ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΛΟΠΟΝΝΗΣΟΥ
University of the Peloponnese

ΣΧΟΛΗ ΟΙΚΟΝΟΜΙΑΣ ΚΑΙ ΤΕΧΝΟΛΟΓΙΑΣ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ

ΠΜΣ ΣΤΗΝ ΕΠΙΣΤΗΜΗ ΥΠΟΛΟΓΙΣΤΩΝ

Διπλωματική Εργασία

Κυβερνοεπιθέσεις σε επιχειρήσεις και οργανισμούς:

Στρατηγικές μετριασμού και ανάκαμψης

Κατερίνα Μουρλά

Α.Μ.: 2022202402010

Επιβλέπων:

καθηγητής Κώστας Βασιλάκης

Τρίπολη, Μάιος 2026

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

Ευρετήριο Σχημάτων

Ευρετήριο Πινάκων

Περίληψη

Η αυξανόμενη ένταση και οι σοβαρές επιπτώσεις των κυβερνοεπιθέσεων αναδεικνύουν την ανάγκη για διαμόρφωση αξιόπιστων στρατηγικών ανάκαμψης που θα διασφαλίσουν την ανθεκτικότητα των επιχειρήσεων και των οργανισμών.

Η εργασία αυτή αφορά τις στρατηγικές ανάκαμψης από κυβερνοεπιθέσεις σε επιχειρήσεις και οργανισμούς. Μέσω της διαθέσιμης βιβλιογραφίας, αναλύονται τα είδη των κυβερνοεπιθέσεων, τα κίνητρα για τη διενέργειά τους, οι τρόποι εκτέλεσής τους, οι επιπτώσεις των κυβερνοεπιθέσεων, καθώς και οι σχετικές προτάσεις που περιλαμβάνονται στα διεθνή κανονιστικά πρότυπα. Μέσα από την μελέτη περιπτώσεων και τη συγκριτική ανάλυσή τους θα διερευνηθούν οι στρατηγικές ανάκαμψης που χρησιμοποιήθηκαν και ο βαθμός που οι προκλήσεις αντιμετωπίστηκαν κατά τη φάση της αποκατάστασης.

Στόχος της εργασίας είναι να εξαχθούν συμπεράσματα για τα κοινά μοτίβα και τις ανάγκες επιτυχούς προσαρμογής των στρατηγικών ανάκαμψης, ανάλογα με τις ιδιαιτερότητες του στόχου και τις πιθανές επιπτώσεις που διακυβεύονται.

Λέξεις κλειδιά:

Κυβερνοεπιθέσεις, Κυβερνοασφάλεια, Μετριασμός, Ανάκαμψη, Ανθεκτικότητα, Επιχειρησιακή συνέχεια, Πλαίσια Κυβενοασφάλειας.

Abstract

The increasing intensity and the important consequences of cyberattacks highlight the need for the formulation of reliable recovery strategies that will ensure the resilience of enterprises and organizations.

This thesis focuses on strategies for recovering from cyber-attacks against enterprises and organizations. The types of cyber-attacks, the motives behind them, the methods for their implementation, the consequences associated with them, as well as the relevant recommendations in international regulatory frameworks are analyzed using the available bibliography. Through the study of use cases and their comparative analysis, we investigate the recovery strategies employed and the degree to which challenges were faced during the recovery phase.

The goal of this thesis is to draw conclusions on common patterns and the need for successful adaptation of recovery strategies, taking into account the particular characteristics of the target and the potential repercussions.

Keywords:

Cyber-attacks, Cybersecurity, Mitigation, Recovery, Resilience, Business continuity, Cybersecurity frameworks.

1 Εισαγωγή

Οι κυβερνοεπιθέσεις αυξάνονται και απειλούν κρίσιμα περιουσιακά στοιχεία των οργανισμών και των επιχειρήσεων, πλήττουν την φήμη και την αξιοπιστία τους, οδηγούν σε οικονομικές επιπτώσεις, άμεσες (διακοπή επιχειρησιακής συνέχειας, πρόστιμα) και μακροπρόθεσμες (απώλεια πελατείας, συνεργασιών). Για τον λόγο αυτό, δεν θα πρέπει να αντιμετωπίζονται ως μια περιφερειακή απειλή της επιχειρησιακής δραστηριότητας, αλλά σαν έναν σημαντικό κίνδυνο που μπορεί να πλήξει τον πυρήνα της επιχείρησης (Balzano & Marzi, 2025).

Καθώς η ψηφιοποίηση των λειτουργιών και των δεδομένων επεκτείνεται, οι κυβερνοεπιθέσεις παραμένουν μια ασύμμετρη απειλή. Οι επιχειρήσεις και οι οργανισμοί, δημόσιοι και ιδιωτικοί, καλούνται να διαμορφώσουν στρατηγικές μετριασμού και ανάκαμψης προκειμένου να την αντιμετωπίσουν. Μέσω των στρατηγικών τίθενται στόχοι, κατανέμονται πόροι, επιλέγονται δράσεις και καθορίζεται ο τρόπος οργάνωσης και εποπτείας της υλοποίησης τους από τη διοίκηση. Για τη διαμόρφωση των στρατηγικών αλλά και την επιλογή και υλοποίηση δράσεων, οι διοικήσεις των οργανισμών μπορούν να ανατρέξουν στα πλαίσια και τα πρότυπα κυβερνοασφάλειας, τα οποία παρέχουν σημαντική υποστήριξη για τις κατευθύνσεις αυτές.

Στην παρούσα εργασία μελετάται το ζήτημα των στρατηγικών ανάκαμψης από κυβερνοεπιθέσεις σε επιχειρήσεις και οργανισμούς. Ειδικότερα, καταγράφονται τα είδη των κυβερνοεπιθέσεων, εξετάζονται τα κίνητρα για τη διενέργειά τους, οι τρόποι εξάπλωσης και οι επιπτώσεις τους, ενώ αναλύονται και οι σχετικές προτάσεις που περιλαμβάνονται στα διεθνή κανονιστικά πρότυπαμε τη βοήθεια της διαθέσιμης βιβλιογραφίας. Μέσα από την μελέτη περιπτώσεων και τη συγκριτική ανάλυσή τους θα διερευνηθούν οι στρατηγικές ανάκαμψης που χρησιμοποιήθηκαν και ο βαθμός που οι προκλήσεις αντιμετωπίστηκαν κατά τη φάση της αποκατάστασης.

Στόχος της εργασίας είναι να εξαχθούν συμπεράσματα για τα κοινά μοτίβα και τις ανάγκες επιτυχούς προσαρμογής των στρατηγικών ανάκαμψης, ανάλογα με τις ιδιαιτερότητες του στόχου και τις πιθανές επιπτώσεις που διακυβεύονται.

Το κείμενο της διπλωματικής εργασίας είναι δομημένο ως ακολούθως:

Στο κεφάλαιο 2 παρουσιάζεται το θεωρητικό πλαίσιο των κυβερνοεπιθέσεων, συμπεριλαμβάνοντας τις βασικές έννοιες, τα κίνητρα πίσω από αυτές, τα συνήθη είδη κυβερνοεπιθέσεων, τους τρόπους διενέργειάς τους, τις συνέπειές τους και το κόστος που σχετίζεται με αυτές, το νομικό και κανονιστικό πλαίσιο που διέπει την περιοχή της κυβερνοασφάλειας.

Το κεφάλαιο 3 εστιάζει στη διαμόρφωση στρατηγικών μετριασμού επιπτώσεων και ανάκαμψης, καλύπτοντας τον πλήρη κύκλο ζωής τους από την προετοιμασία έως την ανατροφοδότηση, τον έλεγχο και τη βελτίωση.

Στο κεφάλαιο 4 παρουσιάζονται μελέτες περίπτωσης κυβερνοεπιθέσεων, αναδεικνύονται ζητήματα μετριασμού και κοινά μοτίβα επιθέσεων.

Τέλος, στο κεφάλαιο 5 παρατίθεται σύνοψη της διπλωματικής εργασίας και εξάγονται συμπεράσματα.

2 Θεωρητικό πλαίσιο

2.1 Βασικές Έννοιες

2.1.1 Κυβερνοεπίθεση

Το National Institute of Standards and Technology (NIST) ορίζει ως κυβερνοεπίθεση «οποιουδήποτε είδους κακόβουλη δραστηριότητα που επιχειρεί να συλλέξει, να διαταράξει, να αρνηθεί, να υποβαθμίσει ή να καταστρέψει πόρους του συστήματος πληροφοριών ή τις ίδιες τις πληροφορίες»[1].

Με βάση τον ορισμό της Cybersecurity and Infrastructure Security Agency (CISA) μια κυβερνοεπίθεση είναι η σκόπιμη και κακόβουλη προσπάθεια για παραβίαση ενός πληροφοριακού συστήματος[2].

2.1.2 Κυβερνοασφάλεια (Cybersecurity) και Κυβερνοανθεκτικότητα (Cyber resilience)

Η κυβερνοασφάλεια και η κυβερνοανθεκτικότητα είναι δυο αλληλοσυμπληρούμενες έννοιες, βασικές για τη διαμόρφωση μιας αποτελεσματικής στρατηγικής έναντι των κυβερνοεπιθέσεων (NIST, 2021a). Η κυβερνοασφάλεια αφορά την πρόληψη, την αποτροπή των παραβιάσεων και την προστασία της διαθεσιμότητας, ακεραιότητας και εμπιστευτικότητας των συστημάτων και των πληροφοριών που αυτά επεξεργάζονται (NIST, 2018b).

Η κυβερνανθεκτικότητα αναφέρεται στη δυνατότητα ενός οργανισμού να παραμένει λειτουργικός ακόμη και όταν μια κυβερνοεπίθεση επιτύχει. Η αντίληψη της κυβερνοανθεκτικότητας ξεκινά από την έννοια της επιχειρηματικής αξίας που δημιουργεί η λειτουργία ενός οργανισμού, η οποία και θα πρέπει να διασφαλιστεί. Τα ανθεκτικά συστήματα σχεδιάζονται με τη λογική να αποτυγχάνουν με ελεγχόμενο τρόπο, έτσι ώστε οι οργανισμοί να τροποποιούν τους μηχανισμούς λειτουργίας τους εν όψει δυσμενών καταστάσεων, να περιορίζουν την υφιστάμενη ζημιά και να αποκαθιστούν την κανονική λειτουργία σε εύλογο χρόνο (Björck et al., 2015).

2.1.3 Μετριασμός και Ανάκαμψη

Ο μετριασμός (mitigation) στο πλαίσιο της κυβερνοασφάλειας αφορά την προετοιμασία ενός συστήματος για να είναι ανθεκτικό. Σύμφωνα με το Πλαίσιο Κυβερνοασφάλειας NIST 2.0 του 2024

[1] https://csrc.nist.gov/glossary/term/cyber_attack
[2] https://niccs.cisa.gov/resources/glossary

ο μετριασμός αναφέρεται στα προληπτικά μέτρα που λαμβάνονται για την αναστολή της εξάπλωσης και την μείωση των επιπτώσεων μιας κυβερνοεπίθεσης (NIST, 2025a).

Η ανάκαμψη (recovery), σύμφωνα με το ίδιο πλαίσιο, αφορά την αποκατάσταση της κανονικής λειτουργίας ενός οργανισμού. Πέρα από τις λειτουργικές επιπτώσεις, επιπτώσεις μπορούν να επέλθουν και στο επίπεδο της φήμης ενός οργανισμού (ENISA, 2010; NIST, 2025a). Σε μια πιο διευρυμένη προσέγγιση, ένας οργανισμός που έχει δεχτεί κυβερνοεπίθεση, συμπληρωματικά προς την αποκατάσταση των λειτουργιών του, θα πρέπει να επιδιώξει και την αποκατάσταση της φήμης και της αξιοπιστίας του.

2.2 Κίνητρα κυβερνοεπιθέσεων – Φορείς απειλών

Ο κυβερνοχώρος δεν αφορά μόνο τεχνολογικές υποδομές αλλά και ανθρώπους -μεμονωμένα άτομα ή οργανωμένες ομάδες- οι οποίοι είναι δυνατό να προβαίνουν στις κυβερνοεπιθέσεις έχοντας ως υπόβαθρο οικονομικές επιδιώξεις, γεωπολιτικές συγκρούσεις, κοινωνικές εντάσεις και πολιτισμικές διαφορές (Gandhi et al., 2011).

2.2.1 Κίνητρα κυβερνοεπιθέσεων

Το κίνητρο, η ικανότητα και η ευκαιρία θα πρέπει να συνυπάρξουν προκειμένου μια δυνητική απειλή να γίνει πραγματικότητα. Η ικανότητα και οι πόροι του επιτιθέμενου, οι ευκαιρίες και οι διαφαινόμενες επιπτώσεις μιας επίθεσης, διαμορφώνουν το μέγεθος της απειλής. Ωστόσο το κίνητρο αποτελεί το σημείο εκκίνησης μιας κακόβουλης δραστηριότητας (Homoliak et al., 2018; G. Sharma et al., 2021).

Η απόσπαση χρημάτων μέσω εκβιασμού για την ανάκτηση δεδομένων, η πώληση πληροφοριών στο σκοτεινό διαδίκτυο (dark web), η εκμετάλλευση κλεμμένης πνευματικής ιδιοκτησίας, η κατασκοπεία σε βάρος ανταγωνιστικών εταιριών, είναι κάποιες από τις δραστηριότητες που αποφέρουν οικονομικό όφελος στους δράστες (Europol, 2024; Everett, 2016; Kshetri, 2006; Spanca & Salihu, 2024).

Από την άλλη πλευρά, κρατικές και κρατικά κατευθυνόμενες κυβερνοεπιθέσεις έχουν χρησιμοποιηθεί για την αποδυνάμωση κρίσιμων υποδομών, την υποκλοπή τεχνογνωσίας, την κατασκοπεία αλλά και την επίδειξη ισχύος (Smeets, 2018). Στις επιθέσεις με γεωπολιτικά κίνητρα φαίνεται να επικρατεί ως κίνητρο η βούληση για πράξεις δολιοφθοράς, κατασκοπείας και υπονόμευσης, οι οποίες δεν συνοδεύονται από τις φυσικές απώλειες των «παραδοσιακών» μορφών πολέμου (Rid, 2011).

Μια άλλη κατηγορία κινήτρων εδράζεται στο το ιδεολογικό/ηθικό υπόβαθρο των δραστών. Άτομα ή ομάδες χρησιμοποιούν τεχνικές hacking με στόχο να δημοσιοποιήσουν τις θέσεις τους, να ευαισθητοποιήσουν την κοινή γνώμη ή να ασκήσουν πίεση σε εταιρίες και κρατικούς οργανισμούς. Με βάση τα δεδομένα που συλλέχθηκαν από συνεντεύξεις που ελήφθησαν από 28 ενεργούς hackers, το πιο διαδεδομένο έναυσμα για την δράση τους, ήταν η παραβίαση των αξιών και των πεποιθήσεων τους από κράτη ή εταιρίες (καταπιεστική άσκηση εξουσίας, διαφθορά, αδιαφορία για το οικοσύστημα κ.λπ.), ακόμη και αν δεν ήταν οι ίδιοι οι άμεσα θιγόμενοι (Romagna & Leukfeldt, 2023).

Ένα κίνητρο ενταγμένο άλλοτε σε εθνικά κατευθυνόμενες ενέργειες και άλλοτε στην ιδεολογία είναι η τρομοκρατία. Ωστόσο η τρομοκρατία στον κυβερνοχώρο, ως αιτία και σκοπός, πέραν από προφανείς περιπτώσεις που θα μπορούσαν να επηρεάσουν άμεσα τους πολίτες, ενδέχεται να αποδίδεται με υποκειμενικούς όρους αν εμπλέκονται εθνικές ή πολιτικές αντιπαραθέσεις. Δραστηριότητες κυβερνοεπιθέσεων σε βάρος οργανισμών «αντιπάλων» κρατών, μπορεί να χαρακτηριστούν είτε ως πατριωτικές ή πολιτικές ενέργειες είτε ως τρομοκρατικές, καθώς στην περίπτωση αυτή η αξιολόγηση γίνεται με βάση το εθνικό ή το ιδεολογικό πλαίσιο (Gandhi et al., 2011; Nye, 2010; Sailio et al., 2020).

Κάποιοι hackers, παρακινούνται από ψυχολογικά κίνητρα όπως η επιθυμία ενός δυσαρεστημένου υπαλλήλου να βλάψει τον οργανισμό που εργάζεται ή εργαζόταν (ENISA, 2020). Επίσης, η αντίληψη ότι το hacking είναι διασκέδαση, η συγκίνηση της πρόκλησης, η ανάγκη για κοινωνικοποίηση (με άλλους hackers) και η επιδίωξη του σεβασμού από τον κύκλο των συνομήλικων ή του κύκλου των hackers, μπορεί να οδηγήσουν νεαρά κυρίως άτομα να εμπλακούν σε κυβερνοεπιθέσεις (Kshetri, 2006). Ο Πίνακας 1 συνοψίζει τις κατηγορίες κινήτρων κυβερνοεπιθέσεων και της συνήθεις επιδιώξεις κάθε κατηγορίας.

Οικονομικά κίνητρα	• απόσπαση χρημάτων μέσω εκβίασης ή πώλησης δεδομένων, εκμετάλευση κλεμμένης πνευματικής ιδιοκτησίας, κατασκοπεία σε βάρος ανταγωνιστών κ.λπ.
Γεωπολιτικά κίνητρα	• επίδειξη δύναμης, σαμποτάζ, υποκλοπή πληροφοριών ή τεχνογνωσίας , υπονόμευση
Ιδεολογικά κίνητρα	• προβολή θέσεων, διαμαρτυρία
Ψυχολογικά κίνητρα	• εκδίκηση, μνησικακία • προβολή ικανοτήτων ή προσωπική ικανοποίηση

Πίνακας 1. Κίνητρα κυβερνοεπιθέσεων.

Αρκετές φορές μπορούν να συνυπάρχουν διαφορετικά κίνητρα. Για παράδειγμα, η επιθυμία για εκδίκηση από την πλευρά ενός δυσαρεστημένου/απολυμένου υπαλλήλου θα μπορούσε να συνυπάρξει με οικονομικά ή ιδεολογικά κίνητρα (Chng et al., 2022).

Σε έκθεση της Ομοσπονδιακής Υπηρεσίας Ασφάλειας Πληροφοριακών Συστημάτων της Γερμανίας[3], σημειώνεται η ενδιαφέρουσα παρατήρηση ότι σε μια σειρά από επιθέσεις σε βάρος κρατικών φορέων, στις οποίες οι επιτιθέμενοι προέβαλαν οικονομικές απαιτήσεις, είναι πιθανόν οι απαιτήσεις αυτές να κάλυπταν ιδεολογικά κίνητρα, γεωπολιτικά ή κίνητρα αναγνώρισης και προβολής. Αυτό βασίζεται στην εκφρασμένη πρόθεση των θεσμών να μην καταβάλουν λύτρα σε κυβερνοεγκληματίες. Η έκθεση αναγνωρίζει πως το κίνητρο του επιτιθέμενου μπορεί να διαφοροποιήσει την πορεία και την διαχείριση μιας επίθεσης, παρ' όλα αυτά δεν είναι πάντα ξεκάθαρο (BSI, 2023).

[3] σελ.15, Die Lage der IT-Sicherheit in Deutschland 2023, Bundesamt für Sicherheit in der Informationstechnik.

2.2.2 Φορείς απειλών (Cyber Threat Actors (CTAs))

Οι φορείς των απειλών διαθέτουν ασύμμετρο προβάδισμα έναντι των στόχων τους εφόσον η πληροφόρησή τους υπερτερεί. Η ταξινόμηση των φορέων απειλής εξυπηρετεί την εκτίμηση κινδύνου και την σχεδίαση των επιλογών άμυνας ενός οργανισμού. Οι κίνδυνοι είναι δυνατό να προέρχονται από το εσωτερικό των οργανισμών (insider threats), το κυβερνοέγκλημα, αντίπαλα κράτη, ομάδες ιδεολογικά υποκινούμενες ή από συνεργασίες φορέων απειλής (Mavroeidis et al., 2021; Nye, 2010).

2.2.2.1 Εσωτερικές Απειλές (Insider Threats)

Στην περίπτωση εκδήλωσης εσωτερικής απειλής, νυν ή πρώην υπάλληλοι και συνεργάτες, μπορεί να χρησιμοποιήσουν τη γνώση που κατέχουν για να αλλοιώσουν πληροφορίες, να υποκλέψουν δεδομένα ή να επηρεάσουν την διαθεσιμότητα ενός πληροφοριακού συστήματος. Οι εσωτερικές απειλές περιλαμβάνουν και τους κινδύνους που οφείλονται σε αμέλεια, αδράνεια, ελλιπή εκπαίδευση ή παράκαμψη των πρωτοκόλλων ασφαλείας για λόγους ευκολίας ή απόδοσης, με συνέπεια την έκθεση από λανθασμένες ενέργειες (όπως η ανταπόκριση στην κοινωνική μηχανική και η χρήση μη ελεγμένου υλικού) που δεν οφείλονται σε κακόβουλη πρόθεση. Περιλαμβάνουν επίσης και την παραβίαση των κανόνων ασφαλείας στα πλαίσια του αυτόβουλου πειραματισμού (Homoliak et al., 2018; Inayat et al., 2024).

Οι συνεργάτες σπάνια εμπλέκονται ως άμεση απειλή σε κυβερνοεπιθέσεις τα προβλήματα κατά κανόνα προκύπτουν χωρίς να υπάρχει πρόθεση πρόκλησης βλάβης και έχουν να κάνουν με την εκμετάλλευση της πρόσβασής τους από κακόβουλους τρίτους (Sailio et al., 2020).

Ως κακόβουλες ενέργειες αναφέρονται η δολιοφθορά, η κατασκοπεία, η κλοπή δεδομένων ή πνευματικής ιδιοκτησίας. Τα κίνητρα των εσωτερικών απειλών παρουσιάζουν σημαντική ποικιλομορφία. Είναι δυνατόν δυσαρεστημένοι υπάλληλοι να λειτουργήσουν εκδικητικά. Είναι επίσης πιθανό, κάποιοι υπάλληλοι λόγω ιδεολογίας να θεωρήσουν ότι ο οργανισμός δεν αντιμετωπίζει σωστά μια υπόθεση τοπικού ή ευρύτερου ενδιαφέροντος. Εργαζόμενοι μπορεί να επιδιώξουν οικονομικό όφελος από την πώληση κλεμμένων πληροφοριών. Επίσης η ένταση του κινδύνου διαφέρει ως προς το επίπεδο του στελέχους που αποτελεί απειλή: έμπειροι χρήστες και διαχειριστές αποτελούν σοβαρότερες απειλές από άπειρους χρήστες και στελέχη με περιορισμένα δικαιώματα πρόσβασης στις λειτουργίες και τα συστήματα ενός οργανισμού (Homoliak et al., 2018; Hunker & Probst, 2011; Inayat et al., 2024).

Οι φορείς των εσωτερικών απειλών (εργαζόμενοι ή συνεργάτες) εκτός από εξουσιοδοτημένοι χρήστες μπορεί να είναι και πρόσωπα που εκμεταλλεύονται μια ευκαιρία μη εξουσιοδοτημένης πρόσβασης. Ο εντοπισμός των εσωτερικών απειλών δυσχεραίνεται από το γεγονός ότι οι επιτιθέμενοι είναι άτομα εμπιστοσύνης και οι κακόβουλες ενέργειες συνυπάρχουν με τη φυσιολογική τους δραστηριότητα. επίσης, κατά κανόνα είναι γνώστες των πρωτοκόλλων ασφαλείας, και αξιοποιούν αυτές τις γνώσεις για να καλύψουν τα ίχνη τους (Homoliak et al., 2018; Nour et al., 2023).

Μοντέλα που έχουν προταθεί για την πρόγνωση κινδύνου αναφέρονται σε ψυχοκοινωνικά δεδομένα των υπαλλήλων όπως η έκφραση δυσαρέσκειας, η άρνηση αποδοχής κριτικής, τα προσωπικά θέματα, η αποστασιοποίηση από την ομάδα, η σύνταξη αρνητικών αξιολογήσεων από τους προϊσταμένους τους ή η απόλυσή τους κ.ά. (Greitzer & Frincke, 2010). Η χρήση της τεχνητής νοημοσύνης και της μηχανικής μάθησης για την ανίχνευση ασυνήθιστης συμπεριφοράς από πλευράς των εργαζομένων, δεν είναι απρόσκοπτη, καθώς η διάκριση ανάμεσα στη νόμιμη/κανονική συμπεριφορά και την αδικαιολόγητη απόκλιση δεν μπορεί πάντοτε να γίνει με ασφάλεια, εφόσον οι απαιτήσεις και οι ρόλοι (και άρα το σύνολο των νομότυπων ενεργειών) μεταβάλλονται δυναμικά. Ψευδείς θετικές αναφορές μπορεί να πλήξουν την αξιοπιστία του μηχανισμού εντοπισμού απειλών. Επίσης τα κρυπτογραφημένα κανάλια επικοινωνίας αποτελούν ένα τεχνικό εμπόδιο για την ανίχνευση εσωτερικών απειλών σε πραγματικό χρόνο (Alzaabi & Mehmood, 2024).

Ένα άλλο θέμα που προκύπτει, είναι πως η αίσθηση της συνεχούς επιτήρησης και πολύ περισσότερο τυχόν κατηγορίες βασιζόμενες σε ψευδώς θετικές αναφορές, μπορεί να δημιουργήσουν ένα δυσμενές εργασιακό περιβάλλον, να βλάψουν την εικόνα ενός οργανισμού αλλά και να οδηγήσουν σε νομικές συνέπειες (Hunker & Probst, 2011).

2.2.2.2 Εξωτερικές Απειλές

2.2.2.2.1 Κυβερνοέγκλημα

Στο περιβάλλον του διαδικτύου η ανωνυμία και η απομακρυσμένη πρόσβαση δυσχεραίνουν τον εντοπισμό όσων έχουν παραβατική συμπεριφορά αλλά και την απόδοση ευθυνών. Το πλαίσιο αυτό μειώνει τον κίνδυνο για τους κυβερνοεγκληματίες (Kshetri, 2006), τόσο τον πραγματικό, όσο και τον αντιλαμβανόμενο (perceived). Επαγγελματίες της πληροφορικής αλλά και ταλαντούχοι νεαροί προσελκύονται από το κυβερνοέγκλημα για να κερδίσουν χρήματα δρώντας είτε ατομικά, είτε ως μισθοφόροι, είτε ενταγμένοι σε οργανωμένες ομάδες. Παράγοντες όπως οι δυσμενείς προοπτικές απασχόλησης, σε χώρες που πλήττονται από οικονομική κρίση και η απληστία που προκαλεί η

αποδοτικότητα του κυβερνοεγκλήματος ενισχύουν την εμφάνιση παραβατικών συμπεριφορών (Gandhi et al., 2011; Kshetri, 2006).

Σύμφωνα με τη Europol, το έγκλημα στον κυβερνοχώρο έχει εξελιχθεί σε μια οργανωμένη αγορά που εκμεταλλεύεται την κάλυψη που εξασφαλίζουν οι συναλλαγές με κρυπτονομίσματα και η πρόσβαση μέσω κρυπτογραφημένων δικτύων στο σκοτεινό διαδίκτυο (Europol, 2021).Το κυβερνοέγκλημα δεν αφορά μόνο μεμονωμένες ενέργειες, αλλά και μια αγορά ανταλλαγής και πώλησης δεδομένων, πόρων και υπηρεσιών από ειδικευμένους επαγγελματίες, που αναπτύσσεται στο σκοτεινό διαδίκτυο. Η έκθεση της Europol για το 2025 για τα αγαθά και τις υπηρεσίες που γίνονται αντικείμενα αγοραπωλησιών στο ψηφιακό περιβάλλον του Dark Web, αναφέρει μεταξύ άλλων ότι σε αυτό διατίθενται:

- εγχειρίδια και σεμινάρια για απάτες,
- κακόβουλο λογισμικό (malware) που προσφέρεται προς πώληση ή μπορεί να δοθεί με συνδρομή ή ακόμη και να κατασκευαστεί επί παραγγελία από δημιουργούς κακόβουλου λογισμικού. Επιπλέον παρέχονται διευκολύνσεις ransomware, παροχή υπηρεσιών phishing, υπηρεσίες ανακάλυψης ευπαθειών σε λογισμικό και δίκτυα, κ.λπ.,
- διαχείριση ή πώληση botnets,
- υπηρεσίες κλοπής διαπιστευτηρίων (Initial Access Brockers),
- εξαγωγή δεδομένων προς πώληση (Data Brockers),
- παροχή υπηρεσιών υποστήριξης σε παράνομες ενέργειες (μεσίτες, διαπραγματευτές, υπηρεσίες ξεπλύματος χρημάτων κ.λπ.),
- forums αλληλεπίδρασης, πωλήσεων, διαφήμισης και αξιολόγησης υπηρεσιών.

Τα ανωτέρω συνθέτουν ένα πολύπλοκο οικοσύστημα αγαθών, υπηρεσιών και επαγγελματιών που προσαρμόζεται στους κανόνες της προσφοράς και της ζήτησης και απευθύνεται σε πελάτες με ποικίλα επίπεδα τεχνογνωσίας (Europol, 2025).

2.2.2.2.2 Κρατικοί φορείς και κρατικά κατευθυνόμενες ομάδες

Ο κρατικές και κρατικά κατευθυνόμενες κυβερνοεπιθέσεις εξασφαλίζουν σημαντικά οφέλη για τα κράτη, γεγονός που οδηγεί τις κρατικές οντότητες να επενδύουν σημαντικούς πόρους, με αποτέλεσμα οι συγκεκριμένες επιθέσεις να είναι επιμελημένες, να αξιοποιούν εξελιγμένες τεχνικές με υψηλό επίπεδο πολυπλοκότητας, να υποστηρίζουν στρατηγικούς στόχους και να είναι αποτελεσματικές, ενώ αρκετές φορές μπορεί να εξελίσσονται σε μακροπρόθεσμο ορίζοντα (Canadian Centre for Cyber Security, 2022).

Οι επιθέσεις αυτές δεν υπόκεινται σε γεωγραφικούς περιορισμούς, επιτρέποντας να πληγούν απομακρυσμένοι στόχοι. Το μέγεθος μιας χώρας δεν αποτελεί αποτρεπτικό παράγοντα για να αναπτύξει μια απειλή σε βάρος άλλης χώρας. Σε πολλές περιπτώσεις μπορούν μόνο να διατυπωθούν υποψίες και εικασίες σε σχέση με την προέλευση των κυβερνοεπιθέσεων και είναι δύσκολο να υπάρχει πλήρης καταλογισμός και να αποδοθούν ευθύνες (Smeets, 2018).

Εκτός από γεωπολιτικά κίνητρα, στα κράτη αποδίδονται και οικονομικά, στην περίπτωση που η στόχευση είναι η κλοπή πνευματικής ιδιοκτησίας για την απόκτηση οικονομικού πλεονεκτήματος, με χρήση ξένης τεχνογνωσίας (Microsoft, 2025).

2.2.2.2.3 Άτομα ή ομάδες με ιδεολογικά κίνητρα

Η κατηγορία αυτή περιλαμβάνει τόσο μεμονωμένα άτομα όσο και ομάδες που διαμορφώνονται στο πλαίσιο κοινών ιδεολογικών πεποιθήσεων και συντονίζονται ως προς τους με τους στόχους και τα μέσα που θα χρησιμοποιήσουν. Κοινή τους πεποίθηση είναι πως το hacking είναι ένας αποτελεσματικός τρόπος δημοσιοποίησης θέσεων και άσκησης πίεσης προς την επίτευξη του εκάστοτε στόχου. Τα κίνητρά τους εκτός από ιδεολογικά μπορεί να περιλαμβάνουν την εκδίκηση ή την αντίδραση σε πτυχές της πολιτικής ή κοινωνικής ζωής στις οποίες οι δρώντες θεωρούν ότι υφίστανται αδικίες (Sailio et al., 2020).

Οι ομάδες αυτές επιτυγχάνουν δημοσιότητα για τις επιθέσεις τους, αλλά οι τεχνικές τους δυνατότητες θεωρούνται μέτριες (Canadian Centre for Cyber Security, 2022).

2.2.2.2.4 Ανταγωνιστές

Οργανισμοί που δραστηριοποιούνται σε ανταγωνιστικούς κλάδους επιδίδονται σε βιομηχανική κατασκοπεία, η οποία περιλαμβάνει την συλλογή επιχειρησιακών πληροφοριών και την κλοπή πνευματικής ιδιοκτησίας με σκοπό να αποκτηθεί ανταγωνιστικό πλεονέκτημα με σημαντικό οικονομικό όφελος. Οι ανθρώπινες αστοχίες [4] και η συνεργασία με εσωτερικούς χρήστες διευκολύνουν την κατασκοπεία (Hou & Wang, 2020; Moschovitis, 2018).

Στο σύγχρονο επιχειρηματικό πλαίσιο, η απειλή της εταιρικής κατασκοπείας ενισχύεται από παράγοντες όπως οι ψηφιακές ευαλωτότητες, οι αθέμιτες συμπράξεις ανταγωνιστών με εσωτερικούς χρήστες και η καθυστέρηση προσαρμογής της νομοθεσίας στις νέες απειλές (Kozłowski, 2025). Οι

[4] Σύμφωνα με την εργασία (Hou & Wang, 2020), μια πηγή που χρησιμοποιούν οι επιτιθέμενοι για άντληση πληροφοριών είναι τα Διαδικτυακά Κοινωνικά Δίκτυα (Online Social Networks - OSN), τα οποία πολλές επιχειρήσεις χρησιμοποιούν για επικοινωνία των υπαλλήλων τους.

άμεσοι δρώντες δυνητικά μπορεί να είναι ομάδες του κυβερνοεγκλήματος, που διαθέτουν την τεχνογνωσία και την ικανότητα να στοχεύουν υψηλής αξίας στόχους. Το πλαίσιο κυβερνοασφάλειας MITRE ATT&CK αναφέρει μεταξύ άλλων παραγόντων κινδύνου και οργανωμένες ομάδες που ειδικεύονται στην βιομηχανική κατασκοπεία[5].

2.2.2.2.5 Δρώντες σε αναζήτηση συναρπαστικών περιπετειών

Πρόκειται για άτομα των οποίων τα κίνητρα τους περιλαμβάνουν τη δοκιμή δυνατοτήτων, την περιέργεια, τη διασκέδαση, καθώς και την προβολή/επίδειξη της αξίας τους. Μεταξύ των ατόμων αυτών, οι «Script kiddies» είναι οι λιγότερο έμπειροι καθώς οι τεχνικές τους δυνατότητες είναι περιορισμένες και χρησιμοποιούν εργαλεία που έχουν αναπτύξει άλλοι. Η ικανότητα ανίχνευσης και αποτροπής απειλών που προέρχονται από αυτή την ομάδα, είναι η ελάχιστη που θα πρέπει να έχουν τα συστήματα ενός οργανισμού (Sailio et al., 2020). Είναι βέβαια επιθυμητό τα συστήματα να διαθέτουν πιο προηγμένες δυνατότητες άμυνας.

2.2.2.3 Υβριδικές Απειλές

Σε κάποιες περιπτώσεις συναντάμε υβριδικές απειλές, στις οποίες υπάρχει συνεργασία μεταξύ εσωτερικών και εξωτερικών φορέων απειλής. Στη βιβλιογραφία, εκτός από την περίπτωση της στρατολόγησης, αναφέρεται η περίπτωση της σκόπιμης τοποθέτησης σε έναν οργανισμό ενός υπαλλήλου – κατασκόπου, με σκοπό να διευκολύνει τις επιδιώξεις του πραγματικού φορέα απειλής (Homoliak et al., 2018).

Σύμφωνα με τον ENISA το κόστος μιας επίθεσης οδηγεί τους επιτιθέμενους να επιδιώκουν την σύμπραξη με εσωτερικούς συνεργάτες. Η έκθεση αναφέρει ότι η συνεργασία επιτυγχάνεται με εξαγορά, εκβιασμό ή παραπλάνηση των εργαζομένων ώστε να αποκαλύπτουν αξιοποιήσιμες πληροφορίες (ENISA, 2020).

2.2.3 Κατανομή κινήτρων και προέλευσης απειλών

Στην έκθεση της Verizon DBI 2025 κυριαρχεί το οικονομικό κίνητρο και ακολουθεί η κατασκοπεία με τα ποσοστά να διαφοροποιούνται ανά τομέα δραστηριότητας (Verizon, 2025). Ο κύριος όγκος των επιθέσεων, σε όλους τους τομείς δραστηριοτήτων, προέχεται κυρίως από το εξωτερικό περιβάλλον. Οι συνεργάτες αποτελούν τους κύριους δράστες σε πολύ μικρό ποσοστό, αν και η έκθεση επισημαίνει ότι η εμπλοκή τρίτων (π.χ. διαρροή από επαναχρησιμοποίηση διαπιστευτηρίων σε διαφορετικά

[5] https://attack.mitre.org/groups/

συστήματα) αυξήθηκε από 15% σε 30% σε σχέση με την προηγούμενη περίοδο, γεγονός που αναδεικνύει τους κινδύνους που προέρχονται από συνεργασίες και εξαρτήσεις.

Τομέας	Κίνητρο		Φορέας Απειλής (κύριος δράστης)		
	Οικονομικό	Κατασκοπεία	Εξωτερικός	Εσωτερικός	(Συνεργάτες)
Εκπαιδευτικές Υπηρεσίες	88%	18%	62%	38%	-
Χρηματοοικονομικά	90%	12%	78%	22%	1%
Λιανικό Εμπόριο	100%	9%	96%	3%	1%
Δημόσιος τομέας	76%	29%	67%	33%	1%

Πίνακας 2 Δεδομένα από την έκθεση της Verizon του 2025[6]

Αντίστοιχα η τελευταία έκθεση της Microsoft αναφέρει ότι περισσότερο από το 50% των κυβερνοεπιθέσεων αφορούσαν οικονομικούς στόχους αναφερόμενη σε εκείνες, που το κίνητρο είναι επιβεβαιωμένα οικονομικό (Microsoft, 2025).

Στον αντίποδα, με βάση την έκθεση του ENISA, η οποία επικεντρώνεται στην Ευρωπαϊκή Ένωση, το μεγαλύτερο μέρος των επιθέσεων (από το δεύτερο εξάμηνο του 2024 έως και το πρώτο του 2025) ήταν ιδεολογικά υποκινούμενες. Οι επιθέσεις με οικονομικά κίνητρα που καταγράφει η έκθεση ανέρχονται στο 13,4% του συνόλου και αποδίδονται κυρίως σε κυβερνοεγκληματίες. Από την άλλη πλευρά, η κυβερνοκατασκοπεία ανερχόταν μόλις στο 7,2 % (ENISA, 2025).

[6] Το άθροισμα των στηλών των κινήτρων υπερβαίνει το 100% ανά γραμμή καθώς ορισμένες περιπτώσεις επιθέσεων ανάγονται σε πολλαπλά κίνητρα.

Σχήμα 1. Κίνητρα κυβερνοεπιθέσεων (ENISA, 2025)

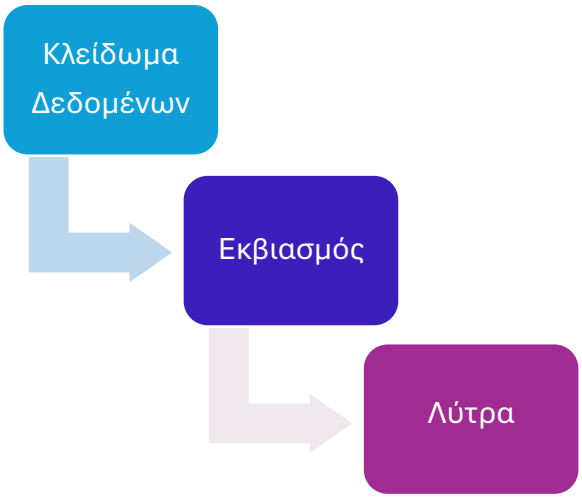
2.3 Διαδεδομένες Μορφές Επιθέσεων

2.3.1 Τεχνικές Επιθέσεις

2.3.1.1 Ransomware

Οι επιθέσεις Ransomware[7] αποτελούν μια κοινή απειλή και πλήττουν επιχειρήσεις και οργανισμούς κάθε μεγέθους. Το Ransomware κρυπτογραφεί αρχεία ή και ολόκληρο το σύστημα αποκόπτοντας τον οργανισμό από τα δεδομένα του. Στην συνέχεια ζητούνται λύτρα με αντάλλαγμα το κλειδί της αποκρυπτογράφησης. Η εκτέλεση ενός μολυσμένου αρχείου, που συχνά φθάνει στον οργανισμό ως συνημμένο σε ένα ηλεκτρονικό μήνυμα ή μέσω λήψης από έναν παραβιασμένο (ή κακόβουλο) ιστότοπο, μπορεί να οδηγήσει στη μόλυνση ενός συστήματος. Η μόλυνση με Ransomware είναι δυνατόν να προκληθεί σε ένα σύστημα κατόπιν εκμετάλλευσης μιας αδυναμίας του συστήματος, που οδηγεί σε παραβίαση.

[7] https://www.nist.gov/itl/smallbusinesscyber/guidance-topic/ransomware



Σχήμα 2. Ransomware

Στην ετήσια έκθεση του για το 2025, ο ENISA αναγνωρίζει το ransomware ως την απειλή με τις μεγαλύτερες συνέπειες ως προς το κόστος και τη συνέχεια λειτουργίας των επιχειρήσεων (ENISA, 2025). Στο πλαίσιο αυτό ο οργανισμός ENISA υποστηρίζει την πρωτοβουλία «No more Ransome»[8] για την παροχή δωρεάν υλικού αποκρυπτογράφησης στις επιχειρήσεις που έχουν πληγεί, ενθαρρύνοντας την απόρριψη του εκβιασμού. Η πρωτοβουλία αποτελεί σύμπραξη της Europol με ιδιωτικές εταιρίες. Άλλωστε η καταβολή λύτρων δεν εξασφαλίζει τα θύματα. Αναφέρονται περιπτώσεις, όπως αυτή του Δήμου της Riviera Beach το 2019 (Kayan et al., 2022), όπου αν και τα λύτρα καταβλήθηκαν, τα θύματα δεν έλαβαν το κλειδί της αποκρυπτογράφησης.

Η εξέλιξη του ransomware ενισχύθηκε από την αύξηση της σύνδεσης με το Διαδίκτυο, την πρόσβαση στα εργαλεία της κρυπτογράφησης που στο παρελθόν αποτελούσαν προνόμιο λίγων και την κυκλοφορία των κρυπτονομισμάτων που διευκολύνουν την ανώνυμη πληρωμή. Επίσης η ηλεκτρονική αποθήκευση σημαντικών δεδομένων αύξησε τα περιουσιακά στοιχεία των οργανισμών σε ψηφιακή μορφή. Επιπλέον, η εισαγωγή του μοντέλου RaaS (Ransomware-as-a-Service) στον χώρο του κυβερνοεγκλήματος επιτρέπει σε επιτιθέμενους χωρίς ιδιαίτερες τεχνικές δεξιότητες να κερδίζουν χρήματα αγοράζοντας τεχνογνωσία ransomware (O'Kane et al., 2018).

Πέρα από το «σύνηθες» ransomware υπάρχει και η παραλλαγή του *διπλού εκβιασμού* (double extortion) η οποία αποτελεί μια πιο σύνθετη μορφή ransomware, όπου οι επιτιθέμενοι δεν κλειδώνουν μόνο τα δεδομένα αλλά επιπλέον τα υποκλέπτουν, και έτσι τα θύματα δέχονται διπλό εκβιασμό: αφ' ενός καλούνται να καταβάλουν λύτρα για να μπορέσουν να αποκτήσουν πρόσβαση στα κλειδωμένα

[8] https://www.nomoreransom.org/el/index.html, https://www.enisa.europa.eu/topics/nomoreransom#:~:text=No%20More%20Ransom%20is%20the%20first%20public%2Dprivate,without%20having%20to%20pay%20the%20ransom%20amount , l.ac.03/01/26

δεδομένα ή συστήματά τους και αφ' ετέρου για να μην διαρρεύσουν δεδομένα. Με τον τρόπο αυτό, το στρατηγικό πλεονέκτημα των επιτιθέμενων αυξάνει, κυρίως εάν πρόκειται για σημαντικές ή ευαίσθητες πληροφορίες. Αν και ο ισχυρισμός της υποκλοπής δεδομένων δεν μπορεί να επιβεβαιωθεί, καθώς η δυνατότητα κρυπτογράφησης αρχείων δεν συνεπάγεται τη δυνατότητα υποκλοπής, η ασσυμετρία της πληροφόρησης είναι υπέρ του εισβολέα (Meurs et al., 2024).

2.3.1.2 Προηγμένη Επίμονη Απειλή (Advanced Persistent Threat-APT)

Οι επιθέσεις αυτού του είδους απαιτούν πόρους και υψηλού επιπέδου προσπάθεια από την πλευρά των επιτιθέμενων. Στόχοι αυτών των επιθέσεων είναι κατά κανόνα κρατικοί φορείς και μεγάλες εταιρίες που διαχειρίζονται δεδομένα υψηλής αξίας ή κρίσιμες υποδομές. Παρόλα αυτά και μικρότερες εταιρίες μπορεί να γίνουν στόχοι, στα πλαίσια της παραβίασης ενός οργανισμού δια μέσου των συνεργατών και των προμηθευτών του[9]. Ο Πίνακας 4 επεξηγεί τα χαρακτηριστικά του APT.

Προηγμένη (Advanced)	**Επίμονη** (Persistent)	**Απειλή** (Threat)
• Οι επιτιθέμενοι έχουν υψηλό τεχνολογικό υπόβαθρο και χρησιμοοποιούν εξελιγμένες τεχνικές.	• Οι εισβολείς μπορεί να παραμείνουν κρυμμένοι επί μακρόν χωρίς να ανιχνευθούν, καθώς έχουν την πρόθεση και την ικανότητά να επιβιώνουν απέναντι στις άμυνες ενός οργανισμού και να αλληλοεπιδρούν με τα συστήματά του, για μεγάλα χρονικά διαστήματα.	• Πρόκειται για συνεχή απειλή που στοχεύει υψηλής αξίας στόχους με σκοπό την κατασκοπεία, την κλοπή πνευματικής ιδιοκτησίας, την εξαγωγή οικονομικών ή απόρρητων δεδομένων, την υπονόμευση ενός οργανισμού ή την εγκατάσταση και προετοιμασία μια μελλοντικές κακόβουλες ενέργειες.

Πίνακας 3. APT[10]

Οι προηγμένες επίμονες απειλές, αποδίδονται σε ομάδες με υψηλό προφίλ τεχνογνωσίας. Σε αρκετές περιπτώσεις υπάρχει ευθεία απόδοση σε κράτη ή υπόνοια ότι οι ομάδες αυτές είναι κρατικά καθοδηγούμενες[11].

[9] https://www.kaspersky.com/resource-center/definitions/advanced-persistent-threats
[10] https://www.kaspersky.com/resource-center/threats/advanced-persistent-threat, https://csrc.nist.gov/glossary/term/advanced_persistent_threat
[11] https://attack.mitre.org/groups/

Οι ισχυροί μηχανισμοί ασφάλειας φαίνεται να μην έχουν τη δυνατότητα να εξαλείψουν τους κινδύνους των APT, αλλά καθιστούν τις ίδιες πιο περίπλοκες, καθώς οι επιτιθέμενοι διαθέτουν το χρόνο να μελετούν τον στόχο, τις άμυνες και τις ευπάθειες των συστημάτων του, εφαρμόζοντας πολύπλοκες τακτικές και αξιοποιώντας εξελιγμένο λογισμικό. Οι επιθέσεις αυτές χαρακτηρίζονται από αργές και προσεκτικά μελετημένες κινήσεις των εισβολέων. Σύμφωνα με τις εργασίες (Alshamrani et al., 2019; Chen et al., 2014; Tan et al., 2025), μια επίθεση *δεν θεωρείται ότι είναι APT* εάν (i) είναι προβλέψιμη και υπήρχαν πρόσφοροι και γνωστοί τρόποι αποτροπής, ή (ii) εάν δεν απαιτούσε αξιοσημείωτη προσπάθεια από τους επιτιθέμενους για να αποφύγουν τον εντοπισμό και (iii) εάν δεν παρουσιάζει καμία καινοτομία στις μεθόδους και τις τεχνικές. Ο Πίνακας 5 παρουσιάει μία σύγκριση μεταξύ APT και κοινών κυβερνοεπιθέσεων.

	APT	**Κοινές επιθέσεις**
Πόροι επιτιθέμενων	Υψηλοί	Περιορισμένοι
Κίνητρα	Στρατηγικά	Ευκαιριακά
Πολυπλοκότητα	Υψηλή	Περιορισμένη
Διάρκεια	Μακροχρόνια	Σύντομη
Πρόβλεψη / Ανίχνευση	Πολύ δύσκολη	Δυνατή

Πίνακας 4. Σύγκριση APT και κοινών κυβερνοεπιθέσεων (Alshamrani et al., 2019; Chen et al., 2014; Tan et al., 2025)

2.3.1.3 DDoS

Στις επιθέσεις τύπου DDoS (κατανεμημένη άρνηση υπηρεσίας) ένας μεγάλος αριθμός υπολογιστών ή συσκευών του IoT (botnet) που έχουν μολυνθεί από κακόβουλο λογισμικό συντονίζονται από έναν φορέα απειλής και εξαπολύουν μια επίθεση που κατακλύζει ένα δίκτυο, τους διακομιστές ή έναν ιστότοπο με ένα τεράστιο όγκο κίνησης δεδομένων ή αιτημάτων, που δημιουργείται επί τούτου, , με αποτέλεσμα να είναι αδύνατο για το σύστημα που δέχεται την επίθεση να ανταποκριθεί στον αυξημένο φόρτο εργασίας. Το αποτέλεσμα είναι το δίκτυο να δυσλειτουργεί ή και να τίθεται εκτός λειτουργίας. Συνέπεια μιας επίθεσης DDoS είναι η αδυναμία εξυπηρέτησης των νόμιμων χρηστών, πλήττοντας την διαθεσιμότητα ενός δικτύου. Ανάλογα με την έκταση της επίθεσης και την κρισιμότητα της υποδομής, οι επιπτώσεις μπορεί να είναι από αμελητέες έως πολύ σοβαρές.

Η δημιουργία αυτού του είδους επίθεσης, βασίζεται στο γεγονός ότι όλα τα συστήματα και τα δίκτυα έχουν πεπερασμένους πόρους. Αν το botnet μπορεί να παράγει κίνηση μεγαλύτερη από τους πόρους που χρειάζονται για την εξυπηρέτησή της και ο στόχος δεν είναι καλά προστατευμένος, τότε η επίθεση επιτυγχάνει. Η ύπαρξη ενός τεράστιου αριθμού συνδεδεμένων στο διαδίκτυο συσκευών (συσκευές IoT) που μπορούν να παραβιαστούν εύκολα (προεπιλεγμένοι κωδικοί, άγνοια κινδύνου από τους νόμιμους χρήστες) δημιουργεί ένα πρόσφορο έδαφος για τη δημιουργία botnets.

Οι επιθέσεις αυτές δεν επηρεάζουν την ακεραιότητα και την εμπιστευτικότητα ενός συστήματος, ωστόσο η CISA επισημαίνει ότι μπορεί να αποσπάσουν την προσοχή από πιο επικίνδυνες ενέργειες όπως η εισαγωγή κακόβουλου λογισμικού ή η εξαγωγή δεδομένων. Οι οργανισμοί θα πρέπει στη διάρκεια μιας τέτοιας επίθεσης να μην αγνοούν την πιθανότητα παράλληλων κακόβουλων κινήσεων (CISA, 2022b).

Σύμφωνα με πρόσφατη έκθεση του ENISA, αυτού τους είδους οι επιθέσεις είναι οι πιο διαδεδομένες στην Ε.Ε. και κατευθύνονται κατά κανόνα από ομάδες «χακτιβιστών» (hackers με ιδεολογικά κίνητρα). Μόνο ένα μικρό μέρος αφορά ransom DDoS (επίθεση DDoS με σκοπό τον εκβιασμό) και πραγματοποιείται από κυβερνοεγκληματίες. Ωστόσο η έκθεση αναφέρει ότι η ανάγκη για χρηματοδότηση μπορεί να οδηγήσει ομάδες χακτιβιστών, εκτός από προβολή ιδεολογικών τοποθετήσεων, να επιδιώξουν και οικονομικά οφέλη. Ο ENISA θεωρεί επίσης, ότι ο χακτιβισμός μπορεί να είναι και κρατικά υποκινούμενος. Ως κύριοι στόχοι για την εξεταζόμενη περίοδο εμφανίζονται οι δημόσιες υπηρεσίες και οι μεταφορές (ENISA, 2025).

2.3.2 Κοινωνική Μηχανική

Σύμφωνα με τον ENISA, κοινωνική μηχανική είναι η προσπάθεια χειραγώγησης της ανθρώπινης συμπεριφοράς ώστε οι επιτιθέμενοι να εκμαιεύσουν μυστικές πληροφορίες ή να αποκτήσουν πρόσβαση σε υπηρεσίες[12].

Οι επιθέσεις κοινωνικής μηχανικής επικεντρώνονται στην ανθρώπινη φύση και επιδιώκουν να προκαλέσουν παρορμητικές συμπεριφορές που διευκολύνουν τους επιτιθέμενους. Οι λόγοι για τους οποίους οι άνθρωποι ανταποκρίνονται ευκολότερα στην κοινωνική μηχανική έχουν να κάνουν τόσο με κάποια χαρακτηριστικά της προσωπικότητάς τους (Yaser Al-Bustani et al., 2023), όσο και με τις συνθήκες που επικρατούν στο εργασιακό περιβάλλον, αλλά και το επίπεδο γνώσης και ενημέρωσής τους. Η εργασία υπό πίεση κάνει τους ανθρώπους απρόσεκτους, καθώς η εργασιακή εξάντληση

[12] https://www.enisa.europa.eu/topics/cyber-threats/threat-landscape

μειώνει την επαγρύπνηση (Kim & Lee, 2025). Επίσης, σύμφωνα με τη CISA, η εκμετάλλευση καταστάσεων από το ευρύτερο περιβάλλον όπως φυσικές καταστροφές, σημαντικά γεγονότα και καταστάσεις που προκαλούν φόβο (όπως η πανδημία COVID-19) για την προσέγγιση των θυμάτων, διευκολύνει τις επιθέσεις που βασίζονται στην κοινωνική μηχανική[13].

2.3.2.1 Στάδια κοινωνικής μηχανικής

Η κοινωνική μηχανική εξελίσσεται σε 6 στάδια (Mouton et al., 2016) (βλ. Πίνακας 6):

Πίνακας 5. Στάδια κοινωνικής μηχανικής

1. Στο πρώτο στάδιο ο επιτιθέμενος αποφασίζει ποιόν θα στοχεύσει (οργανισμό, στέλεχος κ.ά.) και τι θέλει από αυτόν (διαπιστευτήρια, πληροφορίες κ.λπ.)
2. Στο δεύτερο στάδιο συλλέγει πληροφορίες από την εταιρική ιστοσελίδα, τα κοινωνικά δίκτυα, κ.ά.
3. Στο τρίτο στάδιο δημιουργεί ένα σενάριο προσέγγισης και επιλέγει τον τρόπο που θα το υλοποιήσει (email, τηλέφωνο κ.λπ.)
4. Στο τέταρτο στάδιο ξεκινά την επαφή με το θύμα προσπαθώντας να κερδίσει την εμπιστοσύνη του (παραπλάνηση και πρόκληση συναισθηματικής έντασης)

[13] https://www.cisa.gov/news-events/news/avoiding-social-engineering-and-phishing-attacks

5. Στο πέμπτο στάδιο το θύμα ανταποκρίνεται (παρέχει πληροφορίες, κάνει κλικ σε κακόβουλο σύνδεσμο κ.λπ.)
6. Ο επιτιθέμενος διακόπτει την επικοινωνία αφού φροντίσει να δώσει ένα μήνυμα ικανοποίησης στο θύμα για να μην προκαλέσει υποψίες.

2.3.2.2 Η χρήση της ψυχολογίας στην κοινωνική μηχανική

Τα μηνύματα κοινωνικής μηχανικής προκαλούν συναισθήματα όπως ο φόβος, η περιέργεια, η έξαψη, ο θυμός, η ενοχή και η θλίψη, που μειώνουν τις αναστολές και την κρίση των ανθρώπων (Kaspersky, 2020). Παράλληλα, η κοινωνική μηχανική χρησιμοποιεί, συνδυαστικά ή κατά επιλογή, παράγοντες πειθούς που εκμεταλλεύονται πτυχές της ανθρώπινης φύσης. Σε σχετικό άρθρο (Longtchi et al., 2024) αναφέρονται 9 παράγοντες πειθούς, οι 6 πρώτοι προέρχονται από τις αρχές της πειθούς του Cialdini (Cialdini, 2009) και οι υπόλοιποι 3 από τη μεταγενέστερη βιβλιογραφία. Ο Πίνακας 7 καταγράφει τους παράγοντες αυτούς.

Αρχές πειθούς	Ανταπόκριση
1. Liking (Συμπάθεια)	Οι άνθρωποι αντιδρούν θετικά σε όσους φαίνονται φιλικοί και οικείοι
2. Reciprocity (Αμοιβαιότητα)	Έχουν την τάση να ανταποδίδουν όταν τους προσφέρεις κάτι
3. Social Proof (Κοινωνική Συμμόρφωση)	Μιμούνται προβαλλόμενες κοινωνικές συμπεριφορές (προτροπή να κάνεις κάτι που το έκαναν και άλλοι συνάδελφοι, πελάτες κ.λπ.)
4. Consistency (Συνέπεια).	Θέλουν να είναι συνεπείς
5. Authority (Αυθεντία).	Υπακούουν στην εξουσία. Μελέτες θεωρούν αυτόν τον παράγοντα ως τον πιο επιδραστικό καθώς οι άνθρωποι με τάση να υπακούουν στην εξουσία, γίνονται εύκολα θύματα κοινωνικής μηχανικής.

Αρχές πειθούς	Ανταπόκριση
6. Scarcity (Σπανιότητα).	Όταν αντιλαμβάνονται ότι κάτι είναι σπάνιο (όπως π.χ. ένα έκτακτο περιστατικό αυξημένης σημασίας) σπεύδουν να ανταποκριθούν
7. Respect (Σεβασμός).	Δεν αμφισβητούν πρόσωπα με τα οποία συνδέονται προσωπικά
8. Disobedience (Ανυπακοή).	Αντιδρούν στους κανόνες. Άνθρωποι που από την φύση τους δυσανασχετούν στο να ακολουθούν τους κανόνες ασφαλείας μπορεί να υποκύψουν στην κοινωνική μηχανική.
9. Perceptual contrast (Αντιλαμβανόμενη Αντίθεση)	Η αντίληψη των ανθρώπων επηρεάζεται από συγκρίσεις. Ανάμεσα σε δύο διαδοχικά μηνύματα κοινωνικής μηχανικής αυτό που προτείνει κάτι «καλύτερο» μπορεί να γίνει άμεσα αποδεκτό.

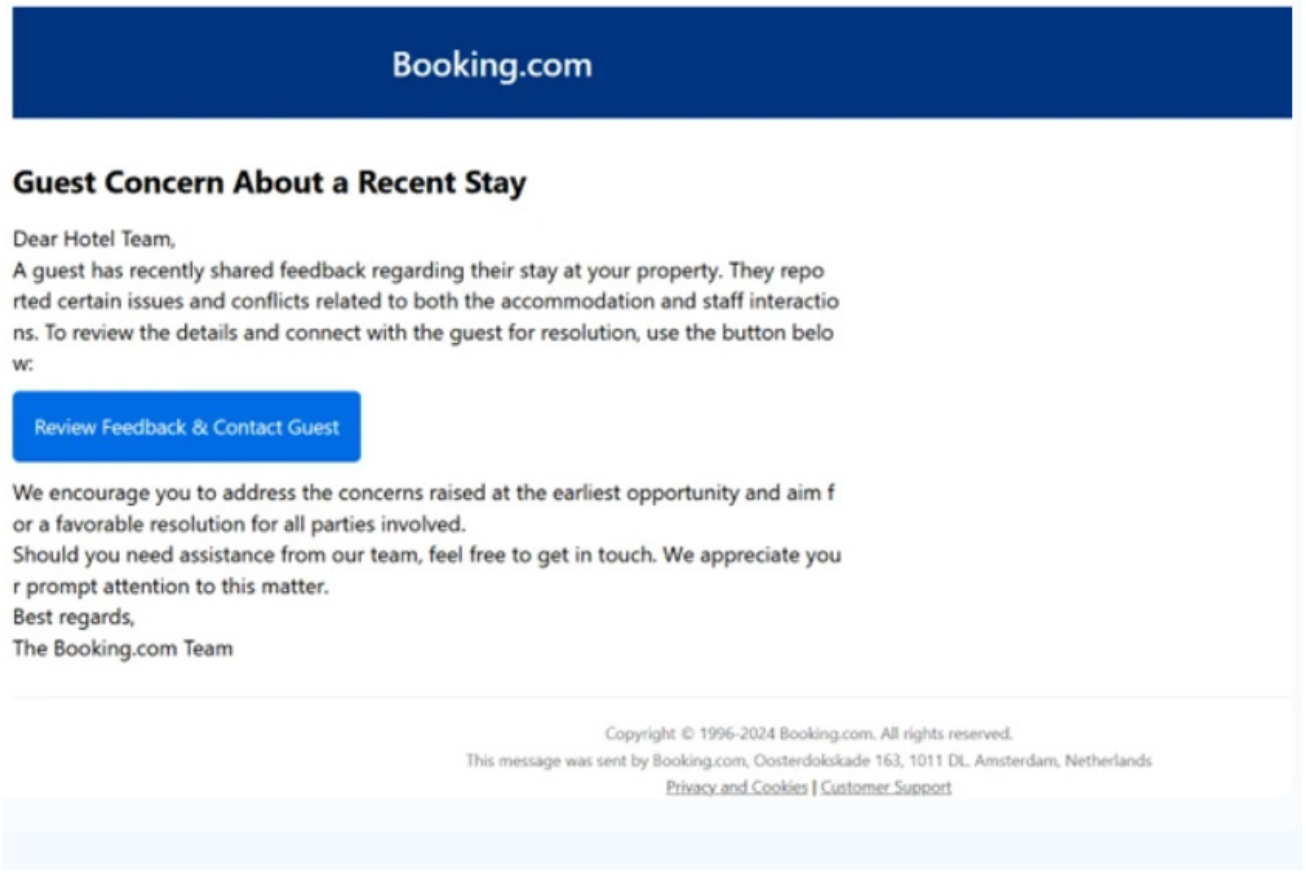
Πίνακας 6. Κοινωνική Μηχανική: Αρχές Πειθούς

Σε πρόσφατη ανασκόπηση της βιβλιογραφίας που αφορά την περίοδο 2020-2024 (Tsauri, 2025) αναφέρει ότι η ατομική ευπάθεια στις επιθέσεις κοινωνικής μηχανικής διαμορφώνεται από το συνδυασμό:

- ψυχολογικών συνθηκών (φόβος, πανικός, εμπιστοσύνη, εξάρτηση από την εξουσία),
- κοινωνικών συνθηκών (εργασιακή πίεση, χαλαρή οργανωσιακή κουλτούρα),
- και ελλείψεων στην ψηφιακή κατάρτιση.

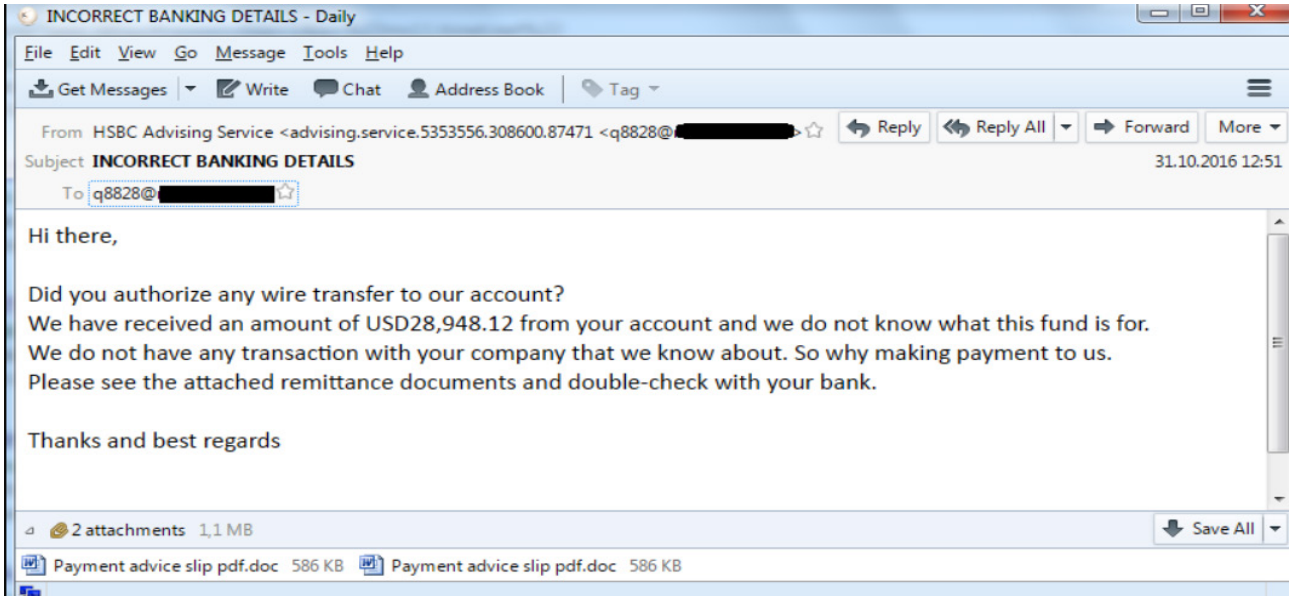
2.3.2.3 Παραδείγματα μηνυμάτων κοινωνικής μηχανικής προς επιχειρήσεις

Στις εικόνες που ακολουθούν φαίνονται δύο μηνύματα κοινωνικής μηχανικής. Τα μηνύματα αυτά αξιοποιούν τις αρχές που καταγράφει ο Πίνακας 7.



Σχήμα 3. Phishing mail a[14]. Το mail μιμείται το διαδικτυακό ταξιδιωτικό πρακτορείο Booking.com και καλεί τον δέκτη του να επιλύσει ένα πρόβλημα (αρνητική κριτική πελάτη).

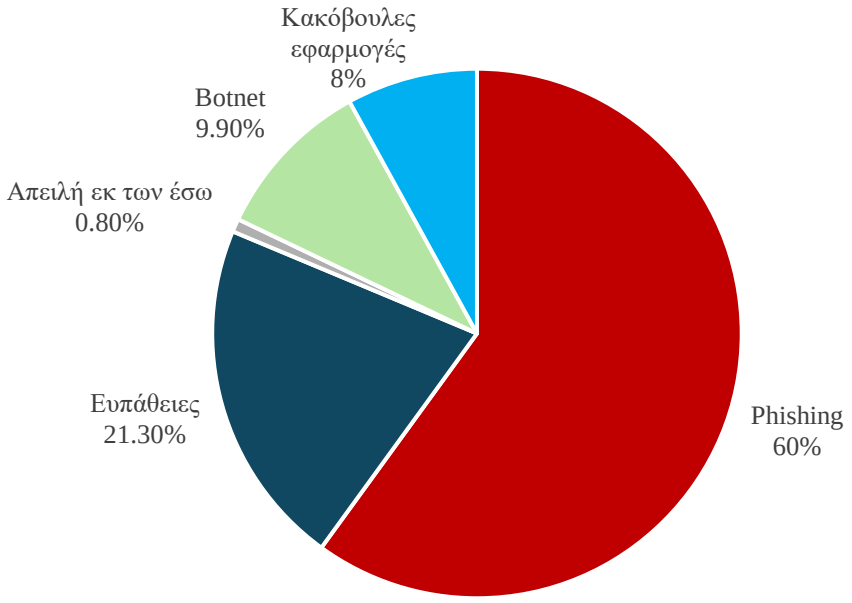
[14] Πηγή: https://www.microsoft.com/en-us/security/blog/2025/03/13/phishing-campaign-impersonates-booking-com-delivers-a-suite-of-credential-stealing-malware/



Σχήμα 4. Phishing email b[15]

2.3.2.4 Είδη επιθέσεων κοινωνικής μηχανικής

Οι επιθέσεις κοινωνικής μηχανικής είναι ιδιαίτερα διαδεδομένες, με την κατηγορία του Phishing να ανέρχεται στο 60% των συνολικών μολύνσεων (Σχήμα 5). Στις ακόλουθες παραγράφους παρουσιάζονται διάφορες μορφές επιθέσεων κοινωνικής μηχανικής.



Σχήμα 5. ENISA threat landscape 2025 (Αρχικοί Φορείς Μόλυνσης)

[15] Πηγή: https://ics-cert.kaspersky.com/publications/reports/2017/06/15/nigerian-phishing-industrial-companies-under-attack/

2.3.2.4.1 Phishing

Οι επιτιθέμενοι αποστέλλουν ένα email από φαινομενικά αξιόπιστη πηγή που περιέχει ένα συνημμένο με κακόβουλο λογισμικό ή ένα πλασματικό URL. Ο αποδέκτης με την τεχνική της κοινωνικής μηχανικής ενθαρρύνεται να ανοίξει το μολυσμένο αρχείο ή να ακολουθήσει το προτεινόμενο URL. Σκοπός είναι να αποσπαστούν στοιχεία σύνδεσης, κωδικοί ή ακόμη και χρήματα. Συχνά είναι η αρχή για μια επίθεση ransomware. Κατά τον οργανισμό ENISA, μια πολύ επιτυχημένη μορφή του phishing είναι το *spear phishing* το οποίο βασίζεται σε προηγούμενη έρευνα σχετικά με τον στόχο και καταφέρνει να παρουσιάζει ένα μήνυμα το οποίο το θύμα θα θεωρήσει αυθεντικό.

Την περίοδο έξαρσης του Covid-19 οι επιτιθέμενοι, εκμεταλλευόμενοι τον πανικό της πανδημίας, χρησιμοποίησαν τεχνικές phishing με πρόσχημα ενημερώσεις για τον κορονοϊό. Το πρόβλημα επιδεινώθηκε από το γεγονός ότι πολλοί άνθρωποι εργάζονταν απομακρυσμένα χρησιμοποιώντας παρωχημένα συστήματα ή ανεπαρκώς προστατευμένους υπολογιστές, γεγονός που αύξησε την αποτελεσματικότητα του phishing και τον κίνδυνο προσβολής εταιρικών πληροφοριακών συστημάτων (ENISA phishing, 2020).

Στις περισσότερες περιπτώσεις οι επιτιθέμενοι παραποιούν μια διεύθυνση ηλεκτρονικού ταχυδρομείου ή ένα domain. Ωστόσο σε κάποιες πιο εξελιγμένες περιπτώσεις οι κακόβουλες εκστρατείες προέχονται από νόμιμους πόρους που έχουν παραβιαστεί (Kaspersky, 2017).

2.3.2.4.2 Vishing

Τα θύματα δέχονται τηλεφωνική κλίση από ένα αξιόπιστο θεωρητικά άτομο ή φορέα και χειραγωγούνται για να αποκαλύψουν πληροφορίες και εμπιστευτικά δεδομένα. Σε κάποιες περιπτώσεις οι επιτιθέμενοι μιμούνται το διαδραστικό σύστημα απόκρισης που χρησιμοποιούν τράπεζες και δημόσιοι φορείς, όπου ο πελάτης καλείται να δώσει πληροφορίες, παρέχοντας την αίσθηση της σύνδεσης με έναν νόμιμο φορέα (Salahdine & Kaabouch, 2019).

2.3.2.4.3 Smising

Οι επιτιθέμενοι στέλνουν SMS τα οποία περιλαμβάνουν παραπλανητικούς συνδέσμους (Kaspersky, 2017).

2.3.2.4.4 Waterholing

Οι επιτιθέμενοι παραβιάζουν έναν ιστότοπο που επισκέπτονται συχνά τα υποψήφια θύματα (μπορεί να στοχεύουν σε συγκεκριμένες εταιρίες ή ολόκληρους κλάδους) και περιμένουν την επίσκεψή τους για να διαμοιράσουν κακόβουλο λογισμικό[16].

2.3.2.4.5 Quid Pro Quo

Οι επιτιθέμενοι προσφέρουν ένα προϊόν ή μια υπηρεσία και ζητούν σαν αντάλλαγμα πληροφορίες (Salahdine & Kaabouch, 2019).

2.3.2.4.6 Pretexting/Impersonation

Ο επιτιθέμενος προσεγγίζει το θύμα του μέσω ενός ψεύτικου σεναρίου / μέσω πλαστοπροσωπίας. Ειδικότερα, προσποιείται ότι υπάρχει επείγουσα ανάγκη και ότι ο ίδιος είναι κάποιος αξιόπιστος συνεργάτης ή άτομο με εξουσία και ζητά πληροφορίες (Salahdine & Kaabouch, 2019).

2.3.2.4.7 Επιθέσεις αντίστροφης κοινωνικής μηχανικής.

Οι επιτιθέμενοι αρχικά προκαλούν ένα πρόβλημα στο δίκτυο και παρουσιάζονται ως τεχνική βοήθεια. Το θύμα απευθύνεται σε αυτούς για αποκατάσταση, και στο πλαίσιο αυτό παρέχουν στους επιτιθέμενους τις πληροφορίες που οι επιτιθέμενοι θέλουν να αντλήσουν (Salahdine & Kaabouch, 2019).

Η χρήση της τεχνητής νοημοσύνης από την πλευρά των επιτιθέμενων δείχνει να έχει ανησυχητική αποτελεσματικότητα σε ό,τι αφορά την κοινωνική μηχανική. Με βάση την αναφορά της Microsoft «Digital Defense Report 2025», η οποία καλύπτει το χρονικό διάστημα από Ιούλιο του 2024 έως τον Ιούνιο του 2025, τα phishing mails που έκαναν χρήση της τεχνητής νοημοσύνης πέτυχαν ποσοστό κλικ 54% (Microsoft, 2025).

2.4 Μοντέλα ανάλυσης κυβερνοεπιθέσεων

Τα μοντέλα και τα πλαίσια επιθέσεων χρησιμοποιούνται για την κατανόηση και τον μετριασμό των κυβερνοεπιθέσεων. Το μοντέλο Cyber kill chain (Khan et al., 2017; Lockheed_Martin, 2015) και το μοντέλο MITRE ATT&CK Framework (Al-Sada et al., 2025; MITRE, 2025) είναι από τα πλέον δημοφιλή. Το πρώτο αναφέρεται στις φάσεις μιας επίθεσης και εξυπηρετεί την διαμόρφωση

[16] https://www.ncsc.gov.uk/collection/supply-chain-security/watering-hole-attacks

στρατηγικής άμυνας, ενώ το δεύτερο αποτελεί μια ανοικτή βάση γνώσεων που αντλούνται από την εμπειρία του πραγματικού κόσμου (Naik et al., 2022). Στις επόμενες παραγράφους αναλύονται συνοπτικά τα δύο πλαίσια.

2.4.1 Μοντέλο Cyber kill chain

Το μοντέλο Cyber kill chain προτάθηκε το 2011 από τη Lockheed Martin [17] και αποτελεί μοντελοποίηση μιας κυβερνοεπίθεσης σε 7 βήματα. Η ανάλυση είναι εμπνευσμένη από την εξέλιξη μιας στρατιωτικής επιχείρησης. Το μοντέλο ακολουθεί γραμμική προσέγγιση και τη λογική ότι οι επιτιθέμενοι θα πρέπει να ολοκληρώσουν διαδοχικά βήματα προκειμένου να φτάσουν στους τελικούς τους στόχους. Σκοπός της κυβερνοασφάλειας είναι η επίθεση να διακοπεί στα στάδια 1 έως 6. Η κατανόηση των κινδύνων που εμφανίζονται σε κάθε στάδιο, μπορεί να διαμορφώσει και τα αντίμετρα που θα επιλεγούν, ανάλογα με την έκθεση του κάθε οργανισμού (Khan et al., 2017; Lockheed_Martin, 2015).

Σχήμα 6. Cyber Kill Chain

2.4.1.1 Περιγραφή των 7 βημάτων

Στις επόμενες παραγράφους παρατίθεται η περιγραφή των επτά βημάτων του μοντέλου Cyber kill chain (Ahmed et al., 2021; Khan et al., 2017; Lockheed_Martin, 2015; Naik et al., 2022).

- **Αναγνώριση (Reconnaissance)**. Στο στάδιο αυτό οι επιτιθέμενοι συγκεντρώνουν πληροφορίες για τον στόχο τους. Η συγκέντρωση πληροφοριών μπορεί να είναι είτε παθητική (χωρίς αλληλεπίδραση με τον στόχο) είτε ενεργητική (ο εισβολέας προσπαθεί να αλληλοεπιδράσει με τον στόχο του για να αποσπάσει πληροφορίες) (Ahmed et al., 2021).

[17] Αμερικάνικη εταιρία ειδικευμένη στην αμυντική τεχνολογία, η οποία δραστηριοποιείται και στον τομέα της κυβερνοασφάλειας https://www.lockheedmartin.com/en-us/who-we-are.html, https://www.lockheedmartin.com/en-us/suppliers/cybersecurity.html

- **Μετατροπή σε όπλο («οπλοποίηση», Weaponization).** Οι επιτιθέμενοι διαμορφώνουν το κατάλληλο λογισμικό αξιοποιώντας τις πληροφορίες του προηγούμενου σταδίου.
- **Παράδοση (Delivery).** Μολυσμένες συσκευές USB, κακόβουλα email, παραπλανητικοί σύνδεσμοι, κ.λπ. επιστρατεύονται για την παράδοση κακόβουλου λογισμικού.
- **Εκμετάλλευση (Exploitation).** Μια ευπάθεια σε σχέση με τους χρήστες, το λογισμικό ή το υλικό ενός συστήματος αξιοποιείται για την είσοδο σε αυτό.
- **Εγκατάσταση (Installation).** Οι εισβολείς εκτελούν το κακόβουλο λογισμικό. Για να αποφύγουν την ανίχνευση απενεργοποιούν εργαλεία παρακολούθησης της ασφάλειας ενός συστήματος όπως π.χ. τα αντι-ικά λογισμικά (antivirus).
- **Διοίκηση & Έλεγχος (Command & Control).** Οι επιτιθέμενοι αποκτούν τον έλεγχο ενός συστήματος από απόσταση. Το κακόβουλο λογισμικό εγκαθιδρύει ένα κανάλι επικοινωνίας δύο κατευθύνσεων (Command & Control channel) με στόχο ο εισβολέας να μπορεί να στέλνει εντολές και να λαμβάνει δεδομένα. Η επικοινωνία γίνεται με χρήση κοινών πρωτοκόλλων (διαδικτύου, email) που χρησιμοποιούνται ήδη από το θύμα, έτσι ώστε η επικοινωνία με τον εισβολέα να διαλανθάνει της προσοχής των συστημάτων άμυνας, καθώς συγχέεται με την νόμιμη κίνηση στο δίκτυο. Η υποδομή από την οποία ασκείται η διοίκηση και ο έλεγχος μπορεί να ανήκει στον επιτιθέμενο ή να γίνεται χρήση ενός μολυσμένου συστήματος που λειτουργεί σαν ενδιάμεσος κόμβος και καλύπτει την πραγματική προέλευση της απειλής (ή εισβολής).
- **Ενέργειες στους Στόχους (Actions on Objectives).** Προωθούνται οι στόχοι της εισβολής που μπορούν να περιλαμβάνουν κλοπή ή αλλοίωση δεδομένων, άρνηση πρόσβασης, καταστροφή συστημάτων, είσοδος σε υποδομές τρίτου κ.λπ.

2.4.1.2 Κριτική στο μοντέλο Cyber kill chain

Στο μοντέλο Cyber kill chain έχει δεχθεί κριτική, η οποία εστιάζει στα ακόλουθα δύο σημεία:

- Μια μοντελοποίηση cyber kill chain αφορά μία εξελισσόμενη απόπειρα εισβολής. Στην πραγματικότητα είναι δυνατόν να έχουμε μια συνεχιζόμενη απόπειρα εισβολής που ακολουθεί πολλαπλές cyber kill chains, όπου κάποια στάδια παραλείπονται ή επαναχρησιμοποιούνται (Khan et al., 2017).
- Το παραδοσιακό μοντέλο εστιάζει στις εξωτερικές απειλές και δεν λαμβάνει υπόψιν τις ιδιαιτερότητες των εσωτερικών απειλών (Naik et al., 2022).

2.4.2 Πλαίσιο MITRE ATT&CK

Το πλαίσιο δημοσιεύτηκε το 2013 και αποτελεί ένα αποθετήριο γνώσεων για τις τακτικές, τεχνικές και διαδικασίες που χρησιμοποιούν οι αντίπαλοι στα πλαίσια μιας κυβερνοεπίθεσης. Έκτοτε αναπτύσσεται δυναμικά, αξιοποιώντας την εμπειρία από τεχνολογικά καθοδηγούμενες παραβιάσεις. Το πλαίσιο έχει ευρεία αποδοχή από μεγάλες και μεσαίες επιχειρήσεις και χρησιμοποιείται ευρέως για προστασία από απειλές, εντοπισμό κενών ασφαλείας και μοντελοποίηση απειλών. Το χαρακτηριστικό του πλαισίου MITRE ATT&CK είναι η επικέντρωση στην τεχνική πλευρά των κυβερνοπιθέσεων. Σε μια ολιστική προσέγγιση το πλαίσιο θα μπορούσε να συνυπάρξει με προσεγγίσεις που αφορούν την διαμόρφωση της ανθρώπινης συμπεριφοράς και την επίδραση της οργανωσιακής κουλτούρας (Georgiadou et al., 2021).

Το MITRE ATT&CK δεν αναφέρεται σε στάδια όπως το Cyber kill chain και δεν ακολουθεί γραμμική εξέλιξη. Λειτουργεί στην βάση ενός πλέγματος τακτικών που εφαρμόζουν καταγεγραμμένες τεχνικές. Μια τεχνική μπορεί να χρησιμοποιείται από διαφορετικές τακτικές (Naik et al., 2022). Για παράδειγμα, η τεχνική (T1078) Valid accounts [18] (αφορά κατάχρηση νόμιμων διαπιστευτηρίων) απαντάται σε 4 διαφορετικές τακτικές του πλαισίου ήτοι την Αρχική Πρόσβαση, την Επιμονή, την Κλιμάκωση Προνομίων και την Αμυντική Διαφυγή.

Ο Πίνακας 8 παρουσιάζει τα στάδια του πλαισίου MITRE ATT&CK, παραθέτοντας μία σύντομη περιγραφή του περιεχομένου του κάθε σταδίου και των αριθμό των τεχνικών που περιλαμβάνονται σε αυτό, κατά τη σύνταξη της παρούσας εργασίας.

MITRE ATT&CK		
Τακτικές	**Τι συμβαίνει**	**Αριθμός τεχνικών**
1. Αναγνώριση *https://attack.mitre.org/tactics/TA0043/*	Συλλογή πληροφοριών για τον οργανισμό, την υποδομή και το προσωπικό.	12
2. Ανάπτυξη πόρων *https://attack.mitre.org/tactics/TA0042/*	Δημιουργία, αγορά ή κλοπή πόρων π.χ. σχηματισμός ή αγορά botnet.	9

[18] https://attack.mitre.org/techniques/T1078/

MITRE ATT&CK		
Τακτικές	**Τι συμβαίνει**	**Αριθμός τεχνικών**
3. Αρχική πρόσβαση *https://attack.mitre.org/tactics/TA0001/*	Οι εισβολείς επιδιώκουν να αποκτήσουν αρχική πρόσβαση. Αυτή μπορεί να εξασφαλίζει συνεχή ή βραχείς διάρκειας πρόσβαση ή να έχει περιορισμένα προνόμια.	11
4. Εκτέλεση επίθεσης *https://attack.mitre.org/tactics/TA0002/*	Ο εισβολέας προσπαθεί να εκτελέσει έναν κακόβουλο κώδικα, απομακρυσμένα ή τοπικά σε ένα σύστημα στο οποίο έχει ήδη αποκτήσει πρόσβαση.	20
5. Επιμονή *https://attack.mitre.org/tactics/TA0003/*	Οι επιτιθέμενοι προσπαθούν να διατηρήσουν την παρουσία τους στο σύστημα, αντιμετωπίζοντας ενέργειες που μπορεί να τη διακόψουν (π.χ. αλλαγή δικαιωμάτων)	22
6. Κλιμάκωση προνομίων *https://attack.mitre.org/tactics/TA0004/*	Οι εισβολείς μπορεί να εισέλθουν σε ένα σύστημα με χαμηλό επίπεδο δικαιωμάτων και να αξιοποιήσουν ευπάθειες για να τα αυξήσουν.	13
7. Αποφυγή εντοπισμού *https://attack.mitre.org/tactics/TA0005/*	Αφορά την αποφυγή του εντοπισμού κατά τη διάρκεια της παραβίασης. Για παράδειγμα, η βραδεία εκτέλεση ενεργειών επιτυγχάνει την αποφυγή εντοπισμού από συστήματα ανίχνευσης ανωμαλιών.	30
8. Απενεργοποίηση μηχανισμών άμυνας *https://attack.mitre.org/tactics/TA0112*	Αφορά την απενεργοποίηση μηχανισμών άμυνας ώστε αφ' ενός να διευκολύνεται ο	19

MITRE ATT&CK		
Τακτικές	**Τι συμβαίνει**	**Αριθμός τεχνικών**
	στόχος της επίθεσης, αφ΄ ετέρου να υποστηρίζεται η αποφυγή εντοπισμού.	
8. Πρόσβαση με διαπιστευτήρια *https://attack.mitre.org/tactics/TA0006/*	Προσπάθεια για πρόσβαση με νόμιμα διαπιστευτήρια που αποτελούν ιδανική κάλυψη. Αποκτώνται με τεχνικές όπως brute force, πλαστογράφηση cookies, Credential Dumping κ.ά.	17
9. Ανακάλυψη *https://attack.mitre.org/tactics/TA0007/*	Ενέργειες για την απόκτηση πληροφορίας σε σχέση με το εσωτερικό δίκτυο.(π.χ. λίστα με λογαριασμούς νέφους (cloud), λεπτομέρειες για τους εσωτερικούς πόρους του δικτύου κ.λπ.)	34
10. Πλευρική κίνηση *https://attack.mitre.org/tactics/TA0008/*	Ο εισβολέας κινείται στο δίκτυο για να αποκτήσει πρόσβαση σε πόρους μεγαλύτερης αξίας ή να επεκτείνει τον έλεγχό του (π.χ. με εσωτερικό spearphishing ή χρήση κοινόχρηστων πόρων).	9
11. Συλλογή *https://attack.mitre.org/tactics/TA0009/*	Συλλογή πληροφοριών και δεδομένων σχετικών με τους στόχους της επίθεσης.	17
12. Διοίκηση και έλεγχος *https://attack.mitre.org/tactics/TA0011/*	Επικοινωνία με τα παραβιασμένα συστήματα και προσπάθεια απόκτησης ελέγχου επ' αυτών.	18

MITRE ATT&CK		
Τακτικές	**Τι συμβαίνει**	**Αριθμός τεχνικών**
13. Εξαγωγή/απόσπαση δεδομένων ***https://attack.mitre.org/tactics/TA0010/***	Εξαγωγή των δεδομένων.	9
14. Προσβολή ***https://attack.mitre.org/tactics/TA0040/***	Χειραγώγηση ή καταστροφή συστημάτων.	15

Πίνακας 7. Στάδια πλαισίου MITRE ATT&CK [19]

Η προδημοσίευση (Jiang et al., 2025) παρουσιάζει μια ανασκόπηση 417 εργασιών που αφορούν το πλαίσιο MITRE ATT&CK και εντοπίζει ευρεία κοινή χρήση του συνδυαστικά με άλλα πλαίσια, προκειμένου να βελτιωθεί η αποτελεσματικότητα της προσέγγισης. Για παράδειγμα ο συνδυασμός cyber kill chain (για την αποτύπωση της χρονικής ακολουθίας) και MITRE ATT&CK (για την λεπτομερή τεχνική προσέγγιση), έχει χρησιμοποιηθεί για τη δημιουργία σεναρίων κινδύνου.

2.5 Τρόποι εξάπλωσης

Η εξάπλωση μιας κυβερνοεπίθεσης μετά την αρχική πρόσβαση μπορεί να διευκολυνθεί από διαφορετικούς παράγοντες. Οι τρόποι αυτοί παρουσιάζονται συνοπτικά στις ακόλουθες παραγράφους.

2.5.1 Εσφαλμένες ρυθμίσεις/τεχνικές ευπάθειες

Τα συστήματα ενσωματώνουν εσφαλμένες ρυθμίσεις ή τεχνικές ευπάθειες που μπορούν να επιτρέψουν την εξέλιξη μιας επίθεσης. Σε αυτές συμπεριλαμβάνονται η ανοικτή πρόσβαση, ο ανεπαρκής έλεγχος εισόδου σε συνδεδεμένα συστήματα, η παραχώρηση υπερβολικών δικαιωμάτων, η χρήση προεπιλεγμένων, επαναχρησιμοποιούμενων ή κωδικών που μπορούν να μαντευτούν εύκολα, καθώς και η έλλειψη κρυπτογράφησης κρίσιμων δεδομένων, είναι κάποιες από τις εσφαλμένες ρυθμίσεις που είναι δυνατόν να επιτρέψουν την επέκταση μιας επίθεσης (NIST, 2023a).

[19] https://attack.mitre.org/

2.5.2 Ανθρώπινος παράγοντας

Οι επιθέσεις κοινωνικής μηχανικής αφορούν τόσο την αρχική πρόσβαση όσο και μετέπειτα στάδια μιας παραβίασης. Ένας παραβιασμένος λογαριασμός μπορεί χρησιμοποιηθεί όχι μόνο για την αρχική πρόσβαση αλλά και για να αποσπαστούν πληροφορίες από άλλους εργαζόμενους, μέσω εσωτερικού spear-phishing (MITRE, τεχνική T1534[20]). Στην περίπτωση αυτή, ο επιτιθέμενος υποδυόμενος ένα πρόσωπο εμπιστοσύνης και χρησιμοποιώντας τον νόμιμο λογαριασμό του συγκεκριμένου προσώπου, μπορεί να αποσπάσει εσωτερικές πληροφορίες ή και διαπιστευτήρια από άλλους χρήστες, π.χ. οδηγώντας τα υποψήφια θύματά του, σε ιστότοπους που μιμούνται οικείες διεπαφές σύνδεσης.

2.5.3 Αλυσίδα εφοδιασμού

Η ψηφιακή αλληλεπίδραση των οργανισμών με προμηθευτές και συνεργάτες, επεκτείνει την επιφάνεια πιθανών επιθέσεων μέσω ενός παραβιασμένου τρίτου μέρους. Η προστασία των «ψηφιακών συνόρων» ενός οργανισμού δεν επαρκεί για την επίτευξη της κυβερνοασφάλειας, καθώς μπορεί να υπάρχουν ευπάθειες στα συστήματα των συνεργατών, οι οποίες μπορεί να είναι άγνωστες. Οι επιτιθέμενοι συνήθως προσβάλουν τον αδύναμο κρίκο της εφοδιαστικής αλυσίδας και στη συνέχεια επιτίθενται στα συστήματα πιο ώριμων ψηφιακά οργανισμών που αποτελούν και τους πραγματικούς στόχους, χρησιμοποιώντας δικαιώματα που έχουν παραχωρηθεί στον αρχικό κρίκο (NISTIR IR 8276 (NIST, 2021b)).

2.5.4 Φυσικά μέσα

Προσβεβλημένες συσκευές και εργαλεία αποθήκευσης μπορεί να ευθύνονται για την παραβίαση ενός συστήματος. Μολυσμένο υλικό (hardware) είναι δυνατόν να περιέχει Backdoors, δούρειους ίππους (Trojans), κακόβουλο λογισμικό κ.λπ. (Maragkou et al., 2025; Mehta et al., 2020).

2.5.5 Διαδίκτυο των πραγμάτων /Κυβερνοφυσικά συστήματα

Στα κυβερνοφυσικά συστήματα (Cyber-Physical Systems) αισθητήρες, λογισμικό και δίκτυα ελέγχουν φυσικές διεργασίες που αφορούν υποδομές, όπως η βιομηχανική δραστηριότητα και τα δίκτυα των έξυπνων πόλεων. Οι αισθητήρες του διαδικτύου των πραγμάτων (Internet of Things, IoT) παρουσιάζουν σημαντικές ευπάθειες λόγω της χαμηλής υπολογιστικής ισχύος που διαθέτουν, χαρακτηριστικό που με τη σειρά του θέτει περιορισμούς στην κρυπτογράφηση. Επιπλέον η φυσική διασπορά των αισθητήρων θέτει περιορισμούς στη δυνατότητα άμυνας έναντι φυσικής δολιοφθοράς ή παραβίασης. Η διασύνδεση των συσκευών αυτών μπορεί να επεκτείνει την παραβίαση σε ολόκληρο

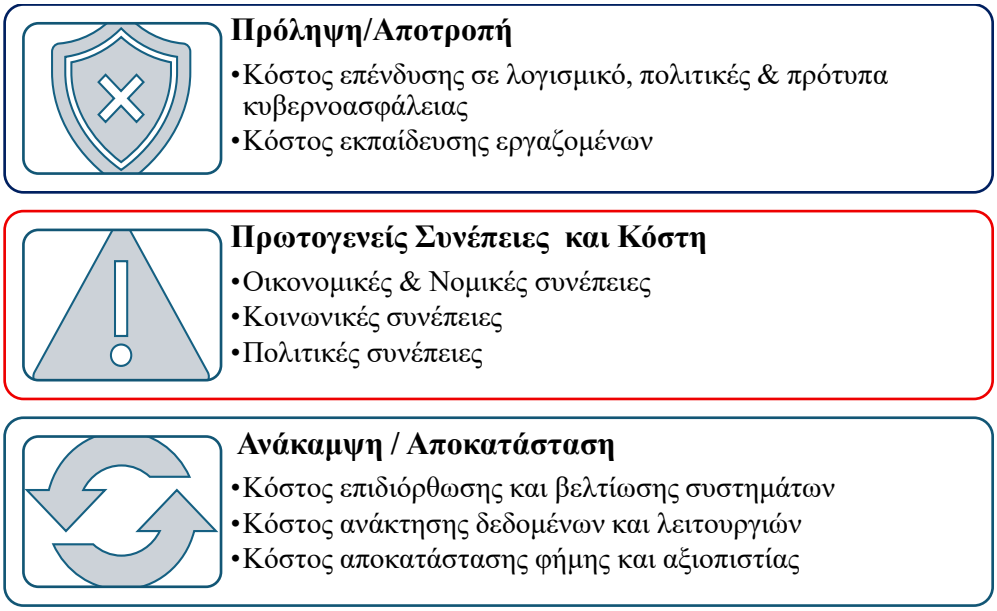
[20] https://attack.mitre.org/techniques/T1534/

το σύστημα προκαλώντας αλλοίωση δεδομένων, βλάβες, διακοπές, λανθασμένες ενέργειες και φυσικούς κινδύνους (Abomhara et al., 2015; Duo et al., 2022).

Η παραβίαση της ακεραιότητας των δεδομένων μέσω Έγχυσης Ψευδών Δεδομένων (False Data Injection attacks) προκαλεί ιδιαίτερη ανησυχία για τα κυβερνοφυσικά συστήματα των έξυπνων πόλεων, της έξυπνης βιομηχανίας, της έξυπνης υγειονομικής περίθαλψης κ.λπ., δημιουργώντας σοβαρά ζητήματα ασφάλειας από τη χρήση ψευδών μετρήσεων. Η διασύνδεση των συστημάτων και η χρήση των δεδομένων στο πλαίσιο αυτοματισμών και λήψης «έξυπνων» αποφάσεων επιτείνει το πρόβλημα και αυξάνει το επίπεδο των επιπτώσεων επιτυχών επιθέσεων. Η δυσκολία ανίχνευσής τους απαιτεί την εφαρμογή προηγμένων τεχνικών, όπως η μηχανική μάθηση και η πρόληψη μέσω προσομοίωσης επιθέσεων (Habib et al., 2025).

2.6 Κόστος και συνέπειες κυβερνοεπιθέσεων

Το κόστος των κυβερνοεπιθέσεων είναι δύσκολο να αποτιμηθεί καθώς αφορά το κόστος πρόληψης και αποτροπής, το κόστος των συνεπειών και τα κόστη αποκατάστασης (Wright & Kumar, 2023). Ο Πίνακας 9 συνοψίζει τις κατηγορίες του κόστους και αναλύει τις υποκατηγορίες εντός κάθε μίας εξ αυτών.



Πίνακας 8. Κόστος κυβερνοεπιθέσεων

2.6.1 Κόστος πρόληψης και αποτροπής

Η αποτροπή και η πρόληψη των κυβερνοεπιθέσεων προϋποθέτει την διάθεση σημαντικών πόρων από την πλευρά των επιχειρήσεων και των οργανισμών. Το κόστος ενημέρωσης και εκπαίδευσης των υπαλλήλων και των υπευθύνων ασφάλειας, η αγορά κατάλληλου λογισμικού, η πρόσβαση σε επιδιορθώσεις και η εγκατάστασή τους, οι αναβαθμίσεις και τα έξοδα ανάπτυξης νέου λογισμικού που επωμίζονται οι τελικοί χρήστες για να αντιμετωπιστούν οι δυναμικά εξελισσόμενες απειλές, καθιστούν την κυβερνοασφάλεια όχι μια άπαξ (one-off) επένδυση, αλλά ένα διαρκές έξοδο (σελ.272 & σελ. 292 της παραπομπής (Anderson et al., 2013)).

Επίσης η συμμόρφωση με πρότυπα κυβερνοασφάλειας ενέχει ένα σημαντικό κόστος που κάποιες φορές περιορίζει την υιοθέτησή τους από τις επιχειρήσεις (Barkat Ullah et al., 2025).

2.6.2 Πρωτογενείς Συνέπειες και Κόστη

Η εκδήλωση μιας κυβερνοεπίθεσης συνδέεται με ένα πλέγμα από οικονομικές, κοινωνικές και πολιτικές συνέπειες που διαμορφώνουν ανάλογα κόστη. Οι συνέπειες αυτές αναλύονται στις ακόλουθες παραγράφους:

2.6.2.1 Οικονομικές συνέπειες

Οι άμεσες και έμμεσες οικονομικές συνέπειες μια κυβερνοεπίθεσης μπορεί να περιλαμβάνουν (Abrardi et al., 2025; Kaspersky, 2024):

- την απώλεια εσόδων από την διακοπή της παραγωγής ή των παρεχόμενων υπηρεσιών καθώς τα παραβιασμένα συστήματα δεν λειτουργούν,
- την απώλεια εσόδων από την κλοπή πνευματικής ιδιοκτησίας,
- η οικονομική αιμορραγία από την καταβολή λύτρων,
- την απώλεια της εμπιστοσύνης των πελατών (ως συνέπεια της αδυναμίας εξυπηρέτησης, της διαρροής οικονομικών ή ευαίσθητων δεδομένων κ.λπ.) και τη στροφή τους σε ανταγωνιστικές επιχειρήσεις,
- την απώλεια συνεργατών, ιδίως σε περίπτωση που η παραβίαση αφορά την εφοδιαστική αλυσίδα,
- την απώλεια επενδυτών λόγω απώλειας φήμης και αξιοπιστίας των παθουσών εταιρειών, ιδίως για εταιρείες που έχουν εισαχθεί στο χρηματιστήριο,

- νομικές συνέπειες όπως η επιβολή προστίμων από τις αρμόδιες αρχές και οι αστικές αγωγές από πελάτες για τη διαρροή ευαίσθητων δεδομένων.

2.6.2.2 Κοινωνικές συνέπειες

Η έκθεση προσωπικών και ευαίσθητων δεδομένων μπορεί να γίνει αιτία κοινωνικής αναστάτωσης και δυσπιστίας απέναντι στους θεσμούς. Η διαρροή και η απειλή διαρροής προσωπικών δεδομένων και πληροφοριών μπορεί να προκαλέσει εξαιρετικό άγχος ακόμη και ακραίες αντιδράσεις από ανθρώπους που θα αισθανθούν ευάλωτοι (Looi et al., 2025; Mills & Harclerode, 2018).

Επιπλέον, επιθέσεις σε κρίσιμους τομείς μπορεί να επηρεάσουν σημαντικά τους πολίτες. Για παράδειγμα, μια επίθεση[21] ransomware τον Σεμπέμβριο του 2025 σε βάρος της Collins Aerospace (εταιρίας που παρέχει συστήματα check-in), προκάλεσε καθυστερήσεις και ταλαιπωρία των επιβατών, σε αεροδρόμια της Ευρώπης.

Επίσης, τα κυβερνοφυσικά συστήματα που έχουν εκτεταμένη χρήση στη βιομηχανία, τις ενεργειακές υποδομές και την υγειονομική περίθαλψη, βασίζονται στην αλληλεπίδραση του ψηφιακού με τον φυσικό κόσμο και τυχόν παραβιάσεις εκτείνονται πέρα από το λογισμικό και τα δίκτυα, έχοντας επιπτώσεις και στο φυσικό κόσμο. Οι ζημιές αυτές μπορεί να περιλαμβάνουν υποβάθμιση υποδομών, απώλειες πόρων, επιπτώσεις από την νόθευση δεδομένων ελέγχου και την αλλοίωση των παραγόμενων προϊόντων, ενώ θα μπορούσαν να κλιμακώνονται και καιτραυματισμούς και απώλειες ανθρώπινων ζωών (Mohamed et al., 2020). Το 2020, εν μέσω πανδημίας, νοσοκομείο στην Τσεχία δέχτηκε κυβερνοεπίθεση[22] με αποτέλεσμα προβλήματα στην φροντίδα των ασθενών από την παύση λειτουργίας του δικτύου των υπολογιστών του (Duo et al., 2022).

Επιπτώσεις θα μπορούσαν να υπάρχουν και για το περιβάλλον, καθώς αυτό μπορεί να επηρεαστεί σημαντικά αν πληγούν βιομηχανικά συστήματα ή συστήματα που συνδέονται με αυτό. Επί παραδείγματι, ένας δυσαρεστημένος πρώην συνεργάτης της αυστραλιανής εταιρείας Maroochy Water Services, το 2000, έγινε η αιτία διαρροής 800.000 λίτρων λυμάτων[23] στο σύστημα ύδρευσης, εκμεταλλευόμενος τα διαπιστευτήρια που κατείχε και ενεργώντας σαν εσωτερικός χρήστης. Ως αποτέλεσμα, προκλήθηκε η μόλυνση ρεμάτων και πάρκων, και υποβαθμίστηκε η ζωή των κατοίκων

[21] https://techcrunch.com/2025/09/23/european-airports-still-dealing-with-disruptions-days-after-ransomware-attack/, https://www.theguardian.com/world/2025/sep/22/flight-delays-europe-cyber-attack-heathrow-brussels-berlin
[22] https://www.zdnet.com/article/czech-hospital-hit-by-cyber-attack-while-in-the-midst-of-a-covid-19-outbreak/
[23] https://www.mitre.org/sites/default/files/pdf/08_1145.pdf, https://csrc.nist.rip/groups/SMA/fisma/ics/documents/Maroochy-Water-Services-Case-Study_briefing.pdf

της περιοχής. Η επίθεση ήταν αποτέλεσμα παραβίασης του ελέγχου 142 αντλιοστασίων λυμάτων (Kayan et al., 2022).

2.6.2.3 Πολιτικές συνέπειες

Η σύνδεση του διαδικτύου με κρίσιμες υποδομές (ενέργεια, επικοινωνίες, μεταφορές, τραπεζικό σύστημα, στρατιωτικά συστήματα) αυξάνει την έκθεση μιας χώρας σε ασύμμετρες επιθέσεις. Οι κυβερνοεπιθέσεις προστίθενται στους παραδοσιακούς κινδύνους για την ασφάλεια ενός κράτους, ανεξάρτητα από το αν καθοδηγούνται από εχθρικές κρατικές οντότητες ή όχι. Η κατασκοπεία, η δολιοφθορά, η αναστάτωση, πλήττουν μια χώρα τόσο σε πρακτικό επίπεδο, αλλά και σε ό,τι αφορά το κύρος και την αντίληψη που έχουν οι πολίτες της, τα εχθρικά κράτη αλλά και οι συμμαχικές δυνάμεις για την αποτρεπτική της ικανότητα.

Επιπρόσθετα, η ασάφεια για την προέλευσή των κυβερνοεπιθέσεων μπορεί να οδηγήσει σε κατηγορίες μεταξύ κρατών που είναι δύσκολο να τεκμηριωθούν και να αποδειχθούν, καθώς επίσης και κλιμακώσεις της όξυνσης και διπλωματική εμπλοκή, σε περίπτωση που επιλεχθεί αντίδραση μέσω αντιποίνων (Nye, 2017; Rid, 2011).

2.6.3 Κόστος ανάκαμψης και αποκατάστασης

Η ανάκαμψη και η αποκατάσταση συστημάτων, λειτουργιών και αξιοπιστίας απαιτεί χρήματα και πόρους από την πλευρά των επιχειρήσεων και των οργανισμών. Το αντίκτυπο μιας επίθεσης μπορεί να προκαλέσει μη αναμενόμενα έξοδα, όπως η ανάγκη για εξωτερική υποστήριξη ή βοήθεια από ειδικούς δημοσίων σχέσεων[24].

2.7 Νομικό πλαίσιο, Θεσμοί και Πολιτικές Κυβερνοασφάλειας

2.7.1 Ευρωπαϊκή Ένωση

Στην Ευρωπαϊκή Ένωση βρίσκεται σε εξέλιξη μια προσπάθεια διαμόρφωσης ενός ενιαίου πλαισίου κυβερνοασφάλειας, με τη νομοθέτηση κανονισμών οι οποίοι έχουν άμεση νομική ισχύ για τα κράτη μέλη, καθώς και με την έκδοση της οδηγίας NIS2 (αντικαθιστά την οδηγία NIS/2016) η οποία θα πρέπει να ενσωματωθεί στις εθνικές νομοθεσίες με τροποποίηση υφιστάμενων νόμων ή την θέσπιση νέου νομικού πλαισίου.

[24] https://techcrunch.com/2021/08/18/ransomware-recovery-can-be-costly-and-not-just-because-of-the-ransom/

2.7.1.1 Οδηγία (ΕΕ) NIS2 (2022/2555)

Η οδηγία NIS2 στοχεύει στην οριζόντια βελτίωση της κυβερνοανθεκτικότητας με:

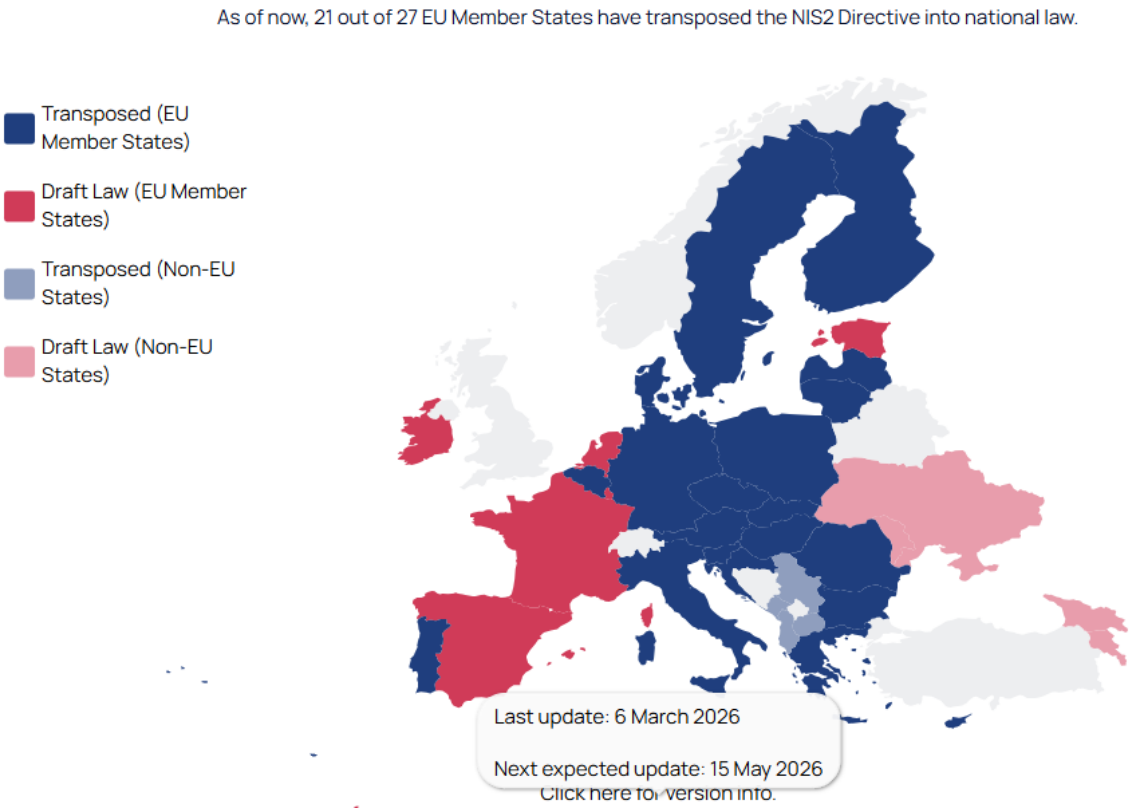
- τη δημιουργία ενός συνεκτικού κανονιστικού πλαισίου, κοινού για τα κράτη μέλη, που θα καταστήσει την διασυνοριακή δραστηριότητα ασφαλέστερη και καλύτερα διαχειρίσιμη.
- τη θέσπιση μηχανισμών συνεργασίας μεταξύ των αρμόδιων φορέων κάθε κράτους.
- τη διεύρυνση της εφαρμογής κανόνων κυβερνοασφάλειας σε περισσότερους τομείς και δραστηριότητες της οικονομίας, εν συγκρίσει με την προηγούμενη οδηγία, καθώς και την προστασία δικτύων και συστημάτων πληροφορικής που κρίνονται κρίσιμα για κάθε χώρα με βάση την οικονομία της.

Η οδηγία αναφέρεται σε *οντότητες ιδιαίτερης κρισιμότητας* (essential entities) και σε *σημαντικές οντότητες* (important entities). Η κατάταξη των οργανισμών στις δύο κατηγορίες λαμβάνει χώρα με βάση τον τομέα δραστηριότητας[25] σε συνάρτηση με το μέγεθος και τη σημασία τους για την κοινωνία και την οικονομία της κάθε χώρας.

Τα άρθρα 21, 22 και 23 της οδηγίας (Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο της ΕΕ, 2022) θεσπίζουν ρητά την υποχρέωση από την πλευρά των οργανισμών (α) να αξιολογούν τους κινδύνους που διατρέχουν, (β) να διαθέτουν μηχανισμούς ανίχνευσης περιστατικών κυβερνοασφάλειας, (γ) να αναφέρουν τα περιστατικά εντός προκαθορισμένου χρονικού πλαισίου, (δ) να διασφαλίζουν την επιχειρησιακή συνέχεια και την ασφάλεια της αλυσίδας εφοδιασμού και (ε) να οργανώνουν τη δυνατότητα ανάκαμψης τους από καταστροφές. Η οδηγία αναφέρεται σε τεχνικά μέτρα προστασίας (κρυπτογραφία, πολυπαραγοντική ταυτοποίηση κ.λπ.) μόνο σε γενικό επίπεδο, χωρίς να δεσμεύει σε συγκεκριμένες επιλογές. Επίσης, αν και στο προοίμιο γίνεται αναφορά σε διεθνή πρότυπα, η εφαρμογή αυτών δεν είναι υποχρεωτική καθώς η εστίαση δίδεται στο επιδιωκόμενο αποτέλεσμα και όχι σε τεχνικές ή προϊόντα.

Η οδηγία βρίσκεται, ακόμη, σε πορεία ενσωμάτωσης στις εθνικές νομοθεσίες, αν και η σχετική προθεσμία (17/10/2024) έχει παρέλθει. Σύμφωνα με τον Ευρωπαϊκό Οργανισμό Κυβερνοασφάλειας, 21 από τις 27 χώρες-μέλη της Ευρωπαϊκής Ένωσης έχουν ενσωματώσει την οδηγία στις εθνικές τους νομοθεσίες, ενώ σε άλλες 6 χώρες διατηρούνται εκκρεμότητες (Σχήμα 7).

[25] Με κριτήριο τον τομέα: ιδιαίτερης κρισιμότητας οντότητες είναι η ενέργεια, οι μεταφορές ,η υγεία, η ύδρευση, οι τράπεζες, η δημόσια διοίκηση, οι ψηφιακές υποδομές κ.ά. και σημαντικές οντότητες είναι η διαχείριση αποβλήτων, η παραγωγή/επεξεργασία/διανομή τροφίμων, οι ταχυδρομικές υπηρεσίες , η βιομηχανία, η έρευνα κ.ά.



Σχήμα 7. Ενσωμάτωση της οδηγίας NIS2 έως 06/03/26[26]

Το γεγονός ότι αυτή δεσμεύει τα κράτη ως προς τον επιδιωκόμενο στόχο, αφήνοντας περιθώρια επιλογών ως προς τον τρόπο εφαρμογής της, έχει οδηγήσει σε διαφορετικές προσεγγίσεις. Με βάση το ECSO NIS2 Implementation White Paper του 2025 (ESCO, 2025), η ανομοιομορφία στα οργανωτικά και τεχνικά μέτρα που λαμβάνουν οι χώρες μέλη, επηρεάζει αρνητικά τον στόχο ενός ενιαίου υψηλού επιπέδου κυβερνοασφάλειας, το οποίο είναι απαραίτητο σε μια οικονομία που διαμορφώνεται και λειτουργεί διασυνοριακά. Ως παραδείγματα διαφορετικών προσεγγίσεων, η Ουγγαρία διεύρυνε το πεδίο εφαρμογής της οδηγίας, στις οντότητες παραγωγής τσιμέντου, ασβέστη και γύψου, ενώ το Βέλγιο θεωρεί την πιστοποίηση ISO 27001 (NQA, 2022) ισοδύναμη με την εκπλήρωση των απαιτήσεων της NIS2. Σημαντικές διαφοροποιήσεις, μεταξύ των χωρών, εμφανίζονται ως προ την κατηγοριοποίηση των υπόχρεων οντοτήτων αλλά και την αναφορά συμβάντων. Από την πλευρά των οργανισμών, όσοι έχουν ήδη διαμορφωμένη κουλτούρα κυβερνοασφάλειας εφαρμόζουν πιο ώριμες πρακτικές που διευκολύνουν την εφαρμογή της οδηγίας. Επίσης, οι μικρομεσαίες επιχειρήσεις υστερούν σε πόρους και τεχνογνωσία. Για τους λόγους αυτούς προτείνεται η ομογενοποίηση των προσεγγίσεων και η οργάνωση υποστηρικτικών μηχανισμών.

[26] Πηγή: ESCO (https://ecs-org.eu/activities/nis2-directive-transposition-tracker/)

Στην Ελλάδα, η ενσωμάτωση πραγματοποιήθηκε με τον νόμο 5160/2024 (Εφημερίδα της Κυβερνήσεως, ΦΕΚ Α΄ 195/ 27.11.2024 (Ελληνική Δημοκρατία, 2024)) στον οποίο καθορίστηκε το πλαίσιο ταξινόμησης των ιδιαίτερης κρισιμότητας και σημαντικών οντοτήτων για τη χώρα. Οι οντότητες αυτές υποχρεούνται να εγγράφονται στο αντίστοιχο μητρώο με βάση την κατηγοριοποίησή τους. Ο νόμος προβλέπει την υποχρέωση των οντοτήτων να λαμβάνουν μέτρα ασφάλειας, να προβαίνουν σε αναφορές και δηλώσεις συμβάντων κ.λπ., με εποπτική αρχή την Εθνική Αρχή Κυβερνοασφάλειας, η οποία αποτελεί και τον σύνδεσμο διασφάλισης της διασυνοριακής συνεργασίας. Οι οντότητες ιδιαίτερης κρισιμότητας υπόκεινται σε προληπτική εποπτεία (ex ante), ενώ οι σημαντικές οντότητες υπόκεινται σε εκ των υστέρων ελέγχους (ex post), οι οποίοι πραγματοποιούνται σε περίπτωση εκδήλωσης συμβάντων ή σε περίπτωση που υπάρχει ένδειξη μη συμμόρφωσης.

2.7.1.2 Κανονισμός Digital Operational Resilience Act, DORA (2022/2554)

Ο κανονισμός αυτός, με άμεση εφαρμογή από 17/1/2025, θεσπίζει ένα υψηλών απαιτήσεων πλαίσιο κυβερνοασφάλειας, με πεδίο εφαρμογής την ψηφιακή και επιχειρησιακή ανθεκτικότητα του χρηματοπιστωτικού τομέα. Η εποπτεία δεν περιορίζεται μόνο σε εθνικό επίπεδο[27] αλλά ανατίθεται και σε τρεις ευρωπαϊκές αρχές (EBA, ESMA, EIOPA)[28]. Οι υπόχρεοι οργανισμοί οφείλουν να καθιερώσουν πλαίσια αναγνώρισης, αξιολόγησης και διαχείρισης κινδύνων, να διασφαλίζουν την ασφάλεια των υπηρεσιών που δέχονται από τρίτους, να πραγματοποιούν τακτικές δοκιμές ανθεκτικότητας των συστημάτων τους, να αναφέρουν περιστατικά κυβερνοασφάλειας στους αρμόδιους φορείς και να ανταλλάσσουν πληροφορίες για απειλές και ευπάθειες (European Parliament & Council of the European Union, 2022).

2.7.1.3 Κανονισμός Cybersecurity Act (2019/881)

Ο κανονισμός αφορά την αναβάθμιση του ENISA (European Union Agency for Cybersecurity), ο οποίος υποστηρίζει ιδιωτικούς και δημόσιους οργανισμούς, καθώς και κράτη και θεσμούς της Ε.Ε. σε σχέση με την κυβερνοασφάλεια, ενώ καλείται να παρέχει στην Ευρωπαϊκή Ένωση την

[27] Τράπεζα της Ελλάδος https://www.bankofgreece.gr/en/main-tasks/supervision/dora-digital-operational-resilience-act-for-the-financial-sector?

[28] Ο οργανισμός EBA (European Banking Authority) ασχολείται με την κεφαλαιακή επάρκεια και την ασφάλεια των καταθέσεων (https://www.eba.europa.eu/)

Ο οργανισμός EIOPA (European Insurance and Occupational Pensions Authority) ασχολείται με την εποπτεία των ασφαλειών και των επαγγελματικών συνταξιοδοτικών ταμείων (https://www.eiopa.europa.eu/).

Ο οργανισμός ESMA (European Securities and Markets Authority) έχει σαν αποστολή την εποπτεία των οργανισμών αξιολόγησης πιστοληπτικής ικανότητας, των χρηματοπιστωτικών αγορών και των οργανισμών διαπραγμάτευσης (https://www.esma.europa.eu/).

εμπειρογνωμοσύνη του κατά την χάραξη πολιτικής. Ο οργανισμός, με βάση τον κανονισμό, λειτουργεί ως γραμματεία του δικτύου των Εθνικών Ομάδων Απόκρισης για περιστατικά κυβερνοασφάλειας (CSIRT)[29], διοργανώνει εκπαιδευτικά προγράμματα και ασκήσεις κυβερνοασφάλειας, προάγει την πιστοποίηση προϊόντων και υπηρεσιών, διευκολύνει την επιχειρησιακή συνεργασία μεταξύ των κρατών μελών και υποστηρίζει την συνεργασία με τρίτες χώρες. Στο Σχήμα 8 φαίνονται οι στρατηγικοί στόχοι του ENISA.

Σχήμα 8. Στρατηγικοί στόχοι του ENISA[30]

Ο κανονισμός αφορά επίσης την πιστοποίηση της κυβερνοασφάλειας στον τομέα της τεχνολογίας πληροφοριών και επικοινωνιών για υπηρεσίες, προϊόντα και διαδικασίες. Τα πιστοποιητικά εκδίδονται από ιδιωτικούς ή δημόσιους φορείς και έχουν ισχύ σε ολόκληρη την Ε.Ε. Ο κανονισμός διέπεται από τη φιλοσοφία ότι η ασφάλεια δεν περιορίζεται μόνο στην αξιοποίηση της τεχνολογίας και στην πιστοποίηση, αλλά αφορά και την κυβερνο-ϋγιεινή [31], την ελαχιστοποίηση των κινδύνων που οφείλονται στην ανθρώπινη συμπεριφορά (European Parliament & Council of the European Union, 2019).

[29] Εθνικές Αρχές Κυβερνοασφάλειας Ε.Ε. (https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/national-cybersecurity-organisations), Ελλάδα: Εθνική Αρχή Κυβερνοασφάλειας (https://cyber.gov.gr/el-csirt/)

[30] Πηγή: ENISA, https://www.enisa.europa.eu/news/enisa-news/enisa-unveils-its-new-strategy-on-cybersecurity-for-a-trusted-and-cyber-secure-europe

[31] Η κυβερνο-υγιεινή (cyber hygiene) περιλαμβάνει τακτικές, καθημερινές συνήθειες και βέλτιστες πρακτικές για τη διατήρηση της ασφάλειας των συσκευών, των δεδομένων και των ψηφιακών λογαριασμών. Λειτουργεί ως «ασπίδα» κατά των κυβερνοεπιθέσεων μέσω της χρήσης ισχυρών κωδικών, ενημερωμένου λογισμικού και προσεκτικής διαδικτυακής συμπεριφοράς.

2.7.1.4 Κανονισμός General Data Protection Regulation, GDPR (2016/679)

Ο κανονισμός περί προστασίας των προσωπικών δεδομένων (European Parliament & Council of the European Union, 2016) καθορίζει ένα ενιαίο, εντός της Ε.Ε., νομικό πλαίσιο προστασίας των δεδομένων προσωπικού χαρακτήρα. Ωστόσο θα πρέπει να σημειωθεί ότι η προστασία των προσωπικών δεδομένων δεν συνιστά απόλυτο δικαίωμα, αλλά για ένα δικαίωμα που σταθμίζεται σε σχέση με τη λειτουργία της κοινωνίας και την προστασία άλλων θεμελιωδών δικαιωμάτων (Αιτιολογική σκέψη (4)). Τα προσωπικά δεδομένα των φυσικών προσώπων επιτρέπεται να κυκλοφορούν ελεύθερα εντός Ε.Ε., ωστόσο η αποθήκευση, η επεξεργασία και η διάθεση τους υπόκειται στην νομική αρχή της αναλογικότητας και κάθε σχετική ενέργεια οφείλει να είναι αιτιολογημένη. Επιπλέον παρέχονται στα φυσικά πρόσωπα μια σειρά από δικαιώματα που σχετίζονται με την συλλογή, επεξεργασία και μεταφορά των δεδομένων τους. Το φυσικό πρόσωπο πρέπει να γνωρίζει ποια δεδομένα του συλλέγονται, για ποιον λόγο και για πόσο χρονικό διάστημα. Διατηρεί επίσης το δικαίωμα πρόσβασης στα δεδομένα που το αφορούν και μπορεί να αιτηθεί την διόρθωση ή την διαγραφή τους, εάν δεν υπάρχει νόμιμος λόγος τήρησής τους. Θα πρέπει επίσης να του παρέχεται η δυνατότητα ενημέρωσης για δεδομένα τα οποία διαβιβάζονται σε τρίτους.

Το άρθρο 32 (β), αναφέρει την υποχρέωση εφαρμογής κατάλληλων οργανωτικών και τεχνικών μέτρων, που να διασφαλίζουν το απόρρητο, την ακεραιότητα, την διαθεσιμότητα και την αξιοπιστία των συστημάτων και των υπηρεσιών επεξεργασίας των προσωπικών δεδομένων, σε συνεχή βάση.

Σε περίπτωση διαρροής δεδομένων (data breach) ο οργανισμός υποχρεούται να αναφέρει το γεγονός στην αρμόδια εποπτική αρχή[32] (αρθ.33) εντός 72 ωρών και αν υπάρχει υψηλός κίνδυνος στους άμεσα εκτιθέμενους (αρθ.34).

2.7.2 Χώρες εκτός Ε.Ε.

2.7.2.1 ΗΠΑ

Σε επίπεδο θεσμών, πρωτεύοντα ρόλο διαδραματίζουν η ομοσπονδιακή υπηρεσία CISA και το Εθνικό Ινστιτούτο NIST. Η υπηρεσία Κυβερνοασφάλειας και Ασφάλειας Υποδομών (Cybersecurity and Infrastructure Security Agency-CISA)[33] έχει σαν αποστολή τον συντονισμό της ασφάλειας των κρίσιμων υποδομών σε εθνικό επίπεδο. Η CISA ενισχύει την συνεργασία μεταξύ της ομοσπονδιακής

[32] Λίστα Αρμόδιων Αρχών Προστασίας Προσωπικών Δεδομένων στην Ε.Ε (https://digital-strategy.ec.europa.eu/lt/node/289?), Ελλάδα: https://www.dpa.gr/el/enimerwtiko/nomothesia/proswpikon_dedomenon

[33] https://www.cisa.gov/about

κυβέρνησης και της βιομηχανίας δίνοντας έμφαση στην ασφάλεια των επικοινωνιών και των υποδομών. Σύμφωνα με το νομικό πλαίσιο που αφορά τις κρίσιμες υποδομές (Cyber Incident Reporting for Critical Infrastructure Act-CIRCIA) και τις κανονιστικές πράξεις τις CISA με τις οποίες αυτό εξειδικεύεται, τα περιστατικά κυβερνοασφάλειας, θα πρέπει να αναφέρονται στην CISA εντός 72 ωρών (Department of Homeland Security & Cybersecurity and Infrastructure Security Agency, 2024)[34] .

Το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας (National Institute of Standards and Technology-NIST)[35] παρέχει στον ιδιωτικό και τον δημόσιο τομέα στρατηγικές κατευθύνσεις κυβερνοασφάλειας όπως το πλαίσιο NIST Cybersecurity Framework 2.0, 2024 και το Πλαίσιο ανάπτυξης ασφαλούς λογισμικού (NIST Secure Software Development Framework) (The White House, 2023).

Στις ΗΠΑ δεν υπάρχει ένα ενιαίο νομοθετικό πλαίσιο κυβερνοασφάλειας αλλά ένα πλέγμα ομοσποδιακών νόμων που ισχύουν σε ολόκληρη την επικράτεια και νόμων που ισχύουν σε επίπεδο πολιτείας[36].

Επίσης σε ομοσπονδιακό επίπεδο υπάρχουν γενικοί νόμοι (FISMA [37], CIRCIA (Department of Homeland Security & Cybersecurity and Infrastructure Security Agency, 2024)) και νόμοι που αφορούν ευαίσθητους κλάδους όπως η Υγεία και τα Χρηματοπιστωτικά ιδρύματα. Παράλληλα η χρήση του εθελοντικού πλαισίου κυβερνοασφάλειας που παρέχει το NIST και των προτύπων της οικογένειας ISO έχουν απήχηση στις επιχειρήσεις και αποτελούν σημαντικό μέρος της κυβερνοασφάλειας. Η κυβερνοασφάλεια στις ΗΠΑ έχει σε μεγάλο βαθμό διαμορφωθεί στην λογική της εθελοντικής συμμόρφωσης, ωστόσο η θέσπιση του CIRCIA που επιβάλει την υποχρεωτική αναφορά περιστατικών αλλά και πληρωμών ransomware δείχνει μια πρόθεση για μεγαλύτερη εμπλοκή της Διοίκησης (Fahey, 2024).

2.7.2.2 Κίνα

Η Κίνα αντιμετωπίζει τον κυβερνοχώρο στο πλαίσιο της κυβερνο-κυριαρχίας (cyber sovereignty), της αντίληψης δηλαδή ότι ένα κυρίαρχο κράτος έχει το δικαίωμα να ελέγχει πλήρως τον εθνικό του κυβερνοχώρο. Η έννοια της κυβερνο-κυριαρχίας δεν ταυτίζεται με την έννοια της κυβερνοασφάλειας,

[34] https://www.cisa.gov/sites/default/files/2024-04/CIRCIA%20NPRM%20Overview%20V2%28FINAL%29_508c%20%28locked%29.pdf
[35] https://www.nist.gov/about-nist
[36] Cybersecurity 2025 Legislation, https://www.ncsl.org/technology-and-communication/cybersecurity-2025-legislation, l.ac.6/1/26
[37] Αφορά την ασφάλεια των πληροφοριακών συστημάτων των Ομοσπονδιακών Υπηρεσιών, https://en.wikipedia.org/wiki/Federal_Information_Security_Management_Act_of_2002

καθώς η κυβερνοασφάλεια αποσκοπεί στην προστασία του δικτύου και των λειτουργιών του, ενώ η κυβερνο-κυριαρχία είναι μια ευρύτερη έννοια όπου ή διακυβέρνηση του διαδικτύου περνά από τα κράτη, τις εταιρίες και τις τεχνικές κοινότητες στον αποκλειστικό έλεγχο των κρατών. Η Κίνα προτείνει στην Διεθνή κοινότητα ένα μοντέλο όπου η διακυβέρνηση του Διαδικτύου θα μεταβιβαστεί σε διακυβερνητικά forum, όπως ο ΟΗΕ, με αποκλεισμό κάθε ιδιώτη. Η κριτική που δέχεται αυτό το μοντέλο είναι πως μετατοπίζει την προοπτική του διαδικτύου από ένα εργαλείο επικοινωνίας σε μια σφαίρα κρατικού ελέγχου που μπορεί να περιορίσει τις ροές δεδομένων (Gjesvik & Schia, 2017).

Με βάση το υπάρχον νομοθετικό πλαίσιο, η κυβερνοασφάλεια αποτελεί μέρος της εθνικής ασφάλειας, της κοινωνικής σταθερότητας και της οικονομικής ευημερίας της χώρας. Μια αξιοσημείωτη αναφορά στον νόμο που διέπει την κυβερνοασφάλεια[38], είναι η υποχρέωση για τοπική αποθήκευση (εντός της χώρας) των κρίσιμων δεδομένων. Σε περίπτωση αναγκαίας παρέκκλισης, λόγω επιχειρηματικών απαιτήσεων, αυτό θα πρέπει να γίνει ακολουθώντας την αξιολόγηση της ασφάλειας των δεδομένων σύμφωνα με τις ρυθμίσεις του κράτους (National People's Congress of China, 2017).

2.7.2.3 Ισραήλ

Το Ισραήλ είναι μια χώρα που αντιμετωπίζει σοβαρό κίνδυνο κυβερνοεπιθέσεων σε δημόσιους και ιδιωτικούς φορείς στα πλαίσια της εμπλοκής της σε γεωπολιτικές συγκρούσεις. Η κυβέρνηση της χώρας έχει υιοθετήσει την άποψη ότι στη σύγχρονη εποχή οι αντιπαραθέσεις μεταφέρονται στον ψηφιακό κόσμο (Tabansky, 2020). Η χώρα επενδύει επίσης στην "ενεργητική κυβερνοάμυνα" ("active defense") εκμεταλλευόμενη ευπάθειες στον χώρο της κυβερνοασφάλειας, σε βάρος όσων αντιλαμβάνεται ως απειλή (Frei, 2020; INCD, 2025).

Ο κεντρικός φορέας κυβερνοασφάλειας είναι η κρατική-κυβερνητική υπηρεσία Israel National Cyber Directorate (INCD)[39], η οποία ενθαρρύνει την ανταλλαγή τεχνογνωσίας ανάμεσα στον στρατό, την ακαδημαϊκή κοινότητα, τον δημόσιο και τον ιδιωτικό τομέα, στη βάση της καθιερωμένης, στο πλαίσιο της χώρας, αντίληψης ότι ο κυβερνοχώρος αποτελεί έναν ενιαίο εθνικό χώρο. Επιπλέον η κρατική

[38]Article 37: Critical information infrastructure operators that gather or produce personal information or important data during operations within the mainland territory of the People's Republic of China, shall store it within mainland China. Where due to business requirements it is truly necessary to provide it outside the mainland, they shall follow the measures jointly formulated by the State cybersecurity and informatization departments and the relevant departments of the State Council to conduct a security assessment; where laws and administrative regulations provide otherwise, follow those provisions.(Cybersecurity Law of the People's Republic of China, 2017, https://digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017/)

[39] Israel National Cyber Directorate , https://www.gov.il/en/departments/israel_national_cyber_directorate/govil-landing-page , https://govextra.gov.il/israel-national-cyber/cyberexhibition-en/home/

υποστήριξη στην καινοτομία, στοχεύει τόσο την κυβερνοασφάλεια όσο και στην στήριξη της επιχειρηματικότητας στον τομέα της υψηλής τεχνολογίας (Cristiano, 2021).

Συγκριτικά με ότι συμβαίνει στην Ε.Ε., η δημοσίευση της κρατικής αρχής INCD για τη στρατηγική κυβερνοασφάλειας του 2025 αναγνωρίζει κενό νόμου στον καθορισμό των ουσιωδών οντοτήτων και των υποχρεώσεών τους και προαναγγέλλει ρύθμιση στα πρότυπα άλλων αναπτυγμένων κρατών. Ωστόσο η INCD δεν περιορίζεται σε συμβουλευτικό ή εποπτικό ρόλο, όπως οι αρχές εντός Ε.Ε., αλλά αναλαμβάνει και επιχειρησιακό ρόλο σε περιστατικά κυβερνοεπιθέσεων που αφορούν τον τομέα της οικονομίας. Υπάρχει σχεδιασμός κρατικής υποστήριξης 24/7 στις επιχειρήσεις, παρεχόμενος από την επιχειρησιακή μονάδα ανταπόκρισης σε περιστατικά (CERT[40]) (Frei, 2020), η οποία αποτελεί τμήμα της INCD και διαθέτει ομάδες προληπτικής ανίχνευσης, μετριασμού και αντιμετώπισης απειλών.

2.8 Πλαίσια κυβερνοασφάλειας και κυβερνοανθεκτικότητας

Τα πλαίσια κυβερνοασφάλειας (Cybersecurity Frameworks-CSFs) αναπτύσσονται από ιδρύματα, κράτη, διεθνείς οργανισμούς, καθώς και εταιρίες, και παρέχουν κατευθύνσεις, γενική δομή και μεθοδολογία για την εφαρμογή και αξιολόγηση πρακτικών μείωσης και διαχείρισης κινδύνου στον κυβερνοχώρο. Τα πλαίσια είναι ευέλικτα και οι οργανισμοί μπορούν να επιλέξουν αν θα υιοθετήσουν ολόκληρο το πλαίσιο ή ένα τμήμα του. Στον τομέα της κυβερνοασφάλειας αφορούν το ανώτερο επίπεδο οργάνωσης (NIST, 2024; Taherdoost, 2022; Toussaint et al., 2024).

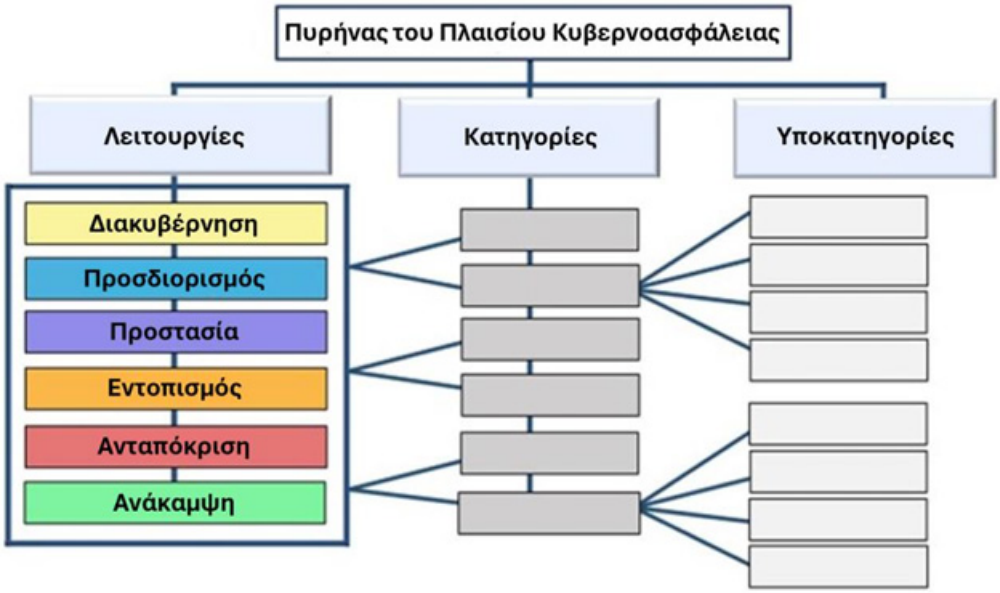
2.8.1 NIST Cybersecurity Framework

Το NIST Cybersecurity Framework σχεδιάστηκε από Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας (National Institute of Standards and Technology - NIST) των ΗΠΑ με τη συνεργασία εθνικών και διεθνών οργανισμών από τον τομέα της βιομηχανίας, κρατικών φορέων και πανεπιστημίων. Παρέχει μια κοινή γλώσσα επικοινωνίας για χρήση τόσο από τεχνικά όσο και μη τεχνικά στελέχη. Μπορεί να προσαρμοστεί σε επιχειρήσεις που δραστηριοποιούνται σε διαφορετικούς τομείς και αντικείμενα, καθώς και σε επιχειρήσεις που έχουν διαφορετικά μεγέθη και ανεξάρτητα από το επίπεδο ωριμότητας τους σε σχέση με την κυβερνοασφάλεια (Taherdoost, 2022). Το πρότυπο παρέχει δωρεάν εργαλεία και καθοδήγηση για την εφαρμογή του. Αποτελείται από τρία τμήματα, (α) τον Πυρήνα, (β) τα Προφίλ και (γ) τις Βαθμίδες Υλοποίησης (tiers). Ο Πίνακας 9 παρουσιάζει συνοπτικά τα τρία αυτά τμήματα.

[40]The Israeli Cyber Emergency Response Team (CERT) https://www.gov.il/en/pages/119en

Πυρήνας	Προφίλ	Βαθμίδες Υλοποίησης
•Λειτουργίες •Κατηγορίες (μονοσήμαντα ορισμένες σε σχέση με τις λειτουργίες) •Υποκατηγορίες (μονοσήμαντα ορισμένες σε σχέση με τις κατηγορίες) •Μέτρα ασφάλειας NIST SP 800-53	•Τρέχον Προφίλ •Προφίλ-Στόχος	•(1) Μερική Υλοποίηση •(2) Επίγνωση Κινδύνου •(3)Επαναλαμβανόμενες πρακτικές •(4)Προσαρμοζόμενες πρακτικές

Πίνακας 9. Τμήματα του πλαισίου κυβερνοασφάλειας NIST.



Σχήμα 9. Πυρήνας Πλαισίου Κυβερνοασφάλειας NIST 2.0 (NIST, 2025a)

2.8.1.1 Πυρήνας

Ο πυρήνας του πλαισίου (έκδοση 2.0) περιλαμβάνει έξι λειτουργίες:

1. **Διακυβέρνηση**. Ορίζεται η στρατηγική διαχείρισης κινδύνων, οι προσδοκίες και η πολιτική του οργανισμού.
2. **Προσδιορισμός**. Προσδιορίζονται οι τρέχοντες κίνδυνοι.
3. **Προστασία**. Αξιοποιούνται μέτρα προστασίας.
4. **Εντοπισμός**. Εντοπίζονται επιθέσεις και παραβιάσεις.

5. **Ανταπόκριση**. Υλοποιούνται ενέργειες για την αντιμετώπιση περιστατικού.
6. **Ανάκαμψη**. Αποκατάσταση λειτουργίας.

Ο κάθε οργανισμός επιλέγει τις Κατηγορίες και τις Υποκατηγορίες του πυρήνα κυβερνοασφάλειας που διαμορφώνει. Για παράδειγμα η λειτουργία ***Εντοπισμός***, περιλαμβάνει δύο κατηγορίες:

A. Συνεχής παρακολούθηση
B. Ανάλυση ανεπιθύμητων συμβάντων

Ο οργανισμός θα επιλέξει και τις 2 Κατηγορίες ή μία από αυτές ανάλογα με την δυναμική και τους πόρους του. Επιπλέον, το πλαίσιο προτείνει μια σειρά από Υποκατηγορίες για την υλοποίηση της κάθε Κατηγορίας και ο κάθε οργανισμός επιλέγει εκείνες που μπορεί να υποστηρίξει.

Ας υποθέσουμε ότι θα επιλεγεί μόνο η Κατηγορία «Συνεχής παρακολούθηση» η οποία αποσκοπεί στην ύπαρξη διαρκούς εποπτείας για τα πληροφοριακά συστήματα, έτσι ώστε να εντοπίζονται ανωμαλίες και περιστατικά απειλητικά για την ασφάλεια τους.

Η κατηγορία *Συνεχής Παρακολούθηση* (DE.CM) περιλαμβάνει με τη σειρά της 5 υποκατηγορίες (NIST, 2025a):

- DE.CM-01: Παρακολούθηση δικτύων με σκοπό την ανίχνευση ύποπτων συμβάντων.
- DE.CM-02: Παρακολούθηση του φυσικού περιβάλλοντος των συστημάτων με σκοπό τον εντοπισμό συμβάντων του αφορούν την ασφάλειά τους.
- DE.CM-03: Παρακολούθηση των ενεργειών του προσωπικού και της χρήσης της τεχνολογίας για τον εντοπισμό παραβιάσεων.
- DE.CM-06: Παρακολούθηση των δραστηριοτήτων εξωτερικών παρόχων υπηρεσιών.
- DE.CM-09: Παρακολούθηση υλικού, λογισμικού, περιβάλλοντος χρόνου εκτέλεσης προγραμμάτων, δεδομένων με σκοπό τον εντοπισμό παραβιάσεων.

Η κάθε υποκατηγορία περιγράφει έναν επιδιωκόμενο στόχο που πρέπει να υλοποιηθεί χωρίς ωστόσο να εισάγονται δεσμεύσεις για τα τεχνικά ή οργανωτικά μέτρα που θα επιλεγούν. Ωστόσο οι οργανισμοί μπορούν να χρησιμοποιήσουν τα NIST SP 800-53 controls[41] για τεχνικούς και διοικητικούς ελέγχους ασφάλειας. Για παράδειγμα εάν θέλουμε να υλοποιήσουμε ελέγχους που αφορούν την υποκατηγορία DE.CM-03, το NIST μεταξύ άλλων προτείνει τον έλεγχο «AC-6: Least Privilege» που αφορά τον περιορισμό δικαιωμάτων των χρηστών. Η αντιστοίχιση υποκατηγοριών – προτεινόμενων ελέγχων παρέχεται σε σχετικές λίστες[42].

[41] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf
[42] https://csrc.nist.gov/files/pubs/sp/800/53/r5/upd1/final/docs/csf-pf-to-sp800-53r5-mappings.xlsx

2.8.1.2 Προφίλ

Το Προφίλ, είναι ένα εργαλείο εναρμόνισης των αναγκών και των πόρων ενός οργανισμού με τις Λειτουργίες, τις Κατηγορίες και τις Υποκατηγορίες του Πυρήνα.

Οι οργανισμοί συντάσσουν τρέχοντα προφίλ με βάση το τι υλοποιούν κατά τη δεδομένη χρονική στιγμή και προφίλ-στόχους με βάση το που στοχεύουν. Σαν παράδειγμα, το τρέχον προφίλ μπορεί να αναφέρει ποιες υποκατηγορίες υλοποιούνται (π.χ. παρακολουθούνται τα δίκτυα και οι υπηρεσίες του δικτύου, Υποκατηγορία DE.CM-01, για εντοπισμό συμβάντων) ενώ το προφίλ – στόχος να αναφέρει και τις υποκατηγορίες εκείνες που δεν υλοποιούνται ακόμη αλλά θα ήταν επιθυμητό να υλοποιηθούν (π.χ. επιθυμία επέκτασης και στην Υποκατηγορία DE.CM-03 που αφορά παρακολούθηση του προσωπικού και της χρήσης της τεχνολογίας και έχει συμπεριληφθεί στον πυρήνα). Στη συνέχεια, οι αποκλίσεις μπορούν να αναλυθούν (gap analysis) και ανάλογα με τους πόρους και τις προτεραιότητες των οργανισμών να αναπτυχθεί σχέδιο δράσης για την κάλυψή τους.

Οι οργανισμοί μπορεί να δημιουργούν πολλαπλά προφίλ ανάλογα με τις ανάγκες τους. Επίσης υπάρχουν και τα κοινοτικά προφίλ[43] (community profiles) που προτείνονται από φορείς κλάδων της οικονομίας, οργανισμούς κ.λπ. και αφορούν τομείς δραστηριοτήτων ή συγκεκριμένες απειλές (όπως π.χ. αντιμετώπιση ransomware) (Souppaya, 2025). Τα προφίλ μπορεί να είναι γενικά και να αφορούν όλο τον οργανισμό ή να έχουν πιο περιορισμένα πεδία εφαρμογής (π.χ. συστήματα οικονομικής διαχείρισης ή ακόμη πιο στοχευμένα). Η χρήση τους μπορεί να διαφέρει: για παράδειγμα κάποια προφίλ μπορεί να απευθύνονται σε στελέχη με εξειδικευμένες ευθύνες, ενώ κάποια άλλα να κοινοποιούνται σε συνεργάτες ως έκφραση απαιτήσεων και προσδοκιών.

2.8.1.3 Βαθμίδες υλοποίησης

Οι οργανισμοί επιλέγουν βαθμίδα υλοποίησης ανάλογα με τις ανάγκες και τους πόρους που μπορούν/επιθυμούν να διαθέσουν. Η βαθμίδα υλοποίησης μπορεί να κυμαίνεται ανάμεσα σε ένα βασικό επίπεδο προστασίας (βαθμίδα 1) και σε πιο προχωρημένα επίπεδα (έως επίπεδο 4). Ειδικότερα, τα επίπεδα έχουν ως ακολούθως:

[43] https://www.nist.gov/cyberframework/profiles

Επίπεδο	Τίτλος	Περιγραφή
1	Μερική υλοποίηση	Περιορισμένη επίγνωση κινδύνων σε οργανωσιακό επίπεδο – διαχείριση όταν εμφανιστούν - άγνοια κινδύνων που προέρχονται από προμηθευτές – ενδεχόμενη απουσία διακίνησης πληροφοριών κυβερνοασφάλειας εντός του οργανισμού
2	Επίγνωση Κινδύνου	Επίγνωση κινδύνων – απουσία τυποποιημένων διαδικασιών – γνώση κινδύνων που προέρχονται από προμηθευτές αλλά δεν υπάρχει επίσημη ανταπόκριση- οι πληροφορίες κυβερνοασφάλειας διακινούνται ανεπίσημα
3	Επαναλαμβανόμενες πρακτικές	Υπάρχουν διαδικασίες διαχείρισης κινδύνων – τηρούνται επίσημα οι διαδικασίες – οι πληροφορίες κυβερνοασφάλειας κοινοποιούνται τακτικά εντός του οργανισμού
4	Προσαρμοζόμενες πρακτικές	Συνεχής βελτίωση των διαδικασιών διαχείρισης κινδύνων – οι πληροφορίες κυβερνοασφάλειας κοινοποιούνται συνεχώς στο εσωτερικό του οργανισμού και σε αρμόδια τρίτα μέρη

Πίνακας 10. Βαθμίδες υλοποίησης

Το NIST CFS προσεγγίζει τον κίνδυνο ολιστικά και σε σχέση με την επιχειρησιακή ικανότητα ενός οργανισμού. Στην πράξη το MITRE ATT&CK μπορεί να χρησιμοποιηθεί συμπληρωματικά[44] σε σχέση με υποκατηγορίες του NIST Cybersecurity Framework, προκειμένου να γίνουν κατανοητές τακτικές και τεχνικές απειλών (NIST, 2018a, 2024, 2025a; Taherdoost, 2022; Toussaint et al., 2024).

2.9 Διεθνή κανονιστικά πρότυπα

Σύμφωνα με έναν από τους ορισμούς που παρέχει το NIST[45], ένα πρότυπο είναι ένα έγγραφο που έχει εγκριθεί από αναγνωρισμένο φορέα και καθορίζει για κοινή και επαναλαμβανόμενη χρήση, κανόνες,

[44] Better Together: NIST CSF and ATT&CK™, Troy L Townsend, https://www.nist.gov/system/files/documents/2022/05/03/04-25-2022-MITRE.pdf

[45] https://csrc.nist.gov/glossary/term/standard "a document, established by consensus and approved by a recognized body, that provides for common and repeated use, rules, guidelines or characteristics for activities or their results, aimed at the achievement of the optimum degree of order in a given context. Note: Standards should be based on the consolidated results of science, technology and experience, and aimed at the promotion of optimum community benefits. Sources: NISTIR 8074 Vol. 2 from ISO/IEC Guide 2:2004"

οδηγίες ή χαρακτηριστικά για δραστηριότητες ή τα αποτελέσματά τους, με στόχο την επίτευξη του βέλτιστου βαθμού τάξης σε ένα συγκεκριμένο περιβάλλον εφαρμογής. Το πρότυπο προκύπτει με συναίνεση και θα πρέπει να βασίζεται στην ενσωμάτωση των αποτελεσμάτων της επιστήμης, της τεχνολογίας και της εμπειρίας, προσφέροντας στην κοινότητα τα μέγιστα οφέλη.

Ένα πρότυπο επιχειρεί να περιγράψει ένα ιδανικό μοντέλο λειτουργίας και ταυτόχρονα θέτει στην πράξη ένα ελάχιστο όριο επίτευξης των απαιτήσεών του. Αν και η εφαρμογή ενός πλαισίου κυβερνοασφάλειας δεν είναι προαπαιτούμενο για την εφαρμογή ενός προτύπου, ένα πλαίσιο βοηθά να καθοριστεί ποιο επίπεδο ασφάλειας επιδιώκεται και να αναδειχθεί το πιο κατάλληλο πρότυπο που μπορεί να οδηγήσει στην επίτευξή του. Συνεπώς, ενώ το πλαίσιο διαμορφώνει τις στρατηγικές επιλογές ενός οργανισμού, τα επιλεγόμενα πρότυπα αποτελούν την καθημερινή εφαρμογή λειτουργειών και διαδικασιών για την επίτευξη των στόχων (Malatji, 2023; Taherdoost, 2022; Toussaint et al., 2024).

Η εφαρμογή ενός προτύπου λειτουργεί επίσης και ως ένα οδηγός συμμόρφωσης με κανονιστικές διατάξεις, στις οποίες υπόκειται ο φορέας που το υλοποιεί. Για παράδειγμα όπως προαναφέρθηκε, το Βέλγιο θεωρεί την πιστοποίηση ISO 27001 ισοδύναμη με την εκπλήρωση των απαιτήσεων της NIS2 (ESCO, 2025).

2.9.1 ISO/IEC 27001 (Information security)

Το ISO 27001[46] είναι ένα διεθνές πρότυπο που καθορίζει τις απαιτήσεις για την εφαρμογή ενός πιστοποιημένου συστήματος διαχείρισης της ασφάλειας των πληροφοριών (ISMS) για οργανισμούς και επιχειρήσεις. Το πρότυπο αναπτύχθηκε με τη συνεργασία του Διεθνούς Οργανισμού Τυποποίησης και της Διεθνούς Ηλεκτροτεχνικής Επιτροπής (IEC). Η πρώτη δημοσίευση του προτύπου έγινε το 2005 και ακολούθησαν αναθεωρήσεις το 2013 και το 2022[47]).

Το πρότυπο περιλαμβάνει 2 μέρη. Το πρώτο μέρος αναφέρει τις 10 ρήτρες, εισαγωγικές (περιγραφές και ορολογία) και απαιτήσεων, που πρέπει να καλυφθούν υποχρεωτικά, για να υπάρχει ένα πιστοποιημένο σύστημα διαχείρισης της ασφάλειας των πληροφοριών (ISMS). Οι απαιτήσεις του προτύπου αφορούν τον καθορισμό του πεδίου εφαρμογής του, την διαχείριση των κινδύνων, την αξιολόγηση της απόδοσης, και τη συνεχή βελτίωση ενός ISMS. Το δεύτερο μέρος του προτύπου

[46] https://www.iso.org/standard/88435.html
[47] https://en.wikipedia.org/wiki/ISO/IEC_27001

(Παράρτημα) παρέχει μια λίστα ενδεικτικών ελέγχων ασφαλείας για την κάλυψη των υποχρεωτικών απαιτήσεων του πρώτου μέρους (NQA, 2022; Toussaint et al., 2024).

Σκοπός ενός ISMS είναι η προστασία ευαίσθητων πληροφοριών (δεδομένα εργαζομένων, πελατών, προμηθευτών), καθώς και πληροφοριών ιδιαίτερης αξίας (πνευματική ιδιοκτησία, επιχειρησιακά δεδομένα, οικονομικά δεδομένα, κ.λπ.). Οι βασικοί κίνδυνοι αφορούν την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα των πληροφοριών (NQA, 2022).

Το συγκεκριμένο πρότυπο, λόγω του κόστους εφαρμογής του, υιοθετείται κυρίως από τον τομέα των υπηρεσιών (πληροφορική, τηλεπικοινωνίες, τράπεζες κ.λπ.) καθώς δεν εξυπηρετεί μόνο τις απαιτήσεις της αγοράς (πελάτες, προμηθευτές) αλλά και κανονιστικές ρυθμιστικές που αφορούν αυτούς τους κλάδους (Barkat Ullah et al., 2025).

2.9.2 ISO 22301 (Business Continuity Management)

Το πρότυπο ISO 22301[48] περιγράφει τις απαιτήσεις ενός Συστήματος Διαχείρισης Επιχειρησιακής Συνέχειας (Business Continuity Management System – BCMS). Σύμφωνα το πρότυπο ISO 22301, η επιχειρησιακή συνέχεια είναι η ικανότητα ενός οργανισμού να συνεχίσει να παρέχει τα προϊόντα που παράγει ή τις υπηρεσίες που προσφέρει σε επίπεδα που έχουν καθοριστεί εκ των προτέρων ως αποδεκτά, μετά από ένα ανατρεπτικό συμβάν το οποίο μπορεί να έχει προκύψει με φυσικό τρόπο (π.χ. πλημμύρα, σεισμός) ή σκόπιμο (εσκεμμένη ανθρώπινη ενέργεια). Το πρότυπο καλύπτει οτιδήποτε μπορεί να θεωρηθεί ανατρεπτικό, συμπεριλαμβάνοντας ενδεικτικά μια φυσική καταστροφή, ένα υγειονομικό γεγονός όπως η πανδημία και οι επιπτώσεις της, έως ένα περιστατικό κυβερνοεπίθεσης (Suresh et al., 2020).

Το πρότυπο δημοσιεύτηκε από τον Διεθνή Οργανισμό Πιστοποίησης το 2012 και ανανεώθηκε το 2019, ακολουθεί δε την κοινή αναφορά των προτύπων ISO αναφορικά με τις 10 υποχρεωτικές ρήτρες, οι οποίες προσαρμόζονται στον στόχο της επιχειρησιακής συνέχειας.

Στο πλαίσια ενός ολοκληρωμένου BCMS, μια βασική ανάλυση είναι η Ανάλυση Επιχειρησιακών Επιπτώσεων (Business Impact Analysis - BIA) που χρησιμοποιείται για να καθοριστούν οι κρίσιμες λειτουργίες και οι ελάχιστοι στόχοι επιχειρησιακής συνέχειας. Από την ανάλυση αυτή είναι δυνατό να προκύψουν οι δείκτες PRO (Recovery Point Objective - μετρά την μέγιστη αποδεκτή απώλεια

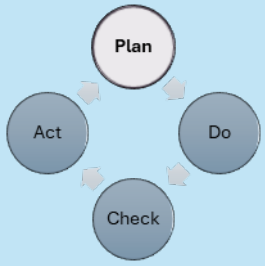
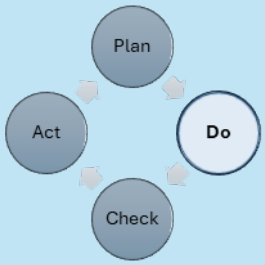
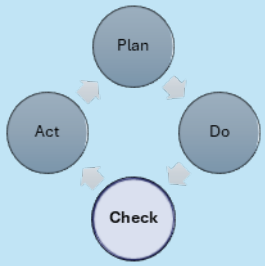
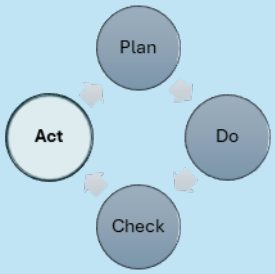
[48] https://www.iso.org/standard/75106.html

δεδομένων) και RTO (Recovery Time Objective - μετρά τον μέγιστο αποδεκτό χρόνο διακοπής της λειτουργίας ενός συστήματος).

Το σχέδιο επιχειρησιακής συνέχειας ενός οργανισμού BCP (Business Continuity Plan) βασίζεται σε μία ανάλυση BIA, λαμβάνοντας υπ' όψιν τις ευθύνες και τους διαθέσιμους πόρους της επιχείρησης (οικονομικούς, τεχνολογικούς και ανθρώπινους). Με βάση τον οδηγό του προτύπου (NQA, 2019) το BCP αφορά «καταγεγραμμένες διαδικασίες που καθοδηγούν έναν οργανισμό να ανταποκριθεί σε μία διατάραξη, να συνεχίσει τη λειτουργία του, να ανακάμψει από τις συνέπειες και να επαναφέρει το επίπεδο της παροχής προϊόντων και υπηρεσιών» (Barkat Ullah et al., 2025; Cascais Brás et al., 2023; NQA, 2019; Suresh et al., 2020; Vengathattil, 2023).

2.9.3 Κύκλος Σχεδιασμού-Εφαρμογής- Εποπτείας-Ενεργειών

Ένα κοινό εργαλείο των προτύπων ISO για τη βελτίωση των συστημάτων διαχείρισης είναι ο κύκλος Σχεδιασμού-Εφαρμογής-Εποπτείας-Ενεργειών (Plan-Do-Check-Act-PDCA) (Malatji, 2023; NQA, 2022). Ο κύκλος αυτός μπορεί να εφαρμόζεται στο σύστημα συνολικά ή σε επιμέρους ενότητες (π.χ. ασφάλεια δικτύου, φυσική ασφάλεια κ.λπ.). Ο κύκλος ενσωματώνει τις απαιτήσεις που υπάρχουν στις ρήτρες για κάθε πρότυπο (Barkat Ullah et al., 2025; Carvalho & Marques, 2019; Cascais Brás et al., 2023; NQA, 2022; Suresh et al., 2020; Toussaint et al., 2024; Vengathattil, 2023). Ο Πίνακας 11 περιγράφει τα στάδια του κύκλου, περιγράφοντας τους ορισμούς του κάθε σταδίου σύμφωνα με τα πρότυπα ISO/IEC 27001 και ISO 22301.

Κύκλος PDCA	Περιγραφή	ISO/IEC 27001 (Ασφάλεια των πληροφοριών)	ISO 22301 (Επιχειρησιακή συνέχεια)
	**Σχεδιασμός**	**Τι απειλείται**	**Τι είναι κρίσιμο να συνεχίσει να λειτουργεί**
		• Οριοθέτηση συστήματος στο οποίο θα εφαρμοστεί το σχέδιο • Ανάλυση κινδύνων • Σχεδιασμός αντιμετώπισης κινδύνων	• Οριοθέτηση συστήματος • Εντοπισμός κρίσιμων διεργασιών και ορίων ανοχής για διακοπές • Ανάλυση κινδύνων • Σχεδιασμός BCP
	**Υλοποίηση**	**Προστασία**	**Απόκριση και Ανάκαμψη**
		• Εφαρμογή τεχνικών, οργανωτικών και φυσικών ελέγχων • Εκπαίδευση προσωπικού • Ημερήσια καταγραφή περιστατικών	• Υιοθέτηση μέτρων ανάκαμψης • Ανάπτυξη διαδικασιών έκτακτης ανάγκης • Εκπαίδευση εργαζομένων • Δοκιμές επιχειρησιακής συνέχειας
	**Εποπτεία και έλεγχος απόδοσης**	**Έλεγχος για Αποτροπή-Περιορισμό**	**Έλεγχος για Αντοχή – Ανάκαμψη**
		• Παρακολούθηση και συνεχείς μετρήσεις • Εσωτερικοί Έλεγχοι • Αξιολόγηση απόδοσης/ ελέγχων του προτύπου	• Αξιολόγηση αποτελεσμάτων δοκιμών επιχειρησιακής συνέχειας • Έλεγχος των συστημάτων επιχειρησιακής συνέχειας
	**Διόρθωση και Βελτίωση**	**Βελτίωση της προστασίας**	**Βελτίωση της αντοχής και της ανάκαμψης**
		• Προληπτικές/Διορθωτικές Ενέργειες • Επανεξέταση πολιτικών • Ενημέρωση της Ανάλυσης Κινδύνου • Βελτίωση διαδικασιών	• Εφαρμογή αλλαγών στρατηγικής • Επικαιροποίηση των σχεδίων ανάκαμψης • Συνεχής βελτίωση ετοιμότητας

Πίνακας 11. PDCA

3 Διαμόρφωση στρατηγικών μετριασμού και ανάκαμψης

3.1 Προετοιμασία για την ανάπτυξη και ανατροφοδότηση στρατηγικής

Η ανάπτυξη και η ανατροφοδότηση μιας στρατηγικής μετριασμού και ανάκαμψης δεν μπορεί να πραγματοποιηθεί χωρίς να έχει προηγηθεί αποτύπωση των προκλήσεων που αντιμετωπίζει ένας οργανισμός. Προς την κατεύθυνση αυτή μπορούν να αξιοποιηθούν μια σειρά από εργαλεία. Στη συνέχεια της παρούσας ενότητας περιγράφονται ορισμένα από αυτά τα εργαλεία.

3.1.1 Αναλύσεις PESTEL/SWOT

Οι αναλύσεις PESTEL/SWOT αξιοποιούνται στο πλαίσιο της διαμόρφωσης της στρατηγικής στο επίπεδο της οργάνωσης μιας επιχείρησης, λαμβάνοντας υπόψιν πολλαπλούς παράγοντες επίδρασης. Αν και δεν παρέχουν πληροφορίες για τον βαθμό επίδρασης του κάθε παράγοντα, παρέχουν μια πρώτη εικόνα των κινδύνων που αντιμετωπίζει η επιχείρηση. Σε περίπτωση που ένας οργανισμός πρέπει να διαχειριστεί έναν ιδιαίτερο κίνδυνο (για παράδειγμα είναι δυνητικός στόχος κοινωνικής μηχανικής) ή ενδιαφέρεται για έναν συγκεκριμένο τομέα της κυβερνοασφάλειας, μπορεί να εξειδικεύσει τις αναλύσεις. Ενδεικτικά η ανάλυση PESTEL (ή PESTLE) έχει χρησιμοποιηθεί σε σχέση με το θέμα της εκπαίδευσης στην κυβερνοασφάλεια[49], ενώ η ανάλυση SWOT έχει αξιοποιηθεί στο πλαίσιο της ενσωμάτωσης της κυβερνοασφάλειας σε κρίσιμα κυβερνοφυσικά συστήματα (Azmi et al., 2025; Banks & Bhowmik, 2025).

Το φαινόμενο των κυβερνοεπιθέσεων αναπτύσσεται στο πλαίσιο του μακροπεριβάλλοντος[50] των επιχειρήσεων και των οργανισμών. Η ανάλυση PESTEL είναι ένα στρατηγικό εργαλείο που αποτυπώνει τους πολιτικούς, οικονομικούς, κοινωνικούς, τεχνολογικούς, περιβαλλοντικούς και νομικούς παράγοντες που συνδέονται με το μακροπεριβάλλον ενός οργανισμού και χρησιμοποιείται για τη διαμόρφωση είτε της γενικής στρατηγικής του, είτε για πιο στοχευμένες στρατηγικές. Μία ανάλυση PESTEL προσαρμοσμένη στην κυβερνοασφάλεια και την κυβερνοανθεκτικότητα μπορεί να λειτουργήσει σαν ένα πρώτο συγκροτημένο βήμα κατανόησης του εξωτερικού περιβάλλοντος μέσα στο οποίο θα πρέπει να ληφθούν στρατηγικές αποφάσεις (Balzano & Marzi, 2025; Ricci et al., 2021).

[49] R.2.1.1. PESTLE analysis results, https://pact-for-skills.ec.europa.eu/system/files/2022-08/PESTLE%20analysis%20results.pdf

[50] Ο όρος *μακροπεριβάλλον* αναφέρεται στους εξωτερικούς παράγοντες που βρίσκονται πέραν των δυνατοτήτων ελέγχου της επιχείρησης ή του οργανισμού. Ο ορισμός αυτός περιλαμβάνει τους οικονομικούς, κοινωνικούς, πολιτικούς, τεχνολογικούς, νομικούς και οικολογικούς παράγοντες που επηρεάζουν το σύνολο του κλάδου ή την οικονομία και όχι μόνο μία εταιρεία/έναν οργανισμό.

Ο Πίνακας 12 παρουσιάζει τις ενότητες που θα μπορούσε ενδεικτικά να περιλαμβάνει μια τέτοια ανάλυση με βάση τη λογική της προσέγγισης PESTEL και όσα καταγράφηκαν στο προηγούμενο κεφάλαιο.

P Political	•Εθνική Στρατηγική Κυβερνοασφάλειας •Γεωπολιτικές εντάσεις
E Economical	• Κόστος κυβερνοεπιθέσεων • Κόστος κυβερνοασφάλειας
S Social	•Ευαισθητοποίηση κοινής γνώμης σε ότι αφορά σημαντικά και ευαίσθητα προσωπικά δεδομένα •Αύξηση επιθέσεων κοινωνικής μηχανικής
T Technologial	•Διεύρυνση της επιφάνειας επιθέσεων (IoT, Cloud, Supply chain κ.λπ.) •Χρήση της τεχνητής νοημοσύνης
E Environmental	•Έκθεση κυβερνοφυσικών συστημάτων σε περιβαντολλογικούς κινδύνους •Ενεργειακή κατανάλωση και ανθεκτικότητα ψηφιακών υποδομών
L Legal	•Κυρώσεις και πρόστιμα •Υποχρέωση αναφοράς περιστατικών κυβενοασφάλειας

Πίνακας 12. Ενδεικτικές ενότητες ανάλυσης PESTEL με προσανατολισμό στην κυβερνοασφάλεια και την κυβερνοανθεκτικότητα

3.1.1.1 Ανάλυση SWOT

Η ανάλυση SWOT (Strengths, Weaknesses, Opportunities, Threats) χρησιμοποιείται από τους οργανισμούς προκειμένου να καταγραφεί μια εικόνα:

- των δυνατοτήτων και των αδυναμιών που πηγάζουν από το εσωτερικό περιβάλλον ενός οργανισμού.
- των ευκαιριών και των απειλών που προέρχονται από το εξωτερικό περιβάλλον ενός οργανισμού. Η ανάλυση PESTEL μπορεί να αξιοποιηθεί ως πηγή για ευκαιρίες και απειλές που σχετίζονται με το μακροπεριβάλλον, ενώ ως πηγές για τα δεδομένα που σχετίζονται με το

μικροπεριβάλλον [51] μπορούν να αντληθούν αναλύοντας πελάτες, προμηθευτές και ανταγωνιστές.

Υιοθετώντας μια ανάλυση SWOT ένας οργανισμός θα πρέπει να απαντήσει σε μια σειρά από ενδεικτικά ερωτήματα, όπως:

1. Εσωτερικό περιβάλλον
    - Υπάρχουν διαθέσιμοι επαρκείς πόροι (άνθρωποι, κεφάλαια κ.λπ.);
    - Υπάρχει κουλτούρα και εκπαίδευση κυβερνοασφάλειας;
    - Υπάρχει συμμόρφωση με πρότυπα;
    - Υπάρχουν τεχνολογίες άμυνας έναντι επιθέσεων;
    - Υπάρχουν εκτεθειμένα ή παρωχημένα συστήματα;
    - Μπορεί ο οργανισμός να διαχειριστεί την ασφάλεια από κινδύνους που προέρχονται από τρίτους;
2. Εξωτερικό περιβάλλον
    - Είναι εκτεθειμένος ο κλάδος και σε απειλές και -εάν ναι- τι είδους;
    - Υπάρχουν αξιόπιστοι συνεργάτες;
    - Πώς αξιοποιείται η τεχνητή νοημοσύνη και οι νέες τεχνολογίες;
    - Πώς διαμορφώνεται η νομοθεσία;
    - Πώς επηρεάζει το κοινωνικό / πολιτικό/οικονομικό περιβάλλον την κυβερνοασφάλεια;
    - Ποιο είναι το επίπεδο κυβερνοασφάλειας των ανταγωνιστών;

Ο Πίνακας 13 παρουσιάζει ενδεικτικά περιεχόμενα μιας ανάλυσης SWOT ενός οργανισμού (Azmi et al., 2025; Banks & Bhowmik, 2025; Bederna et al., 2021).

[51] Το μικροπεριβάλλον αποτελείται από παράγοντες που βρίσκονται πλησίον της εταιρείας/του οργανισμού. Σε αυτό τον ορισμό εμπίπτουν πελάτες, προμηθευτές, ανταγωνιστές, μεσάζοντες και εσωτερικά ενδιαφερόμενα μέρη. Σε αντίθεση με τους μακροοικονομικούς παράγοντες, οι επιχειρήσεις αρκετές φορές διατηρούν κάποιο βαθμό ελέγχου ή επιρροής σε αυτά τα στοιχεία. Βασικά στοιχεία σχετικών αναλύσεων και ενεργειών περιλαμβάνουν την κατανόηση των αναγκών των πελατών, τη διατήρηση των σχέσεων με τους προμηθευτές και την παρακολούθηση των ανταγωνιστικών δράσεων για τη βελτίωση της απόδοσης.

Εσωτερικό Περιβάλλον	
Δυνατά σημεία – Strengths	**Αδύνατα σημεία – Weaknesses**
• Συμμόρφωση με πρότυπα • Ενημερωμένο λογισμικό	▪ Περιορισμένος προϋπολογισμός ▪ Εκτεθειμένες υποδομές ▪ Έκθεση σε κινδύνους από προμηθευτές ▪ Ελλείψεις στην εκπαίδευση του προσωπικού
Εξωτερικό Περιβάλλον	
Ευκαιρίες – Opportunities	**Απειλές – Threats**
• Χαμηλή ωριμότητα κυβερνοασφάλειας στον κλάδο, που συνεπάγεται τη δυνατότητα δημιουργίας ανταγωνιστικού πλεονεκτήματος • Μείωση κόστους συντήρησης συστημάτων και υποδομών	▪ Νομικές συνέπειες/ κυρώσεις από νέους νόμους ▪ Αύξηση περιστατικών ransomware στον κλάδο ▪ Αύξηση περιστατικών κοινωνικής μηχανικής με χρήση τεχνητής νοημοσύνης

Πίνακας 13. Ενδεικτικά περιεχόμενα μελέτης SWOT οργανισμού

3.1.2 Cyber Threat Intelligence (CTI)

Το NIST[52] ορίζει ως Cyber Threat Intelligence (CTI) «πληροφορίες για κυβερνοαπειλές που έχουν συγκεντρωθεί, μετασχηματιστεί, αναλυθεί, ερμηνευτεί ή εμπλουτιστεί για να παρέχουν το απαραίτητο πλαίσιο για τις διαδικασίες λήψης αποφάσεων». Η συλλογή και ανάλυση πληροφοριών (CTI) σχετικά με τις κυβερνοεπιθέσεις διευκολύνει την αναγνώριση των κινήτρων, του βαθμού οργάνωσης, της τεχνικής ικανότητας και των πόρων που οι επιτιθέμενοι διαθέτουν (Mavroeidis et al., 2021).

Πρόσφατη έρευνα (Furumoto et al., 2026) αναφέρει ότι οι οργανισμοί και οι επιχειρήσεις χρησιμοποιούν πολλαπλές πηγές για άντληση πληροφοριών, συμπεριλαμβάνοντας εσωτερικές πηγές, δημόσιες βάσεις δεδομένων (όπως η αμερικάνικη National Vulnerability Database (NVD) [53], αποθετήρια, προμηθευτές, παρόχους κυβερνοασφάλειας, συνδρομητικές υπηρεσίες, τον σκοτεινό

[52] https://csrc.nist.gov/glossary/term/cyber_threat_intelligence
[53] https://nvd.nist.gov/

ιστό, καθώς και ανοικτές πηγές όπως ιστολόγια και forum. Ένα μεγάλο μέρος των δεδομένων είναι μη δομημένα (όπως αφηγήσεις σε ιστολόγια). Η αξιοποίηση όλων αυτών των πληροφοριών διευκολύνεται από τις τεχνολογίες της μηχανικής μάθησης και της βαθιάς μάθησης. Ωστόσο η έρευνα επισημαίνει ότι πολλές σημαντικές πληροφορίες ενδέχεται να βρίσκονται εκτός του συνόλου των πληροφοριών της περιοχής «TLP:CLEAR» του Traffic Light Protocol (TLP) (ήτοι των πληροφοριών που δεν διέπονται από περιορισμούς κοινοποίησης) και να υπάρχει πρόσβαση σ' αυτά μόνο από κλειστές ομάδες.

Η MITRE παρέχει δωρεάν, μέσω του GitHub[54], τα CTI Blueprints, τα οποία είναι σύνολα οδηγιών και προτύπων για τη δημιουργία αναφορών αξιοποιήσιμων από την διοίκηση και τους τεχνικούς της κυβερνοασφάλειας. Στα πρότυπα αυτά υπάρχει δυνατότητα καταχώρησης δομημένης (όπως Technique ID) και μη δομημένης πληροφορίας (ελεύθερο κείμενο).

Τα 4 πρότυπα της MITRE αφορούν:

- *Έκθεση για τον threat actor* (ποιος ήταν ο επιτιθέμενος, τι τεχνικές ακολουθεί, ποιοι είναι οι στόχοι του κ.λπ.).
- *Ανάλυση περιστατικού* (τι συνέβη, πότε, πώς, τι επηρεάστηκε, πώς αντιμετωπίστηκε κ.λπ.).
- *Αναφορά καμπάνιας* (αφορά σειρά επιθέσεων, συσχέτιση περιστατικών και ποιοτική εκτίμηση κινδύνου για τον οργανισμό).
- *Εκτελεστική έκθεση* (απευθύνεται στα όργανα λήψης αποφάσεων, ενημερώνοντας για συγκεκριμένο κίνδυνο, χωρίς να περιλαμβάνει τεχνικές λεπτομέρειες).

3.1.3 Business Impact Analysis (BIA)

Η εκπόνηση ανάλυσης επιπτώσεων μιας κυβερνοεπίθεσης (BIA) είναι ένα βασικό εργαλείο διαμόρφωσης στρατηγικής για τον μετριασμό των επιπτώσεων μιας κυβερνοεπίθεσης. Καταγράφει τις λειτουργίες ενός οργανισμού, τις επιπτώσεις που έχει η διακοπή τους και τους πόρους που απαιτούνται για την επαναφορά τους. Με την ανάλυση αυτή ταυτοποιούνται, μεταξύ άλλων, οι λειτουργίες εκείνες που είναι κρίσιμες και των οποίων η διασφάλισή είναι καίρια για την επιχειρησιακή συνέχεια.

Η BIA προστατεύει έναν οργανισμό από το να υποστεί μεγαλύτερες απώλειες από βεβιασμένη ή μεροληπτική επιλογή προτεραιοποίησης λειτουργιών προς αποκατάσταση, η οποία θα μπορούσε να

[54] https://github.com/center-for-threat-informed-defense/cti-blueprints , https://github.com/center-for-threat-informed-defense/cti-blueprints/blob/main/README.md

έχει ως αποτέλεσμα την επιλογή κατά προτεραιότητα λειτουργιών των οποίων η διακοπή έχει συγκριτικά μικρότερες οικονομικές ή άλλες συνέπειες σε σχέση με άλλες λειτουργίες.

Οι βασικές έννοιες της BIA έχουν ως ακολούθως:

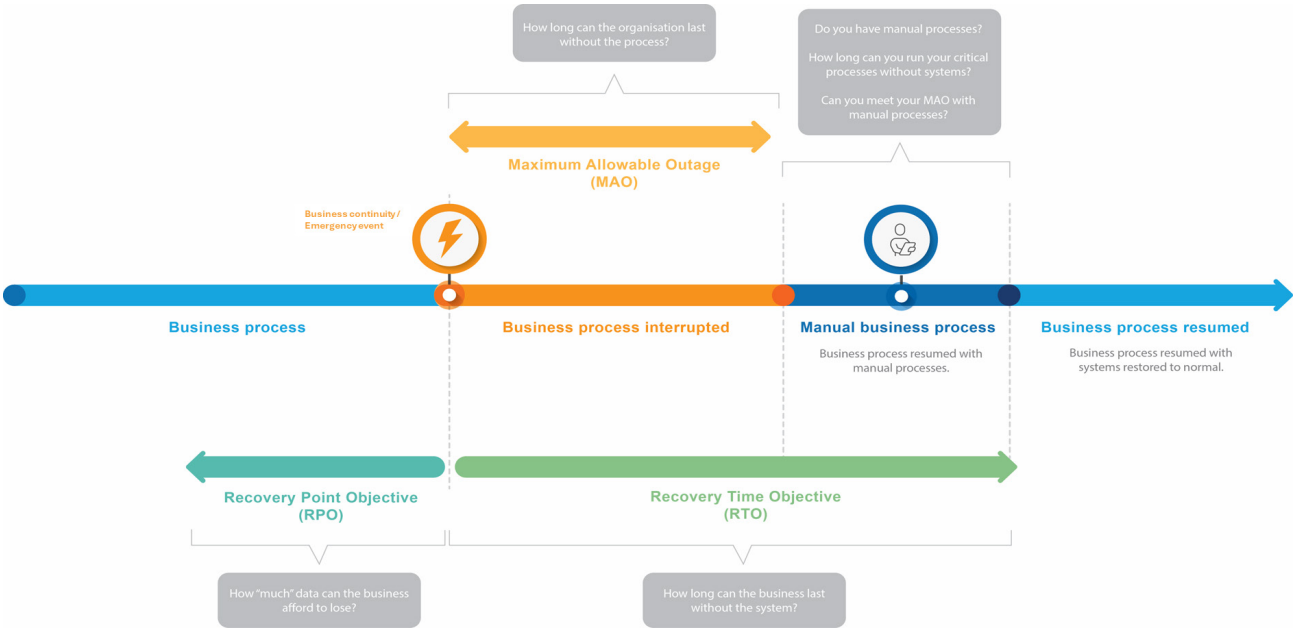
- **Recovery Point Objective (RPO):** Πόσα δεδομένα είναι αποδεκτό να χαθούν, σε μια δεδομένη κλίμακα, λόγω της διατάραξης μιας συγκεκριμένης διαδικασίας.
- **Maximum Allowable Outage (MAO):** Ποιος είναι ο μέγιστος χρόνος που ο οργανισμός μπορεί να υπάρξει χωρίς σοβαρές και μη αναστρέψιμες επιπτώσεις, χωρίς να λειτουργεί η συγκεκριμένη διαδικασία λόγω της διατάραξης.
- **Manual Business Process (MBP):** Μπορεί ο οργανισμός να λειτουργήσει με χειροκίνητες διαδικασίες;
- **Recovery Time Objective (RTO):** Ποιος είναι ο στόχος για τον απαιτούμενο χρόνο αποκατάστασης της διαδικασίας;

Οι επιπτώσεις, οικονομικές και μη οικονομικές, καθώς και οι απαιτούμενοι πόροι αποκατάστασης αξιολογούνται σε σχέση με διαφορετικούς χρόνους ενδεχόμενης διακοπής μιας λειτουργίας (όπως <1h, 1-4h, 4h-1d, κ.λπ.).

Η εφαρμογή της BIA είναι βασικό στοιχείο του προτύπου ISO 22301, ωστόσο αρμόδιοι κυβερνητικοί φορείς προτείνουν την εφαρμογή του ακόμα και ανεξάρτητα από την ένταξη ενός οργανισμού στο πρότυπο (Federal Emergency Management Agency, 2019; Government of South Australia, 2025; HM Government, 2008).

Η BIA συνεισφέρει στη διαμόρφωση στρατηγικής με την ανάδειξη των κρίσιμων διαδικασιών–λειτουργιών ενός οργανισμού. Αυτό που προτείνεται, είτε σε συμμόρφωση με το πρότυπο (ISO 22301) είτε ανεξάρτητα, είναι να δημιουργηθεί ένα σχέδιο επιχειρησιακής συνέχειας (BCP), το οποίο κατευθύνει σε πρακτικό επίπεδο τον μετριασμό των επιπτώσεων και την διαδικασία ανάκαμψης (HM Government, 2008).

Η χρονική εξέλιξη της διατάραξης και της αποκατάστασης στο πλαίσιο της BIA απεικονίζεται στο Σχήμα 10**.**



Σχήμα 10. Χρονική απεικόνιση της διατάραξης των λειτουργιών και της αποκατάστασης τους[55]

3.2 Εφαρμογή ανάλυσης κινδύνου

Τα εργαλεία που ενδεικτικά παρουσιάστηκαν ανωτέρω, παρέχουν προσεγγίσεις με διαφορετική εστίαση, σε ό,τι αφορά την ανάλυση κινδύνου. Ο Πίνακας 14 συνοψίζει τα εργαλεία και την εστίαση του καθενός.

Εργαλείο	Εστίαση
SWOT	*που υστερεί ένας οργανισμός* και από που προέρχονται οι απειλές, σε στρατηγικό επίπεδο
Cyber Threat Intelligence (CTI)	*τι απειλείται συχνότερα*, με ποιον τρόπο και ποιοι είναι οι επιτιθέμενοι, ως επικαιροποιημένη γνώση
Business Impact Analysis (BIA)	*ποιες λειτουργείες είναι κρίσιμες* για την επιχειρησιακή συνέχεια

Πίνακας 14. Εργαλεία ανάλυσης κινδύνου και εστιάσεις

[55] Government of South Australia: https://www.security.sa.gov.au/cyber-security/resources

Από την άλλη πλευρά, τα μαθηματικά μοντέλα και οι νέες τεχνολογίες παρέχουν λύσεις σε σχέση με την ανάλυση κινδύνου, με χρήση και επεξεργασία μεγάλων, πολύπλοκων και ασαφών δεδομένων.

Αναφορικά με τον εντοπισμό των εσωτερικών απειλών, η βαθιά μάθηση σε συνδυασμό με συμπεριφορικά μοντέλα, εντοπίζει περίπλοκες συμπεριφορές χρηστών που μπορεί να αποδοθούν σε κακόβουλες ενέργειες, βελτιώνοντας τις επιδόσεις της κλασσικής μηχανικής μάθησης. Παράλληλα, η επεξεργασία φυσικής γλώσσας για τον εντοπισμό θυμού ή δυσαρέσκειας, σε συνδυασμό με ανίχνευση αλλαγών στα μοτίβα συμπεριφοράς, αποτελεί μια ακόμη προσθήκη στην εργαλειοθήκη ανάλυσης των εσωτερικών κινδύνων (Alzaabi & Mehmood, 2024).

Σε συστήματα παραγωγής αναφέρεται ότι το επίπεδο κινδύνου μπορεί να αξιολογηθεί από μεθόδους βασισμένες στη θεωρία των πιθανοτήτων, τα ασαφή σύνολα (όταν βασιζόμαστε σε δεδομένα που είναι δύσκολο να ποσοστικοποιηθούν[56]) ή τα νευρωνικά δίκτυα (όταν υπάρχουν μεγάλα και πολύπλοκα δεδομένα[57]) (Wu et al., 2018).

Σε ό,τι αφορά την ανίχνευση τεχνικών ευπαθειών, και με δεδομένο ότι ο κίνδυνος ξεκινά από τον εντοπισμό τους από κακόβουλους τρίτους, η τεχνητή νοημοσύνη μπορεί να λειτουργήσει είτε ως σύμμαχος είτε ως απειλή. Είναι σημαντικό να χρησιμοποιείται η τεχνητή νοημοσύνη έγκαιρα από τον οργανισμό, έτσι ώστε να εντοπίζονται οι ευπάθειες και να αντιμετωπίζονται, πριν αυτές εντοπιστούν και αξιοποιηθούν από τους επιτιθέμενους. Η μηχανική μάθηση και η βαθιά μάθηση, συγκρινόμενη με τις παραδοσιακές μεθόδους ανίχνευσης ευπαθειών, παρέχουν αυτοματοποιημένο εντοπισμό χωρίς χειροκίνητους ελέγχους και χωρίς ανθρώπινη επέμβαση. Αυτό δίνει στις ομάδες εργασίας χρόνο να επικεντρωθούν στην επαλήθευση και την αντιμετώπιση των ευπαθειών (Shiri Harzevili et al., 2025).

Η χρήση της τεχνητής νοημοσύνης από hackers, θεωρείται ότι αφορά κυρίως την κοινωνική μηχανική, τη συλλογή πληροφοριών και τον εντοπισμό ευπαθειών. Έως τώρα έχει διαπιστωθεί η εκτεταμένη χρήση της σε επιθέσεις κοινωνικής μηχανικής. Ωστόσο δεν υπάρχει επαρκής πληροφόρηση για την χρήση τεχνητής νοημοσύνης, από κυβερνοεγκληματίες, για εντοπισμό ευπαθειών και πλευρική εξάπλωση απειλών. Το ποιο ανησυχητικό είναι ότι για επιθέσεις zero day που βασίζονται στην εκμετάλλευση τρωτών σημείων σε λογισμικό και υποδομή που μόλις έχουν ανακαλυφθεί (και συνεπώς τα συστήματα άμυνας δεν έχουν ενημερωθεί κατάλληλα για την αντιμετώπισή τους), είναι δυνατό να αξιοποιηθεί η αναζήτηση ευπαθειών με χρήση της τεχνητής νοημοσύνης. Σε σχέση με τα

[56] https://cse.iitkgp.ac.in/~dsamanta/courses/archive/sca/Slides/SCA%20FL-01.pdf
[57] Fangfang Lee, https://www.ibm.com/think/topics/neural-networks

παραπάνω, προκύπτει μια νέα συζήτηση για το πως θα μπορούσαν να αντιμετωπιστούν οι κίνδυνοι από την κακόβουλη χρήση της AI στο πλαίσιο της κυβερνοασφάλειας (Schröer et al., 2024).

3.2.1 Διαχείριση κινδύνων

Η ένταξη των δεδομένων που θα συλλεχθούν σε ένα πλαίσιο διαχείρισης κινδύνου μπορεί να μετατρέψει αποσπασματικές πληροφορίες σε γνώση που μπορεί να αξιοποιηθεί στην λήψη αποφάσεων. Το NIST, εκτός από την ολιστική προσέγγιση της κυβερνοασφάλειας μέσω του Cybersecurity Framework, παρέχει εξειδικευμένα πλαίσια όπως το SP 800-161 και το SP 800-37 που προδιαγράφουν συγκεκριμένα βήματα για την αναγνώριση, αξιολόγηση και διαχείριση των κινδύνων.

Στη στοχευμένη προσέγγιση για τη διαχείριση των κινδύνων της εφοδιαστικής αλυσίδας, το NIST SP 800-161 (NIST, 2022), μέσω του Risk Exposure Framework, παρέχει μια μεθοδολογία για τον εντοπισμό κενών στην ασφάλεια και τη διαχείριση των κινδύνων, βασισμένη στον σχεδιασμό σεναρίων, η οποία υλοποιείται με τα εξής βήματα:

Βήμα		Περιγραφή
1	Σχεδιασμός σεναρίων απειλής	Προετοιμασία της ανάλυσης. Καθορίζονται: • ο σκοπός της ανάλυσης (τι θέλουμε να επιτύχουμε), • το πεδίο εφαρμογής (ποιο τμήμα της αλυσίδας εξετάζεται), • οι πόροι / οι χρόνοι / τα μέσα που θα διατεθούν για την ανάλυση, • τα κριτήρια αξιολόγησης του κινδύνου.
2	Χαρακτηρισμός περιβάλλοντος	Προσδιορισμός: o των κρίσιμων λειτουργειών και σημαντικών εξαρτήσεων, o των πηγών απειλής και των πόρων/δυνατοτήτων τους, o των γνωστών ευπαθειών, o των μέτρων ελέγχου, o των πλαισίων και πρότυπων που ακολουθούνται, o των ανεκτών επιπέδων κινδύνου.
3	Ανάπτυξη σεναρίων απειλής και επιλογή των πιο επιδραστικών	Αφορά: • τους πιθανούς τρόπους εκμετάλλευσης ευπαθειών (με χρήση ιστορικών δεδομένων), • τις πιθανές συνέπειες του κάθε συμβάντος, • την απόρριψη συμβάντων που δεν αφορούν τον σκοπό ή το πεδίο της ανάλυσης, • τις τακτικές και τεχνικές που χρησιμοποιεί η πηγή απειλής, • την επιλογή για περαιτέρω ανάλυση, των σεναρίων με μεγαλύτερη συχνότητα ή αντίκτυπο.

Βήμα		Περιγραφή
4	Ανάλυση κινδύνου για κάθε επιλεγμένο σενάριο	Εντοπίζει: o τις διαδικασίες και τα περιουσιακά στοιχεία που θα πληγούν o τις μονάδες τις επιχείρησης που θα εμπλακούν άμεσα ή θα κληθούν να συμβάλλουν στο περιστατικό με κάποιο τρόπο o τα προγραμματισμένα μέτρα ελέγχου και η συμβολή υφιστάμενων προτύπων, πλαισίων και πολιτικών που αφορούν τον μετριασμό και την επιχειρησιακή ανθεκτικότητα
5	Επιλογή κατάλληλων ελέγχων C-SCRM	Αφορά: • τον εντοπισμό των περιπτώσεων όπου υπάρχει υπέρβαση του αποδεκτού κινδύνου, βάση κριτηρίων • την εκτίμηση της αποτελεσματικότητας των υφιστάμενων μέτρων • την εκτίμηση της δυνατότητας παροχής νέων πόρων για την βελτίωση των μέτρων • την επιλογή των μέτρων που θα κριθούν πιο αποδοτικά
6	Αξιολόγηση και ανατροφοδότηση	Αναφέρεται σε: o δημιουργία ενός πλάνου ελέγχων o αξιολόγηση της αποτελεσματικότητας των μέτρων που επιλέχθηκαν o αξιολόγηση της ανάλυσης o βελτιώσεις όπου κριθεί απαραίτητο

Πίνακας 15 Risk Exprosure Framework NIST SP 800-161

Με δεδομένο ότι οι οργανισμοί πεπερασμένους πόρους και αντίστοιχα περιορισμένη ικανότητα για να αναπτύξουν κάθε τεχνική κυβερνοασφάλειας, θα πρέπει να επιλέξουν πως θα διαχειριστούν κάθε πιθανό κίνδυνο. Σύμφωνα με το NIST SP 800-37, οι πιθανές επιλογές για την διαχείριση ενός κινδύνου είναι *η αποδοχή, η αποφυγή, ο μετριασμός, ο διαμοιρασμός* και *η μεταφορά του κινδύνου* (Bokan & Santos, 2021; NIST, 2018b, 2022; Yang-seo Choi & Dong-il Seo, 2005).

- ***Αποδοχή.*** Αναγνώριση του κινδύνου και λήψη της απόφασης ότι ο κίνδυνος θα εξακολουθήσει να υφίσταται χωρίς να ληφθεί οποιοδήποτε μέτρο. Αν το κόστος για τον μετριασμό του κινδύνου είναι μεγαλύτερο από τις επιπτώσεις του, είναι πιθανό οι οργανισμοί να επιλέξουν την αποδοχή του συγκεκριμένου κινδύνου.
- ***Αποφυγή.*** Αποκλεισμός δραστηριοτήτων που επιφέρουν κίνδυνο. (παράδειγμα: διακοπή συνεργασιών με επισφαλείς προμηθευτές)
- ***Μετριασμός***. Μείωση της πιθανότητας και των επιπτώσεων ενός κινδύνου με εφαρμογή κατάλληλων οργανωτικών και τεχνικών μέσων.
- ***Διαμοιρασμός.*** Αγορά ασφαλιστικής κάλυψης για την αντιμετώπιση των οικονομικών επιπτώσεων.

- ***Μεταφορά του κινδύνου***. Ανάθεση της διαχείρισης της ασφάλειας σε παρόχους (Managed Security Service Provider). Τα συστήματα ασφαλείας έχουν σημαντικό κόστος και απαιτούν εξειδικευμένο προσωπικό. Η συνεργασία με παρόχους μειώνει την ανάγκη για άμεσες επενδύσεις.

Περνώντας από τη στρατηγική προσέγγιση των πλαισίων στο οργανωσιακό και το τακτικό επίπεδο, τα πρότυπα ISO 27001 και 22301, που προαναφέρθηκαν, παρέχουν πιστοποιήσιμα συστήματα διαχείρισης των κινδύνων, τα οποία ενσωματώνουν κυκλικές διαδικασίες συνεχούς βελτίωσης, καλύπτοντας αντίστοιχα την ασφάλεια των πληροφοριών και την επιχειρησιακή ανθεκτικότητα.

3.3 Σχεδιασμός στρατηγικής

Η κυβερνοασφάλεια δεν είναι αυτοσκοπός, αλλά μέσο για να προστατευθούν τα αγαθά του οργανισμού που έχουν πραγματική αξία. Αν η στρατηγική αντιμετώπισης των απειλών, δεν ευθυγραμμίζεται με την αποστολή και τις επιδιώξεις ενός οργανισμού, ακόμη και αν υλοποιηθεί επιτυχώς, δεν θα έχει συνεισφέρει στη δημιουργία αξίας. Ο ρόλος της στρατηγικής είναι διττός. Μέσω της στρατηγικής θα πρέπει να συγχρονιστούν τα μέρη που εμπλέκονται στην επίτευξη της κυβερνοασφάλειας/ανθεκτικότητας, αλλά και να δημιουργηθεί οργανωσιακή αξία, συμβάλλοντας στην βιωσιμότητα ενός οργανισμού (πρβλ. κεφ.4, (Moschovitis, 2018)). Η στρατηγική διαμορφώνει το πλαίσιο, εντός του οποίου, ένας οργανισμός θα επιλέξει, θα διαβαθμίσει και θα συνδυάσει μηχανισμούς μετριασμού και ανάκαμψης για την αντιμετώπιση των απειλών και τη διατήρηση της επιχειρησιακής συνέχειας.

3.3.1 Καθορισμός στόχων

Η διατύπωση των στρατηγικών στόχων ενός οργανισμού κατευθύνεται από την ανάλυση κινδύνου, τους διαθέσιμους πόρους, την υποχρέωση συμμόρφωσης με νομοθετικές ρυθμίσεις και την επιλογή ευθυγράμμισης με πλαίσια και πρότυπα κυβερνοασφάλειας. Παράλληλα, ο καθορισμός στόχων διαμορφώνεται και από την αντίληψη της διάθεσης για έκθεση σε κίνδυνο (“risk appetite”) της διάθεσης μιας επιχείρησης να αναλάβει δραστηριότητες που δημιουργούν αξία και εμπεριέχουν ρίσκο. Η διάθεση για έκθεση για κίνδυνο συνδέεται με τους γενικότερους επιχειρηματικούς στόχους της διοίκησης (Aven, 2013) καθώς και τη φιλοσοφία της.

Η υιοθέτηση της τεχνολογικής καινοτομίας προσφέρει ευκαιρίες για τη δημιουργία αξίας[58], ωστόσο ως προτεραιότητα είναι δυνατό να έρχεται σε αντίθεση με την προτεραιότητα της κυβερνοασφάλειας.

[58] «Value creation comes from projects that generate revenues, save costs, generate efficiencies, improve

Έργα με αντιλαμβανόμενα προβλήματα ως προς τους στόχους της κυβερνοασφάλειας μπορεί να καθυστερήσουν μέχρι να βρεθεί ασφαλέστερη λύση, να ακυρωθούν ή να υλοποιηθούν σε περιορισμένη κλίμακα, ανάλογα με το συμβιβασμό που θα επιλεγεί. Από την άλλη πλευρά, εταιρίες που αντιμετωπίζουν υψηλό ανταγωνισμό και επωφελούνται από την καινοτομία μπορεί να επιδείξουν μεγαλύτερη διάθεση για έκθεση σε κίνδυνο, επαναπροσδιορίζοντας τους στόχους τους (N. Nelson & Madnick, 2017). Στο ίδιο πλαίσιο, αναμένεται επιχειρήσεις και οργανισμοί με χαμηλή διάθεση να αναλάβουν ρίσκο (λόγω νομικών δεσμεύσεων, επιλογών ή άλλων λόγων), να θέτουν αυστηρούς στόχους και να επενδύουν σε υψηλό μετριασμό και γρήγορη ανάκαμψη.

Το πλαίσιο κυβερνοασφάλειας NIST CF 2.0 [59] αναφέρει ότι ο τρόπος εφαρμογής του είναι προσαρμόσιμος, καθώς ο κάθε οργανισμός αντιμετωπίζει τόσο κινδύνους που είναι διαδεδομένοι και αποτελούν κοινό τόπο για επιχειρήσεις, αλλά και κινδύνους που είναι μοναδικοί για τον εν λόγω οργανισμό. Επιπλέον, ο τρόπος εφαρμογής διαμορφώνει ποίκιλες ανοχές και διαθέσεις ανάληψης κινδύνου, εξυπηρετεί διαφορετική αποστολή και θέτει διαφορετικούς στόχους για την επίτευξή της. Οι στόχοι θα πρέπει να είναι σαφείς, μετρήσιμοι, εφικτοί, σχετικοί με την αποστολή του οργανισμού και χρονικά καθορισμένοι (SMART - Specific, Measurable, Achievable, Relevant, Time-Bound)[60].

Σύμφωνα με τη μελέτη (Hubbard & Seiersen, 2016), η αίσθηση της ασφάλειας μέσω της επιλογής των βέλτιστων πρακτικών δεν ισοδυναμεί με επιστημονικά αποδεδειγμένη μείωση των κινδύνων εάν δεν υπάρχουν μετρήσιμα αποτελέσματα. Συνακόλουθα, σε ένα πλάνο κυβερνοασφάλειας θα πρέπει να δηλώνεται ο τρόπος μέτρησης της επιτυχίας. Οι μετρήσεις μπορεί να μην αναφέρονται άμεσα στον στόχο αν αυτός δεν διατυπωθεί με ποσοστικοποιημένα κριτήρια, αλλά στην αποτελεσματική διαχείρισή του, όπως αυτή θα οριστεί από τη διοίκηση. Το ποσοστό των δεδομένων που κρυπτογραφούνται, καθώς και ο αριθμός προσβάσεων που αποτράπηκαν μπορεί να αφορούν τον στόχο της προστασίας κρίσιμων δεδομένων. Οι δείκτες PRO (μέγιστη αποδεκτή απώλεια δεδομένων) και RTO (μέγιστος αποδεκτός χρόνος διακοπής της λειτουργίας ενός συστήματος) μπορεί να αναφέρονται, μεταξύ άλλων, στην εξέλιξη της ανάκαμψης.

Στην έρευνα (Sherif et al., 2024) αναλύεται η επιλογή μετρικών στη διαχείριση της κυβερνοασφάλειας και καταλογογραφείται ένα πλήθος δεικτών που ποσοτικοποιούν ευπάθειες, ανίχνευση επιθέσεων,

customer experience or improve product. Examples of value-creating technology enabled projects:
Mobile applications, ERP, Mobile commerce, Internet of Things projects, Big Data projects. » (Nelson, 2017)

[59] "Nevertheless, the CSF does not embrace a one-size-fits-all approach. Each organization has both common and unique risks, as well as varying risk appetites and tolerances, specific missions, and objectives to achieve those missions."

[60] There's a S.M.A.R.T. Way to Write Management's Goals and Objectives, GT Doran, 1981, Management Review, 1981, v. 70, n. 11, p. 35

χρόνους αποκατάστασης κ.λπ. Οι δείκτες αυτοί μπορούν να αξιοποιηθούν υπό το πρίσμα της προσέγγισης SMART.

3.3.2 Υιοθέτηση επί μέρους πολιτικών και μέτρων προστασίας

Οι οργανισμοί υιοθετούν πλαίσια κυβερνοασφάλειας τα οποία συχνά συμπληρώνονται από επί μέρους πολιτικές προστασίας, οι οποίες αφορούν τομείς ιδιαίτερου ενδιαφέροντος, όπως ο έλεγχος πρόσβασης, η πολιτική κρυπτογράφησης και η προστασία των δεδομένων. Οι πολιτικές αυτές είναι συμβατές αφ' ενός με πρότυπα κυβερνοασφάλειας και αφ' ετέρου νομικές ρυθμίσεις όπως οι κανονισμοί προστασίας των προσωπικών δεδομένων. Επιπρόσθετα, οι πολιτικές παρέχουν διαδικασίες για την αποτελεσματική εφαρμογή των μέτρων μετριασμού και προστασίας από κυβερνοεπιθέσεις.

3.3.2.1 Identity & Access Management (IAM).

Αποτελεί ένα συνδυασμό πολιτικών, τεχνικών και μηχανισμών που στοχεύει να διασφαλίσει ότι μόνο εξουσιοδοτημένοι χρήστες θα έχουν την απαραίτητη πρόσβαση σε συστήματα, διαδικασίες και δεδομένα με σκοπό να επιτελούν τις εργασίες εκείνες που τους έχουν ανατεθεί. Η IAM περιλαμβάνει την Διαχείριση Ταυτοτήτων (την παροχή ταυτότητας χρήστη και την κατάργηση της) και την Διαχείριση Πρόσβασης (επαλήθευση του χρήστη, εξουσιοδότηση με συγκεκριμένα δικαιώματα μετά την ταυτοποίηση και κανόνες βάση των οποίων παρέχονται δικαιώματα, όπως η χρονική διάρκεια). Περιλαμβάνει επίσης την υποβολή εκθέσεων και την διενέργεια ελέγχων συμμόρφωσης (A. Sharma et al., 2015).

Η IAM αποτελεί στρατηγική επιλογή ασφάλειας, η οποία έχει εφαρμοστεί εκτεταμένα εντός τον οργανισμών. Σήμερα αντιμετωπίζει ιδιαίτερες προκλήσεις σε cross-domain περιβάλλοντα, όπου προκύπτουν και θέματα εμπιστοσύνης μεταξύ των συμμετεχόντων οργανισμών, υπάρχει ετερογένεια ταυτοτήτων, διαφορετικές πολιτικές πρόσβασης και δυσκολίες στην ανάκλησή τους. Ως μέτρο η βιβλιογραφία προτείνει την εφαρμογή ομοσπονδιακών μοντέλων διαχείρισης ταυτότητας όπου οι συνεργαζόμενοι οργανισμοί βάση συμφωνίας εμπιστεύονται έναν τρίτο πάροχο που διαχειρίζεται την ταυτότητα των χρηστών ή αποκεντρωμένων μοντέλων όπου η επαλήθευση βασίζεται σε Verifiable Credential (VC)[61] που επιλέγει να παρουσιάσει ο χρήστης κατά βούληση και μπορεί να ελεγχθεί μέσω ενός μητρώου που συχνά βασίζεται στην χρήση της τεχνολογίας blockchain (Badirova et al., 2023).

[61] "Verifiable credential (VC) can be a certificate, diploma, license, or another type of document that can be verified for its legitimacy." (Badirova et al., 2023)

3.3.2.2 Encryption policy

Αφορά την προστασία των δεδομένων (at rest, in transit, in use) είτε είναι αμετακίνητα και αποθηκευμένα σε κάποιο server, σκληρό δίσκο, backup αρχείο ή cloud, είτε μετακινούνται εντός του δικτύου, είτε επεξεργάζονται από κάποια εφαρμογή, με σκοπό την διασφάλιση της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας τους. Βάση της πολιτικής αυτής τα ευαίσθητα δεδομένα εντοπίζονται και αποφασίζεται σε ποιους τομείς εφαρμόζεται η κρυπτογράφηση (cloud, servers κ.λπ.), και με ποια διαδικασία (ποιος δημιουργεί και αποθηκεύει τα κλειδιά, ποιος είναι ο χρόνος ζωής τους κ.λπ.) Οι πολιτικές αυτές εφαρμόζονται σε συμφωνία με κανονιστικές ρυθμίσεις όπως ο GDPR και πρότυπα κυβερνοασφάλειας όπως το ISO/IEC 27001 (AWS, 2026a, 2026b, 2026c; Bonnet, 2022; icom, 2025; National cybersecurity society, 2019, a; University of Bristol, 2025).

Σύμφωνα με τους Vimercati et al. σε έρευνα που αφορά τα δικαιώματα πρόσβασης του παρόχου σε υπηρεσίες cloud και πιθανές ανησυχίες των χρηστών, μια πολιτική κρυπτογράφησης δεν προστατεύει μόνο τα δεδομένα αλλά μπορεί να χρησιμοποιηθεί και για την επιβολή κανόνων πρόσβασης μετατρέποντας τις πολιτικές πρόσβασης σε πολιτικές κρυπτογράφισης. Στο πλαίσιο αυτό η δυνατότητα πρόσβασης στα δεδομένα, συνδέεται με την κατοχή των κατάλληλων κρυπτογραφικών κλειδιών και όχι με τις άδειες που μπορεί να παρέχει το cloud (Vimercati et al., 2010).

3.3.2.3 Data Loss Prevention (DLP)

Σκοπός αυτής της πολιτικής είναι η μη διαρροή ευαίσθητων δεδομένων και ο αποκλεισμός της μη εξουσιοδοτημένης χρήσης τους. Αφορά κυρίως την πνευματική ιδιοκτησία, ιατρικά αρχεία, εταιρικά αρχεία, οικονομικά στοιχεία και προσωπικά δεδομένα. Η προσέγγιση που ακολουθείται είναι ο εντοπισμός των ευαίσθητων δεδομένων, η πρόληψη της πιθανότητας απώλειας και η παρακολούθησή τους είτε είναι ανενεργά, είτε επεξεργάζονται, είτε κινούνται εντός ενός δικτύου (at rest, in use και in transit) με σκοπό την διαρκή προστασία. Η πολιτική αυτή ευθυγραμμίζεται με τις κανονιστικές ρυθμίσεις για την προστασία των δεδομένων (S. Liu & Kuhn, 2010).

3.3.2.4 Μέτρα Προστασίας

Τα μέτρα κυβερνοασφάλειας αποσκοπούν στον μετριασμό των κινδύνων μέσω πρακτικών και οργανωσιακών ενεργειών, υλοποιώντας τις πολιτικές προστασίας.

3.3.2.4.1 Εκπαίδευση χρηστών

Σε έρευνα σχετικά με την εκπαίδευση στην κυβερνοασφάλεια (Alnajim et al., 2023), αναφέρονται παραδοσιακές αλλά και καινοτόμες τεχνικές εκπαίδευσης με διαφορετικό επίπεδο οικονομικού κόστους. Θεωρητική ενημέρωση ή διδασκαλία μέσω διαλέξεων, εξάσκηση σε εργαστηριακό περιβάλλον όπως η διαχείριση ενός firewall, εκμάθηση μέσω παιχνιδοποίησης αλλά και προχωρημένες μορφές προσομοίωσης με χρήση Virtual και Augmented Reality.

Οι στόχοι της εκπαίδευσης μπορεί να περιλαμβάνουν την ανάπτυξη τεχνικών δεξιοτήτων μετριασμού όσο και μη τεχνικών όπως η συνεργασία και η λήψη αποφάσεων υπό πίεση. Εξαρτώνται, επίσης από την εμπειρία των συμμετεχόντων, τα επιλεγμένα σενάρια και το προσδοκώμενο μαθησιακό αποτέλεσμα. Η εκπαίδευση στην κυβερνοασφάλεια είναι απαραίτητο να αξιολογείται ως προς την αποτελεσματικότητα της στην διαχείριση πραγματικών κινδύνων και περιστατικών. Μετρήσεις απόδοσης των εκπαιδευόμενων κατά την διάρκεια ενός προγράμματος και μετά την ολοκλήρωσή του, όπως ο χρόνος απόκρισης, ο αριθμός επιτυχημένων ενεργειών, η ποιότητα τεκμηριώσεων, κ.λπ., συνεισφέρουν στην εκτίμηση της εκπαιδευτικής διαδικασίας και στην μελλοντική κατανομή πόρων βάση αποτελέσματος (Koutsouris et al., 2021).

Μια από τις προκλήσεις στον τομέα της εκπαίδευσης είναι η αντιμετώπιση της κοινωνικής μηχανικής. Ακόμη και χρήστες που είναι ενημερωμένοι για τους κινδύνους μπορεί να παρασυρθούν σε επισφαλείς ενέργειες. Μέσω της εκπαίδευσης οι εργαζόμενοι είναι χρήσιμο να γνωρίσουν τις πολιτικές κυβερνοασφάλειας του οργανισμού τους αλλά και να διαμορφώσουν θετική στάση απέναντι την τήρηση τους, κατανοώντας γιατί είναι σημαντικές, μέσα από ουσιαστικές προσεγγίσεις, όπως οι μελέτες περιπτώσεων (Parsons et al., 2014).

3.3.2.4.2 Έλεγχος ευπαθειών

Οι επιτιθέμενοι προσπαθούν να εντοπίσουν ευπάθειες σε λογισμικό και συστήματα προκειμένου να εξαπολύσουν επιθέσεις. Ο έλεγχος για ευπάθειες αποσκοπεί στην διόρθωσή τους πριν από τον εντοπισμό τους από κακόβουλους τρίτους. Διαδεδομένοι τρόποι ελέγχου είναι:

- Ο Στατικός Έλεγχος Ασφάλειας Εφαρμογών (Static Application Security Testing - SAST): χρησιμοποιείται στην φάση της ανάπτυξης λογισμικού. Ο έλεγχος αυτός γίνεται πριν ο κώδικας εφαρμοστεί σε παραγωγικά συστήματα και δεν διακόπτει λειτουργίες και διαδικασίες. Σε πρόσφατη βιβλιογραφική ανασκόπηση που αφορά την χρήση του, επισημαίνεται αφενός η σημασία του και αφετέρου τα υψηλά ποσοστά ψευδώς θετικών αποτελεσμάτων που πλήττουν

την αξιοπιστία του. Επίσης στην ανασκόπηση αναφέρεται ότι εμπειρικές μελέτες καταδεικνύουν ότι το ποσοστό των τρωτών σημείων που εντοπίζονται, υπολείπονται σημαντικά από αυτά που αποκαλύπτονται στον πραγματικό κόσμο (Dalaq et al., 2025).

- Ο Δυναμικός Έλεγχος Ασφάλειας Εφαρμογών (Dynamic Application Security Testing - DAST): Πρόκειται για δοκιμές κατά την λειτουργία εφαρμογών και αφορά κυρίως εκείνες που δέχονται και απαντούν σε αιτήματα μέσω δικτύου. Στην διάρκεια αυτών των δοκιμών γίνεται ελεγχόμενη μεταφορά κακόβουλων εισόδων (payloads) για αποκάλυψη ευπαθειών μέσω προσομοίωσης κυβερνοεπίθεσης. Ο έλεγχος εντοπίζει ευπάθειες που επιτρέπουν την παραποίηση αιτημάτων προς βάσεις δεδομένων, ακούσιες λειτουργίες σε βάρος χρηστών, έκθεση κωδικών και δεδομένων, αλλοίωση περιεχομένου ιστοτόπων, μη επικυρωμένες ανακατευθύνσεις κ.λπ. (Singh et al., 2024).
- Οι Δοκιμές Διείσδυσης (Penetration Testing). Πρόκειται για μια διαδικασία προσομοίωσης κυβερνοεπίθεσης. Εκτελείται στα πλαίσια του ethical hacking. Πραγματοποιείται κατόπιν υπογεγραμμένης συμφωνίας και στοχεύει στην αποκάλυψη ευπαθειών με τρόπους που χρησιμοποιούν και οι κακόβουλοι hackers. Τα αποτελέσματα της διαδικασίας υποβάλλονται ως αναφορά στον ιδιοκτήτη του συστήματος και ακολουθούν οι διορθώσεις (Altulaihan et al., 2023).
- Χρήση της μηχανικής μάθησης και της τεχνητής νοημοσύνης για την ανίχνευση ευπαθειών.Η μηχανική μάθηση μπορεί να προσαρμόσει τα test ασφάλειας στον πραγματικό χρόνο μαθαίνοντας διαρκώς από πραγματικά συμβάντα. Ο συνδυασμός της με τον στατικό και δυναμικό έλεγχο μπορεί να μειώσει τις λανθασμένα θετικές διαγνώσεις και τον εντοπισμό πραγματικών ευπαθειών. (Paidy, 2023) Σε κυβερνοφυσικά συστήματα με εφαρμογές στην περίθαλψη ασθενών, στις έξυπνες πόλεις, στην βιομηχανία και αλλού, προτείνεται η χρήση της μηχανικής μάθησης για την ανίχνευση ευπαθειών στο υλικό, στο λογισμικό και στο δίκτυο. Τα μοντέλα μηχανικής μάθησης μπορούν να εκπαιδευτούν στην αναγνώριση της κανονικής λειτουργείας και στην συνέχεια να είναι ικανά να εντοπίσουν παρεκκλίσεις από αυτήν (ασυνήθιστη κατανάλωση ενέργειας, ασυνήθιστα μοτίβα μετρήσεων κ.λπ.) που οδηγούν στην αναγνώριση ευπάθειας. Η μηχανική μάθηση θεωρείται ιδιαίτερα χρήσιμη για τον εντοπισμό τρωτών σημείων και την αποφυγή επιθέσεων zero day που βασίζονται στον εντοπισμό άγνωστων ευπαθειών από τους επιτιθέμενους (Abshari & Sridhar, 2025; Saha et al., 2021).

3.3.2.4.3 Προστασία και έλεγχος πρόσβασης

Το έγγραφο NIST SP 800-53 Rev. 5 (NIST, 2020a) σε ευθυγράμμιση με το NIST CSF προτείνει ένα εκτεταμένο πλαίσιο ρυθμίσεων που αφορούν την πρόσβαση σε πληροφοριακά συστήματα, όπως:

- **Αρχή Ελάχιστων Προνομίων (Principle of Least Privilege – PoLP)** Σύμφωνα με την αρχή αυτή η πρόσβαση σε δεδομένα και πληροφοριακά συστήματα υπόκειται σε περιορισμούς και είναι η απολύτως αναγκαία για την διεκπεραίωση συγκεκριμένων εργασιών. Η αρχή αναγνωρίζει την δυνατότητα να υπάρχουν χρήστες ή διεργασίες με προνομιακούς λογαριασμούς (για παράδειγμα ο διαχειριστής ή μια υπηρεσία ασφάλειας που εκτελείται μέσω ενός προγράμματος) που αντιστοιχούν σε αυξημένα αλλά όχι απεριόριστα δικαιώματα και χρήστες με μη προνομιακούς λογαριασμούς με λιγότερα δικαιώματα. Ωστόσο επισημαίνει την ανάγκη περιορισμού των προνομιακών λογαριασμών, την περιοδική επανεκτίμηση παροχής τους και την ανάγκη ελέγχου και ανάλυσης της χρήσης τους. (Control AC-6)
- **Authentication και Multi-Factor Authentication**.Σύμφωνα με το πλαίσιο, η μοναδική αναγνώριση χρήστη εκτός από τον άμεσο προστατευτικό της ρόλο, επιτρέπει την λογοδοσία για την δραστηριότητα των χρηστών. Οι τρόποι ταυτοποίησης που αναφέρονται είναι η χρήση κωδικών, η χρήση βιομετρικών στοιχείων, οι φυσικοί έλεγχοι ταυτότητας και η συνδυαστική πολυπαραγοντική ταυτοποίηση. Η ταυτοποίηση μέσω συνδυασμού παραγόντων (παράδειγμα: κωδικός + βιομετρικά στοιχεία) προτείνεται ιδιαίτερα σε σχέση με τους προνομιακούς λογαριασμούς.

  Σε πιο σύγχρονες προσεγγίσεις προτείνονται επίσης μέθοδοι αυθεντικοποίησης των χρηστών οι οποίες είναι ανθεκτικές σε απόπειρες phishing όπως η FIDO2[62]. Σε αυτή την περίπτωση η ταυτοποίηση γίνεται με την χρήση της ασύμμετρης κρυπτογραφίας όπου το ιδιωτικό κλειδί είναι αποθηκευμένο σε ασφαλή συσκευή που προστατεύεται με την χρήση PIN ή βιομετρικών δεδομένων. Όταν επιχειρείται σύνδεση, το ιδιωτικό κλειδί χρησιμοποιείται για την υπογραφή δεδομένων που στέλνονται από τον ιστότοπο (challenge-response). Η επαλήθευση του νόμιμου χρήστη βασίζεται στο ότι το ιδιωτικό κλειδί μπορεί να χρησιμοποιηθεί μόνο στο αυθεντικό domain.
- Η **Zero Trust Architecture** (αρχιτεκτονική μηδενικής εμπιστοσύνης) όπως περιγράφεται από το NIST Zero Trust Architecture (SP 800-207) αποτελεί επέκταση των αρχών που περιγράφει ο προηγούμενος οδηγός, σε ολόκληρο το δίκτυο ενός οργανισμού. Κάποιες από τις βασικές τεχνικές που υιοθετούνται είναι η αρχή των ελάχιστων προνομίων, η πολυπαραγοντική ταυτοποίηση, η τμηματοποίηση του δικτύου σε μικρότερες απομονωμένες ζώνες και η συνεχής αξιολόγηση κάθε νέου αιτήματος πρόσβασης σε εταιρικό πόρο (υπηρεσία, λογαριασμό δικτύου, περιουσιακά στοιχεία κ.λπ.). Η βασική αρχή της Zero Trust είναι ότι η εμπιστοσύνη θα πρέπει να αξιολογείται συνεχώς και να μην τεκμαίρεται ακόμη και αν κάποιος βρίσκεται

[62] https://www.passkeycentral.org/introduction-to-passkeys/how-passkeys-work , https://www.cisa.gov/sites/default/files/2023-01/fact-sheet-implementing-phishing-resistant-mfa-508c.pdf

ήδη στο δίκτυο ενός οργανισμού. Το περίγραμμα ενός οργανισμού με την υιοθέτηση των υπηρεσιών cloud και την απομακρυσμένη εργασία μεταβάλλεται και είναι δύσκολο να προστατευθεί. Στόχος της αρχιτεκτονικής αυτής είναι ο αποκλεισμός της μη εξουσιοδοτημένης πρόσβασης και η προστασία από την πλευρική εξάπλωση απειλών, προστατεύοντας τον οργανισμό από εσωτερικές και εξωτερικές απειλές (NIST, 2020b, 2020a, 2025b).

3.3.2.4.4 Προστασία δεδομένων

Ο έλεγχος της πρόσβασης σε συστήματα ενισχύει την προστασία των δεδομένων αλλά δεν αρκεί. Ο οδηγός NIST SPECIAL PUBLICATION 1800-28B[63] (2024), ο οποίος αφορά την προστασία των δεδομένων και προσαρμόζεται στο πλαίσιο κυβερνοασφάλειας του NIST, προτείνει κρυπτογράφηση των δεδομένων σε κάθε κατάσταση (at rest, in transit, in use). Προτείνει επίσης ανωνυμοποίηση των απόρρητων δεδομένων ώστε να μην είναι ορατή η σύνδεσή τους με συγκεκριμένα πρόσωπα, αλλά και υιοθέτηση από τους οργανισμούς ενός κύκλου ζωής για τα δεδομένα, που να καταλήγει στην καταστροφή τους όταν δεν υπάρχει λόγος διατήρησης. Αναφορικά με την δευτερογενή χρήση των δεδομένων, ο οδηγός επισημαίνει την ανάγκη να ληφθούν μέτρα ώστε να καταστεί προβλέψιμη και διαχειρίσιμη. Η χρήση των δεδομένων για την επίτευξη της αποστολής ενός οργανισμού ή εμπορικούς σκοπούς δεν αποκλείεται, αλλά συνδέεται με την ανάγκη εφαρμογής τεχνολογιών που ενισχύουν την ιδιωτικότητα και επιτυγχάνουν την αποσύνδεση από τα υποκείμενα των πληροφοριών.

Για την διασφάλισή της ιδιωτικότητας πέραν της παραδοσιακής κρυπτογράφησης, μεταξύ άλλων, προτείνονται η ομόσπονδη μάθηση και η ομομορφική κρυπτογράφηση. Σε έρευνα που αφορά την χρήση ιατρικών αρχείων εικόνας με σκοπό την εκπαίδευση μοντέλων μηχανικής μάθησης για τον εντοπισμό παθολογικών καταστάσεων (Adnan et al., 2022), προτείνεται η τεχνική της ομόσπονδης μάθησης η οποία δεν αποκρούει τις επιθέσεις αλλά προστατεύει την ιδιωτικότητα των δεδομένων. Η τεχνική αυτή, στα πλαίσια της μηχανικής μάθησης, επιτρέπει την εκπαίδευση τοπικών μοντέλων από τα νοσοκομεία και την αποστολή μόνο ενημερωτικών παραμέτρων σε έναν κεντρικό server για συνένωση με τα υπόλοιπα δεδομένα. Η ίδια έρευνα προτείνει επίσης τη χρήση της διαφορικής ιδιωτικότητας για τον αποκλεισμό της έμμεσης αντιστοίχισης με τα υποκείμενα των πληροφοριών στην περίπτωση που επιχειρείται ο εντοπισμός μοτίβων και τάσεων μέσω της αξιοποίησης ιδιαίτερα ευαίσθητων δεδομένων. Σε βιβλιογραφική ανασκόπηση που αφορά την συλλογή γεωργικών δεδομένων (Dembani et al., 2025) αναφέρεται ότι η ψηφιοποίηση δεδομένων που μπορεί να χαρακτηριστούν απόρρητα για τους κατόχους τους, όπως η απόδοση των καλλιεργειών τους και δεδομένα διαχείρισης, καθώς και η συγκέντρωσή τους σε μια κεντρική τοποθεσία, εγείρει ανησυχία

[63] https://www.nccoe.nist.gov/publication/1800-28/,l.ac.24/1/26

για την περίπτωση διαρροής τους. Η ομόσπονδη μάθηση προτείνεται και εδώ, ως λύση, για να αποκομίσει κανείς όφελος από την συνολική ανάλυση χωρίς να θυσιαστεί η προστασία της ιδιωτικότητας και της ιδιοκτησίας των δεδομένων, γεωργικών οργανισμών και επιχειρήσεων. Επισημαίνεται επίσης ότι η ομομορφική κρυπτογράφηση η οποία επιτρέπει υπολογισμούς σε κρυπτογραφημένα δεδομένα ενισχύει την προστασία της ιδιωτικότητας.

Σε ότι αφορά την προστασία των δεδομένων που συλλέγονται στα πλαίσια του IoT, η κατανεμημένη και ανομοιογενής φύση του, οι περιορισμένοι πόροι πολλών συσκευών που δυσκολεύουν την ισχυρή κρυπτογράφηση και η διαχείριση μεγάλου όγκου πληροφορίας αποτελούν προκλήσεις για την ασφάλεια των δεδομένων.(Saha et al., 2021) Οι τεχνικές της ομομορφικής κρυπτογράφησης και της διαφορικής ιδιωτικότητας προτείνονται και σε σχέση με την διασφάλιση δεδομένων που συλλέγονται στα πλαίσια του IoT. Οι συσκευές του IoT είναι ευάλωτες σε υποκλοπές και η αποστολή κρυπτογραφημένων δεδομένων ή δεδομένων που έχουν δεχτεί ελεγχόμενη και αμελητέα επίδραση θορύβου στα πλαίσια των τεχνικών της διαφορικής ιδιωτικότητας, ώστε να μην μπορούν να ταυτοποιηθούν έμμεσα, είναι επιλογές που προσφέρουν περισσότερη προστασία. Επίσης η ομόσπονδη μάθηση μπορεί να λύσει προβλήματα που συνδέονται με το ρίσκο της μαζικής συγκέντρωσης ευαίσθητων δεδομένων σε έναν κεντρικό server (Dritsas & Trigka, 2025).

3.3.2.5 Υιοθέτηση τρόπων εντοπισμού απειλής

Τα συστήματα ανίχνευσης και πρόληψης απειλών συμπληρώνουν ενεργητικά, συστήματα ελέγχου πρόσβασης (firewalls) σε πόρους του δικτύου, ενισχύοντας την ασφάλεια των δικτύων με τον εντοπισμό κακόβουλης δραστηριότητας που μπορεί να τα παρακάμψει. Τα IDS, IPS ανιχνεύουν επιθέσεις DDoS, επιθέσεις με κακόβουλο λογισμικό, κακόβουλες σαρώσεις σημείων επικοινωνίας (θυρών) στο δίκτυο για εντοπισμό ευπαθειών, κ.λπ. (Alzaabi & Mehmood, 2024; Ashoor & Gore, 2011; Coulibaly, 2020; NIST, 2007; Wang & Zhu, 2022). Τα συστήματα αυτά βασίζονται σε κανόνες (προκαθορισμένες λογικές συνθήκες) και υπογραφές (μοτίβα που περιγράφουν γνωστές κακόβουλες μορφές επιθέσεων). Το γεγονός αυτό δυσχεραίνει την αποτελεσματικότητά τους όταν ένας οργανισμός αντιμετωπίζει άγνωστες ή εξελιγμένες απειλές. Ωστόσο η ενσωμάτωση της μηχανικής μάθησης είναι μια νέα προσθήκη που μπορεί να βελτιώσει την αναγνώριση σύνθετων απειλών.

Instrusion Detection System(IDS)	Instrusion Prevention System(IPS)	Behavioral Monitoring
•Ανιχνεύει: Γνωστές παραβιάσεις δικτύου και πολιτικών ασφαλείας. Αναγνωρίζει και καταγράφει εισβολείς. •Παρακολουθεί την δραστηριότητα του δικτύου χωρίς να πραγματοποιεί ενέργειες μετριασμού ή αποκλεισμού. 'Οταν ανιχνεύει ύποπτη συμπεριφορά **στέλνει ειδοποιήσεις**	•Ανιχνεύει: Ενεργές επιθέσεις που απαιτούν άμεση αντίδραση •Παρακολουθεί την δραστηριότητα του δικτύου και **αποτρέπει κακόβουλες ενέργειες** λειτουργώντας σε πραγματικό χρόνο	•Ανιχνεύει: Ασυνήθιστες συμπεριφορές (εσωτερικές απειλές, παραβιάσεις σε υπηρεσίες κοινωνικής δικτύωσης, απάτες σε ηλεκτρονικές πληρωμές, κ.λπ.) •Βασίζεται στην δημιουργία προφίλ "κανονικής συμπεριφοράς" οντοτήτων μέσω στατιστικών και μοντέλων μηχανικής μάθησης •Μπορεί να εντοπίσει αποκλίσεις από την κανονικότητα, ακόμη και αν δεν παραβιάζεται κανένας κανόνας. **Λειτουργεί προληπτικά.**

Πίνακας 16. Τρόποι εντοπισμού απειλής

3.3.3 Οργάνωση της απόκρισης σε περιστατικό κυβερνοεπίθεσης

Μετά τον εντοπισμό της απειλής ακολουθούν η απόκριση στο περιστατικό και η ανάκαμψη. Το τεχνικό μέρος είναι η βάση, αλλά η διαχείριση ενός περιστατικού αποτελεί μέρος της συνολικής διοίκησης ενός οργανισμού και δεν περιορίζεται σε αυτό. Σχετίζεται επίσης με κοινωνικούς και νομικούς παράγοντες. Μια ολιστική προσέγγιση που εντάσσεται στο πλαίσιο ενός οργανωμένου σχεδίου έχει τη δυνατότητα να περιορίσει τις αντίστοιχες συνέπειες, τόσο τις άμεσες όσο και τις επακόλουθες. Σε ένα περιστατικό είναι σημαντικό να υπάρχει συντονισμός από την ανώτερη διοίκηση, άμεση τεχνική υποστήριξη, διαχείριση του ανθρώπινου παράγοντα, διαχείριση της δημόσιας εικόνας του οργανισμού που δέχεται την επίθεση, καθώς και υποστήριξη για νομική συμμόρφωση με υποχρεώσεις που προκύπτουν σε κάθε φάση του περιστατικού[64] (Mitropoulos et al., 2006).

Στην εργασία (Edwards & Weaver, 2024) παρουσιάζεται η ανάγκη μιας ολοκληρωμένης πολιτικής αντιμετώπισης συμβάντων, η οποία θα λειτουργεί ως οδηγός και θα ορίζει πρωτόκολλα, ρόλους και ευθύνες. Η αντιμετώπιση ενός κινδύνου πραγματοποιείται μέσα από διακριτές φάσεις ανάληψης

[64] Στα σύγχρονα πλαίσια, υπάρχει χρονοδιάγραμμα, για παράδειγμα, υποχρέωσης αναφορών για σημαντικό συμβάν(που προκαλεί λειτουργική διαταραχή ή επηρεάζει τρίτους) βάση της εφαρμογής της οδηγίας NIS2 (Πηγή: Εθνική Αρχή Κυβερνοασφάλειας (Ελλάδα): https://cyber.gov.gr/kyvernoepitheseis/anafora-symvanton/)

δράσεων. Αρχικά, κατά την περίοδο προετοιμασίας δημιουργείται ένα *σχέδιο απόκρισης*, εκπαιδεύεται το προσωπικό και αναλύονται πιθανά σενάρια, με στόχο τη δημιουργία συνθηκών ετοιμότητας απέναντι σε πιθανή κρίση. Ακολουθεί η *ενεργή απόκριση σε περιστατικό* (περιορισμός-εξάλειψη-ανάκαμψη). Κρίσιμος παράγοντας σε όλη τη διάρκεια των φάσεων θεωρείται η καλή επικοινωνία μεταξύ των συμμετεχόντων.

3.3.3.1 Προετοιμασία

Κατά τη φάση της προετοιμασίας πραγματοποιείται η διαμόρφωση σχεδίων και η κατανομή ρόλων.

Τα πλαίσια και τα πρότυπα κυβερνοασφάλειας, καθώς και οι επιμέρους πολιτικές, παρέχουν κατευθύνσεις για την εκπόνηση σχεδίων απόκρισης/ανάκαμψης και επιχειρηματικής συνέχειας. Επίσης, διαδικασίες όπως η προτεραιοποίηση των κρίσιμων υποδομών και ο καθορισμός στόχων συντελούν στην διαμόρφωση τους. Σύμφωνα με τον οδηγό SP 800-61 Rev. 3 (A. Nelson et al., 2025) που αφορά την εφαρμογή του NIST CFS στην διαχείριση περιστατικών, ανεξάρτητα από το πλαίσιο κυβερνοασφάλειας που εξυπηρετεί κάθε οργανισμό ανάλογα με την πολυπλοκότητα και τον βαθμό εξάρτησής του από την κυβερνοασφάλεια, αυτός οφείλει να οργανώνει την αντίδραση του οριζόντια, σε όλη τη διάρκεια διαχείρισης ενός περιστατικού, ενώ η κατανομή ρόλων παρέχει την απαιτούμενη ετοιμότητα για τη διαχείριση μιας κυβερνοεπίθεσης. Με βάση τον οδηγό, η ομάδα διαχείρισης περιστατικών θα πρέπει να έχει την κατάλληλη σύνθεση ώστε να περιλαμβάνει στελέχη με την εξουσία να λαμβάνουν κρίσιμες αποφάσεις, όπως η διακοπή λειτουργιών, αλλά και στελέχη που να μπορούν να καλύψουν τεχνικές, νομικές και επικοινωνιακές ανάγκες.

3.3.3.2 Ενεργή φάση (εκδήλωση κυβερνοεπίθεσης)

Κατά τη φάση εκδήλωσης της κυβερνοεπίθεσης, λαμβάνονται κατάλληλα μέτρα για τον περιορισμό των ζημιών, την αποτροπή διάδοσης της μόλυνσης, την κατά το δυνατόν συνέχισης της λειτουργίας, την αφαίρεση του κακόβουλου λογισμικού και την επαναφορά στη φυσιολογική ροή λειτουργιών (Edwards & Weaver, 2024; Goldman, 2010; Keogh et al., 2024; NIST, 2025a). Τα μέτρα αυτά περιγράφονται συνοπτικά στις επόμενες παραγράφους.

- *Απομόνωση τμημάτων του δικτύου*. Το πρώτο βήμα μετά την ανίχνευση της απειλής είναι να απομονωθούν τα παραβιασμένα συστήματα για να μην εξαπλωθεί περαιτέρω η επίθεση. Ακολουθούνται ενέργειες όπως η αλλαγή διαπιστευτηρίων και η διακοπή υπηρεσιών. Στο πλαίσιο αυτό αξιοποιούνται αυτοματοποιημένα μέτρα (όπως π.χ. θέση εκτελέσιμων αρχείων σε καραντίνα και μπλοκάρισμα κακόβουλου λογισμικού από antivirus,

απομόνωση παραβιασμένων τελικών σημείων κ.λπ.), ανθρώπινη παρέμβαση και βοήθεια από τρίτους (όπως οι πάροχοι υπηρεσιών cloud και οι πάροχοι υπηρεσιών δικτύου) για τον περιορισμό της εξάπλωσης. Σε αυτή τη φάση, η διασφάλιση ψηφιακών αποδεικτικών στοιχείων για την επίθεση θεωρείται χρήσιμη για μελλοντικές ενέργειες από την πλευρά του οργανισμού.

- *Εναλλαγή σε εφεδρικές επιλογές / χειροκίνητη λειτουργία*. Ανάλογα με το εφαρμοζόμενο σχέδιο επιχειρησιακής συνέχειας και το είδος του οργανισμού μπορούν να εφαρμοστούν μέτρα εναλλακτικής λειτουργίας. Σε παραβιασμένη μονάδα υγείας, για παράδειγμα, που δέχθηκε επίθεση ransomware, η επικοινωνία μέσω emails αντικαταστάθηκε με εναλλακτικά δίκτυα επικοινωνίας και τηλεδιασκέψεις, ενώ ιατρικές πράξεις όπως η ακτινοθεραπεία ανατέθηκαν σε τρίτους (Keogh et al., 2024). Η εξασφάλιση της συνέχειας των εργασιών επιτυγχάνεται μέσω πλεονασμού (redundancy), με την αξιοποίηση εφεδρικών ή διπλών υποδομών, καθώς και με την χρήση των αντιγράφων ασφαλείας. Επίσης η δυνατότητα προσφυγής σε λιγότερο εξαρτημένες από την τεχνολογία διαδικασίες, ακόμη και σε χειροκίνητες λειτουργίες, μπορεί να επιλεγεί για την συνέχιση κρίσιμων διεργασιών (Goldman, 2010).
- *Αφαίρεση κακόβουλου λογισμικού*. Παράλληλα, η πλήρης εκρίζωση της απειλής είναι απαραίτητη πριν την επαναφορά της κανονικής λειτουργίας. Κατάλοιπα μόλυνσης μπορεί να οδηγήσουν σε νέο κύκλο επίθεσης. Η εκρίζωση της απειλής ξεκινά από τον προσδιορισμό όλων των συστημάτων, υπηρεσιών, εφαρμογών που επηρεάστηκαν. Ακολουθεί η διαγραφή του κακόβουλου λογισμικού, η διακοπή κακόβουλων διεργασιών και η αντιμετώπιση των ευπαθειών, ιδίως εκείνων που αξιοποιήθηκαν από τους επιτιθέμενους για την εισβολή. Η αντιμετώπιση μπορεί να γίνει είτε αυτοποιημένα είτε χειροκίνητα.
- *Επαναφορά Συστημάτων και Λειτουργιών*. Στη φάση αυτή πραγματοποιείται επιστροφή στην κανονικότητα, η οποία συνδέεται με την εξάλειψη ευπαθειών και την ενίσχυση των συστημάτων που είχαν παραβιαστεί. Ο οδηγός του NIST και η βιβλιογραφία αναφέρουν ως λειτουργίες ανάκαμψης την αντικατάσταση του λογισμικού με νέες εκδόσεις, την επανεγκατάσταση συστημάτων, την αποκατάσταση των δεδομένων από αντίγραφα ασφαλείας, την αλλαγή κωδικών πρόσβασης και την ανανέωση/συμπλήρωση των μέτρων ασφαλείας. Ο οδηγός NIST SP 800-61r3 αναφέρει ότι σε εξελιγμένες επιθέσεις όπου υπάρχει ανησυχία για τυχόν κρυμμένες παραβιάσεις, μπορεί να απαιτείται ακόμη και αντικατάσταση του hardware (A. Nelson et al., 2025).

Σε ερευνητική μελέτη που εστιάζει στην διαχείριση ευπαθειών λογισμικού για τη μείωση των κινδύνων στο IoT (Sotiropoulos et al., 2023), αναφέρεται ότι με δεδομένο το κόστος της, μπορεί να απαιτηθεί προτεραιοποίηση των ενεργειών αποκατάστασης σε συνδυασμό με τον εκτιμώμενο κίνδυνο κάθε ευπάθειας. Με τον τρόπο αυτό ακόμη και αν η άμεση πλήρης αποκατάσταση δεν είναι εφικτή λόγω περιορισμένων πόρων, επιτυγχάνεται ο βέλτιστος συνδυασμός επισκευών που οδηγεί στη μέγιστη μείωση του συνολικού κινδύνου Μια ανάλογη προσέγγιση, θα μπορούσε να λειτουργήσει και στην φάση της επαναφοράς, σε οργανισμούς που αντιμετωπίζουν περιορισμούς λόγω στενότητας πόρων.

3.3.3.3 Μετά την επίθεση

Ο οδηγός NIST SP 800-61r3 αναφέρει ότι η πλήρης ανάκαμψη μπορεί να διαρκέσει εβδομάδες ή μήνες ανάλογα με το εύρος και την πολυπλοκότητά της επίθεσης (A. Nelson et al., 2025). Για τον λόγο αυτό, τα διδάγματα από μια επίθεση θα πρέπει να αξιοποιούνται άμεσα και πριν την ολοκλήρωση της ανάκαμψης (NIST, 2025a).

Σύμφωνα με το National Cyber Security Centre του Ηνωμένου Βασιλείου (NCSC UK, 2019), ένας οργανισμός μετά από τη λήξη του περιστατικού θα πρέπει να απαντήσει σε μια σειρά από ερωτήματα όπως αν η απόκριση ήταν αποτελεσματική, εάν υπήρχαν σημεία που θα έπρεπε να αντιμετωπιστούν καλύτερα και αν τις κρίσιμες ώρες υπήρχαν δεδομένα (π.χ. αρχεία καταγραφής για προσπάθειες συνδέσεων) που θα έπρεπε να ήταν διαθέσιμα αλλά ο οργανισμός λόγω αστοχιών δεν κατείχε.

Η αποτελεσματικότητα της απόκρισης σε ένα περιστατικό, θα πρέπει με βάση τον οδηγό του NIST SP 800-184 (*Guide for Cybersecurity Event Recovery* (NIST, 2016)) να εκτιμηθεί συγκρίνοντας την απόδοση της ομάδας διαχείρισης ενός συμβάντος σε σχέση με το επίπεδο που αναμενόταν στα σχέδια και μετρήσεις που αφορούν την ποιοτική αποτίμηση των ενεργειών ανάκαμψης και την ολοκλήρωση συγκεκριμένων ενεργειών με βάση το κόστος, τον χρόνο, τη διαχείριση πόρων και τις επιπτώσεις.

3.3.3.4 Επικοινωνιακή διαχείριση

Σύμφωνα με τον οδηγό κρίσεων του ENISA, ένας σχεδιασμός επικοινωνιακής διαχείρισης έχει σκοπό να μετριάσει τον αντίκτυπο από την αρνητική δημοσιότητα και τις απώλειες που θα υποστεί η εμπιστοσύνη προς ένα οργανισμό μετά από μια κυβερνοεπίθεση (ENISA, 2023). Ο Πίνακας 17 παρουσιάζει στοιχεία για τον σχεδιασμό επικοινωνιακής διαχείρισης συμβάντος (ENISA, 2023; Knight & Nurse, 2020; NCSC UK, 2019).

Σχεδιασμός επικοινωνιακής διαχείρισης συμβάντος	
1. **Προληπτικός σχεδιασμός**	• Εξέταση σεναρίων κρίσης • Ασκήσεις προσομοίωσης εταιρικής αντίδρασης • Σύνταξη προτύπων σχεδίων αντίδρασης που θα ενεργοποιούνται ανάλογα με την σοβαρότητα του περιστατικού
2. **Καθορισμός ρόλων**	• Επιλογή του στελέχους που θα συντονίσει την διαδικασία • Επιλογή των ατόμων που θα λειτουργήσουν ως εκπρόσωποι του οργανισμού • Επιλογή της ομάδας υποστήριξης
3. **Καθορισμός target group**	• Χαρτογράφηση των ενδιαφερόμενων μερών που πρέπει να ενημερωθούν για το περιστατικό (προσωπικό, πελάτες, προμηθευτές, συνεργάτες, ΜΜΕ, υπηρεσίες)
4. **Προετοιμασία templates δηλώσεων**	• Δημιουργία προτύπων δηλώσεων και εγγράφων ερωτήσεων-απαντήσεων με βάση το τι θα ήθελαν να μάθουν τα ΜΜΕ
5. **Εσωτερική επικοινωνία**	• Συναντήσεις εντός της εταιρίας και συζήτηση για τις ανησυχίες κάθε τομέα σε σχέση με τις επιπτώσεις • Ενημέρωση για απαιτούμενες ενέργειες αναφορικά με τους ρόλους που έχουν ανατεθεί (π.χ. διανομή ενημερώσεων, υποδοχή ΜΜΕ κ.ά.)
6. **Εξωτερική επικοινωνία**	• Δημιουργία εναλλακτικών καναλιών επικοινωνίας (π.χ. πλατφόρμες κοινωνικής δικτύωσης εάν τα emails ενέχουν κίνδυνο παραβίασης) • Επιλογή του τρόπου και του μέσω επικοινωνίας περιστατικού
7. **Διαχείριση έκτακτων αντιδράσεων**	• Ετοιμότητα για αντιμετώπιση παραπληροφόρησης, αρνητικής δημοσιότητας κ.λπ.
8. **Συνέχεια ενημέρωσης**	• Επιμέλεια στη διατήρηση επικοινωνίας και συνεργασίας με τα ενδιαφερόμενα μέρη

Σχεδιασμός επικοινωνιακής διαχείρισης συμβάντος	
9. **Αξιολόγηση διαχείρισης/ ενεργειών**	• Αξιολόγηση της αποτελεσματικότητας της επικοινωνίας και λήψη μαθημάτων για το μέλλον • Εφαρμογή μετρήσεων σε σχέση με την αποδοχή της επικοινωνιακής προσπάθειας (π.χ. επισκεψιμότητα ιστοτόπου, ποσοστό ανοίγματος emails κ.λπ.)

Πίνακας 17 Σχεδιασμός επικοινωνιακής διαχείρισης συμβάντος

Το Βρετανικό Εθνικό Κέντρο Κυβερνοασφάλειας επισημαίνει, μεταξύ άλλων, αφενός την υποχρέωση έγκυρης πληροφόρησης προς τους θιγόμενους και αφετέρου την ανάγκη ο οργανισμός να προστατευθεί ο ίδιος από παρορμητικές συμπεριφορές που θα αποκαλύπτουν ευαίσθητες λεπτομέρειες ή θα οδηγούν σε μη τεκμηριωμένα συμπεράσματα, τα οποία στο μέλλον θα πρέπει να ανακληθούν[65]. Επιπλέον, η προσέγγιση με την οποία η διοίκηση θα επικοινωνήσει ένα συμβάν, μπορεί να δημιουργήσει επιπλέον κρίσεις. Σε εργασίες που αφορούν την αποτελεσματική εταιρική επικοινωνία αναφέρονται οι αρνητικές συνέπειες από την ανακριβή ενημέρωση σε περιστατικό παραβίασης. Συγκεκριμένα στο περιστατικό διαρροής δεδομένων που αφορούσε την εταιρία TalkTalk το 2015, η CEO της εταιρείας εμφανίστηκε στον τύπο χωρίς να γνωρίζει σημαντικά στοιχεία, όπως για το αν τα δεδομένα που χάθηκαν ήταν κρυπτογραφημένα, πλήττοντας σοβαρά την εικόνα της εταιρίας (Boakye et al., 2024; Knight & Nurse, 2020).

Στην ερευνητική μελέτη (Ruohonen et al., 2024) που αξιοποιεί εμπειρικά δεδομένα από τη διαχείριση της επικοινωνίας σε οκτώ περιστατικά έκθεσης δεδομένων στην Φιλανδία, παρουσιάζονται τόσο επιτυχημένες όσο και αποτυχημένες προσεγγίσεις των οργανισμών κατά την επικοινωνία των συμβάντων, με βάση την έγκαιρη γνωστοποίηση, την ειλικρινή ανάληψη ευθύνης, την παροχή συμβουλών και υποστήριξης προς τα θύματα και την ενημέρωση των αρχών, βάσει των κανονιστικών υποχρεώσεων. Η καθυστερημένη πληροφόρηση επιτρέπει τη δημιουργία σεναρίων που εκθέτουν περεταίρω έναν οργανισμό, η μη ανάληψη ευθύνης, η μετάθεση ευθυνών σε τρίτους, ο περιορισμός στην εικόνα του θύματος χωρίς ουσιαστική δράση για επανόρθωση, δημιουργούν οργή στα άμεσα θύματα και απώλεια εμπιστοσύνης στην κοινωνία, ενώ η μη ενημέρωση των αρχών έχει νομικές συνέπειες και επιφέρει πρόστιμα.

Σύμφωνα με σχετική εργασία (Knight & Nurse, 2020), η ανάληψη ευθύνης προσκρούσει στον φόβο των οργανισμών για επακόλουθες δικαστικές διαμάχες, νομικά έξοδα και αποζημιώσεις, ωστόσο στα

[65] https://www.ncsc.gov.uk/guidance/effective-communications-in-a-cyber-incident

σύγχρονα πλαίσια, ο φόβος αυτός εξισορροπείται, καθώς η μη τήρηση των υποχρεώσεων του οργανισμού έναντι των επηρεαζόμενων υποκειμένων επιφέρει αυστηρές κυρώσεις. Επιπλέον, η ανάληψη ευθύνης ενισχύει την θέση του οργανισμού ως υπεύθυνης οντότητας έναντι υποτιμητικών αναρτήσεων στα μέσα κοινωνικής δικτύωσης και αρνητικής δημοσιότητας στα μαζικής ενημέρωσης, τα οποία επηρεάζουν την φήμη του οργανισμού.

3.4 Έλεγχος και Βελτίωση

Ο συνεχής έλεγχος και η βελτίωση της στρατηγικής είναι πρακτικές για να παραμένει το επίπεδο κυβερνοασφάλειας επίκαιρο και επαρκές σε σχέση με τις προκλήσεις. Η εφαρμογή και η προσομοίωση σεναρίων παρέχει χρήσιμα συμπεράσματα σε ελεγχόμενο περιβάλλον. Η εμπειρία από περιστατικά προσφέρει μαθήματα από την αντιμετώπιση πραγματικών κρίσεων.

3.4.1 Εφαρμογή και προσομοίωση σεναρίων

Τα μοντέλα προσομοίωσης διερευνούν, σε εικονικά περιβάλλοντα, ζητήματα που αφορούν την αλληλεπίδραση διαφορετικών παραγόντων όπως ο ανθρώπινος παράγοντας, το λογισμικό και τα υλικά συστήματα στη διαμόρφωση μέτρων ασφάλειας και στο επίπεδο της ανθεκτικότητας. Με τον τρόπο αυτό αξιολογούν την επίδραση των κυβερνοεπιθέσεων και των μέτρων άμυνας χωρίς να διαταράσσεται η κανονική λειτουργία των συστημάτων. Η προσομοίωση, μεταξύ άλλων, αξιοποιείται για την ανάλυση κινδύνου, τη δοκιμή αμυντικών τεχνικών, την εκπαίδευση των επαγγελματιών ασφάλειας και την μελέτη της ανθεκτικότητας των χρηστών στην διάρκεια μιας κυβερνοεπίθεσης (Kavak et al., 2021). Στις επόμενες παραγράφους εξετάζονται μοντέλα προσομοίωσης που χρησιμοποιούνται για την κυβερνοασφάλεια.

3.4.1.1 Ενδεικτικά Μοντέλα Αυτοματοποιημένων Προσομοιώσεων

Στην εργασία (Engström & Lagerström, 2022) καταγράφονται τα κάτωθι μοντέλα αυτοματοποιημένων προσομοιώσεων:

- **Graph-based simulation**: εστιάζει στην μοντελοποίηση πιθανών μοτίβων κυβερνοεπίθεσης με ενσωμάτωση παραμέτρων, όπως το κόστος προσπαθειών και η πιθανότητα επιτυχίας. Διερευνά μέσω προσομοίωσης τις συμπεριφορές του επιτιθέμενου και του αμυνόμενου με βάση το προφίλ τους (στόχος, σημείο εκκίνησης, παρεχόμενος χρόνος) και τις πιθανότητες.
- **State-based simulation**: εστιάζει στο πώς αλλάζει η κατάσταση του συστήματος μετά από κυβερνοεπίθεση. Τα μοντέλα χρησιμοποιούν πράκτορες (οντότητες όπως επιτιθέμενος,

αμυνόμενος) που λειτουργούν βάση επίσημων μαθηματικών/ συμπεριφορικών μοντέλων και πιθανοτήτων.

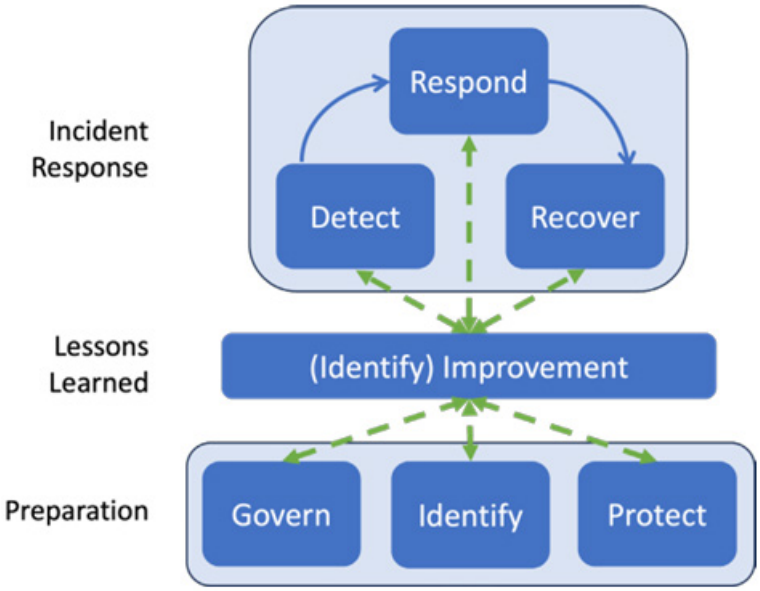
3.4.1.2 Διαδραστική Προσομοίωση

Τα εικονικά περιβάλλοντα προσομοίωσης (Cyber Range) προσομοιώνουν δίκτυα, συστήματα και υπηρεσίες που λειτουργούν διαδραστικά, με τους συμμετέχοντες να επηρεάζουν την εξέλιξη των σεναρίων. Με την ενσωμάτωση των νέων τεχνολογιών δημιουργούν σενάρια επιθέσεων και άμυνας για έρευνα και εκπαίδευση, τα οποία παρουσιάζουν αυξημένο επίπεδο ρεαλιστικότητας. Τεχνολογίες όπως η εικονοποίηση (virtualization) μπορούν να συμβάλλουν στην προσομοίωση των υποδομών με πιο ρεαλιστικό τρόπο, η χρήση του υπολογιστικού νέφους δίνει την δυνατότητα εκτέλεσης σεναρίων σε μεγάλη κλίμακα, ενώ η τεχνητή νοημοσύνη υποστηρίζει την προσαρμογή των σεναρίων στην συμπεριφορά και τις αντιδράσεις των συμμετεχόντων (Shin et al., 2024).

3.4.2 Συνεχής αξιολόγηση και βελτίωση της στρατηγικής

Από την οπτική του οδηγού NIST SP 800-61 Rev. 3, η διαχείριση ενός περιστατικού κυβερνοασφάλειας, περιλαμβάνει έναν κύκλο ζωής όπου το κάθε συμβάν μετά την ανίχνευση, απόκριση και ανάκαμψη, αποτελεί ένα μάθημα καλύτερης διαχείρισης του επόμενου, οδηγώντας σε αναγνώριση κενών, βελτιώσεις και επιστροφή στην προετοιμασία. Με τον τρόπο αυτό ανανεώνονται η διακυβέρνηση και οι πολιτικές ασφάλειας, ο καθορισμός προτεραιοτήτων και η παρεχόμενη προστασία (A. Nelson et al., 2025). Παράλληλα η αξιοποίηση της εμπειρίας τρίτων από πραγματικά περιστατικά μπορεί να βελτιώσει την στρατηγική ενός οργανισμού απέναντι στην κυβερνοασφάλεια. Η κοινή χρήση πληροφοριών για κυβερνοαπειλές μέσω των κέντρων Κοινοποίησης και Ανάλυσης Πληροφοριών (Information Sharing and Analysis Centers - ISACs) τα οποία παρέχουν ανωνυμοποιημένη πληροφόρηση και ενημερώνουν για ευπάθειες χωρίς άμεση έκθεση των παθόντων ή των εκτεθειμένων οργανισμών, προσφέρουν ένα ασφαλές πλαίσιο για τον διαμοιρασμό και την αποκόμιση οφέλους από την συλλογική εμπειρία (Abraham et al., 2025).

Επιπλέον, όπως αναφέρθηκε ανωτέρω, το MITRE ATT&CK παρέχει πληροφόρηση για τεχνικές και τακτικές που έλαβαν χώρα σε πραγματικά περιστατικά. Οργανισμοί όπως ο ENISA αλλά και ιδιωτικοί φορείς όπως η Microsoft και η VERIZON προσφέρουν αναλύσεις κυβερνοαπειλών που είναι δυνατόν να αξιοποιηθούν στην επαναξιολόγηση της στρατηγικής ενός οργανισμού. Το Σχήμα 11 παρουσιάζει τον κύκλος ζωής της απόκρισης σε περιστατικά που βασίζεται στις λειτουργίες CSF 2.0, σύμφωνα με το πρότυπο SP 800-61.



Σχήμα 11. Κύκλος ζωής της απόκρισης σε περιστατικά που βασίζεται στις λειτουργίες CSF 2.0, σύμφωνα με το πρότυπο SP 800-61

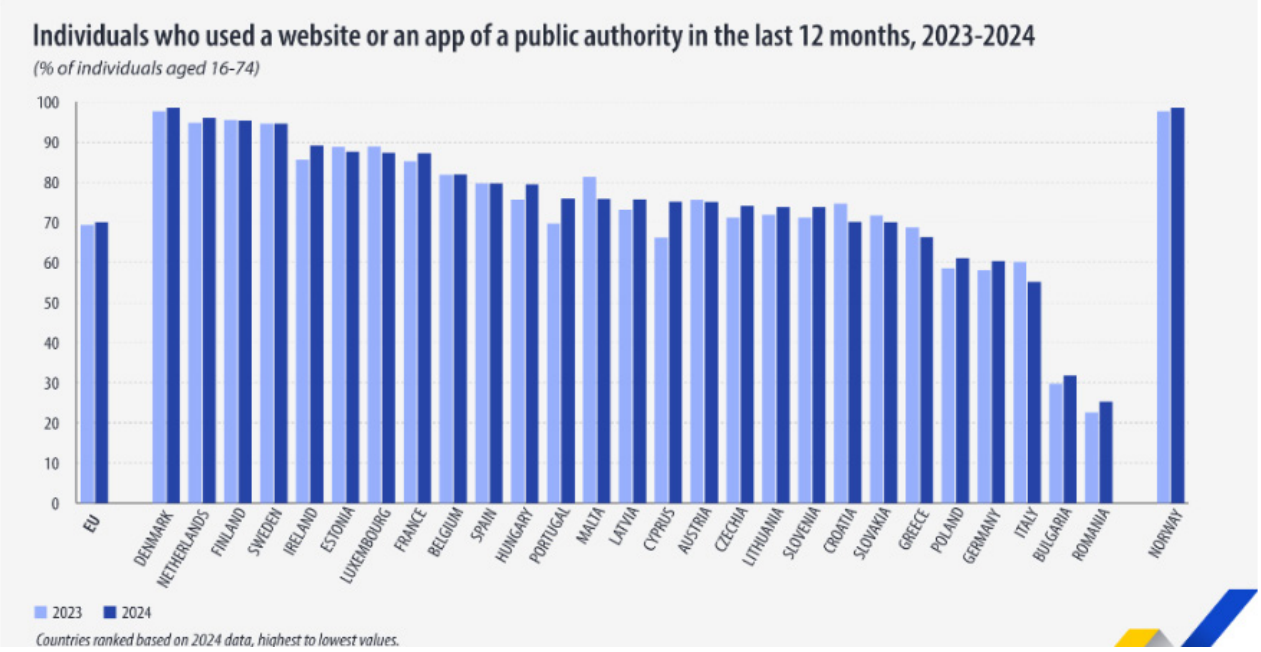
4 Στόχοι κυβερνοεπιθέσεων

Οι κυβερνοεπιθέσεις κατευθύνονται προς διαφορετικούς τομείς. Στη συνέχεια θα παρουσιαστούν ορισμένοι από τους δημοφιλείς στόχους, τόσο θεωρητικά και αλλά και αναφορικά με πραγματικές περιπτώσεις, σε μια προσπάθεια κατανόησης των επιπτώσεών τους στον φυσικό κόσμο.

Τα κριτήρια επιλογής των περιπτώσεων ήταν τα ακόλουθα: 1) να προσφέρουν διαφορετικές παραμέτρους των απειλών και 2) να υπάρχουν κυρίως ακαδημαϊκές ή πρωτογενείς πηγές και δευτερευόντως αξιόπιστες ειδησεογραφικές πηγές αναφορικά με αυτές.

4.1 Δημόσια διοίκηση

Σύμφωνα με έκθεση της Eurostat (26/2/25)[66], το 70% των ευρωπαίων πολιτών σε ηλικία μεταξύ 16 και 74 χρόνων χρησιμοποίησε ηλεκτρονικές υπηρεσίες για τις συναλλαγές του με το δημόσιο κατά το έτος 2024. Αυτές αφορούσαν κυρίως την αναζήτηση πληροφοριών, την πρόσβαση σε προσωπικά δεδομένα και την εκτύπωση επίσημων εγγράφων.



Σχήμα 12. Χρήση ψηφιακών εφαρμογών δημοσίων φορέων στην Ε.Ε.

Ο δημόσιος τομέας, στο πλαίσιο της ψηφιοποίησης του κράτους, καλείται να διασφαλίσει την πρόσβαση σε μια σειρά από υπηρεσίες που είναι σημαντικές για τη λειτουργία της δημόσιας διοίκησης και να διαχειριστεί την ασφάλεια ενός μεγάλου όγκου δεδομένων. Σε επίπεδο τοπικής αυτοδιοίκησης,

[66] https://ec.europa.eu/eurostat/web/products-eurostat-news/w/ddn-20250226-1, last acc. 15/3/26

η δημοσίευση (Hossain et al., 2024), εντοπίζει 20 διαφορετικούς τύπους δεδομένων που οι δήμοι διαχειρίζονται μέσω του ψηφιακού μετασχηματισμού και περιλαμβάνουν από προσωπικές πληροφορίες, οικονομικά στοιχεία, πληροφορίες ακινήτων, εκπαιδευτικά αρχεία, ιστορικά αρχεία, εκλογικούς καταλόγους και αρχεία εκλογών, δεδομένα εργαζομένων, προμηθευτών και προμηθειών, υποδομών και υπηρεσιών κοινής ωφελείας έως και δεδομένα που συλλέγονται μέσω του IoT. Στο ίδιο άρθρο, αναγνωρίζονται ως κίνητρα των κυβερνοεπιθέσεων το οικονομικό όφελος, ο χακτιβισμός (ως έκφραση πολιτικών παραπόνων), οι εσωτερικές απειλές από δυσαρεστημένους υπαλλήλους και η κατασκοπεία από ξένες χώρες, όταν υπάρχει στρατηγικό όφελος.

Σε ανασκόπηση που αφορά την περίοδο 2020-2024 (Ardhi et al., 2025) και βασίζεται σε 50 δημοσιευμένα επιστημονικά άρθρα αναφέρεται ότι οι απειλές στον δημόσιο τομέα κατά κανόνα αφορούν κοινωνική μηχανική (phishing), κακόβουλο λογισμικό ransomware, προηγμένες επίμονες απειλές (APT), επιθέσεις άρνησης υπηρεσίας, εισαγωγή παραποιημένων δεδομένων (False Data Injection attacks) και επιθέσεις που σχετίζονται με την εφοδιαστική αλυσίδα. Σύμφωνα με την ανασκόπηση αυτή, οι δράσεις αποτροπής και μετριασμού που εφαρμόζονται από τις κυβερνήσεις περιλαμβάνουν (α) τη δημιουργία εθνικών πλαισίων και στρατηγικών κυβερνοασφάλειας, (β) τη δημιουργία ομάδων κυβερνοάμυνας και αντίδρασης σε περιστατικά, οι οποίες αποτελούνται από ειδήμονες του χώρου και (γ) την εισαγωγή στους δημόσιους οργανισμούς προτύπων όπως το ISO 27001 και συστημάτων ανίχνευσης ανώμαλης δραστηριότητας. Επίσης, με βάση έρευνες που απευθύνθηκαν στα ανώτερα στελέχη κυβερνοασφάλειας διαφορετικών χωρών, η ευαισθητοποίηση και η εκπαίδευση του μη τεχνικού προσωπικού είναι μια πρακτική που θεωρείται απαραίτητη.

Σε επιστημονική εργασία που αφορά την αποκατάσταση της εμπιστοσύνης μετά από κρίσεις που προκλήθηκαν από παραβίαση δεδομένων (Choi et al., 2025), επισημαίνεται πως σε ό,τι αφορά τον δημόσιο τομέα, η εμπιστοσύνη επηρεάζει τον συντονισμό μεταξύ των διαφόρων υπηρεσιών αλλά και τον βαθμό συμμόρφωσης των πολιτών με τις δημόσιες πολιτικές. Οι πολίτες είναι πιο πρόθυμοι να αποδεχτούν εθελοντικά τις υποχρεώσεις τους όταν αντιλαμβάνονται ότι οι δημόσιες υπηρεσίες είναι αξιόπιστες. Επίσης, συνήθως, έχουν μεγαλύτερες απαιτήσεις όταν αξιολογούν την απόδοση του δημόσιου έναντι του ιδιωτικού τομέα. Το αποτέλεσμα είναι περιστατικά κρίσεων, συχνά να μην γίνονται αντιληπτά ως μεμονωμένα συμβάντα, αλλά ως συνολική θεσμική αποτυχία, και έτσι να επέρχεται σημαντικό πλήγμα στο κύρος της δημόσιας διοίκησης.

Στις επόμενες παραγράφους καταγράφεται ένα μείζον περιστατικό κυβερνοεπίθεσης που αφορά τη δημόσια διοίκηση, οι ενέργειες μετριασμού που ακολουθήθηκαν, στοιχεία για την ανάκαμψη και τις διορθωτικές ενέργειες, καθώς και μία συνολική αποτίμηση.

4.1.1 Περιστατικό «Ατλάντα, ΗΠΑ 2018»: Κυβερνοεπίθεση ransomware στους υπολογιστές του Δήμου

Η επίθεση	Στις 22 Μαρτίου του 2018 ο δήμος της Ατλάντα δέχθηκε επίθεση ransomware με το κακόβουλο λογισμικό SamSam. Η είσοδος στα συστήματα του Δήμου πιθανολογείται ότι έγινε «σπάζοντας» αδύναμους κωδικούς μέσω επίθεσης τύπου brute force (αυτοματοποιημένη δοκιμή κωδικών). Στη συνέχεια, οι επιτιθέμενοι εγκατέστησαν λογισμικό ransomware και απαίτησαν την καταβολή περίπου 50.000 δολαρίων σε bitcoin. Ως συνέπεια της επίθεσης, μια σειρά από λειτουργίες του Δήμου διακόπηκαν. Στις διακοπείσες υπηρεσίες συγκαταλέγεται ο προγραμματισμός των δικαστηρίων, η διαδικτυακή πληρωμή οφειλών, η πρόσβαση σε αρχεία και αλληλογραφία κ.λπ. Οι αρχές δεν ανέφεραν παραβίαση δεδομένων (City of Atlanta, 2018b; Cureton, 2018; Cyber Florida, 2021).
Μετριασμός	Η πόλη συγκρότησε μια ομάδα διαχείρισης του περιστατικού (City of Atlanta, 2018a) αποτελούμενη όχι μόνο από στελέχη του Δήμου αλλά και από μέλη των αρχών επιβολής του νόμου όπως το FBI, το υπουργείο εσωτερικής ασφάλειας και ειδικούς από τον ιδιωτικό τομέα, για να αξιολογηθεί η κατάσταση και να επιλεγούν οι τρόποι προστασίας της πόλης. Εφαρμογές του Δήμου και το WiFi του αεροδρομίου της πόλης απενεργοποιήθηκαν για να μην εξαπλωθεί η επίθεση. Στη διάρκεια της κρίσης οι υπάλληλοι του Δήμου, η αστυνομία και το δημοτικό δικαστήριο διεκπεραίωναν όσες εργασίες δεν ήταν δυνατό να αναβληθούν με χειρογραφικά («χαρτί και μολύβι»). Για μια σειρά υπηρεσιών, η υποβολή αιτημάτων από τους πολίτες γινόταν μέσω τηλεφώνου (έναντι της υποβολής μέσω διαδικτύου) ή εξυπηρετούνταν με χειροκίνητες διαδικασίες (City of Atlanta, 2018b; Cureton, 2018). Η πόλη πρόσθεσε μια σελίδα στον ιστότοπό της, ειδικά για την ενημέρωση των πολιτών και των ΜΜΕ για την αντιμετώπιση της επίθεσης (Douglas, 2018).
Ανάκαμψη	Η πόλη δεν κατέβαλε λύτρα στους επιτιθέμενους για την απόκτηση του κλειδιού της αποκρυπτογράφησης. Η ανάκαμψη βασίστηκε στην ανοικοδόμηση των συστημάτων της και διήρκεσε για μήνες, χωρίς να επιτευχθεί η αποκατάσταση του συνόλου των στοιχείων. Σε δημόσια συνάντηση αποκαλύφθηκε από στελέχη του Δήμου ότι το 35% του λογισμικού επηρεάστηκε από την επίθεση, και σε αυτό το ποσοστό συμπεριλαμβανόταν 49 κρίσιμες εφαρμογές. Κάποιες από τις εφαρμογές αυτές χρειάστηκε ανακατασκευαστούν από προμηθευτές με κόστος για τον Δήμο και κάποιες άλλες ξαναδημιουργήθηκαν εσωτερικά. Επίσης αρχεία

	δεκαετιών δεν κατέστη δυνατό να ανακτηθούν, λόγω της κρυπτογράφησης (Schwartz, 2018). Σύμφωνα με δηλώσεις με πηγές από την αστυνομία χάθηκαν και αρχεία από κάμερες που θα μπορούσαν να αξιοποιηθούν σε ποινικές υποθέσεις, όπως π.χ. η οδήγηση υπό την επήρεια αλκοόλ (McGuire, 2018).
Διορθωτικές ενέργειες	Η αρμόδια υπηρεσία (AIM- Atlanta Information Management) ζήτησε επιπλέον του αναμενόμενου προϋπολογισμού 9,5 εκατομμύρια δολάρια, για ενίσχυση της ασφάλειας και των υποδομών και επιπλέον δαπανήθηκαν από τα έκτακτα ταμεία 2,6 εκατομμύρια δολάρια για την αντιμετώπιση του περιστατικού (Cyber Florida, 2021). Οι πόλεις διαχειρίζονται συγκεκριμένα κεφάλαια και δέχονται έντονες πιέσεις να διαθέτουν πόρους για την βελτίωση της ζωής των πολιτών, συνθήκη που θέτει όρια στις επενδύεις στην κυβερνοασφάλεια. Παρόλα αυτά, η πόλη ανέστειλε την έγκριση του προϋπολογισμού του 2019 και επαναπροσδιόρισε τις δαπάνες της. Ο προϋπολογισμός που εγκρίθηκε τελικά παρείχε μια αύξηση 3,5 εκατομμύρια δολαρίων στην AIM έναντι των 9,5 εκατομμυρίων δολαρίων που η υπηρεσία είχε αιτηθεί και αναφερόταν σε αναβαθμίσεις στη ασφάλεια και τις υποδομές. Ο προϋπολογισμός της υπηρεσίας ήταν αυξημένος κατά 10%, σε σχέση με το προηγούμενο έτος. Στο πλαίσιο μιας πιο πειθαρχημένης προσέγγισης από την πλευρά του Δήμου, οι ειδικοί όρισαν τρεις πυλώνες κυβερνοαφάλειας (Schwartz, 2018): o Διακυβέρνηση με συμμόρφωση σε κανόνες o Διαχείριση ευπαθειών o Συνολική αντιμετώπιση απειλών
Αποτίμηση	Σύμφωνα με τις ανασκοπήσεις του περιστατικού (Cyber Florida, 2021; Douglas, 2018; Schwartz, 2018), τα σημαντικά στοιχεία της αποτίμησης μπορούν να συνοψισθούν ως ακολούθως: • Δεν καταβλήθηκαν λύτρα γεγονός που θεωρήθηκε αποτρεπτικό για μελλοντικές επιθέσεις. • Η ανάκαμψη ήταν δαπανηρή και χρονοβόρα, και επιπλέον όχι απόλυτη. • Διαδικτυακές εφαρμογές και συστήματα της πόλης έμειναν εκτός λειτουργίας για μέρες, εβδομάδες ή μήνες και υπήρξε απώλεια δεδομένων. • Η επιστροφή στις παραδοσιακές (χειρογραφικές, τηλεφωνικές) μεθόδους παροχής υπηρεσιών διατήρησε ένα μέρος της λειτουργικότητας του Δήμου. Σύμφωνα με σχετικές δηλώσεις, αυτό οφείλεται στο ότι υπήρχε στους θεσμούς γνώση σχετικά με τις χειρογραφικές διαδικασίες. • Από την εμπειρία του περιστατικού του Δήμου της Ατλάντα, αναδείχθηκε από τους ειδικούς η σημασία της πρόληψης και η λήψη μέτρων όπως όπως η τμηματοποίηση (segregation) του δικτύου για την προστασία των κρίσιμων συστημάτων, η πολυπαραγοντική

	ταυτοποίηση, ο περιορισμός της πρόσβασης των διαδικτυακών εφαρμογών, η εκπαίδευση στην αποφυγή του phishing και η λήψη ενημερωμένων εφεδρικών αντιγράφων.

Πίνακας 18. Περιστατικό «Ατλάντα, 2018» (City of Atlanta, 2018b; Cureton, 2018; Cyber Florida, 2021)

4.2 Πλατφόρμες ηλεκτρονικού εμπορίου

Η εμπιστοσύνη των πελατών είναι ζωτική για την ανάπτυξη του ηλεκτρονικού εμπορίου, καθώς η εμπιστοσύνη επηρεάζει τη διάθεση των καταναλωτών να χρησιμοποιήσουν τις ηλεκτρονικές πλατφόρμες για τις αγορές τους. Η αντιλαμβανόμενη (perceived) κυβερνοασφάλεια είναι ένας από τους παράγοντες που διαμορφώνουν την εμπιστοσύνη προς τα ηλεκτρονικά καταστήματα, αναφορικά με τη διατήρηση της ιδιωτικότητας των δεδομένων που κοινοποιούνται σε αυτά και την ασφάλεια των ηλεκτρονικών συναλλαγών. Σημειώνεται ότι ενώ υπό κανονικές συνθήκες οι προσφερόμενες τιμές και οι αξιολογήσεις άλλων πελατών είναι εκείνες που κατευθύνουν τους καταναλωτές σε μια ηλεκτρονική αγορά και στην επιλογή συγκεκριμένων ηλεκτρονικών καταστημάτων, οι κυβερνοεπιθέσεις μπορούν να μεταβάλλουν ριζικά την καταναλωτική συμπεριφορά, διαμορφώνοντας αρνητική αντίληψη για την ασφάλεια των διαδικτυακών αγορών (Chauhan & Singh, 2025).

Τα δεδομένα που κοινοποιούνται στις ηλεκτρονικές πλατφόρμες αφορούν ονόματα, φυσικές και ηλεκτρονικές διευθύνσεις, τηλέφωνα, στοιχεία τραπεζικών καρτών αλλά και καταναλωτικές προτιμήσεις. Οι συνήθεις κίνδυνοι που καταγράφονται στο ηλεκτρονικό εμπόριο είναι η κλοπή δεδομένων μέσω παραβίασης ή κοινωνικής μηχανικής σε βάρος πελατών ή εργαζομένων, οι πλαστογραφημένες ιστοσελίδες και οι επιθέσεις DDoS που διακόπτουν την ομαλή λειτουργία των ηλεκτρονικών καταστημάτων (Bhatia et al., 2021; X. Liu et al., 2022).

Στις παραγράφους που ακολουθούν καταγράφονται σημαντικά περιστατικά παραβιάσεων στον χώρο του ηλεκτρονικού εμπορίου.

4.2.1 Περιστατικό «Shopify 2020»: Εσωτερική παραβίαση δεδομένων και συνεργασία με τρίτο μέρος

Η επίθεση	Η Shopify είναι μια διεθνής καναδική πλατφόρμα ηλεκτρονικού εμπορίου, η οποία διαθέτει ένα περιβάλλον ανάπτυξης ηλεκτρονικών καταστημάτων που παρέχει σε εμπόρους πρόσβαση σε πλήρη επιχειρηματική λειτουργία, με την αξιοποίηση εφαρμογών με μικρές απαιτήσεις συγγραφής κώδικα (low code applications), προσφέροντας έναν προσιτό (από οικονομικής και διαχειριστικής άποψης), τρόπο εισόδου στο ηλεκτρονικό εμπόριο (Dushnitsky & Stroube,

	2021). Η εταιρία φιλοξενεί πάνω από ένα εκατομμύριο επιχειρήσεις και παρουσίασε μεγάλη άνοδο την περίοδο του lockdown (Reuters, 2020). Τον Σεπτέμβριο του 2020 η Shopify ανακοίνωσε ότι 2 υπάλληλοί της, μέλη της ομάδας υποστήριξης, απέκτησαν κακόβουλα πρόσβαση στα δεδομένα πελατών «λιγότερο από 200 εμπόρων». Σύμφωνα με την πλατφόρμα, τα δεδομένα περιλάμβαναν ονόματα, φυσικές και ηλεκτρονικές διευθύνσεις και στοιχεία παραγγελιών ενώ απέκλεισε την περίπτωση πρόσβασης σε πλήρεις αριθμούς τραπεζικών καρτών. Η σχετική ανακοίνωση καταλογίζει στους δύο υπαλλήλους, σχέδιο για την απόκτηση των αρχείων συναλλαγών (Shopify, 2020) Κατά τη διερεύνηση της υπόθεσης, οι δικαστικές αρχές των ΗΠΑ απήγγειλαν κατηγορίες εναντίον ενός άνδρα από την Καλιφόρνια ότι αυτός εξασφάλισε μέσω δωροδοκίας εσωτερική συνεργασία, προκειμένου να αποκτήσει δεδομένα εμπόρων και πελατών από τα ηλεκτρονικά καταστήματα που φιλοξενούσε η πλατφόρμα. Με βάση το κείμενο της κατηγορίας, ο σκοποί της παραβίασης ήταν α) η δημιουργία ιστοσελίδων που θα προσιδίαζαν με αυτές των εμπόρων, με στόχο την απόσπαση πελατείας και β) η πώληση των δεδομένων εμπόρων και πελατών για την διάπραξη απάτης [67] . Σύμφωνα με το κατηγορητήριο, η απόσπαση των δεδομένων γινόταν μέσω screenshots και αφού οι εμπλεκόμενοι είχαν συζητήσει μέσω μηνυμάτων τρόπους ώστε αυτό να μην γίνει αντιληπτό (United States District Court, 2021; Whittaker, 2021). Αναφορικά με το συμβάν, προέκυψαν ομαδικές δικαστικές προσφυγές που προβάλουν ισχυρισμούς για έκθεση των δεδομένων 272.000 χρηστών με δυνατότητα ταυτοποίησης τους σε σχέση με την αγορά κρυπτονομισμάτων, εξ αιτίας αμέλειας της πλατφόρμας και της εταιρείας ασφάλειας κρυπτονομισμάτων (Ledger) που την χρησιμοποιούσε (Joseph C. Stepina, 2022; Top Class Actions, 2022).
Μετριασμός	Σύμφωνα με τις ανακοινώσεις της εταιρίας, μόλις έγινε αντιληπτή η παραβίαση (ο ακριβής τρόπος δεν αναφέρεται), η πλατφόρμα Shopify ξεκίνησε έρευνα που οδήγησε στον εντοπισμό των δύο υπαλλήλων. Η πρόσβασή τους διακόπηκε, απολύθηκαν και η υπόθεση παραπέμφθηκε στις αρχές. Παράλληλα ενημερώθηκαν ομοσπονδιακές υπηρεσίες όπως το FBI. Επίσης, η Shopify απευθύνθηκε σε εταιρία που ασχολείται με το ηλεκτρονικό έγκλημα για να συνδράμει στη διαλεύκανση της υπόθεσης και την αποκατάσταση. Οι έμποροι που έγιναν στόχοι της επίθεσης ενημερώθηκαν μέσω email, ενώ σύμφωνα με την ανακοίνωση της εταιρίας, στελέχη της ήρθαν σε επικοινωνία με τα θύματα, για τα τους βοηθήσουν να διαχειριστούν το περιστατικό (Shopify, 2020).
Ανάκαμψη	Η εταιρία δημοσιοποίησε το περιστατικό και διατήρησε επικοινωνία με το κοινό μέσω της ιστοσελίδας της, προκειμένου να διατηρήσει την αξιοπιστία της. Μέσω αυτής της επικοινωνίας απάντησε σε ανησυχίες χρηστών, σε υπόνοιες για

[67] 5.Defendant HEINRICH and UCC2 would use the stolen data for their personal benefit, including (a) by setting up merchant pages that were similar to the pages of the real merchants whose data had been stolen in order to take business away from those merchants, and (b) by selling the data to other co-conspirators who would use the data to commit fraud against the merchants and their customers. UNITED STATES DISTRICT COURT

	σύνδεση του περιστατικού με παράνομες χρεώσεις καρτών κ.λπ. (Shopify, 2020). Το συμβάν αποδόθηκε από την εταιρία σε κατάχρηση προνομίων των υπαλλήλων στήριξης και όχι σε τεχνική αδυναμία της πλατφόρμας. Σε σχέση με την ευθύνη της πλατφόρμας απέναντι στους εμπόρους που φιλοξενεί και την δυνατότητα διεκδικήσεων, υπάρχει μεταξύ των όρων χρήσης της, αποδοχή από μέρους τους άρνησης ευθύνης και αποζημίωσης σε περίπτωση απώλειας κερδών και φήμης από αμέλεια της πλατφόρμας[68]. Η εταιρεία Ledger, στην οποία χρεώθηκε επίσης ευθύνη από τελικούς καταναλωτές, στην ιστοσελίδα της αναφέρει μέτρα που έλαβε μόλις ενημερώθηκε και εκείνα που προτίθεται να λαμβάνει αναφορικά με το περιστατικό και άλλες καταγεγραμμένες απειλές. Μεταξύ των μέτρων αυτών είναι η πρόσληψη νέου διευθυντή ασφαλείας, οι διενέργεια δοκιμών διείσδυσης και η εφαρμογή νέων πολιτικών, όπως η διαγραφή δεδομένων (Ledger, 2025).
Διορθωτικές ενέργειες	Σε email που απέστειλε θιγόμενος λιανοπωλητής (Kylie Cosmetics) με στόχο να ανακτήσει την εμπιστοσύνη των πελάτων του, αναφέρει ότι η Shopify έχει δεσμευτεί ότι μετά το συμβάν εφαρμόζει πρόσθετους ελέγχους για την αποτροπή παρόμοιων περιστατικών (BBC, 2020).
Αποτίμηση	Η ανακοίνωση της εταιρίας αναφέρει ότι η πλατφόρμα δεν αντιμετώπιζε τεχνική ευπάθεια (Shopify, 2020), ωστόσο αυτό δεν ήταν αρκετό για να αποτρέψει την απειλή εκ των έσω και να εμπλέξει την εταιρία σε δικαστικές διεκδικήσεις με αιτιολογία την αμέλεια.

Πίνακας 19. Περιστατικό Shopify 2020, Εσωτερική παραβίαση δεδομένων και συνεργασία με τρίτο μέρος (Reuters, 2020; Shopify, 2020)

4.2.2 Περιστατικό «Dyn 2016»: DDoS σε βάρος του παρόχου υπηρεσιών DNS με επιπτώσεις σε ηλεκτρονικές πλατφόρμες μέσω εφοδιαστικής αλυσίδας

Η επίθεση	Στις 21 Οκτωβρίου του 2016 ο Dyn, πάροχος υπηρεσιών DNS, δέχθηκε επιθέσεις DDoS οι οποίες αποδόθηκαν από επιστημονικές μελέτες κατά 71 % σε IP που συνδέονται με συσκευές του IoT μολυσμένες με το λογισμικό Mirai, αφήνοντας ανοικτό το ενδεχόμενο να συμμετείχαν και άλλες συσκευές (Antonakakis et al., 2017). Αναφέρθηκε η πιθανότητα να ήταν μια εκδικητική επίθεση κατά του Dyn για την συμβολή του, στην σύλληψη 2 χάκερς που διαχειρίζονταν ένα κύκλωμα παροχής υπηρεσιών DDoS επί πληρωμή (Schneier, 2016). Ωστόσο ομάδες χάκερς διεκδίκησαν το συμβάν ως πράξη διαμαρτυρίας και υποστήριξης προς τον WikiLeaks και τον Julian Assange, με τους ερευνητές να

[68] «You expressly understand and agree that, to the extent permitted by applicable laws, Shopify and its suppliers will not be liable for any direct, indirect, incidental, special, consequential or exemplary damages, including but not limited to, damages for loss of profits, goodwill, use, data or other intangible losses arising out of or relating to the use of or inability to use the Service or these Terms of Service (however arising, including negligence).» https://www.shopify.com/legal/terms#7-limitation-of-liability-and-indemnification

	αμφισβητούν τις δηλώσεις και τις αποδείξεις τους. Το γεγονός είναι ότι ως αποτέλεσμα των επιθέσεων, υπήρξε διακοπή της πρόσβασης σε δημοφιλείς πλατφόρμες μεταξύ των οποίων το Netflix, το Twitter, το Spotify, την Amazon κ.ά. (Geller & Romm, 2016; Leonardo Pizzuti, 2016). Σύμφωνα με την εργασία (Antonakakis et al., 2017), από την τεχνική ανάλυση διαδοχικών επιθέσεων στον Dyn και σε πλατφόρμες ηλεκτρονικών παιχνιδιών, προέκυψε η πιθανότητα η επίθεση στον Dyn να εκμεταλλεύτηκε την εφοδιαστική αλυσίδα και ο πραγματικός στόχος να ήταν πλατφόρμες παιχνιδιών (PlayStation, Xbox Live,Valve Steam, Nuclear Fallout) οι οποίες έγιναν στόχοι έμμεσης (μέσω του Dyn), αλλά και άμεσης επίθεσης κατά το ίδιο χρονικό διάστημα. Στην περίπτωση αυτή, οι συνέπειες για την ευρύτερη βάση πελατών του παρόχου ήταν παράπλευρες.
Μετριασμός	Σύμφωνα με αρχειοθετημένη ανακοίνωσή της Dyn (Dyn, 2016), στις 21/10/16 η εταιρία δέχθηκε επίμονες επιθέσεις DDoS σε διαφορετικούς χρόνους. Η πρώτη διήρκησε περίπου 2 ώρες (11:10-13:20) μέχρι η εταιρία να καταφέρει να την αντιμετωπίσει και επηρέασε τις ΗΠΑ. Η δεύτερη επίθεση διήρκησε 1 ώρα περίπου (15:50-17:00) και είχε παγκόσμιο χαρακτήρα. Επιθέσεις των επόμενων ωρών και ημερών, σύμφωνα με την εταιρία, δεν έγιναν αισθητές καθώς αποτράπηκαν κατά την εκδήλωσή τους. Οι τεχνικοί της εταιρίας εφάρμοσαν μια σειρά από τεχνικές μετριασμού που στόχευαν στο να μειώσουν τον όγκο της κίνησης στο δίκτυο, να διαμοιράσουν το φορτίο, να διαχωρίσουν την ύποπτη κίνηση από την νόμιμη δραστηριότητα και να αποκλείσουν τα κακόβουλα πακέτα.
Ανάκαμψη	Οι πελάτες των ιστοτόπων που εξυπηρετούσε ο Dyn αντιμετώπισαν προβλήματα διαθεσιμότητας. Ο Dyn αποκατέστησε τη διαθεσιμότητα, αντιμετωπίζοντας σταδιακά τις επιθέσεις. Επίσης μέσω της αναφοράς και των ανακοινώσεών του του ενημέρωσε το κοινό για τις προσπάθειες που κατέβαλε και τις προκλήσεις που αντιμετώπισε (Dyn, 2016).
Διορθωτικές ενέργειες	Οι διορθωτικές ενέργειες που πραγματοποιήθηκαν έχουν ως ακολούθως (Haq et al., 2022): • Μετά το περιστατικό η εταιρία δήλωσε ότι επεκτείνει επιθετικά τα μέτρα που χρησιμοποίησε κατά την διάρκεια της επίθεσης και συζητά με τους παρόχους υποδομών με σκοπό την ανταλλαγή γνώσεων για τις μεθόδους μετριασμού τέτοιων επιθέσεων (Dyn, 2016). • Κάποιοι ιστότοποι που εξυπηρετούσε αποκλειστικά ο Dyn, προχώρησαν σε συνεργασία με περισσότερους παρόχους DNS για να μειώσουν τον κίνδυνο για μελλοντικά, παρόμοια, περιστατικά που θα απειλούσαν την διαθεσιμότητα τους.
Αποτίμηση	Τα σημαντικά στοιχεία της αποτίμησης του περιστατικού μπορούν να κωδικοποιηθούν ως ακολούθως: • Στην περίπτωση αυτή, με βάση την αναφορά της εταιρίας, ο διαχωρισμός της νόμιμης από την κακόβουλη κίνηση ήταν πολύ δύσκολος, λόγω του ότι τα αιτήματα προερχόταν από τεράστιο αριθμό διευθύνσεων IP από

διαφορετικές γεωγραφικές περιοχές. Κατά τη διάρκεια της επίθεσης, η κυκλοφορία στο δίκτυο αυξήθηκε 40-50 φορές σε σχέση με τα φυσιολογικά/συνήθη επίπεδα. Οι εκτιμήσεις για το μέγεθος των bits που στέλνονταν ανά δευτερόλεπτο έφτασαν στα 1,2 Tbits, περιλαμβάνοντας τόσο τα νόμιμα αιτήματα DNS όσο και τα αιτήματα των επιθέσεων. Σημειώνεται ότι μερίδιο της αύξησης, το οποίο εκτιμάται μεταξύ 10 και 20 φορών επί της κανονικής κίνησης, οφείλεται στα νομότυπα αιτήματα, τα οποία αποτύγχαναν λόγω της επίθεσης και επαναλαμβάνονταν (Dyn, 2016).

Σε μια γενικότερη αποτίμηση (Schneier, 2016) οι επιθέσεις αυτές ανέδειξαν δύο σημαντικά θέματα:

- Η δυναμική των επιθέσεων αυτών οφειλόταν σε μεγάλο βαθμό στην χειραγώγηση συσκευών του IoT. Αυτό μας οδηγεί στο συμπέρασμα ότι όσο το IoT εξαπλώνεται, προκύπτει η ανάγκη να περιοριστεί η δυνατότητα συσκευές αυτού του είδους να αξιοποιούνται σε επιθέσεις DDoS. Ο Schneier επισημαίνει ότι η αγορά δεν έχει ουσιαστικά κίνητρα να βελτιώσει την ασφάλεια των συσκευών, γιατί οι συνέπειες από την χρήση τους σε botnet δεν επηρεάζουν ούτε τους κατασκευαστές ούτε τους αγοραστές τους. Επίσης βελτιώσεις στην ασφάλεια τους επιβαρύνουν το κόστος τους.
- Η Ευρωπαϊκή Ένωση αντιμετώπισε αυτή την πρόκληση το 2024 με τον Κανονισμό 2847. Στο προοίμιο του κανονισμού αναγνωρίστηκε ότι θα πρέπει οι κατασκευαστές να σχεδιάζουν και να αναπτύσσουν συσκευές, μεταξύ των οποίων και συσκευές που συνδέονται έμμεσα με δίκτυα, με βάση τις στοιχειώδεις αρχές κυβερνοασφάλειας[69]. Η υποχρέωση αυτή καθίσταται νομικά δεσμευτική με τις διατάξεις του άρθρου 13 του κανονισμού. Επίσης στις ΗΠΑ με ομοσπονδιακό νόμο του 2020 έχουν τεθεί ανάλογες απαιτήσεις για συσκευές του IoT που αγοράζονται από το κράτος[70].

Επιπρόσθετα, σύμφωνα με τον Schneier, οι επιθέσεις αυτές θα μπορούσαν να είχαν αντιμετωπιστεί από τους παρόχους υπηρεσιών κορμού (backbone) πριν φτάσουν στον τελικό στόχο, αλλά αυτοί επίσης δεν είχαν κίνητρα γιατί δεν επηρεάζονταν από την επίθεση και δεν αμειβόταν για να εξασφαλίζουν την ασφάλεια του δικτύου.

[69] «οι κατασκευαστές θα πρέπει να διασφαλίζουν ότι όλα τα προϊόντα με ψηφιακά στοιχεία σχεδιάζονται και αναπτύσσονται σύμφωνα με τις ουσιώδεις απαιτήσεις κυβερνοασφάλειας που ορίζονται στον παρόντα κανονισμό. Η εν λόγω υποχρέωση αφορά τόσο προϊόντα που μπορούν να συνδεθούν φυσικά μέσω διεπαφών υλισμικού όσο και προϊόντα που συνδέονται λογικά, όπως μέσω υποδοχών δικτύου, σωλήνων, αρχείων, διεπαφών προγραμματισμού εφαρμογών ή οποιουδήποτε άλλου είδους διεπαφής λογισμικού. Δεδομένου ότι οι κυβερνοαπειλές μπορούν να διαδοθούν μέσω διαφόρων προϊόντων με ψηφιακά στοιχεία πριν από την επίτευξη συγκεκριμένου στόχου, για παράδειγμα με την αλυσιδωτή προσέγγιση εκμετάλλευσης πολλαπλών ευπαθειών, οι κατασκευαστές θα πρέπει επίσης να διασφαλίζουν την κυβερνοασφάλεια των προϊόντων με ψηφιακά στοιχεία που συνδέονται μόνο έμμεσα με άλλες συσκευές ή δίκτυα.» (9)/Κανονισμός (ΕΕ) 2024/2847 , Πηγή: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX:32024R2847

[70] Internet of Things Cybersecurity Improvement Act of 2020, https://www.govinfo.gov/content/pkg/COMPS-15863/pdf/COMPS-15863.pdf

	Σε πιο πρόσφατη μελέτη (Collier & Clayton, 2025) αναφέρεται ότι για την αντιμετώπιση των επιθέσεων DDoS υπάρχουν τεχνικές λύσεις, ωστόσο η εφαρμογή τους απαιτεί συλλογική και παγκόσμια δράση η οποία δυσχεραίνεται από την έλλειψη ευθυγράμμισης κινήτρων στους παρόχους του Διαδικτύου και τον εμπορικό χαρακτήρα των υπηρεσιών.

Πίνακας 20. Περιστατικό DDos σε βάρος του παρόχου DNS με επιπτώσεις σε ηλεκτρονικές πλατφόρμες μέσω εφοδιαστικής αλυσίδας (Dyn, 2016)

4.3 Βιομηχανικά συστήματα και κρίσιμες υποδομές

Τα βιομηχανικά συστήματα και οι κρίσιμες υποδομές μπορεί να πληγούν είτε έμμεσα μέσω πληροφοριακών συστημάτων και δικτύων (IT) είτε άμεσα μέσω του ελέγχου φυσικών διαδικασιών (OT). Για το λόγο αυτό, ο οδηγός του NIST για την ασφάλεια της επιχειρησιακής τεχνολογίας (NIST, 2023) προτείνει μια αρχιτεκτονική διαχωρισμού ανάμεσα στα βιομηχανικά και τα πληροφοριακά συστήματα με την χρήση μηχανισμών όπως firewalls, δημιουργία ενδιάμεσης δικτυακής ζώνης (DMZ-Demilitarized Zone), εφαρμογή πολυεπίπεδης αρχιτεκτονικής προστασίας κ.λπ. Στόχος είναι να διασφαλίζονται τα κρίσιμα βιομηχανικά συστήματα μέσω μηχανισμών ελέγχου και περιορισμού της επικοινωνίας με τα εταιρικά πληροφοριακά συστήματα. Επισημαίνει επίσης την ανάγκη πρόσβασης με διαφορετικούς μηχανισμούς πιστοποίησης και διαπιστευτηρίων μεταξύ χρηστών των εταιρικών (IT) και των βιομηχανικών (OT) συστημάτων. Σε μελέτη που αφορά την περίπτωση της επίθεσης στην εταιρία Colonial pipeline το 2021, μια από τις ευπάθειες που οδήγησαν στο κλείσιμο του αγωγού αναφέρεται πως ήταν η έλλειψη επαρκούς διαχωρισμού των δικτύων (Musluoglu et al., 2024).

Επιπλέον ο οδηγός του NIST δίνει έμφαση στον περιορισμό της φυσικής πρόσβασης ως μέτρο για την διασφάλιση της ορθής λειτουργίας των βιομηχανικών διαδικασιών.

Σε κάθε περίπτωση, είναι σημαντικό να διασφαλιστεί η διαθεσιμότητα των βιομηχανικών συστημάτων και η ασφάλεια του φυσικού κόσμου. Και αυτό εξαρτάται από την ασφαλή λειτουργία των συστημάτων OT (NIST, 2023).

4.3.1 Περιστατικό «Colonial pipeline», ΗΠΑ 2021: Ransomware με στόχο τα πληροφοριακά συστήματα της εταιρίας διαχείρισης αγωγού καυσίμων

Η επίθεση	Τον Μάιο του 2021 η εταιρεία Colonial pipeline, η οποία διαχειρίζεται το 45% των καυσίμων της Ανατολικής Ακτής των ΗΠΑ, δέχθηκε επίθεση ransomware η οποία επηρέασε τα πληροφοριακά συστήματα της εταιρίας. Επίσης κλάπηκαν 100 gigabytes δεδομένων. Η κακόβουλη είσοδος στα συστήματα της πραγματοποιήθηκε με χρήση νόμιμων διαπιστευτηρίων που αφορούσαν μη χρησιμοποιούμενο λογαριασμό υπαλλήλου που είχε συνταξιοδοτηθεί. Ο

	ακριβής τρόπος διαρροής των διαπιστευτηρίων δεν έχει προσδιοριστεί. Η παύση λειτουργιών (shutdown) που ακολούθησε είχε σαν αποτέλεσμα να υπάρξουν ελλείψεις σε καύσιμα, με σημαντικές κοινωνικές και οικονομικές συνέπειες. Η εταιρία πλήρωσε στην ομάδα DarkSide 4,4 εκατομμύρια δολάρια σε Bitcoin για το κλειδί της αποκρυπτογράφησης. Οι εισβολείς κατάφεραν να αποχωρήσουν διαγράφοντας τα ίχνη τους, με αποτέλεσμα να μην είναι γνωστή η μεθοδολογία που ακολούθησαν (Beerman et al., 2023).
Μετριασμός	Για την αποτροπή διάδοσης της επίθεσης, η εταιρία για το διάστημα 7-13 Μαΐου του 2021, επέλεξε την παύση λειτουργίας (shutdown). Επίσης ο κρατικός μηχανισμός ενεργοποιήθηκε για τον μετριασμό των επιπτώσεων στην βιομηχανία και τους καταναλωτές, υποστηρίζοντας τις προσπάθειες διαχείρισης της κατάστασης. Παράλληλα ζητήθηκε η συνδρομή του FBI και της CISA (U.S. Department of Energy, 2021).
Ανάκαμψη	Υπό το βάρος των επιπτώσεων και παρά τις αντίθετες συστάσεις, πληρώθηκαν τα λύτρα και τα συστήματα αποκαταστάθηκαν σε μερικές μέρες. Ποσό 2,3 εκατομμυρίων εκ των λύτρων επανακτήθηκε με ενέργειες των αρχών. Με δήλωση του ο διευθύνων σύμβουλος της εταιρίας δικαιολόγησε την απόφαση με το επιχείρημα ότι η σύντομη αποκατάσταση μιας κρίσιμης υποδομής ήταν το καλύτερο για την χώρα. Ωστόσο η επιλογή της εταιρίας να υποκύψει στον εκβιασμό δέχεται κριτική, καθώς θεωρείται ότι έδωσε ισχυρό κίνητρο στους χάκερς για παρόμοιες μελλοντικές επιθέσεις (Beerman et al., 2023).
Διορθωτικές ενέργειες	Η είσοδος στα συστήματα της εταιρίας δεν απαιτούσε έλεγχο πολλαπλών παραγόντων με αποτέλεσμα οι επιτιθέμενοι με απλή είσοδο (όνομα χρήστη και κωδικό) να αποκτήσουν πρόσβαση στο δίκτυο. Μετά την επίθεση εγκαταστάθηκαν κατάλληλοι μηχανισμοί ώστε εάν κάποιος επιχειρούσε πρόσβαση σε κρίσιμα σημεία ενώ δεν κατείχε τα απαραίτητα δικαιώματα, να ενεργοποιείται συναγερμός (Beerman et al., 2023). Μετά την επίθεση οι αρχές επέβαλαν μια σειρά από υποχρεώσεις στους διαχειριστές των αγωγών καυσίμων, όπως η αναφορά των επιθέσεων στη CISA, η υλοποίηση σχεδίου κυβερνοασφάλειας, η ανάπτυξη σχεδίου αντιμετώπισης περιστατικών και η καθιέρωση προγράμματος αξιολόγησης της κυβερνοασφάλειας μέσω προληπτικού ελέγχου (U.S. Transportation Security Administration, 2022).
Αποτίμηση	Αν και η επίθεση δεν στόχευε απ' ευθείας τον αγωγό, είχε επιπτώσεις στην λειτουργία του. Το αποτέλεσμα ήταν κοινωνική αναστάτωση, οικονομικές επιπτώσεις (πληρωμή λύτρων και διαταραχές στην αγορά), ενώ απειλήθηκε η ενεργειακή επάρκεια της χώρας και επλήγη η αξιοπιστία και η φήμη της εταιρίας (Beerman et al., 2023). Η περίπτωση αυτή αποκάλυψε σοβαρές αδυναμίες στην κυβερνοασφάλεια κρίσιμων υποδομών. Ο απολογισμός του περιστατικού έδειξε την ανάγκη για περιορισμό της έκθεσης ενός οργανισμού μέσω σχεδίων αποχώρησης για τους υπαλλήλους που δεν εργάζονται πλέον σε αυτόν και της ύπαρξης οργανωμένων σχεδίων προστασίας και αντίδρασης (Segal, 2022). Σύμφωνα με μελέτες (Beerman et al., 2023; Musluoglu et al., 2024), η επίθεση και οι επιπτώσεις της θα μπορούσαν να είχαν αποσοβηθεί εύκολα, αν είχε γίνει

	χρήση προληπτικών μέτρων. Μέτρα όπως ο ισχυρός έλεγχος ταυτότητας, ο διαχωρισμός των δικτύων και η συνεχής παρακολούθηση ύποπτης δραστηριότητας δεν είχαν εφαρμοστεί στο σύστημα της Colonial pipeline.

Πίνακας 21. Περιστατικό «Colonial pipeline, 2021» (Beerman et al., 2023)

4.3.2 Περιστατικό «Trisis 2017»: εξελιγμένη απειλή με στόχο το σύστημα ασφαλείας πετροχημικής εγκατάστασης

Η επίθεση	Η επίθεση που έμεινε γνωστή ως Trisis ή Triton ή Hatman, είχε στόχο το σύστημα ασφαλείας μιας εγκατάστασης στη Μέση Ανατολή (Maynard et al., 2020). Σύμφωνα με πηγές το συμβάν αφορά πετροχημικό εργοστάσιο στην Σαουδική Αραβία. Ο αρχικός τρόπος εισόδου των επιτιθέμενων και ο φορέας της απειλής δεν έγιναν γνωστοί. Οι πιθανολογούμενοι στόχοι ήταν η διακοπή λειτουργίας του εργοστασίου ή η λειτουργεία του σε επισφαλείς συνθήκες (Geiger et al., 2020). Το κακόβουλο λογισμικό Trisis εγκαταστάθηκε σε υπολογιστή που χρησιμοποιούνταν για τη διαχείριση και τον προγραμματισμό συστημάτων ελέγχου που αφορούν την ασφαλεία (engineering workstation). Μέσω αυτού υπήρξε πρόσβαση και έγινε διαμόρφωση στο τελικό σύστημα ασφαλείας, χωρίς την χρήση του επίσημου λογισμικού. Το σύστημα αυτό (Triconex SIS), είχε κατασκευαστεί από την Schneider Electric και περιείχε την ασφαλιστική δικλείδα να προχωρά σε διακοπή διεργασιών σε περίπτωση κινδύνου φυσικής βλάβης (Maynard et al., 2020). Το κακόβουλο λογισμικό ήταν εξελιγμένο και είχε την δυνατότητα απομακρυσμένου ελέγχου και τροποποίησης των συστημάτων ασφαλείας. Η επίθεση χαρακτηρίζεται από εξειδικευμένη τεχνογνωσία καθώς εκτός των άλλων απαιτούσε γνώση προηγμένων βιομηχανικών συστημάτων. Εξ αυτού του γεγονότος, αλλά και από το γενικότερο πλαίσιο της επίθεσης, συνάγεται ότι για τη διενέργεια της επίθεσης δαπανήθηκαν πολλοί πόροι (Maynard et al., 2020; Mekdad et al., 2021).
Μετριασμός και Ανακάμψη	Το κακόβουλο λογισμικό δεν ανιχνεύτηκε από τα συστήματα άμυνας, ωστόσο οι ρυθμίσεις που επέφερε στη λογική και τη μνήμη του συστήματος ασφάλειας δεν είχαν πλήρη συμβατότητα με την συγκεκριμένη διαμόρφωση του στόχου, με αποτέλεσμα να υπάρξει αποτυχία στον έλεγχο επικύρωσης. Η αποτυχία οδήγησε το σύστημα ασφαλείας σε κατάσταση σφάλματος με αποτέλεσμα να τεθεί εκτός λειτουργίας. Αυτό οδήγησε σε έρευνα και εντοπισμό της επίθεσης. Η εγκατάσταση τέθηκε εκτός λειτουργίας και απομονώθηκε το βιομηχανικό δίκτυο ελέγχου για λόγους ασφαλείας και εξάλειψης της απειλής (FireEye, 2017; Maynard et al., 2020).
Αποτίμηση	Η επίθεση αυτή, τουλάχιστον κατά το τμήμα της που μας είναι γνωστό, πραγματοποιήθηκε μέσω απομακρυσμένης πρόσβασης. Το ενδιαφέρον είναι, ότι δεν ανιχνεύθηκε από κάποιον μηχανισμό κυβερνοασφάλειας αλλά αποκαλύφθηκε μέσω της αποτυχίας του ελέγχου επικύρωσης που εκτελούσε το σύστημα ασφάλειας. Το γεγονός αυτό καταδεικνύει ότι σε βιομηχανικά

	συστήματα η λειτουργική ασφάλεια μπορεί να διαδραματίσει και ρόλο πρόσθετου ή τελικού μηχανισμού άμυνας έναντι των κυβερνοεπιθέσεων.

Πίνακας 22. Περιστατικό Trisis, 2017 (Geiger et al., 2020)

4.4 Υπηρεσίες Υγείας

Στην επιστημονική έρευνα (Ewoh & Vartiainen, 2024), στην οποία πραγματοποιείται ανασκόπηση μελετών που αφορούν την περίοδο 2012-2022, εντοπίζονται 5 βασικές ευπάθειες στον τομέα της Υγείας:

- **Ανθρωπογενείς ευπάθειες.** Ανθρώπινα λάθη λόγω έλλειψης δεξιοτήτων ή εμπειρίας και εσωτερικές απειλές. Αναφορικά με τα ανθρώπινα λάθη, επισημαίνεται η διάδοση του phishing.
- **Παλαιά συστήματα.** Στον τομέα αυτό, συχνά χρησιμοποιούνται παλιά λειτουργικά προγράμματα που δεν ενημερώνονται ως προς την ασφάλεια τους, καθώς και παρωχημένη υλικοτεχνική υποδομή.
- **Χαμηλές επενδύσεις στην κυβερνοασφάλεια.** Στην Υγεία, με βάση μελέτες, συγκριτικά με άλλες δραστηριότητες, οι επενδύσεις στην κυβερνοασφάλεια και στην σχετική εκπαίδευση των εργαζομένων, είναι χαμηλές.
- **Ευπάθειες στις συσκευές τελικού σημείου που συνδέονται με το διαδίκτυο**. Συσκευές όπως αυτές του IoMT (Internet of Medical Things) επεκτείνουν την επιφάνεια άμεσης επίθεσης αλλά και τη δυνατότητα επέκτασης της παραβίασης λόγω διασυνδέσεων με δίκτυα, λογισμικό τρίτων, ή με το υπολογιστικό νέφος. Επίσης, οι συσκευές αυτές, παρουσιάζουν ευπάθειες λόγω σχεδιαστικής ανεπάρκειας ως προς την ασφάλεια ή ακόμη και λόγω παλαιότητας.
- **Επέκταση της ψηφιοποίησης** Ο ψηφιακός μετασχηματισμός του τομέα διευρύνει την επιφάνεια πιθανής απειλής, ενώ συνήθως δεν συνοδεύεται από επαρκή επένδυση στην κυβερνοασφάλεια, καθώς επιλέγεται οι πόροι να κατευθύνονται κυρίως προς την επέκτασή του.

Ο τομέας της Υγείας έχει γίνει στόχος για τους κυβερνοεγκληματίες καθώς η ευαισθησία των δεδομένων και η ανάγκη για συνέχιση των λειτουργιών μπορούν να εντείνουν την πίεση προς τον οργανισμό να υποκύψει στον εκβιασμό. Σύμφωνα με την επιστημονική εργασία (Al-Qarni, 2023), η οποία επισημαίνει την σημασία της κυβερνοασφάλειας στα νοσοκομεία, η κρισιμότητα του τομέα της Υγείας είναι τόσο υψηλή που είναι προτιμότερο να καταβληθούν λύτρα σε περίπτωση αποτυχίας των μηχανισμών άμυνας, παρά να τεθούν σε κίνδυνο οι ζωές ανθρώπων ή να επιτραπεί η διαρροή ευαίσθητων δεδομένων. Η άποψη αυτή δεν συνάδει με τις οδηγίες οργανισμών όπως ο ENISA, οι οποίοι αποθαρρύνουν την πληρωμή λύτρων προκειμένου να μην διαδοθεί το κυβερνοέγκλημα,

ωστόσο αποδίδει τη βαρύτητα του εκβιασμού και το δίλλημα που πρέπει να αντιμετωπίσει η διοίκηση εάν η αποτροπή και ο μετριασμός δεν λειτουργήσουν.

Οι τομείς της Υγείας και των χρηματοοικονομικών, σύμφωνα με την εργασία (Ghanbari & Koskinen, 2024) είναι πρωταρχικοί στόχοι σε ό,τι αφορά την παραβίαση προσωπικών δεδομένων, λόγω του αντικτύπου που έχει η πιθανή διαρροή τους σε περίπτωση εκβιασμού αλλά και λόγω της αξίας μεταπώλησής τους στο Dark Web. Επιπλέον, σε ανάλυση που αφορά την προστασία των προσωπικών δεδομένων στον τομέα της Υγείας (Pool et al., 2024), αναφέρεται ότι τα ιατρικά δεδομένα έχουν μεγαλύτερη αξία μεταπώλησης στον σκοτεινό ιστό από ό,τι τα στοιχεία πιστωτικών καρτών. Αυτό οφείλεται στο γεγονός ότι είναι αξιοποιήσιμα επί μακρόν (δεν ανακαλούνται) και είναι δυνατόν να χρησιμοποιηθούν για ασφαλιστικές απάτες, πλαστή συνταγογράφηση και (εφόσον περιέχουν πλήρη στοιχεία), ακόμη και για κλοπή ταυτότητας.

4.4.1 Περιστατικό «Vastaamo, Φιλανδία 2020»: Παραβίαση και διαρροή δεδομένων ψυχικής υγείας μετά από εκβιασμό

Η επίθεση	Η Vastaamo υπήρξε μια ανερχόμενη εταιρία παροχής υπηρεσιών ψυχικής υγείας, με ετήσια ανάπτυξη άνω του 10%. Η εταιρεία αυτή λειτουργούσε ως υπερεργολάβος για το σύστημα υγείας της Φιλανδίας (Ghanbari & Koskinen, 2024), παρέχοντας υπηρεσίες τηλεϊατρικής αλλά και θεραπεία σε φυσικές τοποθεσίες (Looi et al., 2025). Αναφορικά με την επίθεση, αυτή εξελίχθηκε ως ακολούθως: • Τον Δεκέμβριο του 2018 έγινε η πρώτη παραβίαση δεδομένων. • Στις 15 Μαρτίου του 2019 η σύνδεση με την βάση δεδομένων χάθηκε για ένα διάστημα, ο εισβολέας αφαίρεσε εκ νέου δεδομένα των ασθενών και άφησε μήνυμα με το οποίο απαίτησε λύτρα για να μην τα δημοσιοποιήσει. • Τον Σεπτέμβριο του 2020 η εταιρία κοινοποίησε στις αρχές την παραβίαση δεδομένων. Η εταιρία υποστήριξε ότι τότε δέχθηκε τον πρώτο εκβιασμό, και ότι νωρίτερα δεν γνώριζε τίποτε για παραβίαση, αλλά μόνο για κάποιο τεχνικό θέμα. Ωστόσο, η Αρχή Προστασίας Δεδομένων της Φιλανδίας αναφέρει ότι το σημείωμα για λύτρα που στάλθηκε στις 15/3/19, προσπελάστηκε την ίδια μέρα (Data Protection Ombudsman, 2021). • Τον Οκτώβριο του 2020, εφόσον ο εκβιασμός προς την εταιρία δεν ευοδώθηκε, ο εισβολέας, απευθύνθηκε με email στους ασθενείς ζητώντας τους να του καταβάλουν χρήματα προκειμένου να μη δημοσιοποιήσει τα δεδομένα και τις συνεδρίες τους. Για να γίνει πιο πειστικός δημοσιοποίησε ένα μέρος από τα κλεμμένα δεδομένα στο σκοτεινό διαδίκτυο (Dark Web). Με τον τρόπο αυτό εκτέθηκαν σε κίνδυνο σημαντικά και ευαίσθητα δεδομένα πάνω από 30.000 ασθενών, όπως στοιχεία ταυτοποίησης και σημειώσεις θεραπευτών από συνεδρίες. Σημειώνεται ότι μεταξύ των ασθενών των οποίων τα δεδομένα εκτέθηκαν, συγκαταλεγόταν παιδιά και ευάλωτοι άνθρωποι. Πολλοί άνθρωποι υπέστηκαν σοβαρό κλονισμό από

	το γεγονός, καθώς οι συνεδρίες τους σχετίζονταν με εξαιρετικά ευαίσθητες πληροφορίες (Data Protection Ombudsman, 2021; Ghanbari & Koskinen, 2024).
Μετριασμός	Μεταξύ 18 και 20 Μαρτίου του 2019 η εταιρία εγκατέστησε λογισμικό και τείχος προστασίας για να αποφύγει περαιτέρω βλάβες. Αφού αποκαλύφθηκε η διαρροή συνεργάστηκε με την αστυνομία, ωστόσο δεν είχε προηγηθεί ούτε έγκαιρη ενημέρωση των ασθενών ούτε ενημέρωση της αρμόδιας αρχής (Data Protection Ombudsman, 2021; Ghanbari & Koskinen, 2024).
Ανάκαμψη	• Η Vastaamo αποκατέστησε τα αρχεία που είχαν κλαπεί στις 15 Μαρτίου του 2019, με παλαιότερα εφεδρικά αντίγραφα. Η αποκατάσταση ολοκληρώθηκε στις 12 Απριλίου του 2019 (Data Protection Ombudsman, 2021). • Η εταιρία[71] σε μια προσπάθεια ανάκαμψης μετά τον εκβιασμό προς τους ασθενείς, δημιούργησε γραμμή υποστήριξης και ανακοίνωσε πως θα παρέχει μία δωρεάν συνεδρία στα θύματα. • Στην προσπάθεια να αντιμετωπιστούν οι επιπτώσεις της επίθεσης για να θύματα, ο κρατικός φορέας Victim Support Finland, η εκκλησία και ο δήμος παρείχαν ψυχολογική υποστήριξη, ενώ άλλοι φορείς νομική. Επίσης η αστυνομία έδωσε σχετικές οδηγίες για την καταγγελία και την διαχείριση του περιστατικού[72].
Ευπάθειες και Διορθωτικές ενέργειες	• Η εταιρία δεν χρησιμοποιούσε ένα έτοιμο πιστοποιημένο σύστημα αλλά ανέπτυξε δικό της χωρίς (όπως φαίνεται εκ των πραγμάτων) να είχε την τεχνική ικανότητα. Το λογισμικό αναπτύχθηκε από τον ιδρυτή της εταιρίας που αυτοχαρακτηριζόταν ως αυτοδίδακτος προγραμματιστής, ενώ δεν χρησιμοποιήθηκαν εμπειρογνώμονες για να πιστοποιήσουν την ασφάλεια του (Ghanbari & Koskinen, 2024). Επιπλέον, υπήρχε δυνατότητα απομακρυσμένης πρόσβασης και τα δεδομένα αποθηκεύονταν σε ένα sever MySQL. Σε αυτόν η εταιρία μετέφερε και αποθήκευε τα δεδομένα και τις συνεδρίες των ασθενών χωρίς να τα κρυπτογραφεί. Στα συστήματα επιτρεπόταν απομακρυσμένοι πρόσβαση, και οι κωδικοί που χρησιμοποιούνταν σε αυτό το πλαίσιο (α) διαμοιράζονταν μεταξύ των χρηστών και (β) ήταν χαμηλής πολυπλοκότητας, συνεπώς ο καθένας μπορούσε να επιχειρήσει απομακρυσμένη σύνδεση με το σύστημα της εταιρείας (Looi et al., 2025). • Προσελήφθη μια εταιρία κυβερνοασφάλειας (NIXU) για να ερευνήσει το περιστατικό και να βελτιώσει τα συστήματα της Vastaamo. Ωστόσο η πλήρης διερεύνηση της επίθεσης αποδείχθηκε δύσκολη, μιας και δεν υπήρχαν επαρκείς καταγραφές για τις προσπάθειες παραβίασης. Η NIXU πρότεινε 17 συστάσεις βελτίωσης μεταξύ των οποίων ο server της βάσης δεδομένων να μην είναι άμεσα προσβάσιμος από το δημόσιο δίκτυο αλλά

[71] Sarah Coble , Finnish Patients Blackmailed After Clinic Data Breach, 26/10/20, https://www.infosecurity-magazine.com/news/finnish-patients-blackmailed ,last acc. 18/2/26.

[72] Λίστα ελέγχου για θύματα παραβίασης δεδομένων, 8/11/20, https://kybervpk.fi/en/releases/checklist-for-victims-of-a-data-breach, / Η υπόθεση Vastaamo από την οπτική γωνία του θύματος, 4/1/21, https://www.riku.fi/en/vastaamo-case-from-the-victim-perspective-2, last acc.18/2/2026

	να υπάρχει κρυπτογραφημένη σύνδεση μέσω Virtual Private Network (VPN), να υπάρχουν διακριτοί λογαριασμοί διαχειριστών, ισχυροί κωδικοί, καταγραφή συμβάντων ασφαλείας, ενημερώσεις λογισμικού κ.λπ. (Data Protection Ombudsman, 2021; Ghanbari & Koskinen, 2024). • Η εταιρία προσπάθησε να αναδιαρθρωθεί διοικητικά και επιχειρησιακά, αλλάζοντας διοίκηση και αναζητώντας πόρους. Διερεύνησε την πιθανότητα πρόσβασης σε χρηματοδότηση, χωρίς όμως επιτυχία[73], λόγω της απώλειας εμπιστοσύνης και φήμης και τελικά οδηγήθηκε σε πτώχευση και εξαγορά. Τόσο τα παραβιασμένα αρχεία των ασθενών όσο και το πληροφοριακό της σύστημα, εξαιρέθηκαν από την πώληση. Η αποζημίωση που δόθηκε στα θύματα ήταν μόλις 90 ευρώ στον καθένα (Ghanbari & Koskinen, 2024). • Το αρμόδιο υπουργείο συνέστησε ομάδα εμπειρογνωμόνων για να προτείνει αλλαγές στο νομικό πλαίσιο ώστε να αποτραπεί η εμφάνιση παρόμοιου συμβάντος[74] στο μέλλον.
Αποτίμηση	• Σε ό,τι αφορά τα θύματα, το τραυματικό αντίκτυπο αυτής της επίθεσης στους ασθενείς, στις οικογένειες τους και αλλά και στην κοινωνία που εμπιστευόταν τις υπηρεσίες υγείας, δείχνει το πόσο σημαντικό είναι η προστασία των ευαίσθητων δεδομένων να αποτελεί προτεραιότητα για τον τομέα της υγείας. • Σε ό,τι αφορά την επιχείρηση, η Vastaamo ήταν μια αναπτυσσόμενη εταιρία με πολύ καλές προοπτικές σε σχέση με τον σκοπό της ίδρυσής της. Παρόλα αυτά, το γεγονός ότι κατεύθυνε τους πόρους της στην ψηφιακή ανάπτυξή της, χωρίς να επενδύει παράλληλα στην κυβερνοασφάλεια την οδήγησε σε αποτυχία και πτώχευση. • Σε ό,τι αφορά την κρατική εποπτεία, μια εταιρία που χειριζόταν ευαίσθητα δεδομένα και αποτελούσε επιλογή τους κράτους για την παροχή υπηρεσιών θα έπρεπε να ελέγχεται με βάση ένα αυστηρότερο πλαίσιο ώστε να διασφαλίζεται στην πράξη η συμμόρφωση με τους κανονισμούς και τα πρότυπα ασφάλειας δεδομένων. Αντί για αυτό, η εταιρία, ως οργανισμός που άνηκε στην κλάση Β [75] υποχρεούνταν απλά να αυτοπιστοποιεί την εκπλήρωση των απαιτήσεων ασφαλείας. (Hadi Ghanbari, 2024), (Jeffrey CL Looi, 2024)

Πίνακας 23. Περιστατικό «Vastasmo, 2020» (Data Protection Ombudsman, 2021)

[73] Yle News 29.1.2021 10:23 , Hacked therapy centre Vastaamo goes into liquidation, https://yle.fi/a/3-11762655 , last acc. 25/2/2026.

[74] Expert group appointed to prevent massive data breaches like Vastaamo's , 9/11/2020, https://www.thenomadtoday.com/articulo/finland/government-appoints-experts-to-prevent-data-breaches-such-that-of-vastaamo/20201109194456008958.html , last access 24/2/26

[75] Στη Φινλανδία, τα συστήματα κοινωνικών και υγειονομικών πληροφοριών χαρακτηρίζονται ως συστήματα κλάσης Α ή ως κλάσης Β. Τα συστήματα Κλάσης Β προορίζονται γενικά για μικρότερους οργανισμούς, γεγονός που επέτρεψε στην Vastaamo να αυτό-πιστοποιήσει ότι πληρούσε τις απαιτήσεις ασφαλείας αντί να υποβληθεί σε ανεξάρτητο έλεγχο. Εκτιμάται ότι αυτός ήταν ένας από τους λόγους που οδήγησαν στην παραβίαση.

4.4.2 Περιστατικό «Health Service Executive (HSE)», Ιρλανδία 2021: Ransomware σε βάρος της δημόσιας υγείας

Η επίθεση	• Στις 18 Μαρτίου 2021 μετά από πολλές προσπάθειες phishing, ένα μολυσμένο αρχείο Excel, που είχε επισυναφθεί σε email ανοίχθηκε, μολύνοντας τον αρχικό σταθμό εργασίας. Στην συνέχεια κακόβουλο λογισμικό εξαπλώθηκε πλευρικά στο δίκτυο και αποκτήθηκε πρόσβαση σε λογαριασμούς με υψηλά προνόμια. • Στις 14 Μαΐου 2021 ο φορέας δημόσιας υγείας της Ιρλανδίας δέχθηκε την τελική επίθεση από το κακόβουλο λογισμικό «Conti» το οποίο αγοράστηκε στο Dark Web (Ransomware-as-a-Service) και εγκαταστάθηκε αφού αποκτήθηκε πρώτα έλεγχος του δικτύου. Το λογισμικό αυτό θεωρείται εξελιγμένο καθώς παρέχει δυνατότητα κρυπτογράφησης αλλά και εξαγωγής δεδομένων, γεγονός που αυξάνει την πίεση για λύτρα. Κρίσιμες ιατρικές λειτουργίες (όπως η πρόσβαση σε ιατρικούς φακέλους) και διοικητικές υπηρεσίες (π.χ. λειτουργία πληροφοριακών συστημάτων διαχείρισης και διοίκησης) διακόπηκαν σε πάνω από 50 νοσοκομεία της χώρας, είτε λόγω της κακόβουλης κρυπτογράφησης που έκαναν οι εισβολείς, είτε λόγω της αποσύνδεσης συστημάτων για περιορισμό της εξάπλωσης. • Η επίθεση εκτελέστηκε από 2 διαφορετικές ομάδες, η πρώτη από τις οποίες χειρίστηκε την αρχική πρόσβαση και η δεύτερη την εγκατάσταση του ransomware (Mashinchi et al., 2024).
Μετριασμός	Ο οργανισμός συνεργάστηκε άμεσα με την Interpol, οργανισμούς κυβερνοασφάλειας και ομάδες διαχείρισης περιστατικών. Επίσης μέσα στην ημέρα που εκδηλώθηκε η επίθεση με ransomware, εγκαταστάθηκε λογισμικό για να εντοπιστούν τα μολυσμένα συστήματα και να συλλεχθούν αποδεικτικά στοιχεία για την εγκληματολογική έρευνα (Mashinchi et al., 2024). Στο πλαίσιο του μετριασμού, απενεργοποιήθηκαν κρίσιμα συστήματα για τον περιορισμό της επίθεσης. Το προσωπικό των νοσοκομείων κατέφυγε σε χειρογραφικές λύσεις με τη βοήθεια των πιο έμπειρων στελεχών, μιας και το νεότερο προσωπικό αγνοούσε αυτές τις διαδικασίες. Επίσης ιδιωτικοί φορείς επιστρατεύτηκαν για τη διαχείριση ευάλωτων ασθενών, όπως π.χ. οι ογκολογικοί ασθενείς (Moore et al., 2023).
Ανάκαμψη	Ο οργανισμός αρνήθηκε να πληρώσει λύτρα. Στις 20 Μαΐου οι επιτιθέμενοι παρείχαν το κλειδί της αποκρυπτογράφησης χωρίς αντάλλαγμα, αλλά συνέχισαν να ζητούν λύτρα για να μην διαρρεύσουν δεδομένα ασθενών. Μέχρι της 21 Σεπτεμβρίου ανακτήθηκαν όλοι οι διακομιστές και οι 1075 από τις 1087 εφαρμογές των νοσοκομείων. Για την παρεμπόδιση της διαρροής των δεδομένων εκδόθηκε δικαστική διαταγή, αλλά η τύχη τους παραμένει άγνωστη (Mashinchi et al., 2024).

Ευπάθειες και Διορθωτικές ενέργειες	Το δίκτυο του οργανισμού λειτουργούσε με «επίπεδη» δικτυακή αρχιτεκτονική (flat network architecture)[76], χωρίς τμηματοποίηση και η πλευρική εξάπλωση της απειλής διευκολύνθηκε. Λόγω του Covid19 οι επενδύσεις στην κυβερνοασφάλεια είχαν επιβραδυνθεί εξ αιτίας του του κόστους αντιμετώπισης της πανδημίας και του περιορισμού εσόδων που έφερε το lockdown. Για παράδειγμα, παρωχημένα προγράμματα (Windows 7) χρησιμοποιούνταν σε περισσότερους από 30.000 σταθμούς εργασίας. Επίσης υπήρχαν οργανωτικά κενά, καθώς ο οργανισμός δεν διέθετε Διευθυντή Ασφάλειας και Κέντρο Επιχειρήσεων για περιστατικά κυβερνοασφάλειας (Mashinchi et al., 2024). Ο οργανισμός απευθύνθηκε σε μια εταιρία συμβούλων (PricewaterhouseCoopers - PwC) για αξιολόγηση της επίθεσης και τη λήψη προτάσεων για διορθωτικές ενέργειες. Η PwC πρότεινε μια σειρά από ενέργειες που περιλαμβάνουν αναβάθμιση της τεχνολογικής υποδομής, επανασχεδιασμό του δικτύου, δημιουργία θέσεων κυβερνοασφάλειας σε υψηλό επίπεδο, συνεχή αξιολόγηση κινδύνων, υιοθέτηση μέτρων όπως η διατήρηση αντιγράφων εκτός σύνδεσης (offline), εκπαίδευση του προσωπικού, συνεχείς δοκιμές και συνεργασία με εμπειρογνώμονες κυβερνοασφάλειας (PricewaterhouseCoopers, 2021). Οι διορθωτικές ενέργειες πραγματοποιήθηκαν σταδιακά. Άρθρο των Irish Times (8/5/2024) που αφορά την πορεία των διορθωτικών ενεργειών, αναφέρεται στις δυσκολίες υλοποίησής τους και στο μεγάλο κόστος της επίθεσης και των βελτιώσεων που απαιτήθηκαν βάση της έκθεσης των συμβούλων[77].
Αποτίμηση	Η προσπάθεια για phishing δεν αναγνωρίστηκε έγκαιρα ώστε να αποτραπεί. Για ένα μεγάλο χρονικό διάστημα, η παρουσία των εισβολέων δεν αντιμετωπίστηκε αποτελεσματικά, με αποτέλεσμα αυτοί να εκμεταλλεύονται ευπάθειες και να αυξάνουν τα δικαιώματα τους σε συστήματα και εφαρμογές μέχρι να εγκαταστήσουν το λογισμικό ransomware. Ο οργανισμός διέθετε μέτρα κυβερνοασφάλειας, δεν μπόρεσε ωστόσο να τα εκσυγχρονίσει λόγω περιορισμού πόρων και έμεινε εκτεθειμένος (Mashinchi et al., 2024). Η ανάκαμψη καθυστέρησε. Το προσωπικό, παρ' όλη την εξάντλησή του από την δοκιμασία της πανδημίας και το χάος που δημιούργησε η κυβερνοεπίθεση, λειτούργησε ομαδικά και επέδειξε εξαιρετική επινοητικότητα, γεγονός που καταδεικνύει την δυναμική του ανθρώπινου παράγοντα στην ανθεκτικότητα των οργανισμών (Moore et al., 2023). Παρόλο που δεν πληρώθηκαν λύτρα, με βάση το άρθρο των Irish Times που προαναφέρθηκε και την σχετική συζήτηση στη Φινλανδική Βουλή, η επίθεση κόστισε μεγάλα ποσά στο κράτος και οι διορθωτικές ενέργειες καθυστέρησαν λόγω αυξημένου κόστους.

[76] Κάθε υπολογιστής του δικτύου είχε δηλαδή πρόσβαση σε όλες τις υπηρεσίες οποιουδήποτε άλλου υπολογιστή, συμπεριλαμβανομένων των διακομιστών.

[77] Marie O'Halloran, «Senior HSE cybersecurity roles still not filled three years after major ransomware attack, Some computer devices still using outdated, vulnerable Windows 7 system», https://www.irishtimes.com/politics/oireachtas/2024/05/08/senior-hse-cybersecurity-roles-still-not-filled-three-years-after-malware-attack , last acc.22/2/2026

Πίνακας 24. Περιστατικό Health Service Executive (HSE), 2021 (Mashinchi et al., 2024)

4.5 Εκπαιδευτικά ιδρύματα

Σε πρόσφατη επιστημονική εργασία (Lallie et al., 2025), στην οποία αναλύονται οι κυβερνοεπιθέσεις και οι ευπάθειες στον πανεπιστημιακό τομέα, αναφέρεται ότι στόχοι των επιθέσεων είναι τα προσωπικά στοιχεία φοιτητών και προσωπικού, η πνευματική ιδιοκτησία και τα ερευνητικά δεδομένα. Επιπλέον η κοινωνική μηχανική και ειδικότερα το spear-phishing είναι οι τρόποι που κατά κανόνα εκδηλώνεται η απειλή, με το ransomware να κατατάσσεται δεύτερο στην οικεία λίστα. Το άρθρο διαπιστώνει, με βάση τα αποτελέσματα έρευνας, ότι οι φορείς απειλής είναι κυρίως κυβερνοεγκληματίες που λειτουργούν με στόχο τον εκβιασμό, αλλά αναφέρεται επίσης και σε κρατική κατασκοπεία σε ό,τι αφορά ερευνητικά δεδομένα, στον ακτιβισμό αλλά και τους δυσαρεστημένους ή ανήσυχους φοιτητές που δοκιμάζουν τις ικανότητές τους. Παρατηρείται επίσης, ότι οι ευπάθειες επιδεινώνονται από το γεγονός ότι δεν διαθέτουν όλοι οι χρήστες, επάρκεια στις δεξιότητες πληροφορικής και προτείνει την πολυπαραγοντική ταυτοποίηση όπου χρειάζεται ενισχυμένη προστασία.

Έκθεση που αφορά την κυβενοασφάλεια στην εκπαίδευση (Chapman, 2019), επισημαίνοντας την ιδιαιτερότητα του ακαδημαϊκού χώρου, αναφέρει ότι τα πανεπιστήμια θα πρέπει να εξισορροποίησουν την κουλτούρα ενός φυσικού και ακαδημαϊκού περιβάλλοντος ανοικτής πρόσβασης με την ανάγκη για κυβερνοασφάλεια.

Η Ελληνική αρχή κυβερνοασφάλειας προτείνει 15 σημεία ενίσχυσης της κυβερνοασφάλειας στα πανεπιστημιακά ιδρύματα[78], μεταξύ των οποίων (α) τη δημιουργία μιας ρουτίνας λήψης αντιγράφων και διενέργειας ασκήσων ανάκτησης υπό πίεση, (β) την εκπαίδευση στην κοινωνική μηχανική, (γ) την τμηματοποίηση του δικτύου, (δ) τη χρήση Penetration Tests για τον εντοπισμό ευπαθειών μέσω προσομοίωσης και (ε) την ορθολογική διαχείριση της προνομιακής πρόσβασης.

4.5.1 Περιστατικό «Πανεπιστήμιο του Σαν Φρανσίσκο», ΗΠΑ 2020: Ransomware, κρυπτογράφηση ερευνητικών δεδομένων

Η επίθεση	Τον Ιούνιο του 2020 το τμήμα Ιατρικής του πανεπιστημίου του Σαν Φρανσίσκο στις ΗΠΑ δέχτηκε επίθεση ransomware η οποία ξεκίνησε από

[78] https://cyber.gov.gr/antimetopisi-apeilon/odigos-15-simeion-enischysis-tis-kyvernoasfaleias-kai-apotropis-lytrismikon-epitheseon-ransomware-gia-ta-panepistimiaka-idrymata, τελευταία πρόσβαση στις 13/2/2026

	ένα phishing email [79]. Συστήματα του πανεπιστημίου επηρεάστηκαν, δεδομένα κρυπτογραφήθηκαν και σημαντικές έρευνες τέθηκαν σε κίνδυνο. Η επίθεση μπορεί να καταταχθεί στην κατηγορία του «διπλού εκβιασμού» (Double-extortion): Στην περίπτωση αυτή κρυπτογραφήθηκαν αρχεία με αποτέλεσμα την αδυναμία πρόσβασης σε αυτά, αλλά επιπρόσθετα πριν την κρυπτογράφηση αποσπάστηκαν και ερευνητικά δεδομένα του Πανεπιστημίου άγνωστης έκτασης[80] και ενδεχομένως προσωπικά δεδομένα (University of San Francisco, 2020; Wu, 2020).
Μετριασμός	Τα συστήματα του τμήματος Ιατρικής τέθηκαν σε καραντίνα για περιορισμό της εξάπλωσης και το Πανεπιστήμιο συνεργάστηκε με εξωτερικούς εμπειρογνώμονες και σύμβουλο ασφαλείας για την διαχείριση του περιστατικού[81].
Ανάκαμψη	Το Πανεπιστήμιο έλαβε την απόφαση να καταβάλει περίπου 1,14 εκατομμύρια δολάρια, μετά από διαπραγματεύσεις στο Dark Web, για να μπορέσει να ξεκλειδώσει τα κρυπτογραφημένα αρχεία, υπό το σκεπτικό ότι αυτά ήταν σημαντικά για το ακαδημαϊκό του έργο[82].
Διορθωτικές ενέργειες	Το πανεπιστήμιο ενημέρωσε τον Νοέμβριο του 2020 με σχετική επιστολή, όλους όσους τα στοιχεία τους (αριθμοί κοινωνικής ασφάλισης, αριθμοί ταυτότητας, ιατρικές πληροφορίες, οικονομικές πληροφορίες κ.λπ.) υπήρχε πιθανότητα να διέρρευσαν και δημιούργησε ειδική τηλεφωνική γραμμή υποστήριξης [83]. Δεσμεύτηκε επίσης να επανεξετάζει τα πρωτόκολλα ασφαλείας σε σχέση με τα προσωπικά δεδομένα. Όπως αναφέρουν τα πρακτικά συνεδρίασης της Συγκλήτου του Ιδρύματος που έλαβε χώρα στις 17/12/2020[84], τον Ιούλιο του 2020 συγκροτήθηκε ομάδα εργασίας και με βάση τα συμπεράσματα της, έγινε αποδεκτή μια νέα προσέγγιση, βασισμένη σε 3 πυλώνες: α) δημιουργία τοπικών ομάδων για την προστασία των δεδομένων της έρευνας, β) ανάπτυξη πρωτοβουλιών για ευαισθητοποίηση, γ) καθολικά backups με ευελιξία ως προς τις επιλογές με βάση το κόστος (λόγω της αυξημένης δαπάνης δεν αποκλείστηκε το κόστος να βαρύνει και τους μεμονωμένους ερευνητές).

[79] Σύμφωνα με την πηγή τα δεδομένα κλειδώθηκαν στις 1 Ιουνίου, η πληρωμή των λύτρων έγινε στις 15 Ιουνίου και τα δεδομένα ανακτήθηκαν έως τις 20 Ιουνίου. https://www.scribd.com/document/959542995/UCSF-Ransomware-Final-Report, τελευταία πρόσβαση στις 14/2/26

[80] «The attackers obtained some data as proof of their action, to use in their demand for a ransom payment» https://www.ucsf.edu/news/2020/06/417911/update-it-security-incident-ucsf, τελευταία πρόσβαση 14/2/26

[81] https://www.ucsf.edu/news/2020/06/417911/update-it-security-incident-ucsf, τελευταία πρόσβαση 14/2/26

[82] Σύμφωνα με την πηγή, η αρχική πρόσβαση επιτεύχθηκε με κλεμμένα διαπιστευτήρια που αποσπάστηκαν με phishing email. Τα δεδομένα κλειδώθηκαν στις 1 Ιουνίου, η πληρωμή των λύτρων έγινε στις 15 Ιουνίου και τα δεδομένα ανακτήθηκαν έως τις 20 Ιουνίου. https://www.scribd.com/document/959542995/UCSF-Ransomware-Final-Report, τελευταία πρόσβαση 14/2/26

[83] https://www.ucsf.edu/news/2020/11/418981/ucsf-notifies-individuals-regarding-cybersecurity-incident, τελευταία πρόσβαση 14/2/26

[84] https://senate.universityofcalifornia.edu/_files/committees/ucacc/meetings/ucacc-12-17-20-minutes.pdf, Πρακτικά Συνεδρίασης (17/12/2020) σελίδες 2 έως 3, τελευταία πρόσβαση 15/2/26

	Τον Ιούλιο του 2021[85] τέθηκε σε ισχύ η νέα πολιτική, η οποία περιλαμβάνει, μεταξύ άλλων, πέντε επίπεδα ανάκαμψης, ανάλογα με την κρισιμότητα των δεδομένων, καθορισμό ρόλων και έμφαση στη χρήση των backups για την διατήρηση της επιχειρησιακής συνέχειας και την αντιμετώπιση συγκεκριμένων απειλών.
Αποτίμηση	Από την επίθεση προέκυψαν οι κάτωθι αρνητικές επιπτώσεις: • διακοπή λειτουργίας, διακοπή ερευνών, • πληρωμή λύτρων, • απόσπαση δεδομένων με άγνωστες μελλοντικές συνέπειες, • κόστος πρόσληψης συμβούλων και υλοποίησης διορθωτικών ενεργειών. Από την άλλη πλευρά, ως θετική επιπτώση μπορεί να θεωρηθεί η βελτίωση της ανθεκτικότητας μετά το συμβάν, λόγω της λήψης κατάλληλων μέτρων (University of San Francisco, 2020; Wu, 2020).

Πίνακας 25. Περιστατικό «Πανεπιστήμιο του Σαν Φρανσίσκο, 2020» (University of San Francisco, 2020)

4.6 Ψηφιακή τραπεζική

Η επέκταση της ψηφιοποίησης των τραπεζικών συναλλαγών αυξάνει την έκθεση σε απειλές που οδηγούν σε απώλεια περιουσίας ιδιωτών αλλά και επιχειρήσεων. Μια διαδεδομένη μορφή απειλής είναι οι επιθέσεις που βασίζονται στον ανθρώπινο παράγοντα. Αυτού του είδους οι απειλές αξιοποιούν τόσο την κοινωνική μηχανική όσο και στην ικανότητα των επιτιθέμενων να δημιουργούν ιστοτόπους που προσομοιάζουν με τους αυθεντικούς ιστοτόπους των τραπεζών, οδηγώντας τους χρήστες των ψηφιακών συναλλαγών αρχικά σε σύνδεση με τους πλαστογραφημένους ιστοχώρους και εν συνεχεία σε αποκάλυψη διαπιστευτηρίων (οι χρήστες εισάγουν τα διαπιστευτήριά τους στον πλαστογραφημένο ιστοχώρο και στη συνέχεια τα εισαχθέντα στοιχεία διαβιβάζονται στους επιτιθέμενους). Για την αντιμετώπιση αυτής της απειλής, τα χρηματοπιστωτικά ιδρύματα οφείλουν να εφαρμόζουν αξιόπιστους μηχανισμούς αυθεντικοποίησης αλλά και να επενδύουν στην εκπαίδευση όσων χρησιμοποιούν τις ψηφιακές υπηρεσίες τους. Επιπλέον, η τεχνητή νοημοσύνη και η μηχανική μάθηση ενισχύουν την ανίχνευση ασυνήθιστων συμπεριφορών, εντοπίζοντας ύποπτες συναλλαγές σε πραγματικό χρόνο. Οι κανονισμοί ασφάλειας από τις ρυθμιστικές αρχές προβλέπουν μέτρα ελέγχου ταυτότητας, ανίχνευση της απάτης σε πραγματικό χρόνο και ισχυρά πρωτόκολλα κρυπτογράφησης, ωστόσο οι προκλήσεις εξελίσσονται και επηρεάζουν την εμπιστοσύνη στην ψηφιακή τραπεζική (Waliullah et al., 2025).

[85] https://security.ucop.edu/files/documents/policies/is-12-it-recovery-policy.pdf, University of California – Policy IS-12: IT Recovery, July 1, 2021, τελευταία πρόσβαση 15/2/26

Οι επιθέσεις phishing έχουν εξελιχθεί σε τέτοιο βαθμό ώστε να μπορούν να υπερβαίνουν και την ασφάλεια που προσφέρει η πολυπαραγοντική ταυτοποίηση. Οι επιτιθέμενοι μπορεί να αποκτήσουν τον κωδικό μιας χρήσης (OTP) μέσω κοινωνικής μηχανικής. Είναι δυνατό επίσης σε εξελιγμένες περιπτώσεις να χρησιμοποιούν τεχνικές όπως η Adversary-in-the-Middle (AiTM) όπου οι επιτιθέμενοι παρεμβάλλονται ανάμεσα στον νόμιμο χρήστη που χρησιμοποιεί τον πλαστογραφημένο ιστότοπο και το νόμιμο σύστημα στο οποίο εισάγουν κωδικούς και στοιχεία αυθεντικοποίησης πριν την λήξη τους. Οι επιθέσεις αυτές δεν παραβιάζουν την πολυπαραγοντική ταυτοποίηση αλλά την υποκλέπτουν σε πραγματικό χρόνο (Blancaflor et al., 2025). Η CISA ενθαρρύνει τους οργανισμούς να χρησιμοποιούν ως ανθεκτική στο phishing την αυθεντικοποίηση FIDO2 (Fast Identity Online)[86], η οποία εξαλείφει την ανάγκη αποκάλυψης κωδικών και βασίζεται σε κρυπτογραφικούς μηχανισμούς δημόσιου και ιδιωτικού κλειδιού (CISA, 2022a).

4.6.1 Περιστατικό «Luzerner Kantonalbank (LUKB)», Ελβετία 2025-2026: Πλαστογράφηση ιστοτόπου και phishing

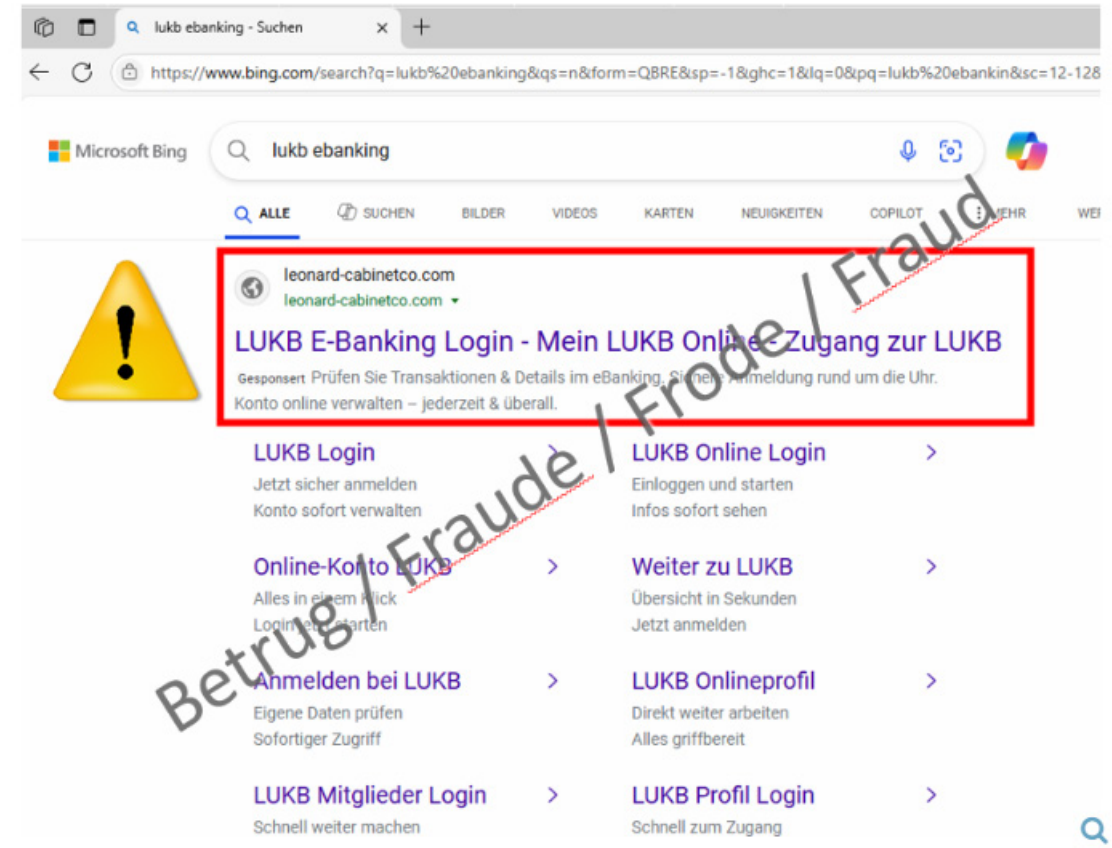
Συμβάντα	Στις 3.7.2025 το Εθνικό Κέντρο Κυβερνοασφάλειας (NCSC SUI, 2025) εξέδωσε ανακοίνωση για να προειδοποιήσει τους χρήστες της ψηφιακής τραπεζικής για ιστοτόπους που μιμούνται πύλες εισόδου σε τραπεζικούς λογαριασμούς. Σύμφωνα με την ανακοίνωση, τα θύματα μετά από αναζήτηση στο διαδίκτυο επιλέγουν την πλαστογραφημένη ιστοσελίδα και καταχωρούν σε αυτή τα διαπιστευτήρια τους. Επιπλέον, οι επιτιθέμενοι χρησιμοποιούν τεχνικές phishing σε πραγματικό χρόνο για να υποκλέψουν και τον δεύτερο παράγοντα ταυτοποίησης που απαιτεί η σύνδεση. Το Κέντρο αναφέρει ότι καταγράφηκαν αρκετές περιπτώσεις εξαπάτησης. Αναφέρεται ως παράδειγμα η πλαστογράφηση του ιστοτόπου της Τράπεζας LUKB και παρουσιάζονται στιγμιότυπα που αντιπαραβάλουν τον πραγματικό ιστότοπο με τον πλαστογραφημένο. Τον Φεβρουάριο του 2026 η LUKB ανακοίνωσε στα κοινωνικά δίκτυα[87], την κυκλοφορία δολίων επιστολών, όπου οι παραλήπτες τους, λαμβάνοντας επείγοντα μηνύματα, καλούνται να εισέλθουν μέσω QR σε υποτιθέμενο ιστότοπο της Τράπεζας.
Μετριασμός και ανάκαμψη	Αναφορικά με το περιστατικό του Ιουλίου, το εθνικό κέντρο κυβερνοασφάλειας καλεί τους χρήστες να αναφέρουν κάθε περίπτωση εξαπάτησης ή ύποπτης δραστηριότητας τόσο στην τράπεζά τους όσο και στο εθνικό κέντρο. Σύμφωνα με ανταπόκριση τοπικού ειδησεογραφικού μέσου (Meier, 2026) για το περιστατικό του Φεβρουαρίου, η εκπρόσωπος τύπου της της LUKB, S. Umiker δήλωσε ότι η τράπεζα μπλοκάρισε τον ιστόποπο που συνδεόταν

[86] https://fidoalliance.org/passkeys/

[87] https://www.instagram.com/p/DU3HNytjWuv/ , https://de.linkedin.com/posts/luzernerkb_achtung-betrugsbriefe-mit-qr-codes-im-activity-7429518053157023744-7Yhy

	με το QR και ενημέρωσε την Ομοσπονδιακή Υπηρεσία Κυβερνοασφάλειας. Επίσης, σύμφωνα με τη δήλωσή της, οι πελάτες ενημερώθηκαν και από τον επίσημο ιστότοπο της τράπεζας. Ενημέρωση, όπως προαναφέρθηκε, υπήρξε και μέσω των κοινωνικών δικτύων.
Αποτίμηση	Στην πρώτη περίπτωση γίνεται αναφορά σε υπέρβαση της ασφάλειας που παρέχει η ταυτοποίηση 2 παραγόντων σε πραγματικό χρόνο, γεγονός που καταδεικνύει ότι οι σχετικές τεχνικές εξαπλώνονται. Τα παραπάνω συμβάντα αφορούν την εμπιστοσύνη στην ψηφιακή τραπεζική και την ασφάλεια της περιουσίας ιδιωτών και επιχειρήσεων. Επίσης, αν και οι επιθέσεις δεν έπληξαν το λειτουργικό σύστημα της Τράπεζας και η εκπρόσωπος της, σύμφωνα με τις πηγές (Meier, 2026), αποδίδει σε τυχόν θύματα βαριά αμέλεια αποκρούοντας αιτήματα αποζημίωσης, τα περιστατικά αυτά συνδέουν το ψηφιακό οικοσύστημα της τράπεζας με τον φόβο επισφαλών συναλλαγών.

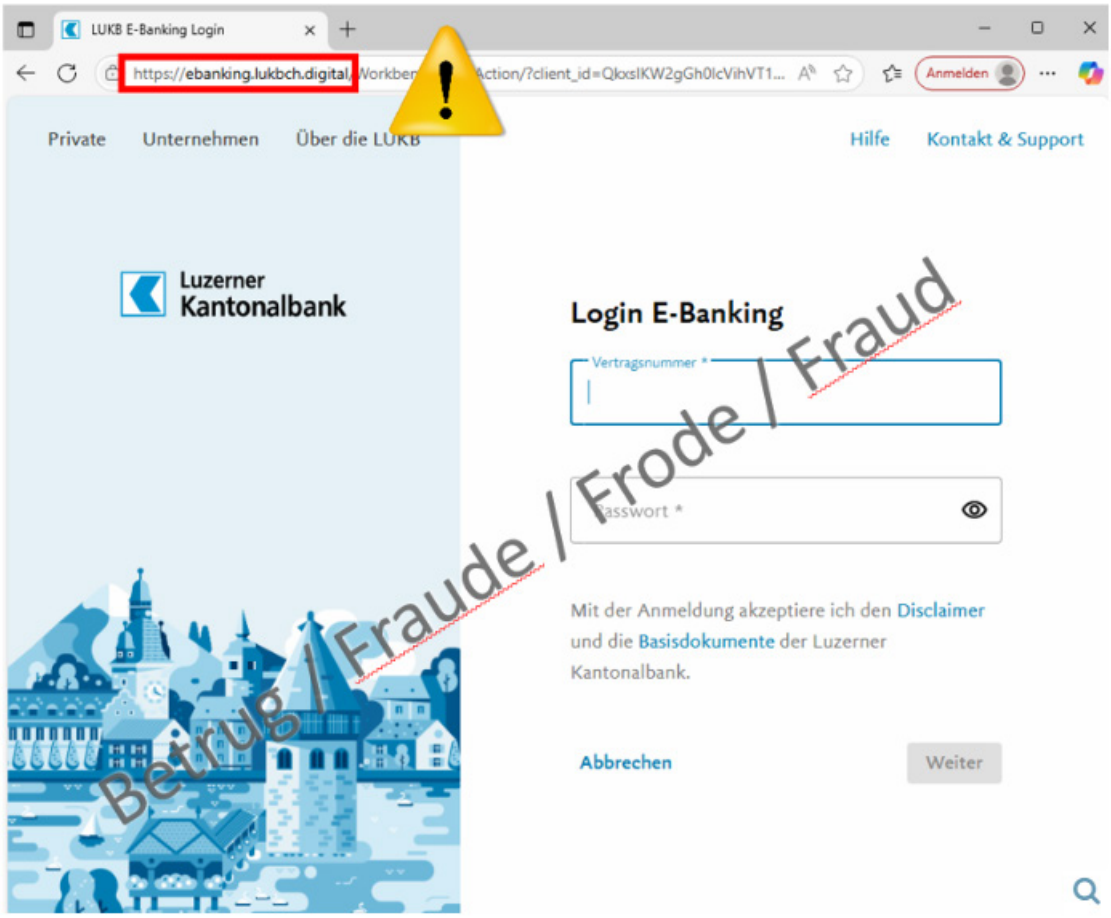
Πίνακας 26. Περιστατικό LUKB, 2025-2026 (Meier, 2026)



Fraudulent search results with hits for the alleged LUKB e-banking site.

Σχήμα 13. Πλασματικά αποτελέσματα αναζήτησης [88]

[88] Πηγή: Εθνικό Κέντρο Κυβερνοασφάλειας Ελβετίας, https://www.ncsc.admin.ch/ncsc/en/home/aktuell/im-fokus/2025/realtimephishing.html



Σχήμα 14. Πλασματική Ιστοσελίδα της LUKB[89]

4.7 Ανακεφαλαίωση

Στην παρούσα ενότητα ανακεφαλαιώνονται οι επιθέσεις, συνοψίζοντας αρχικά τις δράσεις μετριασμού και ανάκαμψης ανά περίπτωση, ενώ στη συνέχεια αναδεικνύονται κοινά μοτίβα επιθέσεων και τέλος συνοψίζονται οι συνέπειες κυβερνοεπιθέσεων.

4.7.1 Μετριασμός και ανάκαμψη ανά περίπτωση

Ο Πίνακας 27 συνοψίζει τις ενέργειες μετριασμού και ανάκαμψης ανά περίπτωση.

[89] Πηγή: Εθνικό Κέντρο Κυβερνοασφάλειας Ελβετίας, https://www.ncsc.admin.ch/ncsc/en/home/aktuell/im-fokus/2025/realtimephishing.html

Τομέας	Στόχοι Μετριασμού	Στόχοι ανάκαμψης		Περιπτώσεις	
Δημόσια Διοίκηση	• Συνέχιση βασικών υπηρεσιών • προστασία συστημάτων και δεδομένων.	• Αποκατάσταση λειτουργιών • Αποκατάσταση της εμπιστοσύνης των πολιτών		**Ατλάντα 2018** **Μετριασμός** • Συνεργασία με τις αρχές • Βοήθεια από ειδικούς, • Απομόνωση παραβιασμένων συστημάτων • Αξιοποίηση της γνώσης χειροκίνητων διαδικασιών • Ενημέρωση πολιτών για εναλλακτικούς τρόπους εξυπηρέτησης **Ανάκαμψη** • Ανοικοδόμηση συστημάτων με μεγάλο κόστος • Αδυναμία πλήρους αποκατάστασης αρχείων από αντίγραφα	
Πλατφόρμες Ηλεκτρονικού Εμπορίου	• Ασφάλεια δεδομένων και ασφάλεια συναλλαγών. • Περιορισμός εξάπλωσης	• Σύντομη αποκατάσταση διαθεσιμότητας. • Ανάκτηση αξιοπιστίας		**Shopify 2020** **Μετριασμός** • Διακοπή της πρόσβασης των υπευθύνων στα συστήματα της εταιρίας • Συνεργασία με FBI και εταιρία διερεύνησης • Ενημέρωση θιγόμενων εμπόρων **Ανάκαμψη** • Συνεχής επικοινωνία με το κοινό • Ανακοινώσεις για ανανεώσεις στελεχών και διαδικασιών	**Dyn** **Μετριασμός** • Εφαρμογή τεχνικών μετριασμού DDos από την τεχνική ομάδα της εταιρίας (διαμοιρασμός φορτίου, διαχωρισμός νόμιμης-κακόβουλης δραστηριότητας κ.λπ.) **Ανάκαμψη** • Επαναφορά της διαθεσιμότητας • Ενημέρωση του κοινού για τις προκλήσεις που αντιμετώπισε και τον τρόπο που τις χειρίστηκε

Τομέας	Στόχοι Μετριασμού	Στόχοι ανάκαμψης		Περιπτώσεις	
Βιομηχανικά Συστήματα και Υποδομές	• Διατήρηση της ασφάλειας. • Συνέχιση κρίσιμων λειτουργιών. • Περιορισμός εξάπλωσης	• Ταχεία και πλήρης αποκατάσταση συστημάτων και λειτουργιών		**Colonial pipeline 2021** **Μετριασμός** • Διακοπή της λειτουργίας του αγωγού για αποτροπή διάδοσης της επίθεσης • Εμπλοκή του κράτους για διαχείριση συνεπειών **Ανάκαμψη** • Αποκατάσταση συστημάτων μετά από πληρωμή λύτρων και λήψης του κλειδιού της αποκρυπτογράφησης	**Πετροχημική εγκατάσταση 2017** **Μετριασμός** • Το κακόβουλο λογισμικό δεν ανιχνεύθηκε από την κυβερνοασφάλεια • Έλλειψη συμβατότητας των ρυθμίσεων που προκάλεσε το κακόβουλο λογισμικό στο σύστημα ασφαλείας, έθεσε προληπτικά εκτός λειτουργίας τις βιομηχανικές διαδικασίες **Ανάκαμψη** • Το βιομηχανικό δίκτυο απομονώθηκε και η απειλή εξαλείφθηκε.
Υπηρεσίες Υγείας	• Προστασία της ανθρώπινης ζωής, • προστασία δεδομένων και συστημάτων	• Ταχεία επαναφορά των λειτουργιών. • Στήριξη στα θύματα σε περίπτωση διαρροής ευαίσθητων δεδομένων		**Vastaamo 2020** **Μετριασμός** • Η εταιρία εγκατέστησε λογισμικό προστασίας ενώ είχε ήδη υπάρξει διαρροή δεδομένων. • Η ενημέρωση των αρχών αλλά και των θιγόμενων ασθενών καθυστέρησε **Ανάκαμψη** • Η εταιρία αποκατέστησε από αντίγραφα αρχεία που είχαν κλαπεί • Πρόσφερε κάποιες παροχές στους πελάτες της • Τελικά δεν κατάφερε να ανακάμψει, λόγω νομικών συνεπειών και απώλειας της φήμης της	**HSE 2021** **Μετριασμός** • Ο οργανισμός αντέδρασε άμεσα και προσέφυγε στη συμβολή των αρχών αλλά και εξωτερικής βοήθειας • Εγκαταστάθηκε λογισμικό για να εντοπιστούν τα μολυσμένα συστήματα και στοιχεία για τους εισβολείς • Κρίσιμα συστήματα τέθηκαν εκτός λειτουργίας για να μην διαδοθεί η επίθεση • Κρίσιμες ιατρικές πράξεις πραγματοποιήθηκαν με την προσφυγή σε ιδιωτικούς φορείς. • Όπου ήταν δυνατό υπήρξαν χειροκίνητες διαδικασίες **Ανάκαμψη** • Η ανάκαμψη διήρκησε για μήνες αν και το κλειδί της αποκρυπτογράφησης είχε παραδοθεί • Η αναβάθμιση των συστημάτων δεν έγινε άμεσα, αλλά ακολούθησε τη διαθεσιμότητα των πόρων • Εκδόθηκε δικαστική εντολή για παρεμπόδιση μελλοντικής διαρροής κλεμμένων δεδομένων

Τομέας	Στόχοι Μετριασμού	Στόχοι ανάκαμψης		Περιπτώσεις	
Εκπαιδευτικά Ιδρύματα	• Προστασία δεδομένων και εκπαιδευτικής λειτουργίας	• Αποκατάσταση δεδομένων, λειτουργιών και φήμης		**Πανεπιστήμιο του Σαν Φρανσίσκο 2020** **Μετριασμός** • Τα συστήματα της Ιατρικής Σχολής τέθηκαν σε καραντίνα για να μην εξαπλωθεί η επίθεση. • Ζητήθηκε εξωτερική συνδρομή **Ανάκαμψη** • Η ανάκαμψη βασίστηκε στην απόκτηση του κλειδιού της αποκρυπτογράφησης μέσω της πληρωμής λύτρων	
Ψηφιακή Τραπεζική	• Προστασία των συναλλαγών	• Ταχεία αντιμετώπιση του συμβάντος και ανάκτηση της εμπιστοσύνης των πελατών.		**Luzerner Kantonalbank** **2025-2026** **Μετριασμός** • Ο μετριασμός βασίστηκε στην ενημέρωση των χρηστών και στο μπλοκάρισμα των πλαστογραφημένων ιστοτόπων	

Πίνακας 27. Μετριασμός και Ανάκαμψη ανά περίπτωση

Βασιζόμενοι στη σύνοψη, αλλά και στην αναλυτική παρουσίαση, μπορούμε να σημειώσουμε τα ακόλουθα:

- Ο ανθρώπινος παράγοντας σε ό,τι αφορά την απόκριση στην κοινωνική μηχανική, τις εσωτερικές απειλές αλλά και την απόδοση σε περίοδο κρίσεων είναι μια σημαντική παράμετρος της κυβερνοασφάλειας. (Περιστατικά: Ατλάντα, Shopify, HSE, LUKB, Πανεπιστήμιο του Σαν Φρανσίσκο)
- Τα παρωχημένα συστήματα αυξάνουν τον κίνδυνο. Επιπλέον σε κάποιες περιπτώσεις η ψηφιοποίηση και η αξιοποίηση του διαδικτύου αναπτύχθηκε χωρίς να λαμβάνεται επαρκώς υπόψιν, η ανάγκη της προστασίας των δεδομένων και των λειτουργιών από κυβερνοεπιθέσεις. Θα πρέπει πάντα να συνυπολογίζεται το γεγονός ότι αν και η τεχνολογία είναι ένα εξαιρετικό εργαλείο για τη βελτίωση της αποτελεσματικότητας των λειτουργιών, από την άλλη πλευρά αξιοποιείται και από τους φορείς απειλών και συνακόλουθα θα πρέπει οι μηχανισμοί άμυνας να βρίσκονται στο κατάλληλο επίπεδο και να εξελίσσονται διαρκώς. (Περιστατικά: Vastaamo, HSE)
- Η κυβερνοασφάλεια έχει κόστος, τόσο προληπτικό όσο και κόστος αποκατάστασης. Η προληπτική επένδυση στην αντιμετώπιση ενός απροσδιόριστου κινδύνου μπορεί να δείχνει λιγότερο επιτακτική από την κάλυψη ορατών και πιο «χειροπιαστών» αναγκών, όπως π.χ. αγορά νοσοκομειακού εξοπλισμού ή από έργα ενός δήμου με ορατό αντίκτυπο στην βελτίωση της ζωής των δημοτών. Ωστόσο θα πρέπει να συνεκτιμάται ότι οι κυβερνοεπιθέσεις έχουν συχνά, σοβαρό αντίκτυπο κι η ανάκαμψη από αυτές αποδεικνύεται εξαιρετικά δαπανηρή εάν ο οργανισμός δεν έχει αναπτύξει προληπτικά μέτρα, όπως η επιμελής διατήρηση εφεδρικών αντιγράφων και η εκπαίδευση του προσωπικού. (Περιστατικά: Ατλάντα, Colonial pipeline, Dyn κ.λπ.)
- Το διαδίκτυο είναι ένα κατακερματισμένο οικοσύστημα όπου πολλοί δρώντες λειτουργούν με εμπορικά κριτήρια και απαιτείται η παρέμβαση των ρυθμιστικών αρχών για να ξεπεραστούν (Dyn). Επιπλέον, σε κάποιες περιπτώσεις όπως η πλαστογράφηση ιστοσελίδων τραπεζών, είναι αναγκαία η εμπλοκή των αρχών, τόσο για την ενημέρωση των χρηστών για κακόβουλες ενέργειες όσο και για την επιβολή υποχρέωσης των τραπεζών να βελτιώνουν τον τρόπο πρόσβασης στα συστήματά τους και να εκπαιδεύουν τους πελάτες τους με δικές τους ενέργειες.
- Η εργασία με αποσύνδεση από το διαδίκτυο και η επιστροφή σε χειροκίνητες διαδικασίες σε περιόδους κρίσεων, φαίνεται να είναι μία δόκιμη προσέγγιση για τη διατήρηση της επιχειρησιακής συνέχειας, συνακόλουθα θα ήταν σκόπιμο να αποτελεί μέρος της εκπαίδευσης του ανθρώπινου δυναμικού. Η επιτυχία της κυβερνοασφάλειας προϋποθέτει την επάρκεια του

τεχνικού προσωπικού, αλλά και την εκπαίδευση του μη τεχνικού προσωπικού έτσι ώστε να μην πέφτουν θύματα επιθέσεων κοινωνικής μηχανικής, να χρησιμοποιούν βέλτιστες πρακτικές και να έχουν τη δυνατότητα να εφαρμόζουν εναλλακτικούς τρόπους λειτουργίας σε κρίσιμες φάσεις. (Περιστατικά: Ατλάντα, HSE)

4.7.2 Κοινά μοτίβα επιθέσεων

Με βάση τα περιστατικά που παρουσιάστηκαν προηγουμένως, διαπιστώνεται η ύπαρξη κοινών μοτίβων στις επιθέσεις. Ο Πίνακας 28 συνοψίζει τα μοτίβα αυτά.

Κοινά μοτίβα επιθέσεων
1. Ξεκινούν από την εκμετάλλευση μιας αδυναμίας ανθρώπινης, τεχνικής ή οργανωσιακής
2. Συνήθως λαμβάνουν χώρα σε στάδια
3. Έχουν προκαθορισμένους στόχους (άμεση απόσπαση χρημάτων, κλοπή δεδομένων, σαμποτάζ)
4. Η προετοιμασία των οργανισμών και ο χρόνος απόκρισης επηρεάζει τις συνέπειες

Πίνακας 28. Κοινά Μοτίβα Επιθέσεων

4.7.3 Συνέπειες κυβερνοεπιθέσεων σε επίπεδο στόχου βάση των προηγούμενων περιπτώσεων

Λόγω των επιθέσεων υπάρχουν σημαντικές επιπτώσεις τόσο στα άμεσα θύματα όσο και στο σύνολο της εφοδιαστικής αλυσίδας που τα περιλαμβάνει. Ο Πίνακας 29 συνοψίζει τις επιπτώσεις αυτές ανά κατηγορία στόχου.

Τομέας	Λειτουργικές Συνέπειες	Οικονομικές Συνέπειες	Κοινωνικές Συνέπειες	Ασφάλεια
Δημόσια Διοίκηση	Διαθεσιμότητα συστημάτων και δεδομένων	Κόστος από την ελλιπή είσπραξη εσόδων/ κόστη μετριασμού και ανάκαμψης	Απώλεια εμπιστοσύνης των πολιτών	Κίνδυνοι από την παραβίαση ή απώλεια δεδομένων
Πλατφόρμες Ηλεκτρονικού Εμπορίου	Διαθεσιμότητα συστημάτων	Κόστος από την δυσλειτουργία του εμπορίου / κόστη μετριασμού και ανάκαμψης	Απώλεια εμπιστοσύνης των πελατών	Κίνδυνοι από την υποκλοπή προσωπικών ή οικονομικών δεδομένων
Βιομηχανικά Συστήματα και Υποδομές	Διαθεσιμότητα συστημάτων	Κόστος από την απώλεια παραγωγής και την απορρύθμιση της αγοράς / κόστη μετριασμού και ανάκαμψης	Κοινωνική αναταραχή από την επίδραση στην εφοδιαστική αλυσίδα	Φυσικοί κίνδυνοι, προβλήματα εθνικής ασφάλειας
Υπηρεσίες Υγείας	Διαθεσιμότητα συστημάτων και δεδομένων	Απώλεια εσόδων/ Κόστη μετριασμού και ανάκαμψης	Κοινωνική αναταραχή	Φυσικός κίνδυνος για τις ζωές των ασθενών, κίνδυνοι από την απώλεια εμπιστευτικών δεδομένων
Εκπαιδευτικά Ιδρύματα	Διαθεσιμότητα συστημάτων και δεδομένων.	Κλοπή ή καθυστέρηση ερευνητικού έργου / Κόστη μετριασμού και ανάκαμψης	Απώλεια φήμης	Κίνδυνοι από την απώλεια προσωπικών και ερευνητικών δεδομένων με άγνωστη χρήση
Ψηφιακή Τραπεζική (πλαστογράφηση ιστοσελίδων και phishing)		Απώλεια περιουσίας	Απώλεια εμπιστοσύνης	Κίνδυνοι από την απώλεια εμπιστευτικών πληροφοριών

Πίνακας 29. Συνέπειες κυβερνοεπιθέσεων σε επίπεδο στόχου

Η πλήρης πρόληψη μιας κυβερνοεπίθεσης δεν είναι εφικτή ακόμη και σε τομείς που θεωρούνται ψηφιακά ώριμοι, όπως οι ηλεκτρονικές πλατφόρμες και η ψηφιακή τραπεζική. Επιπλέον σε κάθε τομέα οι συνέπειες διαφέρουν και έχουν ξεχωριστό προφίλ αντίκτυπου. Η διαμόρφωση στρατηγικής είναι ζωτικής σημασίας να ξεκινά από τον προσδιορισμό των κρίσιμων αγαθών που πρέπει να προστατευθούν, και αντίστοιχα των συνεπειών που πρέπει κατά προτεραιότητα να αποφευχθούν. Στο πλαίσιο αυτό, η επένδυση στην ανθεκτικότητα και την προστασία κρίσιμων υποδομών και δεδομένων θα πρέπει να εξειδικεύεται και να συνδέεται με την αποστολή του κάθε οργανισμού.

Η προσαρμογή της στρατηγικής μετριασμού και ανάκαμψης αφορά πέρα από τον καθορισμό των κρίσιμων περιουσιακών στοιχείων και διαδικασιών, και τον αποδεκτό χρόνο διακοπής των λειτουργιών που θα ορίσει η διοίκηση. Επίσης, η χαρτογράφηση των πιθανών απειλών σε συνδυασμό με τη βαρύτητα των επιπτώσεων τους και η συμμόρφωση με νομικές απαιτήσεις διαφοροποιούνται από το είδος του οργανισμού.

5 Συμπεράσματα

Οι επιχειρήσεις και οι οργανισμοί, ανεξαρτήτως πόρων, δεν μπορούν να αντιμετωπίσουν τις απειλές με αντιδράσεις που διαμορφώνονται κατ' απαίτηση όταν έχει υπάρξει επίθεση ή παραβίαση, αλλά μόνο στην βάση στρατηγικών μετριασμού και ανάκαμψης που θα βασίζονται στην εκτίμηση κινδύνου, στην ρεαλιστική στόχευση, στην ουσιαστική εφαρμογή των πλαισίων κυβερνοασφάλειας, στη συνεργασία ανάμεσα σε οργανισμούς και κράτη, στην αξιοποίηση των μέτρων προστασίας και των νέων τεχνολογιών καθώς και την ευαισθητοποίηση και εκπαίδευση του ανθρώπινου δυναμικού.

Η ύπαρξη κοινών μοτίβων επιτρέπει την αντιμετώπιση των απειλών στα πλαίσια της εφαρμογής των αναγνωρισμένων πλαισίων κυβερνοασφάλειας και ανάλυσης των κυβερνοεπιθέσεων. Ωστόσο αποφάσεις όπως η ιεράρχηση της σημαντικότητας των αγαθών, η εφαρμογή μέτρων προστασίας και οι πόροι που μπορούν να διατεθούν προς αυτή την κατεύθυνση, είναι στρατηγικές επιλογές των οργανισμών που αφορούν την αποστολή, την επιβίωση τους, τις δεσμεύσεις τους απέναντι στον νόμο, αλλά και υποχρεώσεις που αφορούν την ευημερία των ανθρώπων και την ασφάλεια της κοινωνίας.

6 Βιβλιογραφία – Πηγές

Abomhara, M., Department of Information and Communication Technology, University of Agder, Norway, K�ien, G. M., & Department of Information and Communication Technology, University of Agder, Norway. (2015). Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks. *Journal of Cyber Security and Mobility*, *4*(1), 65–88. https://doi.org/10.13052/jcsm2245-1439.414

Abraham, C., Bélanger, F., & Daultrey, S. (2025). Promoting research on cyber threat intelligence sharing in ecosystems. *Journal of Cybersecurity*, *11*(1), tyaf016. https://doi.org/10.1093/cybsec/tyaf016

Abrardi, L., Comino, S., & Grassini, S. (2025). The economics of cyber risk: A survey of the literature. *Journal of Industrial and Business Economics*. https://doi.org/10.1007/s40812-025-00370-3

Abshari, D., & Sridhar, M. (2025). *Cyber-Physical Systems Security: A Comprehensive Review of Anomaly Detection Techniques* (Version 2). arXiv. https://doi.org/10.48550/ARXIV.2502.13256

Adnan, M., Kalra, S., Cresswell, J. C., Taylor, G. W., & Tizhoosh, H. R. (2022). Federated learning and differential privacy for medical image analysis. *Scientific Reports*, *12*(1), 1953. https://doi.org/10.1038/s41598-022-05539-7

Ahmed, Y., Asyhari, A. T., & Arafatur Rahman, M. (2021). A Cyber Kill Chain Approach for Detecting Advanced Persistent Threats. *Computers, Materials & Continua*, *67*(2), 2497–2513. https://doi.org/10.32604/cmc.2021.014223

Alnajim, A. M., Habib, S., Islam, M., AlRawashdeh, H. S., & Wasim, M. (2023). Exploring Cybersecurity Education and Training Techniques: A Comprehensive Review of Traditional, Virtual Reality, and Augmented Reality Approaches. *Symmetry*, *15*(12), 2175. https://doi.org/10.3390/sym15122175

Al-Qarni, E. A. (2023). Cybersecurity in Healthcare: A Review of Recent Attacks and Mitigation Strategies. *International Journal of Advanced Computer Science and Applications*, *14*(5). https://doi.org/10.14569/IJACSA.2023.0140513

Al-Sada, B., Sadighian, A., & Oligeri, G. (2025). MITRE ATT&CK: State of the Art and Way Forward. *ACM Computing Surveys*, *57*(1), 1–37. https://doi.org/10.1145/3687300

Alshamrani, A., Myneni, S., Chowdhary, A., & Huang, D. (2019). A Survey on Advanced Persistent Threats: Techniques, Solutions, Challenges, and Research Opportunities. *IEEE Communications Surveys & Tutorials*, *21*(2), 1851–1877. https://doi.org/10.1109/COMST.2019.2891891

Altulaihan, E. A., Alismail, A., & Frikha, M. (2023). A Survey on Web Application Penetration Testing. *Electronics*, *12*(5), 1229. https://doi.org/10.3390/electronics12051229

Alzaabi, F. R., & Mehmood, A. (2024). A Review of Recent Advances, Challenges, and Opportunities in Malicious Insider Threat Detection Using Machine Learning Methods. *IEEE Access*, *12*, 30907–30927. https://doi.org/10.1109/ACCESS.2024.3369906

Anderson, R., Barton, C., Böhme, R., Clayton, R., Van Eeten, M. J. G., Levi, M., Moore, T., & Savage, S. (2013). Measuring the Cost of Cybercrime. In R. Böhme (Ed.), *The Economics of Information Security and Privacy* (pp. 265–300). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-39498-0_12

Antonakakis, M., April, T., Bailey, M., Bernhard, M., Bursztein, E., Cochran, J., Durumeric, Z., Halderman, J. A., Invernizzi, L., Kallitsis, M., Kumar, D., Lever, C., Ma, Z., Mason, J., Menscher, D., Seaman, C., Sullivan, N., Thomas, K., & Zhou, Y. (2017). *Understanding the Mirai Botnet*. 1093–1110. https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/antonakakis

Ardhi, D. C., Sari, D. P., & Yankson, B. (2025). Cyberattacks in government organizations: A systematic literature review of attack types and mitigation strategies. *Conference on Digital Government Research, 1*. https://doi.org/10.59490/dgo.2025.1021

Ashoor, A. S., & Gore, S. (2011). Difference between Intrusion Detection System (IDS) and Intrusion Prevention System (IPS). In D. C. Wyld, M. Wozniak, N. Chaki, N. Meghanathan, & D. Nagamalai (Eds.), *Advances in Network Security and Applications* (Vol. 196, pp. 497–501). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-22540-6_48

Aven, T. (2013). On the Meaning and Use of the Risk Appetite Concept. *Risk Analysis*, *33*(3), 462–468. https://doi.org/10.1111/j.1539-6924.2012.01887.x

AWS. (2026a). *Encryption best practices and features for AWS services*. AWS. https://docs.aws.amazon.com/prescriptive-guidance/latest/encryption-best-practices/welcome.html

AWS. (2026b). *Encryption policy—AWS Prescriptive Guidanc*. AWS. https://docs.aws.amazon.com/prescriptive-guidance/latest/strategy-data-at-rest-encryption/policy.html

AWS. (2026c). *General encryption best practices—AWS Prescriptive Guidance*. AWS. https://docs.aws.amazon.com/pdfs/prescriptive-guidance/latest/encryption-best-practices/encryption-best-practices.pdf

Azmi, N. N., Abdul Rahim, F., Hassan, N. H., & Ahmad, N. A. (2025). SWOT ANALYSIS OF CYBERSECURITY VULNERABILITIES AND STRATEGIES IN RENEWABLE ENERGY SYSTEM: A CASE STUDY ON EUROPEAN WIND POWER SYSTEM. *Malaysian Journal of Sustainable Environment*, *12*(2), 103–126. https://doi.org/10.24191/myse.v12i2.7072

Badirova, A., Dabbaghi, S., Moghaddam, F. F., Wieder, P., & Yahyapour, R. (2023). A Survey on Identity and Access Management for Cross-Domain Dynamic Users: Issues, Solutions, and Challenges. *IEEE Access*, *11*, 61660–61679. https://doi.org/10.1109/ACCESS.2023.3279492

Balzano, M., & Marzi, G. (2025). At the Cybersecurity Frontier: Key Strategies and Persistent Challenges for Business Leaders. *Strategic Change*, *34*(2), 181–192. https://doi.org/10.1002/jsc.2622

Banks, J., & Bhowmik, P. K. (2025). *Internship Presentation: Integrating Safety and Cybersecurity: Security-by-Design with SOWT Analysis for Reactor Testing* (INL/MIS-25-86970). Idaho National Laboratory (INL), Idaho Falls, ID (United States). https://www.osti.gov/biblio/2587221

Barkat Ullah, A., Ma, W., Ahmed, M., Rashid, B., Saeed, M. A., Arshad, O., & Raghav, U. (2025). A comprehensive review of cyber security and current practices in global mining critical infrastructure. *Journal of Cyber Security Technology*, *10*(1), 1–27. https://doi.org/10.1080/23742917.2025.2475563

BBC. (2020, September 30). *Kylie Jenner's make-up firm warns of Shopify data breach*. https://www.bbc.com/news/technology-54354526

Bederna, Z., Rajnai, Z., & Szadeczky, T. (2021). Business Strategy analysis of Cybersecurity Incidents. *Land Forces Academy Review*, *26*(2), 139–148. https://doi.org/10.2478/raft-2021-0020

Beerman, J., Berent, D., Falter, Z., & Bhunia, S. (2023). A Review of Colonial Pipeline Ransomware Attack. *2023 IEEE/ACM 23rd International Symposium on Cluster, Cloud and Internet Computing Workshops (CCGridW)*, 8–15. https://doi.org/10.1109/CCGridW59191.2023.00017

Bhatia, N. L., Shukla, V. K., Punhani, R., & Dubey, S. K. (2021). Growing Aspects of Cyber Security in E-Commerce. *2021 International Conference on Communication Information and Computing Technology (ICCICT)*, 1–6. https://doi.org/10.1109/ICCICT50803.2021.9510152

Björck, F., Henkel, M., Stirna, J., & Zdravkovic, J. (2015). Cyber Resilience – Fundamentals for a Definition. In A. Rocha, A. M. Correia, S. Costanzo, & L. P. Reis (Eds.), *New Contributions*

in Information Systems and Technologies (Vol. 353, pp. 311–316). Springer International Publishing. https://doi.org/10.1007/978-3-319-16486-1_31

Blancaflor, E. B., Duldulao, J. O., Espeño, J. V. E., Patag, G. S. M., Theresa Menor, Ma., & Intal, G. L. (2025). Advanced Phishing Techniques: Analyzing Adversary-in-the-Middle and Browser-in-the-Browser Attacks in Modern Cybersecurity. *Cybernetics and Information Technologies*, *25*(1), 55–77. https://doi.org/10.2478/cait-2025-0004

Boakye, D., Sarpong, D., Meissner, D., & Ofosu, G. (2024). How TalkTalk did the walk-walk: Strategic reputational repair in a cyber-attack. *Information Technology & People*, *37*(4), 1642–1673. https://doi.org/10.1108/ITP-08-2022-0589

Bokan, B., & Santos, J. (2021). Managing Cybersecurity Risk Using Threat Based Methodology for Evaluation of Cybersecurity Architectures. *2021 Systems and Information Engineering Design Symposium (SIEDS)*, 1–6. https://doi.org/10.1109/SIEDS52267.2021.9483736

Bonnet, O. (2022, October). *(PDF) ENCRYPTION IN TRANSIT, AT REST, AND IN USE (CONFIDENTIAL COMPUTING) ACROSS CLOUD PROVIDERS*. ResearchGate. https://www.researchgate.net/publication/396896116_ENCRYPTION_IN_TRANSIT_AT_REST_AND_IN_USE_CONFIDENTIAL_COMPUTING_ACROSS_CLOUD_PROVIDERS

BSI. (2023). *Die Lage der IT-Sicherheit in Deutschland 2023*. Bundesamt für Sicherheit in der Informationstechnik. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2023.html?nn=132646

Canadian Centre for Cyber Security. (2022). *An introduction to the cyber threat environment—Canadian Centre for Cyber Security*. https://www.cyber.gc.ca/en/guidance/introduction-cyber-threat-environment

Carvalho, C., & Marques, E. (2019). Adapting ISO 27001 to a Public Institution. *2019 14th Iberian Conference on Information Systems and Technologies (CISTI)*, 1–6. https://doi.org/10.23919/CISTI.2019.8760870

Cascais Brás, J., Pereira, R. F., Moro, S., Bianchi, I. S., & Ribeiro, R. (2023). Understanding How Intelligent Process Automation Impacts Business Continuity: Mapping IEEE/2755:2020 and ISO/22301:2019. *IEEE Access*, *11*, 134239–134258. https://doi.org/10.1109/ACCESS.2023.3337159

Chapman, J. (2019). *How safe is your data? Cyber-security in higher education*. https://www.hepi.ac.uk/wp-content/uploads/2019/03/Policy-Note-12-Paper-April-2019-How-safe-is-your-data.pdf

Chauhan, A. A., & Singh, P. (2025). Examining the Role of Perceived Cyber Security and Privacy in Shaping E-Commerce Buying Behavior. *2025 International Conference on Digital Innovations for Sustainable Solutions (ICDISS)*, 1–6. https://doi.org/10.1109/ICDISS68238.2025.11320687

Chen, P., Desmet, L., & Huygens, C. (2014). A Study on Advanced Persistent Threats. In C. Salinesi, M. C. Norrie, & Ó. Pastor (Eds.), *Advanced Information Systems Engineering* (Vol. 7908, pp. 63–72). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-662-44885-4_5

Chng, S., Lu, H. Y., Kumar, A., & Yau, D. (2022). Hacker types, motivations and strategies: A comprehensive framework. *Computers in Human Behavior Reports*, *5*, 100167. https://doi.org/10.1016/j.chbr.2022.100167

Choi, J., Robinson, S., Ruddle, T., & Fister, A. (2025). Restoring Public Trust After a Data Breach Crisis: Reputational Response Strategies for Government, For-Profit, and Nonprofit Organizations. *Risk, Hazards & Crisis in Public Policy*, *16*(3), e70026. https://doi.org/10.1002/rhc3.70026

Cialdini, R. B. (2009). *Influence: Science and practice* (5. ed., internat. ed). Pearson Education [u.a.].

CISA. (2022a). *Implementing Phishing-Resistant MFA*. https://www.cisa.gov/sites/default/files/2023-01/fact-sheet-implementing-phishing-resistant-mfa-508c.pdf

CISA. (2022b). *Understanding and Responding to Distributed Denial of Service Attacks*. https://www.cisa.gov/sites/default/files/publications/understanding-and-responding-to-ddos-attacks_508c.pdf

City of Atlanta. (2018a). *Atlanta, GA : Ransomware Cyberattack Information*. https://web.archive.org/web/20180718205511/https://www.atlantaga.gov/government/ransomware-cyberattack-information

City of Atlanta. (2018b). *Mayor Keisha Lance Bottoms Provides Update on City of Atlanta Ransomware Cyberattack | Press Releases | Atlanta, GA*. https://www.atlantaga.gov/Home/Components/News/News/11524/672

Collier, B., & Clayton, R. (2025). Peer(ing) pressure: A cybersecurity intervention at global scale in the internet infrastructure. *Journal of Cybersecurity*, *11*(1), tyaf014. https://doi.org/10.1093/cybsec/tyaf014

Coulibaly, K. (2020). *An overview of Intrusion Detection and Prevention Systems* (Version 1). arXiv. https://doi.org/10.48550/ARXIV.2004.08967

Cristiano, F. (2021). Israel: Cyber defense and security as national trademarks of international legitimacy. In *ROUTLEDGE COMPANION TO GLOBAL CYBER-SECURITY STRATEGY* (pp. 409–417). https://doi.org/10.4324/9780429399718-34%3Furlappend=%3Futm_source=researchgate.net&utm_medium=article

Cureton, E. (2018, March 29). *Atlanta Cyber Attack Updates | Georgia Public Broadcasting*. http://gpbnews.org/post/atlanta-cyber-attack-updates

Cyber Florida. (2021). *Cybersecurity for Local Government Guide.indd*. https://flmanagers.com/wp-content/uploads/2021/01/Cybersecurity-for-Local-Government-Guide.pdf

Dalaq, D., Daya, K. F., Dalaq, A., Arefin, M. N., & Niazi, M. K. (2025). A Systematic Literature Review on Static Application Security Testing (SAST) Tools: Evaluation, Benchmarks, Challenges, and Future Directions. *Proceedings of the 2025 29th International Conference on Evaluation and Assessment in Software Engineering Companion*, 162–168. https://doi.org/10.1145/3727967.3756838

Data Protection Ombudsman. (2021). *Failure to ensure proper security of personal data processing and failure to notify a data breach*. Finlex. https://www.finlex.fi/en/authorities/data-protection-ombudsman/2021/1183

Dembani, R., Karvelas, I., Akbar, N. A., Rizou, S., Tegolo, D., & Fountas, S. (2025). Agricultural data privacy and federated learning: A review of challenges and opportunities. *Computers and Electronics in Agriculture*, *232*, 110048. https://doi.org/10.1016/j.compag.2025.110048

Department of Homeland Security & Cybersecurity and Infrastructure Security Agency. (2024). *Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements*. Federal Register. https://www.federalregister.gov/documents/2024/04/04/2024-06526/cyber-incident-reporting-for-critical-infrastructure-act-circia-reporting-requirements

Douglas, T. (2018, September 25). *What Can We Learn from Atlanta?* GovTech. https://www.govtech.com/security/What-Can-We-Learn-from-Atlanta.html

Dritsas, E., & Trigka, M. (2025). A Survey on Cybersecurity in IoT. *Future Internet*, *17*(1), 30. https://doi.org/10.3390/fi17010030

Duo, W., Zhou, M., & Abusorrah, A. (2022). A Survey of Cyber Attacks on Cyber Physical Systems: Recent Advances and Challenges. *IEEE/CAA Journal of Automatica Sinica*, *9*(5), 784–800. https://doi.org/10.1109/JAS.2022.105548

Dushnitsky, G., & Stroube, B. K. (2021). Low-code entrepreneurship: Shopify and the alternative path to growth. *Journal of Business Venturing Insights*, *16*, e00251. https://doi.org/10.1016/j.jbvi.2021.e00251

Dyn. (2016). *Dyn Analysis Summary Of Friday October 21 Attack | Dyn Blog*. https://perma.cc/YW5C-MDEV

Edwards, J., & Weaver, G. (2024). *The cybersecurity guide to governance, risk, and compliance*. John Wiley & Sons.

Engström, V., & Lagerström, R. (2022). Two decades of cyberattack simulations: A systematic literature review. *Computers & Security*, *116*, 102681. https://doi.org/10.1016/j.cose.2022.102681

ENISA. (2010). *Incident_Management_guide*. https://www.enisa.europa.eu/sites/default/files/publications/Incident_Management_guide.pdf

ENISA. (2020). *ENISA Threat Landscape 2020—Insider threat | ENISA*. https://www.enisa.europa.eu/publications/insider-threat

ENISA. (2023). *Cyber crisis communication guide*. Publications Office of the European Union. https://data.europa.eu/doi/10.2824/802357

ENISA. (2025, November 6). *ENISA Threat Landscape 2025 | ENISA*. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025

ENISA phishing, P. (2020). *ENISA Threat Landscape 2020—Phishing | ENISA*. https://www.enisa.europa.eu/publications/phishing

ESCO. (2025, January). *WG3 White Paper NIS2 FINAL VERSION*. https://ecs-org.eu/ecso-uploads/2025/01/ECSO-White-Paper-NIS2-Implementation.pdf

European Parliament & Council of the European Union. (2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance)*. Official Journal of the European Union. https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

European Parliament & Council of the European Union. (2019, July 6). *Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Text with EEA relevance)*. Official Journal of the European Union. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R0881

European Parliament & Council of the European Union. (2022, December 27). *Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (Text with EEA relevance)*. European Union. https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng

Europol. (2021). *Europol Spotlight—Cryptocurrencies—Tracing the evolution of criminal finances*. https://www.europol.europa.eu/cms/sites/default/files/documents/Europol%20Spotlight%20-%20Cryptocurrencies%20-%20Tracing%20the%20evolution%20of%20criminal%20finances.pdf

Europol. (2024). *Uncovering the ecosystem of intellectual property crime: A focus on enablers and impact*. Υπηρεσία Εκδόσεων της Ευρωπαϊκής Ένωσης. https://data.europa.eu/doi/10.2814/1947113

Europol. (2025). *Steal, deal and repeat: How cybercriminals trade and exploit your data – Internet Organised Crime Threat Assessment (IOCTA) 2025*. Europol. https://www.europol.europa.eu/publication-events/main-reports/steal-deal-and-repeat-how-cybercriminals-trade-and-exploit-your-data

Everett, C. (2016). Ransomware: To pay or not to pay? *Computer Fraud & Security*, *2016*(4), 8–12. https://doi.org/10.1016/S1361-3723(16)30036-7

Ewoh, P., & Vartiainen, T. (2024). Vulnerability to Cyberattacks and Sociotechnical Solutions for Health Care Systems: Systematic Review. *Journal of Medical Internet Research*, *26*, e46904. https://doi.org/10.2196/46904

Fahey, E. (2024). The evolution of EU–US cybersecurity law and policy: On drivers of convergence. *Journal of European Integration*, *46*(7), 1073–1088. https://doi.org/10.1080/07036337.2024.2411240

Federal Emergency Management Agency. (2019). *Business Process Analysisand Business Impact AnalysisUser Guide*. https://www.fema.gov/sites/default/files/2020-07/fema_BPA-BIA-Users-Guide_070119.pdf

FireEye. (2017). *Attackers Deploy New ICS Attack Framework "TRITON" and Cause Operational Disruption to Critical Infrastructure*. https://cyber-peace.org/wp-content/uploads/2017/12/triton.pdf

Frei, J. (with Cordey, Sean). (2020). *Israel's National Cybersecurity and Cyberdefense Posture: Policy and Organizations* (p. 24 p.) [Application/pdf]. ETH Zurich. https://doi.org/10.3929/ETHZ-B-000438397

Furumoto, K., Morikawa, T., Kolehmainen, A., Silverajan, B., Takahashi, T., & Inoue, D. (2026). A Comprehensive Survey of Threat Intelligence Research: A Measurement-Based Study. *ACM Computing Surveys*, *58*(6), 1–35. https://doi.org/10.1145/3772280

Gandhi, R., Sharma, A., Mahoney, W., Sousan, W., Zhu, Q., & Laplante, P. (2011). Dimensions of Cyber-Attacks: Cultural, Social, Economic, and Political. *IEEE Technology and Society Magazine*, *30*(1), 28–38. https://doi.org/10.1109/MTS.2011.940293

Geiger, M., Bauer, J., Masuch, M., & Franke, J. (2020). An Analysis of Black Energy 3, Crashoverride, and Trisis, Three Malware Approaches Targeting Operational Technology Systems. *2020 25th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA)*, 1537–1543. https://doi.org/10.1109/ETFA46521.2020.9212128

Geller, E., & Romm, T. (2016, October 21). *WikiLeaks supporters claim credit for massive U.S. cyberattack, but researchers skeptical*. POLITICO. https://www.politico.com/story/2016/10/websites-down-possible-cyber-attack-230145

Georgiadou, A., Mouzakitis, S., & Askounis, D. (2021). Assessing MITRE ATT&CK Risk Using a Cyber-Security Culture Framework. *Sensors*, *21*(9), 3267. https://doi.org/10.3390/s21093267

Ghanbari, H., & Koskinen, K. (2024). When data breach hits a psychotherapy clinic: The Vastaamo case. *Journal of Information Technology Teaching Cases*, 20438869241258235. https://doi.org/10.1177/20438869241258235

Gjesvik, L., & Schia, N. N. (2017). *China's cyber sovereignty*. https://www.jstor.org/stable/82226b2b-b1f2-341a-bfa2-59a6208bf3e0?seq=1

Goldman, H. G. (2010). *Building Secure, Resilient Architectures for Cyber Mission Assurance*. https://apps.dtic.mil/sti/html/trecms/AD1108588/

Government of South Australia, S. (2025, October 23). *Cyber security > Resources* [Text]. Security SA. (South Australia). Security SA. https://www.security.sa.gov.au/cyber-security/resources

Greitzer, F. L., & Frincke, D. A. (2010). Combining Traditional Cyber Security Audit Data with Psychosocial Data: Towards Predictive Modeling for Insider Threat Mitigation. In C. W. Probst, J. Hunker, D. Gollmann, & M. Bishop (Eds.), *Insider Threats in Cyber Security* (Vol. 49, pp. 85–113). Springer US. https://doi.org/10.1007/978-1-4419-7133-3_5

Habib, A. K. M. A., Hasan, M. K., Hassan, R., Islam, S., & Abbas, H. S. (2025). False data injection attack dataset for classification, identification, and detection for IIoT in Industry 5.0. *Data in Brief*, *61*, 111692. https://doi.org/10.1016/j.dib.2025.111692

Haq, M. Y. M., Jonker, M., Van Rijswijk-Deij, R., Claffy, K., Nieuwenhuis, L. J. M., & Abhishta, A. (2022). No Time for Downtime: Understanding Post-Attack Behaviors by Customers of Managed DNS Providers. *2022 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, 322–331. https://doi.org/10.1109/EuroSPW55150.2022.00039

HM Government. (2008). *How prepared are you? Business Continuity Management Toolkit*. https://assets.publishing.service.gov.uk/media/5a7b283de5274a34770e9d01/Business_Continuity_Managment_Toolkit.pdf

Homoliak, I., Toffalini, F., Guarnizo, J., Elovici, Y., & Ochoa, M. (2018). Insight Into Insiders and IT: A Survey of Insider Threat Taxonomies, Analysis, Modeling, and Countermeasures. *ACM Computing Surveys*, *52*(2), 1–40. https://doi.org/10.1145/3303771

Hossain, S. T., Yigitcanlar, T., Nguyen, K., & Xu, Y. (2024). Local Government Cybersecurity Landscape: A Systematic Review and Conceptual Framework. *Applied Sciences*, *14*(13), 5501. https://doi.org/10.3390/app14135501

Hou, T., & Wang, V. (2020). Industrial espionage – A systematic literature review (SLR). *Computers & Security*, *98*, 102019. https://doi.org/10.1016/j.cose.2020.102019

Hubbard, D. W., & Seiersen, R. (2016). *How to Measure Anything in Cybersecurity Risk* (1st ed.). Wiley. https://doi.org/10.1002/9781119162315

Hunker, J., & Probst, C. (2011). Insiders and Insider Threats—An Overview of Definitions and Mitigation Techniques. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, *2*(1), 4–27. https://doi.org/10.22667/JOWUA.2011.03.31.004

icom. (2025, October 2). *Data Encryption*. ICOM Policies. https://policies.icom.edu/hc/en-us/articles/35356707688471-Data-Encryption

Inayat, U., Farzan, M., Mahmood, S., Zia, M. F., Hussain, S., & Pallonetto, F. (2024). Insider threat mitigation: Systematic literature review. *Ain Shams Engineering Journal*, *15*(12), 103068. https://doi.org/10.1016/j.asej.2024.103068

INCD. (2025). *Israel_national_cybersecurity_strategy_feb2025*. https://www.gov.il/BlobFolder/news/cyber_strategy_2025/he/israel_national_cybersecurity_strategy_feb2025.pdf

Jiang, Y., Meng, Q., Shang, F., Oo, N., Minh, L. T. H., Lim, H. W., & Sikdar, B. (2025). *MITRE ATT&CK Applications in Cybersecurity and The Way Forward* (Version 1). arXiv. https://doi.org/10.48550/ARXIV.2502.10825

Joseph C. Stepina. (2022, April 19). *Shopify And Leger Facing Second Class Action Over 2020 Data Breach*. https://hallboothsmith.com/shopify-and-leger-facing-second-class-action-over-2020-data-breach/

Kaspersky. (2017). *Nigerian phishing: Industrial companies under attack*. Kaspersky. https://ics-cert.kaspersky.com/publications/reports/2017/06/15/nigerian-phishing-industrial-companies-under-attack/

Kaspersky. (2020). *What is Social Engineering?* Kaspersky. https://www.kaspersky.com/resource-center/definitions/what-is-social-engineering

Kaspersky. (2024). *The costs of cyberattacks: How one breach can sink a business*. Kaspersky. https://me-en.kaspersky.com/about/press-releases/the-costs-of-cyberattacks-how-one-breach-can-sink-a-business

Kavak, H., Padilla, J. J., Vernon-Bido, D., Diallo, S. Y., Gore, R., & Shetty, S. (2021). Simulation for cybersecurity: State of the art and future directions. *Journal of Cybersecurity*, *7*(1), tyab005. https://doi.org/10.1093/cybsec/tyab005

Kayan, H., Nunes, M., Rana, O., Burnap, P., & Perera, C. (2022). Cybersecurity of Industrial Cyber-Physical Systems: A Review. *ACM Computing Surveys*, *54*(11s), 1–35. https://doi.org/10.1145/3510410

Keogh, R. J., Harvey, H., Brady, C., Hassett, E., Costelloe, S. J., O'Sullivan, M. J., Twomey, M., O'Leary, M. J., Cahill, M. R., O'Riordan, A., Joyce, C. M., Moloney, G., Flavin, A., M Bambury, R., Murray, D., Bennett, K., Mullooly, M., & O'Reilly, S. (2024). Dealing with digital paralysis: Surviving a cyberattack in a National Cancer center. *Journal of Cancer Policy*, *39*, 100466. https://doi.org/10.1016/j.jcpo.2023.100466

Khan, M. S., Ferens, K., & Siddiqui, S. A. waheed. (2017). A Cognitive and Concurrent Cyber Kill Chain Model | Request PDF. In *ResearchGate*. https://doi.org/10.1007/978-3-319-58424-9_34

Kim, B.-J., & Lee, J. (2025). The impact of corporate social responsibility on cybersecurity behavior: The crucial role of organizationally-prescribed perfectionism. *Humanities and Social Sciences Communications*, *12*(1), 172. https://doi.org/10.1057/s41599-025-04511-w

Knight, R., & Nurse, J. R. C. (2020). A framework for effective corporate communication after cyber security incidents. *Computers & Security*, *99*, 102036. https://doi.org/10.1016/j.cose.2020.102036

Koutsouris, N., Vassilakis, C., & Kolokotronis, N. (2021). Cyber-Security Training Evaluation Metrics. *2021 IEEE International Conference on Cyber Security and Resilience (CSR)*, 192–197. https://doi.org/10.1109/CSR51186.2021.9527946

Kozłowski, K. (2025). *(PDF) Corporate espionage from an Information Security Management Perspective: A Case Study Analysis*. ResearchGate. https://www.researchgate.net/publication/390532926_Corporate_espionage_from_an_Information_Security_Management_Perspective_A_Case_Study_Analysis

Kshetri, N. (2006). The simple economics of cybercrimes. *IEEE Security & Privacy Magazine*, *4*(1), 33–39. https://doi.org/10.1109/MSP.2006.27

Lallie, H. S., Thompson, A., Titis, E., & Stephens, P. (2025). Analysing Cyber Attacks and Cyber Security Vulnerabilities in the University Sector. *Computers*, *14*(2), 49. https://doi.org/10.3390/computers14020049

Ledger. (2025, October 12). *E-commerce and Marketing data breach—FAQ*. https://support.ledger.com/de/article/E-commerce-and-Marketing-data-breach-FAQ

Leonardo Pizzuti. (2016). *Behind DYN attack: Mirai malware – European Affairs Magazine*. https://www.europeanaffairs.it/blog/2016/11/12/behind-dyn-attack-mirai-malware/

Liu, S., & Kuhn, R. (2010). Data Loss Prevention. *IT Professional*, *12*(2), 10–13. https://doi.org/10.1109/MITP.2010.52

Liu, X., Ahmad, S. F., Anser, M. K., Ke, J., Irshad, M., Ul-Haq, J., & Abbas, S. (2022). Cyber security threats: A never-ending challenge for e-commerce. *Frontiers in Psychology*, *13*, 927398. https://doi.org/10.3389/fpsyg.2022.927398

Lockheed_Martin. (2015). *Gaining_the_Advantage_Cyber_Kill_Chain*. https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/Gaining_the_Advantage_Cyber_Kill_Chain.pdf

Longtchi, T. T., Rodriguez, R. M., Al-Shawaf, L., Atyabi, A., & Xu, S. (2024). Internet-Based Social Engineering Psychology, Attacks, and Defenses: A Survey. *Proceedings of the IEEE*, *112*(3), 210–246. https://doi.org/10.1109/JPROC.2024.3379855

Looi, J. C., Allison, S., Bastiampillai, T., Maguire, P. A., Kisely, S., Reutens, S., & Looi, R. C. (2025). Cybersecurity lessons from the Vastaamo psychotherapy data breach for psychiatrists and other mental healthcare providers. *Australasian Psychiatry*, *33*(1), 106–110. https://doi.org/10.1177/10398562241291340

Malatji, M. (2023). Management of enterprise cyber security: A review of ISO/IEC 27001:2022. *2023 International Conference On Cyber Management And Engineering (CyMaEn)*, 117–122. https://doi.org/10.1109/CyMaEn57228.2023.10051114

Maragkou, S., Rappel, L., Dettmer, H., Sauter, T., & Jantsch, A. (2025). The Pains of Hardware Security: An Assessment Model of Real-World Hardware Security Attacks. *IEEE Open Journal of the Industrial Electronics Society*, *6*, 603–617. https://doi.org/10.1109/OJIES.2025.3561675

Mashinchi, M. I., Acton, T., & Datta, P. M. (2024). When healthcare becomes sick: Recovering from ransomware. *Journal of Information Technology Teaching Cases*, 20438869241279443. https://doi.org/10.1177/20438869241279443

Mavroeidis, V., Hohimer, R., Casey, T., & Jesang, A. (2021). Threat Actor Type Inference and Characterization within Cyber Threat Intelligence. *2021 13th International Conference on Cyber Conflict (CyCon)*, 327–352. https://doi.org/10.23919/CyCon51939.2021.9468305

Maynard, P., McLaughlin, K., & Sezer, S. (2020). Decomposition and sequential-AND analysis of known cyber-attacks on critical infrastructure control systems. *Journal of Cybersecurity*, *6*(1), tyaa020. https://doi.org/10.1093/cybsec/tyaa020

McGuire, S. (2018, June 5). *Atlanta Cyberattack Affected Police Evidence, Chief Says | Georgia Public Broadcasting*. http://gpbnews.org/post/atlanta-cyberattack-affected-police-evidence-chief-says

Mehta, D., Lu, H., Paradis, O. P., M. S., M. A., Rahman, M. T., Iskander, Y., Chawla, P., Woodard, D. L., Tehranipoor, M., & Asadizanjani, N. (2020). The Big Hack Explained: Detection and Prevention of PCB Supply Chain Implants. *ACM Journal on Emerging Technologies in Computing Systems*, *16*(4), 1–25. https://doi.org/10.1145/3401980

Meier, R. (2026, February 18). *Betrüger verschicken im Namen der Luzerner Kantonalbank gefälschte QR-Codes*. www.bote.ch. https://www.bote.ch/nachrichten/zentralschweiz/luzerner-kantonalbank-warnt-vor-gefaelschten-qr-codes-art-1689468

Mekdad, Y., Bernieri, G., Conti, M., & Fergougui, A. E. (2021). A threat model method for ICS malware: The TRISIS case. *Proceedings of the 18th ACM International Conference on Computing Frontiers*, 221–228. https://doi.org/10.1145/3457388.3458868

Meurs, T., Cartwright, E., Cartwright, A., Junger, M., & Abhishta, A. (2024). Deception in double extortion ransomware attacks: An analysis of profitability and credibility. *Computers & Security*, *138*, 103670. https://doi.org/10.1016/j.cose.2023.103670

Microsoft. (2025). Microsoft Digital Defense Report 2025 | Microsoft. *Microsoft Corporate Responsibility*. https://www.microsoft.com/en-us/corporate-responsibility/cybersecurity/microsoft-digital-defense-report-2025/

Mills, J. L., & Harclerode, K. (2018). *Privacy, Mass Intrusion and the Modern Data Breach* (SSRN Scholarly Paper No. 3443717). Social Science Research Network. https://papers.ssrn.com/abstract=3443717

MITRE. (2025). *MITRE ATT&CK Framework*. https://attack.mitre.org/

Mitropoulos, S., Patsos, D., & Douligeris, C. (2006). On Incident Handling and Response: A state-of-the-art approach. *Computers & Security*, *25*(5), 351–370. https://doi.org/10.1016/j.cose.2005.09.006

Mohamed, N., Al-Jaroodi, J., & Jawhar, I. (2020). Cyber–Physical Systems Forensics: Today and Tomorrow. *Journal of Sensor and Actuator Networks*, *9*(3), 37. https://doi.org/10.3390/jsan9030037

Moore, G., Khurshid, Z., McDonnell, T., Rogers, L., & Healy, O. (2023). A resilient workforce: Patient safety and the workforce response to a cyber-attack on the ICT systems of the national health service in Ireland. *BMC Health Services Research*, *23*(1), 1112. https://doi.org/10.1186/s12913-023-10076-8

Moschovitis, C. (Ed.). (2018). *Cybersecurity Program Development for Business: The Essential Planning Guide* (1st ed.). Wiley. https://doi.org/10.1002/9781119430018

Mouton, F., Leenen, L., & Venter, H. S. (2016). Social engineering attack examples, templates and scenarios. *Computers & Security*, *59*, 186–209. https://doi.org/10.1016/j.cose.2016.03.004

Musluoglu, M., Kunicina, N., & Caiko, J. (2024). Vulnerability Assessment of Industrial Control Systems for Colonial Pipeline and WannaCry Ransomware. *2024 IEEE 65th International Scientific Conference on Power and Electrical Engineering of Riga Technical University (RTUCON)*, 1–7. https://doi.org/10.1109/RTUCON62997.2024.10830848

Naik, N., Jenkins, P., Grace, P., & Song, J. (2022). Comparing Attack Models for IT Systems: Lockheed Martin's Cyber Kill Chain, MITRE ATT&CK Framework and Diamond Model.

2022 IEEE International Symposium on Systems Engineering (ISSE), 1–7. https://doi.org/10.1109/ISSE54508.2022.10005490

National cybersecurity society. (2019). *Encryption Policy Template FINAL.docx*. https://nationalcybersecuritysociety.org/wp-content/uploads/2019/10/Encryption-Policy-Template-FINAL.pdf

National cybersecurity society. (a). *Home*. National Cybersecurity Society. https://nationalcybersecuritysociety.org/

National People's Congress of China. (2017). Translation: Cybersecurity Law of the People's Republic of China (Effective June 1, 2017). *DigiChina*. https://digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017/

NCSC SUI. (2025). *Warning: Real-time phishing on behalf of cantonal banks*. https://www.ncsc.admin.ch/ncsc/en/home/aktuell/im-fokus/2025/realtimephishing.html

NCSC UK. (2019, September 19). *Plan: Your cyber incident response processes | National Cyber Security Centre - NCSC.GOV.UK*. https://www.ncsc.gov.uk/collection/incident-management/cyber-incident-response-processes

Nelson, A., Rekhi, S., Souppaya, M., & Scarfone, K. (2025). *Incident response recommendations and considerations for cybersecurity risk management: A CSF 2.0 community profile* (NIST SP 800-61r3; p. NIST SP 800-61r3). National Institute of Standards and Technology (U.S.). https://doi.org/10.6028/NIST.SP.800-61r3

Nelson, N., & Madnick, S. (2017). Studying the tension between digital innovation and cybersecurity. *MIT Web Domain*. https://dspace.mit.edu/handle/1721.1/120720

NIST. (2007). *Guide to Intrusion Detection and Prevention Systems (IDPS)* (NIST SP 800-94; 0 ed., p. NIST SP 800-94). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-94

NIST. (2016). *Guide for cybersecurity event recovery* (NIST SP 800-184; p. NIST SP 800-184). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-184

NIST. (2018a). Cybersecurity Framework V1.1. *NIST*. https://www.nist.gov/cyberframework/csf-11-archive

NIST. (2018b). *Risk management framework for information systems and organizations: A system life cycle approach for security and privacy* (NIST SP 800-37r2; p. NIST SP 800-37r2). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-37r2

NIST. (2020a). *Security and Privacy Controls for Information Systems and Organizations (800-53 rev.5)* (Revision 5). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-53r5

NIST. (2020b). *Zero Trust Architecture*. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-207

NIST. (2021a). *Developing cyber-resilient systems: A systems security engineering approach (800-160)* (NIST SP 800-160v2r1; p. NIST SP 800-160v2r1). National Institute of Standards and Technology (U.S.). https://doi.org/10.6028/NIST.SP.800-160v2r1

NIST. (2021b). *Key practices in cyber supply chain risk management: Observations from industry* (NIST IR 8276; p. NIST IR 8276). National Institute of Standards and Technology (U.S.). https://doi.org/10.6028/NIST.IR.8276

NIST. (2022). *Cybersecurity supply chain risk management for systems and organizations* (NIST SP 800-161r1; p. NIST SP 800-161r1). National Institute of Standards and Technology (U.S.). https://doi.org/10.6028/NIST.SP.800-161r1

NIST. (2023). *Guide to Operational Technology (OT) security* (NIST SP 800-82r3; p. NIST SP 800-82r3). National Institute of Standards and Technology (U.S.). https://doi.org/10.6028/NIST.SP.800-82r3

NIST. (2024). *The NIST Cybersecurity Framework (CSF) 2.0* (NIST CSWP 29; p. NIST CSWP 29). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.29

NIST. (2025a). *Incident response recommendations and considerations for cybersecurity risk management: A CSF 2.0 community profile* (NIST SP 800-61r3; p. NIST SP 800-61r3). National Institute of Standards and Technology (U.S.). https://doi.org/10.6028/NIST.SP.800-61r3

NIST. (2025b, June). *Implementing a Zero Trust Architecture | NCCoE (1800-35)*. https://www.nccoe.nist.gov/projects/implementing-zero-trust-architecture

NIST. (2023a). *NVD - Vulnerabilities*. https://nvd.nist.gov/vuln/categories

NIST. (2025a). *The NIST Cybersecurity Framework (CSF) 2.0 (Greek translation)* (NIST CSWP 29 gre; p. NIST CSWP 29 gre). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.29.gre

Nour, B., Pourzandi, M., & Debbabi, M. (2023). A Survey on Threat Hunting in Enterprise Networks. *IEEE Communications Surveys & Tutorials*, *25*(4), 2299–2324. https://doi.org/10.1109/COMST.2023.3299519

NQA. (2019). *ISO 22301:2019 Business Continuity Standard Implementation Guide*. NQA. https://www.nqa.com/medialibraries/NQA/NQA-Media-Library/PDFs/NQA-ISO-22301-Implementation-Guide.pdf

NQA. (2022). *ISO 27001:2022 Information Security Implementation Guide*. NQA. https://www.nqa.com/getmedia/ae12c945-4dbb-4b73-a4e3-996261a540af/NQA-ISO-27001-Implementation-Guide.pdf

Nye, J. S. (2010). *Cyber Power | The Belfer Center for Science and International Affairs*. https://www.belfercenter.org/publication/cyber-power

Nye, J. S. (2017). Deterrence and Dissuasion in Cyberspace. *International Security, 41*(3), 44–71. https://doi.org/10.1162/ISEC_a_00266

O'Kane, P., Sezer, S., & Carlin, D. (2018). Evolution of ransomware. *IET Networks*, *7*(5), 321–327. https://doi.org/10.1049/iet-net.2017.0207

Paidy, P. (2023). Adaptive Application Security Testing with AI Automation. *International Journal of AI, BigData, Computational and Management Studies*, *4*, 55–63. https://doi.org/10.63282/3050-9416.IJAIBDCMS-V4I1P106

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Computers & Security*, *42*, 165–176. https://doi.org/10.1016/j.cose.2013.12.003

Pool, J., Akhlaghpour, S., Fatehi, F., & Burton-Jones, A. (2024). A systematic analysis of failures in protecting personal health data: A scoping review. *International Journal of Information Management*, *74*, 102719. https://doi.org/10.1016/j.ijinfomgt.2023.102719

PricewaterhouseCoopers. (2021). *Conti cyber attack on the HSE: Independent Post Incident Review*. https://www.lenus.ie/entities/publication/1bd0b513-9ffb-4b6f-94f4-cf68116c1e89

Reuters. (2020, September 22). Shopify says customer data likely exposed as employees accessed records. *Reuters*. https://www.reuters.com/business/finance/shopify-says-customer-data-likely-exposed-employees-accessed-records-2020-09-22/

Ricci, S., Janout, V., Parker, S., Jerabek, J., Hajny, J., Chatzopoulou, A., & Badonnel, R. (2021). PESTLE Analysis of Cybersecurity Education. *Proceedings of the 16th International Conference on Availability, Reliability and Security*, 1–8. https://doi.org/10.1145/3465481.3469184

Rid, T. (2011). Cyber War Will Not Take Place. *Journal of Strategic Studies*, *35*(1), 5–32. https://doi.org/10.1080/01402390.2011.608939

Romagna, M., & Leukfeldt, R. E. (2023). Becoming a hacktivist. Examining the motivations and the processes that prompt an individual to engage in hacktivism. *Journal of Crime and Justice*, *47*(4), 511–529. https://doi.org/10.1080/0735648X.2023.2216189

Ruohonen, J., Hjerppe, K., & Kortesuo, K. (2024). *Crisis Communication in the Face of Data Breaches* (Version 2). arXiv. https://doi.org/10.48550/ARXIV.2406.01744

Saha, T., Aaraj, N., Ajjarapu, N., & Jha, N. K. (2021). *SHARKS: Smart Hacking Approaches for RisK Scanning in Internet-of-Things and Cyber-Physical Systems based on Machine Learning*. https://doi.org/10.48550/ARXIV.2101.02780

Sailio, M., Latvala, O.-M., & Szanto, A. (2020). Cyber Threat Actors for the Factory of the Future. *Applied Sciences*, *10*(12), 4334. https://doi.org/10.3390/app10124334

Salahdine, F., & Kaabouch, N. (2019). Social Engineering Attacks: A Survey. *Future Internet*, *11*(4), 89. https://doi.org/10.3390/fi11040089

Schneier, B. (2016). Lessons From the Dyn DDoS Attack. *Schneier on Security*. https://www.schneier.com/essays/archives/2016/11/lessons_from_the_dyn.html

Schröer, S. L., Apruzzese, G., Human, S., Laskov, P., Anderson, H. S., Bernroider, E. W. N., Fass, A., Nassi, B., Rimmer, V., Roli, F., Salam, S., Shen, A., Sunyaev, A., Wadhwa-Brown, T., Wagner, I., & Wang, G. (2024). *SoK: On the Offensive Potential of AI* (Version 4). arXiv. https://doi.org/10.48550/ARXIV.2412.18442

Schwartz, S. (2018, October 4). *Why us? 6 months after ransomware attack Atlanta has no answers | CIO Dive*. https://www.ciodive.com/news/why-us-6-months-after-ransomware-attack-atlanta-has-no-answers/533512/

Segal, E. (2022). *1 Year Later: Actions Taken, Lessons Learned Since The Colonial Pipeline Cyberattack*. Forbes. https://www.forbes.com/sites/edwardsegal/2022/05/07/1-year-later-actions-taken-lessons-learned-since-the-colonial-pipeline-cyberattack/

Sharma, A., Sharma, S., & Dave, M. (2015). Identity and access management- a comprehensive study. *2015 International Conference on Green Computing and Internet of Things (ICGCIoT)*, 1481–1485. https://doi.org/10.1109/ICGCIoT.2015.7380701

Sharma, G., Vidalis, S., Menon, C., Anand, N., & Kumar, S. (2021). Analysis and Implementation of Threat Agents Profiles in Semi-Automated Manner for a Network Traffic in Real-Time Information Environment. *Electronics*, *10*(15), 1849. https://doi.org/10.3390/electronics10151849

Sherif, E., Yevseyeva, I., Basto-Fernandes, V., & Cook, A. (2024). The Smart Approach to Selecting Good Cyber Security Metrics. *Journal of Internet Services and Information Security*, *14*(4), 312–330. https://doi.org/10.58346/JISIS.2024.I4.019

Shin, Y., Kwon, H., Jeong, J., & Shin, D. (2024). A Study on Designing Cyber Training and Cyber Range to Effectively Respond to Cyber Threats. *Electronics*, *13*(19), 3867. https://doi.org/10.3390/electronics13193867

Shiri Harzevili, N., Boaye Belle, A., Wang, J., Wang, S., Jiang, Z. M. (Jack), & Nagappan, N. (2025). A Systematic Literature Review on Automated Software Vulnerability Detection Using Machine Learning. *ACM Computing Surveys*, *57*(3), 1–36. https://doi.org/10.1145/3699711

Shopify. (2020, September 22). *What happened in the recent data incident involving less than 200 Shopify merchants?* Shopify Community. https://community.shopify.com/t/what-happened-in-the-recent-data-incident-involving-less-than-200-shopify-merchants/21195

Singh, R., Kumar Gupta, M., Patil, D. R., & Maruti Patil, S. (2024). Analysis of Web Application Vulnerabilities using Dynamic Application Security Testing. *2024 IEEE 9th International Conference for Convergence in Technology (I2CT)*, 1–6. https://doi.org/10.1109/I2CT61223.2024.10543484

Smeets, M. (2018). The Strategic Promise of Offensive Cyber Operations. *Strategic Studies Quarterly*, *12*(3), 90–113.

Sotiropoulos, P., Mathas, C.-M., Vassilakis, C., & Kolokotronis, N. (2023). A Software Vulnerability Management Framework for the Minimization of System Attack Surface and Risk. *Electronics*, *12*(10), 2278. https://doi.org/10.3390/electronics12102278

Souppaya, M. (2025). *Ransomware Risk Management: A Cybersecurity Framework 2.0 Community Profile* (NIST IR 8374r1 ipd; p. NIST IR 8374r1 ipd). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8374r1.ipd

Spanca, F., & Salihu, A. (2024). Unveiling the Consequences of Data Breaches: Risks, Impacts, and Mitigation in the Digital Age. *2024 International Conference on Electrical, Communication and Computer Engineering (ICECCE)*, 1–8. https://doi.org/10.1109/ICECCE63537.2024.10823432

Suresh, N., Sanders, G. L., & Braunscheidel, M. J. (2020). Business Continuity Management for Supply Chains Facing Catastrophic Events. *IEEE Engineering Management Review*, *48*(3), 129–138. https://doi.org/10.1109/EMR.2020.3005506

Tabansky, L. (2020). Israel Defense Forces and National Cyber Defense. *Connections: The Quarterly Journal*, *19*(1), 45–62. https://doi.org/10.11610/Connections.19.1.05

Taherdoost, H. (2022). Understanding Cybersecurity Frameworks and Information Security Standards—A Review and Comprehensive Overview. *Electronics*, *11*(14), 2181. https://doi.org/10.3390/electronics11142181

Tan, Z., Parambath, S. P., Anagnostopoulos, C., Singer, J., & Marnerides, A. K. (2025). Advanced Persistent Threats Based on Supply Chain Vulnerabilities: Challenges, Solutions, and Future Directions. *IEEE Internet of Things Journal*, *12*(6), 6371–6395. https://doi.org/10.1109/JIOT.2025.3528744

The White House. (2023, March). *National-Cybersecurity-Strategy-2023*. https://bidenwhitehouse.archives.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

Top Class Actions,. (2022, April 5). Shopify Class Action Alleges Company Failed To Secure Personal Information Of Customers Who Purchased Ledger Crypto Wallets. *Top Class Actions,*. https://topclassactions.com/lawsuit-settlements/lawsuit-news/shopify-class-action-alleges-

company-failed-to-secure-personal-information-of-customers-who-purchased-ledger-crypto-wallets/

Toussaint, M., Krima, S., & Panetto, H. (2024). Industry 4.0 data security: A cybersecurity frameworks review. *Journal of Industrial Information Integration, 39,* 100604. https://doi.org/10.1016/j.jii.2024.100604

Tsauri, M. S. (2025). Human Vulnerabilities to Social Engineering Attacks: A Systematic Literature Review for Building a Human Firewall. *Journal of Applied Informatics and Computing*, *9*(4), 1127–1136. https://doi.org/10.30871/jaic.v9i4.9585

United States District Court. (2021, February 19). *US grand jury indictment Tassilo Heinrich*. https://www.documentcloud.org/documents/20580321-us-grand-jury-indictment-tassilo-heinrich/

University of Bristol. (2025). *ISP-16 Encryption policy | About the University | University of Bristol*. https://www.bristol.ac.uk/university/governance/university-policies/isp-16-encryption-policy/

University of San Francisco. (2020, June 27). *Update on IT Security Incident at UCSF | UC San Francisco*. https://www.ucsf.edu/news/2020/06/417911/update-it-security-incident-ucsf

U.S. Department of Energy. (2021). *Colonial Pipeline Cyber Incident*. Energy.Gov. https://www.energy.gov/ceser/colonial-pipeline-cyber-incident

U.S. Transportation Security Administration. (2022). *TSA revises and reissues cybersecurity requirements for pipeline owners and operators | Transportation Security Administration*. U.S. Department of Homeland Security Transportation Security Administration. https://www.tsa.gov/news/press/releases/2022/07/21/tsa-revises-and-reissues-cybersecurity-requirements-pipeline-owners

Vengathattil, S. (2023). Exploring Information Systems for Business Continuity Planning in IT-Driven Organizations Post-Pandemic: Insight into Enhancing Future Resilience. *International Journal for Multidisciplinary Research (IJFMR), 5*(2). https://www.researchgate.net/profile/Sunish-

Vengathattil-2/publication/389215507_Exploring_Information_Systems_for_Business_Continuity_Planning_in_IT-Driven_Organizations_Post-Pandemic_Insight_into_Enhancing_Future_Resilience/links/67b960878311ce680c6f638

Verizon. (2025). *2025 Data Breach Investigations Report*. Verizon Business. https://www.verizon.com/business/resources/reports/dbir/

Vimercati, S. D. C. D., Foresti, S., Jajodia, S., Paraboschi, S., Pelosi, G., & Samarati, P. (2010). Encryption-Based Policy Enforcement for Cloud Storage. *2010 IEEE 30th International Conference on Distributed Computing Systems Workshops*, 42–51. https://doi.org/10.1109/ICDCSW.2010.35

Waliullah, Md., George, M. Z. H., Hasan, M. T., Alam, M. K., Munira, M. S. K., & Siddiqui, N. A. (2025). *Assessing the influence of cybersecurity threats and risks on the adoption and growth of digital banking: A systematic literature review*. https://doi.org/10.48550/ARXIV.2503.22710

Wang, C., & Zhu, H. (2022). Wrongdoing Monitor: A Graph-Based Behavioral Anomaly Detection in Cyber Security. *IEEE Transactions on Information Forensics and Security, 17*, 2703–2718. https://doi.org/10.1109/TIFS.2022.3191493

Whittaker, Z. (2021, April 5). US charges California man over Shopify data breach. *TechCrunch*. https://techcrunch.com/2021/04/05/shopify-breach-hacker-indicted/

Wright, D., & Kumar, R. (2023). Assessing the socio-economic impacts of cybercrime. *Societal Impacts, 1*(1–2), 100013. https://doi.org/10.1016/j.socimp.2023.100013

Wu, D. (2020, July 1). *UCSF Pays Hackers $1.14M to Recover Encrypted Data*. GovTech. https://www.govtech.com/security/UCSF-Pays-Hackers-1-14M-to-Recover-Encrypted-Data.html

Wu, D., Ren, A., Zhang, W., Fan, F., Liu, P., Fu, X., & Terpenny, J. (2018). Cybersecurity for digital manufacturing. *Journal of Manufacturing Systems*, *48*, 3–12. https://doi.org/10.1016/j.jmsy.2018.03.006

Yang-seo Choi & Dong-il Seo. (2005). An analysis of ISPs' role as managed security service providers (MSSPs). *The 7th International Conference on Advanced Communication Technology, 2005, ICACT 2005.*, 624–626. https://doi.org/10.1109/ICACT.2005.245948

Yaser Al-Bustani, A. M., Almutairi, A. K., Alrashed, A., & Muzaffar, A. W. (2023). Social Engineering via Personality Psychology—Bypassing Users Based on Their Personality Pattern To Raise Security Awareness. *2023 International Conference on IT Innovation and Knowledge Discovery (ITIKD)*, 1–8. https://doi.org/10.1109/ITIKD56332.2023.10100048

Ελληνική Δημοκρατία. (2024). *ΕΝΟΤΗΤΑ_5_ΝΟΜΟΘΕΣΙΑ_fek_a_195_2024-5160-2024*. https://cyber.gov.gr/wp-content/uploads/2024/12/ENOTHTA_5_%CE%9D%CE%9F%CE%9C%CE%9F%CE%98%CE%95%CE%A3%CE%99%CE%91_fek_a_195_2024-5160-2024.pdf

Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο της ΕΕ. (2022). *NIS2_EL_ΟΔΗΓΙΑ-ΕΕ-2022_2555-_14-Δεκ-2022-1*. https://cyber.gov.gr/wp-content/uploads/2024/12/NIS2_EL_%CE%9F%CE%94%CE%97%CE%93%CE%99%CE%91-%CE%95%CE%95-2022_2555-_14-%CE%94%CE%B5%CE%BA-2022-1.pdf