ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΑΤΤΙΚΗΣ

ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΥΠΟΛΟΓΙΣΤΩΝ

Πρόγραμμα Μεταπτυχιακών Σπουδών
Επιστήμη και Τεχνολογία της Πληροφορικής και των Υπολογιστών

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Κυβερνοασφάλεια στη Ναυτιλία

Νικόλαος Α. Κουναλάκης
Α.Μ. mcse20012

Ευάγγελος Δ. Χαρίτος
Α.Μ. mcse20004

Εισηγητής: Καντζάβελου Ιωάννα, Επίκουρη Καθηγήτρια

(Κενό φύλλο)

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Κυβερνοασφάλεια στην Ναυτιλία

Νικόλαος Α. Κουναλάκης
Α.Μ. mcse20012

Ευάγγελος Δ. Χαρίτος
Α.Μ. mcse2004

Εισηγητής:

Καντζάβελου Ιωάννα, Επίκουρη Καθηγήτρια

Ioanna Kantzavelou Digitally signed by Ioanna Kantzavelou Date: 2022.07.12 11:28:17 +03'00'

Εξεταστική Επιτροπή:

Αντώνιος Μπόγρης Καθηγητής Antonios Bogris Digitally signed by Antonios Bogris Date: 2022.07.12 23:49:00 +03'00'

Βασίλειος Μάμαλης Καθηγητής Vasileios Mamalis Digitally signed by Vasileios Mamalis Date: 2022.07.13 02:52:54 +03'00'

Ημερομηνία εξέτασης

07/07/2022

(Κενό φύλλο)

ΔΗΛΩΣΗ ΣΥΓΓΡΑΦΕΑ ΜΕΤΑΠΤΥΧΙΑΚΗΣ ΕΡΓΑΣΙΑΣ

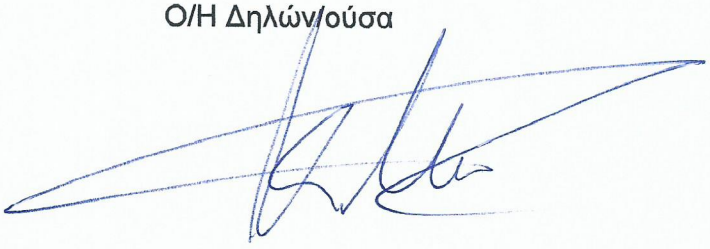
Ο/η κάτωθι υπογεγραμμένος/η ...ΚΟΥΝΑΛΗΣ ΝΙΚΟΛΑΟΣ..... του ΑΛΕΞΑΝΔΡΟΥ με αριθμό μητρώου 20012 φοιτητής/τρια του Προγράμματος Μεταπτυχιακών Σπουδών Επιστήμη και Τεχνολογία της Πληροφορίας του Τμήματος Μηχ. Πληροφορικής και Υλ. της Σχολής Μηχανολόγων ..... του Πανεπιστημίου Δυτικής Αττικής, δηλώνω ότι:

«Είμαι συγγραφέας αυτής της μεταπτυχιακής εργασίας και ότι κάθε βοήθεια την οποία είχα για την προετοιμασία της, είναι πλήρως αναγνωρισμένη και αναφέρεται στην εργασία. Επίσης, οι όποιες πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών ή λέξεων, είτε ακριβώς είτε παραφρασμένες, αναφέρονται στο σύνολό τους, με πλήρη αναφορά στους συγγραφείς, τον εκδοτικό οίκο ή το περιοδικό, συμπεριλαμβανομένων και των πηγών που ενδεχομένως χρησιμοποιήθηκαν από το διαδίκτυο. Επίσης, βεβαιώνω ότι αυτή η εργασία έχει συγγραφεί από μένα αποκλειστικά και αποτελεί προϊόν πνευματικής ιδιοκτησίας τόσο δικής μου, όσο και του Ιδρύματος.

Παράβαση της ανωτέρω ακαδημαϊκής μου ευθύνης αποτελεί ουσιώδη λόγο για την ανάκληση του πτυχίου μου».

Επιθυμώ την απαγόρευση πρόσβασης στο πλήρες κείμενο της εργασίας μου μέχρι ..... και έπειτα από αίτηση μου στη Βιβλιοθήκη και έγκριση του επιβλέποντα καθηγητή.

Ο/Η Δηλών/ούσα



ΔΗΛΩΣΗ ΣΥΓΓΡΑΦΕΑ ΜΕΤΑΠΤΥΧΙΑΚΗΣ ΕΡΓΑΣΙΑΣ

Ο/η κάτωθι υπογεγραμμένος/η ..... του Δικαίου., με αριθμό μητρώου ..... φοιτητής/τρια του Προγράμματος Μεταπτυχιακών Σπουδών ..... του Τμήματος ..... της Σχολής ..... του Πανεπιστημίου Δυτικής Αττικής, δηλώνω ότι:

«Είμαι συγγραφέας αυτής της μεταπτυχιακής εργασίας και ότι κάθε βοήθεια την οποία είχα για την προετοιμασία της, είναι πλήρως αναγνωρισμένη και αναφέρεται στην εργασία. Επίσης, οι όποιες πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών ή λέξεων, είτε ακριβώς είτε παραφρασμένες, αναφέρονται στο σύνολό τους, με πλήρη αναφορά στους συγγραφείς, τον εκδοτικό οίκο ή το περιοδικό, συμπεριλαμβανομένων και των πηγών που ενδεχόμενως χρησιμοποιήθηκαν από το διαδίκτυο. Επίσης, βεβαιώνω ότι αυτή η εργασία έχει συγγραφεί από μένα αποκλειστικά και αποτελεί προϊόν πνευματικής ιδιοκτησίας τόσο δικής μου, όσο και του Ιδρύματος.

Παράβαση της ανωτέρω ακαδημαϊκής μου ευθύνης αποτελεί ουσιώδη λόγο για την ανάκληση του πτυχίου μου».

Επιθυμώ την απαγόρευση πρόσβασης στο πλήρες κείμενο της εργασίας μου μέχρι ..... και έπειτα από αίτηση μου στη Βιβλιοθήκη και έγκριση του επιβλέποντα καθηγητή.

Ο/Η Δηλών/ούσα

(Κενό φύλλο)

ΕΥΧΑΡΙΣΤΙΕΣ

Η παρούσα διπλωματική εργασία ολοκληρώθηκε στα πλαίσια των μεταπτυχιακών μας σπουδών με τίτλο «Τεχνολογία και Επιστήμη της Πληροφορικής και των Υπολογιστών» του τμήματος Μηχανικών Πληροφορικής του Πανεπιστημίου Δυτικής Αττικής. Σε αυτό το σημείο, θα θέλαμε να ευχαριστήσουμε θερμά την καθηγήτρια Κα. Ιωάννα Καντζάβελου για την στήριξη και την συμβολή της στην διεκπεραίωση της εργασίας, τον χρόνο που αφιέρωσε και την καθοδήγηση της σε επιστημονικά ζητήματα που τέθηκαν.

Επίσης, θα θέλαμε να ευχαριστήσουμε τον υπεύθυνο του ΠΜΣ, καθηγητή κ. Αντώνιο Μπόγρη, για την υποστήριξη του, την ομαλή και επιμορφωτική διεξαγωγή του προγράμματος καθώς και για την επίλυση των όποιον ζητημάτων δημιουργήθηκαν καθόλη την διάρκεια του κύκλου σπουδών.

Επιπλέον, θα θέλαμε να ευχαριστήσουμε όλο το εκπαιδευτικό προσωπικό, το οποίο απαρτίζεται από εξαιρετικούς επιστήμονες, για την βοήθεια, την καθοδήγηση και την εκπαίδευση που μας προσέφεραν μέσω των διδακτικών τους ωρών.

Τέλος, θα θέλαμε να ευχαριστήσουμε τις οικογένειές μας που με την επιμονή τους και υπομονή τους μας βοήθησαν να εκπληρώσουμε τους στόχους μας και να προχωρήσουμε στην ζωή μας.

(Κενό φύλλο)

ΠΕΡΙΛΗΨΗ

Η παρούσα διπλωματική εργασία εμβαθύνει στην μελέτη και ανάπτυξη των τεχνολογιών της Κυβερνοασφάλειας στην εμπορική ναυτιλία. Σε αυτό το πεδίο, παραχωρούνται κάποιες από τις τεχνολογίες που εφαρμόζονται στην διασφάλιση του δικτύου ενός εμπορικού πλοίου, οι κίνδυνοι από τους οποίους απειλείται ένα δίκτυο και πως αυτοί διαχειρίζονται. Έμφαση δίνεται στην αξιολόγηση των προαναφερόμενων κινδύνων και τι μπορεί να συμβεί η να βλάψει η κάθε απειλή μεμονωμένα. Τέλος, παρατίθενται το θεωρητικό υπόβαθρο του 5G και λύσεις τις οποίες καλείται να δώσει και να συμβάλει σε κρίσιμα ζητήματα κυβερνοασφάλειας.

Εν συνεχεία της εργασίας, υλοποιείται παραμετροποίηση του Firewall ενός πραγματικού δικτύου μεταξύ εμπορικού πλοίου και πάροχου και σε πραγματικό χρόνο εξάγονται τα δεδομένα ενός ολόκληρου μήνα από την αναφορά της κίνησης του δικτύου. Ειδικότερα το Firewall, το οποίο παραμετροποείται βάσει προκαθορισμένων κανόνων, ελέγχει όλη την εισερχόμενη και εξερχόμενη κίνηση του. Στο πρώτο σκέλος της αναφοράς, ύστερα από έναν μήνα παρακολούθησης, αναγράφονται οι τύποι προστασίας δικτύου και η αυστηρότητας του κάθε τύπου. Επιπλέον, για κάθε τύπο προστασίας εκδίδεται και ένα log αρχείο με ολόκληρη την κίνηση που παρακολουθούσε το πεπερασμένο διάστημα. Επίσης, έμφαση δίνονται στις δραστηριότητες των Malwares και την επικινδυνότητα που είχαν για τον κάθε τύπο προστασίας. Τέλος, γίνεται επιστημονική αναφορά του πρωτοκόλλου 5G και την συμβολή που έχει στην επίλυση ζητημάτων ταχύτητας και μετάδοσης στην πραγμάτωση ενός ασφαλέστερου δικτύου.

Με την ραγδαία εξέλιξη της τεχνολογίας και των επικοινωνιών, όλο και περισσότερες προσωπικές πληροφορίες αναρτώνται στο διαδίκτυο κεντρίζοντας το ενδιαφέρον κακόβουλων χρηστών που κλείνονται να τις συλλέξουν. Η εργασία αποσκοπεί κυρίως στην ανάλυση των κινδύνων που συναντάμε στα πλαίσια της κυβερνοασφάλειας στην εμπορική ναυτιλία και την διαχείριση, αν όχι εξ ολόκληρου επίλυση, αυτών. Παρατίθενται βασικές αρχές αντιμετώπισης και ιδέες προς μελλοντική χρήση.

ΛΕΞΕΙΣ ΚΛΕΙΔΙΑ: Κυβερνοασφάλεια, Εμπορική Ναυτιλία, δίκτυο, 5G, Firewall, Malwares

ABSTRACT

The present thesis concerns the study and development of Cybersecurity technologies in Maritime. In this field, technologies that are implemented to secure a vessel's network, the threats that a network faces, and alternative ways to manage those threats are demonstrated. It is given an evaluation of the possible hazard the threats might cause and the section it might get harmed by one single threat. Finally, it discusses the whole 5G theoretical background and its solutions for crucial issues in Maritime Cybersecurity.

Furthermore, a Firewall of a legit network between a vessel and a payload is configured and the entire month's network traffic data in real-time is extracted from a report. In particular, the Firewall, which is configured according to predefined rules, controls all the incoming and outgoing traffic on the network. The first part of the report, after a month of monitoring, lists the network protection types and the severity of each one of them. In addition, for each protection type, a log file is created which contains all the traffic issues monitored at this finite time. Moreover, emphasis is also placed on Malwares' activities and the risk they pose to each protection type. Lastly, there is a scientific reference to the 5G protocol and its contribution to solving speed and transmission issues and the implementation of a more secure network.

With the rapid development of technology and in the section of communications, more personal and sensitive information is being posted on the internet, sparking the interest of malicious users who are willing to collect it. This work is aimed at analyzing the risks that are encountered in the context of cybersecurity in vessels and its management, if not the complete solution, to these. There are plenty of tips that are given at this work to help in future work.

KEYWORDS: Cybersecurity, Maritime, Network, 5G, Firewall, Malwares

ΠΕΡΙΕΧΟΜΕΝΑ

ΚΑΤΑΛΟΓΟΣ ΕΙΚΟΝΩΝ

ΚΑΤΑΛΟΓΟΣ ΠΙΝΑΚΩΝ

ΣΥΝΤΟΜΟΓΡΑΦΙΕΣ

1G First Generation

2G Second Generation

3G Third Generation

3GPP Third-Generation Partnership Project

4G Fourth Generation

5G Fifth Generation

5G-VCC 5G Vehicular Cloud Computing

AI Artificial Intelligence

AIS Automatic Identification System

AMPS Advanced Mobile Phone Service

APRANET Advanced Research Projects Agency Network

CCTV Closed Circuit Television

CC Cloud Computing

DDOS Distributed Denial-of-Service

DOC Document of Compliance

ECDIS Electronic Chart Display and Information System

EGC Enhanced Group Call

EICAR European Institute for Computer Antivirus Research

EPC Enhanced Packet Core

FBB Fleet Broadband

FC Fog Computing

FDD Frequency Division Duplexing

FM Frequency Modulation

FX Fleet Express

GMDSS Global Maritime Distress and Safety System

GPS Global Positioning System

GX Global Express

HQ Head Quarters

HSDPA High Speed Downlink Packet Access

IMO International Maritime Organization

IOT Internet of Things

ISM International Safety Management

ISPS International Ship and Port Facility Security

IP Internet Protocol

IT Information technology

LTE Long Term Evolution

MEC Mobile Edge Computing

MES Mobile Earth Station

MFA Multi-Factor Authentication

MPDS Mobile Packet Data Service

MSC Maritime Safety Committee

MSI Maritime Safety Information

NBA Network Behavioral Analysis

NMT Navy Multiband Terminal

NSA National Security Agency

OT Operational Technology

PLC Programmable Logic Controllers

PSK Phase Shift Keying

RMG Rail Mounted Gantry

RTG Rubber Tired Gantry

SCADA Supervisory Control and Data Acquisition

SDN Software Defined Networks

SMS Short Message Service

SSAS Software Support Activity System

TACS Total Access Telecommunications Systems

TDD Time Division Duplexing

TDMA Time Division Multiple Access

UDN Ultra Dense Networks

URL Uniform Resource Locator

VMS Vendor Management System

VPN Virtual Private Network

WAF Web application firewalls

WCDMA Wide Code Division Multiple Access

ΕΙΣΑΓΩΓΗ

Σε αυτό το κεφάλαιο αναλύεται το αντικείμενο της διπλωματικής εργασίας και γίνεται μια αναδρομή στον χρόνο για την πορεία και την εξέλιξη της ναυτιλίας. Εν συνεχεία. Παρατίθενται οι εμπορικές τεχνολογίες που είναι διαθέσιμες γύρω από τις εμπορικές συνδέσεις των επικοινωνιών ενός εμπορικού πλοίου καθώς και τα τεχνικά χαρακτηριστικά τους. Ιστορική αναφορά πραγματοποιείται στα πλαίσια της κυβερνοασφάλειας και την εξέλιξη που είχε μέχρι και σήμερα.

Η ναυτιλία είναι ένας κλάδος ανερχόμενος και άκρως σημαντικό στον βιοπορισμό των ανθρώπων. Παράλληλα όμως, είναι ένας κλάδος ο οποίος συνεχίζει να εξελίσσεται και τα συστήματα που χρησιμοποιεί δεν συμβαδίζουν με αυτά του βιομηχανικού τομέα. Ως συνέπεια αυτού, η κίνηση του δικτύου και ο διαμοιρασμός πληροφοριών από και προς ένα εμπορικό πλοίο, μπορεί να είναι ευάλωτα και με ιδιαίτερο ενδιαφέρον προς τους κακόβουλους χρήστες. Οι κίνδυνοι που παραμονεύουν διαφέρουν και τα μέτρα που πρέπει να ληφθούν πρέπει να είναι άμεσα και καθοριστικά. Οι εταιρείες των πλοίων δεν μπορούν πλέον να αρκεστούν στην προστασία του παρόχου και οφείλουν να λάβουν πιο σοβαρά τα ζητήματα της κυβερνοασφάλειας καθώς πλέον οι επιθέσεις ανέρχονται σε μεγάλο βαθμό με τα παραδείγματα να ποικίλουν, όπως θα αναφερθούν κάποια στη συνέχεια των κεφαλαίων. [20]

Η ναυτιλία αποτελεί αναπόσπαστο κομμάτι των μεταφορών πρώτων υλών, αγαθών ή ακόμη και καυσίμων και δεν θα μπορούσε να αναιρεθεί η λειτουργικότητα της. Ωστόσο, για την ομαλή διένεξη των παραπάνω, θα πρέπει να εξασφαλιστεί η ασφάλεια του δικτύου στον τομέα της ναυτιλίας και των επικοινωνιών. Στα επόμενα κεφάλαια αναφέρονται πολύ από του κίνδυνους και αναλύεται μία αναφορά σε πραγματικό χρόνο από επιθέσεις στο δίκτυο ενός εμπορικού πλοίου στους τύπους προστασίας που χρησιμοποιήθηκαν και η καλύτερη διαχείριση αυτών. Τέλος, περιγράφεσαι η 5^{ης} γενιάς δικτύου και όλα τα πρωτόκολλα που μεσολάβησαν για την ανάδειξη ης τελευταίας τεχνολογίας. Η ασφάλεια του δικτύου ενός εμπορικού πλοίου είναι ζωτικής σημασίας και χρήζει αντιμετώπισης.

1.1 Περιγραφή του αντικειμένου της διπλωματικής εργασίας

Αντικείμενο της παρούσας διπλωματικής εργασίας είναι η ασφάλεια των δικτύων και η υποδομή που θα το υποστηρίζει στην εμπορική ναυτιλία. Σύμφωνα με το παραπάνω περιγράφονται οι υποδομές ενός εκάστοτε εμπορικού πλοίου και πως πραγματώνεται η καλύτερη δυνατή υποδομή για την ασφάλεια του. Τέλος προτείνονται τρόποι διαχείρισης και αξιολογήσεις τυχόν απειλών. [1] [4]

1.2 Η Ναυτιλία στο Χρόνο

1.2.1 Ιστορική αναδρομή στην ναυτιλία

Η πράξη της μεταφοράς φορτίου δια θαλάσσης υπάρχει εδώ και χιλιετίες, συναρπαστικό γεγονός το αρχαιότερο παράδειγμα ιστιοφόρου βρέθηκε σε έναν ζωγραφισμένο δίσκο στο Κουβέιτ και χρονολογείται από τα τέλη της 5ης χιλιετίας π.Χ. [19]

Εικόνα 1: Εμπορικό Πλοίο της Σύγχρονης Ναυτιλίας

Η ναυτιλιακή ιστορία έχει ως βασικό κεφάλαιο τη σχέση του ανθρώπου με τη θάλασσα με βασικό γνώμονα την μεταφορά φορτίων στην πάροδο των χρόνων. Ως εκ τούτου, ασχολείται κυρίως με το περιεχόμενο των φορτίων, την ιδιότητα των πλοίων τις θάλασσες που μεταφέρονται τα φορτία και στα λιμάνια που γίνεται η φόρτωση και εκφόρτωση αυτών. Επιπλέον, ως αποτέλεσμα των παραπάνω, η ιστορία εκτυλίσσεται γύρω από τις συνθήκες διαβίωσης πάνω σε ένα εμπορικό πλοίο και τα διεθνή θεσμικά πλαίσια που έχουν οργανωθεί για την επίτευξη των μεταφορών από ΄χωρά σε χώρα. Είχε και έχει τεράστιο αντίκτυπο στην ανάπτυξη του πολιτισμού παγκοσμίως . Με την

έλευση της ναυτιλίας, οι ναυτικοί μπόρεσαν ξαφνικά να ταξιδέψουν πολύ πιο μακριά από ό,τι επέτρεπαν τα χερσαία ταξίδια. Φυσικά, τα θαλάσσια ταξίδια για λόγους αναψυχής δεν έγιναν παρά πολύ αργότερα σε παγκόσμιο χρονοδιάγραμμα. [16] [18] [15]

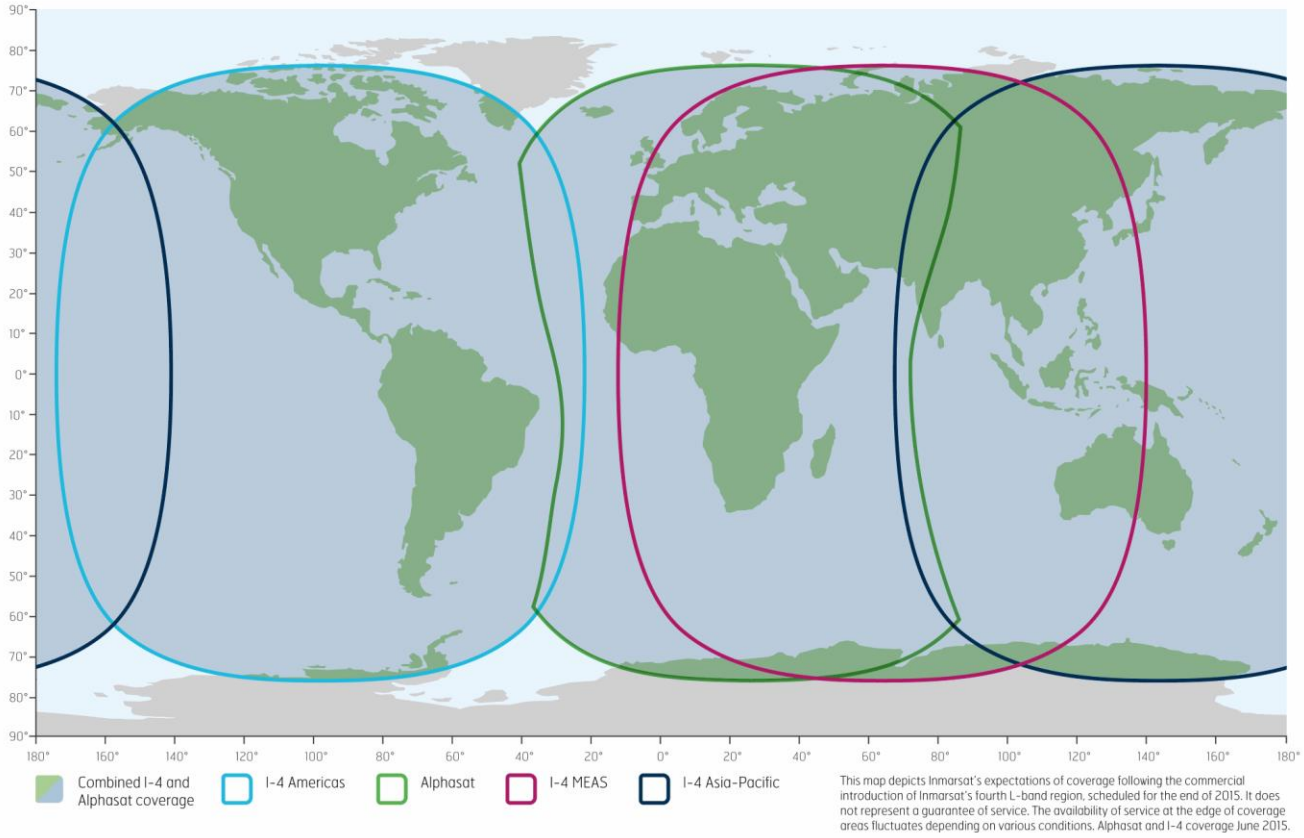
Κυρίως για τον δυτικό κόσμο, οι θαλάσσιες μεταφορές ήταν και είναι στην κορυφή μεταφοράς των προϊόντων, καθώς η μεταφορά υπέρογκων στοιχείων δεν μπορεί ακόμη και σήμερα να πραγματοποιηθεί με άλλο μέσο . Χρονικά, θεωρείται η απαρχή της σύγχρονης ναυτιλίας η οποία εξελίσσεται μέχρι σήμερα με την λήξη του δευτέρου παγκοσμίου πολέμου. Πάνω από μισό αιώνα χρονικά τα πλοία έχουν εξελίξει τα μέσα πρόωσης και έχουν ενστερνιστεί τα τεχνολογικά άλματα με συνέπεια την ταχύτερη και ασφαλέστερη μεταφορά φορτίων. [17]

Η σύγχρονη διεθνής νομοθεσία προϋποθέτει για ένα εμπορικό πλοίο (βλ. Εικόνα 1) να είναι ασφαλές τόσο για το πλήρωμα όσο και προς το περιβάλλον. Όσον αναφορά το δεύτερο, ένα σύγχρονο τρανταχτό παράδειγμα για την προστασία του περιβάλλοντος, είναι οι διαχωριστές λαδιού που επιβάλλεται κάθε ναυτιλιακή εταιρεία να εφαρμόσει στα πλοία της. Πρακτικά, διαχωρίζεται το νερό του μηχανοστασίου από λάδια ή καύσιμο και απορρέεται στην θάλασσα. Εν συνεχεία πραγματοποιείται έλεγχος από τις αρμόδιες αρχές προς διαπίστωση τήρηση του νομικού πλαισίου. [26] [22]

Στην Ευρώπη και την ανάπτυξη του οικονομικού τομέα, η ναυτιλία έχει καθοριστικό ρόλο έχοντας το 75% των εισαγωγών και το 37% των εξαγωγών που τελούνται πανευρωπαϊκά. Η ναυτιλία έχει ουσιαστικό ρόλο για την οικονομική ανάπτυξη της Ευρωπαϊκής Ένωσης. Πλέον, όλες οι περιφέρειες και οι νησιωτικές περιοχές είναι ενωμένες και το εμπορικό δίκτυο εξυπηρετείται από την ναυτιλία. [17] [12]

1.2.2 Δορυφορικές συνδέσεις των εμπορικών πλοίων

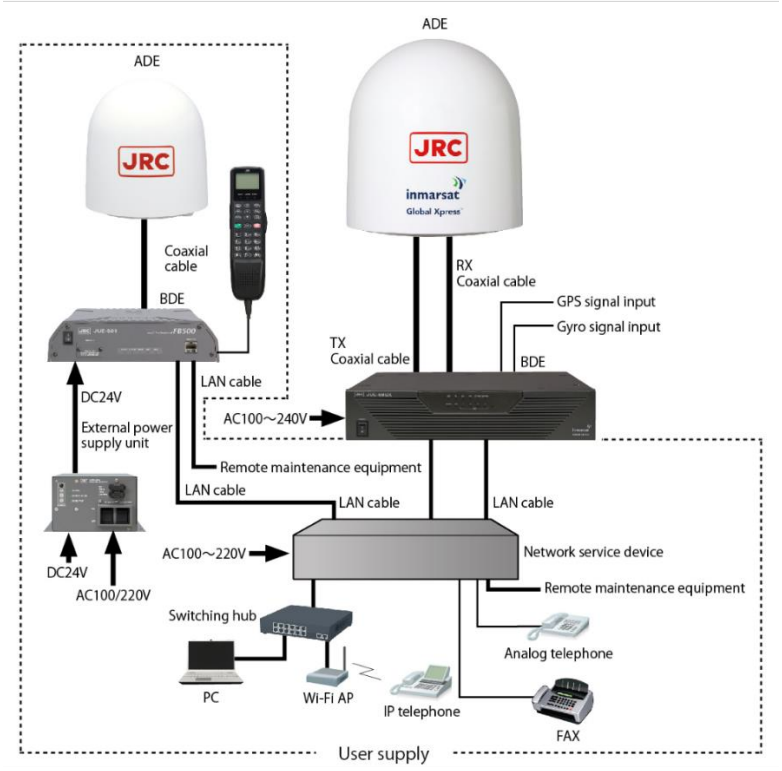
Το Inmarsat, είναι ένα δορυφορικό σύστημα το οποί απαρτίζεται από ένα υποσύνολο δορυφορικών υπηρεσιών , κάθε μία εξ αυτών προϋποθέτει τον ανάλογο πομποδέκτη για την επικοινωνία με το δίκτυο των γεωστατικών δορυφόρων, τον Mobile Earth Station (MES). Η συνολική επιφάνεια που καλύπτει ο Inmarsat δορυφόρος στην επιφάνεια των ωκεανών είναι από πλάτος 70° Βόρεια έως 70° Νότια (βλ. Εικόνα 2). Το σύστημα αποτελείται από την τρίτη γενιά δορυφόρων, ενώ ο πρώτός δορυφόρος της τέταρτης γενιάς είναι ήδη δρομολογημένος. Θα είναι σε θέση να προσφέρει ευρυζωνικές υπηρεσίες 3G και 4G στους χρήστες. [51]



Εικόνα 2 : Παγκόσμια κάλυψη γεωστατικών δορυφόρων INMARSAT

1.2.2.1 Inmarsat A

Η παροχή υπηρεσιών ξεκίνησε το 1982. Η κεραία είχε την δυνατότητα να παρέχει τηλετυπική, τηλεφωνική, τηλεομοιοτυπική επικοινωνία (φαξ) και μεταγωγή δεδομένων. Είναι τα πρώτα προϊόντα που προώθησε ο Inmarsat με μεγάλη απήχηση . Αυτό είχε ως αποτέλεσμα μεγάλος αριθμός συσκευών να είναι εγκατεστημένος σε πολλά εμπορικά πλοία. Το μοντέλο Α (βλ. Εικόνα 3) χρησιμοποιεί διαμόρφωση FM για τηλεφωνία και PSK (Phase Shift Keying) για 20 τηλέτυπα. Λόγω του παραπάνω τρόπου διαμόρφωσης, το πλάτος των καναλιών που χρησιμοποιούνται είναι μεγάλο (25 kc/s). Αναφορικά με την στενότητα της περιοχής συχνοτήτων που έχει εκχωρηθεί στις επικοινωνίες και με την εκθετική μορφή αύξησης των συσκευών του πλοίου , δημιουργήθηκε η ανάγκη διεύρυνσης των διατιθέμενων καναλιών για την εξυπηρέτηση των ναυτιλιακών αναγκών. Σαν λύση του παραπάνω προβλήματος θα μπορούσαμε να θέσουμε την μείωση του εύρους του καναλιού. Για να επιτευχθεί το παραπάνω θα πρέπει να εκτελεστεί διαφορετική τεχνική όπου καταλήγουμε σε διαφορετικού τύπου συσκευή. Συνεπώς, ο Inmarsat υποδέχτηκε το επόμενο μοντέλο της συσκευής, αλλά θα παρέχει υποστήριξη τύπου Α για αρκετά χρόνια ακόμα. [63]



Εικόνα 3: Τεχνικά Χαρακτηριστικά Inmarsat A

1.2.2.2 Inmarsat B

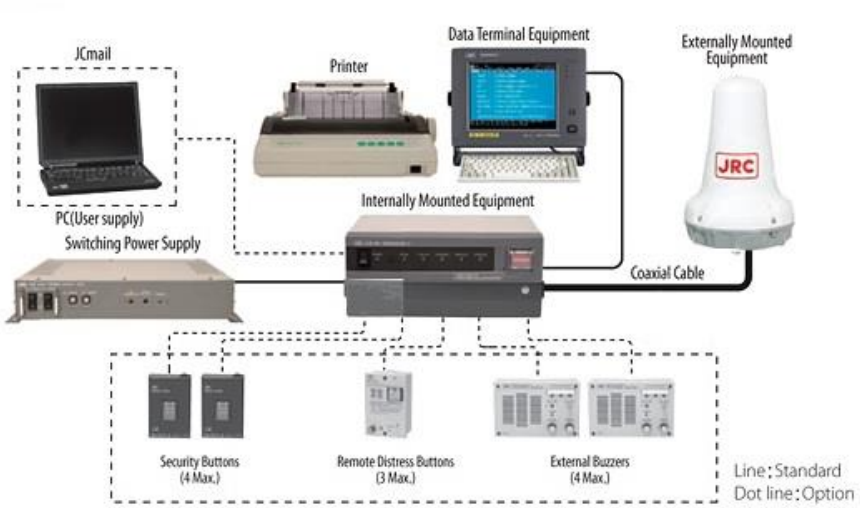
Ο διάδοχος του τύπου Α ήρθε κάποια χρόνια μετά και άρχισε η εφαρμογή του περίπου το 1994, με την ονομασία Inmarsat B (βλ. Εικόνα 4). Οι δυνατότητες παροχής τηλεπικοινωνιακών υπηρεσιών είναι ίδιες με τον προκάτοχο του, με βασικό πλεονέκτημα όμως ότι απαιτεί μικρότερο εύρος καναλιού (περίπου 10 IχΑ). Αυτό είχε ως αποτέλεσμα της καλύτερη δυνατή αξιοποίηση του φάσματος συχνοτήτων που διατίθενται.

Με την χρήση νέων τρόπων διαμόρφωσης είναι δυνατή η παροχή περισσότερων υπηρεσιών. Το κόστος προμήθειας της συσκευής είναι περίπου ίδιο με τον τύπο Α αλλά το τηλεπικοινωνιακό κόστος είναι μικρότερο χάριν των πλεονεκτημάτων που προαναφέρθηκαν. Αναφορικά με την εγκατάσταση του εξοπλισμού δεν παρατηρήθηκαν μεγάλες διαφορές στις διαστάσεις της κεραίας. Η συσκευή διατίθεται σε εκδόσεις απλών και πολλαπλών διαύλων. [64]

Εικόνα 4: Inmarsat B

1.2.2.3 Inmarsat C

Το Inmarsat-C (βλ. Εικόνα 5) έγινε πλήρως λειτουργικό μετά από μια περίοδο προ-επιχειρησιακών δοκιμών τον Ιανουάριο του 1991. Είναι μια αμφίδρομη υπηρεσία πακέτων δεδομένων η οποία λειτουργεί μεταξύ κινητών επίγειων σταθμών (MES) και επίγειων σταθμών επίγειας (LES). Τα πλεονεκτήματα του Inmarsat-C σε σύγκριση με το Inmarsat-A είναι το χαμηλό κόστος, το μικρότερο μέγεθος και ότι χρησιμοποιεί μια μικρότερη πανκατευθυντική κεραία. Το μειονέκτημα είναι ότι η φωνητική επικοινωνία δεν είναι δυνατή με το Inmarsat-C. Η υπηρεσία έχει εγκριθεί για χρήση στο πλαίσιο του Παγκόσμιου Συστήματος Θαλάσσιας Κινδύνου και Ασφάλειας (GMDSS), πληροί τις απαιτήσεις για Συστήματα Προειδοποίησης Ασφάλειας Πλοίων (SSAS) που ορίζονται από τον Διεθνή Ναυτιλιακό Οργανισμό (IMO) και είναι η πιο ευρέως χρησιμοποιούμενη υπηρεσία στα συστήματα παρακολούθησης αλιευτικών σκαφών (VMS). [62] [63]



Εικόνα 5: Υπηρεσίες Inmarsat C

1) EGC-Enhanced Group Call. Η υπηρεσία αυτή, προσφέρει σε εγκεκριμένους χρήστες να καλούν ομάδες πλοίων. Ως ομάδες πλοίων ορίζονται πλοία συγκεκριμένης γεωγραφικής θέσης ή συνόλου. Δύο υπηρεσίες είναι ήδη σε ισχύ:

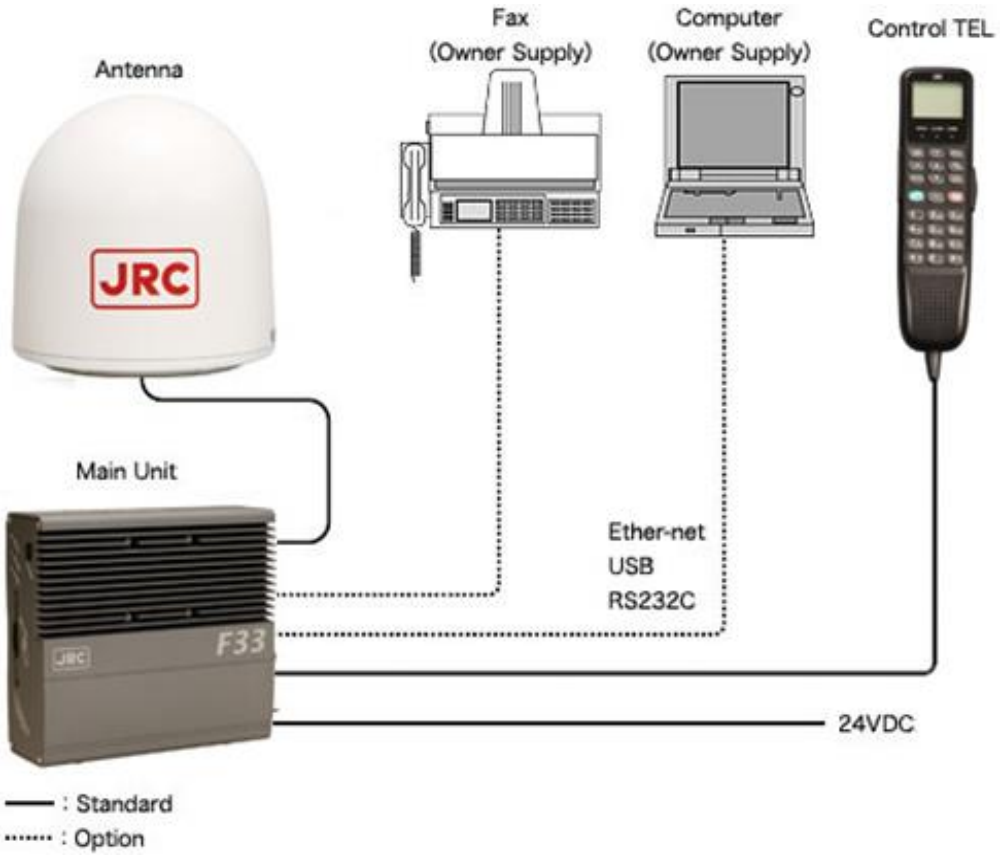
- SafetyNet για την αποστολή μηνυμάτων στα πλοία ναυτικής ασφαλείας (MSI), π.χ. ακραία καιρικά φαινόμενα ή περιπτώσεις κινδύνου κ.α.
- FleetNet, για την αποστολή μηνυμάτων εμπορικής φύσεως.

2) Ηλεκτρονικό Ταχυδρομείο (E-mail)

3) Επικοινωνίες Κινδύνου

1.2.2.4 Inmarsat Fleet 33

Το σύστημα Inmarsat Fleet 33 (βλ. Εικόνα 6) (3ης γενιάς), κάνει είσοδο στον χώρο των δορυφορικών συστημάτων προσφέροντας υπηρεσίες e-mail, web και Internet Access. Οι υπηρεσίες που προσφέρει είναι φωνής, Fax και Data και την υπηρεσία Mobile Packet Data Service (MPDS), η οποία επιτρέπει την σύνδεση στο διαδίκτυο μέσω του IP δικτύου. Η MPDS υπηρεσία έχει διαφορετική ταχύτητα για την λήψη δεδομένων από την ταχύτητα της αποστολής δεδομένων. Η ταχύτητα λήψης φτάνει τα 64 kbps, ενώ η ταχύτητα αποστολής δεδομένων τα 28 kpbs. Η διαφροά αυτή έγκειται στον αυξημένο όγκο που έχουν τα δεδομένα όταν στέλνονται στο διαδίκτυο έναντι αυτών που λαμβάνονται. [63]



Εικόνα 6: Διαμόρφωση Inmarsat Fleet 33

Ο παραπάνω εξοπλισμός είναι ειδικά σχεδιασμένος για την κάλυψη των αναγκών στο στον τομέα της αναψυχής και των τηλεπικοινωνιών, παρέχοντας κεραία μικρής διαμέτρου, φιλικό προς την χρήση με εύκολη εγκατάσταση. Επιπλέον, το Inmarsat Fleet 33 αποτελεί την βέλτιστη λύση για την επικοινωνία των πληρωμάτων της ναυτιλίας (φωνή, email, SMS) αποτελώντας συμπλήρωμα του συστήματος Inmarsat Fleet 77 ή του Inmarsat FleetBroadband. Στην συνέχεια παρατίθενται τεχνικές λεπτομέρειες αναφορικά με την ταχύτητα αποστολής δεδομένων αλλά και των πλεονεκτημάτων του.

Παγκόσμιας κάλυψης παρέχοντας:

- Υπηρεσία φωνής 4.8 kbps
- Υπηρεσία Fax 9.6 kbps
- Υπηρεσία data 9.6 kbps
- Mobile Packet Data Service (MPDS)

Πλεονεκτήματα συστήματος:

- Συνεχής σύνδεση στο διαδίκτυά με την υπηρεσία MPDS
- Εξοπλισμό υψηλής αντοχής
- Παγκόσμια κάλυψη
- Εμπλουτισμένα χαρακτηριστικά ασφαλείας
- Ευελιξία
- Ανταγωνιστικά τηλεπικοινωνιακά τέλη
- Πλήρης προσαρμογή στους διεθνείς κανόνες της ναυτιλίας
- Αξιοπιστία

1.2.2.5 Inmarsat Fleet 77

Το Inmarsat Fleet 77 (βλ. Εικόνα 7), είναι παλιάς τεχνολογίας υπηρεσία δορυφορικής επικοινωνίας. Βασικό χαρακτηριστικό του είναι η αξιοποίηση των υφιστάμενων τεχνολογικών υποδομών καλύπτοντας όλες τις τηλεπικοινωνιακές ανάγκες που προκύπτουν. Με τον συνδυασμό όλων των τεχνολογικών εφαρμογών που ήδη υπάρχουν και με την προσθήκη νέων τεχνολογιών ανταποκρίνεται επάξια στις απαιτήσεις των σύγχρονων επιχειρηματικών μοντέλων. Εκτός των υπηρεσιών φωνής και e-mail που έχουν προαναφερθεί, προσφέρει την υπηρεσία μεταφοράς ηλεκτρονικών αρχείων ήχου και εικόνας σε ταχύτητες 128 ή 64 kbps. Το επιπλέον βασικό χαρακτηριστικό του συστήματος, είναι η 24ωρη πρόσβαση που παρέχει στο διαδίκτυο με χρέωση αναλογική της χρήσης. Το σύστημα Inmarsat Fleet 77 καλύπτει τις προδιαγραφές του International Maritime Organisation (IMO) δίνοντας την σκυτάλη σε νέα τεχνολογικά ευρήματα τα οποία εισάγονται στο παγκόσμιο σύστημα ασφάλειας στη θάλασσα (GMDSS), προσφέροντας εξασφάλιση επικοινωνίας με τερματισμό, αν χρειασθεί, μιας κανονικής κλήσης (prioritisation and pre-emption). [62]

Εικόνα 7: Inmarsat Fleet 77

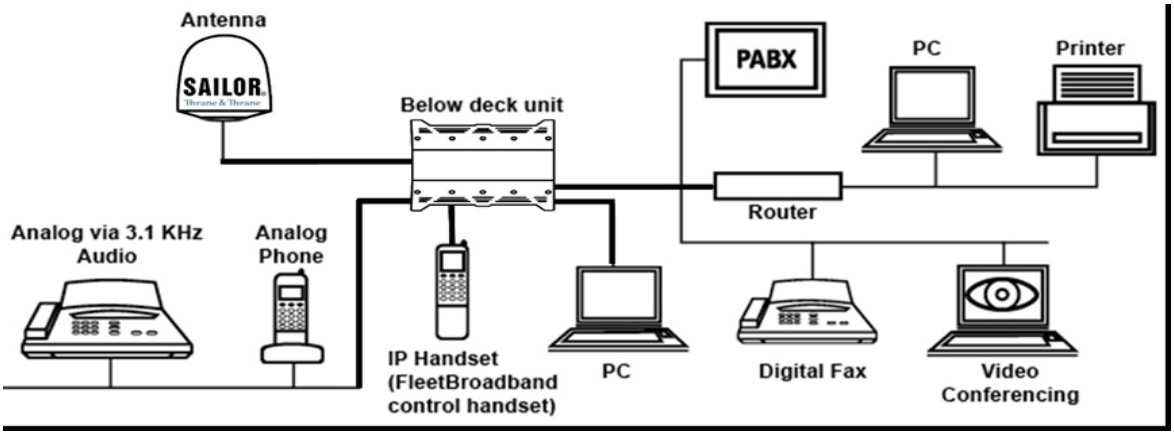
1.2.2.6 Fleet Broadband

Το δίκτυο Fleet Broadband αναπτύχθηκε από την Inmarsat και αποτελείται από τρεις γεωσύγχρονους δορυφόρους σε τροχιά που ονομάζονται I-4 και επιτρέπουν συνεχή παγκόσμια κάλυψη, εκτός από τους πόλους. Τα συστήματα Fleet Broadband (βλ. Εικόνα 8) που είναι εγκατεστημένα σε πλοία μπορούν να ταξιδεύουν από ωκεανό σε ωκεανό χωρίς ανθρώπινη αλληλεπίδραση. Εάν υπάρχει οπτική επαφή με έναν από τους τρεις δορυφόρους I-4, τότε μπορεί να επιτευχθεί συνδεσιμότητα, ακόμη και σε θαλασσοταραχές. Δεδομένου ότι το δίκτυο Fleet Broadband χρησιμοποιεί τη ζώνη L, η εξασθένιση της βροχής είναι πολύ λιγότερο πρόβλημα από τα μεγαλύτερα συστήματα VSAT Ku band ή C Band. Δυνατότητες του Fleet Broadband: [62]

- Standard IP για e-mail, Internet και Intranet πρόσβαση μέσω ασφαλούς VPN σύνδεσης με ταχύτητα έως και 432 kbps.
- Streaming IP για εγγυημένες ταχύτητες μεταφοράς δεδομένων, κατόπιν αίτησης, μέχρι και 256 kbps. Η ταχύτητα επιλέγεται ανά περίπτωση ανάλογα με τις απαιτήσεις της εκάστοτε εφαρμογής.
- Επικοινωνία Φωνής με δυνατότητα ταυτόχρονής μεταφοράς δεδομένων
- Επικοινωνία Fax υποστηρίζοντας Group 3 Fax μέσω του καναλιού φωνής

Πλεονεκτήματα του Fleet Broadband:

- Υψηλή ποιότητα και ταχύτητα επικοινωνίας
- Ταυτόχρονη επικοινωνία φωνής και δεδομένων
- Πλήρης Ασφάλεια
- Αξιόπιστος, φορητός και εύκολος στην εγκατάσταση τερματικός εξοπλισμός



Εικόνα 8: Διαμόρφωση δικτύου με FleetBoard

1.2.2.7 FleetXpress

Το μοντέλο που λανσάρει τον τελευταίο καιρό ο INMARSAT είναι το FleetXpress (FX) (βλ. Εικόνα 9) με συνδυασμό GX κεραίας και Fleetbroadband 500 μέσω της Ka-Band και της L-Band. Η ναυτιλιακή εταιρία που θα επιλέξει να εγκαταστήσει στα πλοία της αυτή την νέα τεχνολογία θα επωφεληθεί από το μεγάλο bandwidth το οποίο μπορεί να προσαρμοστεί βάσει των αναγκών κάθε πελάτη.

Το Fleet Xpress προσφέρεται μέσω του παγκόσμιου δορυφορικού δικτύου GX (Global Xpress) και Inmarsat-4 (AlphaSat) αυτό έχει ως αποτέλεσμα να μην υπάρχει εναλλαγή μεταξύ παρόχων δορυφόρων, επιτρέποντας την πλήρη βελτιστοποίηση των υπηρεσιών σε ολόκληρο το δίκτυο. Η ισχύς του σήματος δεν εξαρτάται από το μέγεθος της κεραίας, επιτρέποντας μια μικρότερη κεραία σε σύγκριση με μια αντίστοιχη υπηρεσία Ku. Η διπλή δομή επίγειου σταθμού, διασφαλίζει ότι το δίκτυο είναι πλήρως στιβαρό και πάντα διαθέσιμο. Κάθε δορυφόρος χρησιμοποιεί δύο τηλεμεταφορές, που βρίσκονται σε ξεχωριστές περιοχές, για να αποφευχθούν διακοπές της υπηρεσίας που προκαλούνται από καιρικά φαινόμενα . [62]

Εικόνα 9: Απεικόνιση FleetXpress

Τα πλεονεκτήματα που θα ήθελε να βρει μια ναυτιλιακή εταιρεία γεννιούνται από τις ανάγκες της . Ο πλοιοκτήτης και οι διαχειριστές των πλοίων χρειάζονται την συνεχή συνδεσιμότητα, την εγγύτητα της απόδοσης του εξοπλισμού και της επίγειας κάλυψης , την όσο το δυνατόν ελεγχόμενη κοστολόγηση των υπηρεσιών , την δυνατότητα προσθήκης και κάλυψης μελλοντικών αναγκών π.χ. IOT , κάμερες ασφαλείας κλπ. , καθώς και την παροχή βέλτιστων υπηρεσιών επικοινωνίας και ψυχαγωγίας του πληρώματος.

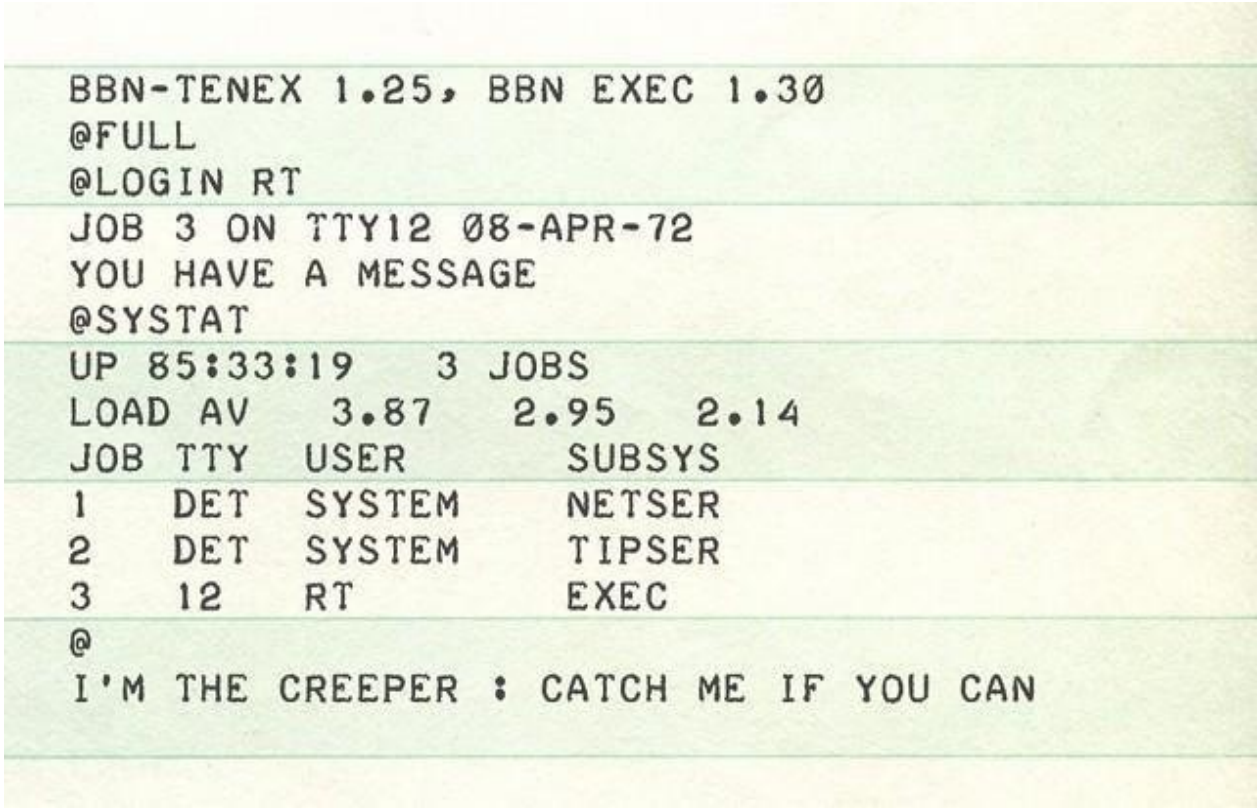
1.2.3 Η ιστορία της κυβερνοασφάλειας

Η επίκληση του cybersecurity δεν ήταν πάντοτε επιτακτική. Η ανάγκη δημιουργήθηκε παράλληλα με την ραγδαία εξέλιξη της τεχνολογίας και ειδικότερα την περίοδο της δεκαετίας του 40'. Η απειλή των υπολογιστών, της εποχής εκείνης, ήταν σχεδόν ανύπαρκτη, καθώς ο αριθμός των ατόμων που είχαν πρόσβαση σε αυτούς ήταν περιορισμένος και οι υπολογιστές δεν ήταν δια δικτυωμένοι. Παρόλα αυτά, ο πρώτος ιός έκανε την εμφάνιση του το 1949 και είχε ως αίτιο την αναπαραγωγή προγραμμάτων στον υπολογιστή που πρόσβαλε.

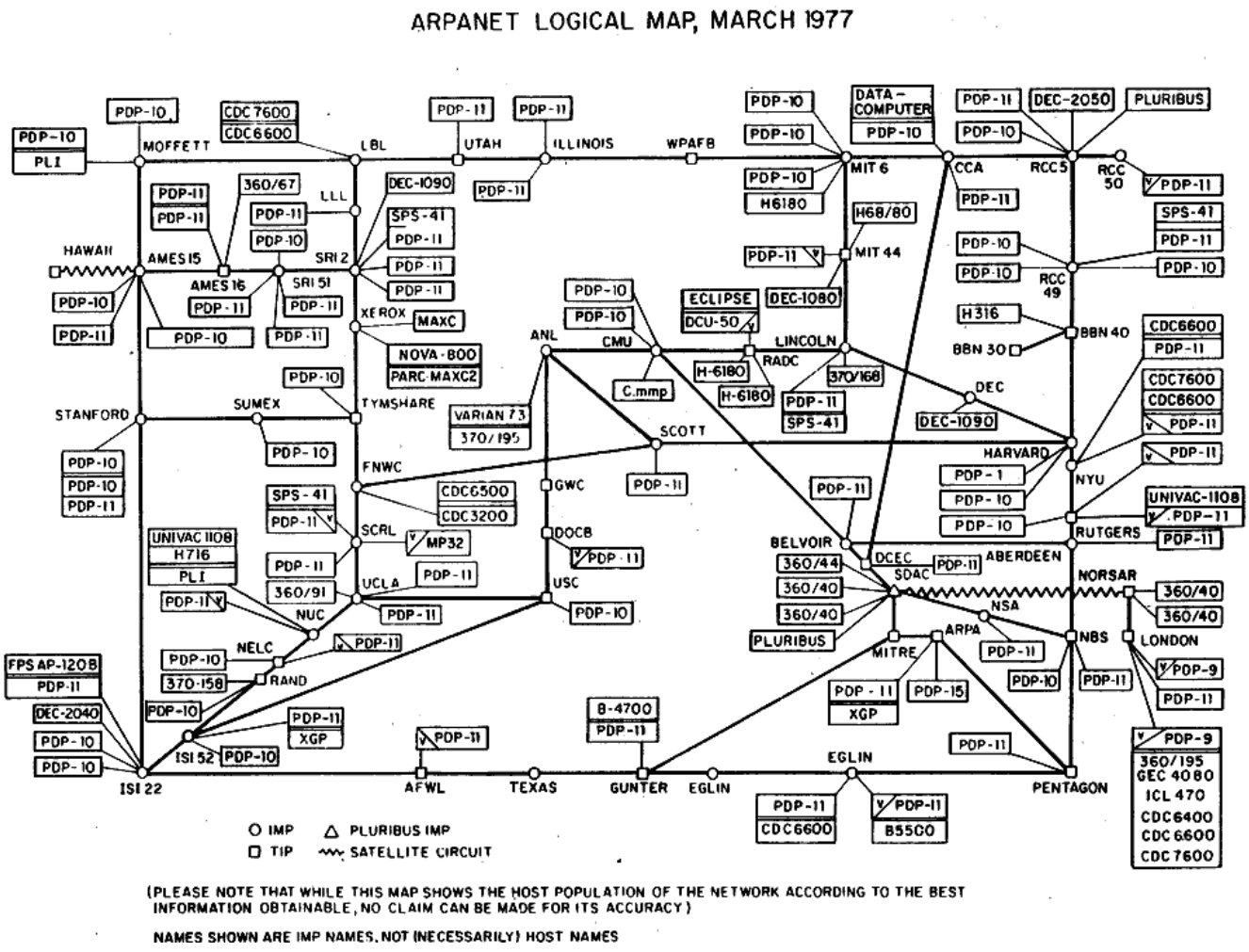
Για την ιστορία, το Hacking δεν σταματούσε στα υπολογιστικά συστήματα μόνο. Στα τέλη του 1950, εμφανίστηκε το "τηλεφωνικό phreaking". Άνθρωποι και κυρίως μηχανικοί του χώρου των τηλεπικοινωνιών παραβίαζαν τα πρωτόκολλα των εκάστοτε εταιριών κινητής τηλεφωνίας προς αποφυγή χρεώσεων στις τηλεφωνικές τους κλήσεις. Εκείνη την περίοδο, οι μεγάλοι κολοσσοί είχαν προβληματιστεί ιδιαίτερα με το φαινόμενο που επικρατούσε και αδυνατούσαν να το αντιμετωπίσουν, κάτι που συνέβη 30 χρόνια μετά.

Το πρώτο κακόβουλο hacking (βλ. Εικόνα 10) δημοσιεύτηκε επισήμως στην εφημερίδα Ινστιτούτου Τεχνολογίας της Μασαχουσέτης. Το 1960, οι υπολογιστές είχαν ακόμη μεγάλο μέγεθος και ήταν κλειδωμένοι σε ασφαλή δωμάτια με περιορισμένη πρόσβαση στο ανθρώπινο δυναμικό. Ωστόσο, επιθέσεις υπήρξαν εκ των έσω μη έχοντα εμπορικό ή γεωπολιτικό όφελος. Το hacking αποσκοπούσε στην βελτιστοποίηση του συστήματος. Η IBM, για πρώτη φορά εφαρμόζει το Ethical hacking, το οποίο υφίσταται μέχρι και σήμερα, καλώντας τους νέους μαθητές να δοκιμάσουν τους νέους τους υπολογιστές στο σύστημα τους. Η IBM αναγνώρισε τα ευάλωτα σημεία του συστήματος δίνοντας πρόσβαση στα παιδία να εμβαθύνουν σε αυτό. Στην πάροδο των χρόνων, οι υπολογιστές μειώθηκαν σε μέγεθος και κόστος, και οι εταιρείες επένδυαν περισσότερο στην αποθήκευση και διαχείριση των δεδομένων καθιστώντας απαραίτητο την ασφάλεια μόνο του συστήματος, κάτι που πραγματοποιήθηκε με κωδικούς πρόσβασης. [21]

Η Κυβερνοασφάλεια ξεκίνησε το 1972 με το ερευνητικό πρόγραμμα του APRANET (The Advanced Research Projects Agency Network), έναν προτεστάντη του διαδικτύου. Ο τότε ερευνητής, Bob Thomas, έφτιαξε ένα πρόγραμμα με το όνομα Creeper, το οποίο περνούσε μέσα στο δίκτυο του APRANET (βλ. Εικόνα 11) και άφηνε ένα μήνυμα " I'm the creeper, catch me if you can". Ο εφευρέτης τότε του email, Ray Tomlinson, έφτιαξε ένα antivirus πρόγραμμα, το πρώτο στην ιστορία, με το όνομα Reaper για την εξάλειψη του ιού. Στα μέσα των 70s, η Κυβερνοασφάλεια ωρίμαζε και έμπαινε δυναμικότερα στα λειτουργικά συστήματα OS. [21]

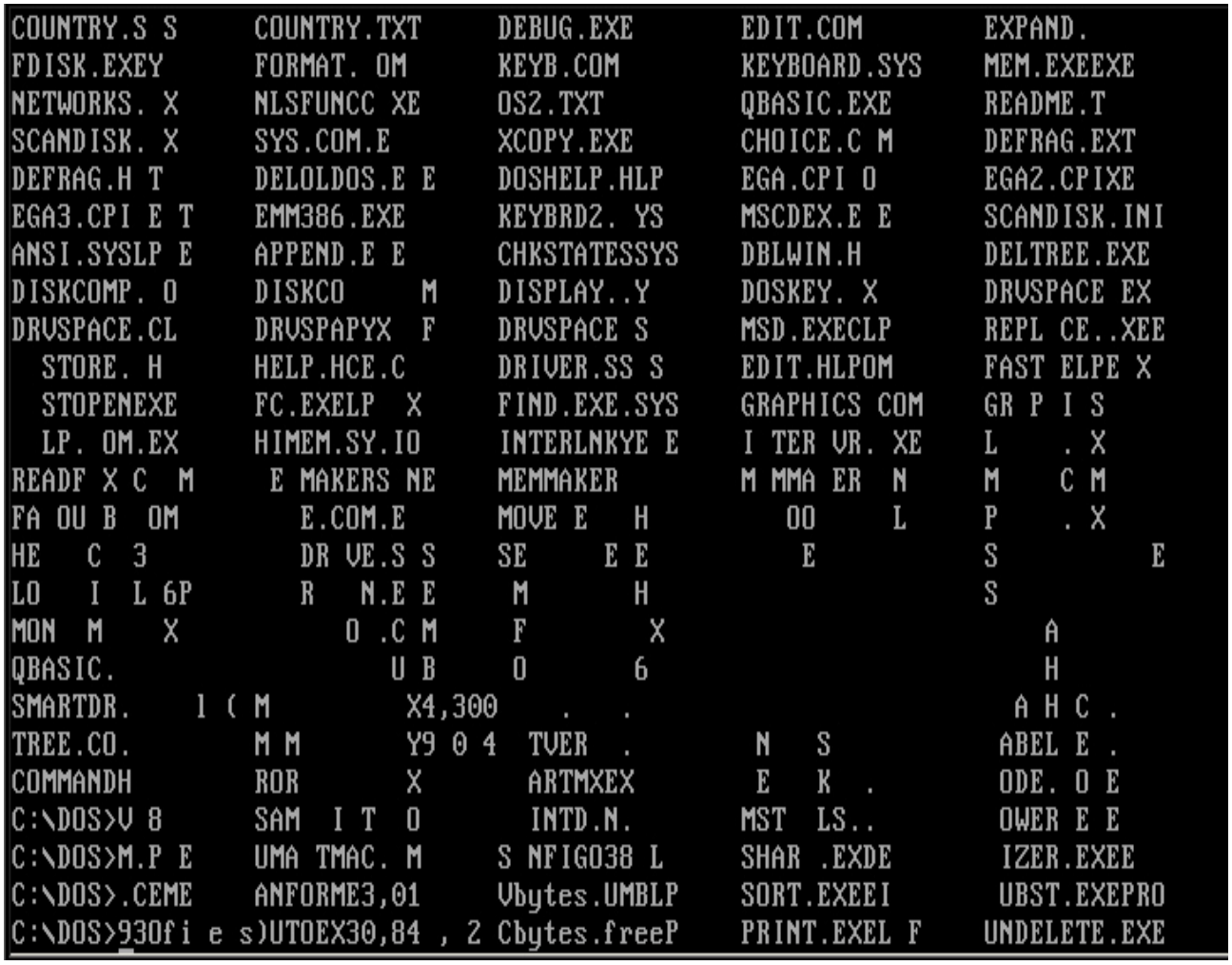


Εικόνα 10: Creeper program το πρώτο καταγεγραμμένο κακόβουλο πρόγραμμα



Εικόνα 11: logical map του Apranet

Η δεκαετία των 80s, καταφθάνει με αυξημένη σειρά επιθέσεων υψηλού προφίλ, συμπεριλαμβανομένων των National CSS, AT&T και το εθνικό εργαστήριο του Los Alamos. Το 1983, χρησιμοποιείται για πρώτη φορά ο όρος του Trojan Horse και Computer Virus. Το 1985, το Υπουργείο Άμυνας των ΗΠΑ αξιολογεί τα κριτήρια ενός αξιόπιστου συστήματος υπολογιστών, θέτοντας ένα πρωτόκολλο με τις προδιαγραφές που πρέπει να εμπεριέχονται σε ένα σύστημα. Το 1986, μία επίθεση πρόσβαλε 400 υπολογιστές του στρατού δημιουργώντας αμφιβολίες για την φερεγγυότητα της ασφάλειας. Το 1987, δημιουργούνται τα πρώτα εμπορικά Antivirus. Το UVK, το NOD και το McAfee. Την ίδια χρονιά, έκανε την εμφάνιση του και το κρυπτογραφημένο Cascade Virus (βλ. Εικόνα 12), δημιουργώντας ποικίλα προβλήματα στην IBM.



Εικόνα 12: Ο κρυπτογραφημένο ιός Cascade Virus

1.2.3.1 Cascade virus

Ο κόσμος σιγά σιγά αντιλαμβανόταν την σοβαρότητα που αντιμετώπιζε με τους ιούς των υπολογιστών και κλήθηκε να πάρει σοβαρότερα μέτρα. Αργότερα την χρονιά του 1988, δημιουργήθηκε το πρώτο φόρουμ αφιερωμένο στην ασφάλεια κατά των ιών με την ονομασία Virus L και εμφανίστηκε στο δίκτυο Usenet.

Την δεκαετία του 1990, ο κόσμος ”συνδέεται” online. Ο πρώτος πολυμορφικός ιός δημιουργείται (του οποίου ο κώδικας αποτρέπει την ανίχνευση). Επιπλέον την ίδια δεκαετία εδραιώνεται το EICAR (European Institute for Computer Antivirus Research). Τα antivirus που χρησιμοποιήθηκαν για τις απειλές εκείνες, κατανάλωναν μεγάλη υπολογιστική ισχύς με αποτέλεσμα να κάνουν τους υπολογιστές αργούς. Από το 1996 και ύστερα, οι ιοί εξέλισσαν τις μεθόδους και τεχνικές τους δυσκολεύοντας όλο και περισσότερο τους προγραμματιστές στο να αντιμετωπιστούν. Ένα ερευνητής της NASA, αναπτύσσει το πρώτο firewall πρόγραμμα, προς αποφυγή της διασποράς των ιών.

Στα τέλη των 90s, τα email πολλαπλασιάζονταν υποσχόμενα να φέρουν την επανάστασή στην επικοινωνία. Συνέπεια αυτής της ανάπτυξης, ήταν να δημιουργηθεί και ένα καινούριο σημείο εισόδου για τους ιούς.

Με την αλλαγή της χιλιετίας, το διαδίκτυο και οι υπολογιστές ήταν διαθέσιμα σχεδόν στα περισσότερα σπίτια και γραφεία σε όλο τον κόσμο. Τα δεδομένα όλο και περισσότερο διατηρούνταν ψηφιακά, δίνοντας έναυσμα σε κακόβουλους χρήστες να τα υποκλέψουν. Από το 2001 εμφανίζεται ένα νέο είδος ιού, μέσω του οποίου ο χρήστης πλέον δεν χρειαζόταν να “κατεβάσει” κάποιο μολυσματικό αρχείο για να προσβληθεί το σύστημα του, αρκούσε να επισκεφθεί ,μολυσμένο ιστότοπο. “Καθαρές” σελίδες αντικαταστάθηκαν με μολυσμένες, αποκρύπτοντας κακόβουλο λογισμικό από τους επισκέπτες. Συνοψίζοντας, το 2000 διατίθεται η πρώτη μηχανή προστασίας από ιούς ανοικτού κώδικα Open Antivirus Project. Εν συνεχεία, το 2001, κυκλοφορεί το ClamAV η πρώτη μηχανή προστασίας από ιούς ανοικτού κώδικα η οποία διατίθεται στο εμπόριο. Την ίδια χρονιά η Avast κυκλοφορεί δωρεάν λογισμικό προστασίας από ιούς στο εμπόριο. Μέσα στα επόμενα 5 χρόνια είχε πάνω από 20 εκατομμύρια χρήστες. Το βασικότερο πρόβλημα των antivirus ήταν οι επιβραδύνσεις που δημιουργούσαν στους υπολογιστές λόγω της βαρύτητας τους. Μία πρώτη λύση ήταν να μετακινηθεί το λογισμικό από τον υπολογιστή στο cloud για να λειτουργεί ταχύτερα το σύστημα. Την παραπάνω καινοτομία ανέπτυξε η Panda Security το 2007 και εν συνεχεία το παράδειγμα ακολούθησε η McAfee Labs το 2008, προσθέτοντας την λειτουργία

VirusScan. Με τον πολλαπλασιασμό των smartphones, αναπτύχθηκε antivirus και για Android και Windows κινητά.

Την δεκαετία του 2010, σημειώθηκαν πολλές παραβιάσεις και επιθέσεις υψηλού προφίλ επηρεάζοντας την εθνική ασφάλεια των χωρών. Το 2012, ο χάκερ 0X0MAR δημοσιεύει περισσότερες από 400.000 πιστωτικές κάρτες στο διαδίκτυο. Το 2013, πρώην υπάλληλος ης CIA αντέγραψε και διέρρευσε απόρρητες πληροφορίες από την NSA (National Security Agency). Το 2014, κακόβουλοι χάκερ εισβάλλουν στο Yahoo, θέτοντας σε κίνδυνο τους λογαριασμούς και τα προσωπικά δεδομένα 3 δισεκατομμυρίων χρηστών. Το 2017, το Wannacry ransomware, μολύνει 230.000 υπολογιστές σε μία ημέρα. Δύο χρόνια αργότερα το 2019, πολλαπλές επιθέσεις DDos ανάγκασαν το χρηματιστήριο της Νέα Ζηλανδίας να κλείσει προσωρινά. Καθώς η Κυβερνοασφάλεια αναπτύχθηκε για να αντιμετωπίσει το διευρυμένο φάσμα των τύπων επιθέσεων, οι εγκληματίες ανταποκρίθηκαν με τις δικές τους καινοτομίες. Οι εισβολείς γίνονταν πιο έξυπνοι και τα προγράμματα προστασίας από ιούς αναγκάστηκαν να απομακρυνθούν από τις συνηθισμένες μεθόδους ανίχνευσης. Η Κυβερνοασφάλεια επόμενης γενιάς χρησιμοποιεί διαφορετικές προσεγγίσεις για να αυξήσει τον εντοπισμό νέων και πρωτόγνωρων απειλών. Ένα τυπικό antivirus περιλαμβάνει:

- Multi-factor authentication (MFA)
- Network Behavioural Analysis (NBA)
- Threat intelligence and update automation
- Real-time protection
- Sandboxing – creating an isolated test environment where you can execute a suspicious file or URL
- Forensics – replaying attacks to help security teams better mitigate future breaches
- Back-up and mirroring
- Web application firewalls (WAF)

Οι απειλές παρουσιάζονται από κακόβουλες ενέργειες (π.χ. παραβίαση ή εισαγωγή κακόβουλου λογισμικού) ή τις ακούσιες συνέπειες καλοήθων ενεργειών (π.χ. συντήρηση λογισμικού ή χρήστη άδειες). Γενικά, αυτές οι ενέργειες εκθέτουν τρωτά σημεία (π.χ. απαρχαιωμένο λογισμικό ή αναποτελεσματικά τείχη προστασίας) ή εκμεταλλεύονται μια ευπάθεια στη λειτουργική τεχνολογία ή την τεχνολογία πληροφοριών. [21]

1.3 Οδηγία του παγκόσμιου οργασμού ναυσιπλοΐας σχετικά με την κυβερνοασφάλεια (IMO).

Με απόφαση του Διεθνούς Ναυτιλιακού Οργανισμού (IMO), το αργότερο μέχρι τον πρώτο ετήσιο έλεγχο Συμμόρφωσης ενός πλοίου μετά την 1η Ιανουαρίου 2021, κάθε Σύστημα Διαχείρισης Ασφάλειας πρέπει να τεκμηριώνεται ότι περιλαμβάνει διαχείριση κινδύνων στον κυβερνοχώρο, σύμφωνα με τον Διεθνή Κώδικα Διαχείρισης Ασφάλειας. Η Επιτροπή Ναυτικής Ασφάλειας (MSC) ενέκρινε τον Ιούνιο του 2017 το ψήφισμα MSC.428 (98) για τη διαχείριση του θαλάσσιου κυβερνοχώρου και τα συστήματα ασφαλείας. Σύμφωνα με τους στόχους και τις απαιτήσεις του Κώδικα ISM (βλ. Εικόνα 13), ένα σύστημα ασφαλείας οφείλει να λαμβάνει υπόψιν την διαχείριση κινδύνου στον τομέα του κυβερνοχώρου. [26] [6] [7]

Εικόνα 13: Βήματα Συμμόρφωσης με τον IMO

Ο στόχος της διαχείρισης κινδύνων στον κυβερνοχώρο στην ναυτιλία είναι να υποστηρίξει την ασφαλή ναυσιπλοΐα η οποία να είναι επιχειρησιακά ανθεκτική σε κινδύνους στον κυβερνοχώρο.

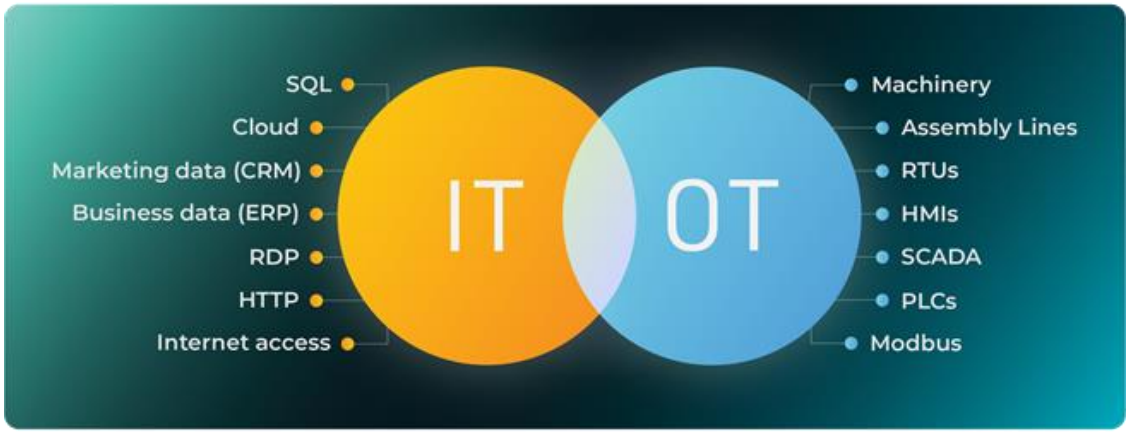
Οι κυβερνοτεχνολογίες έχουν καταστεί ουσιαστικές για τη λειτουργία και τη διαχείριση τους. Πολυάριθμα συστήματα ζωτικής σημασίας λειτουργούν ακατάπαυστα για την ασφάλεια και την ασφάλεια της ναυτιλίας και την προστασία του ναυτικού περιβάλλοντος. [29] [27] [23]

Σε ορισμένες περιπτώσεις, αυτά τα συστήματα πρέπει να συμμορφώνονται με τα διεθνή πρότυπα και τις απαιτήσεις της διαχειρίστριας σημαίας. Ωστόσο, τα τρωτά σημεία που δημιουργούνται από την πρόσβαση, η διασύνδεση ή η δικτύωση αυτών των συστημάτων μπορεί να οδηγήσει σε κινδύνους στον κυβερνοχώρο που θα έπρεπε να απευθύνεται. Τα ευάλωτα συστήματα περιλαμβάνουν:

- Συστήματα γέφυρας.
- Συστήματα διακίνησης και διαχείρισης φορτίου.
- Συστήματα διαχείρισης πρόωσης και μηχανημάτων και ελέγχου ισχύος.
- Συστήματα ελέγχου πρόσβασης.
- Συστήματα εξυπηρέτησης και διαχείρισης επιβατών.
- Συστήματα ευημερίας του πληρώματος.
- Διοικητικά συστήματα.
- Συστήματα επικοινωνίας.

Η διάκριση μεταξύ πληροφορικής και λειτουργικών συστημάτων τεχνολογίας θα πρέπει να ληφθεί υπόψην (IT vs OT). Τα συστήματα πληροφορικής (IT) μπορεί να θεωρηθούν ότι εστιάζουν στην χρήση δεδομένων ως πληροφορία. Τα συστήματα επιχειρησιακής τεχνολογίας (OT) μπορεί να θεωρηθούν ότι εστιάζουν στη χρήση δεδομένων για τον έλεγχο ή την παρακολούθηση φυσικών διεργασιών. Η επιχειρησιακή τεχνολογία (OT) αναφέρεται στο υλικό και το λογισμικό που χρησιμοποιούνται για την αλλαγή, την παρακολούθηση ή τον έλεγχο φυσικών συσκευών, διαδικασιών και συμβάντων σε μια εταιρεία ή οργανισμό. Αυτή η μορφή τεχνολογίας χρησιμοποιείται πιο συχνά σε βιομηχανικά περιβάλλοντα και οι συσκευές στις οποίες αναφέρεται αυτή η τεχνολογία έχουν συνήθως μεγαλύτερη αυτονομία από τις συσκευές ή τα προγράμματα τεχνολογίας πληροφοριών. Παραδείγματα OT περιλαμβάνουν το SCADA (Supervisory Control and Data Acquisition), το οποίο χρησιμοποιείται για τη συλλογή και ανάλυση δεδομένων σε πραγματικό χρόνο και συχνά χρησιμοποιείται για την παρακολούθηση ή τον έλεγχο εξοπλισμού εγκαταστάσεων. Βιομηχανίες όπως οι τηλεπικοινωνίες, ο έλεγχος αποβλήτων, ο έλεγχος του νερού και η διύλιση πετρελαίου και φυσικού αερίου βασίζονται σε μεγάλο βαθμό στα συστήματα SCADA. Πολλοί τύποι OT βασίζονται σε συσκευές όπως PLC (Programmable Logic Controllers), οι οποίοι λαμβάνουν πληροφορίες από συσκευές εισόδου ή αισθητήρες, επεξεργάζονται τα δεδομένα και εκτελούν συγκεκριμένες εργασίες ή εξάγουν συγκεκριμένες πληροφορίες με βάση προ-

προγραμματισμένες παραμέτρους .Στην περίπτωση της ναυτιλίας το OT βασίζεται σε συσκευές που αλληλοεπιδρούν στην ασφαλή ναυσιπλοΐα (ECDIS, Radar, GPS κ.α.) Εν αντιθέσει, Η τεχνολογία πληροφοριών (IT) αναφέρεται σε οτιδήποτε σχετίζεται με την τεχνολογία υπολογιστών, συμπεριλαμβανομένου του υλικού και του λογισμικού. Το email, για παράδειγμα, εμπίπτει στην ομπρέλα πληροφορικής. Αυτή η μορφή τεχνολογίας είναι λιγότερο συνηθισμένη σε βιομηχανικά περιβάλλοντα, αλλά συχνά αποτελεί την τεχνολογική ραχοκοκαλιά των περισσότερων οργανισμών και εταιρειών. Αυτές οι συσκευές και τα προγράμματα έχουν μικρή αυτονομία και ενημερώνονται συχνά. Η πρόσβαση σε προγράμματα πληροφορικής και σε συνδεδεμένες συσκευές είναι συνήθως λιγότερο περιορισμένη από ό,τι σε συσκευές OT και σε πολλούς, αν όχι σε όλους, τους εργαζόμενους σε έναν οργανισμό μπορεί να παραχωρηθεί πρόσβαση. Η κύρια διαφορά μεταξύ των συσκευών OT και IT είναι ότι οι συσκευές OT ελέγχουν τον φυσικό κόσμο, ενώ τα συστήματα IT διαχειρίζονται δεδομένα (βλ. Εικόνα 14). Επιπλέον, η προστασία τους θα πρέπει να ληφθεί υπόψιν στην ανταλλαγή πληροφοριών και δεδομένων στο πλαίσιο αυτών των συστημάτων. Παρακάτω παρουσιάζεται ένα σχηματικό των δύο αυτών τεχνολογιών και η γκρίζα ζώνη στην οποία συναντιόνται και δουλεύουν σαν μία οντότητα. [24] [25]



Εικόνα 14: Υπηρεσίες IT και OT

Ενώ αυτές οι τεχνολογίες και συστήματα παρέχουν σημαντικά κέρδη αποτελεσματικότητας για την ναυτιλιακή βιομηχανία, παρουσιάζουν επίσης κινδύνους για κρίσιμα συστήματα και διαδικασίες που συνδέονται με την λειτουργία των συστημάτων που αποτελούν αναπόσπαστο μέρος της ναυτιλίας.

Τρωτά σημεία μπορεί να προκύψουν από ανεπάρκειες στο σχεδιασμό, την ενσωμάτωση ή και τη συντήρηση συστημάτων, καθώς και ελλείψεις στην πειθαρχία στον κυβερνοχώρο. Γενικά, όπου τα τρωτά σημεία λειτουργούν και η τεχνολογία πληροφοριών εκτίθενται ή γίνεται αντικείμενο εκμετάλλευσης, είτε άμεσα (π.χ. αδύναμοι κωδικοί πρόσβασης που οδηγούν σε μη εξουσιοδοτημένη πρόσβαση) ή έμμεσα (π.χ. απουσία διαχωρισμού δικτύου), μπορεί να έχει συνέπειες για την ασφάλεια και την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα των πληροφοριών. Επιπρόσθετα, όταν εκτίθενται συστήματα ή πληροφορίες τα οποία μπορούν γίνουν εκμεταλλευύσιμα, υπάρχουνεπιπτώσεις στην ασφάλεια, ιδιαίτερα όταν τα κρίσιμα συστήματα είναι σε κίνδυνο. (π.χ. γέφυρα, συστήματα πλοήγησης ή κύριας πρόωσης)

2. Αρχιτεκτονική Δικτύου Εμπορικού Πλοίου

Από την 1η Ιανουαρίου 2021καθίστανται υποχρεωτική η διαχείριση του κυβερνοεπιχειρησιακού κινδύνου από τον IMO. Η Επιτροπή Ναυτικής Ασφάλειας (MSC) ενέκρινε τον Ιούνιο του 2017 το ψήφισμα MSC.428 (98) για τη διαχείριση του θαλάσσιου κυβερνοχώρου και τα συστήματα ασφαλείας. Το ψήφισμα αναφέρει ότι ένα εγκεκριμένο σύστημα ασφαλείας πρέπει να λαμβάνει υπόψιν τη διαχείριση του κινδύνου του κυβερνοχώρου, σύμφωνα με τους στόχους και τις απαιτήσεις του κώδικα ISM. Οι οδηγίες καθορίζουν τις ακόλουθες ενέργειες που μπορούν να ληφθούν για τη στήριξη της αποτελεσματικής διαχείρισης του κυβερνοχώρου:

- Εντοπισμός των συστημάτων, τα οποία προκαλούν δυσλειτουργίες σε περίπτωσης επιθέσεις.
- Σχεδιασμός προστασίας για την ομαλή λειτουργία των ναυτιλιακών επιχειρήσεων σε περίπτωση επίθεσης..
- Εφαρμογή διαδικασιών και αμυντικών μέσων για την άμεση ανίχνευση και αντιμετώπιση επιθέσεων.
- Εφαρμογή σχεδίων προς αποκατάσταση των επιτιθέμενων συστημάτων που είναι απαραίτητα για την διένεξη επιχειρήσεων.
- Δημιουργία αντιγράφων ασφαλείας τουλάχιστον για τα δεδομένα και συστήματα που είναι απαραίτητα των ναυτιλιακών επιχειρήσεων.

Ο ναυτιλιακός τομέας βρίσκεται πλέον σε μια διαδικασία προσαρμογής στο νέο τεχνολογικό περιβάλλον, απαιτείται από τις τεχνολογίες της πληροφορικής να δημιουργεί, να επεξεργάζεται, να αποθηκεύει τις πληροφορίες και να ενσωματώνει την επιχειρησιακή τεχνολογία (οθόνες, έλεγχος κ.λπ.) με στόχο τη βελτιστοποίηση των διαδικασιών διαχείρισης.

Οι τεχνολογικές αλλαγές εφαρμόζονται από τις ναυτιλιακές εταιρείες πιο αργά σε σύγκριση με άλλους παραγωγικούς τομείς. Ως αποτέλεσμα, ο ναυτιλιακός τομέας να υφίσταται σε μεγάλο βαθμό τους κινδύνους των επιθέσεων στον κυβερνοχώρο. Αυτό ενεργοποίησε πολλές ναυτιλιακές εταιρείες να ασχοληθούν και να επενδύσουν χρόνο , χρήματα και ανθρώπινο δυναμικό στην προσπάθεια τους να δημιουργήσουν ένα «τείχος προστασίας» στις κυβερνοεπιθέσεις. Συνήθως, οι «πειρατές» του διαδικτύου “χτυπάνε” τα γραφεία των ομίλων όμως η κατάσταση μπορεί να ξεφύγει όταν “θύμα” είναι το πλοίο που βρίσκεται εν πλω. Μπορούν να “τυφλώσουν” τα μηχανήματά του και να το αφήσουν “ακυβέρνητο” στη θάλασσα.

Ο αδύναμος κρίκος στην αλυσίδα αυτή είναι οι χρήστες. Η εξασφάλιση ότι το πλήρωμα ενός πλοίου είναι σωστά εκπαιδευμένο και στο κατάλληλο επίπεδο επιφυλακής θα χρειαστεί χρόνο. Ειδικότερα, όταν τα πληρώματα αλλάζουν συχνά κάθε λίγους μήνες. Θα χρειαστεί η εταιρεία να έχει ένα συνεχές πρόγραμμα εκπαίδευσης.

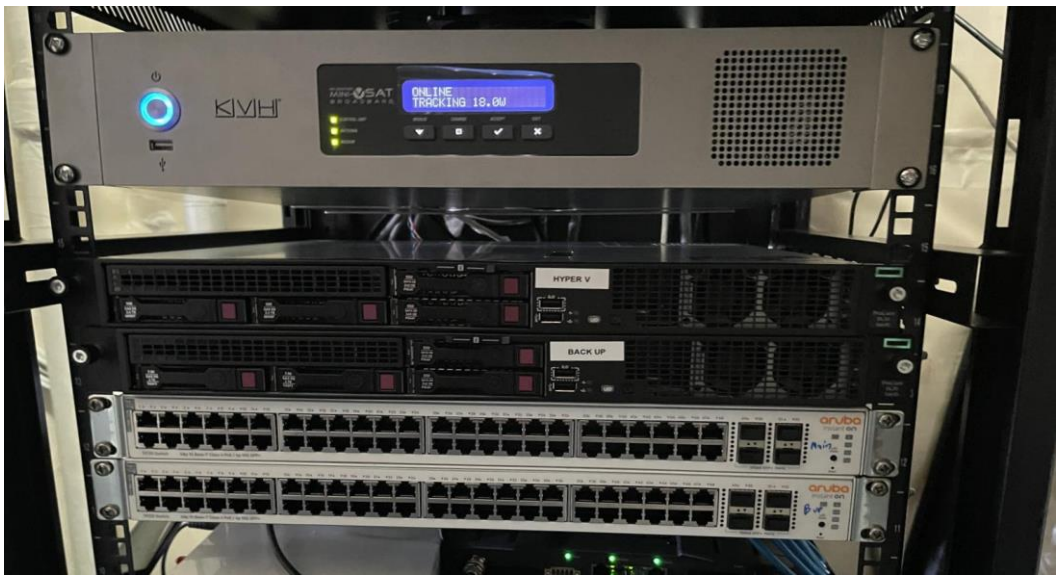
Για την διεύρυνση της ασφάλειας του δικτύου διαχωρίζεται σε (τουλάχιστον) δυο υποδίκτυα ώστε να ελέγχεται καλύτερα η κυκλοφορία και να ορίζονται διαφορετικοί κανόνες δρομολόγησης στα διαφορετικά αυτά υποδίκτυα. Τα παραπάνω υποδίκτυα κυρίως χωρίζονται σε Business και Crew που λεπτομερώς θα αναλυθούν παρακάτω. [1] [3] [2] [6] [11]

2.1 Κατανομή Εξοπλισμού

Ο εξοπλισμός πληροφορικής συντηρείται και εξοπλίζεται κυρίως ανάλογα με το μέγεθος, το είδος και τις ανάγκες του εμπορικού πλοίου. Οι βασικές ανάγκες επικοινωνίας και διαχείρισης των ανάλογων αναγκών που προκύπτουν μας κάνει να παρέχουμε τουλάχιστον 6 με 7 υπολογιστές ευρείας χρήσης, 2 servers (hyperV και Back up), Firewalls και switches (βλ. Εικόνα 15).

Η ανάγκη για υπολογιστές στην γέφυρα (χώρος πλοήγησης) του πλοίου είναι αυξημένη καθώς οι αξιωματικοί και ο καπετάνιος του πλοίου παρευρίσκονται την περισσότερη ώρα σε εκείνον τον χώρο. Στους υπολογιστές αυτούς εγκαθίστανται προγράμματα κυρίως ανταλλαγής μηνυμάτων (email) λήψης χαρτών ναυσιπλοΐας , ERP , sync file software , και πολλά αλλά . Αυτό καθιστά απαραίτητη και απολυτά αναγκαία την χρήση των υπολογιστών στην τοποθεσία αυτή του καραβιού ώστε να τους παρέχεται όλη η απαραίτητή πληροφορία.

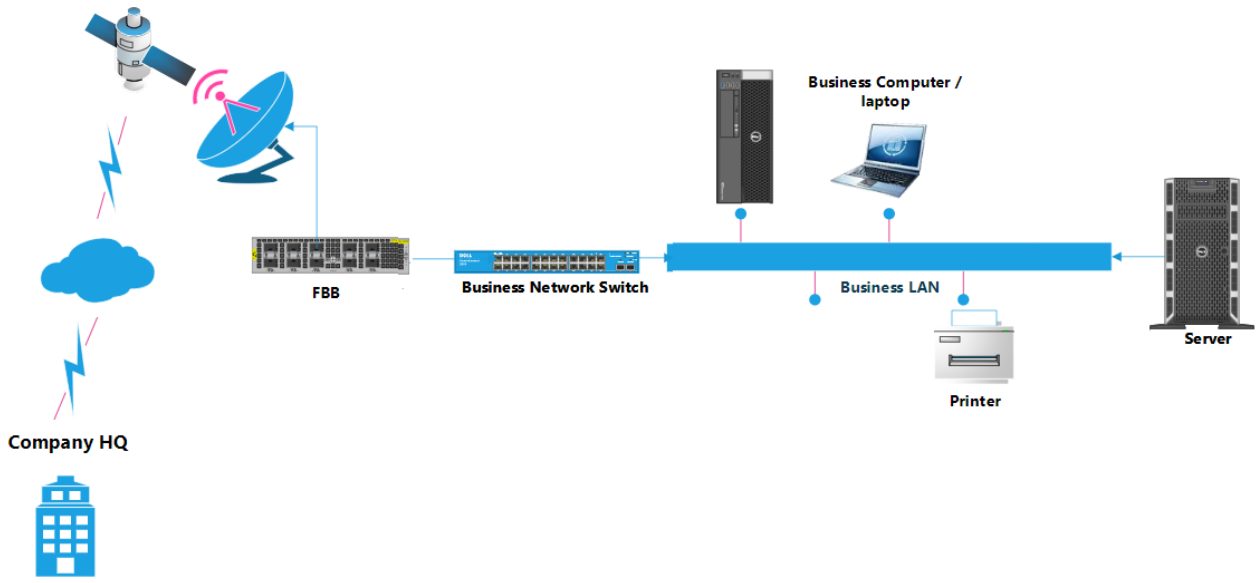
Στην συνέχεια κατανέμεται εξοπλισμός στις καμπίνες του καπετάνιου και του πρώτου μηχανικού καθώς είναι οι αρμόδιοι για την λήψη των πιο σημαντικών αποφάσεων που πρέπει να έχουν πρόσβαση σε όλα τα παραπάνω λογισμικά για την ορθή και ασφαλή ναυσιπλοΐα. Ένας ακόμα υπολογιστή τοποθετείται στο γραφείου του πλοίου για θέματα φόρτωσης - εκφόρτωσής, ένας ακόμα τοποθετείται στο γραφείο διαχείρισης της μηχανής για χρήση λογισμικών ελέγχου της μηχανής. Για την ανάπτυξη του προαναφερόμενου δικτύου, χρησιμοποιείται ο εικονιζόμενος εξοπλισμός:



Εικόνα 15: Firewall, Server HyperV/BackUP και 2 Switches

2.2 Κατανομή Δικτύου

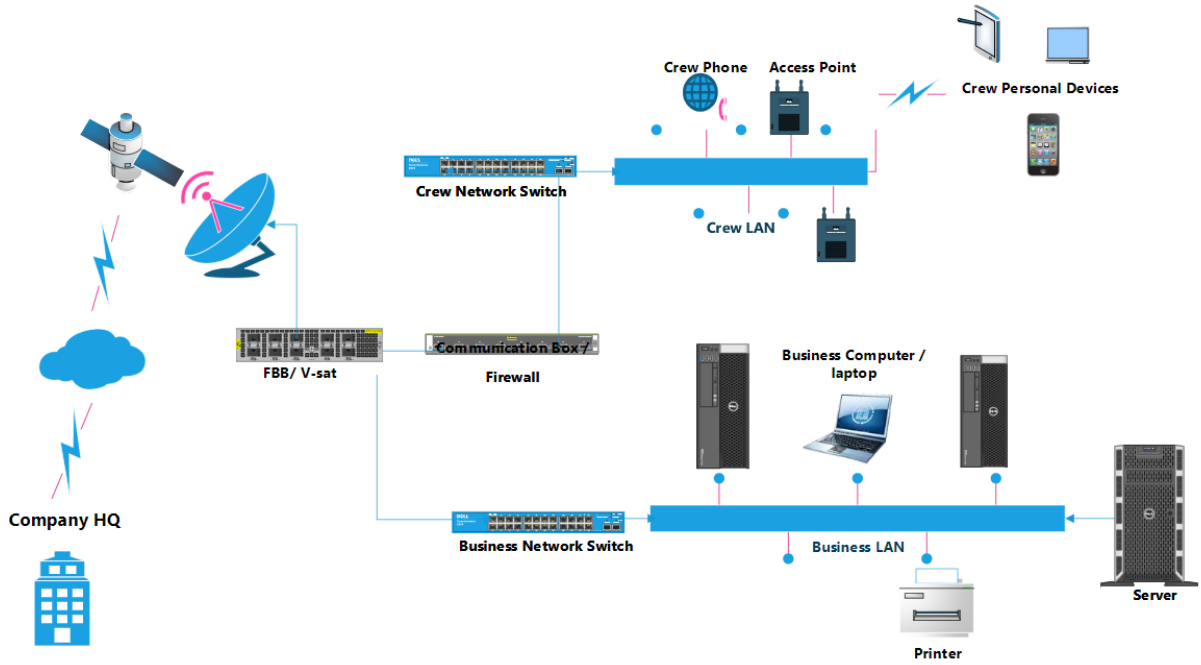
Η κατανομή δικτύου (βλ. Εικόνα 16) και η διαχείριση του πλοίου βελτιώθηκε ανά τα χρόνια καθώς δημιουργήθηκε η ανάγκη για ασφάλεια. Στα πλαίσια της κάλυψης της προαναφερόμενης ανάγκης άλλαξε και η δομή και η αρχιτεκτονική του δικτύου. Ενδεικτικά παρατίθεται η δομή του δικτύου και η ή αρχιτεκτονική που υπήρχε με τα παλιά πρότυπα.



Εικόνα 16: Αρχιτεκτονική Δικτύου παλιού προτύπου

Η δορυφορική επικοινωνία ξεκινούσε από το Head Quarters (HQ - Γραφείο Ναυτιλιακής) και έφτανε στο πλοίο αμφίδρομα κυρίως για επαγγελματική χρήση παρέχοντας πρόσβαση επικοινωνίας μόνο σε εξειδικευμένα μέλη του πληρώματος. Όπως φαίνεται στην παραπάνω εικόνα, η επικοινωνία επιτυγχάνεται μέσω μιας δορυφορικής σύνδεσης χαμηλού bandwidth (**FBB** - aprox. 150 Kbps) και διαμοιράζεται με την χρήση ενός switch (**Busines Network Switch**) στους εκάστοτε υπολογιστές του πλοίου και τον εκτυπωτή (**Business Lan**).

Κατ' επέκταση της κυβερνοασφάλειας και κάλυψης των διεργασιών στο δίκτυο ενός εμπορικού πλοίου, η αρχιτεκτονική του δικτύου εξελίχθηκε (βλ. Εικόνα 17), εικόνα του οποίου φαίνεται παρακάτω.

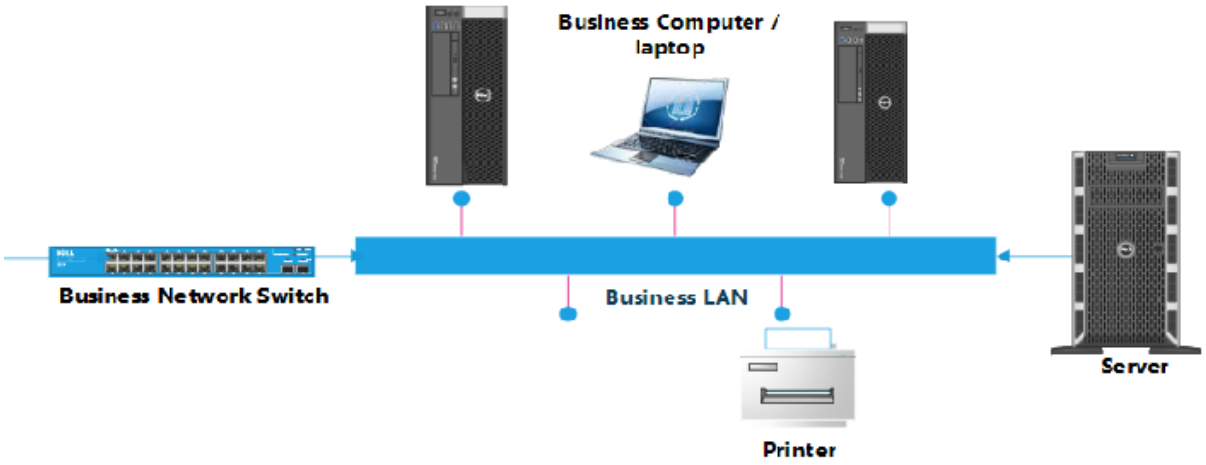


Εικόνα 17: Αρχιτεκτονική Δικτύου σύγχρονου προτύπου

Στην προ υπάρχουσα δομή δικτύου, για την κάλυψη της ανάγκης επικοινωνίας του πληρώματος με την στεριά, προστέθηκε ένα ακόμη δίκτυο (**Crew Network**) στο οποίο συνδέεται το πλήρωμα με τις συσκευές του για την παροχή ψυχαγωγικού υλικού και επικοινωνίας (**Real Time Communication**).

2.2.1 Business Δίκτυο

Το πρότυπο ενός επαγγελματικού δικτύου (**Business Network**) φαίνεται παρακάτω.

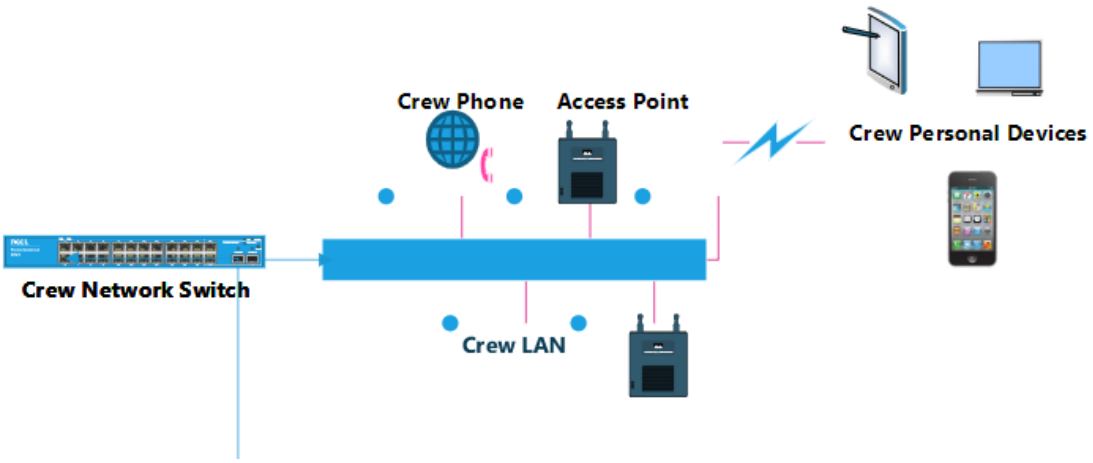


Εικόνα 18: Πρότυπο Business Δικτύου

Για την διαχείριση του δικτύου και για την ασφάλεια του, το υποδίκτυο που ορίζεται στον επαγγελματικό εξοπλισμό είναι το 192.168.X.X/24. Προτείνεται διαφορετική διευθυνσιοδότηση για την προσθήκη οποιασδήποτε άλλης συσκευής, για την διατήρηση της ασφάλειας του επαγγελματικού δικτύου. Το επαγγελματικό δίκτυο συνήθως περιέχει υπολογιστές οι οποίοι διατηρούν λογισμικά επικοινωνίας (email) διαχείρισης χαρτών, ERP (Σύστημα Ενδοεπιχειρησιακού Σχεδιασμού) κ.α. Στο επαγγελματικό δίκτυο εξειδικευμένα μέλη του πληρώματος έχουν πρόσβαση.

2.2.2 Crew δίκτυο

Το πρότυπο ενός δικτύου πληρώματος (**Crew Network**) (βλ. Εικόνα 19) φαίνεται παρακάτω.



Εικόνα 19: Πρότυπο Crew Δικτύου

Για την διαχείριση του δικτύου και για την ασφάλεια του, το υποδίκτυο που ορίζεται στο δίκτυο του πληρώματος συνήθως είναι το 10.0.X.X/24. Η χρήση του γίνεται για ψυχαγωγικούς σκοπούς και επικοινωνίας του πληρώματος και δεν υπάρχει περιορισμός σύνδεσης συσκευών. Αξίζει να σημειωθεί ότι η παροχή αυτών των υπηρεσιών συνηθίζεται να μην παρέχεται δωρεάν στο πλήρωμα. Το κόστος διαμορφώνεται μεταξύ ναυτιλιακής εταιρείας και παρόχου, ενδεικτικά κατά μέσο όρο τα 100 Mb κοστίζουν 10 δολάρια. Στο δίκτυο του πληρώματος έχουν πρόσβαση όλα τα μέλη του εμπορικού πλοίου, καθώς και επισκέπτες.

2.3 Τα Συστήματα Λειτουργίας για Ασφαλή Ναυσιπλοΐα

Ο ναυτιλιακός εξοπλισμός ακολουθώντας την τεχνολογική τάση και την εξέλιξη της δημιουργεί μια σχέση εξάρτησης όλο και συχνότερα με τα συστήματα του κυβερνοχώρου. Πολλές φορές μια πιθανή επίθεση βρίσκει τις εταιρίες ή τους οργανισμούς απροετοίμαστους αναφορικά με τον σχεδιασμό και την αντιμετώπιση της.

Η ασφαλή ναυσιπλοΐα βασίζεται κυρίως σε εξοπλισμό που ανήκει στα «συστήματα του κυβερνοχώρου». Συστήματα όπως το AIS (σύστημα αυτόματης αναγνώρισης) , το (GPS) όπου εκπέμπει την θέση , το σύστημα των ηλεκτρονικών χαρτών (ECDIS) , ο εξοπλισμός επικοινωνίας που συνήθως περιέχει servers και υπολογιστές πρέπει απαραίτητα να διασφαλίζεται η ακεραιότητα τους και η ασφάλεια τους. Η διασύνδεση των παραπάνω συστημάτων και πολλών από αυτών με το διαδίκτυο για ποικίλους τρόπους πολλές φορές δημιουργεί ευκαιρίες επίθεσης.

Οι ναυτιλιακές εταιρίες αλλά και οι βιομηχανίες θα πρέπει να αναφερθεί πως έχουν καταμετρήσει αρκετά οφέλη στηριζόμενες στην εξέλιξη της τεχνολογίας και το διαδίκτυο. Η ασφάλεια της ανθρώπινης ζωής , η προστασία του περιβάλλοντος και η αύξηση της παραγωγικότητας είναι μερικά από τα οφέλη που καταμετρούν. [16] [23]

3. Απειλές και κίνδυνοι

Στο παρακάτω κεφάλαιο περιγράφονται οι απειλές και κίνδυνοι που καλείται ένα σύστημα να αντιμετωπίσει στο ευρύ φάσμα της κυβερνοασφλάλειας. Αναλυτικότερα δίνεται μία καταγραφή επιθέσεων χρονολογικά που έλαβε χώρα και μία σύντομη περιγραφή της εκάστοτε επίθεσης. Το κεφάλαιο κλιμακώνεται με την αναφορά των τύπων επιθέσεων που υφίστανται, με έναν ενδεικτικό χάρτη επιθέσεων και τέλος μία επίθεση που συνέβη σε πραγματικό χρόνο και την έκδοση του επιβλαβούς αρχείου. Στο κλείσιμο το κεφαλαίου περιγράφεται ο ψηφιακός εκφοβισμός.

3.1 Διαχείριση ψηφιακής επίθεσης

Αναφορικά με τις επιθέσεις στα πλοία, σημαντικό θα ήταν να αναφερθεί πως υπάρχει μέριμνα από τον παγκόσμιο οργανισμό ναυσιπλοΐας αναφορικά με την επικοινωνία του πλοίου με την στεριά και με άλλα πλοία . Σε περίπτωση κινδύνου και απώλειας σύνδεσης με το διαδίκτυο επιτυγχάνεται επικοινωνία με τρίτα μέσα όπως του συστήματος Inmarsat-C (αμφίδρομη επικοινωνία πακέτων δεδομένων) , των VHF και των MF/HF (συστήματα αμφίδρομων ραδιοπομπών) . Θα μπορούσαμε να διαχωρίσουμε τις καταστάσεις του πλοίου σε δυο: όταν βρίσκεται σε ταξίδι (εν πλω) και όταν βρίσκεται στο λιμάνι – αγκυροβόλιο.

- Στην κατάσταση «λιμανιού – αγκυροβολίου» είναι πιο εύκολο ο καπετάνιος του πλοίου να διαχειριστεί μια κατάσταση ψηφιακού κινδύνου και μιας καταστροφικής επίθεσης. Ο λόγος είναι διότι δεν έχει να διαχειριστεί ταυτόχρονα και την ναυσιπλοΐα με όλο το φόρτο εργασίας του πλοίου και μπορεί να επικεντρωθεί στην αναγνώριση της επίθεσης και την γνωστοποίηση της στα κεντρικά γραφεία της εταιρίας ώστε να περιοριστεί όσο τον δυνατόν ταχύτερα. Σε αυτή την περίπτωση σε απόλυτη συνεργασία με τους εξειδικευμένους τεχνικούς σε αυτά τα θέματα της ναυτιλιακής εταιρίας αξιολογείται το μέγεθος της επίθεσης και παίρνονται τα ανάλογα μέτρα. Οι εξειδικευμένοι τεχνικοί αναγνωρίζουν το μέγεθος της επίθεσης και προσπαθούν να επαναφέρουν το σύστημα ένα είναι αυτό δυνατό . Εάν η επίθεση είναι καταστροφική σε βαθμό που δεν έχουν πρόσβαση στο σύστημα τους σε συνεργασία με τον τοπικό ατζέντη παρέχουν στο πλοίο νέα συστήματα τα οποία παραμετροποιούν απομακρυσμένα στον βαθμό που τους επιτρέπεται και παράλληλα σχεδιάζουν την επίσκεψη τους στο πλοίο για την ολοκλήρωση της επαναφοράς των συστημάτων.

- Στην κατάσταση «ταξιδιού» η κατάσταση θα μπορούσαμε να αναφέρουμε πως είναι αρκετά πιο περίπλοκη και επικίνδυνη . Ο καπετάνιος του πλοίου εκτός από την ασφαλή ναυσιπλοΐα του έχει να διαχειριστεί και την πιθανή ψηφιακή επίθεση. Η αναγνώριση της επίθεσης και ο περιορισμός της παραμένουν πρωτοπόρα στάδια αλλά προστίθεται και η παράμετρος της διακοπής της επικοινωνίας στην περίπτωση της ολικής επίθεσης καθώς τα e-mail του πλοίου καθορίζονται σαν το πυλώνα της επικοινωνίας. Σε αυτή της περίπτωση ο καπετάνιος ενημερώνει τα κεντρικά γραφεία της εταιρίας και τις πλησιέστερες τοπικές αρχές για την επίθεση που έχει λάβει. Ανάλογα με τα συστήματα που έχουν επηρεαστεί από την επίθεση λαμβάνει και τις ανάλογες οδηγίες. Συνηθώς εάν έχουν επηρεαστεί μόνο πληροφοριακά συστήματα σε συνεννόηση με τα κεντρικά γραφεία ακολουθούν της οδηγία με την προηγούμενη κατάσταση.

Συνοψίζοντας τα παραπάνω παραδείγματα θα πρέπει να αναφερθεί πως κύρια προτεραιότητα είναι η ανθρώπινη ζωή και η ακεραιότητα της και στην συνέχεια η ασφαλή ναυσιπλοΐα. Άξιο αναφοράς είναι επίσης πως ένα ισχυρό τείχος προστασίας δημιουργεί την ανάγκη ενός χρηματικού κεφαλαίου που πολλές φορές οι ναυτιλιακές εταιρίες δυσκολεύονται να καλύψουν ή δεν το αξιολογούν ως κύρια ανάγκη. Τα αποτελέσματα όμως μετά από μια επίθεση επιτυχημένη δυστυχώς είναι τεράστια και χρονικά (ως προς τον χρόνο επαναφοράς των συστημάτων) αλλά και οικονομικά.

3.2 Καταγραφή επιθέσεων

Στην συνέχεια αναφέρονται και καταγράφονται (βλ. Πίνακας 1) ενδεικτικά επιθέσεις που έχουν γνωστοποιηθεί καθώς και οι επιπτώσεις που είχαν. Είναι αρκετά εμφανής ότι με την εξέλιξη της τεχνολογίας και την διασύνδεση συστημάτων στο διαδίκτυο πως όλο και περισσότερες επιθέσεις έρχονται στο προσκήνιο. [52] [53] [54] [55] [56] 57] [58][59]

Αρ	Είδος Επίθεσης	Εμπιστευτικότητα	Ακεραιότητα	Διαθεσιμότητα	Έτος
1	Ransomware attack/Phishing attack		X	X	2022
2	Ransomware attack		X	X	2022
3	Malware attack [52]	X			2019
4	Ransomware attack [54]		X		2018
5	Malware attack [55]	X		X	2020
6	Ransomware attack [56]	X	X		2019
7	Navigation Systems Attack [58]		X		2017
8	Navigation Systems Attack [59]		X		2017
9	Navigation Systems Attack [60]		X	X	2017
10	GPS spoofing [53]	X	X	X	2013

Πίνακας 1: Παραδείγματα Επιθέσεων

Ανάλυση των παραπάνω επιθέσεων:

1) Εμπορικό πλοίο με σημαία Marshall Islands δέχτηκε επίθεση με αποτέλεσμα να μην έχει την δυνατότητα της λήψης και αποστολής e-mail.
2) Εμπορικό πλοίο με σημαία Marshall Islands δέχτηκε επίθεση με αποτέλεσμα να καταστρέψει αρχεία προγράμματος ERP.
3) Επίθεση που πραγματοποιήθηκε σε αμερικάνικο πλοίο διέρρευσε σημαντικά διαπιστευτήρια. Οι τοπικές αρχές διαπίστωσαν κενά ασφαλείας. Παρατηρήθηκε πως οι συσκευές που χρησιμοποιούσε το πλήρωμα για διασκέδαση είχε τα ίδια διαπιστευτήρια με τον υπολογιστή του πλοίου.
4) Κινέζοι χάκερς επιτέθηκαν σε πλοίο του αμερικάνικου ναυτικού στόλου.
5) Η ναυτιλιακή εταιρία MSC για θέματα ασφαλείας τερμάτισε τους διακομιστές της . Αποτέλεσμα είχε τον περιορισμό της επίθεσης εσωτερικά.
6) Μετά από επίθεση χάκερ απέκτησαν πρόσβαση στα συστήματα υπολογιστών.
7) Σύγκρουση πετρελαιοφόρου με αμερικάνικο στρατιωτικό που είχες ως αποτέλεσμα τον θάνατο 10 ναυτικών.
8) Σύγκρουση αμερικάνικου στρατιωτικού πλοίου με κορεάτικο αλιευτικό.
9) Επίθεση που επηρέασε τα συστήματα ναυσιπλοΐας. Είχε ως αποτέλεσμα τη σύγκρουση 2 πλοίων και τον θάνατο 7 ναυτικών στις ακτές της Ιαπωνίας.
10) Πειραματική επίθεση που πραγματοποιήθηκε από ερευνητική ομάδα.

3.3 Τύποι επιθέσεων

Οι τύποι των ψηφιακών επιθέσεων που πραγματοποιούνται σε εταιρίες και πλοία θα μπορούσαν να διαχωρισθούν σε δυο κατηγορίες [61] :

- Στοχευμένες επιθέσεις είναι οι επιθέσεις όπου μια εταιρία ή τα συστήματα ενός πλοίου είναι ο επιδιωκόμενος στόχος από τους επιτιθέμενους. Συνήθως είναι πιο περίπλοκες και χρησιμοποιούν ειδικά εργαλεία και τεχνικές όπως ενδεικτικά θα παρουσιάσουμε παρακάτω:

  - Phishing

    Το «ηλεκτρονικό ψάρεμα» καταφέρνετε με την αποστολή συνήθως email σε πολύ μεγάλο αριθμό στόχων ζητώντας να παρέχουν ευαίσθητες και εμπιστευτικές πληροφορίες. Τα email αυτά εμπεριέχουν κακόβουλα συνημμένα ή ζητούν στον επιτιθέμενο να επισκεφτεί έναν ψεύτικο ιστότοπο χρησιμοποιώντας υπέρ σύνδεσμο και να τα καταθέσει εκεί .

  - Spear-phishing

    Όπως το «ηλεκτρονικό ψάρεμα» τα άτομα στοχοποιούνται με προσωπικά μηνύματα. Σε ορισμένες περιπτώσεις τα πλοία ή οι χρήστες λαμβάνουν μηνύματα με πολύ σημαντικούς τίτλους για να δημιουργούν την αίσθηση του πραγματικού μηνύματος

  - Denial of Services (DoS)

    Αυτός ο τύπος κυβερνοεπίθεσης καταφέρνει να διακόψει η να απενεργοποιήσει ένα δίκτυο ή μια υπηρεσία. Συνήθως ελέγχοντας πολλούς υπολογιστές ακόμα και διακομιστών.

  - Social engineering

    Δεν θα μπορούσαμε να την χαρακτηρίσουμε ως τεχνική επίθεσης καθώς κύριο σκοπό έχει την χειραγώγηση ατόμων που έχουν πρόσβαση στον χώρο που θέλει να αποκτήσει ο επιτιθέμενος

- Brute force

  Ο επιθέμενος στην συγκεκριμένη προσπάθεια του δοκιμάζει πολλούς κωδικούς συνήθως μέσω γεννητριών κωδικών για να καταφέρει να μαντέψει τελικά τον σωστό κωδικό και να έχει πρόσβαση στο σύστημα.

- Credential stuffing

  Ο χρήστης δεν έχει αλλάξει τα διαπιστευτήρια του οπότε ο επιτιθέμενος δοκιμάζει με τα ήδη παραβιασμένα και καταφέρνει την είσοδο του στο σύστημα

❖ Μη στοχευμένες επιθέσεις είναι οι επιθέσεις όπου μια εταιρία ή τα συστήματα ενός πλοίου τυχαία γίνεται ο στόχος από τους επιτιθέμενους. Είναι πιθανό να κάνουν χρήση εργαλείων που είναι ήδη διαθέσιμα στο διαδίκτυο και έτσι καταφέρνουν να ανακαλύψουν τρωτά σημεία που ήδη υπάρχουν.

- Malware

  Το malware είναι κακόβουλο λογισμικό (malicious software) το οποίο έχει σχεδιαστεί και για να παρέχει πρόσβαση χωρίς την συγκατάθεση του χρήστη ή να προξενήσει βλάβη. Υπάρχουν αρκετοί και διαφορετικοί τύποι κακόβουλων λογισμικών όπως οι ransomware , trojan , spyware , worms και άλλα. Ενδεικτικά αναφέρουμε πως τα Ransomware καταφέρνουν να κρυπτογραφούν τα προσωπικά δεδομένα του χρήστη και ο επιτιθέμενος ζητάει λύτρα για να τα αποκρυπτογραφήσει.

- Water holing

  Δημιουργώντας έναν ψεύτικο ιστότοπο ή παραβιάζοντας έναν γνήσιο ιστότοπο προς την εκμετάλλευση του σε ανυποψίαστους επισκέπτες.

- Scanning

  Τυχαία αναζήτηση ευπαθειών που να είναι εκμεταλλεύσιμες στο διαδίκτυο

- Typosquatting

  Ενναλακτικά θα μπορούσαμε να το αποκαλέσουμε και ως πειρατεία των URL (διευθύνσεων ιστοσελίδας). Στηρίζονται στο τυπογραφικό λάθος του χρήστη

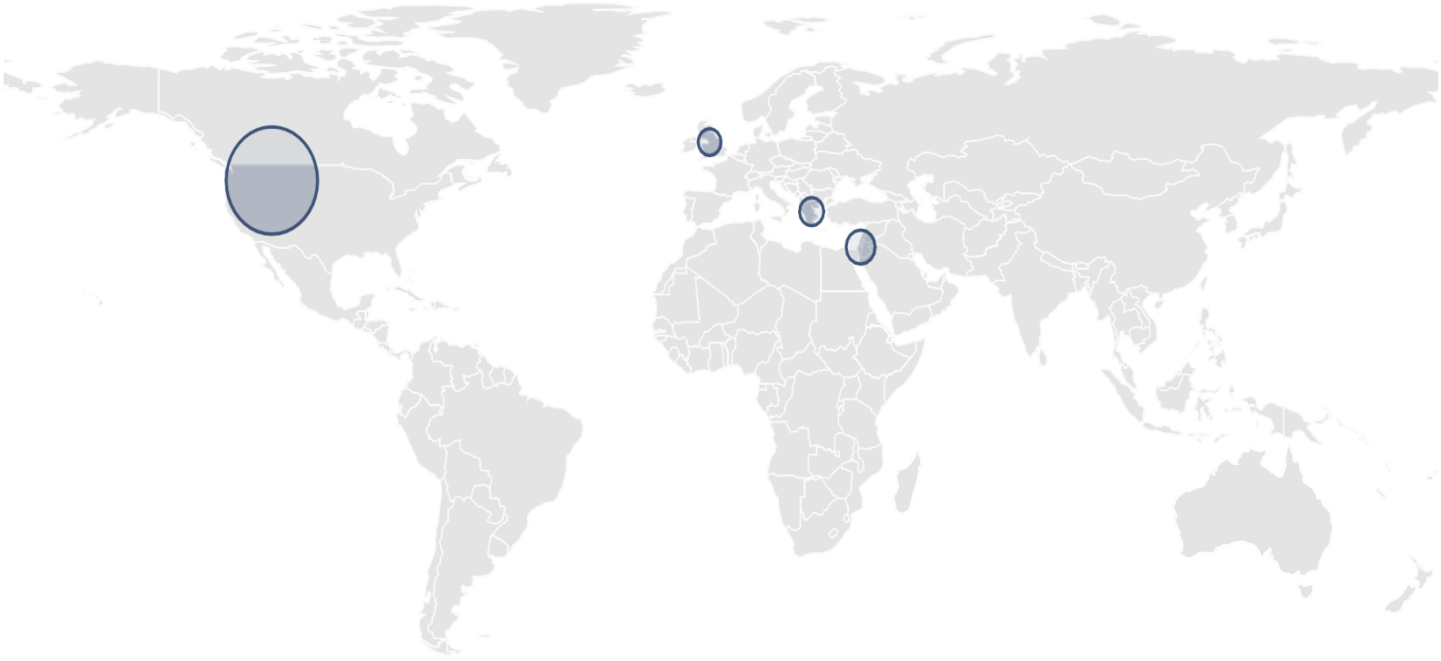
κατά της εισαγωγή της διεύθυνσης . Έτσι στην περίπτωση του λάθους οδηγούνται σε κακόβουλο ιστότοπο.

3.3.1 Ενδεικτικός Χάρτης Επιθέσεων

Παρατίθεται πίνακας (βλ. Πίνακας 2) με τις τοποθεσίες αφετηρίας των επιθέσεων και ο ενδεικτικός χάρτης των αντίστοιχων χωρών (βλ. Εικόνα 20).

Destination Country	Protection Name	Severity	Source	Logs
United States	24 Protections	High	3 Sources	123
Greece	7 Protections	High	1 Source	10
Israel	5 Protections	High	8 Sources	14
United Kingdom	1 Protection	Critical	1 Source	9

Πίνακας 2: Χώρες έναρξης περιστατικών



Εικόνα 20: Ενδεικτικός χάρτης χωρών ανά περιστατικό

3.3.2 Επίθεση σε Πραγματικό Χρόνο

Αναφορικά με τις καθημερινές επιθέσεις που δέχεται ένα πλοίο , παρατίθεται παρακάτω ένα μηνυμα (βλ. Εικόνα 21) που αφησε ο επιθέμενος στον server που επιτέθηκε. Απέκτησε πλήρης πρόσβαση στο σύστημα μας και κατάφερε να κωδικοποιήσει και να κρυπτογραφήσει όλα τα αρχεία και τα προγράμματα που εκτελούνταν σε αυτόν . Είναι μια πάγια κίνηση των επιθεμενων ώστε να μπορέσουν να απειλήσουν την ναυτιλιακή εταιρεία και να της αποσπάσουν κάποιο χρηματικό αντίκτοιπο. Στην συγκεκριμένη επίθεση προλάβαμε και περιορίσαμε την επίθεση απομονώνοντας τον επιθέμενο μόνο στον server και όχι στο υπόλοιπο δίκτυο . Τον αφαιρέσαμε άμεσα από το δίκτυο μας και τον απενεργοποίησαμε.

Στην συνέχεια εκτελέσαμε εκτενείς ελέγχους στο υπόλοιπο δίκτυο ώστε να επιβεβαιώσουμε την ακεραιότητα του. Παράλληλα με την χρήση απομακρυσμένης σύνδεσης καταφέραμε να επαναφέρουμε όσο το δυνατό ταχύτερα τα αρχεία και τα προγράμματα πλοήγησης που χρησιμοποιούσε το πλήρωμα. Η πρόληψη και έγκαιρη αντιμετώπιση σε τέτοιου είδους επιθέσεις αποδίδουν την ασφαλή ναυσιπλοοία αλλά και

την καθημερινότητα των ναυτικών. Παρακάτω παρατίθεται η επίθεση όπως ανιχνεύθηκε:

Hello my dear friend

Unfortunately for you, a major IT security weakness left you open to attack, your files have been encrypted.

If you want to restore them, write to our skype. PIpIkakI Decryption

Also you can write IOQ live chat which works 24/7 $PIPIKAKI

Install IOQ software on your PC https://icq.ccm/windows/ or on your mobile phone search in Appstore / Goggle market IOQ.

Write to our IOQ $PIPIKAKI https://icq.im/PIPIPAKI

If we not reply in 6 hours you can write to our mail but use it only if previous methods not working – pipikaki@onlonmail.org

Attention!

- Do not rename encrypted files.
- Do not try to decrypt your satausing third party software, it may cause permanent data loss.
- We are always ready to cooperate and find the best way to solve your problem.
- The faster you write, the more favorable the conditions will be for you.
- Our company values its reputation,. We give all guarantees of your files decryption, such as test decryption.

We respect your time and waiting for your respone from your side

Tell your unique ID: 76885085

Sensitive data on your system was DOWNLOADED.

If you DON'T WANT your sensitive data to be PUBLISHED you have to act quicly.

Data Includes:

-Employees personal data, CVS, DL, SSN.

-Complete network map including credentials for local and remote services.

-Private financial information including: clients data, bills, budgtes, annual reports, bank statements.

-Manufacturing documents including: datagrams, schems, drawings in solidworks format.

-And more…

Εικόνα 21: Επίθεση σε Πραγματικό Χρόνο

3.3.3 Επίθεση σε Λιμάνι

Παρακάτω, παρατίθεται ένα ιστορικό γεγονός κυβερνοεπίθεσης που έλαβε χώρα το 2013 στην Αμβέρσα. Έμποροι ναρκωτικών πραγματοποίησαν μια επίθεση στον κυβερνοχώρο πολλαπλών σταδίων σε μια περίοδο δύο ετών στο λιμάνι της Αμβέρσας, γεγονός που δείχνει τους κινδύνους στους οποίους είναι ανοιχτά τα συστήματα πληροφορικής της ναυτιλίας σύμφωνα με τους ειδικούς της ναυτιλιακής ασφάλειας και της πληροφορικής.

Ξεκινώντας, στάλθηκε κακόβουλο λογισμικό στο προσωπικό του λιμανιού τον Ιούνιο του 2011, μια εγκληματική ομάδα απέκτησε πρόσβαση σε δεδομένα εξ αποστάσεως, τα οποία στη συνέχεια χρησιμοποίησε για να εντοπίσει και να υποκλέψει κοντέινερ με ναρκωτικά που μεταφέρονταν λαθραία στο πλοίο.

Η κυβερνοεπίθεση ανακαλύφθηκε αφού ολόκληρα κοντέινερ εξαφανίστηκαν από το λιμάνι χωρίς προφανή εξήγηση.

Μόλις το λογισμικό ανακαλύφθηκε και εξουδετερώθηκε, οι επιτιθέμενοι εισέβαλαν σε γραφεία στο λιμάνι, αναπτύσσοντας υπολογιστές κρυμμένους σε καθημερινά αντικείμενα για να υποκλέψουν δεδομένα από συστήματα, συμπεριλαμβανομένων των εγγραφών του πληκτρολογίου του προσωπικού και των στιγμιότυπων οθόνης από τους σταθμούς εργασίας τους.

Η περίπλοκη και παρατεταμένη επίθεση οδήγησε σε προειδοποιήσεις από ειδικούς σε θέματα ασφάλειας ότι οι επιθέσεις στη ναυτιλιακή και λιμενική υποδομή θα συνεχίσουν να εξελίσσονται και η προστασία της εφοδιαστικής αλυσίδας είναι υψίστης σημασίας. [28]

3.4 Ψηφιακός εκφοβισμός

Οι ναυτικοί όπως είναι λογικό είναι αρκετά επιφορτισμένοι από την δύσκολη επαγγελματική τους καθημερινότητα αλλά και από την διαβίωση τους. Η δυσκολίες αυτές τους αφήνουν συχνά λίγο χρόνο ενασχόλησης με θέματα πληροφορικής . Έχει αναφερθεί από πολλούς επίσης πως η έλλειπες εκπαίδευση και η συνεχής εξέλιξη των συστημάτων σε αυτό το τομέα τους κάνει πιο εκτεθειμένους σε μια πιθανή επίθεση. Πολλοί από εκείνους δεν έχουν εκπαιδευτεί σε ότι αφορά την ασφαλή χρήση λογισμικού στα συστήματα ηλεκτρονικών υπολογιστών ακόμα και στην χρήση φορητών μέσων αποθήκευσης (usb sticks) στο πλοίο. Έτσι λοιπόν δεν έχουν επίγνωση των συνεπειών από μια πιθανή επίθεση ή κάποια απειλή.

Ο όρος ψηφιακός εκφοβισμός ή αλλιώς «κυβερνοτρομοκρατία» θα μπορούσαμε να τον ορίσουμε σαν ένα σύνολο από ηλεκτρονικές επιθέσεις με στόχο εσωτερικά ή εξωτερικά δίκτυα οι οποίες έχουν προορισμό συγκεκριμένες κρίσιμες υποδομές. Σκοπός τους είναι να προκληθούν ζημίες είτε να υπονομεύσουν οργανισμούς, είτε να προκαλέσουν σωματικές και ψυχολογικές επιπτώσεις σε άτομα.

3.5 Συνέπειες των Επιθέσεων

Οι συνέπειες των επιθέσεων στον κυβερνοχώρο σήμερα μπορούν να είναι ανυπολόγιστες και έως εκ τούτου χρήζουν άμεσης αντιμετώπισης. Για παράδειγμα, σύγκρουση ή προσάραξη πλοίου μπορεί να προκύψει από παρέμβαση στα μέσα ναυσιπλοΐας ή/και άλλων συστημάτων, που θα μπορούσαν να οδηγήσουν σε:

- Απώλεια ή επικίνδυνες καταστάσεις για τα πλοία (σύγκρουση, προσάραξη).
- Σωματική βλάβη του πληρώματος (σε περίπτωση πειρατείας).
- Απώλεια φορτίου.
- Ρύπανση.
- Απώλεια των λειτουργιών των πλοίων (π.χ. επικοινωνία με το γραφείο, ναυλωτές), όπως και απώλεια των δραστηριοτήτων του λιμένα, ειδικότερα στη μεταφορά εμπορευματοκιβωτίων.

Το ψήφισμα MSC.428 (98) του IMO ενθαρρύνει τα κράτη-μέλη του IMO να διασφαλίσουν ότι οι κίνδυνοι στον κυβερνοχώρο αντιμετωπίζονται με συστήματα διαχείρισης της ασφάλειας το αργότερο κατά την πρώτη ετήσια επιθεώρηση του εγγράφου συμμόρφωσης (Document of Compliance – DOC) της εταιρείας μετά την 1η Ιανουαρίου 2021. [5] [7]

Πολλές εταιρείες έχουν πέσει θύματα εγκλήματος στον κυβερνοχώρο, όπου οι χάκερ έχουν πρόσβαση στους λογαριασμούς ηλεκτρονικού ταχυδρομείου, στους προμηθευτές τους (καύσιμα, ανταλλακτικά) και έχουν στείλει μηνύματα ηλεκτρονικού ταχυδρομείου, ζητώντας αμοιβές και πληρωμές να αποστέλλονται σε διαφορετικούς τραπεζικούς λογαριασμούς απ’ ό,τι συνήθως. Αυτός ο τύπος απάτης ηλεκτρονικού «ψαρέματος» έχει ξεκινήσει από το 2013. [30]

Οποιαδήποτε εταιρεία μπορεί να είναι ευάλωτη σε επιθέσεις στον κυβερνοχώρο και το πρόβλημα απαιτεί ολιστική προσέγγιση στη λύση του, που πρέπει να περιλαμβάνει:

- Αύξηση της ευαισθητοποίησης για τις επιθέσεις, παροχή κατάρτισης και επικοινωνίας των κινδύνων σε όλα τα επίπεδα της εταιρείας.
- Διαδικασίες και πολιτικές για τον εντοπισμό και την αξιολόγηση του κινδύνου.
- Εναρμόνιση των κινδύνων στον κυβερνοχώρο με τις υφιστάμενες απαιτήσεις διαχείρισης κινδύνων ασφάλειας και ασφάλειας που περιέχονται στους κώδικες ISPS και ISM, όπως περιλαμβάνονται στις πολιτικές της εταιρείας.
- Να συμπεριληφθούν απαιτήσεις σχετικές με την εκπαίδευση, τη λειτουργία και τη συντήρηση των κρίσιμων συστημάτων κυβερνοχώρου.

- Συστήματα πληροφορικής – τείχη προστασίας, antivirus και κρυπτογράφηση.

4. Ασφάλεια στο διαδίκτυο

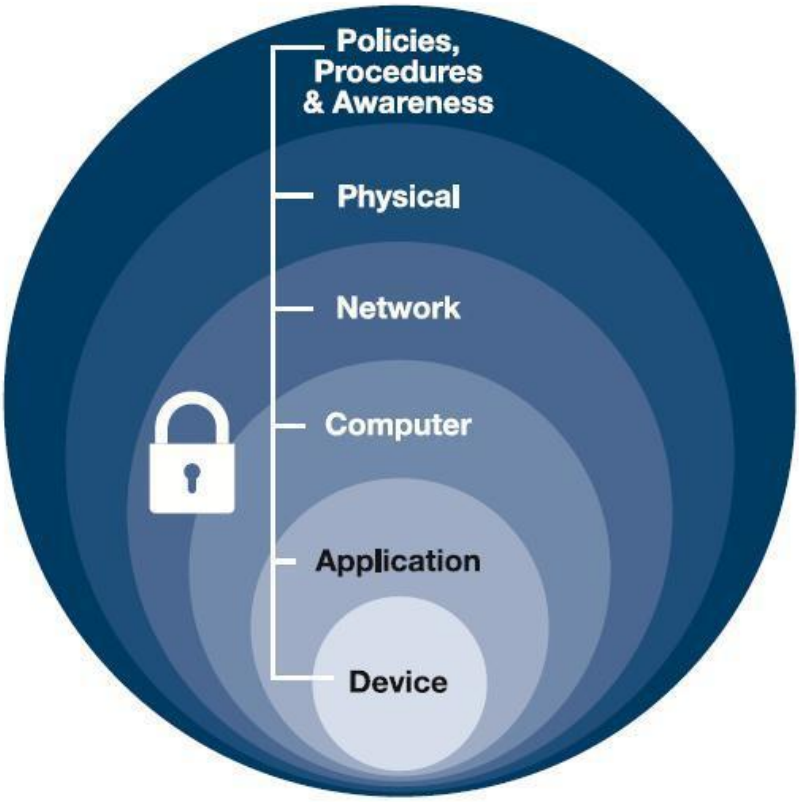
4.1 Πληροφοριακά Συστήματα και αρχιτεκτονικές ασφάλειας

Μια σύγχρονη τυπική δομή ενός πληροφοριακού συστήματος χαρακτηρίζεται από κεντρική υποδομή, με servers που φέρουν δημόσια IP και παρέχουν εσωτερικά δίκτυα. Αυτό συνεπάγεται, ότι ο εκάστοτε εργαζόμενος του οργανισμού που είναι συνδεδεμένος στο διαδίκτυο έχει πρόσβαση σε αυτό με τις δικές του προσωπικές συσκευές. Επιπλέον, ο ίδιος οργανισμός του ίδιο πληροφοριακού συστήματος μπορεί να έχει απομακρυσμένα γραφεία με την ίδια εσωτερική δικτυακή υποδομή. Επιπλέον, ο προαναφερόμενος οργανισμός έχει τις δικές του εφαρμογές ή ιστότοπο στο διαδίκτυο, βασικό πυλώνα ενός πληροφοριακού συστήματος. Τελευταίο και μη εξαιρετέο χαρακτηριστικό του συστήματος, είναι οι υπάλληλοι που συνδέονται οποιαδήποτε ώρα στο δίκτυο του οργανισμού καθώς και πάροχοι οι οποίοι παρέχουν τεχνική υποστήριξη και ανάπτυξη εφαρμογών για χάρη του οργανισμού. Όλα τα παραπάνω, απαρτίζουν την εικόνα ενός βασικού πληροφοριακού συστήματος, βάσει των οποίων γίνεται αντιληπτό ότι λόγω της μεγάλη διασποράς και κυκλοφορίας των δεδομένων το δικτυακό εύρος δεν έχει όριο κάνοντας ευάλωτο τον οργανισμό σε κακόβουλες δραστηριότητες.

Για την αποτελεσματική αντιμετώπιση και την οριοθέτηση του κινδύνου, έχουν αναπτυχθεί δύο βασικά μοντέλα αρχιτεκτονικής τα οποία περιγράφονται στη συνέχεια.

Η πρώτη είναι η αρχιτεκτονική «άμυνα σε βάθος(Defense in Depth)» (βλ. Εικόνα 22). Σε αυτό το μοντέλο η άμυνα που εφαρμόζεται καλύπτει το φάσμα όλου του δικτύου. Σε συλλογικό βαθμό αντιμετωπίζεται ο κίνδυνος μέσω της εφαρμογής αμυντικών μηχανισμών σε κάθε στρώμα δικτύου. Η άμυνα περιλαμβάνει: [64]

- Εκπαίδευση χρηστών και ανάλυση κινδύνου
- Περιορισμούς στην πρόσβαση, να μην είναι όλοι οι χρήστες authorized
- Ασφάλεια του δικτύου (χρήση firewall, VPN κτλ.)
- Προστασία των διαθέσιμων εφαρμογών (data backup, κρυπτογράφηση κτλ.
- Προστασία μεμονωμένα των συσκευών με την χρήση antivirus

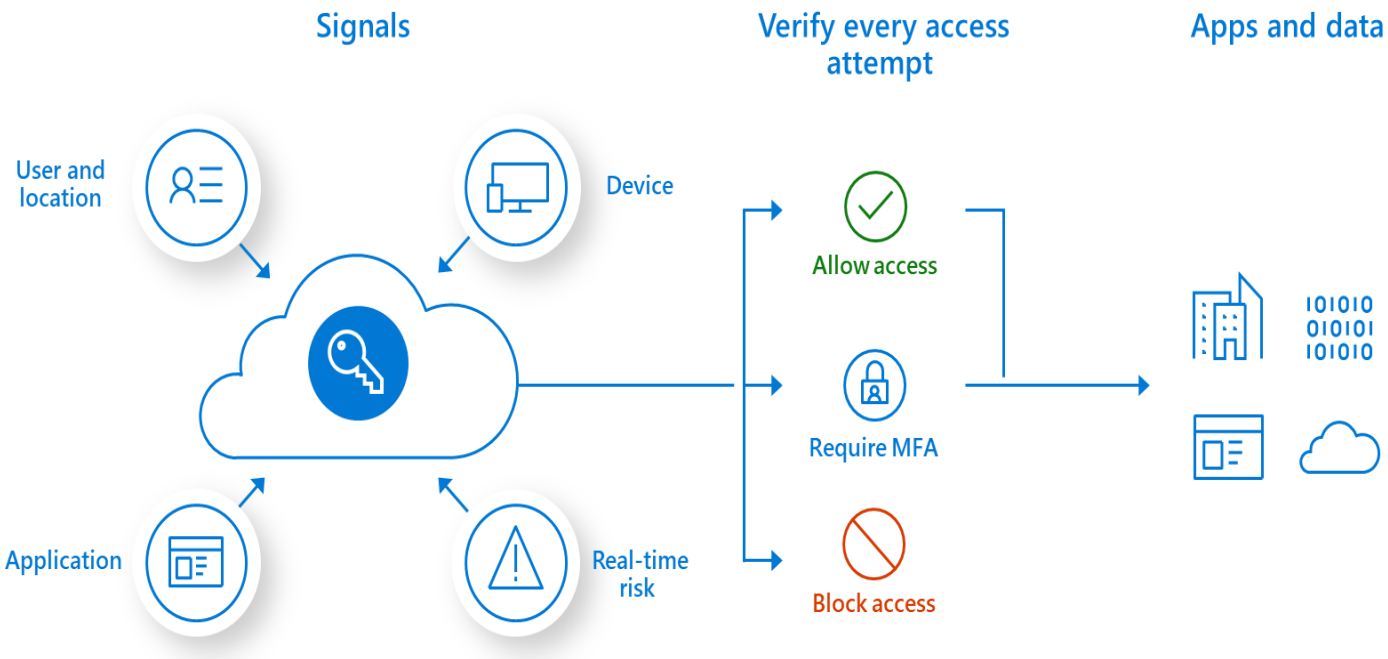


Εικόνα 22: Defense in Depth Μοντέλο

Το δεύτερο αρχιτεκτονικό μοντέλο είναι ευρέως γνωστό με το όνομα «Zero Trust» (βλ. Εικόνα 23). Το συγκεκριμένο μοντέλο βασίζεται στην αποδοχή ύπαρξης απειλών τόσο έξω όσο και μέσα από τις παραδοσιακές περιμέτρους του δικτύου. Συγκεκριμένα, οι αρχές εφαρμογής του μοντέλου είναι: [34]

- “never trust, always verify” : πρακτικά αυτό σημαίνει ότι κάθε χρήστης δεδομένων ή εφαρμογή στο διαδίκτυο θεωρούνται μη έμπιστα. Συνεπώς, πριν από οποιαδήποτε κίνηση, κάθε προαναφερόμενο στοιχείο θα πρέπει να αυθεντικοποιείται πρώτα.
- “assume breach” : οι χρήστες πράττουν σα να έχει παραβιαστεί ήδη το δίκτυο τους από κάποια κακόβουλη κίνηση και εφαρμόζουν την αρχή “deny by default” για κάθε αίτημα πρόσβασης χρήστη, εφαρμογής ή και συσκευής στο δίκτυο του οργανισμού.

Με το μοντέλο αυτό ουσιαστικά παρακολουθείται κάθε κίνηση στο διαδίκτυο. Οποιαδήποτε κίνηση και αν προκύψει, αποθηκεύεται σε log file και αυτομάτως ελέγχεται. Ένα αντιπροσωπευτικό παράδειγμα “Zero Trust” μοντέλου παρουσιάζεται παρακάτω, όπου πρακτικά μας δείχνει των έλεγχο κινήσεων των συσκευών των χρηστών στο διαδίκτυο και των εφαρμογών και απορρίπτει όποιο φαίνεται ύποπτο. [34]



Εικόνα 23: Zero Trust Μοντέλο

4.2 Αξιολόγηση Κινδύνου

Η διαχείριση του κινδύνου αποτελεί πάντα το σημείο εκκίνησης για μία αποτελεσματική προσέγγιση στην κυβερνοασφάλεια. Οι απειλές για τις τεχνολογίες πληροφορικής περιλαμβάνουν τις κυβερνοεπιθέσεις, τα ανθρώπινα λάθη, τις περιβαλλοντικές καταστροφές και τις δομικές αστοχίες. Για τον λόγο αυτό, δημιουργείται η ανάγκη αποτύπωσής και αξιολόγησης του κινδύνου. Αρχικά, στο πλαίσιο αξιολόγησης του κινδύνου θα πρέπει να εντοπίζονται οι πηγές από τις οποίες προέρχεται η απειλή, είτε είναι φυσική είτε από κακόβουλη ομάδα. Εν συνεχεία, θα πρέπει να αναγνωριστεί ο χαρακτήρας των ενεργειών των παραπάνω πηγών, αν δηλαδή είναι κυβερνοεπίθεση ή αποσκοπεί σε βλάβη υλικού. Στο σημείο αυτό, οφείλουν να αξιολογηθούν οι ευπάθειες του δικτύου και ειδικότερα της ναυτιλιακής εταιρείας ως προς τις απειλητικές ενέργειες μιας κακόβουλης επίθεσης. Τέλος, θα πρέπει να συνυπολογιστούν η πιθανότητα πραγματοποίησης των γεγονότων συναρτήσει των επιπτώσεων που θα προκαλέσουν αν τελικά υπάρξει ολοκληρωμένη κακόβουλη επίθεση. Με βάση τα προαναφερόμενα, οι οργανισμοί οφείλουν να ανταποκρίνονται στους κινδύνους που παραμονεύουν και να αναπτύσσουν διαρκώς το σύστημα ώστε να εξασφαλίζεται η ομαλή λειτουργία και η ακεραιότητα των δεδομένων τους. Εν συνεχεία του κεφαλαίου, αναφέρονται μερικές από τις πρακτικές για την επίτευξη της αποδοτικότερης ασφάλειας ενός πληροφοριακού συστήματος. [5] [6] [65] [68]

4.3 Διαχείριση Κινδύνου

Το μεγάλο μέγεθος ενός οργανισμού εγκυμονεί και περισσότερους κινδύνους στην παραβίαση της ασφάλειας του. Περισσότερες συσκευές, μεγαλύτερος αριθμός προσωπικού, ποικίλες υποδομές δημιουργούν ένα μη ασφαλές και ανεξέλεγκτο περιβάλλον που χρήζουν ιδιαίτερης μεταχείρισης με γνώμονα ορισμένες πρακτικές. Συνοπτικά θα αναφερθούν και θα επεξηγηθούν παρακάτω. [6] [1]

4.3.1 Καταγραφή υλικού και λογισμικού

Το περιβάλλον ενός οργανισμό διαρκώς αλλάζει και πρέπει να καθίσταται υπό αυστηρή παρακολούθηση. Εδραιώνεται η καταγραφή σε τακτική βάση του υλικού και λογισμικού ενός οργανισμού. Αντιμετωπίζοντας απειλές όπως την ιχνηλάτιση νόμιμων εγκατεστημένων πόρων που έχουν εισαχθεί στο δίκτυο. Επιπλέον, οι επιτιθέμενοι αποσκοπούν στην εύρεση ευάλωτου συστήματος σαρώνοντας διαρκώς το δίκτυο και ψάχνοντας για ευάλωτα σημεία, πρόβλημα που κλείνεται να λυθεί εν μέσω της καταγραφής. Επίσης, μη καταγεγραμμένοι υπολογιστές θα περνιόνται στο σύστημα κάνοντας γνωστό στο δίκτυο την ύπαρξη τους και την αποφυγή υψηλών κινδύνων. Τέλος, ο οργανισμός λαμβάνει υπόψιν ότι ασύρματες συνδέσεις δεν γίνονται αντιληπτές και σε περίπτωση κυβερνοεπίθεσεις είναι αρκετά δύσκολη η ιχνηλάτιση. Δημιουργείται βάση δεδομένων ηλεκτρονικού αρχείου ακριβής καταγραφής και ταξινόμησης όλων των υλικών αγαθών του οργανισμού ορίζοντας και έναν πιστοποιημένο χρήστη για την διαχείριση τους. [66]

4.3.2 Ασφαλής διαμόρφωση του Εξοπλισμού και των Εφαρμογών

Οι κίνδυνοι που παραμονεύουν είναι, η εκμετάλλευση ευπαθειών στο λογισμικό σε συστήματα πληροφοριών του φορέα. Επιπλέον, μη εξουσιοδοτημένες αλλαγές μπορεί να προκαλέσουν εμπλοκή στις ρυθμίσεις που προστατεύουν συστήματα και εφαρμογές. Ο οργανισμός οφείλει να προστατεύει τα συστήματα του χρησιμοποιώντας αυθεντικές εκδόσεις συστημάτων, αποσύροντας εξοπλισμό των οποίων η αναβάθμιση δεν υποστηρίζεται πλέον, να διασφαλίζει την τροποποίηση των προεπιλεγμένων κωδικών σε κάθε καινούρια συσκευή και να εφαρμόζει ρυθμίσεις ασφαλείας με βάση τα διεθνή πρότυπα λειτουργικών συστημάτων. [67]

4.3.3 Περιορισμός Χρήσης και Εκτέλεσης Προγραμμάτων και Υπηρεσιών

Με των αριθμό των υπηρεσιών να αυξάνονται, αυξάνεται σταδιακά και ο αριθμός επιθέσεων στο σύστημα. Τα διαφορετικά σημεία εισόδου είναι εκτεθειμένα προς απόκτηση παρέχοντας ευκολία εξαγωγής δεδομένων σε μια εφαρμογή του συστήματος. Σε αυτή την περίπτωση, πρέπει να οριστεί ότι στους κεντρικούς servers των οργανισμών λειτουργούν μόνο οι θύρες (ports), τα πρωτόκολλα και οι δικτυακές υπηρεσίες που είναι απαραίτητες. Επιπλέον, σε τακτική βάση θα πρέπει να διενεργείται αυτοματοποιημένο port scanning και να διασφαλίζεται ότι δεν θα έχουν δικαίωμα όλοι οι χρήστες για αλλαγή ή τροποποίηση ρυθμίσεων ασφαλείας στο λειτουργικό σύστημα. [2] [3] [65] [68]

4.3.4 Έλεγχος πρόσβασης

Ένας σημαντικός κίνδυνος που χρήζει προσοχής είναι ο λανθασμένος διαμοιρασμός δικαιωμάτων στους χρήστες που απαρτίζουν έναν οργανισμό. Ο χρήστης ο οποίος έχει πρόσβαση σε χρηματοοικονομικά αρχεία και πέσει θύμα κακόβουλης επίθεσης, είναι πιθανό να δημιουργήσει προβλήματα μη αναστρέψιμα. Συνίσταται η αναγνώριση των χρηστών που έχουν δικαιώματα, τουλάχιστον σε ευαίσθητα αρχεία, με μοναδικό τρόπο. Επιπλέον, στους ίδιους χρήστες που έχουν πρόσβαση σε τέτοιου είδους πλατφόρμες, να τους χορηγείται εναλλακτική άδεια για διεργασίες καθημερινών ρουτίνων έτσι ώστε και αν μία κακόβουλη επίθεση τους προσβάλλει να μην είναι ζωτικής σημασίας για τον οργανισμό. [69]

4.3.5 Ασφάλεια Δικτύων

Η προστασία του δικτύου ενός οργανισμού από εξωγενείς παράγοντες είναι μείζονος σημασίας. Η μόλυνση με κακόβουλο λογισμικό, οι κατανεμημένες επιθέσεις, η αλλοίωση ιστοσελίδων και οι απειλές ασυρμάτων δικτύων είναι μερικά από τα ζητήματα που κλίνονται να επιλυθούν. Μερικές λύσεις που παρέχονται σε αυτό το σημείο είναι, η εγκατάσταση firewall σε εξωτερική περίμετρο του δικτύου, ο διαχωρισμός του δικτύου σε επιμέρους υποδίκτυα, η εφαρμογή φίλτρου κίνησης μεταξύ των υποδικτύων, η χρήση VPN κ.α. [70]

4.3.6 Τήρηση και Ανάλυση Συμβάντων

Η καταγραφή συμβάντων στο δίκτυο, αποτελεί αναπόσπαστο κομμάτι της ανίχνευσής κακόβουλης δραστηριότητας σε αυτό. Τα logs που συλλέγονται πρέπει και να αναλύονται προς αποφυγή μόλυνσης του λογισμικού. Τα αρχεία αυτά ορισμένες φορές αποτελούν την μοναδική ένδειξη ότι κάτι ύποπτο συμβαίνει και για αυτό τον λόγο πρέπει να αναλύονται τακτικά. Συνεπώς, η καταγραφή είναι απαραίτητη και η ρύθμιση των αρχείων αυτών να περιλαμβάνει λεπτομερής περιγραφή των συμβάντων. [45]

4.3.7 Φυσική Ασφάλεια Εγκαταστάσεων

Η φυσική προστασία των εγκαταστάσεων πρέπει να λαμβάνεται με ιδιαίτερη σοβαρότητα. Μη εξουσιοδοτημένα άτομα είναι πιθανό να επιχειρήσουν να εισέλθουν στις εγκαταστάσεις του οργανισμού και να υποκλέψουν ορισμένα αρχεία ακόμη και να μολύνουν απευθείας τα συστήματα εγκαθιστώντας κακόβουλο πρόγραμμα. Ο οργανισμός θα πρέπει να μεριμνήσει προστατεύοντας τις κτηριακές υποδομές που φιλοξενούν τους servers τους και να διατηρεί κατάλογο με τα εξουσιοδοτημένα άτομα που έχουν δικαίωμα στην είσοδο του χώρου. [11]

4.3.8 Λήψη Back Up

Απαραίτητη η λήψη αντιγράφων ασφαλείας και δεδομένων προς αποφυγή μη ηθελημένης διαγραφής ή μόλυνσης αρχείων με ransomware προκαλώντας την απώλεια τους. Θα πρέπει να εξασφαλιστεί ότι όλα τα αρχεία αποθηκεύονται σε ένα τουλάχιστον offline προορισμό μη προσβάσιμο από τον έξω κόσμο, και ό,τι αρχείο λαμβάνεται προστατεύεται και με κρυπτογράφηση. [71]

4.3.9 Αντιμετώπιση Ζητημάτων Κυβερνοασφάλειας

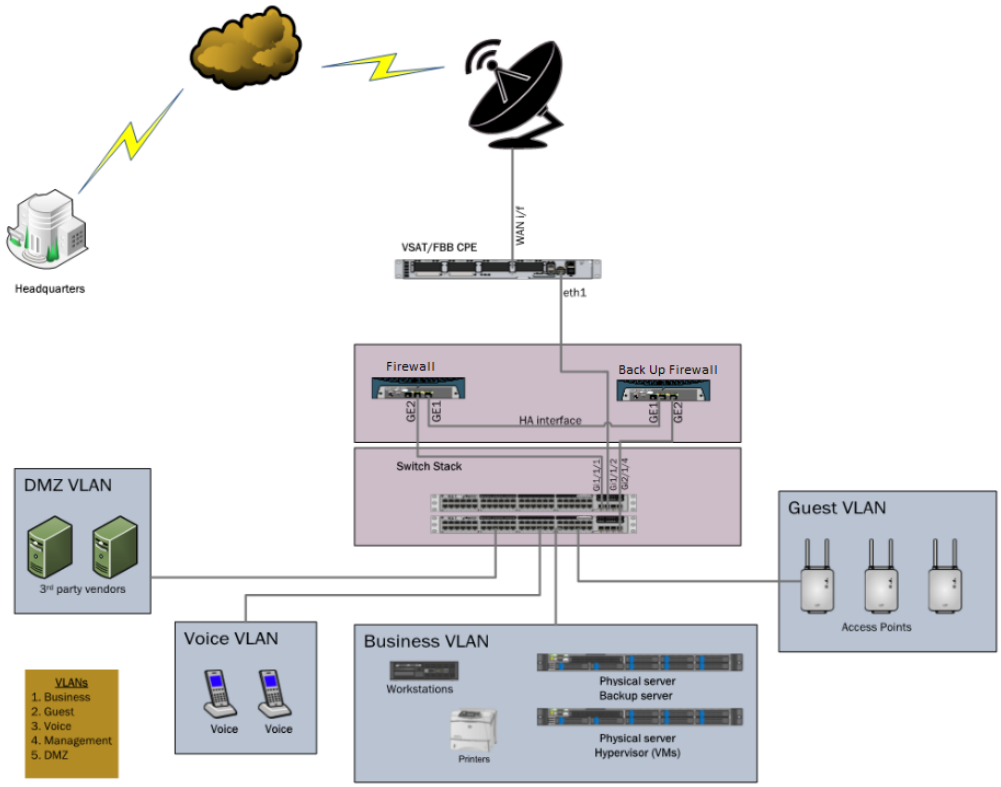
Οι κυρώσεις ενός μη οργανωμένου πλάνου διαχείρισης τέτοιων ζητημάτων μπορεί να αποδειχθούν μοιραίες προκαλώντας συνεχείς βλάβες στα συστήματα λειτουργίας, διοικητικές και οικονομικές επιπλοκές ακόμη και σε διακοπή λειτουργίας ολόκληρου συστήματος. Ανάπτυξη λεπτομερούς πλάνου, συγκρότηση ομάδας αντιμετωπίσεις σε περιόδους κρίσεις και συλλογή και διατήρηση αρχείου ανάλυσης των περιστατικών προς μελλοντική αντιμετώπιση, είναι μερικές από τις ενέργειες που θα μπορούσε να διεξάγει ο οργανισμός εν όψει ενός τέτοιου περιστατικού. [11]

4.4 Firewall

Στην επίτευξη του στόχου ασφαλείας και την διασφάλιση όλων των προαναφερόμενων πρακτικών, η χρήση εξωτερικού firewall είναι απαραίτητη (βλ. Εικόνα 24). Σε μία τυπική αρχιτεκτονική δικτύου μεταξύ του γραφείου και ενός εμπορικού πλοίου, το firewall του παρόχου δεν καθίσταται αρκετό σε κρίσιμα ζητήματα ασφάλειας και ελέγχου της συνολικής κίνησης του δικτύου. Για τον λόγο αυτό, στην ήδη υπάρχουσα διάταξη δικτύου εγκαθίσταται ένα ακόμη Interface και back up αυτού, το Firewall, πριν από τους servers του εμπορικού πλοίου. Το Firewall είναι ένα τοίχος προστασίας το οποίο μπλοκάρει την κυκλοφορία βασιζόμενο στις πληροφορίες του δικτύου που είναι η διεύθυνση IP, η θύρα δικτύου (Port) και το πρωτόκολλο δικτύου. Πρακτικά, το Firewall είναι μία συσκευή ασφαλείας του δικτύου η οποία φιλτράρει την εισερχόμενη και εξερχόμενη κυκλοφορία βασισμένο σε προκαθορισμένους κανόνες (rules) που έχουν γραφτεί εκ των προτέρων. Η κύρια δυνατότητα που παρέχεται, είναι ότι οι κανόνες γράφονται από τον χρήστη και η παραμετροποίηση του ελέγχου γίνεται κατ' επιλογήν. Ο πίνακας που ακολουθεί (βλ. Πίνακας 3) αναδεικνύει τα κύρια χαρακτηριστικά του firewall. [30] [31] [32] [33]

Περιγραφή	Το Firewall είναι μία δικτυακή συσκευή ασφαλείας η οποία «φιλτράρει» όλη την εισερχόμενη και εξερχόμενη λειτουργία στο δίκτυο, βασιζόμενο στους προκαθορισμένους κανόνες
Αρχή Λειτουργίας	«Φιλτράρει» την κυκλοφορία στο δίκτυο με βάση τις διευθύνσεις IP και τον αριθμό των ports.
Λειτουργία Διαμόρφωσης	Λειτουργία επιπέδου 3 ή transparent mode
Τοποθέτηση	Στην inline περίμετρο του δικτύου
Κυκλοφοριακοί patterns	Δεν έχουν αναλυθεί
Τοποθεσία σε σχέση με άλλες συσκευές	Είναι η πρώτη γραμμής άμυνας το firewall
Ενέργεια σε ανίχνευση μη εξουσιοδοτημένης κυκλοφορίας	«Μπλοκάρει» την κυκλοφορία
Σχετικές ορολογίες	• Σταθερό φίλτρο πακέτο • Επιτρέπει και «μπλοκάρει την κυκλοφορία βάσει των port/protocol rules

Πίνακας 3: Χαρακτηριστικά Firewall



Εικόνα 24: Αρχιτεκτονική Δικτύου με Firewall

4.5 Παραμετροποίηση Firewall και Έλεγχος Κυκλοφορίας Δικτύου

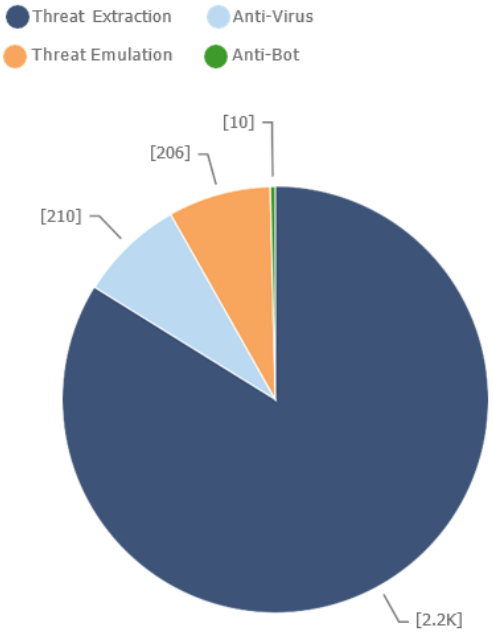
Εν συνεχεία της διπλωματικής μας εργασίας, στα πλαίσια της ασφάλειας του δικτύου ενός εμπορικού πλοίου, πραγματοποιήθηκε παραμετροποίηση firewall ναυτιλιακής εταιρείας και παρατίθεται το report όλης της διαδικτυακής κυκλοφοριακής κίνησης για τον μήνα Απρίλιο του 2022. Για προφανή λόγους το όνομα των χρηστών του δικτύου και της Ναυτιλιακής εταιρεία δεν αναγράφονται στην αναφορά που ακολουθεί.

4.5.1 Γενική Δραστηριότητα

Στο πρώτο σκέλος της αναφοράς που ανακτήσαμε σε βάθος ενός μήνα παρακολούθησης, αναφέρονται οι τύποι προστασίας δικτύου (βλ. Πίνακας 4) (βλ. Εικόνα 25), η αυστηρότητα που έχει ο κάθε τύπος ξεχωριστά και τα αρχεία καταγραφής (βλ. Πίνακας 5) που δημιουργήθηκαν σε όλη την διάρκεια της κίνησης για τον κάθε τύπο. Επιπλέον, παρατίθεται πίνακας με τις δραστηριότητες των κορυφαίων Malwares και τα logs που συνολικά ανακτήθηκαν για κάθε malware δραστηριότητα στο δίκτυο. Ακόμη, δίδεται ένα ιστόγραμμα (βλ. Εικόνα 26) στο διάστημα μίας εβδομάδας σχετικά με την δραστηριότητα των malwares και σε ποια κομβικά σημεία η δραστηριότητα αυτή ήταν πιο έντονη.

Protection Type	Severity	Logs
Content Removal	Critical	2.2K
DNS Reputation	High	160
HTTP Emulation	Informational	113
DNS Trap	High	14
Signature	Critical	8
File SystemEmulation	Critical	6
File Reputation	Low	5
SMTP Emulation	Critical	5
Total: 8 Protection Types	**Critical**	**2.5K**

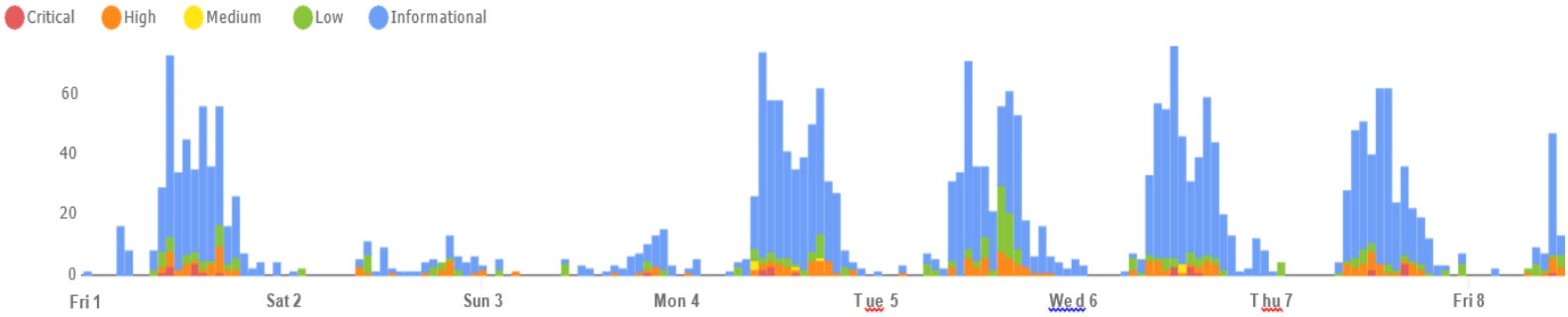
Πίνακας 4: Top Protections



Εικόνα 25: Active Blades

Verified	887
Not Supported	822
	275
Extracted	232
DNS server resolving a site known to contain malware for a client behind it	105
The file doesn't include cleanable parts	68
DNS query for a site known to contain malware	53
Active content was extracted from file	21
Access to site known to containmalware	14
Corrupted File	11
Oversized	9
Malicious network activity	8
Total: 41 Actions	**2.5K**

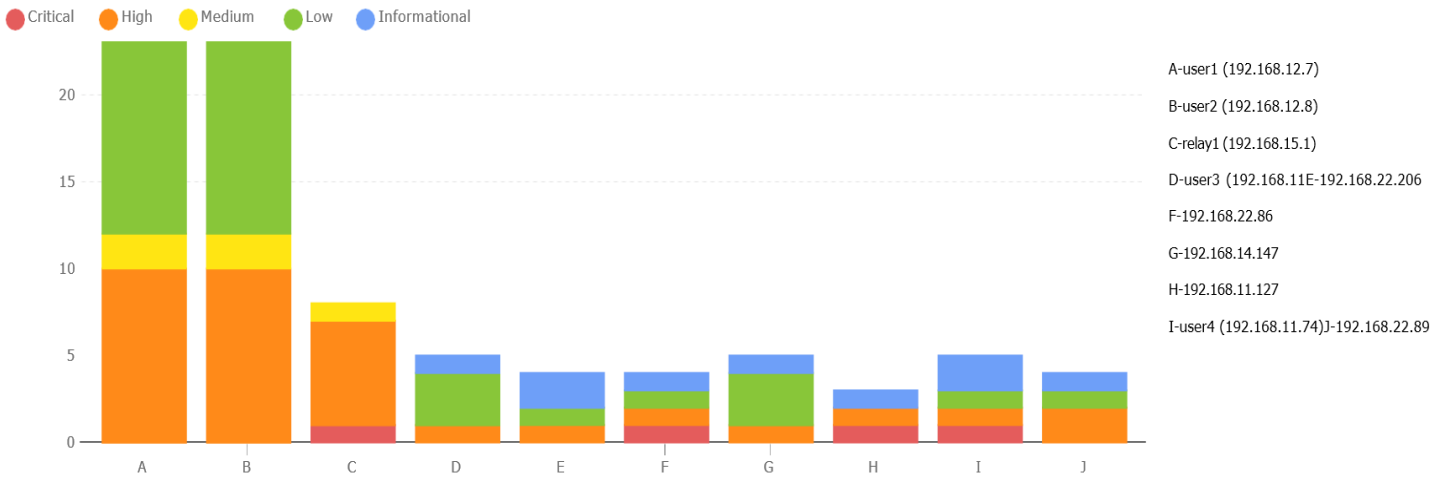
Πίνακας 5: Top Malware Activities



Εικόνα 26: Malware Activity την πρώτη βδομάδα του Απριλίου

4.5.2 Hosts

Παρατίθενται οι Top Hosts (βλ. Εικόνα 27) με βάσει των αριθμό περιστατικών που έχουν συμβεί. Στην συνέχεια, ακολουθεί πίνακας με τους τύπους προστασίας (βλ. Πίνακας 6) που πραγματοποιήθηκαν, την αυστηρότητα που είχαν και ποιες ενέργειες ολοκληρώθηκαν από τους hosts στην κάθε διεργασία.



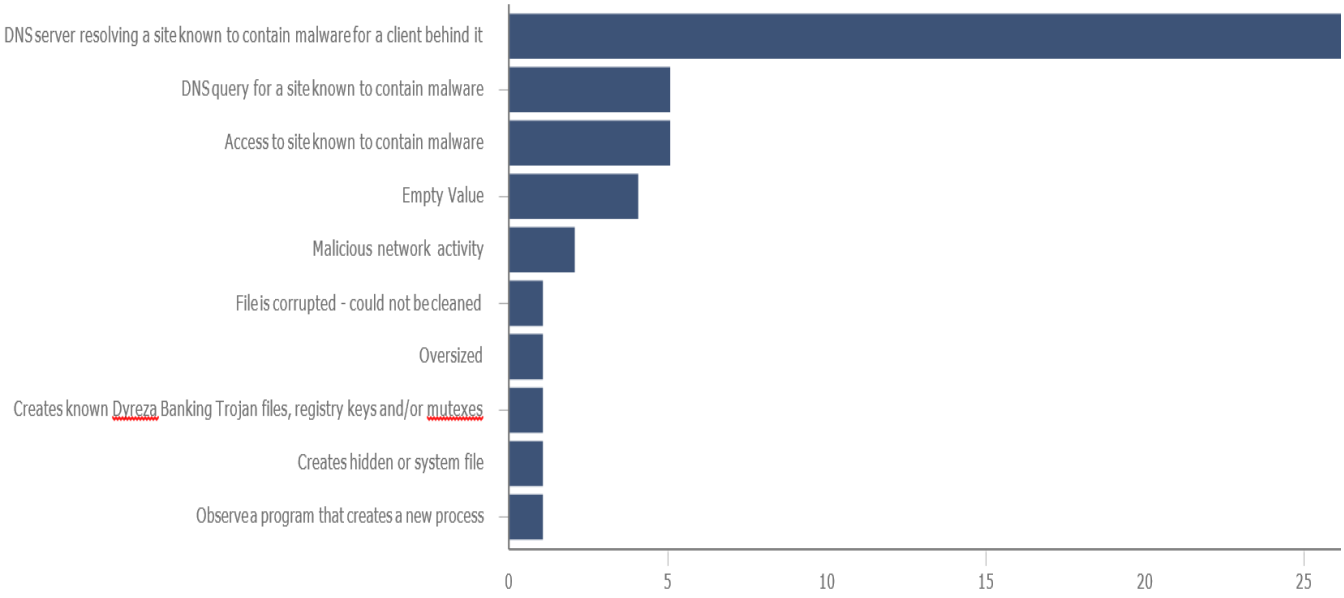
Εικόνα 27: Top hosts βάσει αριθμού περιστατικών

Source	Severity	Blade	Protection Name	Protection Type	Action
User6 (192.168.11.49)	Critical	Threat Extraction	Extract potentially malicious content	Content Removal	Extract
User5 (192.168.11.48)	Critical	Threat Extraction	Extract potentially malicious content	Content Removal	Extract
user4 (192.168.11.74)	Critical	Threat Emulation	Extract potentially malicious content	Content Removal	Detect Extract
User7 (192.168.11.68)	Critical	Threat Extraction	Extract potentially malicious content	Content Removal	Extract

Πίνακας 6: Top Hosts βάσει αυστηρότητας

4.5.3 Malwares

Οι κορυφαίες ενέργειας των malwares (βλ. Εικόνα 28) φαίνονται παρακάτω, όπως και ο αριθμός των logs (βλ. Πίνακας 7) στα οποία καταγράφηκαν οι δραστηριότητες τους. [39]



Εικόνα 28: Ενέργειες Malware

	Protection Name	Source	Logs
DNS server resolving a site known to contain malware for a client behind it	29 Protections	3 Sources	105
DNS query for a site known to containmalware	5 Protections	47 Sources	53
Access to site known to contain malware	5 Protections	8 Sources	14
Malicious network activity	2 Protections	2 Sources	8
Verified	1 Protection	98 Sources	887
Not Supported	1 Protection	157 Sources	822
Extracted	1 Protection	58 Sources	232
The file doesn't include cleanable parts	1 Protection	13 Sources	68

Πίνακας 7: Κορυφαίες δράσης Malware

4.5.4 Hosts με Αυστηρά Περιστατικά

Στο σημείο αυτό δίνονται οι hosts ανά περιστατικό (βλ. Πίνακας 8), με τον τύπο προστασίας που χρησιμοποιήθηκε, τα logs που δημιουργήθηκαν και ποια ήταν η δραστική ενέργεια επί των malwares.

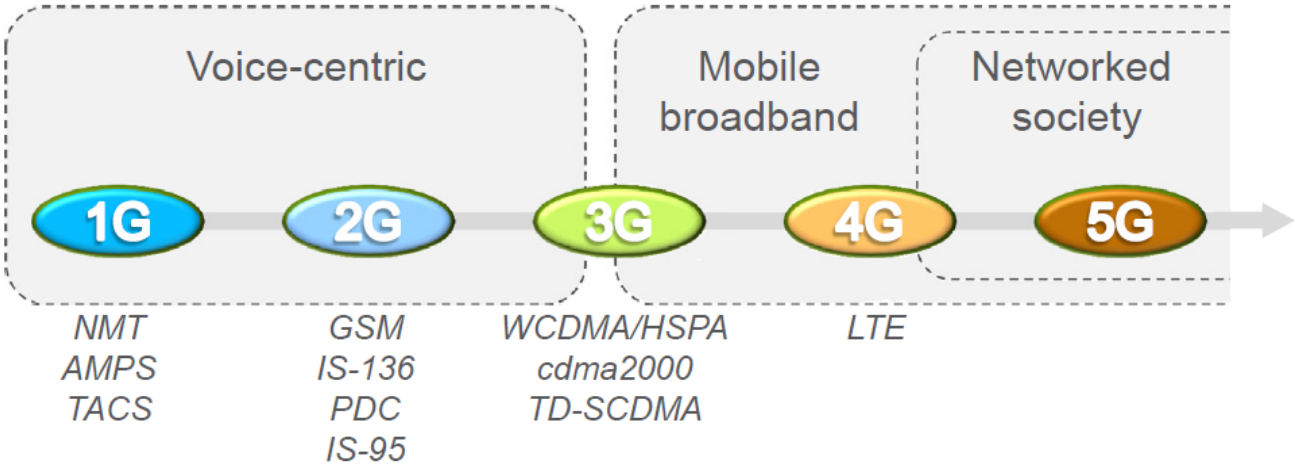
	Source	Severity	Protection Type	Protection Name	Malware Action	Logs
Threat Extraction	user5 (192.168.11.48)	Critical	Content Removal	Extract potentially maliciouscontent	Extracted	19
	user6 (192.168.11.49)	Critical	Content Removal	Extract potentially maliciouscontent	Extracted	15
	user7 (192.168.11.68)	Critical	Content Removal	Extract potentially maliciouscontent	Extracted	7
	192.168.22.183	Critical	Content Removal	Extract potentially maliciouscontent	Extracted	6
	user4 (192.168.11.74)	Critical	Content Removal	Extract potentially maliciouscontent	Active content was extractedfrom file	6
	user8 (192.168.11.65)	Critical	Content Removal	Extract potentially maliciouscontent	Extracted	3
	192.168.22.135	Critical	Content Removal	Extract potentially maliciouscontent	Extracted	2
	192.168.22.83	Critical	Content Removal	Extract potentially maliciouscontent	Extracted	2
	user9 (192.168.11.61)	Critical	Content Removal	Extract potentially maliciouscontent	Extracted	2
	192.168.22.86	Critical	Content Removal	Extract potentially maliciouscontent	Extracted	1

Πίνακας 8: Hosts με αυστηρά Περιστατικά

5. Η 5G Τεχνολογία στη Ναυτιλία

5.1 Ιστορική Αναδρομή της 5G τεχνολογίας

Τα συστήματα πρώτης γενιάς (1G) ήταν τα αναλογικά φωνητικά συστήματα κινητής τηλεφωνίας τη δεκαετία του 1980, συχνά διαθέσιμα σε εθνική βάση με περιορισμένη ή καθόλου διεθνή περιαγωγή. Τα συστήματα 1G περιλαμβάνουν NMT, AMPS και TACS. Η κινητή επικοινωνία ήταν διαθέσιμη πριν από τα συστήματα 1G, αλλά συνήθως σε μικρή κλίμακα και στόχευαν σε μια πολύ επιλεγμένη ομάδα ανθρώπων. Τα συστήματα δεύτερης γενιάς (2G) εμφανίστηκαν στις αρχές της δεκαετίας του 1990. Παραδείγματα 2G είναι οι τεχνολογίες που περιλαμβάνουν την ευρωπαϊκής προέλευσης τεχνολογία GSM, την αμερικανική IS-95/CDMA και τις τεχνολογίες IS-136/TDMA και την ιαπωνική τεχνολογία PDC. Τα συστήματα 2G εξακολουθούσαν να επικεντρώνονται στη φωνή, αλλά χάρη στο ότι ήταν αποκλειστικά ψηφιακά παρείχαν σημαντικά μεγαλύτερη χωρητικότητα από ό,τι τα προηγούμενα συστήματα 1G. Με τα χρόνια, ορισμένες από αυτές τις πρώιμες τεχνολογίες επεκτάθηκαν για την υποστήριξη (πρωτόγονων) υπηρεσιών πακέτων δεδομένων. Αυτές οι επεκτάσεις μερικές φορές αναφέρονται ως 2.5G για να υποδείξουν ότι έχουν τις ρίζες τους στις τεχνολογίες 2G αλλά έχουν ασήμαντα ευρύτερο φάσμα δυνατοτήτων από τις αρχικές τεχνολογίες. Το EDGE είναι γνωστό παράδειγμα τεχνολογίας 2.5G. Το GSM/EDGE εξακολουθεί να χρησιμοποιείται ευρέως σε smartphone αλλά χρησιμοποιείται επίσης συχνά για ορισμένους τύπους επικοινωνίας, τύπους μηχανής όπως συναγερμούς, συστήματα πληρωμών και παρακολούθηση ακινήτων. Οι πρωταρχικές υπηρεσίες δεδομένων που εισήχθησαν στο 2G ήταν τα μηνύματα κειμένου (Short Message Services - SMS) και υπηρεσίες μεταγωγής κυκλώματος για την αποστολή email και άλλων εφαρμογών αρχικά στους χαμηλούς ρυθμούς των 9.6 kbit/s. Υψηλότεροι ρυθμοί έγιναν δυνατοί στα εξελιγμένα 2G συστήματα αναθέτοντας περισσότερες χρονοθυρίδες σε ένα χρήστη. [13] [14] [8] [9] [19]

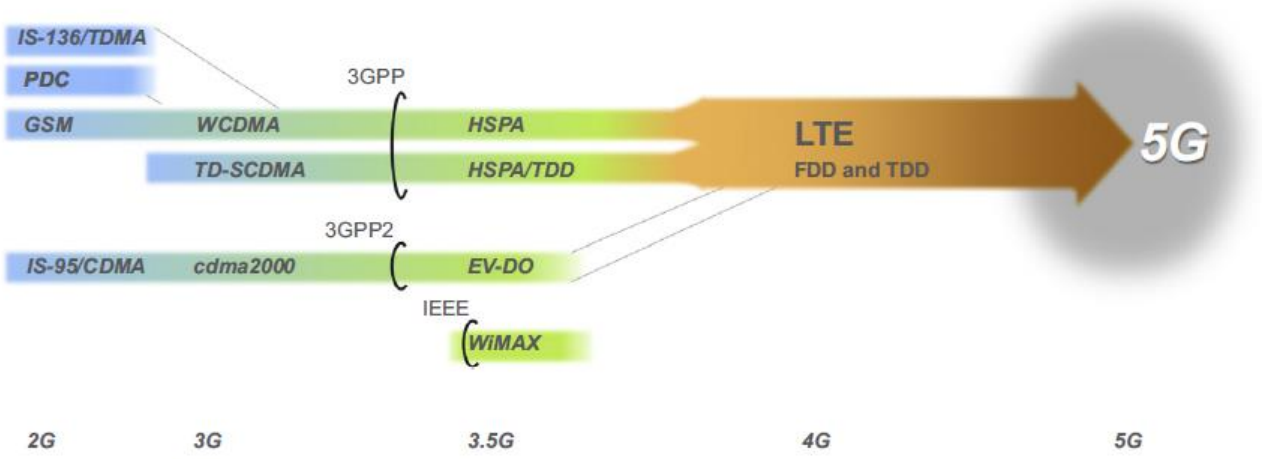


Εικόνα 29: Εξέλιξη Γενεών Δικτύου

Κατά τη δεκαετία του 1990, είχε αρχίσει να υπάρχει ανάγκη υποστήριξης όχι μόνο υπηρεσιών φωνής αλλά και δεδομένων, οδηγώντας την ανάγκη για μια νέα γενιά κυψελοειδών τεχνολογιών. Για να διασφαλιστεί η παγκόσμια εμβέλεια και για τις τεχνολογίες 3G έγινε αντιληπτό ότι η ανάπτυξη 3G έπρεπε να πραγματοποιηθεί σε παγκόσμια βάση. Προς διευκόλυνση αυτού, δημιουργήθηκε το Third-Generation Partnership Project (3GPP) για την ανάπτυξη των τεχνολογιών 3G WCDMA και TD-SCDMA. Λίγο μετά, ο παράλληλος οργανισμός 3GPP2 δημιουργήθηκε για να αναπτύξει την ανταγωνιστική 3G cdma2000 τεχνολογία, μια εξέλιξη της τεχνολογίας 2G IS-95. Η πρώτη κυκλοφορία του WCDMA οριστικοποιήθηκε το 1999. Περιλάμβανε κυκλώματα μεταγωγής, υπηρεσίες φωνής και βίντεο και υπηρεσίες δεδομένων μέσω μεταγωγής πακέτων. Οι πρώτες σημαντικές βελτιώσεις στο WCDMA ήρθαν με την εισαγωγή του High Speed Downlink Packet Access (HSDPA) στην έκδοση 5 ακολουθούμενη από ενισχυμένη ανοδική σύνδεση στην έκδοση 6, συλλογικά γνωστή ως High Speed Packet Access (HSPA) . HSPA, μερικές φορές αναφέρεται ως 3,5G, επιτρέπει μια «αληθινή» εμπειρία ευρυζωνικής κινητής τηλεφωνίας με ταχύτητες δεδομένων πολλών Mbit/s, διατηρώντας παράλληλα τη συμβατότητα με τις αρχικές προδιαγραφές 3G. Προσέφερε υποστήριξη για κινητό ευρυζωνικό, θεμέλιο για την ταχεία απορρόφηση έξυπνων τηλεφώνων όπως το iPhone και μεγάλης γκάμας συσκευών Android.

Η τεχνολογία 4G LTE (βλ. Εικόνα 29) αναπτύχθηκε από την αρχή για υποστήριξη πακέτων δεδομένων. Εν αντιθέσει, το 3G με το HSPA παρείχε πακέτα δεδομένων υψηλής απόδοση στηριζόμενη σε μια υπάρχουσα τεχνολογία. Οι υπηρεσίες ευρυζωνικής κινητής ήταν το επίκεντρο, με σκληρές απαιτήσεις για υψηλούς ρυθμούς δεδομένων, χαμηλής καθυστέρησης και υψηλής χωρητικότητας. Σημαντικές απαιτήσεις

μεταξύ των FDD (Frequency Division Duplexing) και TDD (Time Division Duplexing) λύσεων ήταν η ευελιξία του φάσματος και η μέγιστη συνάφεια. Αναπτύχθηκε επίσης μια νέα αρχιτεκτονική βασικού δικτύου, γνωστή ως Enhanced Packet Core (EPC), για να αντικαταστήσει την αρχιτεκτονική που χρησιμοποιείται από το GSM και WCDMA/HSPA. Η πρώτη έκδοση του LTE (βλ. Εικόνα 30) ήταν μέρος της έκδοσης 8 των προδιαγραφών 3GPP και η πρώτη εμπορική ανάπτυξη πραγματοποιήθηκε στα τέλη του 2009, ακολουθούμενη από μια ταχεία και παγκόσμια ανάπτυξη δικτύων LTE. [14] [8] [9] [47]

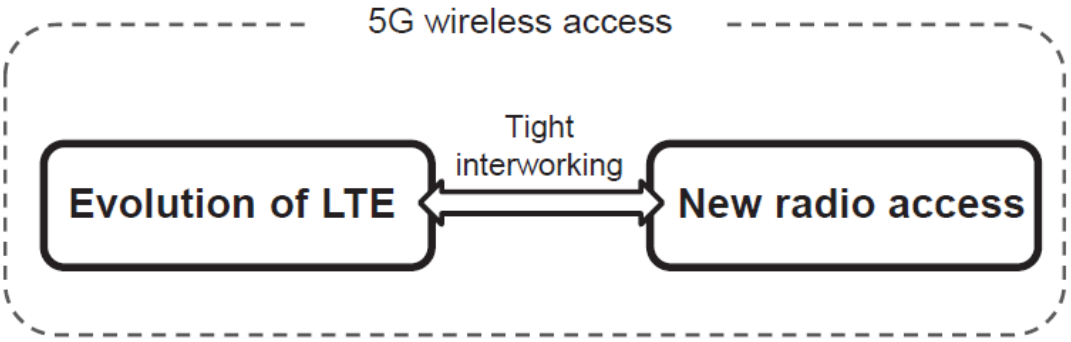


Εικόνα 30: Εξέλιξη Πολυπλεξίας Δικτύου

Η κινητή ευρυζωνική σύνδεση είναι αναπόσπαστο κομμάτι της μελλοντικής κινητής επικοινωνίας, αλλά τα μελλοντικά ασύρματα δίκτυα είναι σε μεγάλο βαθμό επίσης σημαντικά στο ευρύτερο φάσμα χρήσης. Πρακτικά, το 5G θεωρείται μια πλατφόρμα που επιτρέπει την ασύρματη σύνδεση με όλα τα είδη υπηρεσιών, υπάρχουσες καθώς και μελλοντικές μη γνωστές ακόμη υπηρεσίες, οδηγώντας τα ασύρματα δίκτυα ένα βήμα παρά πέρα από την κινητή ευρυζωνική σύνδεση. Θα παρέχεται συνδεσιμότητα οπουδήποτε, οποτεδήποτε σε οποιονδήποτε και οτιδήποτε. Διεύρυνση επικοινωνίας μεταξύ των μηχανών, όπως τα δίκτυα αισθητήρων στη γεωργία, η παρακολούθηση της κυκλοφορίας και η απομακρυσμένη διαχείριση του βοηθητικού εξοπλισμού στα κτίρια είναι ένας τύπος non-mobile-broadband εφαρμογών. Αυτές οι εφαρμογές κατά κύριο λόγο θέτουν απαιτήσεις πολύς χαμηλής κατανάλωσης ενέργειας της συσκευής, ενώ οι ρυθμοί δεδομένων και οι ποσότητες δεδομένων ανά συσκευή είναι χαμηλότερες. Πολλές από αυτές τις εφαρμογές μπορούν ήδη να υποστηριχθούν από την εξέλιξη του LTE. Η κίνηση στα ασύρματα δίκτυα αυξάνεται ραγδαία, όπως και οι προσδοκίες των χρηστών

για τους ρυθμούς δεδομένων, διαθεσιμότητας και καθυστέρησης. Αυτές οι βελτιωμένες απαιτήσεις πρέπει επίσης να αντιμετωπιστούν από το 5G ασύρματα δίκτυα.

Η αύξηση της χωρητικότητας μπορεί να γίνει με τρεις τρόπους: βελτιωμένη φασματική απόδοση, πυκνές αναπτύξεις δικτύου και αυξημένη ποσότητα φάσματος. Η φασματική απόδοση του LTE είναι ήδη υψηλή και παρόλο που μπορούν να γίνουν βελτιώσεις, δεν αρκούν για να ανταποκριθούν στην αύξηση της κυκλοφορίας. Πύκνωση δικτύου αναμένεται επίσης να συμβεί, τόσο στην χωρητικότητα, όσο και στην διαθεσιμότητα υψηλού ρυθμού δεδομένων. Ως εκ τούτου, έχει αυξηθεί, σε υψηλότερες ζώνες συχνοτήτων το φάσμα στο εύρος 3-6 GHz, ενώ στο εύρος 6-30 GHz δεν έχει σχεδιαστεί για κάθε LTE έχοντας αφήσει εν αναμονή την προσθήκη φάσματος. Ωστόσο, καθώς οι συνθήκες διάδοσης σε ζώνες υψηλότερης συχνότητας είναι μικρότερες ευνοϊκά για κάλυψη ευρείας περιοχής και απαιτούν πιο προηγμένες τεχνικές κεραίας όπως ο σχηματισμός δέσμης. Αυτές οι ζώνες μπορούν κυρίως να χρησιμεύσουν ως συμπλήρωμα στο υπάρχων, χαμηλότερης συχνότητας φάσμα (βλ. Εικόνα 31) . Το εύρος των απαιτήσεων για ασύρματα δίκτυα 5G είναι πολύ μεγάλο, απαιτώντας υψηλό βαθμό ευελιξίας δικτύου. [13] [14] [8] [9] [19] [48] [49]



Εικόνα 31: Εξέλιξη 5G Δικτύου

5.2 Θεωρητικό Υπόβαθρο 5G

Τα δίκτυα 5ης Γενιάς (5th Generation) καλύπτουν ένα μεγάλο φάσμα στο πεδίο των τηλεπικοινωνιακών συστημάτων με βασικό παρακλάδι το σύστημα 5G Vehicular Cloud Computing (5G-VCC), το οποία με την ταχεία εξέλιξη προσφέρει σύγχρονες υπηρεσίες στον μέσο χρήστη. Σε υποδομή που φέρει πρωτόκολλα 5G συναντάμε υπηρεσίες όπως το Cloud Computing (CC) , το Fog Computing (FC) , το Mobile Edge Computing (MEC) και τα Software Defined Networks (SDN), που εφαρμόζονται στα δίκτυα των οχημάτων.

Επιπλέον, σε μία αρχιτεκτονική 5G, συνηθίζεται η ανάπτυξη πυκνών υποδομών πρόσβασης στο δίκτυο, γνωστές ως Ultra Dense Networks (UDN) . Στο εν λόγω περιβάλλον ασύρματης πρόσβασης χρησιμοποιούνται ετερογενείς τεχνολογίες για τη μεταφορά των δικτυακών υπηρεσιών από το Cloud στον εκάστοτε εξοπλισμό.

5.3 Η Σταδιακή Ανέλιξη του 5G

Το πρώτο σημείο όπου το 5G έχει αρχίσει να αξιοποιείται είναι το ίδιο το λιμάνι. Ιδίως για τα εμπορευματικά λιμάνια με τις τεράστιες αποθήκες και τους γερανούς που υπάρχουν σε αυτά, το 5G μπορεί να προσφέρει πολλά σε επίπεδα αυτοματοποίησης.

Σαν παράδειγμα μπορούμε να αναφέρουμε το λιμάνι του Ηνωμένου Βασιλείου Felixstowe (βλ. Εικόνα 32) .Το Felixstowe θα είναι το μεγαλύτερο λιμάνι του Ηνωμένου Βασιλείου που θα αναπτύξει την τεχνολογία 5G και το Διαδίκτυο των Πραγμάτων (IoT) για τη βελτίωση της παραγωγικότητας, της αποτελεσματικότητας και της ασφάλειας σε όλες τις βασικές λειτουργίες του. [10] [4]

Χρησιμοποιώντας ένα ιδιωτικό δίκτυο 5G που έχει εγκαταστήσει η εταιρία Three UK. Η εγκατάσταση του λιμανιού επιλέχθηκε ως μέρος του κυβερνητικού προγράμματος δοκιμών 5G για την προώθηση των επενδύσεων και της καινοτομίας στο 5G και για την υποστήριξη της ανάπτυξης νέων περιπτώσεων χρήσης και εμπορικής ανάπτυξης. [4]

Εικόνα 32: Το πρωτοπόρο λιμάνι Felixstowe του Ηνωμένου Βασιλείου

Το έργο θα δοκιμάσει τις δυνατότητες του 5G σε δύο περιπτώσεις χρήσης:

- ενεργοποίηση τηλεκατευθυνόμενων γερανών μέσω μετάδοσης CCTV
- την ανάπτυξη αισθητήρων Internet of Things και Τεχνητής Νοημοσύνης για τη βελτιστοποίηση του προγνωστικού κύκλου συντήρησης των γερανών .

Αξιοποιώντας την ταχύτητα, τη χαμηλή καθυστέρηση και την υψηλή χωρητικότητα του 5G, το έργο θα καταδείξει τα κέρδη παραγωγικότητας και αποδοτικότητας αυτής της τεχνολογίας, ενώ θα μειώσει τις απρογραμμάτιστες διακοπές λειτουργίας. [48]

5.4 Η συμβολή του 5G στην Ναυτιλία

Η έλευση του 5G έχει ξεκλειδώσει έναν ολόκληρο κόσμο δυνατοτήτων για πολλούς τομείς, ένας από τους οποίους είναι η ναυτιλιακή βιομηχανία. Τα λιμάνια διαδραματίζουν καθοριστικό ρόλο στην περιφερειακή ανάπτυξη και το διεθνές εμπόριο ενισχύει την οικονομία κάθε κράτους, γι' αυτό η διασφάλιση της λειτουργικής αποτελεσματικότητας στα λιμάνια είναι καίριας σημασίας. Στην πραγματικότητα, περίπου το 90% του παγκόσμιου εμπορίου βασίζεται στον ναυτιλιακό τομέα.

Η τέταρτη βιομηχανική επανάσταση έδωσε στα λιμάνια την υπόσχεση μετασχηματισμού και ψηφιοποίησης. Με την άνοδο του 5G, οι τηλεπικοινωνίες σε όλο τον κόσμο θα μπορούσαν να βοηθήσουν στην περαιτέρω ανάπτυξη βιώσιμων, φιλικών προς το περιβάλλον έξυπνων λιμένων.

Προκειμένου να διασφαλιστεί η λειτουργική αποτελεσματικότητα στις έξυπνες θύρες, πρέπει να υπάρχουν αξιόπιστα συστήματα επικοινωνιών που να υποστηρίζουν δίκτυα 5G. Αυτό συμβαίνει επειδή το δίκτυο πρέπει να μπορεί να χειρίζεται δεδομένα ελέγχου και δεδομένα πολλαπλών καναλιών. Τα παλαιού τύπου δίκτυα ανήκουν στο παρελθόν και ο ναυτιλιακός τομέας πρέπει τώρα να κοιτάξει μπροστά και να υιοθετήσει την αναδυόμενη τεχνολογία.

Αναδυόμενες τεχνολογίες όπως η τεχνητή νοημοσύνη (AI), το Διαδίκτυο των πραγμάτων (IoT) (βλ. Εικόνα 33), η ανάλυση μεγάλων δεδομένων, η αυτόνομη οδήγηση με το 5G να είναι οι λύσεις σε αυτά τα προβλήματα. Η ανάπτυξη του 5G στα λιμάνια όχι μόνο θα αυξήσει την ανταγωνιστικότητα, αλλά θα εξασφαλίσει υλικοτεχνική απόδοση και με τη σειρά του θα μειώσει το κόστος. Η χρήση των τεχνολογιών της πληροφορίας έχει αποδειχθεί εξαιρετικά επωφελής για τα λιμάνια. [50] [10]

Εικόνα 33: Φουτουριστική Απεικόνιση της Απομακρυσμένης Διασύνδεσης

Η χρήση του 5G σε ένα εξαιρετικά πυκνό περιβάλλον στο πλοίο θα μπορούσε να είναι ιδιαίτερα υποσχόμενη. Στην περίπτωση των επίγειων συστημάτων, το 5G θα μπορούσε να παρέχει βελτιωμένη κάλυψη που θα επέτρεπε το «μαζικό IoT». Αυτό αναφέρεται σε εκτεταμένη συνδεσιμότητα με χιλιάδες συσκευές που τροφοδοτούνται από IoT στην ίδια περιοχή. Το 5G έχει τη δυνατότητα να υποστηρίζει έναν τέτοιο πολλαπλασιασμό συνδεδεμένων συσκευών σε μια δεδομένη περιοχή που το 4G δεν μπορεί.

Αυτό θα μπορούσε επίσης να ισχύει για τεράστια πλοία μεταφοράς εμπορευματοκιβωτίων που μεταφέρουν εμπορεύματα μεταξύ των θαλασσών. Πολλές εταιρείες έχουν συζητήσει τον εξοπλισμό των εμπορευματοκιβωτίων με δυνατότητες IoT σε μια προσπάθεια αποτελεσματικής παρακολούθησης των εμπορευμάτων κατά τη μεταφορά. Εν ολίγοις, η βιομηχανία σχεδιάζει να δημιουργήσει πλωτά νησιά που θα περιέχουν ουσιαστικά τεράστιες ποσότητες συσκευών που τροφοδοτούνται από IoT και θα επεκταθεί με τον εξοπλισμό των αγαθών με συσκευές IoT κατά τη μεταφορά τους. Τα πλοία που εμπλέκονται σε αυτές τις λειτουργίες μπορεί να καταλήξουν να έχουν πάνω από 100.000 συσκευές και το 5G είναι το κατάλληλο για να αντιμετωπιστεί και να υποστηριχθεί. [49] [10]

5.4 Λύσεις Έξυπνων Λιμανιών με 5G

5.4.1 Απομακρυσμένος έλεγχος των γερανών

Ο απομακρυσμένος έλεγχος των γερανών θα μπορούσε να είναι εξαιρετικά επωφελής στο 5G, καθώς θα εξασφαλίσει τη διαχείριση σε πραγματικό χρόνο. Μερικοί από τους πιο συνηθισμένους γερανούς σε τερματικούς σταθμούς εμπορευματοκιβωτίων είναι οι γερανοί γερανογέφυρας που τοποθετούνται σε ράγα (RMG) και οι γερανοί γερανογέφυρας με ελαστικό (RTG). [60]

5.4.2 Επιτήρηση του χώρου με την χρήση καμερών

Τα εμπορευματοκιβώτια θα μπορούσαν να εντοπιστούν με βάση τις κάμερες γερανών με τεχνητή νοημοσύνη και την αυτόματη καταμέτρηση φορτίου. Σχετικά με την ασφάλεια, η αναγνώριση προσώπου θα μπορούσε να αναλύσει τις εκφράσεις του προσώπου των χειριστών που θα υποδεικνύουν εάν το άτομο είναι κουρασμένο, ανήσυχο, στρεσαρισμένο, νυσταγμένο ή ανήσυχο. Αυτό παρέχει απίστευτη εικόνα και προσθέτει ένα ακόμη μεγαλύτερο επίπεδο άνεσης στις λειτουργίες του λιμανιού. [60]

5.4.3 Πλοήγηση εξ αποστάσεως

Τα μη επανδρωμένα σκάφη επιτρέπουν στα πλοία να περνούν περισσότερο χρόνο στη θάλασσα. Επίσης, αυξάνει την παραγωγικότητα και μειώνει την εξάρτηση από ένα ανθρώπινο θέμα, γεγονός που το καθιστά εγγενώς λιγότερο επιρρεπές σε ανθρώπινα σφάλματα. [60] [61]

6. Σύνοψη και Συμπεράσματα

Η δημιουργία και η συντήρηση αρχιτεκτονικής που θα υποστηρίζει την κυβερνοασφάλεια στο πλοίο θα αποτυπώνει το αποτέλεσμα της σε ποικίλες πτυχές. Το συμπέρασμα όλων των παραπάνω είναι ότι οι ιδιόκτητες όλων των εταιριών και οι άνθρωποί που την επανδρώνουν θα πρέπει να ενημερωθούν και να καταλάβουν την σημαντικότητα της οικονομικής επένδυσης και ανθρωπίνου δυναμικού στην κυβερνοασφάλεια. Όσο το δυνατό ταχύτερα αντιληφθούν την ανάγκη αυτής της επένδυσης τόσο πιο “έτοιμοι” θα βρεθούν αντιμέτωποι σε μία επίθεση.

Πολλές εταιρείες αδυνατούν να ανταπεξέλθουν στις απαιτήσεις της σύγχρονης κυβερνοασφάλειας είτε λόγω έλλειψης εκπαιδευμένου ανθρωπίνου δυναμικού είτε έλλειψης χρόνου. Σε αυτές τις περιπτώσεις προτείνεται να απευθυνθούν σε λύσεις εξωτερικών παρόχων, εξειδικευμένων στο αντικείμενο της ασφάλειας. Συνήθως, οι εξωτερικές εταιρείες, προσφέρουν ένα πλήρες πρόγραμμα κάλυψης, ενημέρωσης και ασφάλειας επάνω στο αντικείμενο. Εγκαθίστανται ένα ειδικό λογισμικό παρακολούθησης κίνησης, το οποίο παρέχει πληροφορίες σχετικές με την κατάσταση του πλοίου. Αναλυτικότερα, παρουσιάζεται μία εικόνα από το σύνολο των hardware και software του πλοίου με πλήρης διαφάνεια (εκδόσεις software/hardware). Σχετικά με την ασφάλεια, παρέχεται η δυνατότητα άμεσης ενημέρωσης/δράσης του γραφείου σε περίπτωση πιθανής επίθεσης.

Στην προσπάθεια προσέγγισης της ραγδαίας εξέλιξής της τεχνολογίας, θα πρέπει να υπάρχει διαρκής επαγρύπνηση και εκπαίδευση στα ζητήματα της ψηφιακής ασφάλειας. Οι ναυτιλιακές εταιρείες χρειάζεται να ενημερώνονται και να ενημερώνουν για όποιο νέο θέμα ασφάλειας αντιμετωπίζουν και τα μέτρα ασφαλείας που πάρθηκαν. Νέος εξοπλισμός θα πρέπει να εγκατασταθεί στα πλοία προς υποστήριξη των παραπάνω αναγκών. Σύγχρονοι υπολογιστές, σύγχρονοι server και firewall είναι μερικά από τον ελάχιστο εξοπλισμό που μια εταιρεία θα χρειαστεί να έχει στο δυναμικό της.

Οι περισσότερες ναυτιλιακές εταιρείες έχουν ήδη ξεκινήσει κάνοντας βήματα συμμόρφωσης στα πρότυπα των νέων απαιτήσεων που θέτει ο IMO. Η τωρινή δομή των περισσότερων πλοίων δεν είναι επαρκής στην αντιμετώπιση ψηφιακών επιθέσεων και έτσι δημιουργείται ακόμη περισσότερο η ανάγκη βελτίωσης. Η κυβερνοασφάλεια ασχολείται με την προστασία των συστημάτων πληροφορικής, του υλικού και των αισθητήρων του πλοίου και της διαρροής δεδομένων από μη εξουσιοδοτημένη

πρόσβαση, χειραγώγηση και διακοπή. Οι πολιτικές και τα σχέδια για την ασφάλεια στον κυβερνοχώρο καλύπτουν διαφορετικούς τύπους κινδύνων, όπως την ακεραιότητα των πληροφοριών, τη διαθεσιμότητα συστήματος και υλικού στο πλοίο και στο γραφείο της ναυτιλιακής εταιρείας.

Στην συνέχεια παρατίθενται κάποια από τα πλεονεκτήματα που θα έχει μια ναυτιλιακή εταιρία η οποία θα επενδύσει σε αυτό το σκοπό .

- Συμμόρφωση στον κανονισμό που ελέγχει ο IMO.
- Την δυνατότητα της ασφαλέστερης απομακρυσμένης σύνδεσης στο πλοίο για παροχή υπηρεσιών IT και OT.
- Δημιουργία ελέγχου και διαχείρισης των εφαρμογών που λειτουργούν στο πλοίο. (asset management κ.α.).
- Την δημιουργία αντιγράφων ασφαλείας τοπικά αλλά και απομακρυσμένα για την εξασφάλιση των αρχείων ναυσιπλοΐας.
- Κατάτμηση του δικτύου ανάλογα με τις ανάγκες του (VLans, Business και crew internet).
- Παροχές 4G και 5G (όπου αυτές είναι διαθέσιμες) για ταχύτερη ανταλλαγή δεδομένων .

Παράλληλα θα πρέπει να αναφερθεί πως η εκπαίδευση θα μπορούσε να χαρακτηρισθεί ως πρωταρχικός παράγοντας περιορισμού των κυβερνοεπιθέσεων. Θα πρέπει να δοθεί κύρια προτεραιότητα στην ορθή χρήση των νέων τεχνολογιών στους ναυτικούς αλλά και στα γραφεία της εταιρίας. Οι ναυτικοί θα πρέπει να εκπαιδεύονται για τους κινδύνους που διακατέχει η χρήση του διαδικτύου προκειμένου να αποκομίσουν τα μέγιστα οφέλη της χρήσης του χωρίς να θέτουν σε πιθανό κίνδυνο ούτε τον εαυτό τους, ούτε τα πλοία στα οποία ταξιδεύουν. Θα πρέπει δηλαδή να διατηρηθεί μια ισορροπία μεταξύ ασφάλειας και λειτουργικότητας.

ΒΙΒΛΙΟΓΡΑΦΙΑ

[1] Juan Ignacio Alcaide, Ruth Garcia Llave "Critical infrastructures cybersecurity and the maritime sector," University of Cadiz, Sep. 2010.

[2] International Association of Dry Cargo Shipowners (NTERCARGO), InterManager, International Association of Independent Tanker Owners (INTERTANKO), International Chamber of Shipping (ICS), International Union of Marine Insurance (IUMI), Oil Companies International Marine Forum (OCIMF), Superyacht Builders Association (Sybass) and World Shipping Council (WSC) " The Guidelines on Cyber Security Onboard Ships Version 3, 2020.

[3] BIMCO, CLIA, ICS, INTERCARGO, INTERMANAGER, INTERTANKO, IUMI, OCIMF and WORLD SHIPPING COUNCIL, " The Guidelines on Cyber Security Onboard Ships Version 4", 2020.

[4] Dr. Patrick Verhoeven**,** Rachel White , Max Bobys, Lance Kaneshiro, Chronis Kapalidis, Pascal Ollivier , Frans van Zoelen, Ward Veltman , " PORT COMMUNITY CYBER SECURITY", 2020.

[5] Andrej Androjna, Tanja Brcko , Ivica Pavic and Harm Greidanus, "Assessing Cyber Challenges of Maritime Navigation," Journal of *Marine Science and Engineering, 2020*

[6] International Maritime Organization, "GUIDELINES ON MARITIME CYBER RISK MANAGEMENT," MSC-FAL.1/Circ.3, London, July 2017.

[7] RESOLUTION MSC.428(98), "MARITIME CYBER RISK MANAGEMENT IN SAFETY MANAGEMENT SYSTEMS," June 2017.

[8] Erik Dahlman, Stefan Parkvall , Johan Skold, "4G: LTE/LTE-Advanced for Mobile Broadband-Second Edition", Oxford, 2014.

[9] Erik Dahlman, Stefan Parkvall , Johan Skold, "4G: LTE/LTE-Advanced for Mobile Broadband-Third Edition", Oxford, 2016.

[10] Α. Καλούμενος, Ν. Ραδίτσας, “ Ανάλυση και αλληλεπίδραση του 5G IoT και Υπολογιστικό Νέφος”, Διπλωματική Εργασία, Τμήμα Μηχανικών Ηλεκτρονικών Υπολογιστικών Συστημάτων, ΑΕΙ ΠΕΙΡΑΙΑ Τ.Τ., 2017.

[11] Διεύθυνση Στρατηγικού Σχεδιασμού Κυβερνοασφάλειας-Τμήμα Απαιτήσεων και Αρχιτεκτονικής Ασφαλείας, Α.Π.: 17728, “ Cybersecurity Handbook - Βέλτιστες πρακτικές για την προστασία και την ανθεκτικότητα πληροφοριακών συστημάτων”, 2021.

[12] Γ. Μαργέτη, Δ. Σαλοδημήτρη, Σ. Ψωμά, “Η Σημασία και Προοπτικές της Εμπορικής Ναυτιλίας στην Ανάπτυξη της Ελληνικής Οικονομίας”, Τμήμα Λογιστικής, ΤΕΙ Δυτικής Ελλάδος, 2016.

[13] Dr. Ioannis P. Chochliouros Telecommunications Engineer, “The European Environment for 5G. Development: Overview and Challenges”. 5G PPP, 2020.

[14] Dr. Ioannis P. Chochliouros Telecommunications Engineer, “Small Cells, NFV and Cloud Computing as “5G Enablers”: The Framework of the 5G-PPP “SESAME” and “5G ESSENCE” projects”. 5G PPP, 2020.

[15] Hellenic Chamber of Shipping, “Ιστορική Αναδρομή”, 2022. [Ηλεκτρονικό]. Available:https://nee.gr/%CF%84%CE%BF%CE%BD%CE%B1%CF%85%CF%84%CE%B9%CE%BA%CE%BF-%CE%B5%CF%80%CE%B9%CE%BC%CE%B5%CE%BB%CE%B7%CF%84%CE%B7%CF%81%CE%B9%CE%BF/%CE%B9%CF%83%CF%84%CE%BF%CF%81%CE%B9%CE%BA%CE%AE-%CE%B1%CE%BD%CE%B1%CE%B4%CF%81%CE%BF%CE%BC%CE%AE/

[16] Isalos, “Η ιστορία της Ελληνικής Ναυτίλίας”, 2021. [Ηλεκτρονικό]. Available: https://www.isalos.net/i-elliniki-naftilia/history/

[17] Eve Jones, “The Evolution of The Maritime Industry & Job at Sea”, Martide Seafarer Blog, Jul. 2019. [Ηλεκτρονικό]. Available: https://www.martide.com/en/blog/seafarers/maritime-industry-from-then-until-now/

[18] Web team Ιονίου Πανεπιστημίου, “Ναυτιλιακή Ιστορία”, Ιόνιο Πανεπιστήμιο, Τμήμα Ιστορίας, 2022. [Ηλεκτρονικό]. Available: https://marehist.gr/gr/history/

[19] “Ιστορική Αναδρομή”, Πανεπιστήμιο Πειραιά. [Ηλεκτρονικό]. Available: https://dione.lib.unipi.gr/xmlui/bitstream/handle/unipi/1770/Provatas3.pdf?sequence=25&isAllowed=y

[20] Helmepa, “Τι είναι η Ναυτιλία;”, 2022. [Ηλεκτρονικό]. Available: https://www.helmepacadets.gr/gr/shipping/the-role-of-shipping

[21] Katie Chadd, “The History of Cybersecurity”, 2020. [Ηλεκτρονικό]. Available: https://blog.avast.com/history-of-cybersecurity-avast

[22] Viswa Group, MFAME, “Οδηγίες για τον Κυβερνοχώρο του 2021”, Jan. 2021. [Ηλεκτρονικό]. Available: https://mfame.guru/way-ahead-for-imo-from-2021-cyber-guidelines/

[23] Καπτ. Γ. Γεωργούλη Αξ. Ε.Ν.,” Κυβερνοεπιθέσεις στη Ναυτιλία: Η Σύγχρονη Απειλή Μπορεί να Περιοριστεί”, Aug. 2018. [Ηλεκτρονικό]. Available: https://www.isalos.net/2018/08/kyvernoepitheseis-sti-naftilia-i-synchroni-apeili-borei-na-perioristei/

[24] Stephen J. Bigelow Senio Technology Editor, Ben Lutkevich Technical Writer, “What is IT/OT Convergence? Everything you Need to Know”, 2021. [Ηλεκτρονικό]. Available: https://www.techtarget.com/searchitoperations/definition/IT-OT-convergence

[25] Elise Silagy, “Operation Technology vs. Information Technology: Differences, Similarities, & How They Intermix with Industrial Control Systems”, Nov. 2019. [Ηλεκτρονικό]. Available: https://virtualarmour.com/operational-technology-vs-information-technology-differences-similarities-how-the-intermix-with-industrial-control-systems/

[26] Mission Secure, “IMO 2021: Three Steps to Ensure IMO/ISM Cybersecurity Compliance”, Apr. 2021. [Ηλεκτρονικό]. Available: https://www.missionsecure.com/blog/imo-2021-three-steps-to-ensure-imo-cybersecurity-compliance

[27] Γ. Πουλαρας ENESEL SA, Σ. Σαμπάνης AMMITEC/GASLOG LNG, Θ. Σαρδής COSTAMARE SHIPPING, Β. Φωτεινιάς DANAOS SHIPPING, Μ. Χριστόφης DIAPLOYS GROUP, Κ. Κατσουλιέρης NORTH OF ENGLAND P&I CLUB, “ Οι Πραγματικές Προκλήσεις της Κυβερνοασφάλειας στη Ναυτιλίας”, Oct. 2020. [Ηλεκτρονικό]. Available: https://www.isalos.net/2020/10/isalosnet-oi-pragmatikes-prokliseis-tis-kyvernoasfaleias-sti-naftilia/

[28] Seatrade Maritime News, “Antwerp Incident Highlights Maritime IT Security Risk”, Apr. 2022. [Ηλεκτρονικό]. Available: https://www.seatrade-maritime.com/europe/antwerp-incident-highlights-maritime-it-security-risk

[29] Ελεάνα Χουτέα, “Πως Μπορεί να θωρακιστεί η Ναυτιλίας Απέναντι στης Κυβερνοαπειλές;”, Feb. 2019. [Ηλεκτρονικό]. Available: https://www.liberal.gr/apopsi/pos-mporei-na-thorakistei-i-nautilia-apenanti-stis-kubernoapeiles/241148

[30] Palo Alto Netowroks, “What is an Intrusion Prevention System?” , 2022. [Ηλεκτρονικό]. Available: https://www.paloaltonetworks.com/cyberpedia/what-is-an-intrusion-prevention-system-ips

[31] Rashmi Bhardwaj, “IDS vs IPS vs Firewall – Know the Difference”, 2021. [Ηλεκτρονικό]. Available: https://ipwithease.com/firewall-vs-ips-vs-ids/

[32] The Regents of the University of Michigan, “Differences Between IPS and Firewalls”, 2022. [Ηλεκτρονικό]. Available: https://its.umich.edu/enterprise/wifi-networks/network-security/ips-vs-firewalls

[33] Forcepoint, “What is an Intrusion Prevention System (IPS)?”, 2022. [Ηλεκτρονικό]. Available: https://www.forcepoint.com/cyber-edu/intrusion-prevention-system-ips

[34] National Security Agency, Cybersecurity Information, “Embracing a Zero Trust Security Model”, Feb. 2021. [Ηλεκτρονικό]. Available: https://media.defense.gov/2021/Feb/25/2002588479/1/1/0/CSI_EMBRACING_ZT_SECURITY_MODEL_UOO115131-21.PDF

[35] Computer Science Resource Center, “ Guide for Conducting Risk Assessments”. [Ηλεκτρονικό]. Available: https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final

[36] Andrew Howard, “2022 Cybersecurity Predictions”, Jan. 2022. [Ηλεκτρονικό]. Available: https://modernciso.com/2022/01/13/2022-cybersecurity-predictions/

[37] Balasubramanian Venkatramani, “A Hacker’s Prescription to Prevent Ransomware Attacks”, Aug. 2022. [Ηλεκτρονικό]. Available: https://www.securden.com/blog/tips-to-prevent-ransomware-attacks.html

[38] TitanHQ Web Titan, “Network Segmentation Best Practices to Improve Security”, Mar. 2021. [Ηλεκτρονικό]. Available: https://www.spamtitan.com/web-filtering/network-segmentation-best-practices/

[39] Spambrella Limited, “What is Emotet Malware and How is it Delivered?”, 2020. [Ηλεκτρονικό]. Available: https://www.spambrella.com/what-is-emotet-malware-and-how-is-it-delivered/

[40] Brian Rutledge, “Understanding the Cross-Site Scripting (XSS) Vulnerability”, May. 2019. [Ηλεκτρονικό]. Available: https://spanning.com/blog/cross-site-scripting-web-based-application-security-part-3/

[41] PureID, “ Forget Passwords & Stay Secure”, 2022. [Ηλεκτρονικό]. Available: https://www.pureid.io/

[42] CIS Bechmarks, “CisSecurity”, Apr. 2022. [Ηλεκτρονικό]. Available: https://www.cisecurity.org/cis-benchmarks/

[43] Softwaretestinghelp, “ Most Useful Network Scanning Tools”, Apr. 2022. [Ηλεκτρονικό]. Available: https://www.softwaretestinghelp.com/network-scanning-tools/

[44] Australian Government Australian Signals Directorate,” Implementing Application Control”, 2022. [Ηλεκτρονικό]. Available: https://www.cyber.gov.au/acsc/view-all-content/publications/implementing-application-control

[45] Gartner Inc, “What is Security Information and Event Management (SIEM)?”, 2022. [Ηλεκτρονικό]. Available: https://www.gartner.com/reviews/market/security-information-event-management

[46] National Cyber Security Center, “Incident Management”, 2022. [Ηλεκτρονικό]. Available: https://www.ncsc.gov.uk/collection/incident-management

[47] Ε. Σκόνδρας, “Ανάλυση και Βελτιστοποίηση της Επίδοσης Ασυρμάτων Δικτύων Επόμενης Γενιάς”, 2019. [Ηλεκτρονικό]. Available: https://dione.lib.unipi.gr/xmlui/handle/unipi/11989

[48] Hutchison Ports, “Port of Felixstowe Selected for UK Government 5G Trial”, Jan. 2021. [Ηλεκτρονικό]. Available: https://www.portoffelixstowe.co.uk/press/news-archive/port-of-felixstowe-selected-for-uk-government-5g-trial/

[49] Telecom Review, “Emerging 5G Use Cases for the Maritime Industry”, Aug. 2020. [Ηλεκτρονικό]. Available: https://www.telecomreview.com/index.php/articles/reports-and-coverage/4073-emerging-5g-use-cases-for-the-maritime-industry

[50] Maritimes, “Διαδίκτυο και Ναυτιλία – Χάσμα Τεχνολογίας”, 2022. [Ηλεκτρονικό]. Available: https://maritimes.gr/el/apopseis/29863-diadiktyo-kai-nautilia-xasma-texnologias

[51] Globatt, “Inmarsat”, Απρ. 2022. [Ηλεκτρονικό]. Available: https://www.globaltt.com/en/coverages-inmarsat.html

[52] U.S. Coast Guard Issues Alert after Ship Heading into Port of New York Hit by Cyberattack. [Ηλεκτρονικό]. Available:

https://www.forbes.com/sites/daveywinder/2019/07/09/u-s-coast-guard-issues-alert-after-ship-heading-into-port-of-new-yorkhit-by-cyberattack/?sh=6597dc5c41aa

[53] University of Texas Team Takes Control of a Yacht by Spoofing Its GPS. [Ηλεκτρονικό]. Available: https://newatlas.com/gps-spoofingyacht-control/28644/

[54] China Hackers Steal Data from US Navy Contractor—Reports. [Ηλεκτρονικό]. Available: https://www.bbc.co.uk/news/world-uscanada-44421785

[55] MSC Confirms Malware Attack CausedWebsite Outage. [Ηλεκτρονικό]. Available: https://www.seatrade-maritime.com/containers/msc-confirms-malware-attack-caused-website-outage

[56] Marine Firm James Fisher Reports Cyber Breach. [Ηλεκτρονικό]. Available: https://www.reuters.com/article/us-james-fisher-cybercrimeidUSKBN1XF1SQ

[57] Pentagon Orders Temporary Halt to US Navy Operations after Second Collision. [Ηλεκτρονικό]. Available: https://www.theguardian.com/us-news/2017/aug/21/us-destroyer-uss-john-s-mccain-damaged-after-collision-with-oil-tanker

[58] US Navy Ship Collides with South Korean Fishing Boat. [Ηλεκτρονικό]. Available: https://edition.cnn.com/2017/05/09/politics/fishingvessel-hits-us-navy-ship-south-korea/index.html

[59] 7 Sailors Missing, CO Injured after Destroyer USS Fitzgerald Collided with Philippine Merchant Ship. [Ηλεκτρονικό]. Available: https://news.usni.org/2017/06/16/destroyer-uss-fitzgerald-collides-japanese-merchant-ship

[60] Mohamed Amine Ben Farah , Elochukwu Ukwandu , Hanan Hindy , David Brosset , Miroslav BuresI, Ivan Andonovic and Xavier Bellekens, Cyber Security in the Maritime Industry: A Systematic Survey of Recent Advances and Future Trends. Jan. 2022.

[61] The Guidelines on Cyber Security onboard Ships - Version 4. [Ηλεκτρονικό]. Available: https://www.bimco.org/about-us-and-our-members/publications/the-guidelines-on-cyber-security-onboard-ships

[62] Inmarsat Technical Specifications. [Ηλεκτρονικό]. Available: https://www.inmarsat.com/en/index.html

[63] JRC Technical Specifications. [Ηλεκτρονικό]. Available: https://www.jrc.co.jp/eng/

[64] Furuno Products. [Ηλεκτρονικό]. Available: https://www.furuno.com/en/

[65] Information Technology Laboratory – NIST, COMPUTER SECURITY RESOURCE CENTER - CSRC, “Guide for Conducting Risk Assessments”, [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final

[66] “15 Best Network Scanning Tools”, Jun., 2022, [Online]. Available: https://www.softwaretestinghelp.com/network-scanning-tools/

[67] Center for Internet Security – CIS, “CIS Benchmarks”, [Online]. Available: https://www.cisecurity.org/cis-benchmarks/

[68] Australian Government – Australian Cyber Security Centre - ACSC, “Implementing Application Control”, Jun. 20. [Online]. Available: https://www.cyber.gov.au/acsc/view-all-content/publications/implementing-application-control

[69] WinOSBite, “25 Best Microsoft Active Directory Alternatives”, Aug. 20. [Online]. Available: https://www.winosbite.com/best-microsoft-active-directory-alternatives/

[70] WebTitan “Network Segmentation Best Practices to Improve Security”, Oct.. 21. [Online]. Available: https://www.spamtitan.com/web-filtering/network-segmentation-best-practices/

[71] National Security Agency/Cybersecurity Information, “Hardening Network Devices”, Augt. 20. [Online]. Available: https://media.defense.gov/2020/Aug/18/2002479461/-1/-1/0/HARDENING_NETWORK_DEVICES.PDF