετικά με τη συσκευή, καθώς και δεδομένα για τη δραστηριότητά της όσο παραμένει συνδεδεμένη. Εκτός από την αποτροπή μη εξουσιοδοτημένων χρηστών και συσκευών, τα εργαλεία EDR αποτελούν σημαντικό μέσο συλλογής ψηφιακών αποδεικτικών στοιχείων μετά από παραβίαση δεδομένων. Μέσω της ανάλυσης των αρχείων καταγραφής (logs), είναι δυνατός ο εντοπισμός του υπεύθυνου χρήστη ή συσκευής.

Λογισμικό Antivirus

Παρόλο που τα λογισμικά antivirus σχεδιάστηκαν αρχικά για την αντιμετώπιση ιών υπολογιστών, οι σύγχρονες λύσεις παρέχουν προστασία και απέναντι σε πολλές άλλες μορφές απειλών. Ένα ισχυρό πρόγραμμα antivirus μπορεί να εντοπίσει ποικίλες επιθέσεις κακόβουλου λογισμικού, ελέγχοντας το σύστημα για γνωστά μοτίβα επιθέσεων.

Τα λογισμικά antivirus βασίζονται σε υπάρχοντα προφίλ επιθέσεων που έχουν καταγραφεί σε προηγούμενα περιστατικά. Με αυτόν τον τρόπο εντοπίζουν κακόβουλα προγράμματα, ενημερώνουν τον χρήστη και απομακρύνουν τα επικίνδυνα στοιχεία από το σύστημα. Συνεπώς, η χρήση κατάλληλου antivirus συμβάλλει ουσιαστικά στην προστασία από σοβαρές κυβερνοαπειλές.

Next-Generation Firewalls (NGFW)

Τα firewalls επόμενης γενιάς (NGFW) παρέχουν εκτεταμένη προστασία έναντι πολλών διαφορετικών απειλών, ενώ ταυτόχρονα διευκολύνουν την ασφαλή πρόσβαση εξωτερικών χρηστών στο δίκτυο. Η λειτουργία τους βασίζεται στον έλεγχο των πακέτων δεδομένων που αποστέλλονται προς και από το δίκτυο. Όταν εντοπιστεί γνωστή απειλή, το NGFW απορρίπτει αυτόματα το ύποπτο πακέτο.

Επιπλέον, τα σύγχρονα NGFW αξιοποιούν τεχνικές μηχανικής μάθησης (machine learning) για τον εντοπισμό κακόβουλης συμπεριφοράς. Έτσι, μπορούν να αντιμετωπίσουν ακόμη και επιθέσεις μηδενικής ημέρας (zero-day attacks), αναγνωρίζοντας ύποπτο κώδικα χωρίς να απαιτείται προηγούμενη γνώση της απειλής.

Παράλληλα, ένα NGFW μπορεί να χρησιμοποιηθεί και για τη δημιουργία εικονικού ιδιωτικού δικτύου (VPN).

Προστασία Domain Name System (DNS)

Η προστασία DNS προσθέτει ένα επιπλέον επίπεδο ασφάλειας, αποτρέποντας την πρόσβαση των χρηστών σε επικίνδυνες ιστοσελίδες. Τα συστήματα αυτά μπορούν επίσης να φιλτράρουν περιεχόμενο που θεωρείται ανεπιθύμητο ή επικίνδυνο για το εταιρικό δίκτυο.

Για παράδειγμα, εάν ένας εργαζόμενος επιχειρήσει να επισκεφθεί ιστοσελίδα με γνωστές απειλές μέσω του εταιρικού δικτύου, το σύστημα DNS protection μπορεί να αποκλείσει την πρόσβαση σε αυτήν.

Email Gateway Security

Τα συστήματα ασφάλειας ηλεκτρονικού ταχυδρομείου (email gateway security) αποτρέπουν την εισχώρηση ανεπιθύμητων ή επικίνδυνων μηνυμάτων στους λογαριασμούς των χρηστών. Σε αυτά περιλαμβάνονται τόσο τα μηνύματα spam όσο και emails που περιέχουν κακόβουλο λογισμικό.

Για παράδειγμα, σε επιχειρήσεις με απομακρυσμένα υποκαταστήματα που συνδέονται μέσω δικτύου SD-WAN, το email gateway security διασφαλίζει ότι όλοι οι χρήστες προστατεύονται από επικίνδυνα ή ανεπιθύμητα μηνύματα, ανεξάρτητα από τη γεωγραφική τους θέση.

Intrusion Detection and Prevention Systems (IDS/IPS)

Τα συστήματα ανίχνευσης και πρόληψης εισβολών (IDS/IPS) λειτουργούν εξετάζοντας το περιεχόμενο των πακέτων δεδομένων που επιχειρούν να εισέλθουν στο δίκτυο. Σε αντίθεση με τα παραδοσιακά firewalls, τα οποία ελέγχουν κυρίως τις επικεφαλίδες των πακέτων, τα IDS/IPS αναλύουν σε μεγαλύτερο βάθος το περιεχόμενο της επικοινωνίας.

Με τη χρήση ενός ολοκληρωμένου συστήματος πληροφοριών απειλών (threat intelligence platform), τα IDS/IPS μπορούν να εντοπίσουν και να αποκλείσουν μεγάλο εύρος κακόβουλων επιθέσεων.

Logging και Παρακολούθηση Καταγραφών

Η καταγραφή συμβάντων (logging) και η συνεχής παρακολούθηση της δραστηριότητας του δικτύου συμβάλλουν τόσο στην πρόληψη όσο και στη διερεύνηση περιστατικών ασφαλείας. Τα αρχεία καταγραφής παρέχουν λεπτομερείς πληροφορίες με χρονοσήμανση, διευκολύνοντας τη συσχέτιση επιθέσεων με συγκεκριμένες συσκευές ή χρήστες.

Endpoint Protection

Η προστασία τερματικών συσκευών (endpoint protection) επικεντρώνεται στη διασφάλιση ότι οι φορητοί υπολογιστές, οι σταθεροί υπολογιστές και οι κινητές συσκευές που συνδέονται στο δίκτυο παραμένουν ασφαλείς. Η ανάγκη αυτή είναι ιδιαίτερα σημαντική σε περιβάλλοντα απομακρυσμένης εργασίας.

Μέσω των εργαλείων endpoint protection ενισχύεται η ασφάλεια κάθε συσκευής που συνδέεται στο δίκτυο, επεκτείνοντας ουσιαστικά τα όρια της εσωτερικής άμυνας του οργανισμού.

Υπηρεσίες Αυθεντικοποίησης / VPN

Οι υπηρεσίες αυθεντικοποίησης επιτρέπουν την αποτροπή μη εξουσιοδοτημένων χρηστών από την πρόσβαση στο δίκτυο, εφαρμόζοντας πολιτικές διαχείρισης προνομιακής πρόσβασης

Η χρήση VPN προσφέρει επιπλέον προστασία, καθώς απαιτεί από τους χρήστες την εισαγωγή διαπιστευτηρίων πρόσβασης και ταυτόχρονα κρυπτογραφεί τα δεδομένα που ανταλλάσσονται μεταξύ των συσκευών και του δικτύου.

Cloud-Based Security

Η ασφάλεια υποδομών cloud αναφέρεται στις τεχνολογίες και πολιτικές που χρησιμοποιούνται για την προστασία πόρων που φιλοξενούνται στο υπολογιστικό νέφος από κυβερνοεπιθέσεις. Οι λύσεις αυτές προστατεύουν:

- δεδομένα,
- εφαρμογές,
- υπηρεσίες,
- υποδομές cloud.

Web Application Firewalls (WAF)

Τα Web Application Firewalls (WAF) προστατεύουν τις διαδικτυακές εφαρμογές από επιθέσεις που αποσκοπούν στην εκμετάλλευση ευπαθειών ή στην κλοπή δεδομένων. Όλη η εισερχόμενη και εξερχόμενη κίνηση φιλτράρεται και, εφόσον εντοπιστεί απειλή, τα σχετικά δεδομένα απορρίπτονται αυτόματα.

Πολλές μικρομεσαίες επιχειρήσεις χρησιμοποιούν WAF για προστασία από επιθέσεις DDoS και άλλες διαδικτυακές απειλές.

Software-Defined Wide Area Network (SD-WAN)

Τα δίκτυα SD-WAN επιτρέπουν τον λεπτομερή έλεγχο και τη βελτιστοποίηση της διαχείρισης της κυκλοφορίας δεδομένων. Μέσω αυτών, η επιχείρηση μπορεί να κατευθύνει διαφορετικούς τύπους δεδομένων σε διαφορετικές διαδρομές, επιτυγχάνοντας καλύτερη απόδοση και αυξημένη ασφάλεια.

Παράλληλα, το SD-WAN συμβάλλει στη μείωση του κόστους χρήσης εύρους ζώνης (bandwidth), αξιοποιώντας αποτελεσματικότερα τις υπάρχουσες δικτυακές υποδομές.

Enterprise Password Management / Privileged Access Management (PAM)

Τα συστήματα διαχείρισης εταιρικών κωδικών πρόσβασης και προνομιακής πρόσβασης (PAM) επιτρέπουν τον έλεγχο των δραστηριοτήτων και των ταυτοτήτων όλων των χρηστών και συσκευών που αλληλεπιδρούν με το δίκτυο.

Μόνο οι χρήστες που διαθέτουν τα κατάλληλα δικαιώματα αποκτούν πρόσβαση στο σύστημα, ενώ σε περίπτωση ύποπτης δραστηριότητας τα δικαιώματα μπορούν να ανακληθούν άμεσα.

Vulnerability and Threat Management

Η διαχείριση ευπαθειών και απειλών περιλαμβάνει τη μείωση της έκθεσης της επιχείρησης σε κινδύνους, καθώς και τη διασφάλιση ότι τα τερματικά συστήματα προστατεύονται επαρκώς.

Η διαδικασία αυτή απαιτεί συνδυασμό τεχνολογιών, πολιτικών και ανθρώπινων πόρων, καθώς και αποτελεσματικούς μηχανισμούς αναφοράς και διαχείρισης προβλημάτων ασφαλείας.

Threat Detection

Η ανίχνευση απειλών περιλαμβάνει την ανάλυση όλων των στοιχείων που συνδέονται στο δίκτυο, καθώς και της ίδιας της δικτυακής δραστηριότητας, με στόχο τον εντοπισμό ύποπτων εφαρμογών, χρηστών ή ενεργειών.

Τα συστήματα threat detection αξιοποιούν δεδομένα που παράγονται από διάφορα συμβάντα του δικτύου για τον εντοπισμό πιθανών κινδύνων. Συχνά χρησιμοποιούν επίσης τεχνολογίες

sandboxing, όπου οι απειλές απομονώνονται σε ελεγχόμενο περιβάλλον ώστε να αναλυθούν με ασφάλεια από τους διαχειριστές συστημάτων.[11]

Εικόνα 6.1 : *Εργαλεία Κυβερνοασφάλειας*

6.2 GRC εργαλεία (Governance, Risk, Compliance)

Η διοίκηση λειτουργιών ενός οργανισμού οφείλει να αξιοποιεί εξειδικευμένα εργαλεία λογισμικού GRC (Governance, Risk, Compliance), προκειμένου να διασφαλίζεται ότι η επιχείρηση συμμορφώνεται με τις απαιτήσεις κανονιστικής συμμόρφωσης και διαχείρισης κινδύνων. Τα εργαλεία αυτά συμβάλλουν επίσης στον εντοπισμό και τον μετριασμό κινδύνων που σχετίζονται με τη χρήση, τη διαχείριση, τη λειτουργία, την επιρροή και την υιοθέτηση τεχνολογιών πληροφορικής εντός του οργανισμού.

Τα εργαλεία GRC καλύπτουν συνήθως τομείς όπως η διαχείριση λειτουργικού κινδύνου, οι πολιτικές και η συμμόρφωση, η διακυβέρνηση πληροφοριακών συστημάτων (IT Governance) και ο εσωτερικός έλεγχος. Τα περισσότερα λογισμικά GRC περιλαμβάνουν τις ακόλουθες δυνατότητες:

- **Διαχείριση περιεχομένου και εγγράφων**, που βοηθά τις επιχειρήσεις στη δημιουργία, παρακολούθηση και αποθήκευση ψηφιοποιημένου περιεχομένου με μεγαλύτερη ακρίβεια.
- **Διαχείριση και ανάλυση δεδομένων κινδύνου**, που επιτρέπει τη μέτρηση, ποσοτικοποίηση και πρόβλεψη κινδύνων, καθώς και τον καθορισμό κατάλληλων ενεργειών για τη μείωσή τους.
- **Διαχείριση ροών εργασίας (workflow management)**, η οποία υποστηρίζει τη δημιουργία, εκτέλεση και παρακολούθηση διαδικασιών σχετικών με το GRC.
- **Διαχείριση ελέγχων (audit management)**, με στόχο την οργάνωση πληροφοριών και τη βελτιστοποίηση των διαδικασιών εσωτερικού ελέγχου.
- **Υποστήριξη συνεργασίας μεταξύ επιχειρησιακών μονάδων**, μέσω ενιαίας πλατφόρμας συντονισμού δραστηριοτήτων.
- **Συνδέσεις και ενημερώσεις κανονιστικών αλλαγών**, ώστε ο οργανισμός να παραμένει ενημερωμένος για νέες ρυθμιστικές απαιτήσεις.
- **Έτοιμα πρότυπα (templates)**, τα οποία επιτρέπουν ταχύτερη εγκατάσταση και προσαρμογή του συστήματος στις ανάγκες της επιχείρησης.
- **Κεντρικός πίνακας ελέγχου (dashboard)**, που παρέχει δυνατότητα παρακολούθησης βασικών δεικτών απόδοσης (KPIs) σε πραγματικό χρόνο, σε σχέση με τις επιχειρησιακές διαδικασίες και τους στρατηγικούς στόχους.
-

Επιπλέον, η παροχή πρόσβασης σε λογισμικά Security Information and Event Management (SIEM) στις αρμόδιες μονάδες μπορεί να συμβάλει στον ταχύτερο εντοπισμό απειλών ασφαλείας. Παράλληλα, εργαλεία auditing μπορούν να χρησιμοποιηθούν για την αξιολόγηση της αποτελεσματικότητας των προσπαθειών GRC και τον εντοπισμό πιθανών βελτιώσεων.

Τα αποτελεσματικά εργαλεία GRC επιτρέπουν τη δημιουργία και διανομή πολιτικών και ελέγχων ασφαλείας, καθώς και την αντιστοίχισή τους με κανονιστικές απαιτήσεις και πρότυπα συμμόρφωσης. Επιπλέον, βοηθούν στην αξιολόγηση του κατά πόσο οι έλεγχοι έχουν εφαρμοστεί σωστά, λειτουργούν αποτελεσματικά και συμβάλλουν ουσιαστικά στη διαχείριση και μείωση των κινδύνων.[12]

6.3 Εργαλεία διαχείρισης κινδύνων

Τα εργαλεία διαχείρισης κινδύνων (risk management tools) αποτελούν συστήματα, λογισμικά ή μεθόδους που έχουν σχεδιαστεί για να υποστηρίζουν τους οργανισμούς σε όλα τα στάδια της διαδικασίας διαχείρισης κινδύνων. Ο βασικός τους ρόλος είναι ο εντοπισμός πιθανών κινδύνων, η διεξαγωγή αξιολογήσεων κινδύνου και η εφαρμογή μέτρων για τον μετριασμό των απειλών που επηρεάζουν τις επιχειρησιακές λειτουργίες.

Τα εργαλεία αυτά επιτρέπουν στις ομάδες να λειτουργούν προληπτικά και όχι αντιδραστικά. Μέσω δομημένων διαδικασιών ανάλυσης κινδύνων, βοηθούν τις επιχειρήσεις να προβλέπουν πιθανά προβλήματα, να κατανοούν τις επιπτώσεις τους και να εφαρμόζουν προληπτικά μέτρα προστασίας. Με αυτόν τον τρόπο ενισχύεται η λήψη αποφάσεων που βασίζεται σε δεδομένα και διευκολύνεται η δημιουργία ενός ολοκληρωμένου σχεδίου διαχείρισης κινδύνων.

Η χρήση εργαλείων διαχείρισης κινδύνων θεωρείται ιδιαίτερα σημαντική για την αποτελεσματική αντιμετώπιση αβεβαιοτήτων και τη διατήρηση της επιχειρησιακής συνέχειας και αποδοτικότητας.

Οφέλη από τη Χρήση Εργαλείων Διαχείρισης Κινδύνων

Η υιοθέτηση κατάλληλων εργαλείων διαχείρισης κινδύνων προσφέρει σημαντικά πλεονεκτήματα, συμβάλλοντας άμεσα στην ανθεκτικότητα και την επιτυχία μιας επιχείρησης. Τα σημαντικότερα οφέλη περιλαμβάνουν:

- **Βελτιωμένη λήψη αποφάσεων:**
  Τα εργαλεία παρέχουν σαφή εικόνα των πιθανών απειλών και των επιπτώσεών τους, επιτρέποντας στη διοίκηση να λαμβάνει πιο τεκμηριωμένες και στρατηγικές αποφάσεις.
- **Καλύτερη ορατότητα κινδύνων:**
  Τα λογισμικά διαχείρισης κινδύνων συγκεντρώνουν όλες τις σχετικές πληροφορίες σε μία ενιαία πλατφόρμα, παρέχοντας συνολική εικόνα της έκθεσης του οργανισμού σε κινδύνους.
- **Μείωση λειτουργικών διαταραχών:**
  Η έγκαιρη αναγνώριση κινδύνων και η ανάπτυξη αποτελεσματικών σχεδίων αντιμετώπισης συμβάλλουν στη διατήρηση της επιχειρησιακής συνέχειας και στη μείωση πιθανών διακοπών λειτουργίας.

- **Αύξηση αποδοτικότητας:**
  Η αυτοματοποίηση διαδικασιών, όπως η συλλογή δεδομένων και η παραγωγή αναφορών, εξοικονομεί χρόνο και επιτρέπει στις ομάδες να επικεντρώνονται σε στρατηγικές ενέργειες διαχείρισης κινδύνων.
- **Ενίσχυση συνεργασίας:**
  Πολλά εργαλεία διαχείρισης κινδύνων υποστηρίζουν τη συνεργασία μεταξύ διαφορετικών τμημάτων του οργανισμού, παρέχοντας κοινές πλατφόρμες για αξιολόγηση και αντιμετώπιση κινδύνων.
- **Διασφάλιση κανονιστικής συμμόρφωσης:**
  Σε κλάδους με αυστηρές ρυθμιστικές απαιτήσεις, τα εργαλεία αυτά συμβάλλουν στην τήρηση προτύπων συμμόρφωσης μέσω καταγεγραμμένων διαδικασιών, ελέγχων και αναφορών.

Βασικά Χαρακτηριστικά Εργαλείων Διαχείρισης Κινδύνων

Κατά την επιλογή ενός εργαλείου διαχείρισης κινδύνων, είναι σημαντικό να αξιολογούνται λειτουργίες που ενισχύουν τις δυνατότητες του οργανισμού και ενσωματώνονται ομαλά στις υπάρχουσες διαδικασίες. Τα σημαντικότερα χαρακτηριστικά περιλαμβάνουν:

- **Παραμετροποιήσιμες ροές εργασίας (customizable workflows):**
  Δυνατότητα προσαρμογής των διαδικασιών σύμφωνα με τις ανάγκες και τις απαιτήσεις του οργανισμού.
- **Παρακολούθηση και αναφορές σε πραγματικό χρόνο:**
  Συνεχής ενημέρωση σχετικά με την κατάσταση των κινδύνων, την πρόοδο των ενεργειών μετριασμού και τους σχετικούς δείκτες απόδοσης.
- **Ενσωμάτωση με άλλες πλατφόρμες:**
  Διασύνδεση με υπάρχοντα εργαλεία διαχείρισης έργων, συνεργασίας και επικοινωνίας, ώστε να αποφεύγεται ο κατακερματισμός των δεδομένων.
- **Ευκολία χρήσης:**
  Ένα εύχρηστο και κατανοητό περιβάλλον διευκολύνει την υιοθέτηση του εργαλείου από όλα τα επίπεδα του οργανισμού.
- **Ισχυρές δυνατότητες αναφορών:**
  Παραγωγή αναλυτικών και αξιοποιήσιμων αναφορών που υποστηρίζουν τη λήψη αποφάσεων και τη συμμόρφωση.

- **Δυνατότητα κλιμάκωσης (scalability):**
  Το εργαλείο πρέπει να μπορεί να προσαρμόζεται στην ανάπτυξη της επιχείρησης, υποστηρίζοντας αυξημένο όγκο δεδομένων, περισσότερους χρήστες και πιο σύνθετες διαδικασίες διαχείρισης κινδύνων.

Συνολικά, τα εργαλεία διαχείρισης κινδύνων δεν αποτελούν απλώς τεχνολογικές λύσεις, αλλά στρατηγικά μέσα που ενισχύουν τη συνολική ικανότητα του οργανισμού να εντοπίζει, να αξιολογεί και να αντιμετωπίζει αποτελεσματικά τις κυβερνοαπειλές και τους επιχειρησιακούς κινδύνους.[13]

6.4 Εργαλεία παρακολούθησης και ανίχνευσης περιστατικών

Η αποτελεσματική διαχείριση περιστατικών κυβερνοασφάλειας βασίζεται στη χρήση εξειδικευμένων εργαλείων που επιτρέπουν τον έγκαιρο εντοπισμό, την ανάλυση και την αντιμετώπιση απειλών. Οι σύγχρονες ομάδες ασφαλείας αξιοποιούν ολοκληρωμένες πλατφόρμες παρακολούθησης και απόκρισης, οι οποίες ενισχύουν τη δυνατότητα προστασίας σύνθετων πληροφοριακών υποδομών.

1. Security Information and Event Management (SIEM)

Τα συστήματα Security Information and Event Management (SIEM) συγκεντρώνουν και ενοποιούν δεδομένα καταγραφής (logs) από τερματικές συσκευές, δίκτυα, εφαρμογές και υποδομές cloud.

Τα σύγχρονα SIEM αξιοποιούν τεχνικές ανάλυσης δεδομένων και μηχανικής μάθησης για τον εντοπισμό ανωμαλιών και ύποπτης δραστηριότητας, επιτρέποντας στους αναλυτές ασφαλείας να ιεραρχούν αποτελεσματικότερα τις απειλές.

Βασικές δυνατότητες:

- Υποστήριξη υβριδικών και cloud περιβαλλόντων.
- Παραμετροποιήσιμοι πίνακες ελέγχου (dashboards).
- Διασύνδεση με πλατφόρμες αυτοματοποίησης και orchestration.

Οφέλη:

- Μείωση του φαινομένου alert fatigue μέσω συσχέτισης και εμπλουτισμού συμβάντων.

- Παροχή αξιοποιήσιμων πληροφοριών ασφαλείας σε πραγματικό χρόνο.

Η αποτελεσματικότητα ενός SIEM εξαρτάται σε μεγάλο βαθμό από την ποιότητα των δεδομένων που συλλέγει. Μη ορθά κανονικοποιημένα logs, αδύναμοι κανόνες συσχέτισης ή υπερβολικός θόρυβος μπορούν να οδηγήσουν σε υπερφόρτωση ειδοποιήσεων και μείωση της αποδοτικότητας των ομάδων SOC (Security Operations Center). Για τον λόγο αυτό, η σωστή παραμετροποίηση του συστήματος θεωρείται εξίσου σημαντική με την αρχική εγκατάστασή του.

2. Security Orchestration, Automation, and Response (SOAR)

Τα εργαλεία Security Orchestration, Automation, and Response (SOAR) αυτοματοποιούν επαναλαμβανόμενες διαδικασίες και συντονίζουν την απόκριση μεταξύ διαφορετικών συστημάτων ασφαλείας.

Όταν συνδυάζονται με SIEM πλατφόρμες, μπορούν να εκτελούν αυτοματοποιημένα playbooks για την άμεση αντιμετώπιση περιστατικών.

Παράδειγμα χρήσης:
Σε περίπτωση επίθεσης phishing, το SOAR μπορεί να απομονώσει αυτόματα τις επηρεαζόμενες συσκευές, να επαναφέρει διαπιστευτήρια πρόσβασης και να αποκλείσει κακόβουλα domains χωρίς ανθρώπινη παρέμβαση.

Προηγμένες δυνατότητες:

- Δυναμικά playbooks που προσαρμόζονται βάσει νέων πληροφοριών απειλών.
- Εκτεταμένες δυνατότητες διασύνδεσης μέσω APIs.

Η αποτελεσματικότητα ενός SOAR εξαρτάται από την ικανότητά του να ενσωματώνεται με SIEM, EDR, threat intelligence feeds, ticketing systems και cloud πλατφόρμες. Περιορισμένες διασυνδέσεις μπορεί να αυξήσουν την πολυπλοκότητα αντί να βελτιώσουν τον συντονισμό.

3. Endpoint Detection and Response (EDR)

Τα συστήματα Endpoint Detection and Response (EDR) παρέχουν συνεχή παρακολούθηση τερματικών συσκευών, εντοπίζοντας κακόβουλες διεργασίες και επιτρέποντας την άμεση απομόνωση επηρεαζόμενων endpoints.

Η αυξημένη χρήση απομακρυσμένης εργασίας έχει καταστήσει τα EDR απαραίτητα για τη σύγχρονη κυβερνοασφάλεια.

Βασικά χαρακτηριστικά:

- Συνεχής παρακολούθηση σε πραγματικό χρόνο.
- Προηγμένος εντοπισμός απειλών.
- Αυτοματοποιημένη απόκριση.
- Δυνατότητες ψηφιακής εγκληματολογικής ανάλυσης (forensics).

Τα EDR προσφέρουν λεπτομερή ορατότητα σχετικά με τις ενέργειες που πραγματοποιούνται σε μία συσκευή, όπως η εκτέλεση αρχείων, η δημιουργία διεργασιών και οι δικτυακές συνδέσεις. Οι δυνατότητες αυτές είναι ιδιαίτερα σημαντικές για την ανάλυση της βασικής αιτίας (root cause analysis) ενός περιστατικού ασφαλείας.

4. Network Traffic Analysis

Η ανάλυση δικτυακής κυκλοφορίας αποτελεί κρίσιμο στοιχείο για την κατανόηση της δραστηριότητας επιτιθέμενων εντός του δικτύου.

Τα εργαλεία packet capture και network traffic analysis επιτρέπουν:

- την ανακατασκευή αλυσίδων επιθέσεων,
- τον εντοπισμό lateral movement,
- και την ανάλυση πιθανής διαρροής δεδομένων (data exfiltration).

Τα εργαλεία αυτά είναι ιδιαίτερα χρήσιμα όταν οι επιτιθέμενοι επιχειρούν να παρακάμψουν μηχανισμούς ασφαλείας ή χρησιμοποιούν τεχνικές Living off the Land (LotL).

Παράλληλα, παρέχουν αποδεικτικά στοιχεία υψηλής αξιοπιστίας, τα οποία μπορούν να χρησιμοποιηθούν για κανονιστική συμμόρφωση ή νομικές διαδικασίες.

5. Extended Detection and Response (XDR)

Οι πλατφόρμες Extended Detection and Response (XDR) αποτελούν εξέλιξη των EDR λύσεων, προσφέροντας ενοποιημένη ορατότητα σε περιβάλλοντα cloud, τοπικές υποδομές και απομακρυσμένα endpoints.

Τα XDR συγκεντρώνουν και συσχετίζουν δεδομένα από πολλαπλές πηγές ασφαλείας, όπως:

- endpoints,
- δίκτυα,
- cloud υπηρεσίες,
- εφαρμογές ασφαλείας.

Πλεονεκτήματα:

- Μείωση θορύβου από αποσπασματικά εργαλεία ασφαλείας.
- Αυτοματοποιημένη διερεύνηση περιστατικών.
- Καθοδηγούμενη αποκατάσταση (guided remediation).
- Ενοποιημένη και συντονισμένη απόκριση.

Τα XDR θεωρούνται ιδιαίτερα κατάλληλα για οργανισμούς με ώριμες υποδομές ασφαλείας που επιδιώκουν την ενοποίηση των μηχανισμών παρακολούθησης και απόκρισης.

6. Incident Management Tools

Τα εργαλεία διαχείρισης περιστατικών (incident management tools) διευκολύνουν τον συντονισμό των ομάδων κατά τη διάρκεια ενός περιστατικού κυβερνοασφάλειας.

Παρέχουν:

- τυποποιημένες ροές εργασίας,
- καταγραφή ενεργειών με χρονοσήμανση,
- ενημερώσεις σε πραγματικό χρόνο,
- και κεντρική διαχείριση περιστατικών.

Οφέλη:

- Ενημέρωση διοικητικών στελεχών και νομικών ομάδων.
- Βελτιωμένος συντονισμός μεταξύ διαφορετικών τμημάτων και γεωγραφικών περιοχών.
- Διατήρηση στοιχείων για μεταγενέστερη ανάλυση και συμμόρφωση.

Κατά την επιλογή τέτοιων εργαλείων, ιδιαίτερη σημασία έχουν λειτουργίες όπως:

- role-based access control,

- audit trails,
- σύνδεση σχετικών alerts σε ενιαία υπόθεση,
- και ενσωμάτωση με ITSM ή ticketing συστήματα.

7. Threat Intelligence Platforms

Οι πλατφόρμες threat intelligence παρέχουν πληροφορίες σχετικά με δείκτες παραβίασης (Indicators of Compromise – IOCs), τεχνικές επιτιθέμενων και νέες κυβερνοαπειλές.

Η αξιοποίηση πληροφοριών απειλών σε πραγματικό χρόνο συμβάλλει:

- στην ταχύτερη διερεύνηση περιστατικών,
- στη μείωση ψευδώς θετικών ειδοποιήσεων,
- και στην καλύτερη ιεράρχηση κινδύνων.

Με αυτόν τον τρόπο, οι οργανισμοί μεταβαίνουν από μια καθαρά αντιδραστική προσέγγιση σε ένα πιο προληπτικό μοντέλο άμυνας απέναντι στις κυβερνοαπειλές.[14]

6.5 Εργαλεία τεκμηρίωσης και audit readiness

Τα αυτοματοποιημένα εργαλεία audit readiness αποτελούν λογισμικές λύσεις που έχουν σχεδιαστεί για να μειώνουν τη δυσκολία και τον χειροκίνητο φόρτο εργασίας που σχετίζεται με την προετοιμασία ελέγχων (audits). Τα εργαλεία αυτά λειτουργούν ως κεντρικός κόμβος διαχείρισης όλων των δεδομένων, διαδικασιών και ενεργειών που σχετίζονται με ελέγχους συμμόρφωσης, επιτρέποντας στους οργανισμούς να διατηρούν συνεχή ετοιμότητα και όχι μόνο να προετοιμάζονται λίγο πριν από έναν έλεγχο.

Μέσω της αυτοματοποίησης επαναλαμβανόμενων διαδικασιών, τα εργαλεία audit readiness βελτιώνουν τη διαχείριση συμμόρφωσης και αυξάνουν την αποδοτικότητα των ομάδων εργασίας. Αντί οι οργανισμοί να λειτουργούν αντιδραστικά απέναντι στις απαιτήσεις ενός ελέγχου, μπορούν να διαχειρίζονται προληπτικά τα οικονομικά δεδομένα, τις πολιτικές και τους εσωτερικούς ελέγχους τους. Η προσέγγιση αυτή επιτρέπει ταχύτερο κλείσιμο οικονομικών περιόδων, μείωση σφαλμάτων και αποτελεσματικότερη αντιμετώπιση ελεγκτικών διαδικασιών.

Λειτουργία των Εργαλείων Audit Readiness

Στον πυρήνα τους, τα εργαλεία audit readiness λειτουργούν ως «ψηφιακοί βοηθοί» για την προετοιμασία ελέγχων. Αυτοματοποιούν χρονοβόρες διαδικασίες, όπως:

- εξαγωγή δεδομένων,
- ανάλυση πληροφοριών,
- δημιουργία αναφορών,
- και τεκμηρίωση συμμόρφωσης.

Μέσω διασύνδεσης με οικονομικά και επιχειρησιακά συστήματα, όπως ERP, CRM και λογιστικές πλατφόρμες, τα εργαλεία συλλέγουν δεδομένα σε πραγματικό χρόνο και μειώνουν σημαντικά την πιθανότητα ανθρώπινου σφάλματος.

Παράλληλα, αξιοποιούν τεχνολογίες όπως:

- Τεχνητή Νοημοσύνη (Artificial Intelligence – AI),
- και Robotic Process Automation (RPA),

προκειμένου να εντοπίζουν ανωμαλίες, πιθανά κενά συμμόρφωσης και λειτουργικές αδυναμίες. Επιπλέον, περιλαμβάνουν δυνατότητες διαχείρισης ροών εργασίας (workflow management), ανάθεσης καθηκόντων και παρακολούθησης της προόδου ενεργειών συμμόρφωσης.

Οφέλη Χρήσης Εργαλείων Audit Readiness

Η υιοθέτηση αυτοματοποιημένων εργαλείων audit readiness προσφέρει σημαντικά πλεονεκτήματα στους οργανισμούς:

Ενοποίηση Δεδομένων σε Πραγματικό Χρόνο

Ένα από τα σημαντικότερα προβλήματα κατά την προετοιμασία ελέγχων είναι η συγκέντρωση δεδομένων από διαφορετικά συστήματα. Τα εργαλεία αυτά λειτουργούν ως κεντρικές πλατφόρμες διασύνδεσης, συλλέγοντας οικονομικά και λειτουργικά δεδομένα σε πραγματικό χρόνο. Με αυτόν τον τρόπο εξασφαλίζεται ότι οι πληροφορίες είναι πάντοτε ενημερωμένες και ακριβείς.

Αυτοματοποίηση Εσωτερικών Ελέγχων

Τα εργαλεία audit readiness μπορούν να παρακολουθούν συνεχώς τις διαδικασίες εσωτερικού ελέγχου και να εντοπίζουν αποκλίσεις από τις καθορισμένες πολιτικές ασφαλείας και συμμόρφωσης. Για παράδειγμα, το σύστημα μπορεί να ειδοποιήσει αυτόματα σε περίπτωση μη εξουσιοδοτημένης αλλαγής ή συναλλαγής χωρίς έγκριση.

Συνεχής Παρακολούθηση Συμμόρφωσης

Τα εργαλεία αυτά ενσωματώνουν κανονιστικά πρότυπα και απαιτήσεις συμμόρφωσης, επιτρέποντας τη συνεχή παρακολούθηση της συμμόρφωσης με πρότυπα όπως:

- SOC 2,
- ISO 27001,
- SOX (Sarbanes-Oxley Act),
- και άλλες κανονιστικές απαιτήσεις.

Η δυνατότητα αυτή μειώνει τον κίνδυνο παραβιάσεων συμμόρφωσης και ενισχύει την αξιοπιστία του οργανισμού απέναντι σε ελεγκτικές αρχές.

Δημιουργία Προσαρμοσμένων Αναφορών

Κατά τη διάρκεια ενός audit, οι ελεγκτές συχνά ζητούν εξειδικευμένες αναφορές και τεκμηρίωση. Τα αυτοματοποιημένα εργαλεία επιτρέπουν τη γρήγορη παραγωγή προσαρμοσμένων αναφορών, μειώνοντας σημαντικά τον χρόνο προετοιμασίας και διευκολύνοντας τη διαδικασία ελέγχου.

Εξοικονόμηση Χρόνου και Κόστους

Η αυτοματοποίηση μειώνει δραστικά τις χειροκίνητες διαδικασίες συμφωνίας δεδομένων και προετοιμασίας εγγράφων. Αυτό επιτρέπει στις ομάδες να επικεντρώνονται σε στρατηγικές δραστηριότητες αντί για διοικητικές εργασίες, ενώ παράλληλα μειώνει το συνολικό κόστος ελέγχων και συμμόρφωσης.

Βελτίωση Ακρίβειας και Συνέπειας

Η χρήση αυτοματοποιημένων διαδικασιών μειώνει τα ανθρώπινα λάθη που σχετίζονται με τη χειροκίνητη επεξεργασία δεδομένων. Κάθε συναλλαγή και διαδικασία ακολουθεί

προκαθορισμένους κανόνες, διασφαλίζοντας συνέπεια και αξιοπιστία στις οικονομικές και κανονιστικές αναφορές.

Μείωση Κινδύνων

Τα εργαλεία audit readiness συμβάλλουν στον εντοπισμό ύποπτων δραστηριοτήτων, διπλών πληρωμών ή μη εξουσιοδοτημένων αλλαγών, ενισχύοντας τη συνολική διαχείριση κινδύνων. Μέσω συνεχούς παρακολούθησης και διαφάνειας στις διαδικασίες, οι οργανισμοί μπορούν να περιορίζουν λειτουργικούς, οικονομικούς και κανονιστικούς κινδύνους.

Συμπέρασμα

Τα εργαλεία audit readiness αποτελούν κρίσιμο στοιχείο για τη σύγχρονη διαχείριση συμμόρφωσης και εσωτερικού ελέγχου. Μέσω της αυτοματοποίησης διαδικασιών, της συνεχούς παρακολούθησης και της ενοποίησης δεδομένων, ενισχύουν την αποτελεσματικότητα, τη διαφάνεια και την ετοιμότητα των οργανισμών απέναντι σε ελεγκτικές και κανονιστικές απαιτήσεις. Παράλληλα, υποστηρίζουν τη διατήρηση υψηλού επιπέδου κυβερνοασφάλειας και επιχειρησιακής ανθεκτικότητας.[15]

6.6 Αντιστοίχιση Εργαλείων με τις Απαιτήσεις των NIS2 και SOC 2

Οι απαιτήσεις των NIS2 και SOC 2 μπορούν να αντιστοιχηθούν με τα προαναφερθέντα εργαλεία όπως :

- Εργαλεία Governance, Risk and Compliance (GRC)
- Εργαλεία Διαχείρισης Κινδύνων
- Security Information and Event Management (SIEM)
- Security Orchestration, Automation, and Response (SOAR)
- Endpoint Detection and Response (EDR) και Extended Detection and Response (XDR)
- Network Traffic Analysis και Intrusion Detection Systems (IDS/IPS)
- Πλατφόρμες Threat Intelligence
- Εργαλεία Διαχείρισης Περιστατικών και Audit Readiness

Όλα τα παραπάνω εργαλεία εμπεριέχουν βασικά στοιχεία τα οποία εντοπίζονται κατά την συμμόρφωσή με την οδηγία NIS 2 αλλά και με τον κανονισμό SOC 2.

7. Μελλοντικές Τάσεις

7.1 Το Μέλλον της Συμμόρφωσης και των Εργαλείων Κυβερνοασφάλειας

Η συμμόρφωση αποτελούσε πάντοτε μια δυναμική και συνεχώς μεταβαλλόμενη διαδικασία. Οι απαιτήσεις ασφάλειας και κανονιστικής συμμόρφωσης εξελίσσονται παράλληλα με την τεχνολογική πρόοδο και τις νέες κυβερνοαπειλές.

Κατά τη δεκαετία του 1990, η ασφάλεια πληροφοριακών συστημάτων επικεντρωνόταν κυρίως σε τεχνολογίες όπως τα firewalls και τα antivirus. Στη δεκαετία του 2000, κανονιστικά πλαίσια όπως τα SOX, HIPAA και PCI DSS διαμόρφωσαν ένα πιο αυστηρό περιβάλλον συμμόρφωσης. Στη συνέχεια, τη δεκαετία του 2010, εμφανίστηκαν νέες απαιτήσεις που σχετίζονταν με την προστασία προσωπικών δεδομένων και το cloud computing, όπως οι GDPR και CCPA. Σήμερα, πρότυπα όπως τα ISO 27001, SOC 2 και NIST αποτελούν διεθνή σημεία αναφοράς για την αξιοπιστία και την ασφάλεια οργανισμών.

Ωστόσο, η συμμόρφωση έως το 2030 αναμένεται να μετασχηματιστεί ριζικά, υιοθετώντας χαρακτηριστικά όπως:

- αυτοματοποίηση μέσω τεχνητής νοημοσύνης,
- συνεχής παρακολούθηση σε πραγματικό χρόνο,
- προγνωστική ανάλυση κινδύνων,
- και παγκόσμια ενοποίηση κανονιστικών απαιτήσεων.

Τάση 1: Η Συμμόρφωση Γίνεται Συνεχής

Σήμερα, η συμμόρφωση συχνά αντιμετωπίζεται ως μια ετήσια διαδικασία προετοιμασίας για ελέγχους και audits. Μέχρι το 2030, η προσέγγιση αυτή αναμένεται να αλλάξει σημαντικά.

Η συμμόρφωση θα είναι:

- συνεχής και όχι περιοδική,
- πλήρως ενσωματωμένη στα πληροφοριακά συστήματα,
- και αυτοματοποιημένη μέσω τεχνητής νοημοσύνης.

Τα συστήματα θα παρακολουθούν ελέγχους ασφαλείας σε 24ωρη βάση, συγχρονίζοντας αυτόματα logs, δεδομένα προσωπικού, πολιτικές και αποδεικτικά συμμόρφωσης. Επιπλέον,

θα αναπτύσσονται δυνατότητες «self-healing compliance», όπου αποτυχίες ελέγχων — όπως η μη εφαρμογή πολυπαραγοντικής αυθεντικοποίησης (MFA) — θα διορθώνονται αυτόματα από το ίδιο το σύστημα.

Τάση 2: Πολλαπλασιασμός Κανονιστικών Απαιτήσεων

Οι κανονιστικές απαιτήσεις δεν αναμένεται να μειωθούν αλλά να αυξηθούν σημαντικά τα επόμενα χρόνια.

Νέα ρυθμιστικά πλαίσια θα αφορούν:

- τη διακυβέρνηση τεχνητής νοημοσύνης (AI Governance),
- την κβαντικά ασφαλή κρυπτογραφία (Quantum-safe cryptography),
- καθώς και τις αναφορές βιωσιμότητας και ESG που θα συνδέονται με πληροφοριακά συστήματα.

Έως το 2030, οι περισσότεροι οργανισμοί θα πρέπει να συμμορφώνονται ταυτόχρονα με πολλαπλά και αλληλεπικαλυπτόμενα πρότυπα και κανονισμούς.

Για τον λόγο αυτό, αναμένεται αυξημένη χρήση εργαλείων τεχνητής νοημοσύνης που θα μπορούν να αντιστοιχίζουν ελέγχους ασφαλείας μεταξύ διαφορετικών frameworks, μειώνοντας την ανάγκη επανασχεδιασμού διαδικασιών συμμόρφωσης.

Τάση 3: Από Αντιδραστική σε Προγνωστική Συμμόρφωση

Σήμερα, οι οργανισμοί συνήθως αντιδρούν μετά από ένα περιστατικό ασφαλείας ή μετά από παρατηρήσεις ελεγκτών.

Στο μέλλον, τα εργαλεία συμμόρφωσης θα αξιοποιούν τεχνητή νοημοσύνη για:

- προσομοίωση κινδύνων μέσω “what-if” αναλύσεων,
- πρόβλεψη πιθανών αποτυχιών ελέγχων,
- και έγκαιρη ειδοποίηση των υπευθύνων ασφαλείας πριν από την εμφάνιση προβλημάτων.

Η προσέγγιση αυτή μετατρέπει τη συμμόρφωση σε ένα είδος «ραντάρ κινδύνων», το οποίο προειδοποιεί τους οργανισμούς πριν από πιθανές παραβιάσεις ή κανονιστικά ζητήματα.

Τάση 4: Συνεργασία Ανθρώπου και Τεχνητής Νοημοσύνης

Η τεχνητή νοημοσύνη δεν αναμένεται να αντικαταστήσει πλήρως τις ομάδες συμμόρφωσης, αλλά να λειτουργήσει υποστηρικτικά.

Τα συστήματα AI θα μπορούν:

- να δημιουργούν πολιτικές ασφαλείας,
- να αντιστοιχίζουν πρότυπα και frameworks,
- και να παράγουν αποδεικτικά στοιχεία συμμόρφωσης.

Ωστόσο, οι άνθρωποι θα συνεχίσουν να λαμβάνουν αποφάσεις σχετικά με:

- την αποδοχή κινδύνων,
- τις επιχειρησιακές προτεραιότητες,
- και τα ζητήματα ηθικής και διακυβέρνησης.

Ο ρόλος των υπευθύνων συμμόρφωσης θα μετατοπιστεί από γραφειοκρατικές διαδικασίες προς στρατηγικές συμβουλευτικές δραστηριότητες. Είναι πιθανό να εμφανιστούν νέοι επαγγελματικοί ρόλοι, όπως “AI Compliance Navigator”.

Τάση 5: Η Συμμόρφωση ως Ανταγωνιστικό Πλεονέκτημα

Μέχρι το 2030, η συμμόρφωση δεν θα αποτελεί μόνο μηχανισμό αποφυγής προστίμων ή κυρώσεων, αλλά και σημαντικό ανταγωνιστικό πλεονέκτημα.

Η συμμόρφωση θα λειτουργεί ως:

- μέσο ενίσχυσης πωλήσεων και συνεργασιών,
- δείκτης αξιοπιστίας προς πελάτες και επενδυτές,
- και «παγκόσμιο διαβατήριο» για πρόσβαση σε διεθνείς αγορές.

Οι οργανισμοί που θα μπορούν να αποδεικνύουν σε πραγματικό χρόνο συμμόρφωση με πρότυπα όπως ISO 27001, SOC 2, NIST και ESG θα αποκτούν αυξημένη εμπιστοσύνη και ανταγωνιστικό πλεονέκτημα στην αγορά.

Συμπέρασμα

Το μέλλον της συμμόρφωσης αναμένεται να χαρακτηρίζεται από αυτοματοποίηση, συνεχή παρακολούθηση και αξιοποίηση τεχνητής νοημοσύνης. Οι οργανισμοί θα χρειαστεί να υιοθετήσουν προηγμένα εργαλεία κυβερνοασφάλειας και compliance management προκειμένου να ανταποκριθούν σε ολοένα αυξανόμενες κανονιστικές απαιτήσεις και σύνθετα ψηφιακά περιβάλλοντα.

Η συμμόρφωση δεν θα αποτελεί πλέον μόνο υποχρέωση, αλλά στρατηγικό παράγοντα ανάπτυξης, αξιοπιστίας και επιχειρησιακής ανθεκτικότητας.[16]

7.2 DORA, CSRD και άλλες ευρωπαϊκές πρωτοβουλίες

DORA

(Digital Operational Resilience Act – EU)

Το 2025, ο Κανονισμός Ψηφιακής Επιχειρησιακής Ανθεκτικότητας της Ευρωπαϊκής Ένωσης (DORA) τίθεται σε ισχύ, επιβάλλοντας αυστηρές απαιτήσεις κυβερνοασφάλειας σε χρηματοπιστωτικούς οργανισμούς (τράπεζες, ασφαλιστικές εταιρείες, επενδυτικές εταιρείες και άλλους) καθώς και στους κρίσιμους παρόχους τεχνολογικών υπηρεσιών τους. Οι οργανισμοί αυτοί πρέπει να δημιουργήσουν ολοκληρωμένα πλαίσια διαχείρισης κυβερνοκινδύνων, να διεξάγουν τακτικές δοκιμές ανθεκτικότητας και να αναφέρουν σημαντικά περιστατικά. Επιπλέον, το DORA επιβάλλει αυστηρή εποπτεία στους τρίτους παρόχους, απαιτώντας από τους χρηματοπιστωτικούς οργανισμούς να διαχειρίζονται επιμελώς τους σχετικούς κινδύνους. Η μη συμμόρφωση μπορεί να οδηγήσει σε σημαντικές κυρώσεις, συμπεριλαμβανομένων προστίμων έως 2% του παγκόσμιου κύκλου εργασιών για χρηματοπιστωτικούς οργανισμούς και έως 5 εκατομμυρίων ευρώ για κρίσιμους παρόχους υπηρεσιών.[17]

CSRD

Η Οδηγία Corporate Sustainability Reporting Directive (CSRD) αναμένεται να μετασχηματίσει τον τρόπο με τον οποίο οι εταιρείες αναφέρουν τις προσπάθειές τους σχετικά με τη βιωσιμότητα, σηματοδοτώντας ένα σημαντικό βήμα προόδου στην εταιρική λογοδοσία.

Η οδηγία υιοθετήθηκε από την Ευρωπαϊκή Επιτροπή το 2022 και βασίζεται στην προηγούμενη Οδηγία Non-Financial Reporting Directive (NFRD), την οποία αντικαθιστά. Η

CSRD αντιμετωπίζει τους περιορισμούς του προηγούμενου πλαισίου επεκτείνοντας το πεδίο εφαρμογής της και ενισχύοντας τις απαιτήσεις αναφοράς. Στον πυρήνα της, η CSRD στοχεύει στην προώθηση της διαφάνειας και της λογοδοσίας στις αναφορές βιωσιμότητας σε ολόκληρη την Ευρωπαϊκή Ένωση.

Η οδηγία αυτή δεν αποτελεί απλώς μία ακόμη κανονιστική απαίτηση, αλλά έχει σχεδιαστεί ώστε να επιφέρει ουσιαστικές αλλαγές στη συμπεριφορά των επιχειρήσεων. Η CSRD ευθυγραμμίζει τις επιχειρησιακές πρακτικές με τους στόχους βιωσιμότητας της Ευρωπαϊκής Ένωσης και με τη διεθνή προσπάθεια για μια πιο υπεύθυνη οικονομία.[18]

EU AI Act

Το 2025, ο Κανονισμός Τεχνητής Νοημοσύνης της Ευρωπαϊκής Ένωσης (EU AI Act) ξεκινά να εφαρμόζεται, εισάγοντας ένα πλαίσιο ρύθμισης της τεχνητής νοημοσύνης βασισμένο στον κίνδυνο. Τα συστήματα AI υψηλού κινδύνου σε τομείς όπως η υγειονομική περίθαλψη και η ασφάλεια πρέπει να πληρούν αυστηρές απαιτήσεις σχετικά με τη διαφάνεια, την ασφάλεια και τον μετριασμό της μεροληψίας. Οι οργανισμοί υποχρεούνται να πραγματοποιούν ολοκληρωμένες αξιολογήσεις κινδύνων και να θεσπίζουν διαδικασίες διακυβέρνησης. Ορισμένες πρακτικές AI, όπως το social scoring και συγκεκριμένες μορφές βιομετρικής επιτήρησης, απαγορεύονται. Η εφαρμογή του Κανονισμού πραγματοποιείται σταδιακά, με τις απαγορεύσεις για συστήματα AI απαράδεκτου κινδύνου να ισχύουν από τον Φεβρουάριο του 2025 και την πλήρη συμμόρφωση για συστήματα υψηλού κινδύνου να απαιτείται έως τον Αύγουστο του 2027.[17]

EU Cyber Resilience Act (CRA)

Ο Νόμος Cyber Resilience Act (CRA) τέθηκε σε ισχύ στις 10 Δεκεμβρίου 2024, όταν δημοσιεύθηκε ως Κανονισμός (EU) 2024/2847 στην Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης. Ορισμένες απαιτήσεις του CRA καθίστανται υποχρεωτικές στις 11-09-2026 και ο Κανονισμός θα εφαρμοστεί πλήρως τρία χρόνια αργότερα, στις 11-12-2027. Το CRA θα υποχρεώνει όλα τα προϊόντα με ψηφιακά στοιχεία, συμπεριλαμβανομένης της απομακρυσμένης επεξεργασίας δεδομένων τους, που διατίθενται στην ευρωπαϊκή αγορά να συμμορφώνονται με τον Κανονισμό.

Το CRA στοχεύει στην αντιμετώπιση απειλών και ευπαθειών μέσω της δημιουργίας τυποποιημένων πλαισίων απαιτήσεων κυβερνοασφάλειας ως μέρος ενός ευρύτερου συνόλου ευρωπαϊκής νομοθεσίας προϊόντων. Ρυθμίζει τα λεγόμενα «προϊόντα με ψηφιακά στοιχεία» (products with digital elements – PDE), και η οριζόντια φύση του του προσδίδει ευρύ πεδίο

εφαρμογής, συμπεριλαμβάνοντας μεγάλο εύρος hardware και software, αλλά εξαιρώντας ιατρικές συσκευές, αυτοκίνητα και άλλες κατηγορίες προϊόντων που διαθέτουν δικούς τους κανόνες ασφάλειας και προστασίας. Ο κύριος στόχος είναι η μείωση του κόστους από παραβιάσεις δεδομένων και η αύξηση της εμπιστοσύνης των καταναλωτών σε προϊόντα με ψηφιακά στοιχεία.[19]

7.3 Ρόλος Τεχνητής Νοημοσύνης και αυτοματοποίησης

Το μέλλον είναι η ευελιξία και τα προσαρμοσμένα Πλαίσια Συμμόρφωσης .Η προσέγγιση «ένα μοντέλο για όλους» στη συμμόρφωση δεν είναι πλέον αποτελεσματική. Οι οργανισμοί αντιμετωπίζουν εντελώς διαφορετικούς κινδύνους, κανονισμούς και λειτουργικές απαιτήσεις ανάλογα με τον κλάδο, τη γεωγραφική περιοχή και τη δομή τους. Για να αντιμετωπίσουν αυτήν την πολυπλοκότητα, πολλοί οργανισμοί στρέφονται σε προσαρμοσμένα πλαίσια συμμόρφωσης (tailored compliance frameworks) – ειδικά σχεδιασμένους ελέγχους και διαδικασίες που ευθυγραμμίζονται με τις συγκεκριμένες επιχειρησιακές ανάγκες.

Τα προσαρμοσμένα πλαίσια προσφέρουν αρκετά σαφή πλεονεκτήματα:

- **Συνάφεια (Relevance)** – Οι έλεγχοι ευθυγραμμίζονται με την πραγματική έκθεση σε κινδύνους και το κανονιστικό πεδίο εφαρμογής.
  Για παράδειγμα: Μια fintech startup επικεντρώνεται στο PCI DSS και στους κανόνες κατά του ξεπλύματος χρήματος, αντί να εφαρμόζει πρότυπα που αφορούν την υγειονομική περίθαλψη ή τη βιομηχανία.

- **Αποδοτικότητα (Efficiency)** – Οι πόροι κατευθύνονται εκεί όπου έχουν τη μεγαλύτερη σημασία.
  Για παράδειγμα: Μια βιομηχανική επιχείρηση αντικατέστησε πλεονάζοντες ελέγχους ISO με μέτρα επικεντρωμένα στη NIS2 που στοχεύουν στον κίνδυνο τρίτων παρόχων.

- **Επεκτασιμότητα (Scalability)** – Τα πλαίσια εξελίσσονται μαζί με τον οργανισμό.
  Για παράδειγμα: Ένας οργανισμός υγειονομικής περίθαλψης με έδρα τις ΗΠΑ επέκτεινε το πρόγραμμα HIPAA ώστε να περιλαμβάνει και το GDPR όταν άρχισε να εξυπηρετεί Ευρωπαίους πελάτες.

Ο σχεδιασμός ενός προσαρμοσμένου πλαισίου ξεκινά με την αξιολόγηση του προφίλ κινδύνου, του επιχειρησιακού μοντέλου και των κανονιστικών υποχρεώσεων του οργανισμού. Η διαδικασία αυτή συχνά περιλαμβάνει την αντιστοίχιση υπαρχόντων ελέγχων

με πολλαπλά πρότυπα, τον εντοπισμό κενών και την ενσωμάτωση σχετικών βέλτιστων πρακτικών σε ένα ενιαίο πρόγραμμα συμμόρφωσης.

Αναδυόμενες Τεχνολογίες και η Επίδρασή τους στη Συμμόρφωση

Οι νέες τεχνολογίες αλλάζουν τον τρόπο με τον οποίο οι οργανισμοί προσεγγίζουν τη συμμόρφωση. Παρότι προσφέρουν ισχυρές δυνατότητες, δημιουργούν επίσης νέους κινδύνους και κανονιστικές «γκρίζες ζώνες» που εξακολουθούν να διαμορφώνονται.

- **Τεχνητή Νοημοσύνη (Artificial Intelligence – AI)**
  Η AI επιτρέπει ταχύτερη λήψη αποφάσεων, παρακολούθηση σε πραγματικό χρόνο και καλύτερη ανίχνευση ανωμαλιών. Ωστόσο, δημιουργεί επίσης ανησυχίες σχετικά με τη δυνατότητα επεξήγησης, τη λογοδοσία και την ηθική χρήση – ιδιαίτερα στους τομείς των χρηματοοικονομικών, της υγείας και των προσλήψεων.
- **Μηχανική Μάθηση (Machine Learning – ML)**
  Η ML μπορεί να εντοπίζει ύποπτη συμπεριφορά και να βελτιώνει τα μοντέλα κινδύνου, αλλά χωρίς κατάλληλη εποπτεία μπορεί να ενισχύσει μεροληψίες, να παράγει αδιαφανείς αποφάσεις ή να θέσει σε κίνδυνο την ιδιωτικότητα – ειδικά όταν τα δεδομένα εκπαίδευσης δεν είναι διαφανή.
- **Generative AI και Large Language Models (LLMs)**
  Εργαλεία όπως τα μεγάλα γλωσσικά μοντέλα μπορούν να επιταχύνουν τη δημιουργία αναφορών, τεκμηρίωσης και ανάπτυξης λογισμικού. Ωστόσο, ενέχουν επίσης κινδύνους, όπως η παραγωγή ανακριβούς περιεχομένου (hallucinated content), η διαρροή πνευματικής ιδιοκτησίας και η ακούσια έκθεση ευαίσθητων δεδομένων.
- **Predictive Analytics**
  Τα προγνωστικά μοντέλα βοηθούν στην ιεράρχηση κινδύνων και στον σχεδιασμό προληπτικών ελέγχων. Παρόλα αυτά, οι ρυθμιστικές αρχές δίνουν όλο και μεγαλύτερη προσοχή στον τρόπο με τον οποίο τα μοντέλα αυτά αναπτύσσονται, επικυρώνονται και επεξηγούνται – ιδιαίτερα σε τομείς υψηλού κινδύνου.

Για να διαχειριστούν αυτήν την πολυπλοκότητα, πολλοί οργανισμοί υιοθετούν την προσέγγιση compliance-by-design, ενσωματώνοντας μηχανισμούς διακυβέρνησης, διαφάνειας και ελέγχου κινδύνων απευθείας στην ανάπτυξη και υλοποίηση νέων τεχνολογιών.[17]

8. Συμπεράσματα

8.1 Σύνοψη ευρημάτων

Η παρούσα διατριβή εξέτασε το σύγχρονο κανονιστικό περιβάλλον κυβερνοασφάλειας με έμφαση στη σύγκριση της Οδηγίας NIS2 και του πλαισίου SOC 2. Μέσα από τη μελέτη των απαιτήσεων, των μηχανισμών συμμόρφωσης και των πρακτικών εφαρμογής των δύο πλαισίων, αναδείχθηκαν τόσο οι διαφορές όσο και τα σημεία σύγκλισης μεταξύ τους.

Η έρευνα έδειξε ότι η αυξανόμενη πολυπλοκότητα των κυβερνοαπειλών, η εξάρτηση των οργανισμών από ψηφιακές υποδομές και η ανάγκη προστασίας κρίσιμων πληροφοριών έχουν οδηγήσει στην ανάπτυξη αυστηρότερων πλαισίων κυβερνοασφάλειας και κανονιστικής συμμόρφωσης. Η NIS2 αποτελεί ένα δεσμευτικό κανονιστικό πλαίσιο της Ευρωπαϊκής Ένωσης, το οποίο στοχεύει στην ενίσχυση της κυβερνοανθεκτικότητας οργανισμών που δραστηριοποιούνται σε κρίσιμους και σημαντικούς τομείς. Αντίθετα, το SOC 2 λειτουργεί ως μηχανισμός διασφάλισης και αξιολόγησης εσωτερικών ελέγχων, παρέχοντας αποδείξεις αξιοπιστίας και ασφάλειας προς πελάτες και συνεργάτες.

Μέσα από την αναλυτική σύγκριση διαπιστώθηκε ότι η NIS2 δίνει ιδιαίτερη έμφαση στη διαχείριση κινδύνων, στη λογοδοσία της διοίκησης, στην αναφορά περιστατικών και στην επιχειρησιακή συνέχεια, ενώ το SOC 2 επικεντρώνεται κυρίως στην τεκμηρίωση και αξιολόγηση της αποτελεσματικότητας των ελέγχων ασφάλειας μέσω των Trust Services Criteria. Παρά τις διαφορές τους, και τα δύο πλαίσια προωθούν την υιοθέτηση βέλτιστων πρακτικών κυβερνοασφάλειας και την ανάπτυξη ώριμων μηχανισμών διακυβέρνησης.

8.2 Προτάσεις για μελλοντική έρευνα

Με την κυβερνοασφάλεια αλλά και την κανονιστική συμμόρφωση να αποτελούν συνεχώς αναπτυσσόμενα πεδία δημιουργούνται πολλά περιθώρια για μελλοντικές έρευνες.

Αρχικά, μπορεί να εξεταστεί η εφαρμογή NIS2 σε περαιτέρω κλάδους όπως της όπως της υγείας , των χρηματοπιστωτικών υπηρεσιών, της ενέργειας, με σκοπό την ανακάλυψη των σχετικών προκλήσεων .

Ακόμη , θα μπορούσε να ερευνηθεί το σχετικό κόστος της συμμόρφωσης σε συνδυασμό με το βαθμό ωριμότητας κυβερνοασφάλειας για οργανισμούς που έχουν εφαρμόσει πολλαπλά πλαίσια.

Επιπλέον , με την τεχνολογία AI να αποτελεί συνεχώς εξελισσόμενη τεχνολογία που εισχωρεί όλο και περισσότερο στην καθημερινότητα αναμένεται το πεδίο της κυβερνοασφάλειας να αλλάξει δραματικά στο κοντινό μέλλον το οποίο θα επιφέρει ταχείες αλλαγές σε συμμορφώσεις και κανονισμούς.

Τέλος, η εξέταση της αλληλεπίδρασης μεταξύ των νέων ευρωπαϊκών κανονισμών όπως DORA , CSRD με τα τωρινά πλαίσια κυβερνοασφάλειας καθώς και η μελέτη της επίδραση τους στην στρατηγική διαχείρισης κινδύνων του εκάστοτε οργανισμού αποτελεί ιδιαίτερα ενδιαφέρουσα μελέτη.

9. Βιβλιογραφία

[1]https://www.ibm.com/think/topics/cybersecurity

[2] https://onlinedegrees.sandiego.edu/top-cyber-security-threats/

[3] https://www.kriptos.io/en-post/the-importance-of-regulatory-compliance-according-to-information-security

[4] https://cynomi.com/learn/regulatory-compliance/

[5] https://www.sentinelone.com/cybersecurity-101/cybersecurity/cyber-security-framework/

[6] https://www.veeam.com/blog/nis2-directive-explained.html

[7] https://www.dataguard.com/nis2/requirements/

[8] https://optro.ai/blog/soc-2-framework-guide-the-complete-introduction

[9] https://www.vanta.com/collection/soc-2/what-is-soc-2

[10] https://copla.com/blog/compliance-regulations/nis2-vs-soc2-eu-directive-meets-u-s-framework-key-differences-explained/

[11] https://www.fortinet.com/uk/resources/cyberglossary/smb-cybersecurity-tools

[12] https://www.ibm.com/think/topics/grc

[13] https://www.atlassian.com/blog/work-management/risk-management-tools

[14] https://www.netwitness.com/blog/top-incident-response-tools/

[15] https://www.hubifi.com/blog/automated-audit-readiness-tools

[16] https://isecuredata.com/future-of-compliance/

[17] https://xmcyber.com/navigating-the-new-era-of-cyber-compliance/

[18] https://www.imd.org/blog/sustainability/csrd/

[19] https://openssf.org/public-policy/eu-cyber-resilience-act/