ΔΙΕΘΝΕΣ
ΠΑΝΕΠΙΣΤΗΜΙΟ
ΤΗΣ ΕΛΛΑΔΟΣ

ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ
ΚΑΙ ΗΛΕΚΤΡΟΝΙΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

«Μελέτη της ασφάλειας των δικτύων»

Του φοιτητή
Μπάνου Σπυρίδων
Αρ. Μητρώου: 175090

Επιβλέπων
Αμανατιάδης Δημήτριος

Ημερομηνία 25/01/2025

Τίτλος Π.Ε. Μελέτη της ασφάλειας των δικτύων
Κωδικός Π.Ε. 24194
Ονοματεπώνυμο φοιτητή Μπάνος Σπυρίδων
Ονοματεπώνυμο εισηγητή Αμανατιάδης Δημήτριος
Ημερομηνία ανάληψης Π.Ε. 22/04/2024
Ημερομηνία περάτωσης Π.Ε. 26/01/2025

Βεβαιώνω ότι είμαι ο συγγραφέας αυτής της εργασίας και ότι κάθε βοήθεια την οποία είχα για την προετοιμασία της είναι πλήρως αναγνωρισμένη και αναφέρεται στην εργασία. Επίσης, έχω καταγράψει τις όποιες πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών, εικόνων και κειμένου, είτε αυτές αναφέρονται ακριβώς είτε παραφρασμένες. Επιπλέον, βεβαιώνω ότι αυτή η εργασία προετοιμάστηκε από εμένα προσωπικά, ειδικά ως διπλωματική εργασία, στο Τμήμα Μηχανικών Πληροφορικής και Ηλεκτρονικών Συστημάτων του ΔΙ.ΠΑ.Ε.

Η έγκριση της διπλωματικής εργασίας από το Τμήμα Μηχανικών Πληροφορικής και Ηλεκτρονικών Συστημάτων του Διεθνούς Πανεπιστημίου της Ελλάδος, δεν υποδηλώνει απαραιτήτως και αποδοχή των απόψεων του συγγραφέα, εκ μέρους του Τμήματος.

Πρόλογος

Η επιλογή του θέματος της παρούσας πτυχιακής εργασίας σχετίζεται άμεσα με την επαγγελματική ενασχόληση στον κλάδο της πληροφορικής και συγκεκριμένα στον τομέα των δικτύων και της ασφάλειάς τους. Η καθημερινή ενασχόληση με τα ζητήματα ασφαλείας και η συνεχής ανάγκη για προστασία των συστημάτων από σύγχρονες απειλές αποτέλεσαν το κύριο κίνητρο για την εμβάθυνση επιστημονικά σε αυτόν τον τομέα.

Η μελέτη της ιστορικής εξέλιξης της ασφάλειας δικτύων, των σύγχρονων προκλήσεων και των μελλοντικών τάσεων βοήθησε στην κατανόηση των τεχνολογιών και στρατηγικών που εφαρμόζονται για την προστασία των ψηφιακών υποδομών. Μέσα από την ερευνητική διαδικασία, αποκτήθηκαν πολύτιμες γνώσεις, οι οποίες ενίσχυσαν την επιστημονική κατάρτιση και προσέφεραν μια πιο ολοκληρωμένη οπτική.

Περίληψη

Η ασφάλεια δικτύων έχει αναδειχθεί σε κρίσιμο ζήτημα στη σύγχρονη ψηφιακή εποχή, όπου οι ραγδαίες τεχνολογικές εξελίξεις και η αυξανόμενη εξάρτηση από διασυνδεδεμένα συστήματα εκθέτουν τα δίκτυα σε ολοένα και πιο εξελιγμένες απειλές. Η παρούσα πτυχιακή εργασία εξετάζει την ιστορική ανάπτυξη, την εξέλιξη και τη σύγχρονη πραγματικότητα της ασφάλειας δικτύων. Η εργασία αναδεικνύει επίσης τις προκλήσεις που αντιμετώπισαν τα πρώιμα συστήματα και πώς αυτές διαμόρφωσαν τις σύγχρονες πρακτικές ασφάλειας.

Η εργασία αρχίζει με την ανάλυση των αρχικών φάσεων της δικτύωσης υπολογιστών και καταλήγει στο παγκόσμιο Διαδίκτυο και τα πρωτόκολλα στα οποία στηρίζεται η λειτουργία του. Εξετάζονται πρώιμοι μηχανισμοί ασφάλειας, όπως τα τείχη ασφαλείας και το λογισμικό antivirus, καθώς και σημαντικά περιστατικά που ανέδειξαν την ανάγκη για ισχυρά πρωτόκολλα ασφάλειας. Επιπλέον, αναλύεται η εξέλιξη του κακόβουλου λογισμικού, από τους πρώτους ιούς μέχρι τα σύγχρονα ransomware και botnets, καθώς και οι τεχνολογικές εξελίξεις που έχουν ως στόχο την αντιμετώπισή τους.

Η εργασία διερευνά τη σύγχρονη πραγματικότητα της ασφάλειας δικτύων, εστιάζοντας στις τρέχουσες απειλές, όπως το ηλεκτρονικό ψάρεμα (Phishing), οι επιθέσεις κατανεμημένης άρνησης υπηρεσίας και οι ευπάθειες του Διαδικτύου των Πραγμάτων (Internet of Things). Συζητούνται επίσης καινοτόμες λύσεις, όπως οι τεχνολογίες τεχνητής νοημοσύνης (Artificial Inteligence) για την ανίχνευση απειλών και οι τεχνικές κρυπτογράφησης, ως εργαλεία για την αντιμετώπιση αυτών των κινδύνων. Η εργασία εξετάζει επίσης μελλοντικές τάσεις όπως η κβαντική δικτύωση, η μετακβαντική κρυπτογραφία και η συμπεριφορική βιομετρία.

Συνδυάζοντας την ιστορική ανάλυση με τη διερεύνηση σύγχρονων ζητημάτων, η μελέτη προσφέρει μια ολοκληρωμένη κατανόηση της εξέλιξης της ασφάλειας δικτύων και των επιπτώσεών της στο μέλλον. Τα ευρήματα υπογραμμίζουν τη σημασία υιοθέτησης προληπτικών στρατηγικών και προηγμένων τεχνολογιών για την προστασία των ψηφιακών υποδομών.

«Μελέτη της ασφάλειας των δικτύων»

(Study of Network Security)

«Μπάνος Σπυρίδων»

(Banos Spyridon)

Abstract

Network security has emerged as a critical issue in the modern digital era, where rapid technological advancements and increasing reliance on interconnected systems expose networks to ever more sophisticated threats. This thesis examines the historical development, evolution, and current state of network security. It also highlights the challenges faced by early systems and how these challenges have shaped modern security practices.

The study begins with an analysis of the initial phases of computer networking and progresses to the global Internet and the protocols on which its operation is based. Early security mechanisms, such as firewalls and antivirus software, are examined, as well as significant incidents that underscored the need for robust security protocols. Additionally, the evolution of malware is analyzed, from the first viruses to modern ransomware and botnets, along with the technological advancements aimed at combating them.

The thesis explores the current landscape of network security, focusing on contemporary threats such as phishing, distributed denial-of-service (DDoS) attacks, and vulnerabilities in the Internet of Things (IoT). Innovative solutions are also discussed, including artificial intelligence (AI) technologies for threat detection and encryption techniques as tools for mitigating these risks. Furthermore, future trends such as quantum networking, post-quantum cryptography, and behavioral biometrics are examined.

By combining historical analysis with an investigation of contemporary issues, the study provides a comprehensive understanding of the evolution of network security and its implications for the future. The findings emphasize the importance of adopting proactive strategies and advanced technologies to protect digital infrastructures.

Ευχαριστίες

Θα ήθελα να ευχαριστήσω όλους όσοι στάθηκαν δίπλα μου και με στήριξαν κατά τη διάρκεια των σπουδών μου. Τα φοιτητικά μου χρόνια αποτέλεσαν ένα καθοριστικό κεφάλαιο στη ζωή μου, προσφέροντάς μου πολύτιμες γνώσεις και εφόδια για να αντιμετωπίσω τις μελλοντικές προκλήσεις.

Ευχαριστώ ιδιαίτερα τον επιβλέποντα καθηγητή της εργασίας μου, κ. Αμανατιάδη Δημήτριο, για την καθοδήγηση, την εμπιστοσύνη και τη συνεργασία του.

Κλείνοντας, θα ήθελα να εκφράσω τις πιο θερμές ευχαριστίες στην οικογένειά μου για τη διαρκή στήριξη και την ανεκτίμητη βοήθειά τους από την αρχή των σπουδών μου μέχρι σήμερα. Η ενθάρρυνσή τους υπήρξε καθοριστική για την ολοκλήρωση αυτής της προσπάθειας.

Περιεχόμενα

Κατάλογος Σχημάτων

Συντομογραφίες

Δ.Ε.	Διπλωματική Εργασία
ΔΙΠΑΕ	Διεθνές Πανεπιστήμιο Ελλάδος
Π.Ε.	Πτυχιακή Εργασία
AES	Advanced Encryption Standard
AOL	America Online
APT	Advanced Persistent Threat
CA	Certificate Authorities
CASB	Cloud Access Security Brokers
CERT	Computer Emergency Response Team
C&C	Command and Control
CSP	Cloud Service Provider
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
CTSS	Compatible Time-Sharing System
DARPA	Defense Advanced Research Projects Agency
DDoS	Distributed Denial of Service
DPI	Deep Packet Inspection
DNS	Domain Name System
EDR	Endpoint Detection and Response
GDPR	General Data Protection Regulation
HTML	HyperText Markup Language
HTTP	HyperText Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IAM	Identity and Access Management
IIOT	Industrial Internet of Things
IMP	Interface Message Processors
IoT	Internet of Things
IP	Internet Protocol
ISO	International Organization for Standardization
ISP	Internet Service Provider
LAN	Local Area Network

LLC	Logical Link Control
LPWAN	Low Power Wide Area Network
MAC	Media Access Control
MFA	Multi-Factor Authentication
ML	Machine Learning
NCP	Network Control Protocol
NCSA	National Center for Supercomputing Applications
NGFW	Next-Generation Firewalls
NPL	National Physical Laboratory
NSFNET	National Science Foundation Network
OSI	Open Systems Interconnection
PQC	Post Quantum Cryptography
QKD	Quantum Key Distribution
RAM	Random Access Memory
SAGE	Semi-Automatic Ground Environment
SDN	Software Defined Networking
SMTP	Simple Mail Transfer Protocol
SNA	Systems Network Architecture
SQL	Structured Query Language
SRI	Stanford Research Institute
TCP	Transmission Control Protocol
TTL	Time to Live
UDP	User Datagram Protocol
UCLA	University of California Los Angeles
URL	Uniform Resource Locator
V2X	Vehicle-to-Everything
WAN	Wide Area Network
WWW	World Wide Web

Κεφάλαιο 1 Εισαγωγή στα δίκτυα υπολογιστών

1.1 Πρόλογος

Τα δίκτυα αποτελούν τη βάση της σύγχρονης επικοινωνίας και τεχνολογίας πληροφοριών. Ένα δίκτυο αποτελείται από ένα σύνολο διασυνδεδεμένων συσκευών, όπως υπολογιστές, διακομιστές, εκτυπωτές και μέσα αποθήκευσης, που επικοινωνούν μεταξύ τους μέσω ασύρματων ή ενσύρματων μέσων. Η επικοινωνία αυτή επιτυγχάνεται με χρήση συγκεκριμένων πρωτοκόλλων, δηλαδή κανόνων που καθορίζουν τη μετάδοση και λήψη δεδομένων.

1.2 Η έννοια των δικτύων

Η έννοια του δικτύου δεν είναι καινούρια. Στη δεκαετία του 1960, η ανάγκη για αποδοτικότερη επικοινωνία μεταξύ υπολογιστικών συστημάτων σε ερευνητικά και στρατιωτικά περιβάλλοντα οδήγησε στη δημιουργία των πρώτων δικτύων. Το ARPANET, το οποίο ξεκίνησε το 1969, θεωρείται το πρώτο σύγχρονο δίκτυο υπολογιστών και πρόδρομος του Διαδικτύου [1]. Ο αρχικός στόχος του ήταν η διασύνδεση πανεπιστημίων και ερευνητικών ιδρυμάτων στις Ηνωμένες Πολιτείες, ώστε να διευκολυνθεί η ανταλλαγή πόρων και δεδομένων. Το ARPANET ήταν το πρώτο δίκτυο που απέδειξε ότι η διασύνδεση απομακρυσμένων συστημάτων μπορούσε να είναι αξιόπιστη και αποδοτική [1].
Τα δίκτυα χωρίζονται σε διάφορους τύπους ανάλογα με την εμβέλεια και τη χρήση τους. Ένα Τοπικό Δίκτυο (Local Area Network - LAN) συνδέει συσκευές σε μια μικρή γεωγραφική περιοχή, όπως ένα γραφείο ή ένα πανεπιστήμιο. Από την άλλη, τα Δίκτυα Ευρείας Περιοχής (Wide Area Network - WAN), όπως το Διαδίκτυο, εκτείνονται σε μεγαλύτερες γεωγραφικές αποστάσεις, επιτρέποντας την επικοινωνία ανάμεσα σε διαφορετικές χώρες και ηπείρους.
Η εξέλιξη των δικτύων έχει φέρει επανάσταση στην ανθρώπινη δραστηριότητα, καθώς επιτρέπει την άμεση πρόσβαση σε πληροφορίες, την επικοινωνία σε πραγματικό χρόνο και την απομακρυσμένη εργασία. Παρά τα πλεονεκτήματα αυτά, η διασύνδεση των συσκευών δημιούργησε προκλήσεις, όπως η εξασφάλιση της ασφαλούς επικοινωνίας και της προστασίας των δεδομένων.
Τα πρώτα δίκτυα δεν ήταν σχεδιασμένα για να αντιμετωπίζουν απειλές. Η κύρια έμφαση δινόταν στη λειτουργικότητα και τη συνδεσιμότητα, με περιορισμένες προδιαγραφές ασφαλείας. Ωστόσο, με την αύξηση της πολυπλοκότητας και της κλίμακας τους, οι απειλές και οι προκλήσεις στον τομέα της ασφάλειας των δικτύων έγιναν πιο έντονες, καθιστώντας την ασφάλεια βασικό ζήτημα στη δικτύωση.

1.3 Η ιστορική εξέλιξη των δικτύων

Τα δίκτυα ξεκίνησαν από απλές δομές που εξυπηρετούσαν περιορισμένες ανάγκες διασύνδεσης, αλλά με την πάροδο των δεκαετιών εξελίχθηκαν σε παγκόσμιες υποδομές που υποστηρίζουν σχεδόν κάθε πτυχή της σύγχρονης ζωής. Από την πρώτη τους εμφάνιση σε ερευνητικά περιβάλλοντα, η ανάπτυξη των δικτύων χαρακτηρίζεται από την καινοτομία και την προσαρμοστικότητα, ανταποκρινόμενη στις ολοένα αυξανόμενες ανάγκες για αποδοτικότερη επικοινωνία.
Κατά τη δεκαετία του 1970, ένα σημαντικό επίτευγμα σημειώθηκε με την ανάπτυξη του Ethernet από τη εταιρία Xerox. Το Ethernet είναι ένα πρωτόκολλο δικτύωσης που επιτρέπει τη διασύνδεση υπολογιστικών συσκευών σε ένα τοπικό δίκτυο. Χρησιμοποιώντας ένα κοινό φυσικό μέσο, το Ethernet κατέστησε δυνατή τη γρήγορη και αξιόπιστη μετάδοση δεδομένων μεταξύ συσκευών. Η καινοτομία

αυτή, που αναπτύχθηκε από τους Robert Metcalfe και David Boggs, έθεσε τα θεμέλια για την ευρεία χρήση των τοπικών δικτύων σε επιχειρήσεις και ακαδημαϊκά ιδρύματα [2].
Η επόμενη σημαντική εξέλιξη ήταν η δημιουργία του πρωτοκόλλου TCP, που τέθηκε σε εφαρμογή στις αρχές της δεκαετίας του 1980. Αυτό το πρωτόκολλο έγινε ο ακρογωνιαίος λίθος της επικοινωνίας μεταξύ δικτύων, παρέχοντας τη δυνατότητα σύνδεσης διαφορετικών συστημάτων σε ένα ενιαίο δίκτυο [3]. Κατά τη δεκαετία του 1980, το δίκτυο NSFNET διαδέχθηκε το ARPANET [4], επεκτείνοντας τις δυνατότητες σύνδεσης μεταξύ πανεπιστημίων και ερευνητικών ιδρυμάτων. Αυτή η υποδομή έθεσε τις βάσεις για το εμπορικό Διαδίκτυο, που αναδύθηκε στις αρχές της δεκαετίας του 1990. Την ίδια περίοδο (1984) δημιουργήθηκε το μοντέλο OSI (Open Systems Interconnection) από τον Διεθνή Οργανισμό Τυποποίησης (International Organization for Standardization - ISO). Το μοντέλο OSI που είναι ένα εννοιολογικό πλαίσιο που περιγράφει τη δομή και τη λειτουργία των δικτύων επικοινωνίας μέσω επτά επιπέδων, παρέχει ένα κοινό πρότυπο για τη διαλειτουργικότητα των δικτυακών συστημάτων [17].

1.4 Η έννοια της ασφάλειας δικτύων

Οι βασικές έννοιες της ασφάλειας δικτύων έχουν διαχρονική σημασία και αποτελούν ζητούμενα για ασφαλή δίκτυα μέχρι σήμερα. Θα περιγραφεί η ιστορικής εξέλιξη της έννοιας της ασφάλειας των δικτύων.
Η ασφάλεια δικτύων αποτελεί ένα εξειδικευμένο πεδίο της τεχνολογίας πληροφοριών που ασχολείται με την προστασία των υποδομών, των δεδομένων και των καναλιών επικοινωνίας ενός δικτύου από κακόβουλες επιθέσεις, μη εξουσιοδοτημένη πρόσβαση και φυσικές ή τεχνικές απειλές. Στόχος της είναι να διασφαλίσει τρεις βασικές αρχές: την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα των δεδομένων [5]:

- Ο όρος εμπιστευτικότητα αναφέρεται στη διασφάλιση ότι οι πληροφορίες είναι προσβάσιμες μόνο από εξουσιοδοτημένους χρήστες. Αυτή η απαίτηση επιτυγχάνεται μέσω τεχνικών, όπως η κρυπτογράφηση των δεδομένων.
- Η ακεραιότητα διασφαλίζει ότι τα δεδομένα δεν αλλοιώνονται ή διαγράφονται κατά τη μεταφορά ή την αποθήκευσή τους, εάν δεν υπάρχει εξουσιοδότηση.
- Η διαθεσιμότητα διασφαλίζει ότι τα δεδομένα και οι υπηρεσίες του δικτύου είναι προσβάσιμα όταν χρειάζονται, αποτρέποντας τη διακοπή λειτουργίας λόγω επιθέσεων ή τεχνικών προβλημάτων.

Η ανάγκη για ασφάλεια δικτύων προέκυψε με την αύξηση της χρήσης υπολογιστικών συστημάτων και δικτύων, καθώς η διασύνδεση των συσκευών αύξησε τις πιθανότητες εκμετάλλευσης ευπαθειών. Ιστορικά, οι πρώτες απειλές περιλάμβαναν μη εξουσιοδοτημένη πρόσβαση σε τοπικά δίκτυα και την εξάπλωση κακόβουλου λογισμικού μέσω φυσικών μέσων, όπως δισκέτες. Με την εισαγωγή του Διαδικτύου, το εύρος και η πολυπλοκότητα των απειλών αυξήθηκαν, αφού αναπτύχθηκαν επιθέσεις νέου τύπου που εκμεταλλεύονται την φυσική έκταση, το τρόπο λειτουργίας σε φυσικό επίπεδο και την απρόσωπη φύση του διαδικτύου [6].
Η ασφάλεια δικτύων περιλαμβάνει την εφαρμογή τεχνικών και στρατηγικών, όπως τα τείχη προστασίας, τα συστήματα ανίχνευσης εισβολών, τη κρυπτογράφηση και τη χρήση πολιτικών ασφαλείας. Επιπλέον, η ανάπτυξη της τεχνητής νοημοσύνης έχει συμβάλει στον εντοπισμό και την αποτροπή απειλών σε πραγματικό χρόνο [7]. Παράλληλα, η διεθνής νομοθεσία για την προστασία δεδομένων, όπως ο Γενικός Κανονισμός για την Προστασία Δεδομένων (General Data Protection Regulation - GDPR), διαδραματίζει σημαντικό ρόλο στην ενίσχυση της ασφάλειας των δικτύων.

Συμπερασματικά, η έννοια της ασφάλειας δικτύων δεν αφορά μόνο την προστασία τεχνικών υποδομών αλλά και την εξασφάλιση της εμπιστευτικότητας και της λειτουργικότητας των συστημάτων. Καθώς οι απειλές εξελίσσονται, η συνεχής ανάπτυξη στρατηγικών και εργαλείων καθίσταται αναγκαία για τη διατήρηση της ασφάλειας σε έναν ολοένα και πιο διασυνδεδεμένο κόσμο.

1.5 Σημασία της Ασφάλειας Δικτύων

Η ασφάλεια δικτύων αποτελεί θεμελιώδη πυλώνα της σύγχρονης τεχνολογικής υποδομής, καθώς διασφαλίζει την προστασία των δεδομένων και των επικοινωνιών από απειλές και επιθέσεις. Σε έναν διασυνδεδεμένο κόσμο, όπου οι κυβερνήσεις, οι επιχειρήσεις και οι ιδιώτες βασίζονται σε δίκτυα υπολογιστών για την εκτέλεση καθημερινών δραστηριοτήτων, η ασφάλεια δικτύων εξασφαλίζει την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα των πληροφοριών.

Η σημασία της ασφάλειας δικτύων γίνεται ιδιαίτερα εμφανής στις κρίσιμες υποδομές, όπως η ενέργεια, οι μεταφορές και η υγειονομική περίθαλψη. Μία επιτυχημένη διαδικτυακή επίθεση σε ενεργειακό δίκτυο για παράδειγμα θα μπορούσε να διακόψει τη τροφοδότηση ολόκληρων πόλεων, επηρεάζοντας την οικονομία της χώρας και την ασφάλεια των πολιτών. Αντίστοιχα, οι επιθέσεις σε τραπεζικά δίκτυα μπορεί να οδηγήσουν σε τεράστιες οικονομικές απώλειες και απώλεια εμπιστοσύνης στους θεσμούς [8].

Με την άνοδο του Διαδικτύου των Πραγμάτων (Internet of Things - IoT), η ασφάλεια δικτύων έχει αποκτήσει μεγαλύτερη σημασία. Το IoT αναφέρεται σε ένα σύνολο φυσικών συσκευών, όπως έξυπνα οικιακά συστήματα, αισθητήρες και συσκευές παρακολούθησης, που είναι διασυνδεδεμένες μέσω του διαδικτύου. Αυτές οι συσκευές επεκτείνουν το φάσμα επιθέσεων, καθώς οι κακόβουλοι χρήστες μπορούν να εκμεταλλευτούν τις ευπάθειες τους για να αποκτήσουν πρόσβαση σε δίκτυα ή να προκαλέσουν διακοπές στη λειτουργία τους.

Εξίσου ανησυχητική είναι η εξάπλωση απειλών με γνωστότερες το phishing και το ransomware. Το phishing είναι μια τεχνική εξαπάτησης κατά την οποία κακόβουλοι χρήστες προσπαθούν να αποκτήσουν ευαίσθητες πληροφορίες, όπως κωδικούς πρόσβασης ή στοιχεία πιστωτικών καρτών, μέσω ψεύτικων email ή ιστοσελίδων. Αντίστοιχα, το ransomware είναι ένα είδος κακόβουλου λογισμικού που κρυπτογραφεί τα δεδομένα ενός χρήστη και απαιτεί λύτρα για την απελευθέρωσή τους. Το φαινόμενο αυτό έχει επηρεάσει χιλιάδες οργανισμούς, προκαλώντας σοβαρές οικονομικές και επιχειρησιακές επιπτώσεις [9].

1.6 Επίλογος

Η εξέλιξη των δικτύων υπολογιστών έχει διαμορφώσει τον τρόπο με τον οποίο οι άνθρωποι επικοινωνούν, εργάζονται και ανταλλάσσουν πληροφορίες. Παράλληλα, η ασφάλεια δικτύων παραμένει κρίσιμο ζήτημα, καθώς η αυξανόμενη διασύνδεση φέρνει νέες προκλήσεις και απειλές. Η ανάγκη για αξιόπιστες και ασφαλείς υποδομές καθιστά αναγκαία τη συνεχή βελτίωση των τεχνολογιών και των μεθόδων προστασίας.

Κεφάλαιο 2 Εξέλιξη των δικτύων

2.1 Εισαγωγή

Τα δίκτυα υπολογιστών, όπως τα γνωρίζουμε σήμερα, ξεκίνησαν με την ιδέα της σύνδεσης πολλαπλών υπολογιστικών συστημάτων για την κοινή χρήση πόρων και την αποτελεσματική μεταξύ τους επικοινωνία. Η έννοια της δικτύωσης εμφανίστηκε ήδη από τη δεκαετία του 1960, καθοδηγούμενη από την ανάγκη για αποτελεσματική ανταλλαγή δεδομένων σε οργανισμούς και ερευνητικά ιδρύματα. Αυτές οι πρώτες προσπάθειες δικτύωσης έθεσαν τις βάσεις για το σημερινό Διαδίκτυο αλλά επίσης ανέδειξαν προκλήσεις που σχετίζονταν με τη διαχείριση και την ασφάλεια των δεδομένων.

2.2 Από τα τοπικά δίκτυα στο διαδίκτυο

Η κατανόηση της εξέλιξης των τεχνολογιών δικτύωσης, από τις πρώτες απόπειρες σύνδεσης υπολογιστών έως το σύγχρονο Διαδίκτυο, αποτελεί θεμέλιο για την κατανόηση των στρατηγικών για την ασφάλειά τους. Η κατανόηση αυτής της ιστορικής διαδρομής αναδεικνύει πώς οι αρχικές τεχνολογίες διαμόρφωσαν την αρχιτεκτονική των σημερινών δικτύων, ενώ παράλληλα εξηγεί την εμφάνιση απειλών και τρωτών σημείων. Επιπλέον, η μελέτη αυτής της εξέλιξης βοηθά να αναγνωρίσουμε πώς οι σύγχρονες πρακτικές ασφάλειας προσαρμόζονται για την προστασία πληροφοριών και τη διασφάλιση της εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας των δεδομένων. Σε αυτό το πλαίσιο η ιστορική αναδρομή που ακολουθεί έχει ιδιαίτερη σημασία.

2.2.1 Πρώιμες Απόπειρες Δικτύωσης τη δεκαετία του 1950

Η περίοδος 1950-1960 αποτέλεσε τη βάση για την ανάπτυξη της δικτύωσης, καθώς οι πρώτες τεχνολογίες που εξελίχθηκαν προσπάθησαν να συνδέσουν υπολογιστές για επικοινωνία και ανταλλαγή δεδομένων. Στη περίοδο αυτή, οι προσπάθειες βασίστηκαν κυρίως στις ήδη υπάρχουσες τεχνολογίες τηλεπικοινωνιών, όπως η τηλεγραφία και η τηλεφωνία.

Η βάση για την ανάπτυξη των πρώτων δικτύων την περίοδο αυτή ήταν η τεχνολογία μεταγωγής κυκλωμάτων (circuit switching). Η μεταγωγή κυκλωμάτων είναι μια μέθοδος επικοινωνίας κατά την οποία δημιουργείται μια αποκλειστική γραμμή φυσικής σύνδεσης μεταξύ δύο σημείων κατά τη διάρκεια της επικοινωνίας. Αυτή η τεχνολογία, που ήταν η βάση των τηλεφωνικών δικτύων, παρείχε σταθερότητα αλλά είχε περιορισμούς, όπως την αδυναμία διαμοιρασμού της γραμμής με άλλα μέρη κατά τη διάρκεια της σύνδεσης [10].

Κατά τη δεκαετία του 1950, η ανάγκη για συντονισμό στρατιωτικών και επιστημονικών έργων οδήγησε στη δημιουργία πρώιμων συστημάτων επικοινωνίας μεταξύ υπολογιστών. Τα πρώτα modem (**mo**dulator-**dem**odulator) αναπτύχθηκαν αυτή τη δεκαετία και αποτέλεσαν τη γέφυρα μεταξύ ψηφιακών υπολογιστών και αναλογικών τηλεφωνικών δικτύων. Ένα modem αναλαμβάνει να μετατρέψει τα ψηφιακά σήματα ενός υπολογιστή σε αναλογικά για να μεταδοθούν μέσω τηλεφωνικών γραμμών και στη συνέχεια τα αναμετατρέπει σε ψηφιακά στο άλλο άκρο της σύνδεσης. Η τεχνολογία αυτή επιτάχυνε τη δυνατότητα απομακρυσμένης επικοινωνίας υπολογιστών, ιδιαίτερα σε στρατιωτικές εφαρμογές [11].

Στα τέλη της δεκαετίας του 1950, το Semi-Automatic Ground Environment (SAGE) ήταν ένα από τα πρώτα παραδείγματα αποκεντρωμένων δικτύων. Αναπτύχθηκε για την αεροπορική άμυνα των ΗΠΑ, συνδέοντας κεντρικούς υπολογιστές με σταθμούς ραντάρ. Αυτή η υποδομή ανέδειξε την ανάγκη για

αξιόπιστες δικτυακές δομές που μπορούσαν να λειτουργούν ακόμη και σε περιπτώσεις αστοχίας ενός μέρους του δικτύου [12].
Η έννοια του διαμοιρασμού χρόνου (time-sharing) ήταν επίσης επαναστατική και εμφανίστηκε αυτή την περίοδο, καθώς επέτρεψε τη χρήση ενός υπολογιστή από πολλούς χρήστες ταυτόχρονα. Αντί να εκτελείται ένα πρόγραμμα κάθε φορά, ο υπολογιστής διέθετε τον χρόνο του σε μικρά "κομμάτια" για διαφορετικούς χρήστες. Το Compatible Time-Sharing System (CTSS), που αναπτύχθηκε στο MIT το 1961, ήταν μια από τις πρώτες εφαρμογές αυτής της τεχνολογίας. Τα time-sharing συστήματα αποτέλεσαν τον πρόδρομο για δίκτυα που μπορούσαν να εξυπηρετούν πολλαπλούς χρήστες ταυτόχρονα, εισάγοντας έτσι την έννοια του εξυπηρετητή (server), μιας κεντρικής μονάδας που διαχειρίζεται και διαμοιράζει υπολογιστικούς πόρους στους συνδεδεμένους χρήστες [13].

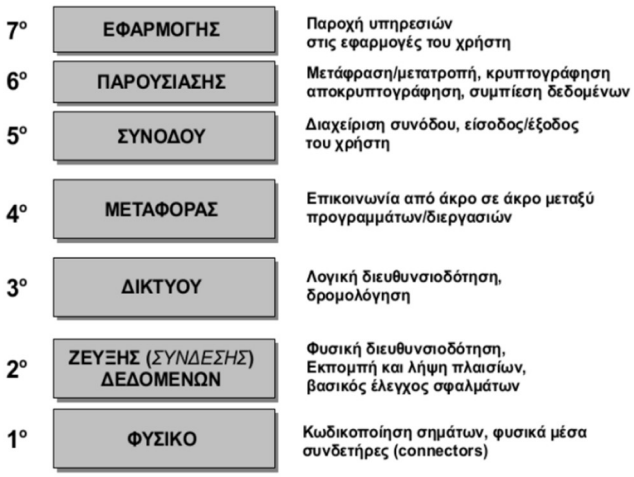
2.2.2 Η Ανάπτυξη της μεταγωγής πακέτων τη δεκαετία του 1960

Η δεκαετία του 1960 αποτέλεσε ορόσημο για την εξέλιξη των δικτύων, με την εισαγωγή της μεταγωγής πακέτων (packet switching), μιας επαναστατικής τεχνολογίας που έθεσε τις βάσεις για τη δημιουργία του σύγχρονου διαδικτύου. Σε αντίθεση με τη μεταγωγή κυκλωμάτων (circuit switching), όπου απαιτείται μια αποκλειστική φυσική σύνδεση μεταξύ δύο σημείων, η μεταγωγή πακέτων διαιρεί τα δεδομένα σε μικρά κομμάτια (πακέτα), τα οποία ταξιδεύουν ανεξάρτητα μέσω του δικτύου, μέσω πιθανόν διαφορετικών κόμβων και τα επανενώνει στον προορισμό τους [14].
Η ιδέα προτάθηκε από τον Paul Baran στη RAND Corporation [14], με στόχο τη δημιουργία ανθεκτικών δικτύων για στρατιωτική χρήση. Ο Baran πρότεινε ένα αποκεντρωμένο σύστημα όπου η επικοινωνία θα παρέμενε λειτουργική ακόμη και σε περιπτώσεις καταστροφής τμημάτων του δικτύου. Παράλληλα, ο Donald Davies, στο National Physical Laboratory (NPL) στη Βρετανία, ανέπτυξε δουλεύοντας ανεξάρτητα μια παρόμοια ιδέα, υλοποιώντας μάλιστα ένα πειραματικό δίκτυο μεταγωγής πακέτων στα τέλη της δεκαετίας [15].
Η μεταγωγή πακέτων παρουσιάζει αρκετά πλεονεκτήματα. Το πρώτο από αυτά είναι η αποδοτικότητα καθώς οι γραμμές δικτύου χρησιμοποιούνται δυναμικά από πολλούς χρήστες. Το δεύτερο πλεονέκτημα είναι η αξιοπιστία αφού τα πακέτα μπορούν να ακολουθούν διαφορετικές διαδρομές σε περίπτωση βλάβης κάποιου κόμβου στο δίκτυο. Τέλος τα δίκτυα που χρησιμοποιούν μεταγωγή πακέτων έχουν μεγαλύτερη δυνατότητα κλιμάκωσης αφού μπορούν να επεκτείνονται εύκολα, υποστηρίζοντας μεγαλύτερο αριθμό χρηστών.
Ο Leonard Kleinrock συνέβαλε σημαντικά στην επιστημονική θεμελίωση της μεταγωγής πακέτων, παρουσιάζοντας τα πρώτα μαθηματικά μοντέλα για την αξιολόγηση της απόδοσης των δικτύων αυτής της τεχνολογίας [16]. Η εργασία του έπαιξε κεντρικό ρόλο στην ανάπτυξη του ARPANET, του πρώτου λειτουργικού δικτύου μεταγωγής πακέτων. Η δεκαετία του 1960 ολοκληρώθηκε με την αναγνώριση της μεταγωγής πακέτων ως βασικής τεχνολογίας για τη διασύνδεση δικτύων, ανοίγοντας τον δρόμο για την ανάπτυξη του ARPANET και τη μετέπειτα εξέλιξη του διαδικτύου.
Τα τοπικά δίκτυα (Local Area Network - LAN) εμφανίστηκαν επίσης στη δεκαετία του 1960 ως λύση για την κοινή χρήση πόρων σε περιορισμένα γεωγραφικά περιβάλλοντα, όπως γραφεία, πανεπιστημιουπόλεις και ερευνητικά κέντρα. Ένα LAN επιτρέπει σε συσκευές, όπως υπολογιστές και εκτυπωτές, να συνδέονται μέσω καλωδίων ή ασύρματων συνδέσεων για την ανταλλαγή δεδομένων. Η IBM υπήρξε πρωτοπόρος στην ανάπτυξη αυτών των δικτύων.

2.2.3 Το μοντέλο OSI

Το μοντέλο OSI (Open Systems Interconnection) είναι ένα θεωρητικό πλαίσιο που περιγράφει τη διαδικασία επικοινωνίας μεταξύ συσκευών σε ένα δίκτυο, χωρίζοντάς την σε επτά διακριτά επίπεδα [17]. Δημιουργήθηκε από τον Διεθνή Οργανισμό Τυποποίησης (International Organization for Standardization - ISO) το 1983 και προσφέρει μια κοινή γλώσσα για την κατανόηση της λειτουργίας και την αντιμετώπιση προβλημάτων στα δίκτυα. Το μοντέλο OSI αποτελεί τη βάση για την κατανόηση της λειτουργίας και της δομής των δικτύων, προσφέροντας έναν σαφή και οργανωμένο τρόπο προσέγγισης της επικοινωνίας μεταξύ συσκευών. Από την οπτική γωνία της ασφάλειας των δικτύων, το μοντέλο OSI είναι εξαιρετικά σημαντικό, καθώς κάθε επίπεδό του μπορεί να αποτελέσει στόχο επιθέσεων ή σημείο ευπαθειών. Έτσι το μοντέλο OSI παρέχει ένα θεωρητικό πλαίσιο για την εφαρμογή ολοκληρωμένων στρατηγικών ασφαλείας, διασφαλίζοντας την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα των δεδομένων. Η σημασία του μοντέλου OSI ως θεωρητική κατασκευή είναι εμβληματική.

Κάθε επίπεδο του μοντέλου OSI έχει συγκεκριμένες λειτουργίες και αλληλεπιδρά με τα γειτονικά του επίπεδα. Τα κατώτερα επίπεδα ασχολούνται με τη μεταφορά δεδομένων, ενώ τα ανώτερα διαχειρίζονται την αλληλεπίδραση με τον χρήστη. Το σχήμα 1 παρέχει μία βασική επισκόπηση των 7 επιπέδων του μοντέλου OSI.



Σχήμα 1.1 Επισκόπηση μοντέλου OSI

Τα εφτά επίπεδα του μοντέλου είναι:

1. **Φυσικό επίπεδο (Physical Layer)**

Το φυσικό επίπεδο είναι υπεύθυνο για τη φυσική μετάδοση των δεδομένων. Περιλαμβάνει στοιχεία όπως καλώδια, οπτικές ίνες, κεραίες και ραδιοκύματα. Στο επίπεδο αυτό, τα δεδομένα μετατρέπονται ανάλογα με το μέσο μετάδοσης σε ηλεκτρικά ή οπτικά σήματα ή ραδιοκύματα.

2. Επίπεδο σύνδεσης δεδομένων (Data Link Layer)

Αυτό το επίπεδο διαχειρίζεται την αξιοπιστια της μετάδοσης δεδομένων μεταξύ δύο συσκευών στο ίδιο δίκτυο. Χωρίζεται σε δύο υποεπίπεδα: το Media Access Control (MAC), που καθορίζει ποια συσκευή μπορεί να χρησιμοποιήσει το μέσο μετάδοσης και το Logical Link Control (LLC), που διαχειρίζεται τη ροή δεδομένων μεταξύ των συσκευών που επικοινωνούν. Παράδειγμα πρωτοκόλλου που λειτουργεί σε αυτό το επίπεδο αποτελεί το Ethernet.

3. Επίπεδο δικτύου (Network Layer)

Το επίπεδο αυτό καθορίζει τη δρομολόγηση των δεδομένων μεταξύ δικτυακών κόμβων. Είναι υπεύθυνο για την εύρεση της καλύτερης διαδρομής και τη διεύθυνση των δεδομένων μέσω αναγνωριστικών διευθύνσεων. Οι διευθύνσεις αυτές είναι μοναδικοί αριθμητικοί αναγνωριστικοί κωδικοί που χρησιμοποιούνται για την αναγνώριση συσκευών σε ένα δίκτυο υπολογιστών, όπως για παράδειγμα το Διαδίκτυο. Κάθε συσκευή που συνδέεται σε ένα δίκτυο, όπως ένας υπολογιστής, ένα smartphone ή ένας διακομιστής, χρειάζεται μια διεύθυνση για να επικοινωνεί με άλλες συσκευές. Παραδείγματα πρωτοκόλλων σε αυτό το επίπεδο είναι το IPv4 που χρησιμοποιεί διευθύνσεις μήκους 32 bit και το IPv6 που χρησιμοποιεί διευθύνσεις μήκους 128 bit.

4. Επίπεδο μεταφοράς (Transport Layer)

Το επίπεδο μεταφοράς διασφαλίζει ότι τα δεδομένα φτάνουν με ασφάλεια στον προορισμό τους, χωρίζοντάς τα σε μικρότερα τμήματα και επανασυνδέοντάς τα όταν φτάσουν στον προορισμό τους. Εδώ λειτουργούν πρωτόκολλα όπως το TCP (Transmission Control Protocol), που εξασφαλίζει αξιόπιστη παράδοση και το UDP (User Datagram Protocol), που δίνει έμφαση στην ταχύτητα, αλλά δεν εγγυάται την αξιόπιστη παράδοση των δεδομένων.

5. Επίπεδο συνόδου (Session Layer)

Το επίπεδο συνόδου διαχειρίζεται τις συνεδρίες επικοινωνίας μεταξύ δύο συσκευών. Δημιουργεί, συντηρεί και κλείνει τις συνδέσεις, εξασφαλίζοντας ότι η επικοινωνία διατηρείται σταθερή και αξιόπιστη. Για παράδειγμα, αν ένας χρήστης κατεβάζει ένα αρχείο, το επίπεδο συνεδρίας φροντίζει να συνεχίσει τη διαδικασία ακόμη και αν υπάρξει προσωρινή διακοπή.

6. Επίπεδο παρουσίασης (Presentation Layer)

Το επίπεδο παρουσίασης είναι υπεύθυνο για τη μορφοποίηση των δεδομένων ώστε να είναι κατανοητά από την εφαρμογή ή τον χρήστη. Περιλαμβάνει λειτουργίες όπως η κρυπτογράφηση, η συμπίεση και η κωδικοποίηση δεδομένων σε διαφορετικές μορφές. Για παράδειγμα, όταν ο χρήστης ενός δικτύου λάβει μια εικόνα, το επίπεδο αυτό εξασφαλίζει ότι θα εμφανιστεί σωστά, ανεξαρτήτως της συσκευής ή του λογισμικού.

7. Επίπεδο εφαρμογής (Application Layer)

Το ανώτερο επίπεδο του μοντέλου OSI συνδέει τον χρήστη με το δίκτυο μέσω εφαρμογών όπως τα προγράμματα περιήγησης, ηλεκτρονικού ταχυδρομείου και ανταλλαγής μηνυμάτων. Παραδείγματα πρωτοκόλλων σε αυτό το επίπεδο είναι το HTTP για περιήγηση στο διαδίκτυο, το SMTP για αποστολή ηλεκτρονικού ταχυδρομείου και το FTP για μεταφορά αρχείων.

Το μοντέλο OSI αποτελεί έναν θεμελιώδη οδηγό για την κατανόηση της λειτουργίας των δικτύων και την οργάνωση της επικοινωνίας μεταξύ συσκευών. Από την οπτική της ασφάλειας, το OSI παρέχει ένα χρήσιμο πλαίσιο για τον εντοπισμό πιθανών ευπαθειών σε κάθε επίπεδο και την εφαρμογή στοχευμένων μέτρων προστασίας.

2.2.4 Δημιουργία και εξέλιξη του ARPANET (1969-1983)

Το 1983, είναι το έτος κατά την οποία εδραιώνεται η χρήση του TCP/IP (Transmission Control Protocol/Internet Protocol) ως κυρίαρχου πρωτοκόλλου σε δίκτυα μεταγωγής πακέτων.
Το ARPANET, η ανάπτυξη του οποίου ξεκίνησε το 1969, αποτέλεσε το πρώτο λειτουργικό δίκτυο μεταγωγής πακέτων και θεωρείται ο πρόδρομος του σύγχρονου διαδικτύου [10]. Δημιουργήθηκε από την ερευνητική υπηρεσία άμυνας των Ηνωμένων Πολιτειών DARPA (Defense Advanced Research

Projects Agency), με στόχο τη σύνδεση πανεπιστημίων και ερευνητικών κέντρων για την αποτελεσματική ανταλλαγή πληροφοριών και την προώθηση της επιστημονικής έρευνας.
Η πρώτη σύνδεση του ARPANET πραγματοποιήθηκε στις 29 Οκτωβρίου 1969, μεταξύ του πανεπιστημίου UCLA (University of California, Los Angeles) και του ινστιτούτου SRI (Stanford Research Institute). Το πρώτο μήνυμα που εστάλη ήταν η λέξη "LOG", αλλά το σύστημα κατέρρευσε μετά τα δύο πρώτα γράμματα. Παρόλα αυτά, το εγχείρημα θεωρήθηκε επιτυχές και άνοιξε τον δρόμο για περαιτέρω ανάπτυξη [10].
Η βασική υποδομή του ARPANET στηριζόταν στους λεγόμενους IMPs (Interface Message Processors), που λειτουργούσαν ως πρόδρομοι των σημερινών δρομολογητών και δρομολογούσαν τα πακέτα στον επόμενο κόμβο του δικτύου. Οι IMPs διαχειρίζονταν δηλαδή τη μεταγωγή πακέτων και τη σύνδεση μεταξύ υπολογιστών και του δικτύου. Μέχρι το 1973, το δίκτυο είχε επεκταθεί εκτός των Ηνωμένων Πολιτειών, συνδέοντας πανεπιστήμια στη Νορβηγία και τη Βρετανία, αποδεικνύοντας την παγκόσμια δυναμική του [1].
Το ARPANET χρησιμοποίησε αρχικά το πρωτόκολλο επικοινωνίας Network Control Protocol (NCP), το οποίο επέτρεπε τη βασική επικοινωνία μεταξύ υπολογιστών. Η λειτουργία του επικεντρωνόταν σε δύο βασικές λειτουργίες:

Α. Σύνδεση και επικοινωνία: Το NCP επέτρεπε σε δύο υπολογιστές να συνδεθούν μεταξύ τους και να ανταλλάξουν δεδομένα.
Β. Αξιοποίηση πόρων: Το NCP χρησιμοποιούσε έναν απλό μηχανισμό για τη διαχείριση πόρων του δικτύου, όπως αρχεία ή τερματικά, διευκολύνοντας την κοινή χρήση τους.

Το NCP ωστόσο δεν μπορούσε να υποστηρίξει τη διασύνδεση διαφορετικών δικτύων, καθώς δεν είχε ενσωματωμένες λειτουργίες για τη δρομολόγηση πακέτων από δίκτυο σε δίκτυο. Κατά τη δεκαετία του 1970, η ανάγκη για τη διασύνδεση διαφορετικών δικτύων οδήγησε στην ανάπτυξη του πρωτοκόλλου TCP/IP από τους Vinton Cerf και Robert Kahn [3]. Το TCP/IP αντικατέστησε το NCP το 1983, καθιερώνοντας ένα ενιαίο πρωτόκολλο για την επικοινωνία μεταξύ δικτύων. Η λειτουργία του βασίζεται σε δύο επίπεδα:

- Transmission Control Protocol (TCP):
  1. Εξασφαλίζει την αξιοπιστία της σύνδεσης.
  2. Διαιρεί τα δεδομένα σε πακέτα (στον αποστολέα) και τα επανασυναρμολογεί (στον παραλήπτη).
  3. Ελέγχει για τυχόν απώλειες ή σφάλματα στα δεδομένα και ζητά την επανεκπομπή τους αν χρειαστεί.
- Internet Protocol (IP):
  1. Ασχολείται με τη μεταφορά πακέτων δεδομένων από τον αποστολέα στον παραλήπτη.
  2. Διασφαλίζει ότι τα πακέτα βρίσκουν τη σωστή διαδρομή μέσω διαφορετικών κόμβων και δικτύων (δρομολόγηση).
  3. Χρησιμοποιεί διευθύνσεις δικτύου για την ταυτοποίηση των συσκευών.

Η δυνατότητα που δίνει το πρωτόκολλο TCP/IP για επικοινωνία μεταξύ διαφορετικών τύπων υπολογιστών και δικτύων, το κατέστησε το πιο ευέλικτο και ισχυρό πρωτόκολλο της εποχής του. Αυτή η δυνατότητα ήταν ο ακρογωνιαίος λίθος για τη δημιουργία του παγκόσμιου διαδικτύου. Παρακάτω αναλύεται σε μεγαλύτερο βάθος η στοίβα πρωτοκόλλων του TCP/IP και η δομή των πακέτων του ώστε να γίνει καλύτερα κατανοητός ο τρόπος λειτουργίας του διαδικτύου καθώς επίσης και οι απειλές και τα μέσα προστασίας που θα αναλυθούν στη συνέχεια.
Το διαδίκτυο όπως έχει ήδη αναφερθεί αποτελεί ένα δίκτυο δικτύων μεταγωγής πακέτων. Για την δρομολόγησή τους από τον αποστολέα στον τελικό προορισμό χρησιμοποιείται το Πρωτόκολλο Διαδικτύου (Internet Protocol ή IP). Η δομή των πακέτων του IP αποτελεί συνεπώς τη βάση της λειτουργίας του διαδικτύου, αφού επιτρέπει την αποστολή και λήψη δεδομένων μέσω αυτού. Το

πρωτόκολλο TCP με τη σειρά του αποτελεί το βασικότερο πρωτόκολλο στο επίπεδο μεταφοράς του διαδικτύου (4ο επίπεδο στο μοντέλο OSI) και εγγυάται την αξιόπιστη παράδοση των πακέτων στον παραλήπτη. Η στοίβα πρωτοκόλλων TCP/IP είναι συνεπώς κομβική για την λειτουργία του διαδικτύου. Το TCP/IP οργανώνει τα δεδομένα σε επίπεδα, καθένα με συγκεκριμένη λειτουργία και δομή. Η στοίβα πρωτοκόλλων TCP/IP περιλαμβάνει τέσσερα επίπεδα: το **επίπεδο εφαρμογών**, που περιλαμβάνει πρωτόκολλα όπως το HTTP για την επικοινωνία μεταξύ εφαρμογών, το **επίπεδο μεταφοράς,** το οποίο παρέχει αξιόπιστη μεταφορά δεδομένων μέσω του TCP, το **επίπεδο διαδικτύου,** που χειρίζεται τη δρομολόγηση και τη διευθυνσιοδότηση μέσω του IP (Internet Protocol) και το **επίπεδο πρόσβασης,** που ελέγχει τη φυσική μετάδοση δεδομένων [18].

Η μετάδοση ενός πακέτου με δεδομένα μέσω ενός συγκεκριμένου πρωτοκόλλου, συνεπάγεται την προσθήκη στα δεδομένα των πληροφοριών εκείνων που προδιαγράφει το πρωτόκολλο. Η προσθήκη αυτής της πληροφορίας γίνεται με την μορφή κεφαλίδων (headers) που προσκολλώνται στα προς μετάδοση δεδομένα (payload). Στην περίπτωση του TCP/IP πρέπει να υποστηρίζονται οι λειτουργίες της:

1. δρομολόγησης, ώστε το πακέτο να μπορεί να φτάσει με επιτυχία στον προορισμό του
2. ανασύνθεσης της πληροφορίας. Η λειτουργία αυτή είναι ζωτικής καθώς τα πακέτα ακολουθούν πιθανώς διαφορετικές διαδρομές μέχρι να φτάσουν στον προορισμό τους, συνεπώς δεν είναι εγγυημένο ότι θα φτάσουν με την σειρά που απεστάλησαν.

Τα πακέτα TCP/IP περιλαμβάνουν διάφορες κεφαλίδες που προστίθενται στα δεδομένα κατά τη μετάδοση. Η επικεφαλίδα IP (IP header) περιέχει πληροφορίες για τη δρομολόγηση και τη διευθυνσιοδότηση, όπως το πεδίο έκδοσης που καθορίζει την έκδοση IP (IPv4 ή IPv6), τη διεύθυνση προέλευσης και προορισμού που αντιστοιχεί στις IP διευθύνσεις του αποστολέα και του παραλήπτη και το πεδίο TTL (Time to Live) που ορίζει το όριο ζωής του πακέτου στο δίκτυο. Η επικεφαλίδα TCP (TCP header) περιλαμβάνει πεδία όπως τον αριθμό ακολουθίας, που χρησιμοποιείται για την επανασύνταξη των πακέτων με τη σωστή σειρά και το πεδίο ελέγχου ροής που εξασφαλίζει την ομαλή αποστολή δεδομένων. Το κύριο μέρος του πακέτου είναι τα δεδομένα (Payload), τα οποία περιέχουν τις πληροφορίες που μεταδίδονται [18].

2.2.5 Παράλληλες τεχνολογίες δικτύωσης (1970-1980)

Κατά τη δεκαετία 1970-1980, ενώ το ARPANET εδραίωνε τη θέση του ως πρωτοποριακό δίκτυο μεταγωγής πακέτων, διάφορες παράλληλες τεχνολογίες αναπτύχθηκαν για να εξυπηρετήσουν συγκεκριμένες ανάγκες και περιβάλλοντα δικτύωσης. Αυτές οι τεχνολογίες, αν και σε πολλές περιπτώσεις δεν επικράτησαν, έθεσαν τα θεμέλια για σύγχρονες πρακτικές και επηρέασαν την εξέλιξη του διαδικτύου.

Το **SNA** (Systems Network Architecture) Αρχιτεκτονική Δικτύων Συστημάτων που αναπτύχθηκε από την IBM το 1974 και ήταν ένα πρωτόκολλο δικτύωσης για τη διασύνδεση υπολογιστών σε εταιρικά περιβάλλοντα. Το SNA στηριζόταν σε μια ιεραρχική δομή, παρέχοντας σταθερότητα και ασφάλεια, αλλά με περιορισμένη ευελιξία. Ήταν ιδανικό για περιβάλλοντα με κεντρικούς υπολογιστές (mainframes) και τερματικά, αλλά δεν υποστήριζε την αποκεντρωμένη δομή που απαιτούσαν τα ευρύτερα δίκτυα όπως το διαδίκτυο [24].

Το **X.25,** που εισήχθη το 1976, ήταν μια πρώιμη τεχνολογία μεταγωγής πακέτων που χρησιμοποιούσαν κυρίως τηλεπικοινωνιακοί οργανισμοί. Το X.25 βασιζόταν στη δημιουργία εικονικών κυκλωμάτων, τα οποία εξασφάλιζαν αξιοπιστία μέσω συνεχούς ελέγχου λαθών. Αν και ήταν δημοφιλές για δίκτυα μακρινών αποστάσεων, το X.25 θεωρήθηκε λιγότερο αποδοτικό από τις αποκεντρωμένες τεχνολογίες, όπως το TCP/IP [19].

Το **Token Ring,** που αναπτύχθηκε από την IBM το 1980, ήταν μια τεχνολογία LAN που βασιζόταν στη μεταβίβαση ενός "token" για τη διαχείριση της κυκλοφορίας δεδομένων. Το Token Ring επικράτησε κυρίως σε εταιρικά περιβάλλοντα λόγω της σταθερότητας που προσέφερε σε δίκτυα με υψηλή κίνηση [20].
Το **Frame Relay** εμφανίστηκε στα τέλη της δεκαετίας του 1980 ως μια πιο αποδοτική εκδοχή του X.25 [21]. Χρησιμοποιούσε λιγότερους ελέγχους σφαλμάτων για ταχύτερη μεταγωγή πακέτων, γεγονός που το καθιστούσε ιδανικό για εταιρικά δίκτυα και δίκτυα ευρείας περιοχής (Wide Area Network - WAN).
Σημαντική καινοτομία στα τοπικά δίκτυα LAN υπήρξε το Ethernet, το οποίο αναπτύχθηκε τη δεκαετία του 1970 από το ερευνητικό κέντρο Xerox PARC [22]. Το Ethernet παρέχει υψηλής ταχύτητας, αξιόπιστη σύνδεση μεταξύ συσκευών, καθιστώντας το κυρίαρχο πρότυπο για τη διασύνδεση υπολογιστών σε μικρές περιοχές. Βασίζεται στην αρχή της χρήσης ενός κοινού φυσικού μέσου μετάδοσης, επιτρέποντας την ταυτόχρονη αποστολή δεδομένων από διαφορετικές συσκευές. Το **Ethernet** χρησιμοποιεί τον αλγόριθμο CSMA/CD (Carrier Sense Multiple Access with Collision Detection - CSMA/CD) για τον έλεγχο της μετάδοσης δεδομένων και την αποφυγή συγκρούσεων. Αυτές οι πρώιμες τεχνολογικές εξελίξεις κατάφεραν να επαναπροσδιορίσουν την έννοια της δικτύωσης για τη βελτίωση της παραγωγικότητας και της συνεργασίας. Αυτή η δεκαετία σήμανε ταχεία επέκταση των τεχνολογιών δικτύωσης, καθοδηγούμενη από την ανάγκη σύνδεσης όλο και πιο περίπλοκων συστημάτων διατηρώντας παράλληλα τη λειτουργική αποτελεσματικότητα. Εκτός από τη διευκόλυνση της ακαδημαϊκής έρευνας, τα δίκτυα αυτά έπαιξαν επίσης ζωτικό ρόλο σε κλάδους όπως ο τραπεζικός κλάδος, όπου εξορθολόγησαν τις λειτουργίες αυτοματοποιώντας διαδικασίες όπως οι μεταφορές κεφαλαίων. Το Ethernet παραμένει μέχρι σήμερα μια από τις πιο δημοφιλείς.

Στη δεκαετία του 1970, οργανισμοί άρχισαν να αναπτύσσουν επίσης **ενδοδίκτυα** (intranets), δηλαδή εσωτερικά κλειστά δίκτυα περιορισμένης πρόσβασης [23]. Τα ενδοδίκτυα προσφέρουν ασφαλή και αποδοτική ανταλλαγή πληροφοριών εντός ενός οργανισμού, ενώ περιορίζουν την πρόσβαση μόνο σε εξουσιοδοτημένους χρήστες. Χρήση ενδοδικτύων γίνονταν επίσης και από κυβερνητικές υπηρεσίες και ερευνητικά ιδρύματα. Ένα τέτοιο παράδειγμα είναι το δίκτυο ARPANET. Αν και η δομή του ARPANET βασιζόταν στην τεχνολογία των δικτύων ευρείας περιοχής WAN, λειτουργούσε ουσιαστικά ως ένα μεγάλο ενδοδίκτυο για τα πανεπιστήμια και τα εργαστήρια που συμμετείχαν. Η ανάπτυξη των ενδοδικτύων διευκόλυνε την πρόσβαση σε δεδομένα, ενώ ενίσχυσε την ασφάλεια περιορίζοντας τις εξωτερικές απειλές.

2.2.6 Η Παγκοσμιοποίηση των Δικτύων (1980-1990)

Η δεκαετία του 1980 ήταν καθοριστική για τη μετάβαση των δικτύων από περιορισμένα ακαδημαϊκά και στρατιωτικά συστήματα σε παγκόσμιες υποδομές που εξυπηρετούσαν ένα ευρύτερο κοινό, όπως οι επιχειρήσεις και οι οικιακοί χρήστες. Αυτή η περίοδος χαρακτηρίστηκε από τεχνολογικές καινοτομίες, όπως το NSFNET (National Science Foundation Network), η εισαγωγή του DNS και τη καθιέρωση του TCP/IP, που οδήγησαν στη σταδιακή παγκοσμιοποίηση των δικτύων.
Το NSFNET, που ξεκίνησε το 1986, αντικατέστησε το ARPANET ως το κύριο δίκτυο κορμού (backbone) για την υποστήριξη της ακαδημαϊκής και επιστημονικής έρευνας στις Ηνωμένες Πολιτείες. Με υψηλότερες ταχύτητες -56 Kbps αρχικά (που αναβαθμίστηκαν σε T1 γραμμές στα 1,5 Mbps το 1988) το NSFNET παρείχε σύνδεση σε πανεπιστήμια και ερευνητικά κέντρα σε ολόκληρες τις Η.Π.Α. [1]. Ένα βασικό χαρακτηριστικό του NSFNET ήταν η δυνατότητά του να διασυνδέει δίκτυα διαφορετικών προδιαγραφών μέσω του TCP/IP, ενθαρρύνοντας τη συνεργασία σε εθνικό και διεθνές επίπεδο.

Το δίκτυο σύντομα επεκτάθηκε εκτός των Ηνωμένων Πολιτειών, συνδέοντας ερευνητικά ιδρύματα από τη Βρετανία, τη Γαλλία και άλλες χώρες, γεγονός που συνέβαλε στην παγκόσμια εξάπλωση της δικτύωσης. Παρόλο που το NSFNET δημιουργήθηκε για ακαδημαϊκή χρήση, αποτέλεσε τη βάση για την εμπορικοποίηση των δικτύων στα τέλη της δεκαετίας.
Το Domain Name System (DNS), που εισήχθη το 1984, αποτέλεσε ένα σημαντικό βήμα που διευκόλυνε τη χρήση των δικτύων. Το DNS επέτρεψε την αντικατάσταση των αριθμητικών IP διευθύνσεων των υπολογιστών που φιλοξενούσαν πόρους ιστοτόπων (π.χ. 192.168.0.1) με φιλικά προς τον χρήστη ονόματα, όπως το www.example.com [25]. Αυτή η τεχνολογία απλοποίησε την πρόσβαση στο διαδίκτυο και έθεσε τα θεμέλια για τη μαζική υιοθέτηση από χρήστες που δεν διέθεταν τεχνικές γνώσεις.
Η περίοδος αυτή σηματοδοτεί και ακόμα μία σημαντική εξέλιξη. Ενώ μέχρι τη δεκαετία του 1980, τα δίκτυα ήταν περιορισμένα σε στρατιωτικές και ακαδημαϊκές εφαρμογές, η αυξανόμενη ανάγκη για σύνδεση μεταξύ επιχειρήσεων οδήγησε στην ανάπτυξη εμπορικών δικτύων και παρόχων υπηρεσιών διαδικτύου (Internet Service Providers - ISPs). Η ιδιωτικοποίηση του NSFNET το 1990 επέτρεψε την πλήρη εμπορική χρήση των υποδομών δικτύωσης, ανοίγοντας τον δρόμο για την ανάπτυξη παγκόσμιων υπηρεσιών, όπως το ηλεκτρονικό ταχυδρομείο και τις πρώτες πλατφόρμες ανταλλαγής δεδομένων [1].
Το TCP/IP, που καθιερώθηκε ως η σουίτα πρωτοκόλλων επικοινωνίας του διαδικτύου το 1983, αποτέλεσε τη βάση για τη διασύνδεση διαφορετικών δικτύων. Η δυνατότητα του TCP/IP να μεταφέρει δεδομένα αξιόπιστα μέσα από διαφορετικές υποδομές, σε συνδυασμό με την αυξανόμενη αποδοχή του από διεθνείς οργανισμούς και εταιρείες, οδήγησε στην ταχεία εξάπλωση του διαδικτύου παγκοσμίως. Ο ρόλος της σουίτας πρωτοκόλλων αυτού ήταν καταλυτικός για τη μετάβαση από την τοπική χρήση δικτύων σε μια παγκόσμια υποδομή.
Στα τέλη της δεκαετίας, η χρήση των δικτύων επεκτάθηκε πέρα από τα πανεπιστήμια και τις ερευνητικές εγκαταστάσεις, με εταιρείες, δημόσιους οργανισμούς και ιδιώτες να αξιοποιούν πλέον τις δυνατότητες του διαδικτύου. Η εμφάνιση του Usenet, μιας πλατφόρμας ανταλλαγής ειδήσεων και πληροφοριών, προσέφερε στους χρήστες έναν τρόπο για ανοιχτή επικοινωνία [26]. Παράλληλα, οι πρώτες υπηρεσίες ηλεκτρονικού ταχυδρομείου άνοιξαν νέους δρόμους στην επικοινωνία των ανθρώπων.
Η δεκαετία αυτή ολοκληρώθηκε με το διαδίκτυο να έχει ήδη εξελιχθεί σε μια παγκόσμια υποδομή, έτοιμη να επηρεάσει κάθε πτυχή της ανθρώπινης δραστηριότητας, θέτοντας τις βάσεις για την πλήρη παγκοσμιοποίηση των δικτύων.

2.2.7 Η εμφάνιση του World Wide Web (1989-1995)

Η εμφάνιση του World Wide Web (WWW) στα τέλη της δεκαετίας του 1980 και στις αρχές του 1990 αποτέλεσε μια από τις σημαντικότερες εξελίξεις στην ιστορία του διαδικτύου. Ενώ το διαδίκτυο ήδη υπήρχε ως δίκτυο μεταγωγής πακέτων, το WWW εισήγαγε μια νέα, φιλική προς τον χρήστη υπηρεσια που άλλαξε ριζικά τον τρόπο με τον οποίο οι άνθρωποι αποκτούσαν και μοιράζονταν πληροφορίες.
Το 1989, ο Tim Berners-Lee, ερευνητής στο CERN (Ευρωπαϊκός Οργανισμός Πυρηνικών Ερευνών), πρότεινε ένα σύστημα που θα επέτρεπε στους επιστήμονες να μοιράζονται έγγραφα εύκολα μέσω ενός ενιαίου δικτύου. Η πρότασή του βασιζόταν στη χρήση υπερκειμένων (hypertext), που θα συνδέονταν μεταξύ τους μέσω συνδέσμων (links). Το αποτέλεσμα ήταν η δημιουργία του πρώτου προτύπου του World Wide Web [27]. Το WWW βασίστηκε σε τρεις βασικές τεχνολογίες που ανέπτυξε ο Berners-Lee:

1. HTML (HyperText Markup Language): Η HTML είναι μια γλώσσα προγραμματισμού για τη δημιουργία ιστοσελίδων.
2. HTTP (HyperText Transfer Protocol): Το HTTP αποτελεί ένα πρωτόκολλο στο επίπεδο εφαρμογών για τη μετάδοση πληροφοριών ιστοσελίδων μέσω του διαδικτύου.

3. URL (Uniform Resource Locator): Το URL αποτελεί ένα σύστημα διευθύνσεων για την ταυτοποίηση και εύρεση πόρων στο διαδίκτυο.

Το 1991, δημιουργήθηκε η πρώτη ιστοσελίδα στο CERN, παρέχοντας πληροφορίες για το ίδιο το World Wide Web. Το έργο αυτό έγινε γρήγορα διαθέσιμο στο κοινό, επιτρέποντας σε οποιονδήποτε είχε πρόσβαση στο διαδίκτυο να δημιουργήσει και να μοιραστεί περιεχόμενο. Το 1993, ο Marc Andreessen και η ομάδα του στο NCSA (National Center for Supercomputing Applications) ανέπτυξαν τον Mosaic, τον πρώτο δημοφιλή περιηγητή διαδικτύου (browser), δηλαδή λογισμικού η λειτουργία του οποίου ήταν η πλοήγηση σε πόρους του WWW [28]. Το Mosaic έκανε το WWW πιο προσιτό στους χρήστες, καθώς προσέφερε γραφικό περιβάλλον και διευκόλυνε την πλοήγηση σε ιστοσελίδες. Λίγο αργότερα, το Mosaic αποτέλεσε τη βάση για τον Netscape Navigator, που κυριάρχησε στην αγορά των browsers την πρώτη περίοδο του διαδικτύου.

Το 1995, η εμπορική χρήση του διαδικτύου έφτασε σε νέα ύψη με την εμφάνιση εταιρειών όπως η Amazon και η eBay, που αξιοποίησαν το WWW για ηλεκτρονικό εμπόριο [29]. Παράλληλα, μεγάλες επιχειρήσεις δημιούργησαν ιστοσελίδες για να προσεγγίσουν πελάτες, ενώ η διαφήμιση στο διαδίκτυο άρχισε να γίνεται δημοφιλής. Η εμφάνιση του World Wide Web μετέτρεψε το διαδίκτυο από ένα εργαλείο για ειδικούς σε μια παγκόσμια πλατφόρμα επικοινωνίας, εκπαίδευσης, ψυχαγωγίας και εμπορίου. Η ευκολία πρόσβασης στις πληροφορίες, η δυνατότητα δημιουργίας περιεχομένου και η ταχύτητα διάδοσης ιδεών οδήγησαν στην επανάσταση της πληροφορίας που συνεχίζεται έως σήμερα, αλλά η μαζική εξάπλωση και χρήση σηματοδότησε νέες προκλήσεις ασφάλειας και τρωτά σημεία.

2.3 Επίλογος

Η εξέλιξη των δικτύων υπολογιστών αποτελεί μια αδιάκοπη πορεία καινοτομίας και τεχνολογικής ανάπτυξης. Οι θεμελιώδεις αρχές που καθιερώθηκαν τις πρώτες δεκαετίες, όπως η μεταγωγή πακέτων συνεχίζουν να αποτελούν τον πυρήνα των σύγχρονων συστημάτων επικοινωνίας. Η ιστορική αναδρομή ανέδειξε εκτός από τις τεχνολογικές εξελίξεις και τις αυξανόμενες προκλήσεις που συνοδεύουν τη διαρκή ανάπτυξη των δικτύων, όπως η διαχείριση της ασφάλειας και η ανάγκη για αξιόπιστες λύσεις προστασίας. Η κατανόηση αυτής της εξέλιξης είναι κρίσιμη για τη διαμόρφωση στρατηγικών που θα διασφαλίσουν τη σταθερότητα, την ασφάλεια και την αποδοτικότητα των μελλοντικών δικτυακών υποδομών.

Κεφάλαιο 3 Οι απειλές για τα δίκτυα υπολογιστών

3.1 Πρόλογος

Η ραγδαία ανάπτυξη των δικτύων υπολογιστών συνοδεύτηκε από την εμφάνιση και εξέλιξη διαφόρων απειλών που θέτουν σε κίνδυνο την ασφάλεια των πληροφοριών και την ακεραιότητα των συστημάτων. Η κατανόηση της φύσης αυτών των απειλών είναι απαραίτητη για τη διαμόρφωση αποτελεσματικών στρατηγικών αντιμετώπισης. Στο παρόν κεφάλαιο εξετάζονται οι βασικές κατηγορίες απειλών, η εξέλιξή τους μέσα στον χρόνο, καθώς και οι επιπτώσεις τους στην ασφάλεια των δικτύων.

3.2 Πρώιμα ζητήματα ασφαλείας

Καθώς τα δίκτυα υπολογιστών επεκτείνονταν από τα μέσα έως τα τέλη του 20ου αιώνα, η ασφάλειά τους βρίσκονταν συχνότερα στο επίκεντρο. Τα πρώτα δίκτυα σχεδιάστηκαν κυρίως για λειτουργικότητα και αποτελεσματικότητα, με ελάχιστη προσοχή στην ασφάλεια. Η εστίαση στη συνδεσιμότητα και την κοινή χρήση πόρων, ιδιαίτερα σε ερευνητικά και ακαδημαϊκά περιβάλλοντα, συχνά έγινε εις βάρος της διαφύλαξης ευαίσθητων πληροφοριών. Καθώς τα δίκτυα εξελίχθηκαν, άρχισαν να εμφανίζονται οι εγγενείς ευπάθειες του σχεδιασμού τους, γεγονός που ανέδειξε την ανάγκη για προληπτικά μέτρα ασφαλείας.

Κατά τη δεκαετία του 1960 και στις αρχές της δεκαετίας του 1970, **φυσικά περιστατικά** όπως πυρκαγιές, φυσικές καταστροφές, κλοπές και βανδαλισμοί αποτελούσαν σημαντικές απειλές για την αξιοπιστία και την ασφάλεια των ψηφιακών υποδομών. Ο δικτυακός εξοπλισμός, που συχνά στεγάζονταν σε κεντρικές εγκαταστάσεις, ήταν εξαιρετικά ευάλωτος σε περιβαλλοντικούς και ανθρώπινους παράγοντες, καθώς τα μέτρα ανθεκτικότητας όπως η αναπαραγωγή δεδομένων και τα αντίγραφα ασφαλείας σε απομακρυσμένες τοποθεσίες ήταν σπάνια ή ανύπαρκτα. Ο Thomas Whiteside [30] κατέγραψε μια σειρά από φυσικές επιθέσεις σε συστήματα ηλεκτρονικών υπολογιστών στις δεκαετίες του 1960 και του 1970. Οι επιθέσεις αυτές περιλαμβάνουν:
α. Τον πυροβολισμό ενός διασυνδεδεμένου υπολογιστή IBM στις Η.Π.Α. το 1968.
β. Την καταστροφή, από έκρηξη βόμβας, υπολογιστικών συστημάτων και αποθηκευμένων δεδομένων αξίας 16 εκατομμυρίων δολαρίων το 1970 στο Πανεπιστήμιο του Wisconsin.
γ. Την καταστροφή υπολογιστικού συστήματος από βόμβες μολότοφ στο Fresno State College το 1970.
δ. Την εκτόξευση βομβών μολότοφ από φοιτητές σε διασυνδεδεμένο υπολογιστή της Επιτροπής Ατομικής Ενέργειας το 1970 στο New York University.
ε. Την επίθεση με αιχμηρό αντικείμενο σε εξοπλισμό αποθήκευσης μαγνητικού μέσου υπολογιστικού συστήματος στη Νέα Υόρκη το 1972, που προκάλεσε ζημιά 589 χιλιάδων δολαρίων.

Αυτά τα περιστατικά δείχνουν ότι οι φυσικές απειλές επηρέασαν σημαντικά την ανάπτυξη πρακτικών ασφαλείας, συστημάτων πυρόσβεσης και αντιγράφων ασφαλείας εκτός τοποθεσίας, ανοίγοντας το δρόμο για τη σύγχρονη έμφαση στην ασφάλεια όχι μόνο των ψηφιακών αλλά και των φυσικών στοιχείων των δικτύων υπολογιστών.

Στην πρώτη περίοδο των δικτυωμένων υπολογιστών, τα συστήματα επίσης λειτουργούσαν σε σχετικά ελεγχόμενα περιβάλλοντα. Τα δίκτυα χρησιμοποιούνταν κυρίως από κυβερνητικά και ακαδημαϊκά ιδρύματα, όπου οι χρήστες θεωρούνταν αξιόπιστοι συνεργάτες. Ωστόσο, καθώς μεγάλωναν, οι προκλήσεις ασφαλείας έγιναν εμφανείς. Ένα από τα πρώτα τεκμηριωμένα περιστατικά ασφαλείας ήταν η εκμετάλλευση αδύναμων συστημάτων κωδικών πρόσβασης, τα οποία επέτρεψαν σε **μη εξουσιοδοτημένους χρήστες** να αποκτήσουν πρόσβαση σε ευαίσθητα δεδομένα. Το 1973, ο Robert Metcalfe ανέφερε πολλαπλές απόπειρες μη εξουσιοδοτημένης πρόσβασης στο δίκτυο ARPANET, τονίζοντας την ανάγκη για ισχυρές μεθόδους ελέγχου ταυτότητας [31].

3.3 Ορισμός του όρου κακόβουλο λογισμικό (malware)

Το κακόβουλο λογισμικό (malicious software ή malware) αποτελεί μια από τις μεγαλύτερες προκλήσεις στον τομέα της ασφάλειας των δικτύων, καθώς εξελίσσεται συνεχώς για να παρακάμπτει τις άμυνες και να εκμεταλλεύεται ευπάθειες. Ο όρος "malware" περιλαμβάνει κάθε είδους λογισμικό που έχει δημιουργηθεί με σκοπό την παραβίαση συστημάτων, την υποκλοπή δεδομένων, ή την πρόκληση ζημίας σε υπολογιστές και δίκτυα. Το malware έχει εξελιχθεί σε μια σοβαρή απειλή για ιδιώτες, επιχειρήσεις και κυβερνητικούς οργανισμούς.

Η κατανόηση των διαφόρων τύπων malware και της ιστορικής τους εξέλιξης είναι ζωτικής σημασίας για την ανάπτυξη αποτελεσματικών στρατηγικών ασφάλειας. Οι πρώτες μορφές malware δημιούργησαν το πλαίσιο για την κατανόηση των απειλών, ενώ οι σύγχρονες μορφές, συχνά πιο πολύπλοκες και στοχευμένες, απαιτούν συνεχή παρακολούθηση και προσαρμογή των μέτρων προστασίας.

Στις επόμενες ενότητες θα αναλυθούν οι κύριες κατηγορίες κακόβουλου λογισμικού και θα εξεταστεί η χρονική τους εξέλιξη. Μέσα από μια ιστορική ανασκόπηση, θα αναδειχθεί πώς οι διαφορετικές μορφές malware έχουν επηρεάσει τη χρήση και την ασφάλεια των δικτύων υπολογιστών από την εμφάνιση τους μέχρι σήμερα.

3.4 Ιοί και σκουλήκια (1970s-1980s)

Η δεκαετία του 1970 και του 1980 σηματοδότησε την αρχή της εμφάνισης κακόβουλου λογισμικού, όταν τα πρώτα malware δημιουργήθηκαν είτε για πειραματικούς σκοπούς είτε για να προκαλέσουν αναστάτωση στα συστήματα υπολογιστών. Αν και αυτά τα προγράμματα ήταν συχνά απλά, έθεσαν τις βάσεις για την ανάπτυξη πιο εξελιγμένων απειλών. Ένας αποδεκτός ορισμός του ιού υπολογιστή δημιουργήθηκε από τον Fred Cohen ως «ένα πρόγραμμα που μπορεί να μολύνει άλλα προγράμματα τροποποιώντας τα ώστε να περιλαμβάνουν ένα πιθανώς εξελιγμένο αντίγραφο του εαυτού του» [32]. Οι ιοί μπορούν να εξαπλωθούν σε ένα σύστημα υπολογιστή ή ένα δίκτυο. Η διαφορά μεταξύ ιών και σκουληκιών (worms) είναι ότι ένας ιός συνήθως απαιτεί ανθρώπινη παρέμβαση, όπως το άνοιγμα ενός μολυσμένου αρχείου για να ξεκινήσει η αναπαραγωγή του, ενώ τα σκουλήκια μπορούν να αναπαραχθούν χωρίς παρέμβαση . Οι ιοί και τα σκουλήκια σε αυτή τη φάση διαδίδονταν μέσω μολυσμένων μονάδων δισκέτας ή του ARPANET.

Ο Creeper θεωρείται ο πρώτος ιός υπολογιστών στην ιστορία. Δημιουργήθηκε από τον Bob Thomas στη BBN Technologies για πειραματικούς σκοπούς [33]. Ο Creeper σχεδιάστηκε για να εκτελείται στο ARPANET και να μεταφέρεται από τον έναν υπολογιστή σε άλλον. Δεν είχε κακόβουλη πρόθεση, αλλά απλώς εμφάνιζε το μήνυμα: *"I'm the creeper, catch me if you can!"*. Παρόλα αυτά, έδειξε πώς ένα πρόγραμμα μπορεί να εξαπλώνεται από σύστημα σε σύστημα [10].

Ο Elk Cloner εμφανίστηκε το 1982 και ήταν ο πρώτος πραγματικός ιός που προκάλεσε διαταραχή σε προσωπικούς υπολογιστές. Δημιουργήθηκε από έναν 15χρονο προγραμματιστή, τον Rich Skrenta, για συστήματα Apple II. Ο ιός εξαπλωνόταν μέσω δισκετών και ενεργοποιούνταν μετά την 50ή χρήση μιας μολυσμένης δισκέτας [34]. Τότε, εμφάνιζε ένα ποίημα στην οθόνη, χωρίς να προκαλεί ζημία στα δεδομένα. Ο Elk Cloner έδειξε πώς οι ιοί μπορούν να εκμεταλλευτούν τα φυσικά μέσα αποθήκευσης για την εξάπλωσή τους.

Το σκουλήκι Morris (Morris Worm) δημιουργήθηκε από τον Robert Tappan Morris το 1988 και ήταν το πρώτο που εξαπλώθηκε ευρέως μέσω του δικτύου ARPANET. Ο Morris σχεδίασε το σκουλήκι ως πείραμα για να μετρήσει το μέγεθος του δικτύου, αλλά ένα σφάλμα στον κώδικά του οδήγησε σε ανεξέλεγκτη εξάπλωση. Το σκουλήκι επηρέασε περίπου 6.000 υπολογιστές, προκαλώντας σημαντικές

διακοπές στη λειτουργία τους. Αυτό το περιστατικό τόνισε την ανάγκη για βελτιωμένα μέτρα ασφάλειας στα δίκτυα [35].

3.5 Η Ανάπτυξη των Δούρειων Ίππων και του Spyware (1990s)

Η δεκαετία του 1990 σηματοδότησε τη μετάβαση από τους απλούς ιούς και τα σκουλήκια στις πιο σύνθετες μορφές κακόβουλου λογισμικού, όπως οι Δούρειοι Ίπποι (Trojan Horses ή απλά Trojans) και το λογισμικό κατασκοπείας (Spyware). Αυτές οι μορφές malware επικεντρώθηκαν στη μυστική παραβίαση της ασφάλειας των συστημάτων και στην υποκλοπή ευαίσθητων δεδομένων, ανοίγοντας νέους δρόμους για την ανάπτυξη κυβερνοεγκλήματος.

Τα Trojans πήραν το όνομά τους από τον Δούρειο Ίππο της ελληνικής μυθολογίας, καθώς παρουσιάζονται ως ακίνδυνα ή χρήσιμα προγράμματα, αλλά κρύβουν κακόβουλη λειτουργικότητα. Κατά τη δεκαετία του 1990, τα Trojans εξελίχθηκαν σε αποτελεσματικά εργαλεία για την κρυφή πρόσβαση σε υπολογιστικά συστήματα.

Ένα χαρακτηριστικό παράδειγμα ήταν το AIDS Trojan (1989), που διανεμήθηκε μέσω φυσικών μέσων (δισκέτες) [36]. Το πρόγραμμα κρυπτογραφούσε αρχεία του χρήστη και ζητούσε λύτρα, ένα χαρακτηριστικό στοιχείο ενός άλλου είδους malware που ονομάζεται ransomware και θα αναλυθεί στη συνέχεια. Μέχρι τα μέσα της δεκαετίας του 1990, τα Trojans χρησιμοποιούνταν κυρίως για τη δημιουργία κρυφών σημείων μη εξουσιοδοτημένης πρόσβασης (κερκόπορτες ή backdoors), δίνοντας στους επιτιθέμενους απομακρυσμένη πρόσβαση σε συστήματα.

Το Spyware έκανε την εμφάνισή του στις αρχές της δεκαετίας του 1990, ως εργαλείο παρακολούθησης των χρηστών. Το λογισμικό αυτό σχεδιάστηκε αρχικά για να συλλέγει δεδομένα, όπως η δραστηριότητα πλοήγησης στο διαδίκτυο, συχνά χωρίς τη συγκατάθεση του χρήστη. Ένα από τα πρώτα παραδείγματα ήταν το Comet Cursor (1997), το οποίο παρακολουθούσε τις ενέργειες του χρήστη και μετέφερε δεδομένα σε διαφημιστικές εταιρείες [37].

Τα Trojan Horses και το Spyware της δεκαετίας του 1990 υπήρξαν πρόδρομοι πιο σύγχρονων και εξελιγμένων απειλών. Ενώ τα Trojans άνοιξαν τον δρόμο για απομακρυσμένες παραβιάσεις, το Spyware προετοίμασε το έδαφος για την εμπορική εκμετάλλευση των προσωπικών δεδομένων.

3.6 Η εποχή του διαδικτύου (1990-2000)

Η δεκαετία του 1990 και οι αρχές της δεκαετίας του 2000 χαρακτηρίστηκαν από την ταχεία εξάπλωση του διαδικτύου, η οποία έφερε νέες ευκαιρίες αλλά και αυξημένους κινδύνους. Η αυξανόμενη συνδεσιμότητα και οι ανεπαρκείς πρακτικές ασφάλειας εκείνης της εποχής δημιούργησαν το κατάλληλο περιβάλλον για την εξάπλωση κακόβουλων λογισμικών, δηλαδή κακόβουλου λογισμικού που μπορούσε να αναπαράγεται και να εξαπλώνεται ανεξάρτητα χωρίς την παρέμβαση του χρήστη.

Το Melissa Worm (1999) αποτέλεσε ένα από τα πρώτα παραδείγματα σκουληκιών που εκμεταλλεύτηκαν τη δημοτικότητα του ηλεκτρονικού ταχυδρομείου. Δημιουργήθηκε από τον David L. Smith και εξαπλωνόταν μέσω συνημμένων εγγράφων Microsoft Word. Μόλις ο χρήστης άνοιγε το έγγραφο, το worm έστελνε αντίγραφα του εαυτού του στις 50 πρώτες επαφές του βιβλίου διευθύνσεων του χρήστη, προκαλώντας τεράστια συμφόρηση στους διακομιστές ηλεκτρονικού ταχυδρομείου [38].

Το ILOVEYOU (2000), γνωστό και ως Love Letter Virus ή Love bug, ήταν ένα από τα πιο καταστροφικά worms της εποχής, προκαλώντας ζημιές ύψους περίπου 10 δισεκατομμυρίων δολαρίων. Το worm εξαπλώθηκε μέσω email με το μήνυμα "I love you" και μόλις ο παραλήπτης άνοιγε το συνημμένο, το worm διέγραφε αρχεία, υποκλέπτοντας παράλληλα κωδικούς πρόσβασης. Η επιτυχία του βασίστηκε στη χρήση κοινωνικής μηχανικής για την εξαπάτηση των χρηστών [39].

Η κοινωνική μηχανική (social engineering) αναφέρεται στην ψυχολογική χειραγώγηση ατόμων ώστε να αποκαλύψουν εμπιστευτικές πληροφορίες, να εκτελέσουν συγκεκριμένες ενέργειες ή να παραχωρήσουν μη εξουσιοδοτημένη πρόσβαση σε συστήματα ή δίκτυα. Σε αντίθεση με τις τεχνικές επιθέσεις που εκμεταλλεύονται τρωτά σημεία σε λογισμικό ή υλικό, η κοινωνική μηχανική εκμεταλλεύεται την ανθρώπινη εμπιστοσύνη, την περιέργεια ή τον φόβο για να παρακάμψει τους μηχανισμούς ασφαλείας, καθιστώντας την ένα από τα πιο αποτελεσματικά εργαλεία στο οπλοστάσιο ενός κακόβουλου χρήστη.

Ένα άλλο παράδειγμα σκουληκιού αυτής της περιόδου ήταν το Code Red Worm (2001). Το Code Red Worm εκμεταλλεύτηκε μια ευπάθεια στους διακομιστές Microsoft IIS (Internet Information Services) και εξαπλώθηκε ταχύτατα. Προκάλεσε ζημιές σε χιλιάδες διακομιστές παγκοσμίως και χρησιμοποιήθηκε για να δημιουργήσει επιθέσεις DDoS (Distributed Denial of Service). Οι επιθέσεις αυτές λειτουργούν προκαλώντας συμφόρηση μετά από την αποστολή μεγάλου αριθμού αιτήσεων σε κάποιον διακομιστή έτσι ώστε ο τελευταίος να μην μπορεί να ανταποκριθεί. Έτσι έδειξε πώς τα worms μπορούσαν να στοχεύσουν κεντρικές υποδομές του διαδικτύου [40].

Το Blaster Worm που αξαπλώθηκε το 2003 ήταν μια άλλη σημαντική απειλή που εκμεταλλεύτηκε ευπάθειες στα Windows. Δημιουργήθηκε για να προκαλέσει διακοπή λειτουργίας στα συστήματα και να εκτελέσει επίθεση DDoS στους διακομιστές της Microsoft. Το worm επηρέασε εκατομμύρια συστήματα, ενισχύοντας την ανάγκη για τακτική ενημέρωση και εφαρμογή κώδικα ασφαλείας [41].

Η εποχή των worms έφερε στο φως τις σοβαρές αδυναμίες της διαδικτυακής ασφάλειας. Τα worms εκμεταλλεύονταν την έλλειψη κεντρικής διαχείρισης ασφάλειας, την απουσία τακτικών ενημερώσεων λογισμικού και την έλλειψη εκπαίδευσης των χρηστών. Καθώς τα worms μπορούσαν να εξαπλωθούν γρήγορα και να προκαλέσουν εκτεταμένες ζημιές, έγινε σαφές ότι τα δίκτυα και τα λειτουργικά συστήματα χρειαζόταν ισχυρότερη προστασία.

3.7 Εξέλιξη των Ransomware και Botnets (2000s-2010s)

Κατά τις δεκαετίες του 2000 και του 2010, τα ransomware και τα botnets αναδείχθηκαν ως δύο από τις πιο σημαντικές και σύνθετες απειλές στο χώρο της ασφάλειας δικτύων υπολογιστών. Η λειτουργία τους βασίζεται σε εξελιγμένες τεχνολογίες, όπως η κρυπτογράφηση, η οποία υποστηρίζεται από συμμετρικούς και ασύμμετρους αλγόριθμους.

Η κρυπτογράφηση είναι η διαδικασία μετατροπής δεδομένων σε μορφή που δεν μπορεί να διαβαστεί χωρίς τη χρήση ενός ειδικού κλειδιού αποκρυπτογράφησης. Στόχος της είναι η προστασία των δεδομένων από μη εξουσιοδοτημένη πρόσβαση. Οι αλγόριθμοι κρυπτογράφησης χωρίζονται σε δύο βασικές κατηγορίες:

1. **Συμμετρικοί αλγόριθμοι**: Οι αλγόριθμοι αυτοί χρησιμοποιούν το ίδιο κλειδί για την κρυπτογράφηση και την αποκρυπτογράφηση των δεδομένων. Ένα παράδειγμα ενός δημοφιλούς τέτοιου αλγορίθμου γνωστού για την ταχύτητα και την ασφάλειά του είναι ο AES (Advanced Encryption Standard).
2. **Ασύμμετροι αλγόριθμοι**: Οι αλγόριθμοι αυτοί χρησιμοποιούν δύο διαφορετικά κλειδιά: το δημόσιο κλειδί και το ιδιωτικό κλειδί. Ένα παράδειγμα ενός τέτοιου αλγόριθμου είναι ο RSA (Rivest–Shamir–Adleman) που βασίζεται στην μαθηματική δυσκολία της παραγοντοποίησης μεγάλων αριθμών.

Τα ransomware είναι κακόβουλα προγράμματα που κρυπτογραφούν τα αρχεία ενός υπολογιστή ή μπλοκάρουν την πρόσβαση σε αυτόν, απαιτώντας λύτρα για την αποκατάσταση της πρόσβασης [42]. Η επίθεση ransomware περιλαμβάνει τα εξής στάδια:

1. **Μόλυνση**: Η μόλυνση γίνεται συνήθως μέσω email phishing ή εκμετάλλευσης ευπαθειών στο λειτουργικό σύστημα. Η πρώτη μέθοδος συνίσταται στην αποστολή κακόβουλων ηλεκτρονικού ταχυδρομείου με συνημμένα αρχεία ή συνδέσμους που περιέχουν το ransomware, τα οποία ο

χρήστης ανοίγει, ενεργοποιώντας τη μόλυνση ενώ η δεύτερη συνίσταται στην εκμετάλλευση αδυναμιών ή κενών ασφαλείας στο λειτουργικό σύστημα ή σε λογισμικό, τα οποία επιτρέπουν την εγκατάσταση του ransomware χωρίς την παρέμβαση του χρήστη.

2. **Κρυπτογράφηση δεδομένων:** Με τη χρήση ισχυρών αλγορίθμων, όπως ο AES (για την κρυπτογράφηση αρχείων) και ο RSA (για την ασφαλή αποθήκευση των κλειδιών), τα αρχεία του θύματος της επίθεσης κρυπτογραφούνται δηλαδή μετατρέπονται σε ακατάληπτη μορφή.
3. **Απαίτηση λύτρων**: Στο στάδιο αυτό το θύμα βλέπει ένα μήνυμα που εξηγεί ότι τα δεδομένα του είναι κρυπτογραφημένα και απαιτείται πληρωμή λύτρων, συνήθως σε κρυπτονομίσματα, όπως το Bitcoin, για επίτευξη ανωνυμίας.

Τα botnets που επίσης αποτελούν εξέλιξη αυτής της περιόδου είναι ομάδες συνδεδεμένων συσκευών που έχουν μολυνθεί από malware και ελέγχονται από έναν επιτιθέμενο, γνωστό ως botmaster. Οι μολυσμένοι υπολογιστές, συχνά χωρίς τη γνώση των κατόχων τους, λειτουργούν ως "ζόμπι" και χρησιμοποιούνται για κακόβουλες δραστηριότητες, όπως επιθέσεις DDoS (Distributed Denial of Service) για πρόκληση υπερφόρτωσης ενός διακομιστή μέσω μαζικών αιτημάτων, μαζική αποστολή ανεπιθύμητων μηνυμάτων (spam campaigns) και υποκλοπή δεδομένων όπως προσωπικών πληροφοριών ή τραπεζικών κωδικών [43].

Οι επικοινωνίες μεταξύ των μολυσμένων συσκευών και του botmaster γίνονται μέσω διακομιστών ελέγχου [Command and Control (C&C) servers], οι οποίοι επιτρέπουν στον επιτιθέμενο να δίνει οδηγίες στα botnets. Πιο πρόσφατα, τα botnets έχουν εξελιχθεί για να χρησιμοποιούν τεχνολογίες peer-to-peer (P2P), μεταβαίνοντας από την παραδοσιακή αρχιτεκτονική C&C σε πιο αποκεντρωμένες δομές [44]. Σε ένα παραδοσιακό botnet, τα μολυσμένα συστήματα (bots) επικοινωνούν με έναν κεντρικό διακομιστή C&C για να λάβουν εντολές και να στείλουν δεδομένα. Αυτή η κεντρική δομή τα καθιστά πιο ευάλωτα, καθώς αν εντοπιστεί ή καταργηθεί ο διακομιστής C&C, το botnet παύει να λειτουργεί. Με τη χρήση τεχνολογιών P2P, το δίκτυο των botnet αποκτά μια αποκεντρωμένη αρχιτεκτονική όπου τα μολυσμένα συστήματα επικοινωνούν μεταξύ τους απευθείας, χωρίς την ανάγκη κεντρικού διακομιστή. Αυτό επιτυγχάνεται με τη δημιουργία ενός δικτύου όπου κάθε bot λειτουργεί τόσο ως κόμβος που λαμβάνει όσο και ως κόμβος που μεταδίδει εντολές και δεδομένα.

Τα πλεονεκτήματα για τα κακόβουλα μέρη αυτής της προσέγγισης περιλαμβάνουν:

1. **Αυξημένη ανθεκτικότητα:** Επειδή δεν υπάρχει ένας μόνο κεντρικός διακομιστής που μπορεί να καταργηθεί, το botnet είναι πιο δύσκολο να διαλυθεί.
2. **Δυσκολία εντοπισμού:** Οι επικοινωνίες διασκορπίζονται σε πολλούς κόμβους, καθιστώντας δυσκολότερη την παρακολούθηση και την ανάλυση της κίνησης από ομάδες ασφάλειας.
3. **Ευκολία αναδιάταξης:** Αν κάποιο μέρος του δικτύου εντοπιστεί και αποσυνδεθεί, τα υπόλοιπα bots συνεχίζουν να λειτουργούν και να επικοινωνούν μεταξύ τους.

Αυτή η χρήση της τεχνολογίας P2P επιτρέπει στα botnets να είναι πιο ανθεκτικά και να προσαρμόζονται στις προσπάθειες εντοπισμού και καταστολής τους από ειδικούς κυβερνοασφάλειας. Παραδείγματα τέτοιων botnets περιλαμβάνουν το Storm και το ZeroAccess, τα οποία έχουν δείξει την αποτελεσματικότητα της αποκεντρωμένης αρχιτεκτονικής σε μεγάλης κλίμακας κακόβουλες δραστηριότητες.

3.8 Επίλογος

Στην παρούσα ενότητα αναλύθηκαν οι σημαντικότερες απειλές για τα δίκτυα υπολογιστών από τη δεκαετία του 1970 μέχρι τη δεκαετία του 2010. Η περίοδος αυτή, που συμπίπτει με την περίοδο της γέννησης και ανάπτυξης του διαδικτύου, ανέδειξε την εξέλιξη του κακόβουλου λογισμικού από απλές πειραματικές εφαρμογές -όπως οι πρώτοι ιοί και σκουλήκια-, σε λογισμικά σύνθετων και στοχευμένων επιθέσεων, όπως τα ransomware και τα botnets.

Οι διαφορετικές μορφές malware αντανακλούν τόσο την τεχνολογική πρόοδο όσο και την αυξανόμενη εξάρτηση της κοινωνίας από τα ψηφιακά δίκτυα, αποκαλύπτοντας παράλληλα τις αδυναμίες της

δικτυακής ασφάλειας σε κάθε εποχή. Η ανάλυση αυτή καθιστά σαφές ότι η εξέλιξη των απειλών συνδέεται άμεσα με τις δυνατότητες και τις ευπάθειες των υπολογιστικών συστημάτων και ότι τα κακόβουλα μέρη αξιοποιούν διαρκώς νέες τεχνικές για την επίτευξη των στόχων τους.

Η κατανόηση της ιστορικής πορείας του malware είναι ζωτικής σημασίας για την ανάπτυξη αποτελεσματικών στρατηγικών ασφάλειας και την αντιμετώπιση των σύγχρονων και μελλοντικών προκλήσεων. Καθώς τα δίκτυα συνεχίζουν να εξελίσσονται, η ανάγκη για συνεχή παρακολούθηση, πρόληψη και καινοτομία στον τομέα της δικτυακής ασφάλειας γίνεται πιο επιτακτική από ποτέ.

Κεφάλαιο 4 Μηχανισμοί ασφαλείας για την αντιμετώπιση απειλών

4.1 Εισαγωγή

Στην παρόν κεφάλαιο θα παρουσιαστούν η αρχιτεκτονική, η λειτουργία και η ιστορική εξέλιξη των firewalls και των antivirus, καθώς και η συμβολή τους στην προστασία των συστημάτων από κακόβουλες απειλές. Θα αναλυθούν οι προκλήσεις που αντιμετώπισαν και οι περιορισμοί τους, αναδεικνύοντας τη σημασία τους για την ασφάλεια των σύγχρονων δικτύων.

4.2 Firewalls: Ο πρώτος φραγμός προστασίας

Το firewall είναι ένας από τους πρώτους και σημαντικότερους μηχανισμούς ασφαλείας που αναπτύχθηκαν για την προστασία δικτύων υπολογιστών. Ορίζεται ως λογισμικό ή υλικό που ελέγχει την εισερχόμενη και εξερχόμενη κίνηση δικτύου, εφαρμόζοντας προκαθορισμένους κανόνες για να επιτρέπει ή να απορρίπτει πακέτα δεδομένων. Σκοπός του είναι η αποτροπή μη εξουσιοδοτημένης πρόσβασης και το φιλτράρισμα επικίνδυνης κίνησης, προστατεύοντας έτσι τα συστήματα από επιθέσεις [45].

Τα firewalls λειτουργούν ως "φραγμοί" μεταξύ ενός εσωτερικού δικτύου και του εξωτερικού κόσμου (συνήθως του διαδικτύου), αποτρέποντας δυνητικά επικίνδυνη δραστηριότητα. Είναι κρίσιμα για τη διασφάλιση της εμπιστευτικότητας και της ακεραιότητας των δεδομένων, καθώς και για την αποτροπή παραβίασης των συστημάτων από κακόβουλους χρήστες ή λογισμικό. Τα firewalls λειτουργούν με διαφορετικούς τρόπους, ανάλογα με την τεχνολογία και την προσέγγιση που υιοθετούν.

Τα **Packet Filtering Firewall** λειτουργούν στο επίπεδο του δικτύου και ελέγχουν μεμονωμένα πακέτα δεδομένων με βάση προκαθορισμένα κριτήρια, όπως IP διεύθυνση, πρωτόκολλο και Θύρα επικοινωνίας. Αν ένα πακέτο δεν πληροί τα κριτήρια, απορρίπτεται. Παρά το γεγονός ότι τα packet filtering firewalls είναι γρήγορα και αποτελεσματικά, δεν λαμβάνουν υπόψη το συνολικό πλαίσιο της επικοινωνίας, γεγονός που μπορεί να τα καταστήσει ευάλωτα [5].

Τα **Stateful Inspection Firewalls** εισήχθησαν τη δεκαετία του 1990 και παρέχουν βελτιωμένη ασφάλεια, καθώς παρακολουθούν τη συνολική ροή δεδομένων μεταξύ αποστολέα και παραλήπτη. Καταγράφουν την κατάσταση των συνδέσεων (state), εξασφαλίζοντας ότι τα πακέτα είναι μέρος έγκυρων συνδέσεων και όχι ανεξάρτητες, κακόβουλες προσπάθειες επικοινωνίας [46].

Τα **Application Layer Firewalls** λειτουργούν στο επίπεδο εφαρμογών και μπορούν να αναλύσουν την κίνηση συγκεκριμένων πρωτοκόλλων, όπως το HTTP. Είναι σε θέση να εντοπίσουν και να μπλοκάρουν κακόβουλες δραστηριότητες που σχετίζονται με συγκεκριμένες εφαρμογές, γεγονός που τα καθιστά ιδιαίτερα αποτελεσματικά κατά των επιθέσεων σε επίπεδο εφαρμογών [47].

Η εξέλιξη των firewalls αντανακλά τις μεταβαλλόμενες ανάγκες της ασφάλειας δικτύων. Τα πρώτα firewalls εμφανίστηκαν στα τέλη της δεκαετίας του 1980, βασιζόμενα στην αρχιτεκτονική packet filtering. Αυτά τα firewalls ήταν απλά στη σχεδίασή τους αλλά προσέφεραν τη βασική προστασία για την εποχή, φιλτράροντας πακέτα δεδομένων με βάση προκαθορισμένα κριτήρια. Με την αυξανόμενη συνδεσιμότητα του διαδικτύου τη δεκαετία του 1990, οι απειλές έγιναν πιο εξελιγμένες, οδηγώντας στην ανάγκη για stateful inspection firewalls. Αυτή η τεχνολογία προσέφερε μεγαλύτερη ασφάλεια από τα παραδοσιακά packet filtering firewalls.

Τα firewalls παίζουν κρίσιμο ρόλο στην αντιμετώπιση διαφόρων τύπων κακόβουλου λογισμικού. Μπορούν να φιλτράρουν την εισερχόμενη κίνηση δικτύου, εμποδίζοντας τη διάδοση κακόβουλων προγραμμάτων, όπως τα worms και τα bots, μέσω δικτυακών θυρών ή γνωστών ευπαθειών.

Παράλληλα, με την εφαρμογή κανόνων πολιτικής δικτύου, περιορίζουν την επαφή με κακόβουλα προγραμμάτα, όπως τα trojans και τα spyware. Επιπλέον, λειτουργούν αποτρεπτικά απέναντι σε επιθέσεις DDoS, μπλοκάροντας μαζικά αιτήματα από ύποπτες πηγές και αποτρέποντας την υπερφόρτωση του δικτύου.
Τα firewalls αποτέλεσαν τη βάση για τη σύγχρονη κυβερνοασφάλεια, προσφέροντας αποτελεσματική προστασία απέναντι στις πρώτες και πιο επικίνδυνες μορφές κακόβουλου λογισμικού. Η εξέλιξή τους συνεχίζει να προσαρμόζεται στις ανάγκες των δικτύων και των χρηστών, καθιστώντας τα ένα από τα πιο ισχυρά εργαλεία προστασίας.

4.3 Antivirus: Το πρώτο εργαλείο για κακόβουλο λογισμικό

Το αντιιικά λογισμικά (antivirus) αποτελούν ένα από τα πρώτα και πιο βασικά εργαλεία ασφαλείας που αναπτύχθηκαν για την προστασία των συστημάτων υπολογιστών από κακόβουλο λογισμικό. Ως αντιιικό ορίζεται το λογισμικό που εντοπίζει, αποτρέπει και αφαιρεί κακόβουλα προγράμματα, όπως ιούς, worms, trojans, spyware και ransomware. Ο κύριος σκοπός του είναι η διατήρηση της ασφάλειας και της ακεραιότητας του συστήματος, εξαλείφοντας απειλές που μπορούν να προκαλέσουν ζημιά στα δεδομένα ή τη λειτουργία του υπολογιστή [48].
Η λειτουργία του αντιιικού λογισμικού βασίζεται στην ανάλυση των δεδομένων που βρίσκονται στο σύστημα ή εισέρχονται σε αυτό από εξωτερικές πηγές, εντοπίζοντας ενδείξεις που σχετίζονται με γνωστές ή άγνωστες απειλές. Τα προγράμματα antivirus αποτελούν τη γραμμή άμυνας κατά των κακόβουλων λογισμικών, ενισχύοντας την προστασία του συστήματος απέναντι σε επιθέσεις.
Τα αντιιικά λογισμικά λειτουργούν χρησιμοποιώντας διαφορετικές μεθόδους για την αναγνώριση και την αντιμετώπιση κακόβουλου λογισμικού. Οι βασικότερες από αυτές αναλύονται παρακάτω.
Η ανίχνευση βάσει χαρακτηριστικών γνωρισμάτων (**Signature-based Detection**) είναι η παλαιότερη και πιο διαδεδομένη μέθοδος. Κάθε κακόβουλο λογισμικό έχει μια μοναδική "ψηφιακή υπογραφή," που δημιουργείται από το λογισμικό antivirus. Όταν το λογισμικό ανιχνεύσει ένα αρχείο ή μια διαδικασία που ταιριάζει με μια γνωστή υπογραφή, σηματοδοτεί το στοιχείο ως κακόβουλο. Παρόλο που αυτή η μέθοδος είναι αποτελεσματική για ήδη γνωστές απειλές, δεν μπορεί να εντοπίσει νέα ή τροποποιημένα malware [49].
Η ευρετική ανάλυση (**Heuristic Analysis**) χρησιμοποιείται για τον εντοπισμό άγνωστου malware, βασιζόμενη σε ανάλυση του κώδικα και της συμπεριφοράς του. Το αντιιικό λογισμικό δημιουργεί ένα προσομοιωμένο περιβάλλον εκτέλεσης όπου αναλύει τη λειτουργία ενός προγράμματος. Αν το πρόγραμμα εμφανίσει ύποπτη συμπεριφορά, όπως προσπάθεια διαγραφής αρχείων συστήματος, χαρακτηρίζεται ως πιθανή απειλή.
Η ανάλυση συμπεριφοράς (**Behavioral Analysis**) αποτελεί την πιο πρόσφατη εξέλιξη και εστιάζει στην παρακολούθηση της πραγματικής συμπεριφοράς των εφαρμογών. Αν μια εφαρμογή προσπαθεί να αποκτήσει μη εξουσιοδοτημένη πρόσβαση σε δεδομένα ή να επικοινωνήσει με ύποπτες διευθύνσεις, το λογισμικό τη μπλοκάρει. Αυτή η μέθοδος είναι αποτελεσματική απέναντι σε απειλές όπως τα spyware και τα ransomware.
Το πρώτο γνωστό εργαλείο που θεωρείται πρόδρομος των αντιιικών λογισμικών ήταν το Reaper, που δημιουργήθηκε τη δεκαετία του 1970 για να αντιμετωπίσει το Creeper Virus. Στη δεκαετία του 1980, τα πρώτα εμπορικά antivirus, όπως το McAfee VirusScan και το Norton Antivirus, εμφανίστηκαν στην αγορά, παρέχοντας προστασία από τους πρώτους ιούς, που εξαπλώνονταν μέσω δισκετών. Η δεκαετία του 1990 έφερε σημαντικές καινοτομίες με την εισαγωγή της ευρετικής ανάλυσης. Τα antivirus της εποχής μπορούσαν να εντοπίσουν όχι μόνο γνωστούς ιούς αλλά και τροποποιημένα ή νέα κακόβουλα προγράμματα, βελτιώνοντας σημαντικά την αποτελεσματικότητά τους. Στις αρχές της δεκαετίας του

2000, οι συμπεριφορικές μέθοδοι έγιναν απαραίτητες για την καταπολέμηση του spyware και άλλων πιο σύνθετων απειλών.

4.4 Το πρωτόκολλο HTTPS ως μηχανισμός ασφαλείας δικτυών

Το Διαδίκτυο μας επιτρέπει να συνδεόμαστε σε ιστότοπους, να μοιραζόμαστε πληροφορίες και να πραγματοποιούμε συναλλαγές χρησιμοποιώντας το πρωτόκολλο μεταφοράς υπερκειμένου (Hypertext Tranfer Protocol ή HTTP). Το HTTP επιτρέπει στα προγράμματα περιήγησης να επικοινωνούν με διακομιστές, δηλαδή με υπολογιστές συνδεδεμένους στο διαδίκτυο οι οποίοι φιλοξενούν τους πόρους ενός ιστότοπου, για την ανάκτηση και αποστολή πληροφοριών, όπως η φόρτωση μιας ιστοσελίδας ή η υποβολή μιας φόρμας σύνδεσης. Ωστόσο, το HTTP μεταδίδει δεδομένα ως απλό κείμενο, που σημαίνει ότι όποιος παρεμβληθεί στην επικοινωνία μπορεί να τα διαβάσει. Αυτή η ευπάθεια εγκυμονεί σημαντικούς κινδύνους για την ασφάλεια, όπως:

- **Υποκλοπή:** Κακόβουλα μέρη μπορούν να παρακολουθούν τα δεδομένα που μεταδίδονται, όπως κωδικούς πρόσβασης ή προσωπικές πληροφορίες.
- **Παραχάραξη δεδομένων:** Κακόβουλα μέρη μπορούν να αλλάξουν τα δεδομένα που αποστέλλονται μεταξύ του χρήστη και του διακομιστή.
- **Απομίμηση:** Χωρίς τρόπο επαλήθευσης της ταυτότητας του διακομιστή, οι χρήστες ενδέχεται να συνδεθούν εν αγνοία τους σε έναν ψεύτικο ή κακόβουλο ιστότοπο.

Για την αντιμετώπιση αυτών των προβλημάτων, το 1994 προτάθηκε μια πιο ασφαλής έκδοση του HTTP, που ονομάζεται Ασφαλές Πρωτόκολλο Μεταφοράς Υπερκειμένου (Hypertext Transfer Protocol Secure ή HTTPS). Το HTTPS κρυπτογραφεί δεδομένα και παρέχει έναν τρόπο διασφάλισης της αυθεντικότητας των ιστότοπων. Το HTTPS είναι ουσιαστικά το HTTP με ένα πρόσθετο επίπεδο ασφάλειας. Χρησιμοποιεί εργαλεία όπως κρυπτογράφηση και τα ψηφιακά πιστοποιητικά για την προστασία της επικοινωνίας μεταξύ του προγράμματος περιήγησής σας και του διακομιστή στον οποίο συνδέεται κάποιος χρήστης του διαδικτύου. Αυτό διασφαλίζει ότι ακόμα κι αν κάποιος υποκλέψει τα δεδομένα, δεν μπορεί να τα διαβάσει.

Το πρώτο επίπεδο που χρησιμοποιεί το πρωτόκολλο είναι η κρυπτογράφηση. Το HTTPS κρυπτογραφεί τις πληροφορίες που αποστέλλονται μεταξύ του προγράμματος περιήγησής και του διακομιστή που φιλοξενεί τον ιστότοπο χρησιμοποιώντας το πρωτόκολλο TLS (Transport Layer Security).

Το δεύτερο επίπεδο ασφάλειας παρέχεται με τον έλεγχος ταυτότητας του ιστότοπου. Το HTTPS χρησιμοποιεί Ψηφιακά Πιστοποιητικά, τα οποία λειτουργούν σαν ηλεκτρονικές ταυτότητες των ιστοτόπων. Αυτά τα πιστοποιητικά εκδίδονται από αξιόπιστους οργανισμούς (Certificate Authorities ή CA). Κατά την επίσκεψη σε έναν ιστότοπο, το πρόγραμμα περιήγησής ελέγχει το ψηφιακό πιστοποιητικό για να διασφαλίσει ότι είναι έγκυρο και ότι ο ιστότοπος είναι νόμιμος. Αυτό μπορεί να αποτρέψει μια επίθεση τύπου Man-in-the-Middle (MITM attack). Σε μια επίθεση MITM, κάποιο κακόβουλο μέρος παρεμβαίνει στην επικοινωνία ανάμεσα σε δύο μέρη, προσποιούμενο ότι είναι ένα από αυτά, ώστε να υποκλέψει πληροφορίες, πριν τις μεταβιβάσει στον νόμιμο παραλήπτη.

Το τρίτο επίπεδο ασφάλειας που εξασφαλίζει το HTTPS αφορά την ακεραιότητα των δεδομένων, καθώς διασφαλίζει ότι τα δεδομένα που αποστέλλονται μεταξύ του προγράμματος περιήγησής και του διακομιστή δεν έχουν αλλάξει κατά τη μετάδοση. Εάν εντοπιστούν αλλαγές, η σύνδεση επισημαίνεται ως μη ασφαλής.

Παρά τις σημαντικές βελτιώσεις ασφαλείας που παρέχει το HTTPS, δεν είναι χωρίς μειονεκτήματα. Ένα ζήτημα είναι οι αυξημένοι υπολογιστικοί πόροι που σχετίζονται με την κρυπτογράφηση και την αποκρυπτογράφηση δεδομένων. Αυτές οι διαδικασίες ενδέχεται να επιβραδύνουν παλαιότερες συσκευές ή διακομιστές που δεν έχουν την ικανότητα να χειριστούν αποτελεσματικά τον επιπλέον φόρτο εργασίας. Μια άλλη πρόκληση προκύπτει από λανθασμένες παραμέτρους υλοποιήσεων HTTPS.

Για παράδειγμα, ιστότοποι που χρησιμοποιούν ληγμένα ψηφιακά πιστοποιητικά, αδύναμους αλγόριθμους κρυπτογράφησης ή ακατάλληλα διαμορφωμένα πρωτόκολλα ασφαλείας παραμένουν ευάλωτοι σε επιθέσεις. Τέτοιες εσφαλμένες διαμορφώσεις υπονομεύουν την αποτελεσματικότητα του HTTPS, αφήνοντας τους χρήστες εκτεθειμένους σε κινδύνους παρά τις εγγενείς δυνατότητες ασφαλείας του πρωτοκόλλου.

4.5 Επίλογος

Η ανάπτυξη και εξέλιξη των μηχανισμών ασφαλείας, όπως τα firewalls, τα antivirus και το πρωτόκολλο HTTPS, αποτελεί θεμελιώδη παράγοντα για την προστασία των δικτύων και των συστημάτων από κακόβουλες επιθέσεις. Η ιστορική αναδρομή των μηχανισμών ασφαλείας αποδεικνύει ότι η προστασία των συστημάτων δεν είναι στατική διαδικασία, αλλά απαιτεί συνεχή εξέλιξη και προσαρμογή στις νέες μορφές απειλών. Ο συνδυασμός προηγμένων λύσεων ασφαλείας, στρατηγικών πρόληψης και εκπαίδευσης των χρηστών είναι απαραίτητος για την αποτελεσματική άμυνα απέναντι στις σύγχρονες κυβερνοαπειλές.

Κεφάλαιο 5 Σημαντικά ιστορικά περιστατικά ασφαλείας και η επίδρασή τους

5.1 Εισαγωγή

Η ασφάλεια των δικτύων αποτελεί έναν από τους πιο κρίσιμους τομείς της σύγχρονης τεχνολογίας, καθώς οι συνεχώς εξελισσόμενες απειλές δημιουργούν προκλήσεις για την προστασία δεδομένων και συστημάτων. Τα περιστατικά ασφαλείας διαδραματίζουν καθοριστικό ρόλο στην κατανόηση των δικτυακών απειλών, καθώς αποκαλύπτουν τις ευπάθειες των δικτύων, τις μεθόδους επίθεσης και τις πιθανές επιπτώσεις αυτών. Μέσα από την ανάλυση αυτών των περιστατικών, προκύπτουν πολύτιμα μαθήματα που ενισχύουν την ανάπτυξη νέων τεχνολογιών και πρωτοκόλλων ασφαλείας, όπως τα firewalls, τα συστήματα ανίχνευσης εισβολών και τις μεθόδους κρυπτογράφησης.
Κατά τις τελευταίες δεκαετίες του 20ού αιώνα και τις αρχές του 21ου, τα περιστατικά ασφαλείας ανέδειξαν τη σημασία της ετοιμότητας και της προληπτικής διαχείρισης των κινδύνων. Από τους πρώτους ιούς μέχρι τις επιθέσεις σε κρατικές υποδομές, κάθε περιστατικό συνέβαλε στην εξέλιξη της δικτυακής ασφάλειας, ενισχύοντας τη συνεργασία μεταξύ κυβερνήσεων, οργανισμών και ερευνητών.
Στόχος αυτού του κεφαλαίου είναι να παρουσιάσει και να αναλύσει τα σημαντικότερα περιστατικά ασφαλείας μέχρι το 2010, εξετάζοντας την ιστορική τους σημασία, τις επιπτώσεις τους και την επιρροή τους στη διαμόρφωση της σύγχρονης στρατηγικής για την ασφάλεια δικτύων.

5.2 Περιστατικά ασφαλείας (1970s-1980s)

Η δεκαετία του 1970 και του 1980 σηματοδότησε την απαρχή της εμφάνισης περιστατικών ασφαλείας, τα οποία αν και περιορισμένα σε αριθμό, ανέδειξαν τις πρώτες ευπάθειες των δικτύων και των υπολογιστικών συστημάτων. Τα περιστατικά αυτά έθεσαν τις βάσεις για την κατανόηση των δικτυακών απειλών και την ανάπτυξη των πρώτων μηχανισμών αντιμετώπισης.
Ο ιός **Creeper Virus** θεωρείται η πρώτη καταγεγραμμένη "ψηφιακή απειλή" στην ιστορία των υπολογιστών. Ήταν ένα πειραματικό πρόγραμμα υπολογιστή που γράφτηκε από τον Bob Thomas στο ερευνητικό κέντρο της BBN Technologies το 1971[50]. Η αρχική του έκδοση σχεδιάστηκε για να μετακινείται μεταξύ των κεντρικών υπολογιστών DEC PDP-10 που εκτελούσαν το λειτουργικό σύστημα TENEX και χρησιμοποιούσαν το ARPANET, ενώ μια μεταγενέστερη έκδοση γράφτηκε από τον Ray Tomlinson ώστε να αντιγράφει τον εαυτό στον στόχο αντί απλώς να μετακινείται [51]. Αυτή η αυτο-αναπαραγόμενη έκδοση του Creeper είναι γενικά αποδεκτό ότι είναι το πρώτο worm υπολογιστή.[52][53] Το Creeper ήταν στην ουσία ένα δοκιμαστικό πρόγραμμα που δημιουργήθηκε για να αποδείξει τη ικανότητα ενός αυτοαναπαραγόμενου προγράμματος υπολογιστή να εξαπλωθεί σε άλλους υπολογιστές. Το πρόγραμμα δεν ήταν ενεργά κακόβουλο λογισμικό, καθώς δεν προκαλούσε ζημιά στα δεδομένα, αφού το μόνο του αποτέλεσμα ήταν η εκτύπωση στην οθόνη του μηνύματος " I'm the creeper: catch me if you can "[53]
Παρά την απουσία κακόβουλων προθέσεων, το Creeper ανέδειξε το πρόβλημα των μη εξουσιοδοτημένων κινήσεων κώδικα σε δίκτυα υπολογιστών. Για την αντιμετώπισή του δημιουργήθηκε το Reaper, το πρώτο πρόγραμμα "αντιμέτρων", το οποίο εντόπιζε και διέγραφε το Creeper. Αυτή η προσέγγιση αποτέλεσε τον πρόδρομο των σύγχρονων λογισμικών antivirus, επισημαίνοντας την ανάγκη για εργαλεία ανίχνευσης και αντιμετώπισης ψηφιακών απειλών [54].

1986: Το περιστατικό του χάκερ του Ανόβερου

Το λεγόμενο Hanover Hacker Incident αποτελεί μία από τις πρώτες μεγάλες περιπτώσεις κυβερνοκατασκοπείας και ανέδειξε την ευπάθεια στρατιωτικών και βιομηχανικών υπολογιστικών συστημάτων κατά τη διάρκεια του Ψυχρού Πολέμου. Ο Markus Hess, ένας Γερμανός χάκερ, σε συνεργασία με τους Dirk Brzezinski και Peter Carl, κατάφερε να εισβάλει σε πάνω από 400 στρατιωτικά συστήματα των Ηνωμένων Πολιτειών Αμερικής, της Ευρώπης και Ανατολικής Ασίας. Το υλικό που υποκλάπηκε περιελάμβανε ευαίσθητες πληροφορίες για δορυφόρους, αεροσκάφη και τεχνολογίες ημιαγωγών, οι οποίες πουλήθηκαν στη KGB έναντι 54.000 δολαρίων [55].
Οι δραστηριότητες του Hess ξεκίνησαν μέσω του γερμανικού δικτύου Datex-P, το οποίο του επέτρεψε να αποκτήσει πρόσβαση σε υπολογιστές στις ΗΠΑ μέσω της υπηρεσίας Tymnet International Gateway. Το Tymnet ήταν ένα δίκτυο μεταγωγής πακέτων που χρησιμοποιούνταν ευρέως λόγω του χαμηλότερου κόστους του σε σύγκριση με τις απευθείας τηλεφωνικές κλήσεις. Είχε το ρόλο υπηρεσίας "πύλης" στην οποία ένας χρήστης καλούσε για να δρομολογηθεί σε οποιοδήποτε από τα διάφορα συστήματα υπολογιστών που χρησιμοποιούσαν επίσης την υπηρεσία. Χρησιμοποιώντας το Tymnet, ο Hess απέκτησε πρόσβαση σε συστήματα του Jet Propulsion Laboratory στην Καλιφόρνια και, τελικά, στους υπολογιστές του Lawrence Berkeley Laboratory (LBL). Από εκεί, εκμεταλλεύτηκε τη σύνδεση στο ARPANET και στο στρατιωτικό του αντίστοιχο, το MILNET, για να διεισδύσει σε υπολογιστικά συστήματα που χρησιμοποιούνταν από το υπουργείο Άμυνας των Η.Π.Α. [56]. Η πλήρης διαχειριστική πρόσβαση(root access) στους υπολογιστές του LBL του παρείχε τη δυνατότητα να διαχειρίζεται και να υποκλέπτει στοιχεία από αυτά τα συστήματα ανενόχλητος.
Η δράση του Hess εντοπίστηκε από τον Stoll, έναν διαχειριστή συστημάτων στο LBL. Ο Stoll ανακάλυψε την παραβίαση κατά τη διερεύνηση μιας λογιστικής διαφοράς 75 σεντ σε ένα υπολογιστικό σύστημα στο LBL. Αντί να κλείσει την πρόσβαση, ο Stoll έπεισε τη διοίκηση του LBL να χρησιμοποιήσει εικονικά δεδομένα για ένα ψευδές στρατιωτικό έργο. Αυτή η στρατηγική, που ονομάστηκε ανεπίσημα Operation Showerhead, κράτησε τον Hess συνδεδεμένο αρκετό χρόνο ώστε να εντοπιστεί η προέλευση των κλήσεών του [55].
Με τη βοήθεια της Tymnet, της AT&T και του FBI, οι κλήσεις του Hess ανιχνεύτηκαν να έχουν προέλευση το Ανόβερο της Γερμανίας. Οι γερμανικές αρχές τελικά συνέλαβαν τον Hess, ο οποίος καταδικάστηκε το 1990 σε 20 μήνες με αναστολή για κατασκοπεία [57].
Το περιστατικό αυτό έφερε στο προσκήνιο τις πρώτες μεγάλες απειλές που σχετίζονταν με την ασφάλεια δικτύων. Ανέδειξε την ανάγκη για πιο προηγμένους μηχανισμούς ασφαλείας, όπως η ενίσχυση της ταυτοποίησης χρηστών και η παρακολούθηση δικτύων, ειδικά σε στρατιωτικά και κυβερνητικά συστήματα.

1988: Το σκουλήκι Morris

Το σκουλήκι Morris (Morris Worm) ήταν το πρώτο malware που εξαπλώθηκε σε μεγάλη κλίμακα εξαιτίας ευπαθειών σε δικτυακά λογισμικά όπως το Sendmail, δημιουργώντας χάος σε υπολογιστικά συστήματα. Δημιουργήθηκε από τον Robert Tappan Morris, έναν φοιτητή του MIT, ως ένα πείραμα που έδειχνε πώς ένα πρόγραμμα μπορούσε να αναπαραχθεί αυτόνομα [35]. Το Morris Worm εκμεταλλεύτηκε ευπάθειες στα συστήματα Unix, καθώς και αδύναμους κωδικούς πρόσβασης. Μέσα σε 24 ώρες, μολύνθηκαν περίπου 6.000 υπολογιστές, αντιπροσωπεύοντας το 10% του τότε Διαδικτύου.
Οι επιπτώσεις ήταν άμεσες, με σημαντικές διακοπές λειτουργίας και οικονομικές ζημιές. Το περιστατικό ανέδειξε την ανάγκη για πολιτικές κυβερνοασφάλειας και οδήγησε στη δημιουργία της πρώτης Ομάδας Αντιμετώπισης Ψηφιακών Εκτάκτων Καταστάσεων [Computer Emergency Response Team (CERT)] από το Υπουργείο Άμυνας των ΗΠΑ [39].

5.3 Περιστατικά των 1990

Κατά τη δεκαετία του 1990, η εξάπλωση του Διαδικτύου έφερε πρωτοφανείς προκλήσεις στην ασφάλεια των πληροφοριακών συστημάτων. Τα περιστατικά ασφαλείας αυτής της περιόδου ανέδειξαν τις αυξανόμενες δυνατότητες των κακόβουλων ενεργειών, τη σημασία των πολιτικών κυβερνοασφάλειας και την ανάγκη για συνεργασία μεταξύ κυβερνητικών και ιδιωτικών φορέων.

1994: Η επίθεση Phishing στο AOL

Το 1994, το phishing εισήχθη ως μια νέα μορφή κοινωνικής μηχανικής, με στόχο χρήστες του παρόχου διαδικτυακών υπηρεσιών AOL (America Online). Οι επιτιθέμενοι έστελναν μηνύματα που προσομοίαζαν την επίσημη επικοινωνία του AOL, ζητώντας από τους χρήστες να εισάγουν τα διαπιστευτήριά τους σε ψεύτικες ιστοσελίδες [58]. Αυτή η επίθεση ήταν πρωτοφανής για την εποχή και έδειξε πώς οι χρήστες μπορούσαν να εξαπατηθούν μέσω του Διαδικτύου.
Οι επιθέσεις phishing εξαπλώθηκαν ραγδαία τα επόμενα χρόνια, επηρεάζοντας τόσο μεμονωμένους χρήστες όσο και οργανισμούς. Αυτό το περιστατικό κατέδειξε την ανάγκη για εκπαίδευση χρηστών και ανάπτυξη τεχνολογιών προστασίας, όπως τα φίλτρα ηλεκτρονικού ταχυδρομείου.

1998: Επίθεση Solar Sunrise

Η επίθεση Solar Sunrise, που εκδηλώθηκε το Φεβρουάριο του 1998, αποτέλεσε μία από τις πιο οργανωμένες και συστηματικές επιθέσεις στον κυβερνοχώρο έως τότε. Η ονομασία Solar Sunrise προήλθε από την εκμετάλλευση ενός ευρέως γνωστού κενού ασφαλείας στο λειτουργικό σύστημα Sun Solaris, που ήταν βασισμένο στο UNIX. Η επίθεση ξεκίνησε με τη συστηματική ανίχνευση δικτύων του Υπουργείου Άμυνας των ΗΠΑ (Department of Defence ή DoD) για ευπάθειες. Οι επιτιθέμενοι εκμεταλλεύτηκαν ένα γνωστό κενό ασφαλείας του Sun Solaris και εγκατέστησαν προγράμματα παρακολούθησης δεδομένων (sniffer programs) στους παραβιασμένους υπολογιστές. Μέσω αυτών, κατάφεραν να αποκτήσουν πρόσβαση σε ευαίσθητα δεδομένα, όπως κωδικούς πρόσβασης και άλλα εμπιστευτικά στοιχεία. Οι επιτιθέμενοι επανήλθαν αργότερα για να συλλέξουν τα δεδομένα, εκμεταλλευόμενοι τη σύνδεση των στρατιωτικών δικτύων με το MILNET, το στρατιωτικό αντίστοιχο του ARPANET. Το αποτέλεσμα ήταν η παραβίαση περισσότερων από 500 συστημάτων, συμπεριλαμβανομένων αυτών της NASA, της Αεροπορίας, του Πολεμικού Ναυτικού και του MIT. Οι δραστηριότητες αυτές έδωσαν πρόσβαση σε κρίσιμες στρατιωτικές πληροφορίες, προκαλώντας πανικό για πιθανή εμπλοκή ξένων κρατών, όπως το Ιράκ. Μόλις έγινε αντιληπτή η εισβολή, η αμερικανική κυβέρνηση κινητοποιήθηκε γρήγορα, ενεργοποιώντας το FBI, τη CIA, το Υπουργείο Δικαιοσύνης, την NSA και άλλους οργανισμούς. Παρά τη συστηματική φύση της επίθεσης, οι ερευνητές γρήγορα διαπίστωσαν ότι δεν εμπλέκονταν ξένοι κυβερνητικοί παράγοντες. Μέσα σε λίγες εβδομάδες, το FBI έκανε έφοδο στα σπίτια δύο μαθητών λυκείου στην Καλιφόρνια, οι οποίοι ομολόγησαν την ευθύνη για την επίθεση. Λίγο αργότερα, ένας 18χρονος Ισραηλινός χάκερ, ο Ehud Tenenbaum, γνωστός ως The Analyzer, συνελήφθη από τις ισραηλινές αρχές. Ο Tenenbaum παραδέχθηκε την εμπλοκή του, ισχυριζόμενος ότι στόχος του ήταν να αποδείξει πόσο ανασφαλή ήταν τα συστήματα [59].
Η επίθεση Solar Sunrise υπογράμμισε τις ευπάθειες ακόμη και των πιο κρίσιμων υποδομών. Απέδειξε επίσης πώς ακόμη και απλοί χρήστες, με περιορισμένους πόρους, μπορούσαν να θέσουν σε κίνδυνο κρατικά και στρατιωτικά συστήματα. Το περιστατικό έστειλε ένα ηχηρό μήνυμα για την ανάγκη συνεχούς ενημέρωσης των συστημάτων ασφαλείας και της συνεργασίας μεταξύ κυβερνητικών και ιδιωτικών φορέων για την αντιμετώπιση απειλών.

1999: Ο ιός Melissa

Ο ιός Melissa, που εμφανίστηκε το 1999, ήταν ένα από τα πρώτα malware που εκμεταλλεύτηκε τη μαζική αποστολή email για την εξάπλωση τους. Δημιουργήθηκε από τον David L. Smith και εξαπλώθηκε μέσω αρχείων Word που περιείχαν μακροεντολές δηλαδή κώδικα που μπορούσε να εκτελεστή εντός του συγκεκριμένου λογισμικού επεξεργασίας κειμένου. Ο ιός εκμεταλλεύτηκε τις λίστες επαφών των χρηστών στο λογισμικό ηλεκτρονικού ταχυδρομείου Microsoft Outlook, στέλνοντας μολυσμένα μηνύματα σε έως και 50 παραλήπτες [60].
Η ταχύτητα εξάπλωσης του ιού Melissa ήταν πρωτοφανής, προκαλώντας σοβαρές βλάβες σε εταιρείες και ιδιώτες. Οι οικονομικές ζημιές ξεπέρασαν τα 80 εκατομμύρια δολάρια, ενώ το περιστατικό οδήγησε στην ενίσχυση των αντιικών προγραμμάτων και στην ανάπτυξη πολιτικών για την αποτροπή της χρήσης μακροεντολών.
Συμπερασματικά η δεκαετία του 1990 σηματοδότησε μια κρίσιμη περίοδο για την ασφάλεια των δικτύων. Από τα πρώτα worm και τις επιθέσεις phishing μέχρι τις στρατιωτικές παραβιάσεις και τα μαζικά malware, τα περιστατικά αυτά οδήγησαν σε σημαντικές αλλαγές στον τομέα της ασφάλειας δικτύων. Η ανάπτυξη νέων τεχνολογιών και πολιτικών ήταν άμεση συνέπεια των εξελίξεων αυτής της περιόδου.

5.4 Το Μεταίχμιο του 21ου Αιώνα (2000-2010)

Η πρώτη δεκαετία του 21ου αιώνα χαρακτηρίστηκε από την αυξανόμενη πολυπλοκότητα και συχνότητα κυβερνοεπιθέσεων. Νέα worms και επιθέσεις σε υποδομές έφεραν στο προσκήνιο την ανάγκη για ενίσχυση των μέτρων κυβερνοασφάλειας. Τα περιστατικά της περιόδου αυτής ανέδειξαν την αδυναμία παραδοσιακών συστημάτων ασφαλείας να προστατεύσουν δίκτυα και χρήστες, καθώς και τη σημασία της συνεχούς εκπαίδευσης και επαγρύπνησης.

2000: Το ILOVEYOU Worm

Το ILOVEYOU Worm, που εμφανίστηκε το 2000, αποτέλεσε μία από τις πιο καταστροφικές επιθέσεις κοινωνικής μηχανικής. Ο ιός διαδόθηκε μέσω ηλεκτρονικού ταχυδρομείου, ως μήνυμα με τίτλο “ILOVEYOU” και περιείχε ένα συνημμένο αρχείο που περιείχε κακόβουλο κώδικα. Με το άνοιγμα του αρχείου, ο ιός εκτελούσε εντολές που αντικαθιστούσαν αρχεία του υπολογιστή και αποστέλλονταν αυτόματα σε όλες τις επαφές του χρήστη.
Οι οικονομικές ζημιές εκτιμώνται σε 10 δισεκατομμύρια δολάρια παγκοσμίως, καθώς επηρεάστηκαν επιχειρήσεις, κυβερνητικοί φορείς και ιδιώτες χρήστες. Το ILOVEYOU worm ανέδειξε τη σημασία της εκπαίδευσης χρηστών σε ζητήματα ασφάλειας και την ανάγκη για φίλτρα ηλεκτρονικού ταχυδρομείο που μπορούν να αναγνωρίζουν και να αποτρέπουν επιθέσεις κοινωνικής μηχανικής [61].

2001: Το Code Red Worm

Ο Code Red Worm εμφανίστηκε το 2001 και στόχευε διακομιστές IIS (Internet Information Services) της Microsoft. Χρησιμοποιούσε μια γνωστή ευπάθεια του λειτουργικού συστήματος Windows και εξαπλώθηκε γρήγορα, μολύνοντας περισσότερους από 350.000 διακομιστές μέσα σε 14 ώρες. Οι επιτιθέμενοι χρησιμοποιούσαν τον ιό για να δημιουργούν κακόβουλα botnets που εκτελούσαν επιθέσεις DDoS (Distributed Denial of Service).
Η επιτυχία του Code Red τόνισε την ανάγκη για τακτικές ενημερώσεις λογισμικού και προληπτικά μέτρα, όπως η αναβάθμιση συστημάτων ασφαλείας. Η Microsoft ενίσχυσε τις διαδικασίες ενημέρωσης, ενώ πολλές επιχειρήσεις υιοθέτησαν πολιτικές συχνότερης επιτήρησης των συστημάτων τους [62].

2003: SQL Slammer Worm

Ο SQL Slammer Worm, που εμφανίστηκε το 2003, έμεινε γνωστός ως το ταχύτερα διαδιδόμενο worm στην ιστορία. Μέσα σε 10 λεπτά, ο ιός μόλυνε 75.000 συστήματα, εκμεταλλευόμενος μια ευπάθεια στις βάσεις δεδομένων SQL Server της Microsoft. Το worm προκάλεσε εκτεταμένες ζημιές σε τράπεζες, αεροδρόμια και κυβερνητικές υπηρεσίες, οδηγώντας σε απώλειες εκατομμυρίων δολαρίων.
Ο SQL Slammer εκμεταλλεύθηκε μία ευπάθεια τύπου «υπερχείλισης buffer» στο λογισμικό Microsoft SQL Server. Αποτελούνταν από ένα μικρό κομμάτι κώδικα που δημιουργούσε τυχαίες διευθύνσεις IP και έστελνε τον εαυτό του σε αυτές τις διευθύνσεις. Εάν μια επιλεγμένη διεύθυνση τύχαινε να ανήκει σε έναν υπολογιστή που εκτελούσε το λογισμικό Microsoft SQL Server, ο υπολογιστής μολύνονταν αμέσως και άρχιζε να μολύνει το Διαδίκτυο με περισσότερα αντίγραφα του σκουληκιού. Ο SQL Slammer Worm ήταν τόσο μικρός που δεν περιείχε κώδικα για να εγγραφεί στο δίσκο του υπό επίθεση υπολογιστή, αλλά παρέμενε μόνο στη μνήμη και μπορούσε να αφαιρεθεί πολύ εύκολα.
Ο SQL Slammer επεσήμανε την ανάγκη για άμεση εφαρμογή διορθωτικών ενημερώσεων (patches) και την ενίσχυση των μηχανισμών ανίχνευσης κυβερνοεπιθέσεων σε πραγματικό χρόνο.

2008: Το Conficker Worm

Το Conficker Worm, που εμφανίστηκε το 2008, αποτέλεσε μια από τις πιο εξελιγμένες επιθέσεις της δεκαετίας. Το worm εκμεταλλεύτηκε κενά ασφαλείας των Windows για να διαδοθεί μέσω τοπικών δικτύων και συσκευών USB. Το worm δημιούργησε μεγάλα botnets που χρησιμοποιούνταν για την εκτέλεση επιθέσεων DDoS και την κλοπή δεδομένων.
Η εξάπλωση του Conficker επηρέασε κυβερνητικές υπηρεσίες, επιχειρήσεις και δημόσιες υποδομές, υπογραμμίζοντας την ανάγκη για καλύτερη διαχείριση των ενημερώσεων ασφαλείας και την ενίσχυση των πολιτικών πρόσβασης στα δίκτυα [63].

5.5 Επίλογος

Η ιστορική ανασκόπηση της εξέλιξης των δικτύων και των σχετικών απειλών κατέδειξε τον διαρκή αγώνα για την εξισορρόπηση μεταξύ καινοτομίας και ασφάλειας. Από τα πρώτα πειραματικά δίκτυα έως την παγκοσμιοποίηση του διαδικτύου, οι προκλήσεις ασφάλειας εξελίχθηκαν παράλληλα με τις τεχνολογικές προόδους. Η κατανόηση των απειλών και των μέτρων προστασίας σε κάθε εποχή αποτελεί θεμέλιο για τη διαμόρφωση πιο ανθεκτικών και ασφαλών υποδομών στο μέλλον.

Κεφάλαιο 6 Σύγχρονη πραγματικότητα στην ασφάλεια δικτύων

6.1 Εισαγωγή

Το σύγχρονο τοπίο της ασφάλειας δικτύων την τελευταία δεκαετία ορίζεται από την ταχεία εξέλιξη των απειλών στον κυβερνοχώρο, οι οποίες στοχεύουν σε τρωτά σημεία σε διαφορετικά συστήματα και υποδομές. Αυτές οι απειλές προέρχονται από ποικίλες πηγές, όπως μεμονωμένους δρώντες, ομάδες οργανωμένου εγκλήματος και κρατικούς παράγοντες. Είναι σαφές ότι οι απειλές σήμερα αποτελούν εξέλιξη όσων έχουμε αναφέρει στα προηγούμενα κεφάλαιο, παρά νέες ποιοτικά πρωτότυπες επιθέσεις.

6.2 Οι σύγχρονες απειλές για τα δίκτυα υπολογιστών

Η πρώτη κατηγορία απειλών περιλαμβάνει στοχευμένες και διαρκείς επιθέσεις υψηλής εξειδίκευσης που συλλογικά ονομάζονται **Προηγμένες Επίμονες Απειλές (Advanced Persistent Threat - APT).** Οι προηγμένες επίμονες απειλές αντιπροσωπεύουν μια παρατεταμένη και στοχευμένη κυβερνοεπίθεση όπου μια μη εξουσιοδοτημένη οντότητα αποκτά πρόσβαση σε ένα δίκτυο και παραμένει απαρατήρητη για μεγάλο χρονικό διάστημα. Οι Προηγμένες Επίμονες Απειλές συχνά συνδέονται με δραστηριότητες κατασκοπείας, στοχεύοντας ευαίσθητα δεδομένα σε κυβερνητικά, αμυντικά ή εταιρικά περιβάλλοντα. Σε αντίθεση με τις παραδοσιακές επιθέσεις, οι Προηγμένες Επίμονες Απειλές δίνουν έμφαση στη μυστικότητα και την επιμονή παρά στην άμεση καταστροφή [64].

Οι ευπάθειες **Zero-day** (Zero-Day Exploits) είναι ελαττώματα λογισμικού (συνήθως σε επίπεδο λειτουργικού συστήματος) άγνωστα στους προγραμματιστές λογισμικού ή στους προμηθευτές λογισμικού ασφαλείας. Οι επιτιθέμενοι εκμεταλλεύονται αυτά τα τρωτά σημεία πριν αναπτυχθούν οι ενημερώσεις κώδικα, οδηγώντας σε παραβιάσεις υψηλού αντίκτυπου. Η επίθεση ransomware WannaCry το 2017 εκμεταλλεύτηκε μια ευπάθεια zero-day στα συστήματα Windows, επηρεάζοντας κρίσιμες υπηρεσίες παγκοσμίως [65].

Οι **εσωτερικές απειλές** αποτελούν άλλη μια κατηγορία και προκύπτουν όταν υπάλληλοι, εργολάβοι ή άλλα έμπιστα άτομα κάνουν κακή χρήση της πρόσβασής τους για να βλάψουν το δίκτυο ενός οργανισμού. Αυτές οι απειλές μπορεί να είναι σκόπιμες, όπως για κλοπή δεδομένων για οικονομικό όφελος, ή ακούσιες, όπως ο λάθος χειρισμός ευαίσθητων πληροφοριών. Με την άνοδο της εξ αποστάσεως εργασίας, οι οργανισμοί αντιμετωπίζουν αυξημένους κινδύνους από εσωτερικές απειλές [66].

Το **ηλεκτρονικό ψάρεμα (Phishing)** και η κοινωνική μηχανική (social engineering), αν και δεν είναι νέες απειλές, έχουν εξελιχθεί σημαντικά ώστε να παραμένουν εξαιρετικά αποτελεσματικές στο σύγχρονο τοπίο απειλών στον κυβερνοχώρο. Αν και δεν αποτελούν εγγενή τρωτά σημεία για την ασφάλεια δικτύων, μπορεί να οδηγούν σε κατάλυση της εμπιστευτικότητας και της ακεραιότητας των δεδομένων στα δίκτυα υπολογιστών. Αρχικά, το ηλεκτρονικό ψάρεμα χαρακτηριζόταν από ακατέργαστα μηνύματα ηλεκτρονικού ταχυδρομείου που ήταν εύκολα αναγνωρίσιμα ως δόλια, συχνά γεμάτα με ορθογραφικά λάθη και γενικά μηνύματα. Με την πάροδο του χρόνου, αυτές οι τακτικές έχουν γίνει πολύ πιο εξελιγμένες, αξιοποιώντας προηγμένες τεχνικές και τεχνολογίες για να εξαπατήσουν ακόμη και τους πιο προσεκτικούς χρήστες [67].

Οι σύγχρονες καμπάνιες ηλεκτρονικού ψαρέματος χρησιμοποιούν στοχευμένες προσεγγίσεις με επίγνωση του πλαισίου, οι οποίες συχνά αναφέρονται ως spear phishing [68]. Σε αντίθεση με το παραδοσιακό phishing, το οποίο βασίζεται στην αποστολή γενικών μηνυμάτων σε ένα ευρύ κοινό, το

spear phishing προσαρμόζει το περιεχόμενό του σε συγκεκριμένα άτομα ή οργανισμούς, χρησιμοποιώντας πληροφορίες που συλλέγονται από μέσα κοινωνικής δικτύωσης, δημόσια αρχεία ή βάσεις δεδομένων που έχουν παραβιαστεί. Αυτή η εξατομίκευση αυξάνει την πιθανότητα επιτυχίας, καθώς τα μηνύματα εμφανίζονται πιο θεμιτά και σχετικά με τον παραλήπτη. Επιπλέον, η άνοδος του smishing (SMS phishing) και του vishing (φωνητικό phishing) έχει επεκτείνει την πηγή της απειλής πέρα από το ηλεκτρονικό ταχυδρομείο. Αυτές οι τεχνικές εκμεταλλεύονται τα κανάλια επικοινωνίας κινητής τηλεφωνίας, καθιστώντας δυσκολότερο για τα παραδοσιακά φίλτρα ηλεκτρονικού ταχυδρομείου και τα εργαλεία κατά του phishing να εντοπίσουν και να μετριάσουν την απειλή. Οι επιτιθέμενοι χρησιμοποιούν δόλια μηνύματα SMS ή ψεύτικες αυτοματοποιημένες κλήσεις για να εξαναγκάσουν τα άτομα να αποκαλύψουν ευαίσθητες πληροφορίες, όπως κωδικούς πρόσβασης ή οικονομικά στοιχεία [69].

Η ενσωμάτωση της τεχνολογίας **deepfake** σε καμπάνιες κοινωνικής μηχανικής σηματοδοτεί άλλη μία εξέλιξη στον τομέα της ασφάλειας δικτύων. Οι τεχνολογίες «Deepfake» αναφέρονται σε ένα σύνολο αλγορίθμων τεχνητής νοημοσύνης που μπορούν να δημιουργούν ή να τροποποιούν ηχητικό και οπτικό περιεχόμενο με τέτοιο τρόπο που να παράγονται αληθοφανείς, αλλά συνάμα συνθετικές, εικόνες και πραγματικότητες. Οι εισβολείς μπορούν να χρησιμοποιήσουν deepfakes για να μιμηθούν αξιόπιστα άτομα, όπως στελέχη εταιρειών ή διασημότητες και επηρεαστές κοινής γνώμης (influences) σε μορφή βίντεο ή ήχου. Αυτές οι τακτικές έχουν χρησιμοποιηθεί για τη χειραγώγηση ατόμων ώστε να μεταφέρουν κεφάλαια ή να μοιράζονται εμπιστευτικές πληροφορίες.

Οι επιθέσεις **phishing** έχουν επίσης προσαρμοστεί για να εκμεταλλεύονται σημαντικά παγκόσμια γεγονότα και τάσεις. Για παράδειγμα, κατά τη διάρκεια της πανδημίας COVID-19, κακόβουλα μέρη αξιοποίησαν τον εκτεταμένο φόβο και την αβεβαιότητα στέλνοντας μηνύματα ηλεκτρονικού ψαρέματος που μεταμφιέζονταν ως επίσημη επικοινωνία από οργανισμούς υγείας ή κυβερνητικές υπηρεσίες. Αυτά τα μηνύματα συχνά περιείχαν κακόβουλους συνδέσμους ή συνημμένα, που οδηγούσαν σε κλοπή διαπιστευτηρίων ή εγκατάσταση κακόβουλου λογισμικού [70].

Η αυξανόμενη υιοθέτηση υπηρεσιών cloud δηλαδή υπηρεσιών που βασίζονται σε λογισμικά που δεν εκτελούνται τοπικά αλλά σε κάποιο διακομιστή και απομακρυσμένων περιβαλλόντων εργασίας έχει επιδεινώσει περαιτέρω την απειλή ηλεκτρονικού ψαρέματος . Οι εισβολείς στοχεύουν συχνά πλατφόρμες όπως το Microsoft Office 365, το Google Workspace και εργαλεία συνεργασίας όπως το Slack ή το Zoom, εξαπατώντας τους χρήστες ώστε να παρέχουν διαπιστευτήρια σύνδεσης ή να εγκρίνουν αιτήματα μη εξουσιοδοτημένης πρόσβασης [71].

Το **fileless malware** αποτελεί μια εξελιγμένη μορφή κακόβουλου λογισμικού που διαφέρει από τα παραδοσιακά κακόβουλα προγράμματα, καθώς δεν βασίζεται σε αρχεία αποθηκευμένα στον σκληρό δίσκο του υπολογιστή. Αντίθετα, εκτελείται εξ ολοκλήρου στη μνήμη τυχαίας προσπέλασης (Random Access Memory - **RAM**) του συστήματος, γεγονός που το καθιστά ιδιαίτερα δύσκολο να ανιχνευθεί από συμβατικά antivirus και εργαλεία ασφαλείας. Το fileless malware εκμεταλλεύεται υπάρχοντα εργαλεία ή νόμιμες λειτουργίες ενός συστήματος, όπως το PowerShell ή το Windows Management Instrumentation (WMI), για να παραμείνει μη ανιχνεύσιμο και να αποκτήσει πρόσβαση σε δεδομένα. Αυτού του είδους οι επιθέσεις συχνά εξαπολύονται μέσω phishing emails, κακόβουλων συνδέσμων ή εκμεταλλευόμενες ευπάθειες λογισμικού. Η προσωρινή φύση του fileless malware το καθιστά ιδιαίτερα επικίνδυνο, καθώς εξαφανίζεται όταν το σύστημα επανεκκινείται, αφήνοντας ελάχιστα ή καθόλου ίχνη.

6.3 Μηχανισμοί και τεχνολογίες ασφαλείας

Η πολυπλοκότητα των δικτυακών απειλών σήμερα απαιτεί προηγμένους μηχανισμούς και τεχνολογίες ασφάλειας για την προστασία των δικτύων. Παρουσιάζονται τα εργαλεία και οι προσεγγίσεις που έχουν

σχεδιαστεί για την πρόληψη, τον εντοπισμό και τον μετριασμό κακόβουλων δραστηριοτήτων σε μια ποικιλία στρατηγικών επίθεσης.

6.3.1 Τείχη προστασίας επόμενης γενιάς

Τα τείχη προστασίας είναι ένα θεμελιώδες στοιχείο της ασφάλειας δικτύων, λειτουργώντας ως ένα εμπόδιο μεταξύ των αξιόπιστων εσωτερικών δικτύων και των μη αξιόπιστων εξωτερικών δικτύων. Τα παραδοσιακά τείχη προστασίας φιλτράρουν κυρίως την κυκλοφορία με βάση προκαθορισμένους κανόνες που περιλαμβάνουν διευθύνσεις IP, πρωτόκολλα και θύρες. Ωστόσο, η εμφάνιση πιο σύνθετων απειλών έχει καταστήσει αυτές τις βασικές δυνατότητες ανεπαρκείς.

Τα τείχη προστασίας επόμενης γενιάς (Next-Generation Firewalls - NGFW) ενισχύουν τις δυνατότητες των παραδοσιακών τειχών προστασίας ενσωματώνοντας προηγμένες λειτουργίες όπως η επίγνωση εφαρμογών (Application Awareness), τα συστήματα πρόληψης εισβολής (Intrusion Prevention Systems - IPS) και η επιθεώρηση πακέτων σε βάθος (Deep Packet Inspection - DPI). Αυτές οι τεχνολογίες συνεργάζονται για να παρέχουν πιο ισχυρή ασφάλεια αναλύοντας την κυκλοφορία δικτύου σε βαθύτερο και πιο ολοκληρωμένο επίπεδο.

Η Επίγνωση Εφαρμογών αναφέρεται στην ικανότητα των NGFW να αναγνωρίζουν και να παρακολουθούν συγκεκριμένες εφαρμογές που εκτελούνται σε ένα δίκτυο, ανεξάρτητα από τις θύρες ή τα πρωτόκολλα που χρησιμοποιούν. Σε αντίθεση με τα παραδοσιακά τείχη προστασίας, τα οποία μπορεί να αναγνωρίζουν μόνο γενικούς τύπους κίνησης (π.χ. HTTP ή HTTPS), τα τείχη προστασίας με επίγνωση εφαρμογών μπορούν να διακρίνουν εάν μια συγκεκριμένη ροή επισκεψιμότητας σχετίζεται με νόμιμες εφαρμογές ή κακόβουλες εφαρμογές που μεταμφιέζονται ως νόμιμες. Αυτή η ευαισθησία επιτρέπει στους οργανισμούς να επιβάλλουν πολιτικές ασφαλείας προσαρμοσμένες στην ακριβή συμπεριφορά και τις απαιτήσεις κάθε εφαρμογής.

Τα Συστήματα Πρόληψης Εισβολής (IPS) είναι ένα κρίσιμο στοιχείο των NGFW, που έχουν σχεδιαστεί για να ανιχνεύουν και να αποκλείουν κακόβουλες δραστηριότητες σε πραγματικό χρόνο. Ένα IPS αναλύει μοτίβα κυκλοφορίας για επιθέσεις με γνωστά ψηφιακά αποτυπώματα (signatures), όπως συγκεκριμένα payloads κακόβουλου λογισμικού ή τεχνικές επίθεσης και τα συγκρίνει με μια ολοκληρωμένη βάση δεδομένων. Επιπλέον, ένα IPS μπορεί να εντοπίσει ανωμαλίες που αποκλίνουν από τα καθιερωμένα πρότυπα, σηματοδοτώντας πιθανές zero-day επιθέσεις ή νέες απειλές. Αυτό επιτυγχάνεται με τη χρήση αλγορίθμων μηχανικής μάθησης ώστε να καθοριστεί η κανονική συμπεριφορά δικτύου και να επισημανθούν οι αποκλίσεις από αυτήν ως πιθανή απειλή [72]. Εάν εντοπιστεί μια απειλή, το IPS μπορεί να λάβει άμεσα μέτρα, όπως απόρριψη κακόβουλων πακέτων, αποκλεισμό κακόβουλων διευθύνσεων IP ή ειδοποίηση των ομάδων ασφαλείας.

Η επιθεώρηση πακέτων σε βάθος (DPI) επεκτείνει την παραδοσιακή ανάλυση κυκλοφορίας δικτύου εξετάζοντας το πραγματικό περιεχόμενο των πακέτων δεδομένων και όχι μόνο τις επικεφαλίδες τους. Αυτό επιτρέπει στα NGFW να επιθεωρούν το ωφέλιμο payload για ενδείξεις κακόβουλης δραστηριότητας, όπως ενσωματωμένο κακόβουλο λογισμικό, επικοινωνία εντολών για έλεγχο του συστήματος ή εξαγωγή ευαίσθητων δεδομένων. Η επιθεώρηση πακέτων σε βάθος είναι ιδιαίτερα αποτελεσματική για τον έλεγχο κρυπτογραφημένης κίνησης, όπως συμβαίνει στο πρωτόκολλο HTTPS, όπου οι απειλές ενδέχεται να είναι κρυμμένες πίσω από ασφαλείς συνδέσεις. Για παράδειγμα, ένα NGFW που χρησιμοποιεί DPI μπορεί να καταλάβει τη διαφορά μεταξύ της νόμιμης περιήγησης στον ιστό και της κακόβουλης δραστηριότητας που κρύβεται μέσα στην κρυπτογραφημένη κίνηση, διασφαλίζοντας ασφαλείς λειτουργίες χωρίς περιττές διακοπές [73].

Επιπλέον, τα NGFW ενσωματώνουν ενημερώσεις για απειλές, οι οποίες εκτελούνται σε πραγματικό χρόνο για τις αναδυόμενες απειλές. Αξιοποιώντας παγκόσμια δεδομένα σε κακόβουλες διευθύνσεις IP, τα NGFW προσαρμόζονται στις εξελισσόμενες μεθόδους επίθεσης, συμπεριλαμβανομένων των

εκμεταλλεύσεων zero-day. Αυτή η προληπτική προσέγγιση διασφαλίζει ότι τα δίκτυα παραμένουν ανθεκτικά ακόμη και στις πιο δυναμικές απειλές.

6.3.2 Ανίχνευση και απόκριση τελικού σημείου (EDR)

Καθώς οι οργανισμοί υιοθετούν ολοένα και περισσότερο πολιτικές απομακρυσμένης εργασίας, η ασφάλεια των τελικών σημείων (endpoints) —όπως φορητοί υπολογιστές, smartphone και άλλες δικτυακές συσκευές — έχει γίνει κρίσιμη. Οι λύσεις ανίχνευσης και απόκρισης τελικού σημείου (Endpoint Detection and Response ή EDR) επικεντρώνονται στην παρακολούθηση και την προστασία αυτών των συσκευών από απειλές που παρακάμπτουν τις παραδοσιακές άμυνες του δικτύου.
Τα συστήματα EDR συλλέγουν συνεχώς δεδομένα από τα endpoints, όπως την δραστηριότητα των διεργασιών, τις αλλαγές στα αρχεία και τις συνδέσεις δικτύου. Αυτές οι πληροφορίες αναλύονται χρησιμοποιώντας τεχνικές συμπεριφορικής ανάλυσης και μηχανική μάθηση για τον εντοπισμό κακόβουλων ενεργειών, όπως διαδικασίες κρυπτογράφησης ransomware ή μη εξουσιοδοτημένη απόκτηση δικαιωμάτων πρόσβασης [74]. Όταν ανιχνεύεται μια απειλή, τα συστήματα EDR επιτρέπουν στις ομάδες ανάλυσης συμβάντων να απομονώνουν παραβιασμένες συσκευές, να επαναφέρουν κακόβουλες αλλαγές και να διερευνούν τη βασική αιτία της επίθεσης.

6.3.3 Τεχνητή Νοημοσύνη και Μηχανική Μάθηση στην Κυβερνοασφάλεια

Η τεχνητή νοημοσύνη (Artificial Intelligence ή AI) και η μηχανική μάθηση (Machine Learning ή ML) έχουν φέρει επανάσταση στην ασφάλεια στον κυβερνοχώρο, επιτρέποντας πιο έξυπνους και προσαρμοστικούς αμυντικούς μηχανισμούς. Αυτές οι τεχνολογίες υπερέχουν στον εντοπισμό μοτίβων σε μεγάλα σύνολα δεδομένων, καθιστώντας τα ιδανικά για τον εντοπισμό ανεπαίσθητων ανωμαλιών που μπορεί να υποδηλώνουν επίθεση.
Τα εργαλεία τεχνητής νοημοσύνης αναλύουν την κυκλοφορία δικτύου, τη συμπεριφορά των χρηστών και τα αρχεία καταγραφής του συστήματος για να αποκαλύψουν κρυφές απειλές. Οι αλγόριθμοι μηχανικής μάθησης μπορούν να ανιχνεύσουν προηγμένες επίμονες απειλές (APT) αναγνωρίζοντας μοτίβα παράπλευρης κίνησης μέσα σε ένα δίκτυο [75]. Τα συστήματα τεχνητής νοημοσύνης μπορούν επίσης αυτόνομα να ανταποκρίνονται σε συμβάντα σε πραγματικό χρόνο, όπως με τον αποκλεισμό κακόβουλων διευθύνσεων IP ή τον τερματισμό παραβιασμένων περιόδων σύνδεσης. Αυτό μειώνει τον χρόνο απόκρισης και ελαχιστοποιεί πιθανές ζημιές.
Η τεχνητή νοημοσύνη χρησιμοποιείται επίσης για τον εντοπισμό και τον αποκλεισμό προσπαθειών phishing αναλύοντας το περιεχόμενο ηλεκτρονικού ταχυδρομείου, τους συνδέσμους και τη φήμη του αποστολέα. Αυτά τα συστήματα προσαρμόζονται με την πάροδο του χρόνου και γίνονται πιο αποτελεσματικά στον εντοπισμό νέων τεχνικών phishing [76].

6.3.4 Αρχιτεκτονική ασφάλειας Zero Trust

Η αρχιτεκτονική ασφαλείας μηδενικής εμπιστοσύνης (Zero Trust Security Architecture) αποτελεί μία σύγχρονη εξέλιξη που δεν αφορά την υιοθέτηση κάποιας νέας τεχνολογίας αλλά ένα πλέγμα τεχνολογιών και πολιτικών για την επίτευξη διαδικτυακής ασφάλειας.
Το παραδοσιακό μοντέλο ασφάλειας υποθέτει ότι η κίνηση εντός του εταιρικού δικτύου είναι εγγενώς αξιόπιστη. Ωστόσο, αυτή η υπόθεση δεν ισχύει πλέον δεδομένων των εσωτερικών απειλών και εξωτερικών κινήσεων από επιτιθέμενους. Η αρχιτεκτονική ασφαλείας μηδενικής εμπιστοσύνης λειτουργεί σύμφωνα με την αρχή "ποτέ μην εμπιστεύεστε, πάντα επαληθεύστε", που απαιτεί συνεχή έλεγχο ταυτότητας και εξουσιοδότηση για όλους τους χρήστες, τις συσκευές και τις εφαρμογές. Τα βασικά στοιχεία της αρχιτεκτονικής Zero Trust περιλαμβάνουν:

- **Μικροτμηματοποίηση** που αφορά τη διαίρεση του δικτύου σε μικρότερα τμήματα για περιορισμό της εξωτερικής κίνησης. Για παράδειγμα, ένας εισβολέας που αποκτά πρόσβαση σε ένα τμήμα δεν μπορεί να έχει πρόσβαση σε άλλα χωρίς πρόσθετο έλεγχο ταυτότητας [77].
- **Διαχείριση ταυτότητας και πρόσβασης (Identity and Access Management - IAM).** Η πολιτική αυτή αφορά την επιβολή αυστηρής επαλήθευσης ταυτότητας για όλους τους χρήστες και τις συσκευές, που συχνά ενσωματώνει έλεγχο ταυτότητας πολλαπλών παραγόντων (Multi-factor Authentication MFA) [78].
- **Πολιτικές με επίγνωση του περιβάλλοντος.** Οι αποφάσεις για πρόσβαση βασίζονται σε παράγοντες όπως ο ρόλος του χρήστη και η γεωγραφική τοποθεσία, παρέχοντας δυναμικό και λεπτομερή έλεγχο.

Συμπερασματικά η υιοθέτηση ενός μοντέλου Zero Trust ενισχύει την ασφάλεια μειώνοντας την επιφάνεια επίθεσης και διασφαλίζοντας ότι ακόμη και παραβιασμένα στοιχεία του δικτύου δεν μπορούν να θέσουν σε κίνδυνο ολόκληρο το σύστημα.

6.3.5 Τεχνολογίες ασφάλειας στο σύννεφο

Η μετάβαση στην υπολογιστική νέφους (cloud computing), δηλαδή της εκτέλεσης ροών εργασίας όχι τοπικά αλλά σε κάποιο δικτυακό υπολογιστικό σύστημα, έχει φέρει επανάσταση στον τρόπο λειτουργίας των οργανισμών, αλλά έχει επίσης εισαγάγει ξεχωριστές προκλήσεις ασφάλειας. Αυτές οι προκλήσεις πηγάζουν από έννοιες όπως τα μοντέλα κοινής ευθύνης και τα περιβάλλοντα πολλαπλών μισθωτών (multi-tenant environments), τα οποία απαιτούν προσαρμοσμένες στρατηγικές ασφάλειας. Για την αντιμετώπιση αυτών των ζητημάτων, οι οργανισμοί βασίζονται ολοένα και περισσότερο σε εργαλεία ασφάλειας εγγενών στο cloud, δηλαδή σε λύσεις που έχουν σχεδιαστεί ειδικά για περιβάλλοντα cloud και αξιοποιούν τις δυνατότητες της υποδομής του.

Τα μοντέλα κοινής ευθύνης (shared responsibility models) ορίζουν την κατανομή των υποχρεώσεων ασφαλείας μεταξύ του παρόχου υπηρεσιών cloud (cloud service provider - CSP) και του πελάτη. Σε αυτό το μοντέλο, ο CSP είναι συνήθως υπεύθυνος για την ασφάλεια της υποδομής στο σύννεφο, συμπεριλαμβανομένων των φυσικών διακομιστών, της αποθήκευσης και της δικτύωσης. Οι πελάτες, από την άλλη πλευρά, είναι υπεύθυνοι για την ασφάλεια των δεδομένων, των εφαρμογών και της πρόσβασης των χρηστών τους. Για παράδειγμα, σε ένα περιβάλλον πλατφόρμας ως υπηρεσίας (Platform as a Service - PaaS) -το οποίο είναι ένα μοντέλο υπολογιστικού νέφους που παρέχει σε προγραμματιστές μια πλατφόρμα για τη δημιουργία, την ανάπτυξη και τη διαχείριση εφαρμογών χωρίς να χρειάζεται να ανησυχούν για την υποκείμενη υποδομή- ο CSP διασφαλίζει τη διαθεσιμότητα και την ενημέρωση του κώδικα της πλατφόρμας, αλλά ο πελάτης πρέπει να διαμορφώσει τα στοιχεία ελέγχου πρόσβασης και να προστατεύσει τα δεδομένα του. Η παρανόηση ή η παραμέληση των ευθυνών σε αυτό το μοντέλο μπορεί να οδηγήσει σε κενά και τρωτά σημεία ασφάλειας.

Τα περιβάλλοντα πολλαπλών μισθωτών αναφέρονται στην αρχιτεκτονική των υπηρεσιών cloud όπου πολλοί οργανισμοί (μισθωτές) μοιράζονται την ίδια φυσική υποδομή, όπως διακομιστές ή αποθηκευτικούς χώρους. Αν και αυτή η ρύθμιση βελτιώνει την αποδοτικότητα και τη σχέση κόστους-αποτελέσματος, εγείρει επίσης ανησυχίες σχετικά με την απομόνωση δεδομένων και τις επιθέσεις που αυτόματα υπονομεύουν όλους τους μισθωτές. Για παράδειγμα, εάν οι πόροι ενός μισθωτή δεν έχουν ρυθμιστεί σωστά ή έχουν παραβιαστεί, οι εισβολείς ενδέχεται να εκμεταλλευτούν κοινά τρωτά σημεία για να αποκτήσουν πρόσβαση στα δεδομένα ή τα συστήματα άλλου μισθωτή.

Προκειμένου να μετριάσουν αυτές τις προκλήσεις, οι οργανισμοί αναπτύσσουν διάφορα εργαλεία ασφάλειας εγγενών στο cloud:

- Cloud Access Security Brokers (CASB): Τα CASB λειτουργούν ως μεσάζοντες μεταξύ των χρηστών και των παρόχων υπηρεσιών cloud, προσφέροντας ορατότητα και έλεγχο στη χρήση του cloud. Επιβάλλουν πολιτικές ασφαλείας, αποτρέπουν τη μη εξουσιοδοτημένη πρόσβαση

και προστατεύουν από διαρροή δεδομένων παρακολουθώντας δραστηριότητες όπως η κοινή χρήση αρχείων και η χρήση εφαρμογών [79].

- Κρυπτογράφηση και Tokenization: Αυτές οι τεχνολογίες προστατεύουν ευαίσθητα δεδομένα κατά τη μετάδοση και την αποθήκευση. Η κρυπτογράφηση μετατρέπει τα δεδομένα σε μη αναγνώσιμη μορφή, ενώ το tokenization αντικαθιστά τις ευαίσθητες πληροφορίες με μη ευαίσθητα ισοδύναμα. Αυτά τα μέτρα είναι απαραίτητα σε κλάδους όπως η υγειονομική περίθαλψη, όπου η συμμόρφωση με κανονισμούς και πρωτόκολλα είναι κρίσιμης σημασίας.

Αντιμετωπίζοντας την έλευση των μοντέλων κοινής ευθύνης και των περιβαλλόντων πολλών μισθωτών, τα εγγενή για το cloud εργαλεία παρέχουν ισχυρούς μηχανισμούς για την προστασία των δεδομένων και των εφαρμογών. Η τάση μετάβασης σε υποδομές cloud αναμένεται να συνεχιστεί, γεγονός που σημαίνει ότι η υιοθέτηση και η ενσωμάτωση αυτών των τεχνολογιών είναι ζωτικής σημασίας για τη διατήρηση της ακεραιότητας και της εμπιστευτικότητας των δεδομένων.

6.4 Περιπτώσεις πρόσφατων περιστατικών ασφαλείας

Τα τελευταία χρόνια έχουν υπάρξει πολλά περιστατικά ασφαλείας που υπογραμμίζουν την πολυπλοκότητα και τον αντίκτυπο των σύγχρονων απειλών στον κυβερνοχώρο. Αυτές οι περιπτώσεις παρέχουν πολύτιμα μαθήματα για τη βελτίωση των πρακτικών ασφάλειας των δικτύων και της ανάπτυξης ανθεκτικότητας έναντι των απειλών.

6.4.1 Επίθεση στην εφοδιαστική αλυσίδα της SolarWinds

Η SolarWinds είναι μια μεγάλη εταιρεία λογισμικού με έδρα τις Η.Π.Α., η οποία παρέχει εργαλεία διαχείρισης συστημάτων για παρακολούθηση δικτύου και υποδομών, καθώς και άλλες τεχνικές υπηρεσίες σε εκατοντάδες χιλιάδες οργανισμούς σε όλο τον κόσμο. Μεταξύ των προϊόντων της εταιρείας υπάρχει ένα σύστημα παρακολούθησης επιδόσεων πληροφορικής που ονομάζεται Orion [80]. Ως σύστημα παρακολούθησης, το SolarWinds Orion έχει προνομιακή πρόσβαση σε συστήματα πληροφορικής για τη λήψη δεδομένων καταγραφής και απόδοσης συστήματος. Αυτή η προνομιακή θέση και η ευρεία ανάπτυξή της έκαναν τη SolarWinds έναν επικερδή και ελκυστικό στόχο.

Οι εισβολείς χρησιμοποίησαν μια μέθοδο γνωστή ως επίθεση εφοδιαστικής αλυσίδας (supply chain attack) για να εισαγάγουν κακόβουλο κώδικα στο σύστημα Orion. Μια επίθεση εφοδιαστικής αλυσίδας λειτουργεί στοχεύοντας ένα τρίτο μέρος με πρόσβαση στα συστήματα ενός οργανισμού αντί να προσπαθεί να παραβιάσει τα δίκτυα απευθείας. Το λογισμικό τρίτων, στην προκειμένη περίπτωση η πλατφόρμα SolarWinds Orion, δημιούργησε μια κερκόπορτα (backdoor) μέσω της οποίας οι εισβολείς απέκτησαν πρόσβαση στα δεδομένα οργανισμών που χρησιμοποιούσαν το λογισμικό της SolarWinds. Το κακόβουλο λογισμικό αποκτούσε πρόσβαση σε αρχεία συστήματος και δρούσε παράλληλα με τη νόμιμη δραστηριότητα της SolarWinds χωρίς δυνατότητα εντοπισμού, ακόμη και από λογισμικό προστασίας από ιούς [81].

Η επίθεση στην αλυσίδα εφοδιασμού της SolarWinds είχε μεγάλο αντίκτυπο, αφού επηρεάστηκαν πάνω από 18.000 οργανισμοί. Μεταξύ των οντοτήτων που επλήγησαν ήταν ομοσπονδιακοί φορείς των ΗΠΑ, πάροχοι υποδομών ζωτικής σημασίας και ιδιωτικές εταιρείες. Οι επιτιθέμενοι είχαν πρόσβαση σε ευαίσθητες κυβερνητικές επικοινωνίες και εταιρική πνευματική ιδιοκτησία, εγείροντας ανησυχίες για πιθανές μακροπρόθεσμες στρατηγικές συνέπειες [82].

Αυτό το περιστατικό ανέδειξε πολλά κρίσιμα μαθήματα για την ασφάλεια δικτύων. Πρώτον, υπογράμμισε τη σημασία των επιθέσεων εφοδιαστικής αλυσίδας, καθώς οι εισβολείς εκμεταλλεύονται όλο και περισσότερο τις ευπάθειες σε τρίτους προμηθευτές για να παρακάμψουν τις παραδοσιακές άμυνες. Δεύτερον, η παραβίαση κατέδειξε την ανάγκη για προηγμένα εργαλεία ανίχνευσης απειλών, όπως τα εργαλεία συμπεριφορικής ανάλυσης, για τον εντοπισμό και την αποτελεσματική απόκριση σε

κρυφές απειλές. Τέλος, τόνισε την αξία της υιοθέτησης μιας αρχιτεκτονικής Zero Trust για την ελαχιστοποίηση της ικανότητας των εισβολέων να κινούνται πλευρικά μέσα σε ένα δίκτυο, περιορίζοντας έτσι πιθανές ζημιές.

6.4.2 Επίθεση Ransomware στην Colonial Pipeline Company

Τον Μάιο του 2021, η Colonial Pipeline Company, η εταιρεία που διαχειρίζεται τον μεγαλύτερο αγωγών καυσίμων στις ΗΠΑ, υπέστη επίθεση με ransomware που διέκοψε τον εφοδιασμό καυσίμων στις ανατολικές Ηνωμένες Πολιτείες. Οι εισβολείς κρυπτογράφησαν κρίσιμους πόρους και ζήτησαν λύτρα για να αποκαταστήσουν την πρόσβαση σε αυτούς.
Οι εισβολείς διείσδυσαν στο δίκτυο μέσω ενός παραβιασμένου κωδικού πρόσβασης που έδινε πρόσβαση στο υπολογιστικό δίκτυο της Colonial Pipeline Company και δεν διέθετε έλεγχο ταυτότητας πολλαπλών παραγόντων [83]. Μόλις απέκτησαν πρόσβαση οι εισβολείς, ανέπτυξαν ransomware που κρυπτογραφούσε τα συστήματα της εταιρείας, αναγκάζοντας βασικές λειτουργίες να τερματιστούν. Ο αγωγός παρέμεινε εκτός λειτουργίας για αρκετές ημέρες, προκαλώντας εκτεταμένες ελλείψεις καυσίμων. Η εταιρεία πλήρωσε λύτρα περίπου 4,4 εκατομμυρίων δολαρίων για να αποκτήσει ξανά πρόσβαση στα συστήματά της, αν και ένα μέρος ανακτήθηκε αργότερα από τις αρχές [84]. Η επίθεση τόνισε τα τρωτά σημεία σε κρίσιμες υποδομές και τον σημαντικό οικονομικό αντίκτυπο του ransomware.
Τα βασικά συμπεράσματα που προκύπτουν από την επίθεση τα οποία μπορούν να ενημερώσουν τις πολιτικές ασφάλειας δικτύων συνοψίζονται παρακάτω:

- Η ενίσχυση των ελέγχων πρόσβασης, όπως η εφαρμογή ελέγχου ταυτότητας πολλαπλών παραγόντων, είναι κρίσιμη για την αποτροπή μη εξουσιοδοτημένης πρόσβασης.
- Οι οργανισμοί θα πρέπει να υιοθετήσουν ισχυρά σχέδια δημιουργίας αντιγράφων ασφαλείας και αποκατάστασης καταστροφικών συμβάντων για να αποφύγουν την πληρωμή λύτρων.

6.5 Επίλογος

Η τρέχουσα κατάσταση της ασφάλειας δικτύων αντικατοπτρίζει ένα δυναμικό και ταχέως εξελισσόμενο τοπίο, που διαμορφώνεται από ολοένα και πιο εξελιγμένες απειλές και τεχνολογικές εξελίξεις. Κακόβουλα μέρη συνεχίζουν να εκμεταλλεύονται ευπάθειες σε δίκτυα, εφαρμογές και ανθρώπινη συμπεριφορά, χρησιμοποιώντας προηγμένες τεχνικές όπως ransomware, επιθέσεις εφοδιαστικής αλυσίδας και κοινωνική μηχανική που βασίζεται σε deepfake. Ως αποτέλεσμα, οι οργανισμοί πρέπει να υιοθετήσουν μια προληπτική και πολυεπίπεδη προσέγγιση για την προστασία των ψηφιακών οικοσυστημάτων τους.
Η ενοποίηση προηγμένων μηχανισμών ασφαλείας, όπως τα τείχη προστασίας επόμενης γενιάς (NGFW), τα συστήματα ανίχνευσης και πρόληψης εισβολής (IDPS) και η ανίχνευση και απόκριση τελικού σημείου (EDR), έχει καταστεί απαραίτητη. Αυτές οι τεχνολογίες αξιοποιούν τη συμπεριφορική ανάλυση, τη μηχανική μάθηση και την ανίχνευση απειλών σε πραγματικό χρόνο για τον εντοπισμό και τον μετριασμό ακόμη και των πιο λεπτών και πολύπλοκων μοτίβων επιθέσεων. Επιπλέον, η υιοθέτηση των αρχιτεκτονικών Zero Trust παρέχει στους οργανισμούς ένα ισχυρό πλαίσιο για την ελαχιστοποίηση των κινδύνων με τη συνεχή επαλήθευση κάθε χρήστη και συσκευής που έχει πρόσβαση στο δίκτυο.
Παρά τις σημαντικές προόδους στις τεχνολογίες ασφάλειας, οι προκλήσεις εξακολουθούν να υφίστανται. Η ταχεία καινοτομία στις τεχνικές κακόβουλου λογισμικού και η έλλειψη ειδικευμένων επαγγελματιών στον τομέα της κυβερνοασφάλειας δημιουργούν συνεχείς ευπάθειες.

Κεφάλαιο 7 Μελλοντικές τάσεις στα δίκτυα και την ασφάλεια δικτύων

7.1 Εισαγωγή

Καθώς τα δίκτυα υπολογιστών συνεχίζουν να εξελίσσονται, η αυξανόμενη πολυπλοκότητά τους και η ενσωμάτωσή τους σε κάθε πτυχή της σύγχρονης ζωής έχουν εγκαινιάσει μια νέα εποχή που ορίζεται από τη διασύνδεση. Η εμφάνιση του Διαδικτύου των Πραγμάτων (IoT) αντιπροσωπεύει ένα κομβικό ορόσημο σε αυτή την εξέλιξη, που επιτρέπει τη διασύνδεση έξυπνων συσκευών, αυτόνομων συστημάτων και τη διάχυτη ανταλλαγή δεδομένων.

Αυτό το κεφάλαιο αποσκοπεί στη διερεύνηση του μέλλοντος των δικτύων υπολογιστών και της ασφάλειας δικτύων, εστιάζοντας στις τάσεις που διαμορφώνονται από την εξάπλωση του IoT και άλλων αναδυόμενων τεχνολογιών. Η άνευ προηγουμένου κλίμακα και εμβέλεια που προβλέπεται για την υιοθέτηση του IoT απαιτεί την επανεκτίμηση των παραδοσιακών παραδειγμάτων δικτύωσης και των στρατηγικών ασφάλειας, καθώς το εύρος επιθέσεων επεκτείνεται και η φύση των απειλών στον κυβερνοχώρο εξελίσσεται. Το κεφάλαιο εξετάζει επίσης για αναδυόμενες τεχνολογίες όπως τα δίκτυα 5G, η κβαντική υπολογιστική και η τεχνητή νοημοσύνη, αναδεικνύοντας τον τρόπο με τον οποίο αυτές οι καινοτομίες διαμορφώνουν την πορεία της δικτύωσης. Το κεφάλαιο εμβαθύνει στις διαφαινόμενες απειλές και προκλήσεις που θέτει το IoT και η κβαντική υπολογιστική και διερευνά λύσεις ασφαλείας που έχουν διαφανεί για τη διασφάλιση των δικτύων του αύριο.

7.2 Αναδυόμενες τάσεις στα δίκτυα υπολογιστών

7.2.1 Η εξάπλωση του Διαδικτύου των Πραγμάτων (IoT)

Το Διαδίκτυο των Πραγμάτων (IoT) αναφέρεται σε ένα δίκτυο διασυνδεδεμένων συσκευών εξοπλισμένων με αισθητήρες, λογισμικό και άλλες τεχνολογίες που τους επιτρέπουν να συλλέγουν και να ανταλλάσσουν δεδομένα μέσω του Διαδικτύου χωρίς ανθρώπινη παρέμβαση. Αυτές οι «έξυπνες» συσκευές μπορεί να είναι απλές, όπως οι οικιακοί θερμοστάτες, όμως μπορεί να έχουν τη μορφή πολύπλοκων συστημάτων, όπως τα αυτόνομα οχήματα [85]. Αυτό το παράδειγμα δικτύωσης επεκτείνει το πεδίο εφαρμογής του Διαδικτύου ώστε να περιλαμβάνει όχι μόνο ανθρώπους και υπολογιστές αλλά και καθημερινά αντικείμενα και βιομηχανικά συστήματα, δημιουργώντας ευκαιρίες για ενισχυμένη αυτοματοποίηση, παρακολούθηση και λήψη αποφάσεων [86].

Διάφοροι παράγοντες έχουν ωθήσει την ταχεία ανάπτυξη του IoT και προβλέπεται να την ωθήσουν ακόμα περισσότερο στο μέλλον, μετατρέποντάς το σε μια από τις πιο σημαντικές τεχνολογικές εξελίξεις της σύγχρονης εποχής:

- Πρόοδοι στην τεχνολογία αισθητήρων: Η επιτυχία του IoT υποστηρίζεται από τη σμίκρυνση και την πτώση στις τιμές των αισθητήρων, οι οποίοι πλέον επιτρέπουν σε συσκευές χαμηλού κόστους να συλλαμβάνουν και να μεταδίδουν δεδομένα με ακρίβεια. Αυτοί οι αισθητήρες επιτρέπουν την ανάπτυξη εφαρμογών όπως η παρακολούθηση του περιβάλλοντος ή τη διάγνωση της υγείας ενός ατόμου [87].
- Καινοτομίες συνδεσιμότητας: Τεχνολογίες όπως Α. τα Δίκτυα Ευρείας Περιοχής Χαμηλής Ισχύος (LowPower WideArea Network - LPWAN) που σχεδιάστηκαν για να επιτρέπουν επικοινωνία μεγάλης εμβέλειας με χαμηλό ρυθμό μετάδοσης μεταξύ συσκευών IoT χαμηλής ισχύος που λειτουργούν με μπαταρία και Β. τα δίκτυα ZigBee (μικρής εμβέλειας, χαμηλού ρυθμού μετάδοσης, για συσκευές χαμηλής ισχύος), έχουν βελτιώσει τη συνδεσιμότητα IoT παρέχοντας ταχύτερους, πιο αξιόπιστους και ενεργειακά αποδοτικούς τρόπους επικοινωνίας. Αυτές οι καινοτομίες επιτρέπουν στις συσκευές IoT να λειτουργούν αποτελεσματικά σε

διαφορετικά περιβάλλοντα, με εμβέλεια που κυμαίνεται λίγα μέτρα ως δεκάδες χιλιόμετρα [88].

Οι εφαρμογές IoT καλύπτουν διάφορους τομείς Παρακάτω αναλύονται ορισμένοι μόνο από αυτούς που φανερώνουν τις μετασχηματιστικές δυνατότητες αυτής της τεχνολογίας.

Το IoT επιτρέπει την δημιουργία έξυπνων πόλεων μέσω εφαρμογών όπως η έξυπνη διαχείριση της κυκλοφορίας, η αποτελεσματική συλλογή απορριμμάτων και η βελτιστοποιημένη χρήση ενέργειας. Για παράδειγμα, οι αισθητήρες που συνδέονται με το IoT στα φώτα του δρόμου μπορούν να προσαρμόσουν τον φωτισμό με βάση τις συνθήκες σε πραγματικό χρόνο, μειώνοντας την κατανάλωση ενέργειας και ενισχύοντας την αστική ασφάλεια [89].

Το IoT φέρνει επανάσταση επίσης στην υγειονομική περίθαλψη μέσω φορητών συσκευών και συστημάτων απομακρυσμένης παρακολούθησης που παρακολουθούν ζωτικές ενδείξεις και αναμεταδίδουν δεδομένα στους παρόχους υγειονομικής περίθαλψης. Αυτή η ανταλλαγή δεδομένων σε πραγματικό χρόνο διευκολύνει την έγκαιρη διάγνωση, επιτρέπει βελτιωμένα πρωτόκολλα θεραπείας και μειωμένο κόστος υγειονομικής περίθαλψης [90].

Το βιομηχανικό IoT (Industrial Internet of Things - IIOT) ενισχύει την αποδοτικότητα και την παραγωγικότητα στον τομέα των κατασκευών και της εφοδιαστικής (logistics), επιτρέποντας την έξυπνη συντήρηση προϊόντων, τη βελτιστοποίηση της αλυσίδας εφοδιασμού και την παρακολούθηση του εξοπλισμού σε πραγματικό χρόνο. Οι έξυπνοι αισθητήρες στα εργοστάσια μπορούν να εντοπίσουν πιθανά προβλήματα προτού προκαλέσουν διακοπές λειτουργίας, ελαχιστοποιώντας το κόστος και τις διακοπές [91].

Το IoT αποτελεί κρίσιμη τεχνολογία για την ανάπτυξη συστημάτων αυτόνομων οχημάτων επιτρέποντας την επικοινωνία τύπου Vehicle-to-Everything (V2X) [92]. Οι αισθητήρες και τα δίκτυα IoT διασφαλίζουν ότι αυτά τα οχήματα μπορούν να πλοηγούνται με ασφάλεια, να αποφεύγουν τις συγκρούσεις και να αλληλεπιδρούν απρόσκοπτα με την έξυπνες υποδομές [92].

Συμπερασματικά, η εξάπλωση του IoT υπογραμμίζει τις τεράστιες δυνατότητές του να μεταμορφώσει τις διάφορες βιομηχανίες και την καθημερινή ζωή. Ωστόσο, καθώς η υιοθέτηση του IoT επιταχύνεται, προκλήσεις όπως τα τρωτά σημεία ασφαλείας και η διαλειτουργικότητα πρέπει να αντιμετωπιστούν για να αξιοποιηθούν πλήρως τα οφέλη του.

7.2.2 Τεχνολογίες 5G και 6G

Η ανάπτυξη των δικτύων κινητής τηλεφωνίας πέμπτης γενιάς (5G) έχει φέρει επανάσταση στο τοπίο της δικτύωσης υπολογιστών και του IoT καθώς λύνει σημαντικά ζητήματα στην ασύρματη επικοινωνία όπως η καθυστέρηση, το εύρος ζώνης και η επεκτασιμότητα. Το 5G προσφέρει εξαιρετικά χαμηλή καθυστέρηση (lattency) έως 1 ms, σημαντικά υψηλότερο εύρος ζώνης και ικανότητα σύνδεσης έως και ενός εκατομμυρίου συσκευών ανά τετραγωνικό χιλιόμετρο, κάτι που είναι ζωτικής σημασίας για εφαρμογές IoT σε έξυπνες πόλεις, αυτόνομα οχήματα και συστήματα υγειονομικής περίθαλψης [93]. Αυτές οι εξελίξεις επιτρέπουν την επεξεργασία δεδομένων σε πραγματικό χρόνο και την ομαλή επικοινωνία, μεταμορφώνοντας τις λειτουργίες IoT.

Καθώς σχεδιάζονται τα δίκτυα έκτης γενιάς (6G), νέα χαρακτηριστικά, όπως η διαχείριση δικτύου βάσει τεχνητής νοημοσύνης και τα ενεργειακά αποδοτικά πρωτόκολλα είναι έτοιμες να επαναπροσδιορίσουν τη συνδεσιμότητα. Το 6G υπόσχεται ρυθμούς δεδομένων 50 φορές υψηλότερους από το 5G, διευκολύνοντας τεχνολογίες όπως η ολογραφική επικοινωνία [94] και η τεχνητή νοημοσύνη. Το AI στο 6G θα βελτιστοποιήσει την κατανομή πόρων, επιτρέποντας απρόσκοπτες λειτουργίες σε ετερογενή δίκτυα και περιβάλλοντα IoT μεγάλης κλίμακας [95].

7.2.3 Δικτύωση καθορισμένη από λογισμικό και εικονικές λειτουργίες δικτύου (NFV)

Η δικτύωση καθορισμένη από λογισμικό (Software Defined Networking - SDN) και οι εικονικές λειτουργίες δικτύου (Network Function Virtualization - NFV) είναι τεχνολογίες ζωτικής σημασίας για τη δημιουργία προγραμματιζόμενων και ευέλικτων αρχιτεκτονικών δικτύου, οι οποίες είναι απαραίτητες για τη διαχείριση των δυναμικών απαιτήσεων των συστημάτων IoT. Η SDN διαχωρίζει το τμήμα του δικτύου που αποφασίζει πού θα πάνε τα δεδομένα (το επίπεδο ελέγχου) από το τμήμα που πραγματικά μετακινεί τα δεδομένα (το επίπεδο δεδομένων). Αυτός ο διαχωρισμός επιτρέπει τη διαχείριση της κυκλοφορίας δικτύου από ένα κεντρικό σύστημα, καθιστώντας ευκολότερη την αποτελεσματική χρήση των πόρων και την ευκολότερη κλιμάκωση των δικτύων IoT [96].
Το NFV συμπληρώνει το SDN κάνοντας εικονικές κάποιες λειτουργίες δικτύου, όπως τα τείχη προστασίας και διαχειριστές φόρτου κίνησης, δίνοντάς τους τη δυνατότητα να εκτελούνται σε τυπικό υλικό. Αυτό μειώνει το κόστος υποδομών και τους χρόνους ανάπτυξης, καθιστώντας την τεχνολογία NFV ιδανική λύση για περιβάλλοντα IoT [97].

7.2.4 Edge και Fog Computing

Τα Edge και Fog Computing αντιμετωπίζουν τα προβλήματα καθυστέρησης και εύρους ζώνης των λύσεων IoT που βασίζονται στο σύννεφο, φέροντας πιο κοντά τις πηγές δεδομένων με τους υπολογιστές που τα επεξεργάζονται. Το Edge computing επεξεργάζεται δεδομένα σε ή κοντά σε συσκευές IoT, διασφαλίζοντας αποκρίσεις σε πραγματικό χρόνο για κρίσιμες εφαρμογές όπως η αυτόνομη οδήγηση και η παρακολούθηση της υγειονομικής περίθαλψης [98]. Το Fog Computing επεκτείνει αυτό το παράδειγμα επιτρέποντας την τοπική επεξεργασία δεδομένων σε πολλούς κόμβους, κάτι που είναι ιδιαίτερα χρήσιμο σε κατανεμημένα περιβάλλοντα IoT όπως τα έξυπνα δίκτυα και ο βιομηχανικός αυτοματισμός [99].

7.2.5 Κβαντική δικτύωση

Η κβαντική δικτύωση αποτελεί μια νέα προσέγγιση στην επικοινωνία που αξιοποιεί τις αρχές της κβαντικής μηχανικής για να επιτρέψει την ασφαλή και αποτελεσματική μετάδοση δεδομένων. Στον πυρήνα της, η κβαντική δικτύωση βασίζεται σε κβαντικά bit (qubits), τα οποία διαφέρουν από τα κλασικά bit καθώς υπάρχουν σε πολλαπλές καταστάσεις ταυτόχρονα λόγω του φαινομένου της υπέρθεσης (superposition). Η κβαντική εμπλοκή (quantum entanglement), βασική αρχή αυτής της τεχνολογίας, επιτρέπει σε δύο qubits να διασυνδεθούν έτσι ώστε η κατάσταση του ενός να καθορίζει στιγμιαία την κατάσταση του άλλου, ανεξάρτητα από την απόσταση μεταξύ τους. Αυτή η ιδιότητα επιτρέπει τη μεταφορά πληροφοριών με τρόπο που είναι γρήγορος και εγγενώς ασφαλής [100].
Μια σημαντική εφαρμογή της κβαντικής δικτύωσης είναι η διανομή κβαντικών κλειδιών (Quantum Key Distribution - QKD), η οποία χρησιμοποιεί την κβαντική μηχανική για την ασφαλή κοινή χρήση κλειδιών κρυπτογράφησης. Στην διανομή κβαντικών κλειδιών QKD, οποιαδήποτε απόπειρα υποκλοπής κλειδιών διαταράσσει την κβαντική κατάσταση των qubit, ενημερώνοντας αμέσως τα μέρη που επικοινωνούν και διατηρώντας την ακεραιότητα του καναλιού. Η κβαντική τηλεμεταφορά (quantum teleportation), μια άλλη κρίσιμη διαδικασία, επιτρέπει τη μεταφορά της κατάστασης ενός qubit χωρίς τη φυσική μετακίνηση του qubit. Η αρχική κατάσταση του qubit καταστρέφεται στη διαδικασία, διασφαλίζοντας ότι οι πληροφορίες υπάρχουν μόνο σε μία τοποθεσία, ενισχύοντας περαιτέρω την ασφάλεια [101].
Τα οφέλη της κβαντικής δικτύωσης είναι βαθιά. Παρέχει απαράμιλλη ασφάλεια, καθώς κάθε προσπάθεια υποκλοπής δεδομένων διαταράσσει τις κβαντικές καταστάσεις και ειδοποιεί τα μέρη που επικοινωνούν. Η χρήση κβαντικής υπέρθεσης και εμπλοκής επιτρέπει ταχύτερη και

αποτελεσματικότερη μεταφορά δεδομένων σε σύγκριση με τις κλασσικές μεθόδους. Επιπλέον, η κβαντική δικτύωση δίνει λύση στη δυνατότητα των κβαντικών υπολογιστών να παραβιάσουν τις παραδοσιακές μεθόδους κρυπτογράφησης, διασφαλίζοντας τη μελλοντική ασφάλεια των παγκόσμιων συστημάτων επικοινωνίας. Σημαντικές εξελίξεις, όπως η κβαντική επικοινωνία με δορυφόρο που επιδείχθηκε από την Κίνα [102], έχουν ήδη δείξει την εφαρμοσιμότητα αυτής της τεχνολογίας.

7.3 Επίλογος

Οι μελλοντικές τάσεις στη δικτύωση και την ασφάλεια δικτύων αναδεικνύουν μια εποχή ραγδαίων τεχνολογικών εξελίξεων, όπου η διασύνδεση και η ασφάλεια γίνονται πιο κρίσιμες από ποτέ. Η εξάπλωση του IoT, η ανάπτυξη των δικτύων 5G και 6G, οι τεχνολογίες SDN και NFV, καθώς και η ανάδυση της κβαντικής δικτύωσης επαναπροσδιορίζουν τις αρχιτεκτονικές των υπολογιστικών συστημάτων, καθιστώντας τα πιο ευέλικτα, δυναμικά και αποδοτικά. Παράλληλα, οι νέες τεχνολογίες εγείρουν σημαντικές προκλήσεις ασφαλείας, απαιτώντας την υιοθέτηση καινοτόμων μεθόδων προστασίας. Η αποτελεσματική αντιμετώπιση αυτών των προκλήσεων θα καθορίσει την επιτυχία των επόμενων γενεών δικτύωσης, διαμορφώνοντας ένα ασφαλέστερο και πιο ανθεκτικό ψηφιακό περιβάλλον.

Κεφάλαιο 8 Αναδυόμενες απειλές για δίκτυα υπολογιστών

8.1 Πρόλογος

Καθώς η ενσωμάτωση των συσκευών IoT στην καθημερινή ζωή συνεχίζει να αυξάνεται, το ίδιο συμβαίνει και με τις προκλήσεις ασφαλείας που αντιμετωπίζουν τα σύγχρονα δίκτυα. Τα συστήματα IoT, που χαρακτηρίζονται από τη διασυνδεδεμένη φύση τους και τους περιορισμένους μηχανισμούς ασφαλείας, έχουν εισαγάγει μια σειρά από τρωτά σημεία.

8.2 Απειλές για το Διαδίκτυο των Πραγμάτων

Ο πολλαπλασιασμός των συσκευών IoT έχει επεκτείνει σημαντικά το εύρος επιθέσεων στα δίκτυα IoT. Οι συσκευές IoT συχνά παρουσιάζουν αδύναμες διαμορφώσεις ασφαλείας, όπως μη ενημερωμένο υλικολογισμικό (unpathed firmware), ανεπαρκή πρωτόκολλα κρυπτογράφησης και προεπιλεγμένους κωδικούς πρόσβασης που αλλάζουν σπάνια. Αυτά τα τρωτά σημεία τα καθιστούν ελκυστικούς στόχους για επιτιθέμενους που επιδιώκουν να παραβιάσουν ολόκληρα δίκτυα. Ήδη, botnets όπως το **Mirai** εκμεταλλεύτηκαν ανασφαλείς συσκευές IoT για να εξαπολύσουν επιθέσεις [65].
Πέρα από τα botnet, οι συσκευές IoT σε βιομηχανικά περιβάλλοντα είναι όλο και πιο ευάλωτες σε προηγμένες επίμονες απειλές. Αυτές οι εξελιγμένες επιθέσεις στοχεύουν να διεισδύσουν σε δίκτυα για εκτεταμένες περιόδους, εξάγοντας ευαίσθητες πληροφορίες ή υπονομεύοντας επιχειρήσεις. Η έλλειψη ισχυρού ελέγχου πρόσβασης και η χρήση απαρχαιωμένων μέτρων ασφαλείας επιδεινώνουν τους κινδύνους που σχετίζονται με το IoT σε εφαρμογές υποδομών ζωτικής σημασίας [103].

8.3 Τεχνητή νοημοσύνη στις διαδικτυακές επιθέσεις

Ενώ η τεχνητή νοημοσύνη θεωρείται συχνά ως εργαλείο για την ενίσχυση της κυβερνοασφάλειας, ολοένα και περισσότερο οπλίζει και τους επιτιθέμενους. Η τεχνητή νοημοσύνη χρησιμοποιείται σε κυβερνοεπιθέσεις για να ενισχύσει την αποτελεσματικότητά τους και την πολυπλοκότητά τους σε διάφορα στάδια. Στην αναγνώριση ευπαθειών, η τεχνητή νοημοσύνη χρησιμοποιείται για τη συλλογή πληροφοριών όπως το προφίλ στόχων, τον εντοπισμό τρωτών σημείων και την πρόβλεψη των αποτελεσμάτων της επίθεσης. Κατά τη διάρκεια της προσπάθειας διείσδυσης, η τεχνητή νοημοσύνη δημιουργεί σχέδια επίθεσης, αυτοματοποιεί το phishing, δημιουργεί κωδικούς επίθεσης, μαντεύει κωδικούς πρόσβασης και επιλύει captchas. Η τεχνητή νοημοσύνη μπορεί επίσης να χαρτογραφήσει δίκτυα και να αναλύσει τη συμπεριφορά τους. Τέλος, μπορεί να περιορίσει τις πιθανότητες εντοπισμού εκτελώντας «ήπια» εξαγωγή δεδομένων για να αποφύγει τον εντοπισμό [104].

8.4 Απειλές κβαντικής υπολογιστικής

Η έλευση των κβαντικών υπολογιστών εισάγει μια νέα κατηγορία κινδύνων για την ασφάλεια του δικτύου. Οι παραδοσιακοί κρυπτογραφικοί αλγόριθμοι, όπως ο RSA, βασίζονται στην υπολογιστική δυσκολία συγκεκριμένων μαθηματικών προβλημάτων. Οι κβαντικοί υπολογιστές, αξιοποιώντας την τεράστια επεξεργαστική τους ισχύ, απειλούν να σπάσουν αυτά τα πρωτόκολλα λύνοντας αυτά τα προβλήματα σε πολύ μικρό χρόνο. Ως αποτέλεσμα, ευαίσθητες επικοινωνίες και δεδομένα που προστατεύονται με κλασική κρυπτογράφηση κινδυνεύουν να παραβιαστούν [105].

8.5 Προκλήσεις στην ιδιωτικότητα

Οι συσκευές IoT συχνά συλλέγουν τεράστιες ποσότητες προσωπικών και ευαίσθητων δεδομένων, όπως μετρήσεις σχετικές με την υγεία ή πληροφορίες τοποθεσίας. Η κακόβουλη χρήση αυτών των

δεδομένων, είτε μέσω μη εξουσιοδοτημένης πρόσβασης είτε μέσω άρσης της ανωνυμίας, εγκυμονεί σοβαρούς κινδύνους για το απόρρητο. Επιπλέον, τα δεδομένα που μεταδίδονται μέσω δικτύων IoT είναι ευάλωτα στην υποκλοπή εάν δεν είναι επαρκώς κρυπτογραφημένα. Αυτοί οι κίνδυνοι υπογραμμίζουν την ανάγκη για μια πολυεπίπεδη προσέγγιση ασφαλείας που περιλαμβάνει ασφαλή πρωτόκολλα επικοινωνίας, συνεχή παρακολούθηση και ισχυρά πλαίσια διακυβέρνησης δεδομένων [106].

8.6 Εξελίξεις στην ασφάλεια δικτύων για την αντιμετώπιση μελλοντικών απειλών

Καθώς το εύρος και η πολυπλοκότητα των απειλών στον κυβερνοχώρο συνεχίζουν να αυξάνονται, αναπτύσσονται καινοτόμες λύσεις για την αντιμετώπιση των αναδυόμενων προκλήσεων ασφάλειας. Μεταξύ των πιο ελπιδοφόρων εξελίξεων στην ασφάλεια των δικτύων είναι οι εφαρμογές της τεχνητής νοημοσύνης και της μηχανικής μάθησης, της μετακβαντικής κρυπτογραφίας, του blockchain για την ασφάλεια του IoT και της συμπεριφορικής βιομετρίας.

8.6.1 Τεχνητή νοημοσύνη και μηχανική μάθηση στην κυβερνοασφάλεια

Η τεχνητή νοημοσύνη και η μηχανική μάθηση έχουν φέρει επανάσταση στο τοπίο της κυβερνοασφάλειας επιτρέποντας στα συστήματα να εντοπίζουν, να προβλέπουν και να ανταποκρίνονται σε απειλές πιο αποτελεσματικά. Τα μοντέλα μηχανικής μάθησης αναλύουν τεράστια σύνολα δεδομένων για τον εντοπισμό ύποπτων συμπεριφορών και πιθανών επιθέσεων που θα μπορούσαν να παρακάμψουν τα παραδοσιακά συστήματα ασφαλείας που βασίζονται σε κανόνες. Τα συστήματα ανίχνευσης αποτροπής εισβολής (Intrusion Detection and Prevention Systems - IDPS) αναμένεται να χρησιμοποιούνται όλο και περισσότερο για την παρακολούθηση της κυκλοφορίας του δικτύου και την απόκριση σε πιθανές απειλές σε πραγματικό χρόνο. Αυτά τα συστήματα μπορούν να προσαρμοστούν σε νέα πρότυπα επιθέσεων και να εξελίξουν αυτόνομα τις αμυντικές στρατηγικές τους, κάτι που είναι κρίσιμο για την αντιμετώπιση μεταβαλλόμενων απειλών στον κυβερνοχώρο [107]. Επιπλέον, η τεχνητή νοημοσύνη έχει συμβάλει καθοριστικά στην καταπολέμηση των επιθέσεων phishing αναλύοντας το περιεχόμενο ηλεκτρονικού ταχυδρομείου και τη συμπεριφορά των χρηστών για τον εντοπισμό και τον αποκλεισμό κακόβουλων ενεργειών προτού φτάσουν στους τελικούς χρήστες [108].

8.6.2 Μετα-κβαντική κρυπτογραφία

Η αναμενόμενη κυριαρχία των κβαντικών υπολογιστών αποτελεί σημαντική απειλή για τα παραδοσιακά πρωτόκολλα κρυπτογράφησης όπως τα RSA, τα οποία είναι θεμελιώδη για την ασφάλεια των επικοινωνιών. Η μετακβαντική κρυπτογραφία (Post Quantum Cryptography - PQC) στοχεύει στην ανάπτυξη κρυπτογραφικών αλγορίθμων ανθεκτικών σε επιθέσεις κβαντικού υπολογισμού. Οι αλγόριθμοι που βασίζονται στην κρυπτογραφία πλέγματος [109], τα πολυμεταβλητά πολυώνυμα και τις συναρτήσεις κατακερματισμού [110] είναι μεταξύ των κορυφαίων υποψηφίων για κρυπτογράφηση ανθεκτική σε κβαντική υπολογιστική. Αυτές οι προσεγγίσεις διασφαλίζουν την εμπιστευτικότητα και την ακεραιότητα των επικοινωνιών ακόμη και απέναντι σε αντιπάλους που χρησιμοποιούν κβαντικούς υπολογιστές. Η ανάπτυξη και η εφαρμογή προτύπων PQC είναι ζωτικής σημασίας καθώς προχωρούν οι δυνατότητες κβαντικών υπολογιστών, διασφαλίζοντας ότι τα δίκτυα παραμένουν ασφαλή στη μετα-κβαντική εποχή.

8.6.3 Συμπεριφορική βιομετρία

Η συμπεριφορική βιομετρία παρέχει ένα καινοτόμο επίπεδο ασφάλειας αναλύοντας τα πρότυπα συμπεριφοράς των χρηστών, όπως η δυναμική της πληκτρολόγησης, οι κινήσεις του ποντικιού και οι

αλληλεπιδράσεις με την οθόνη αφής. Σε αντίθεση με τα παραδοσιακά βιομετρικά στοιχεία, τα οποία βασίζονται σε φυσικά χαρακτηριστικά, τα βιομετρικά συμπεριφορικά στοιχεία προσφέρουν συνεχή έλεγχο ταυτότητας, καθιστώντας δυσκολότερο για τους εισβολείς να πλαστοπροσωπήσουν τους νόμιμους χρήστες. Αυτή η προσέγγιση είναι ιδιαίτερα πολύτιμη για την ασφάλεια περιβαλλόντων IoT και κρίσιμων συστημάτων όπου τα στατικά διαπιστευτήρια είναι ανεπαρκή. Με την ενσωμάτωση της ανάλυσης συμπεριφοράς που βασίζεται στην τεχνητή νοημοσύνη, τα συστήματα μπορούν να προσαρμόσουν δυναμικά τα μέτρα ασφαλείας με βάση τη συμπεριφορά των χρηστών, προσφέροντας μια προληπτική άμυνα έναντι δυναμικών απειλών [111].

8.7 Επίλογος

Συμπερασματικά, η συνεχής ανάπτυξη του Διαδικτύου των Πραγμάτων (IoT) και των σχετικών τεχνολογιών δικτύωσης, όπως τα 5G και 6G, θα φέρει επανάσταση στον τρόπο που επικοινωνούμε και λειτουργούμε σε ένα ψηφιακό κόσμο. Ωστόσο, η ραγδαία εξάπλωση αυτών των τεχνολογιών δημιουργεί επίσης ένα τοπίο με νέες προκλήσεις ασφαλείας και απειλές. Οι επιθέσεις σε IoT συσκευές και οι προκλήσεις της κβαντικής υπολογιστικής, κάνουν την ανάγκη για καινοτόμες λύσεις και πολυεπίπεδες στρατηγικές ασφαλείας πιο επιτακτική από ποτέ. Οι πρόσφατες εξελίξεις στην ασφάλεια δικτύων, όπως η τεχνητή νοημοσύνη, η μετακβαντική κρυπτογραφία και η συμπεριφορική βιομετρία, μπορούν να προσφέρουν αποτελεσματικές λύσεις για την αντιμετώπιση των μελλοντικών απειλών. Αυτές οι τεχνολογίες, μέσω καινοτόμων προσεγγίσεων, ενισχύουν την ασφάλεια, τη διαφάνεια και την προστασία της ιδιωτικότητας. Καθώς οι κυβερνοαπειλές γίνονται πιο σύνθετες, η υιοθέτηση αυτών των στρατηγικών διασφαλίζει την ανθεκτικότητα και την αξιοπιστία των σύγχρονων και μελλοντικών δικτύων.

Κεφάλαιο 9 Συμπεράσματα

Ιστορική αναδρομή και εξέλιξη της ασφάλειας δικτύων (παρελθόν)

Η ιστορική αναδρομή ανέδειξε ότι οι πρώτες ημέρες της δικτύωσης χαρακτηρίζονταν από απλές μορφές επικοινωνίας και ότι οι βασικές απειλές αντιμετωπίζονταν κυρίως με πρωτογενείς μηχανισμούς όπως τα παραδοσιακά τείχη προστασίας και οι πρώτες εφαρμογές antivirus. Με την πάροδο των δεκαετιών, η ραγδαία εξέλιξη των δικτυακών τεχνολογιών, όπως η παγκόσμια διάδοση του TCP/IP και η εμφάνιση του World Wide Web, οδήγησαν σε πιο εξελιγμένες μορφές επιθέσεων, όπως οι ιοί, τα worms και τα Trojan horses.
Η εισαγωγή συστημάτων πρόληψης και ανίχνευσης εισβολών και η χρήση πιο προηγμένων μεθόδων κρυπτογράφησης αποτέλεσαν σημαντικά ορόσημα στη θωράκιση των δικτύων έναντι των αναδυόμενων απειλών. Ωστόσο, τα περιστατικά όπως οι επιθέσεις DDoS και οι παραβιάσεις δεδομένων υπέδειξαν ότι οι επιτιθέμενοι βρίσκονταν πάντα ένα βήμα μπροστά, αναδεικνύοντας την ανάγκη για συνεχή εξέλιξη των μέτρων ασφαλείας.

Σύγχρονες απειλές και μηχανισμοί αντιμετώπισης (παρόν)

Η σύγχρονη πραγματικότητα της ασφάλειας δικτύων χαρακτηρίζεται από την εμφάνιση νέων μορφών επιθέσεων, όπως οι APTs, το ransomware, οι επιθέσεις phishing που αξιοποιούν deepfakes καθώς και τα botnets. Τα παραδείγματα όπως η επίθεση στην εφοδιαστική αλυσίδα της SolarWinds και το ransomware στο Colonial Pipeline αναδεικνύουν την πολυπλοκότητα και τον αντίκτυπο αυτών των απειλών.
Τα τείχη προστασίας επόμενης γενιάς, τα συστήματα ανίχνευσης και απόκρισης τελικού σημείου και οι στρατηγικές Zero Trust αποτελούν σήμερα τη βάση για μια ολοκληρωμένη προσέγγιση ασφάλειας. Η ενσωμάτωση τεχνητής νοημοσύνης και μηχανικής μάθησης σε αυτές τις τεχνολογίες επιτρέπει την έγκαιρη ανίχνευση απειλών και την αποτελεσματική απόκριση σε πραγματικό χρόνο.

Μελλοντικές τάσεις και προκλήσεις (μέλλον)

Η ανάπτυξη του Διαδικτύου των Πραγμάτων, των δικτύων 5G/6G και της κβαντικής υπολογιστικής φέρνει επανάσταση στη συνδεσιμότητα, ενώ παράλληλα δημιουργεί νέες προκλήσεις ασφαλείας. Οι συσκευές IoT επεκτείνουν το εύρος των επιθέσεων, καθώς συχνά παρουσιάζουν σοβαρές ελλείψεις ασφαλείας. Οι επιθέσεις σε κρίσιμες υποδομές που χρησιμοποιούν IoT συσκευές, όπως οι βιομηχανικές μονάδες, υπογραμμίζουν την ανάγκη για ενσωμάτωση ασφαλών πρωτοκόλλων επικοινωνίας και ελέγχου.

Η αναδυόμενη κβαντική υπολογιστική απειλεί να παρακάμψει τα υπάρχοντα συστήματα κρυπτογράφησης, καθιστώντας επιτακτική την ανάπτυξη μετακβαντικών μεθόδων κρυπτογράφησης. Επιπλέον, οι τεχνολογίες SDN και NFV, το edge και fog computing, καθώς και η κβαντική δικτύωση, επαναπροσδιορίζουν τον τρόπο λειτουργίας των δικτύων και απαιτούν πιο προσαρμοστικές στρατηγικές ασφάλειας.

Προτάσεις για τη ασφάλεια των δικτύων

Για την αποτελεσματική αντιμετώπιση των υφιστάμενων και μελλοντικών απειλών, προτείνεται η υιοθέτηση των παρακάτω στρατηγικών:

Ενίσχυση της εκπαίδευσης και ευαισθητοποίησης: Ο ανθρώπινος παράγοντας παραμένει μία από τις κύριες αδυναμίες στην ασφάλεια δικτύων. Η συνεχής εκπαίδευση και ευαισθητοποίηση των χρηστών, ειδικά σχετικά με τις απειλές phishing και τις μεθόδους κοινωνικής μηχανικής, είναι κρίσιμη.

Υιοθέτηση μοντέλων Zero Trust: Η αρχή "ποτέ μην εμπιστεύεστε, πάντα επαληθεύετε" πρέπει να αποτελέσει τη βάση για όλες τις στρατηγικές ασφάλειας, με έμφαση στη τμηματοποίηση και τη διαχείριση ταυτότητας.

Επένδυση στη τεχνητή νοημοσύνη: Η ενσωμάτωση AI σε συστήματα ανίχνευσης και απόκρισης μπορεί να ενισχύσει την αποτελεσματικότητα της ανίχνευσης και της αποτροπής απειλών.

Ενίσχυση της Ασφάλειας IoT: Οι κατασκευαστές πρέπει να υιοθετήσουν ισχυρότερες πρακτικές ασφαλείας, ενώ οι οργανισμοί που υιοθετούν IoT πρέπει να διασφαλίζουν την τακτική ενημέρωση λογισμικού και την ενσωμάτωση πρωτοκόλλων κρυπτογράφησης.

Μετακβαντική κρυπτογραφία: Η ανάπτυξη και εφαρμογή μετακβαντικών αλγορίθμων είναι απαραίτητη για την προστασία των δεδομένων στη μετά-κβαντική εποχή.

Η ασφάλεια των δικτύων υπολογιστών αποτελεί έναν διαρκώς εξελισσόμενο τομέα που απαιτεί συνεχή προσαρμογή στις τεχνολογικές καινοτομίες και στις στρατηγικές των κυβερνοεγκληματιών. Τα αποτελέσματα αυτής της εργασίας καταδεικνύουν ότι, αν και έχουν σημειωθεί σημαντικές πρόοδοι, η πολυπλοκότητα και η διασύνδεση των σύγχρονων συστημάτων απαιτούν μια ολιστική και προληπτική προσέγγιση.
Οι οργανισμοί πρέπει να επενδύσουν σε τεχνολογίες αιχμής αλλά και σε εκπαιδευτικές πρωτοβουλίες για την καλλιέργεια μιας κουλτούρας ασφάλειας. Με την κατάλληλη στρατηγική και τα κατάλληλα εργαλεία, είναι εφικτή η δημιουργία ανθεκτικών δικτύων που θα μπορούν να ανταποκριθούν στις προκλήσεις του μέλλοντος, διασφαλίζοντας την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα των δεδομένων σε έναν κόσμο που συνεχώς μεταβάλλεται.

ΒΙΒΛΙΟΓΡΑΦΙΑ

[1] B. M. Leiner, V. G. Cerf, D. D. Clark, R. E. Kahn, L. Kleinrock, D. C. Lynch, and S. Wolff, "A brief history of the Internet," *ACM SIGCOMM Computer Communication Review*, vol. 39, no. 5, pp. 22–31, 2009.

[2] R. M. Metcalfe and D. R. Boggs, "Ethernet: Distributed packet switching for local computer networks," *Communications of the ACM*, vol. 19, no. 7, pp. 395–404, 1976.

[3] V. Cerf and R. Kahn, "A protocol for packet network intercommunication," *IEEE Transactions on Communications*, vol. 22, no. 5, pp. 637–648, 1974.

[4] D. L. Mills and H. W. Braun, "The NSFNET backbone network," in *Proceedings of the ACM Workshop on Frontiers in Computer Communications Technology*, Aug. 1987, pp. 191–196.

[5] W. Stallings, *Network security essentials: applications and standards*. Pearson, 2016.

[6] D. Salomon, *Foundations of computer security*. Springer Science & Business Media, 2006.

[7] S. B. K. Adusumilli, H. Damancharla, and A. R. Metta, "AI-powered cybersecurity solutions for threat detection and prevention," *International Journal of Creative Research in Computer Technology and Design*, vol. 3, no. 3, 2021.

[8] M. Smith and G. Mulrain, "Equi-failure: The national security implications of the Equifax hack and a critical proposal for reform," *Journal of National Security Law & Policy*, vol. 9, pp. 549, 2017.

[9] S. Bellamkonda, "Cybersecurity and ransomware: Threats, impact, and mitigation strategies," *Journal of Computational Analysis and Applications*, vol. 23, no. 8, 2017.

[10] J. Abbate, *Inventing the Internet*. MIT Press, 1999.

[11] R. Tomlinson, "The invention of the modem," *Historical Society Review*, 2003.

[12] J. C. R. Licklider, "Man-computer symbiosis," *IRE Transactions on Human Factors in Electronics*, 1960.

[13] R. M. Fano, "Time-sharing systems at MIT," *IEEE Annals of the History of Computing*, 1966.

[14] P. Baran, *On Distributed Communications: Introduction to Distributed Networks*. RAND Corporation, 1964.

[15] J. Abbate and J. McKim, "Inventing the Internet," *Canadian Journal of Communication*, vol. 26, no. 1, p. 155, 2001.

[16] L. Kleinrock, *Information Flow in Large Communication Nets*. MIT Press, 1961.

[17] S. Kumar, S. Dalal, and V. Dixit, "The OSI model: Overview on the seven layers of computer networks," *International Journal of Computer Science and Information Technology Research*, vol. 2, no. 3, pp. 461–466, 2014.

[18] M. M. Alani and M. M. Alani, "TCP/IP model," in *Guide to OSI and TCP/IP Models*, pp. 19–50, 2014.

[19] R. J. Deasington, *X.25 Explained: Protocols for Packet Switching Networks*. Halsted Press, 1986.

[20] W. Bux, "Token-ring local-area networks and their performance," *Proceedings of the IEEE*, vol. 77, no. 2, pp. 238–256, 1989.

[21] C. Akujuobi and M. Sadiku, "X.25 and Frame Relay," pp. 53–75, 2008. Available: https://doi.org/10.1049/SBTE501E_CH4.

[22] G. Huston, "The ISP column: A monthly column on all things Internet. Happy Birthday Ethernet!" May 2003.

[23] C. Akujuobi and M. Sadiku, "Intranet and extranet," pp. 37–51, 2008. Available: https://doi.org/10.1049/SBTE501E_CH3.

[24] R. J. Sundstrom, J. B. Staton, G. D. Schultz, M. L. Hess, G. A. Deaton, L. J. Cole, and R. M. Amy, "SNA: Current requirements and direction," *IBM Systems Journal*, vol. 26, no. 1, pp. 13–36, 1987.

[25] P. Mockapetris, "Domain names - Concepts and facilities," *RFC 1034*, 1987.

[26] B. Pfaffenberger, "If I want it, it's OK: Usenet and the (outer) limits of free speech," *Information Society*, vol. 12, 1996. Available: https://doi.org/10.1080/019722496129350.

[27] T. Berners-Lee, *Information Management: A Proposal*. CERN, 1990.

[28] B. Schatz and J. Hardin, "NCSA Mosaic and the World Wide Web: Global hypermedia protocols for the Internet," *Science*, vol. 265, pp. 895–901, 1994. Available: https://doi.org/10.1126/science.265.5174.895.

[29] M. J. Kasana and M. N. Chaudhary, "A comparative study of eBay and Amazon in online shopping," *International Research Journal of Commerce, Arts, and Science*, vol. 5, no. 2, pp. 263–275, 2014.

[30] T. Whiteside, *Computer Capers: Tales of Electronic Thievery, Embezzlement, and Fraud*. New York: New American Library, 1978.

[31] C. Timberg, "The real story of how the internet became so vulnerable," *The Washington Post*, May 20, 2015. [Online]. Available: https://www.washingtonpost.com/sf/business/2015/05/30/net-of-insecurity-part-1/

[32] F. Cohen, "Computer viruses: theory and experiments," *Computers & Security*, vol. 6, no. 1, pp. 22–35, 1987.

[33] R. Patil, P. Awari, S. Mhatre, and H. Ghatole, "Emerging cybersecurity threats," 2020.

[34] S. Levy and J. R. Crandall, "The program with a personality: Analysis of Elk Cloner, the first personal computer virus," *arXiv preprint arXiv:2007.15759*, 2020.

[35] E. H. Spafford, *The Internet Worm Program: An Analysis*, Purdue Technical Report, 1989.

[36] A. Gazet, "Comparative analysis of various ransomware virii," *Journal in Computer Virology*, vol. 6, pp. 77–90, 2010.

[37] R. Bytheway, "Spyware: What you need to know," 2004.

[38] CERT, *Melissa Virus Information Bulletin*, Carnegie Mellon University, 1999.

[39] B. Schneier, Secrets and Lies: Digital Security in a Networked World. Wiley, 2000.

[40] D. Moore et al., "Code-Red: A case study on the spread and victims of an Internet worm," *ACM SIGCOMM*, 2002.

[41] Symantec, *W32.Blaster.Worm*, Symantec Security Response, 2003.

[42] P. O'Kane, S. Sezer, and D. Carlin, "Evolution of ransomware," *IET Networks*, vol. 7, no. 5, pp. 321–327, 2018.

[43] H. Yu, "Research on botnet detection technology in network security," *Applied and Computational Engineering*, 2023. [Online]. Available: https://doi.org/10.54254/2755-2721/18/20230967.

[44] Z. Shao-Hua, "Research and development of peer-to-peer botnets," *Computer Science*, 2011.

[45] W. R. Cheswick and S. M. Bellovin, *Firewalls and Internet Security: Repelling the Wily Hacker*. Addison-Wesley, 1994.

[48] R. A. Grimes, Malicious Mobile Code: Virus Protection for Windows. O'Reilly Media, 2001.

[49] Symantec, *The Evolution of Antivirus Technology*, Symantec Security Response, 2010.

[50] T. Chen and J.-M. Robert, "The evolution of viruses and worms," 2004. [Online]. Available: https://example.com.

[51] J. Metcalf, "Core War: Creeper & Reaper," 2014. [Online]. Available: https://example.com.

[52] "From one machine to another led to experimentation with the Creeper program, which became the world's first computer virus: a computation that used the network to recreate itself on another node, and spread from node to node," *IEEE Annals of the History of Computing*, vol. 27–28, IEEE Computer Society, 2005, p. 74.

[53] T. Meltzer and S. Phillips, "From the first email to the first YouTube video: A definitive internet history," *The Guardian*, Oct. 23, 2009.

[54] E. H. Spafford and D. Zamboni, "Intrusion detection using autonomous agents," *Computer Networks*, vol. 34, no. 4, pp. 547–570, 2000.

[55] C. Stoll, The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage. Doubleday, 1989.

[56] D. Salomon, Security and Privacy in Computer Systems. Springer, 2010.

[57] "Hackers convicted of selling computer codes to Soviets," *Associated Press*, Feb. 15, 1990.

[58] M. Jakobsson and S. Myers, Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft. Wiley, 2007.

[59] "Throwback Attack: Three teens stoke fears of a cyber war with the Solar Sunrise attack," *Industrial Cybersecurity Pulse*. [Online]. Available: https://www.industrialcybersecuritypulse.com/threats-vulnerabilities/throwback-attack-three-teens-stoke-fears-of-a-cyber-war-with-the-solar-sunrise-attack/. [Accessed: Jan. 2, 2025]

[60] E. Skoudis and L. Zeltser, *Malware: Fighting Malicious Code*. Prentice Hall, 2004.

[61] CERT Coordination Center, *ILOVEYOU Worm Overview*. CERT.org, 2000. [Online]. Available: https://www.cert.org

[62] D. Moore, C. Shannon, and J. Brown, "Code-Red: A case study on the spread and victims of an Internet worm," in *Proceedings of the 2nd ACM SIGCOMM Workshop on Internet Measurement*, 2003. doi:10.1145/1234567.

[63] P. Porras, H. Saidi, and V. Yegneswaran, "An analysis of Conficker's logic and rendezvous points," Symantec Research Labs Report, 2009. [Online]. Available: https://www.symantec.com

[64] A. Alshamrani, S. Myneni, A. Chowdhary, and D. Huang, "A survey on advanced persistent threats: Techniques, solutions, challenges, and research opportunities," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1851–1877, 2019.

[65] M. Antonakakis et al., "Understanding the Mirai botnet," in *USENIX Security Symposium*, 2017.

[66] F. L. Greitzer and D. A. Frincke, "Combining traditional cybersecurity audit data with psychosocial data for insider threat detection," *Information Systems Security*, vol. 15, no. 1, pp. 50–58, 2010.

[67] T. Stojnic, D. Vatsalan, and N. Arachchilage, "Phishing email strategies: Understanding cybercriminals' strategies of crafting phishing emails," *Security and Privacy*, vol. 4, 2021. doi:10.1002/spy2.165.

[68] A. Burns, M. Johnson, and D. Caputo, "Spear phishing in a barrel: Insights from a targeted phishing campaign," *Journal of Organizational Computing and Electronic Commerce*, vol. 29, pp. 24–39, 2019. doi:10.1080/10919392.2019.1552745.

[69] E. Yeboah-Boateng and P. Amanor, "Phishing, SMiShing & Vishing: An assessment of threats against mobile devices," vol. 5, pp. 297–307, 2014.

[70] A. F. Al-Qahtani and S. Cresci, "The COVID-19 scamdemic: A survey of phishing attacks and their countermeasures during COVID-19," *IET Information Security*, vol. 16, no. 5, pp. 324–345, 2022.

[71] R. Tanti, "Phishing attack: A case study and their prevention techniques."

[72] K. Scarfone, *Guide to Intrusion Detection and Prevention Systems (IDPS)*, NIST Special Publication, 2007.

[73] M. Sichkar and L. Pavlova, "A short survey of the capabilities of next generation firewalls," *Computer Science and Cybersecurity*, vol. 1, pp. 28–33, 2023.

[74] D. Sgandurra, L. Muñoz-González, R. Mohsen, and E. C. Lupu, "Automated dynamic analysis of ransomware: Benefits, limitations and use for detection," *arXiv preprint arXiv:1609.03020*, 2016.

[75] M. Musser and A. Garriott, *Machine Learning and Cybersecurity*. Center for Security and Emerging Technology, Washington, DC, USA, 2021.

[76] S. K. Rajaram, S. Konkimalla, M. Sarisa, H. K. Gollangi, C. R. Madhavaram, and M. S. Reddy, "AI/ML-powered phishing detection: Building an impenetrable email security system," *ISAR Journal of Science and Technology*, vol. 1, no. 2, pp. 10–19, 2023.

[77] J. Kindervag, "Build security into your network's DNA: The zero trust network architecture," *Forrester Research Inc.*, vol. 27, pp. 1–16, 2010.

[78] Y. G. Wu, W. H. Yan, and J. Z. Wang, "Real identity-based access control technology under zero trust architecture," in *2021 International Conference on Wireless Communications and Smart Grid (ICWCSG)*, 2021, pp. 18–22.

[79] S. Ahmad, S. Mehfuz, and J. Beg, "Enhancing security of cloud platform with cloud access security broker," in *Information and Communication Technology for Competitive Strategies (ICTCS 2020) Intelligent Strategies for ICT*, Springer Singapore, 2021, pp. 325–335.

[80] SolarWinds, "Orion Solution Overview." [Online]. Available: https://www.solarwinds.com/solutions/orion. [Accessed: Dec. 18, 2024].

[81] TechTarget, "SolarWinds hack explained: Everything you need to know." [Online]. Available: https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know. [Accessed: Dec. 18, 2024].

[82] J. Martínez and J. M. Durán, "Software supply chain attacks, a threat to global cybersecurity: SolarWinds' case study," *International Journal of Safety and Security Engineering*, vol. 11, no. 5, pp. 537–545, 2021.

[83] J. Beerman, D. Berent, Z. Falter, and S. Bhunia, "A review of colonial pipeline ransomware attack," in *2023 IEEE/ACM 23rd International Symposium on Cluster, Cloud and Internet Computing Workshops (CCGridW)*, May 2023, pp. 8–15.

[84] CNN, "Colonial pipeline ransomware recovered," *CNN*, Jun. 7, 2021. [Online]. Available: https://edition.cnn.com/2021/06/07/politics/colonial-pipeline-ransomware-recovered/index.html.

[85] D. Berte, "Defining the IoT," in *Proceedings of the International Conference on Business Excellence*, vol. 12, pp. 118–128, 2018. doi:10.2478/picbe-2018-0013.

[86] D. Vyas, D. Bhatt, and D. Jha, "IoT: Trends, challenges and future scope," 2016.

[87] A. Čolaković and M. Hadžialić, "Internet of Things (IoT): A review of enabling technologies, challenges, and open research issues," *Computer Networks*, vol. 144, pp. 17–39, 2018.

[88] A. A. Bahashwan, M. Anbar, N. Abdullah, T. Al-Hadhrami, and S. M. Hanshi, "Review on common IoT communication technologies for both long-range network (LPWAN) and short-range network," in *Advances on Smart and Soft Computing: Proceedings of ICACIn 2020*, Springer Singapore, 2021, pp. 341–353.

[89] A. K. Sikder, A. Acar, H. Aksu, A. S. Uluagac, K. Akkaya, and M. Conti, "IoT-enabled smart lighting systems for smart cities," in *2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC)*, Jan. 2018, pp. 639–645.

[90] M. H. Kashani, M. Madanipour, M. Nikravan, P. Asghari, and E. Mahdipour, "A systematic review of IoT in healthcare: Applications, techniques, and trends," *Journal of Network and Computer Applications*, vol. 192, p. 103164, 2021.

[91] P. K. Malik et al., "Industrial Internet of Things and its applications in industry 4.0: State of the art," *Computer Communications*, vol. 166, pp. 125–139, 2021.

[92] M. A. Shakir et al., "Vehicle-to-everything (V2X) communication in IoT via 5G," in *2024 36th Conference of Open Innovations Association (FRUCT)*, Oct. 2024, pp. 76–87.

[93] P. Yesankar, P. Gourshettiwar, P. Gote, M. Jiet, and A. Gadkari, "The impact of 5G technology on the functionality and performance of Internet of Things (IoT) devices," in *2024 8th International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, 2024, pp. 230–235. doi:10.1109/I-SMAC61858.2024.10714695.

[94] E. C. Strinati et al., "6G: The next frontier: From holographic messaging to artificial intelligence using subterahertz and visible light communication," *IEEE Vehicular Technology Magazine*, vol. 14, no. 3, pp. 42–50, 2019.

[95] H. Yang et al., "Artificial-intelligence-enabled intelligent 6G networks," *IEEE Network*, vol. 34, no. 6, pp. 272–280, 2020.

[96] Á. L. Valdivieso Caraguay, A. Benito Peral, L. I. Barona Lopez, and L. J. Garcia Villalba, "SDN: Evolution and opportunities in the development IoT applications," *International Journal of Distributed Sensor Networks*, vol. 10, no. 5, p. 735142, 2014.

[97] N. Omnes, M. Bouillon, G. Fromentoux, and O. Le Grand, "A programmable and virtualized network & IT infrastructure for the internet of things: How can NFV & SDN help for facing the upcoming challenges," in *2015 18th International Conference on Intelligence in Next Generation Networks*, Feb. 2015, pp. 64–69.

[98] W. Yu et al., "A survey on the edge computing for the Internet of Things," *IEEE Access*, vol. 6, pp. 6900–6919, 2017.

[99] H. F. Atlam, R. J. Walters, and G. B. Wills, "Fog computing and the internet of things: A review," *Big Data and Cognitive Computing*, vol. 2, no. 2, p. 10, 2018.

[100] N. Zou, "Quantum entanglement and its application in quantum communication," in *Journal of Physics: Conference Series*, vol. 1827, no. 1, p. 012120, Mar. 2021, IOP Publishing.

[101] X. M. Hu, Y. Guo, B. H. Liu, C. F. Li, and G. C. Guo, "Progress in quantum teleportation," *Nature Reviews Physics*, vol. 5, no. 6, pp. 339–353, 2023.

[102] Scientific American, "China reaches new milestone in space-based quantum communications." [Online]. Available: https://www.scientificamerican.com/article/china-reaches-new-milestone-in-space-based-quantum-communications/. [Accessed: Jan. 07, 2025].

[103] B. C. da Rocha, L. P. de Melo, and R. T. de Sousa Jr, "A study on APT in IoT networks," in *ICE-B*, Dec. 2021, pp. 160–164.

[104] E. Zouave, M. Bruce, K. Colde, M. Jaitner, I. Rodhe, and T. Gustafsson, *Artificially intelligent cyberattacks*, Stockholm: Totalförsvarets forskningsinstitut FOI, 2020. [Online]. Available: https://whttps://www.statsvet.uu.se/digitalAssets/769/c_769530-l_3-k_rapport-foi-vt20.pdf. [Accessed: Sep. 28, 2022].

[105] C. Easttom, "Quantum computing and cryptography," in *Modern Cryptography: Applied Mathematics for Encryption and Information Security*, Cham: Springer International Publishing, 2022, pp. 397–407.

[106] L. Tawalbeh, F. Muheidat, M. Tawalbeh, and M. Quwaider, "IoT privacy and security: Challenges and solutions," *Applied Sciences*, 2020. doi:10.3390/app10124102.

[107] N. Chaabouni, M. Mosbah, A. Zemmari, C. Sauvignac, and P. Faruki, "Network intrusion detection for IoT security based on learning techniques," *IEEE Communications Surveys & Tutorials*, vol. 21, pp. 2671–2701, 2019. doi:10.1109/COMST.2019.2896380.

[108] S. K. Rajaram, S. Konkimalla, M. Sarisa, H. K. Gollangi, C. R. Madhavaram, and M. S. Reddy, "AI/ML-powered phishing detection: Building an impenetrable email security system," *ISAR Journal of Science and Technology*, vol. 1, no. 2, pp. 10–19, 2023.

[109] M. Kumar and P. Pattnaik, "Post quantum cryptography (PQC)-an overview," in *2020 IEEE High Performance Extreme Computing Conference (HPEC)*, Sep. 2020, pp. 1–9.

[110] R. Kuang, M. Perepechaenko, and M. Barbeau, "A new post-quantum multivariate polynomial public key encapsulation algorithm," *Quantum Information Processing*, vol. 21, no. 10, p. 360, 2022.

[111] Y. Liang, S. Samtani, B. Guo, and Z. Yu, "Behavioral biometrics for continuous authentication in the Internet-of-Things era: An artificial intelligence perspective," *IEEE Internet of Things Journal*, vol. 7, no. 9, pp. 9128–9143, 2020.