Πολιτικές Ασφάλειας και Ιδιωτικότητας στο Διαδίκτυο

Κυβερνοεπιθέσεις

Ελένη Χριστοπούλου
hristope@ionio.gr

Βασικές Έννοιες

Βασικές έννοιες

- Ασφάλεια Υπολογιστών (Computer Security)
- Ασφάλεια Πληροφοριών (Information Security)
- Κυβερνοασφάλεια (Cyber Security)
- Ασφάλεια ΤΠΕ (ITC Security)
- Ιδιωτικότητα (Privacy)

- Ποιο πληροφοριακό αγαθό ή πόρος ασφαλίζεται ή προστατεύεται και
- τι σκοπό εξυπηρετεί;

Ασφάλεια Υπολογιστών

- Μέτρα και έλεγχοι που που διασφαλίζουν
  - Εμπιστευτικότητα (**C**onfidentiality): εξασφαλίζει εξουσιοδοτημένη πρόσβαση και αποκάλυψη *(encryption)*
  - Ακεραιότητα (**I**ntegrity): εξασφαλίζει την κατάλληλη τροποποίηση ή καταστροφή *(hashing)*
  - Διαθεσιμότητα (**A**vailability): εξασφαλίζει έγκαιρη και αξιόπιστη πρόσβαση και χρήση

- Αγαθά στα συστήματα πληροφορικής που προστατεύει:
  - υπολογιστικές συσκευές (υλικό): εξυπηρετητές, υπολογιστές, φορητούς υπολογιστές, tablet, κινητά τηλέφωνα
  - συσκευές δικτύου: router, switch
  - λογισμικό: ενσωματωμένο λογισμικό, λειτουργικά συστήματα

Ασφάλεια Πληροφοριών (Δεδομένων)

"Preservation of confidentiality, integrity and availability (CIA) of Information.

In addition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved."

International Standards Organization (ISO) (2014)

- Τα δεδομένα σε οποιαδήποτε μορφή διατηρούνται ασφαλή από πλευρά εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητάς τους
- Ιδιότητες όπως η αυθεντικότητα, η μη-αποποίηση ευθύνης και η αξιοπιστία μπορεί να εμπλέκονται

Κυβερνοχώρος

"Cyberspace is a time-dependent set of interconnected information systems and the humans that interact with these systems".

Ottis and Lorents (2010)

It is a dynamic, evolving, virtual, connected, multilevel ecosystem of physical infrastructure, software, regulations, processes, and interactions influenced by an expanding population of contributors who represent the range of human intentions.

- Ο κυβερνοχώρος είναι ένα χρονικά εξαρτώμενο σύνολο διασυνδεδεμένων συστημάτων πληροφοριών και των ανθρώπων που αλληλεπιδρούν με αυτά τα συστήματα
- Είναι ένα δυναμικό, εξελισσόμενο, εικονικό, συνδεδεμένο, πολυεπίπεδο οικοσύστημα φυσικής υποδομής, λογισμικού, κανονισμών, διαδικασιών και αλληλεπιδράσεων που επηρεάζονται από τον αυξανόμενο αριθμό των συνεισφερόντων που αντιπροσωπεύουν το φάσμα των ανθρώπινων προθέσεων

Κυβερνοχώρος
3 επίπεδα λειτουργίας

- Φυσικό (physical layer)
  - το υλικό: τα μηχανικά (π.χ «κουτιά» Η/Υ, εκτυπωτές, scanners), ηλεκτρικά (π.χ καλώδια) και ηλεκτρονικά (π.χ chips, ολοκληρωμένα κυκλώματα) μέρη των δικτύων των Η/Υ
- Συντακτικό (syntactic layer)
  - οι οδηγίες του κατασκευαστή και του χρήστη που δίνονται στις πληροφοριακές συσκευές, αλλά και τα πρωτόκολλα μέσω των οποίων αλληλεπιδρούν οι συσκευές
- Σημασιολογικό (semantic layer)
  - περιλαμβάνει όλες τις πληροφορίες που περιέχει ο Η/Υ
  - τροφοδότηση του συστήματος με λανθασμένες πληροφορίες

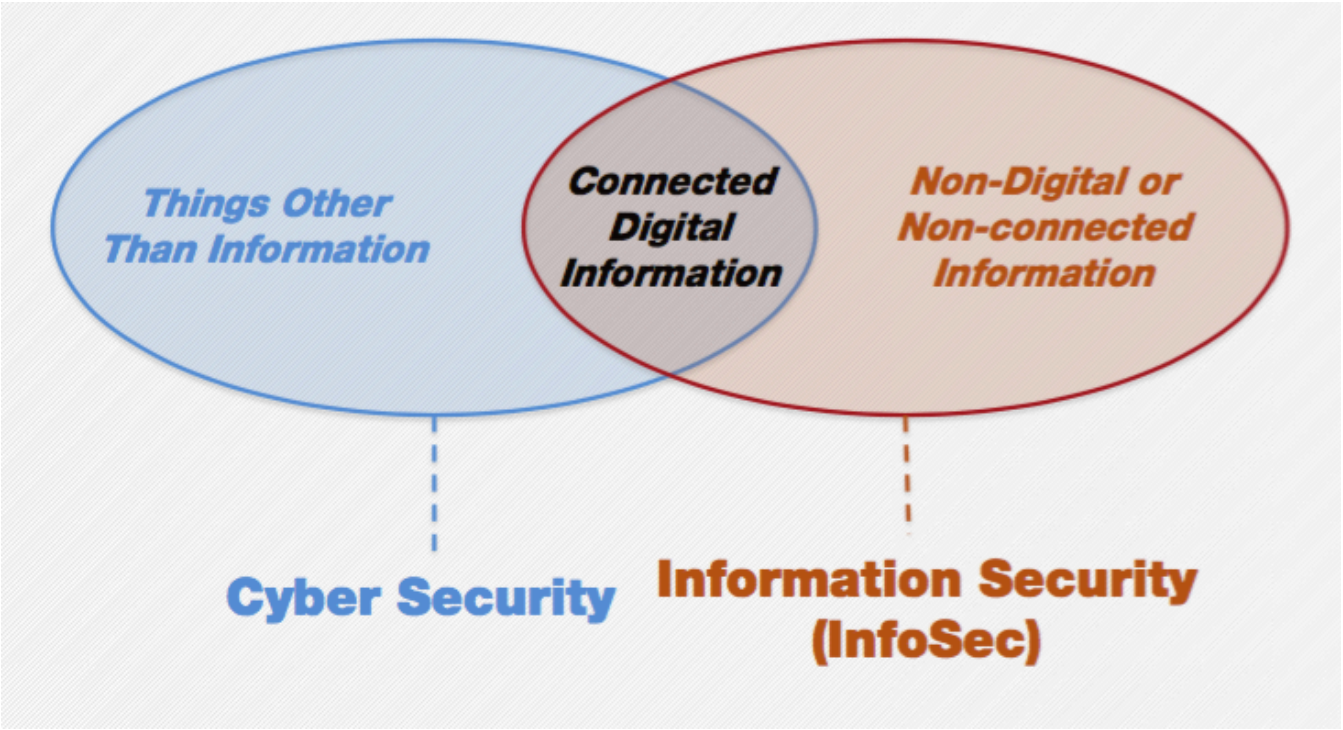
Libicki, Martin C., Cyberdeterrence and Cyberwar (RAND Corporation, Santa Monica, CA, 2009)

Αγαθά στο κυβερνοχώρο

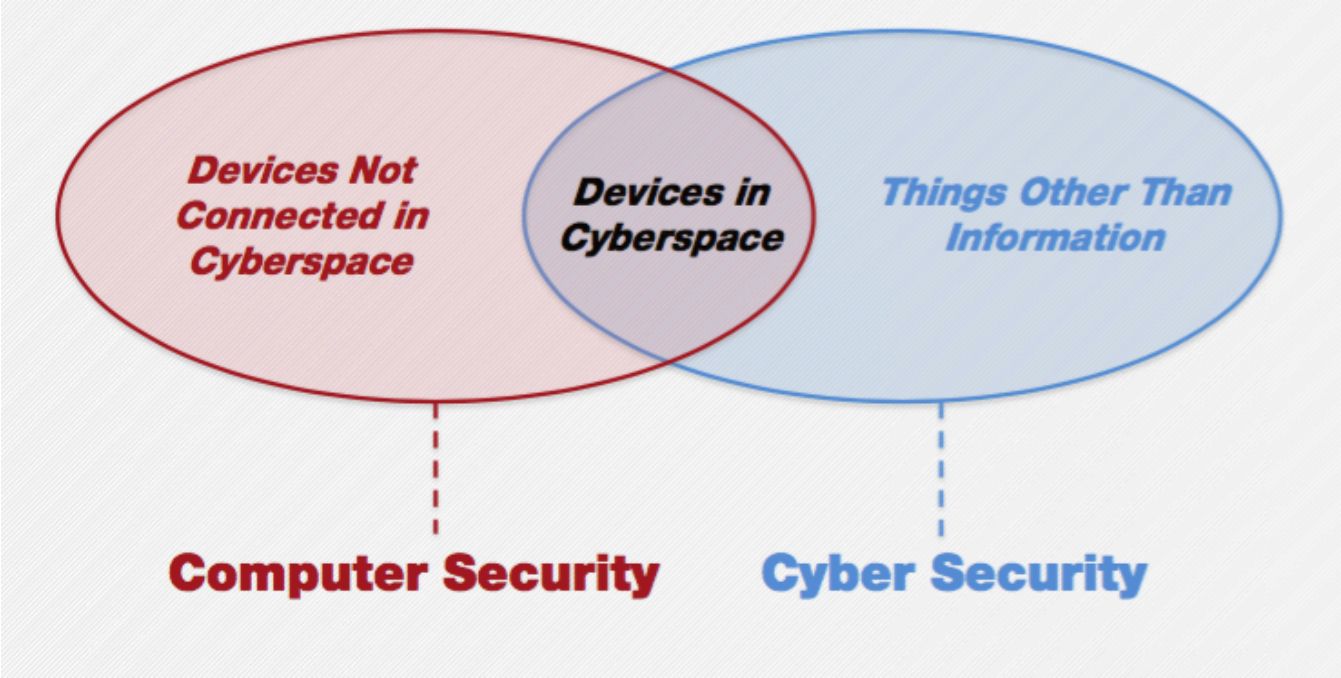
- Η ίδια η πληροφορία
- Υποδομές πληροφορικής
  - *Internet, embedded software, firmware, communication protocols*
- Μη πληροφοριακά αγαθά (φυσικές οντότητες που συνδέονται στο internet)
  - κρίσιμες υποδομές
    - *δίκτυο ενέργειας, παροχή νερού, δημόσια υγεία, μεταφορές, τηλεπικοινωνίες, οικονομικές υπηρεσίες, κ.α.*
  - Internet of Things
    - *Connected and self-driving vehicles*
    - *Connected medical devices*
    - *Connected home automation and entertainment systems*

Κυβερνοασφάλεια
Μοντέλο ΑΑΑ

- Authentication (Αυθεντικότητα): *αποδεικνύω ποιος είμαι*
  - Κάτι που γνωρίζω: κωδικό
  - Κάτι που έχω: κλειδί
  - Κάτι που είμαι: βιομετρικά
- Authorization (Εξουσιοδότηση): *δικαιώματα πρόσβασης*
- Accounting (Λογοδοσία): *γνωρίζω ποιος έκανε τι*



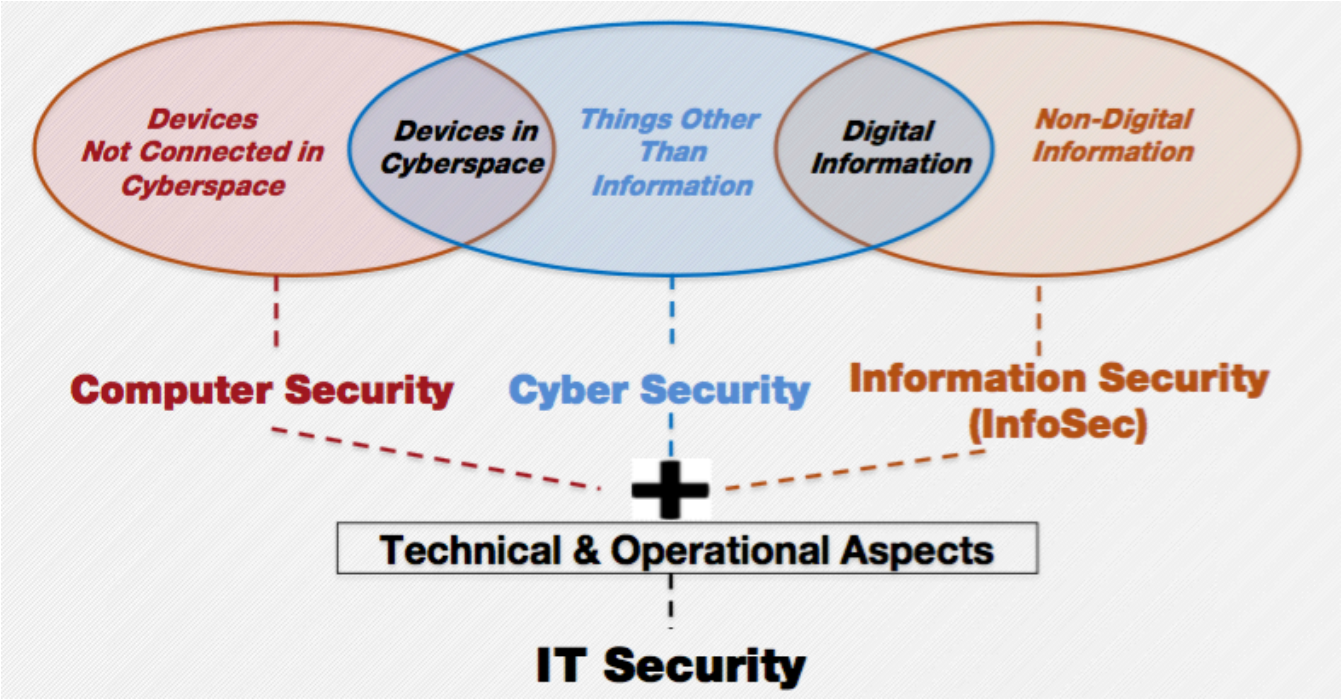
Cyber Security VS Information Security



Computer Security VS Cyber Security

Stuxnet malware

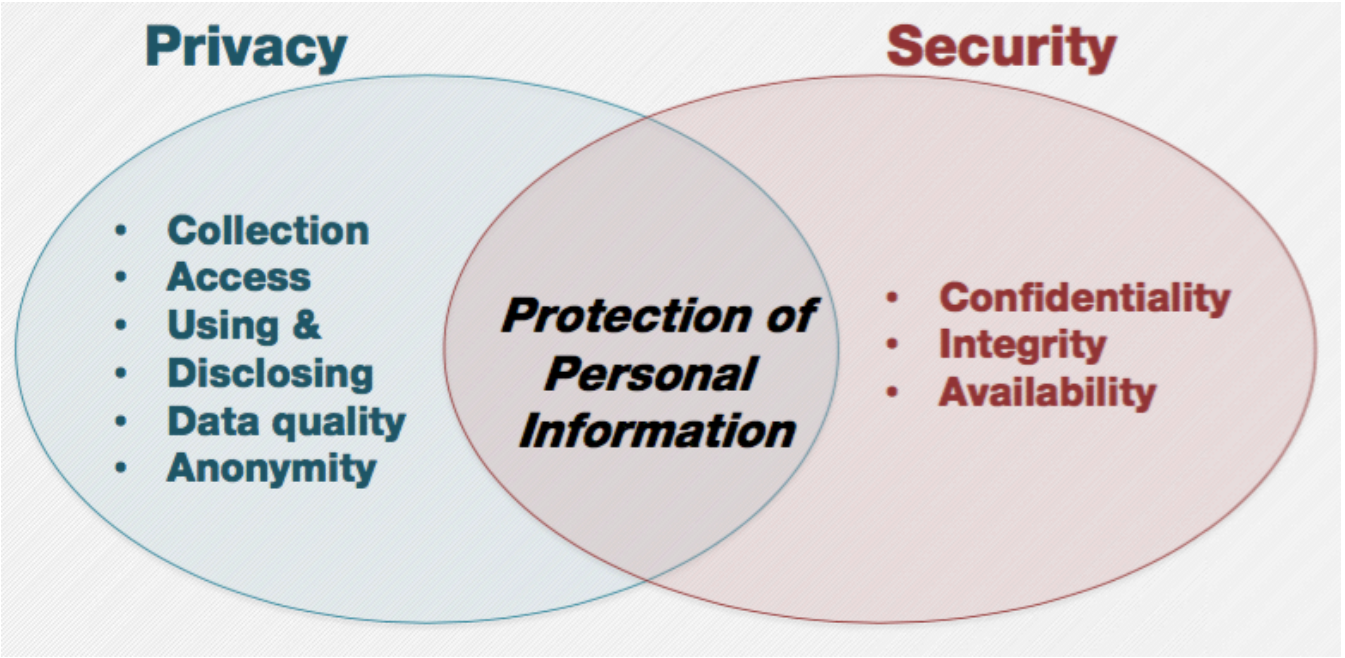
Στο εσωτερικό δίκτυο πυρηνικής εγκατάστασης στο Ιράν μέσω «μολυσμένου» USB


Devices Not Connected in Cyberspace
Devices in Cyberspace
Things Other Than Information
Digital Information
Non-Digital Information
Computer Security
Cyber Security
Information Security (InfoSec)
Technical & Operational Aspects
IT Security

IT Security VS Information Security

- **IT Security**
  - Firewalls
  - Antivirus
  - Vulnerability Scans
  - Penetration Testing
  - Intrusion Detection
  - Computer Forensics
  - Access Control
  - Network Security
  - System Monitoring
  - Patch Management
  - Encryption
- Technology-oriented

- **Information Security (InfoSec)**
  - Intellectual property
  - Regulatory compliance
  - Business/financial integrity
  - Insider abuse
  - Industrial espionage
  - Data Privacy
  - Governance
  - Crisis Management
  - Business Continuity
  - Risk analysis
  - Organizational view
- Business-oriented



Ιδιωτικότητα και Ασφάλεια

Προστασία προσωπικών πληροφοριών
Προστασία δημόσιων πληροφοριών

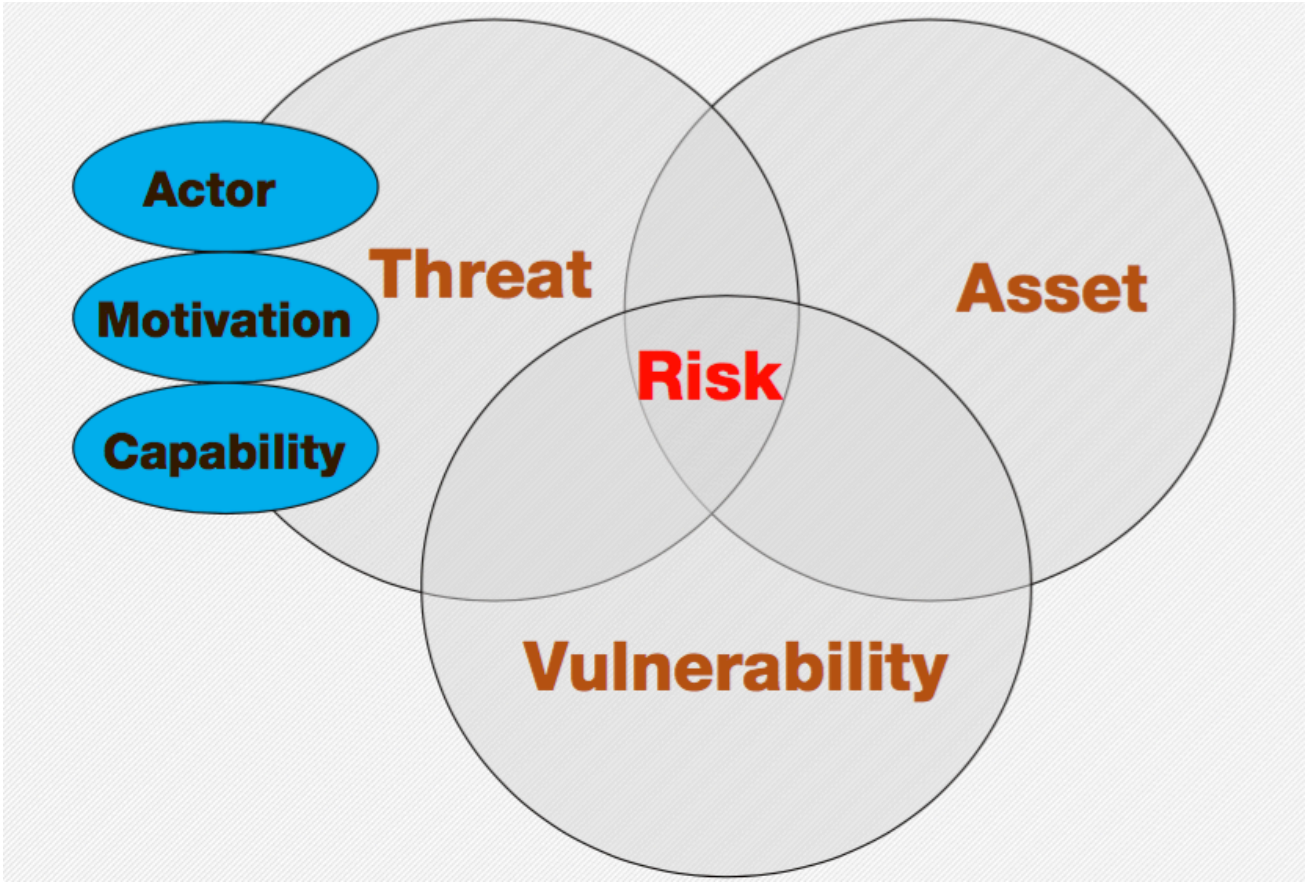
"87% of the US population are uniquely identified by {DateOfBirth, gender, zip code}"

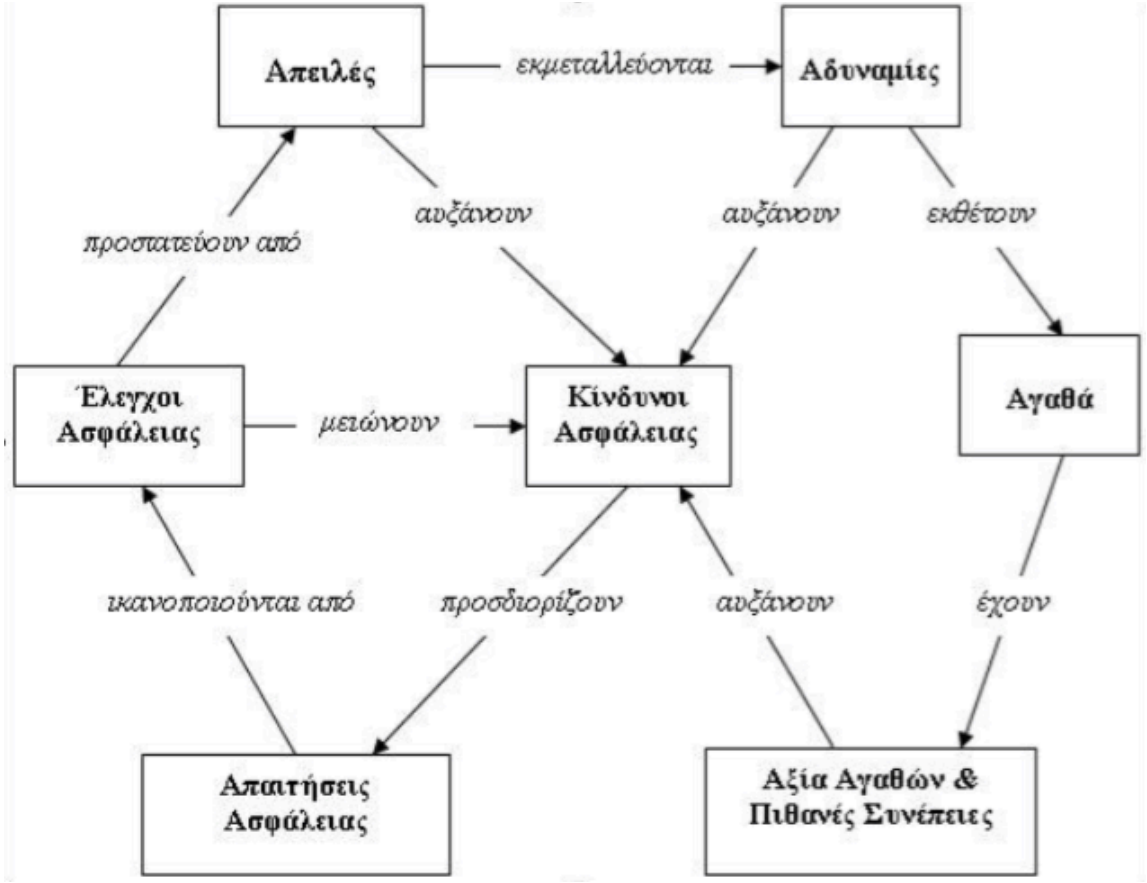
Βασικές έννοιες

- Πληροφοριακός πόρος ή Αγαθό (Asset)
  - οποιοδήποτε πολύτιμο πράγμα που αξίζει να προστατευθεί
- Συνέπεια ή Αξία Αγαθού (Impact/Value)
  - η απώλεια που θα προκληθεί από την προσβολή ενός αγαθού
- Αδυναμία (Vulnerability)
  - οποιοδήποτε χαρακτηριστικό κάνει ευάλωτο ένα αγαθό σε κάποια απειλή
- Απειλή (Threat)
  - οποιοδήποτε γεγονός που προκαλεί αρνητικές συνέπειες σε κάποιο αγαθό
- Επίθεση (Attack)
  - μία απειλή εκμεταλλεύεται μία ή περισσότερες αδυναμίες και εξαπολύει μία επίθεση

Βασικές έννοιες

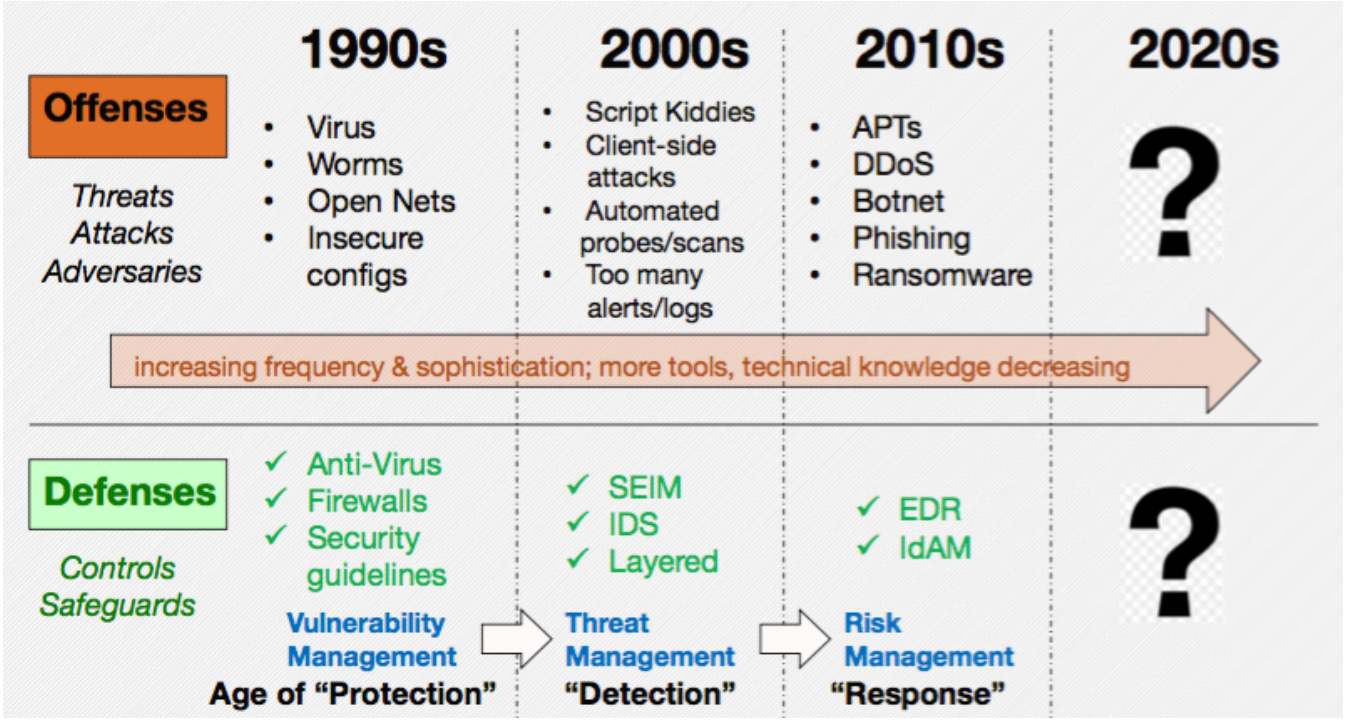
- Επίθεση / Απειλή
  - η δυνατότητα ενός “πράκτορα” με κάποιο κίνητρο να εκμεταλλευτεί μια συγκεκριμένη αδυναμία
    - “πράκτορας” *(agent/actor)*: πρόσωπο, οργάνωση, κυβέρνηση
    - κίνητρα: δημοσιότητα, οικονομική, πολιτική / θρησκεία
    - δυνατότητα: απαιτούμενη γνώση, διαθέσιμα εργαλεία
- Κίνδυνος (Risk): Αδυναμία που εκτίθεται σε μία Απειλή που προσβάλλει ένα Αγαθό
- Έλεγχοι Ασφάλειας
  - Μέτρα αντιμετώπισης για τη μείωση του Κινδύνου


Actor
Motivation
Capability
Threat
Asset
Risk
Vulnerability



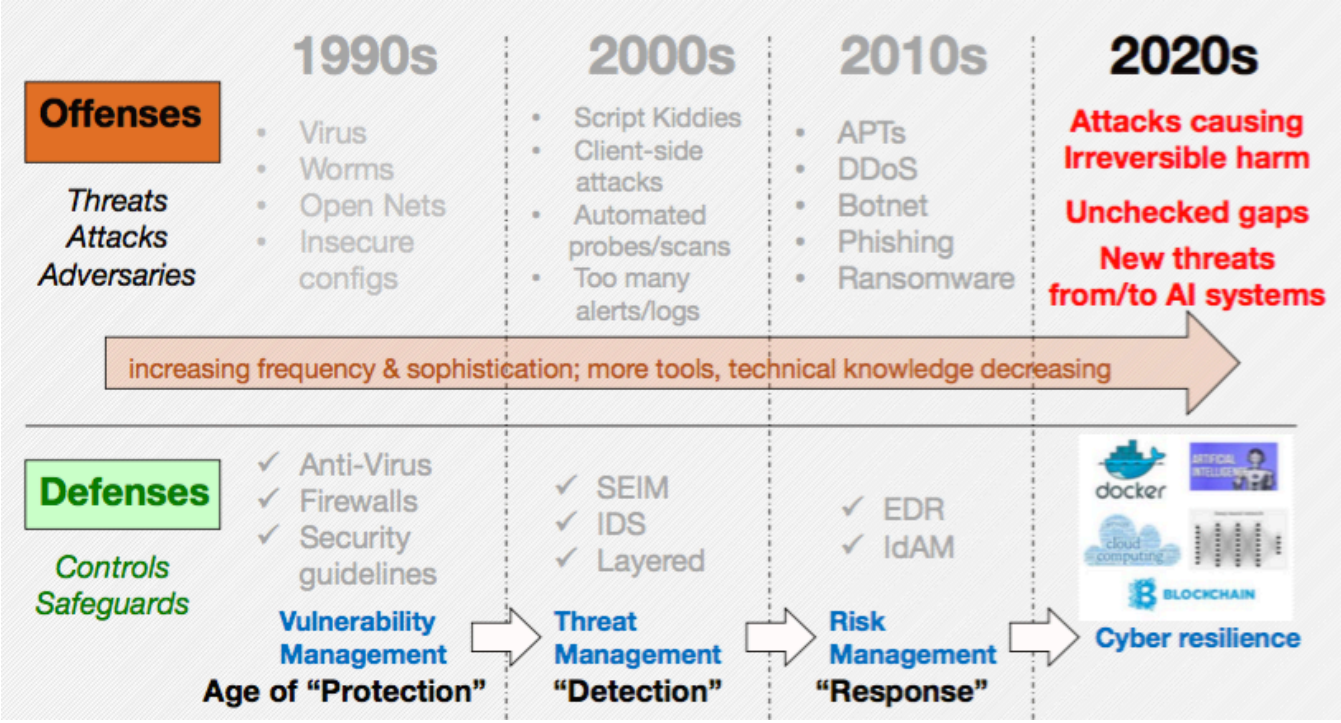
Σύνδεση όρων ανάλυσης και διαχείριση κινδύνου

Π. Κοτζανικολάου, «Τεχνολογία και Πολιτικές Ασφάλειας», Παν. Πειραιώς



Η εξέλιξη

- SIEM: Security Information and Event Management
  IDS: Intrusion Detection System
  EDR: Endpoint Detection and Response
  IdAM: Identity Access Management
  APT: Advanced Persistent Threat
  DDoS: Distributed Denial of Service



Resilience

η ικανότητα να γίνεται γρήγορα η αποκατάσταση από δυσκολίες

Cloud platform, AI, machine learning, deep learning, data-driven analytics, serverless architecture, immutable infrastructure

Μερικά παραδείγματα

2020s: Cyber Threats

- Distributed Denial of Service (DDoS)
- Data Breach
- Ransomware
- Integrity – Sabotaging data
- Social engineering

Δικές σας προτάσεις;

Distributed Denial of Service (DDoS)
Availability

- Dyn - Internet naming services
  - PayPal, Amazon, Twitter, CNN, Fox News, GitHub, Visa,
- Fake visitors flooded their servers
  - 100,000 DVRs, security cameras, webcams, thermostats, refrigerators, coffee makers, and other internet of things devices
  - hijacked devices through malware
  - instructed to attack Dyn's servers

Data Breaches
Confidentiality

- Sony
  - 25 million users
- MySpace
  - 427 million users
- Yahoo!
  - 500 million users
  - 1 billion users
- LinkedIn
  - 117 million users

Ransomware
Availability

- WannaCry in May 2017
  - healthcare data and paralyzed operations

Τύποι κυβερνοεπιθέσεων

Ποιοι είναι υπεύθυνοι για μία κυβερνοεπίθεση;

- Classic Hackers
- Mercenary Hackers (μισθοφόροι)
- Hactivists
- Rogue insiders (απατεώνες)
- Κράτη

Τύποι κυβερνοεπιθέσεων

- Device Compromise – Έκθεση Συσκευής
- Service Disruption – Διακοπή Υπηρεσίας
- Data Exfiltration – Ανάκτηση/Αντιγραφή Δεδομένων
- Bad Data Injection – Έγχυση Κακών Δεδομένων
- Advanced Persistent Threat (APT)

Device Compromise – Έκθεση συσκευής

- Σκοπός: να αποκτηθεί ο έλεγχος μίας συσκευής
- Απαιτήσεις
  - root credentials
  - privilege escalation exploit (περαιτέρω εκμετάλλευση προνομίων)
- Εξουσίας
  - arbitrary execution on compromised device
  - network foothold
  - ability to carry out other types of cyber attacks!

Service Disruption – Διακοπή Υπηρεσίας

- Σκοπός: να αποτραπεί μία συσκευή από την εκτέλεση των καθηκόντων της (υπηρεσίες)
- Απαιτήσεις
  - LOTS of computing power
- Εξουσία
  - Συνέπειες όταν μία συσκευή αποτυγχάνει να «κάνει» τη δουλειά της
    - Device downtime
    - Revenue loss
    - Public attention/shaming
    - System failure

Data Exfiltration – Αντιγραφή/ Ανάκτηση δεδομένων

- Σκοπός: κλοπή ευαίσθητων πληροφοριών από ένα στόχο
- Απαιτήσεις
  - Access (legit or otherwise) to device storing data
- Εξουσία
  - Arbitrary Data Operations!
  - Reconnaissance
  - IP Theft
  - Expose private information

Bad Data Injection – Έγχυση κακών δεδομένων

- Σκοπός: υποβολή εσφαλμένων δεδομένων σε ένα σύστημα χωρίς να ανιχνευθεί (γίνει αντιληπτό)
- Απαιτήσεις
  - • Access (legit or otherwise) to device storing data
- Εξουσία
  - Determine the state of datadriven services!
  - Real-world consequences, potentially catastrophic

Advanced Persistent Threat (APT)

- Σκοπός: απόκτηση εκτεταμένης πρόσβασης σε μία συσκευή
- Απαιτήσεις
  - Time, patience, resources
  - Extensive target knowledge
- εξουσία:
  - Long-term reconnaissance
  - Ability to act on target quickly
  - Complete and invisible control of systems!

Εργαλεία επιθέσεων

Virus – Ιός

- Μικρό πρόγραμμα το οποίο προσκολλά τον εαυτό του σε άλλα προγράμματα ή αρχεία και μεταδίδεται από η/υ σε η/υ, σε δίκτυα, συσκευές αποθήκευσης κ.λπ., φτιάχνοντας αντίγραφα του εαυτού του.

- Ένας ιός είναι συνήθως εφοδιασμένος και με ένα εκτελέσιμο κομμάτι λογισμικού (payload), το οποίο μπορεί να προγραμματιστεί έτσι ώστε να προκαλέσει κακόβουλα αποτελέσματα, όπως διαγραφές αρχείων, αλλοίωση δεδομένων, διαταραχή λειτουργιών κ.λπ.

- Σχεδόν όλοι οι ιοί προσαρτώνται σε εκτελέσιμα αρχεία, πράγμα που σημαίνει ότι ο ιός μπορεί να υπάρχει για ένα διάστημα σε κάποιον η/υ, χωρίς να είναι ανιχνεύσιμος, μέχρι τη στιγμή που το μολυσμένο εκτελέσιμο αρχείο θα εκτελεστεί.[

Worms – «σκουλήκια»

- Οι αναπαραγωγοί λειτουργούν με τρόπο που μοιάζει με αυτόν των ιών, επειδή μεταδίδονται από η/υ σε η/υ.
- Σε αντίθεση, όμως, με τους ιούς, τα ‘σκουλήκια’ λογισμικού έχουν την ικανότητα να ταξιδεύουν χωρίς (έστω και την ακούσια) βοήθεια προσώπων
  - αυτό επιτυγχάνεται επειδή αυτού του είδους το κακόβουλο λογισμικό εκμεταλλεύεται τα δεδομένα μεταφοράς και κινήσεως των αρχείων εντός του δικτύου.
- Ωστόσο, ο μεγαλύτερος κίνδυνος που παριστούν τα ‘σκουλήκια’ συνίσταται στο γεγονός ότι έχουν την ιδιότητα και την ικανότητα να αναπαράγουν τον εαυτό τους εντός του συστήματος, έτσι ένας μολυσμένος η/υ μπορεί να διαβιβάζει σε άλλους (και κατ’ επέκταση σε ολόκληρα δίκτυα ή συστήματα) εκατοντάδες ή και χιλιάδες αντίγραφα ενός ηλεκτρονικού ‘σκουληκιού’.
- Το τελικό αποτέλεσμα στις περισσότερες περιπτώσεις είναι ότι τα ηλεκτρονικά ‘σκουλήκια’ καταναλώνουν μεγάλα ποσοστά της διαθέσιμης μνήμης ή ακόμη και του εύρους (bandwidth) των γραμμών επικοινωνιών των δικτύων, με συνέπεια μεμονωμένοι υπολογιστές, εξυπηρετητές ιστοσελίδων (web servers) ή και εξυπηρετητές δικτύων (network servers), απλά να μην μπορούν να εκτελέσουν ούτε ένα ποσοστό της φυσιολογικής λειτουργίας τους

Trojan horses - Δούρειοι ίπποι

- Δούρειοι ίπποι είναι φαινομενικά χρήσιμα προγράμματα που περιλαμβάνουν κρυφές λειτουργίες, οι οποίες μπορούν να εκμεταλλευτούν τα δικαιώματα του χρήστη που εκτελεί το πρόγραμμα, με συνέπεια μια απειλή στην ασφάλεια του συστήματος.
- Δεν αναπαράγονται μόνοι τους. Βασίζονται (ξεγελούν) (σ)τους χρήστες για την εγκατάσταση και την εκτέλεσή τους.
- Ο δούρειος ίππος είναι ένα μη βλαβερό πρόγραμμα, το οποίο, ωστόσο, περιέχει κατά τρόπο μη εμφανή κακόβουλο ή επιβλαβή κώδικα λογισμικού και μπορεί να προκαλέσει ζημία ή να εκτελέσει οποιαδήποτε άλλη (κακόβουλη) εργασία για την οποία είναι προορισμένος.
- Οι χρήστες η/υ που λαμβάνουν έναν δούρειο ίππο, παρασύρονται διότι χρησιμοποιούν ένα φαινομενικά αβλαβές πρόγραμμα ή ανοίγουν αρχεία από φαινομενικά 'νόμιμη' και γνωστή πηγή προέλευσης.
- Οι δούρειοι ίπποι μπορούν να προκαλέσουν σοβαρά προβλήματα διαγράφοντας αρχεία ή καταστρέφοντας πληροφορίες· μπορούν επίσης να δημιουργήσουν ηλεκτρονικές 'κερκόπορτες' στο σύστημα.

Spyware - Κατασκοπευτικό λογισμικό

- Έχει σκοπό την παρακολούθηση - υποκλοπή ευαίσθητων δεδομένων.
- Εγκαθίσταται κρυφά ξεγελώντας το χρήστη σε ένα Υ.Σ. και εκτελείται στο παρασκήνιο.
- Τυπικά, συγκεντρώνει πληροφορίες σχετικά με το χρήστη, π.χ., sites που επισκέπτεται, κωδικούς πρόσβασης, κ.ά.
- Συνήθως μεταδίδεται με την εγκατάσταση προγραμμάτων (freeware, shareware), με την εγκατάσταση πρόσθετων (browser add-ons), με την επίσκεψη σε δικτυακούς τόπους.
- Ως spyware κατηγοριοποιούνται τα adware, tracking cookies, system monitors.

Rootkits

- Λογισμικό που μπορεί να ανήκει σε μία από τις προηγούμενες κατηγορίες
- Έχει την ιδιαιτερότητα ότι κρύβει κάποια κακόβουλα προγράμματα ώστε να μην γίνονται ορατά από το λογισμικό ασφάλειας
  - Κρύβει την παρουσία τόσο δεδομένων όσο και προγραμμάτων
- Μπορεί να λειτουργήσει προστατευτικά για τους χάκερ διαγράφοντας τις πληροφορίες του εισβολέα
- Απαιτεί root privileges στο μηχάνημα

Bot - Διαδικτυακό ρομπότ 1/2

- Παράγεται από τη λέξη robot και αποτελεί λογισμικό που εκτελεί μια αυτοματοποιημένη διαδικασία που αλληλοεπιδρά με άλλες υπηρεσίες του δικτύου.
- Συχνά, ένα bot αυτοματοποιεί διαδικασίες (tasks) και παρέχει πληροφορίες σε υπηρεσίες που διαφορετικά θα έπρεπε να προσφέρονται από ανθρώπους.
  - Για παράδειγμα, υπηρεσίες συγκέντρωσης πληροφοριών (web crawlers).
- Ένα bot μπορεί να χρησιμοποιηθεί καλόβουλα ή κακόβουλα.

Bot - Διαδικτυακό ρομπότ 2/2

- Κακόβουλο bot
- Έχει σχεδιαστεί για να προσβάλει ένα Υ.Σ. και να συνδέεται πίσω σε έναν κεντρικό (ή κεντρικούς) servers.
- Αυτοί λειτουργούν ως κέντρο ελέγχου και μεταβίβασης εντολών (Command and Control (C&C)) για ολόκληρο το δίκτυο των προσβεβλημένων συσκευών που αποκαλείται botnet.
- Μια μηχανή που έχει μολυνθεί από ένα bot συχνά αναφέρεται ως zombie.
- Έχοντας ένα botnet, ο επιτιθέμενος μπορεί να εξαπολύσει μια πλειάδα επιθέσεων που περιλαμβάνουν DoS και διάδοση ανεπιθύμητων μηνυμάτων (spam).
- Συνήθως ένα bot έχει την ικανότητα να καταγράφει το πληκτρολόγιο (log keystrokes), να συλλέγει συνθηματικά, να συλλέγει καν να αναλύει IP πακέτα, να εγκαθιστά backdoors, κ.ά.
- Γενικά ένα bot έχει όλα τα πλεονεκτήματα ενός σκουληκιού, αλλά είναι εξυπνότερο όσον αφορά τη φάση προσβολής του στόχου και ο κώδικάς του τροποποιείται συχνότερα.
- Επίσης,γίνεται δυσκολότερα αντιληπτό.

Logic bombs – Λογικές βόμβες

- Προγράμματα που εκτελούν μια ενέργεια,η οποία παραβιάζει την πολιτική ασφαλείας ενός συστήματος όταν πληρείται κάποια λογική συνθήκη στο σύστημα
  - (π.χ., όταν το όνομα του προγραμματιστή δε βρίσκεται στη μισθοδοσία της επιχείρησης).
- Πρόκειται για κώδικα κακόβουλου λογισμικού, σχεδιασμένο να τίθεται σε εφαρμογή (να εκτελείται αυτοματοποιημένα) όταν πληρωθούν ορισμένες προϋποθέσεις, ή όταν συντρέξουν ορισμένα κριτήρια, ή, τέλος, σε μία δεδομένη χρονική στιγμή στο μέλλον.
- Μόλις συμβεί αυτό, ο κακόβουλος κώδικας μπορεί να διακόψει ή να καταστήσει δυσχερή τη λειτουργία ενός η/υ ή δικτύου, να διαγράψει δεδομένα, ή ακόμη και να ξεκινήσει μία επίθεση τύπου DoS /DDoS.
- Χρονικές βόμβες

Social Engineering – Κοινωνική μηχανική

- Η επιστήμη της χρήσης της κοινωνικής αλληλεπίδρασης ως μέσο πειθούς ενός ατόμου ή οργανισμού, προκειμένου αυτό να συναινέσει σε ένα συγκεκριμένο αίτημα ενός επιτιθέμενου, όπου είτε η κοινωνική αλληλεπίδραση, είτε η μέθοδος πειθούς, είτε το αίτημα εμπλέκει κάποια μονάδα σχετιζόμενη με κάποιον υπολογιστή.

- Το SE εφαρμόζεται για να εξυπηρετήσει δύο διακριτές σκοπιμότητες
  - προπαγάνδα
    - μέσα κοινωνικής δικτύωσης
  - απάτη
    - συλλογή εμπιστευτικών δεδομένων γύρω από κάποιο πρόσωπο

Phishing

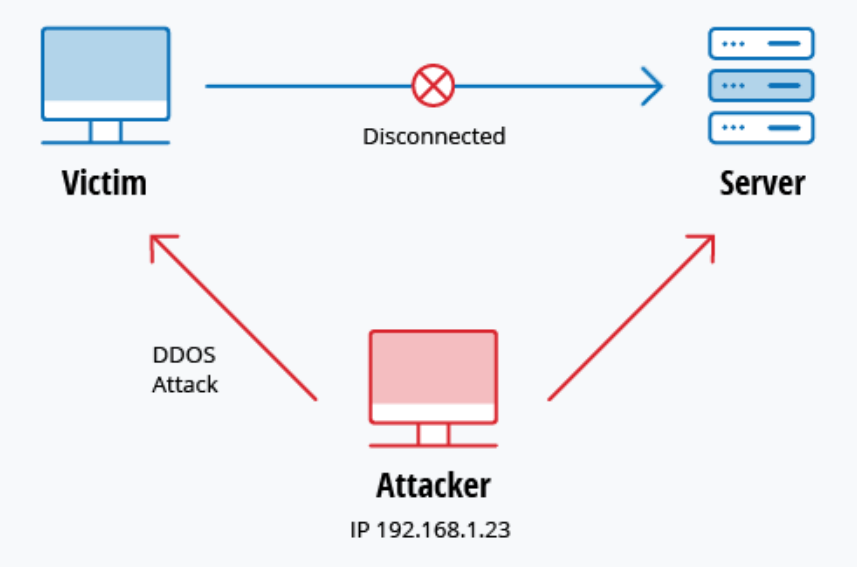
- Η πιο συχνή μορφή επίθεσης κοινωνικής μηχανής.
- Οι επιτιθέμενοι χρησιμοποιούν mails, τα social media απευθείας μηνύματα και SMS.
  - επισυναπτόμενα σε email
  - links σε «μη νόμιμα» site
- Στόχος είναι να εξαπατηθούν τα θύματα και να εξαχθούν από αυτά ευαίσθητες πληροφορίες ή να εγκατασταθεί κακόβουλο λογισμικό στον υπολογιστή τους.

Denial of Service – Dos / DDos

- Μια επίθεση άρνησης εξυπηρέτησης «συντρίβει» τους πόρους ενός συστήματος ώστε να μην μπορεί να ανταποκριθεί σε αιτήματα υπηρεσιών.
- Μια επίθεση DDoS είναι επίσης επίθεση κατά των πόρων του συστήματος, αλλά εκκινείται από μεγάλο αριθμό άλλων μηχανών υποδοχής που έχουν προσβληθεί από κακόβουλο λογισμικό που ελέγχεται από τον εισβολέα.
- Σε αντίθεση με τις επιθέσεις που έχουν σχεδιαστεί για να επιτρέπουν στον εισβολέα να αποκτήσει ή να αυξήσει την πρόσβαση, η άρνηση παροχής υπηρεσιών δεν παρέχει άμεσα οφέλη για τους επιτιθέμενους.
  - Για μερικούς από αυτούς, αρκεί να υπάρχει ικανοποίηση για άρνηση υπηρεσίας. Ωστόσο, αν ο επιτιθέμενος πόρος ανήκει σε επιχειρηματικό ανταγωνιστή, τότε το όφελος για τον εισβολέα μπορεί να είναι αρκετά πραγματικό.
- Ένας άλλος σκοπός μιας επίθεσης DoS μπορεί να είναι να καταστήσουμε ένα σύνδεση χωρίς σύνδεση (offline), ώστε να ξεκινήσει ένα διαφορετικό είδος επίθεσης.

Man in the Middle (MitM) 1/2

- Μια επίθεση MitM συμβαίνει όταν ένας hacker εισέρχεται μεταξύ των επικοινωνιών ενός πελάτη και ενός διακομιστή.
  - Session hijacking
    - Ένας εισβολέας απειλεί μια σύνοδο μεταξύ ενός αξιόπιστου πελάτη και του διακομιστή δικτύου. Ο επιτιθέμενος υπολογιστής αντικαθιστά τη διεύθυνση IP του για τον αξιόπιστο πελάτη, ενώ ο διακομιστής συνεχίζει τη συνεδρία, πιστεύοντας ότι επικοινωνεί με τον πελάτη.



Man in the Middle (MitM) 2/2

- Μη ασφαλή δημόσια Wi-Fi
- Κακόβουλο λογισμικό έχει παραβιάσει (breach) μία συσκευή → επιτιθεμένος εγκαθιστά λογισμικό που επεξεργάζεται όλες τις πληροφορίες του θύματος

Drive-by attack

- Drive-by downloads είναι μια κοινή μέθοδος διάδοσης κακόβουλου λογισμικού.
- Οι χάκερ αναζητούν ανασφαλείς ιστότοπους και δημιουργούν ένα κακόβουλο σενάριο στον κώδικα HTTP ή PHP σε μία από τις σελίδες. Αυτό το σενάριο ενδέχεται να εγκαταστήσει κακόβουλο λογισμικό απευθείας στον υπολογιστή κάποιου που επισκέπτεται τον ιστότοπο ή ενδέχεται να επαναπροσανατολίσει το θύμα σε έναν ιστότοπο που ελέγχεται από τους hackers.
- Drive-by downloads μπορεί να συμβούν όταν επισκέπτεστε έναν ιστότοπο ή προβάλλετε ένα μήνυμα ηλεκτρονικού ταχυδρομείου ή ένα αναδυόμενο παράθυρο. Σε αντίθεση με πολλούς άλλους τύπους επιθέσεων ασφάλειας στον κυβερνοχώρο, ένα drive-by δεν βασίζεται σε έναν χρήστη για να κάνει τίποτα για να ενεργοποιήσει ενεργά την επίθεση
  - δεν χρειάζεται να κάνετε κλικ σε ένα κουμπί λήψης ή να ανοίξετε ένα κακόβουλο συνημμένο ηλεκτρονικού ταχυδρομείου για να μολυνθείτε.
- Drive-by download μπορεί να επωφεληθεί από μια εφαρμογή, λειτουργικό σύστημα ή πρόγραμμα περιήγησης στο Web που περιέχει ελαττώματα ασφαλείας λόγω ανεπιτυχών ενημερώσεων ή έλλειψης ενημερώσεων.
- Προστασία:
  - ενημερωμένα προγράμματα περιήγησης και λειτουργικά συστήματα
  - Αποφυγή ιστοτόπων που ενδέχεται να περιέχουν κακόβουλο κώδικα.

Password attack

- Η απόκτηση κωδικών πρόσβασης είναι μια κοινή και αποτελεσματική προσέγγιση επίθεσης.
- Η πρόσβαση στον κωδικό πρόσβασης ενός ατόμου μπορεί να επιτευχθεί
  - κοιτάζοντας γύρω από το γραφείο του ατόμου
  - 'sniffing' τη σύνδεση στο δίκτυο για να αποκτήσετε μη κρυπτογραφημένους κωδικούς πρόσβασης
  - χρησιμοποιώντας την κοινωνική μηχανική
  - αποκτώντας πρόσβαση σε μια βάση δεδομένων κωδικών πρόσβασης ή τελικά μαντεύοντας. Η τελευταία προσέγγιση μπορεί να γίνει είτε τυχαία είτε συστηματικά:
    - Brute-force password guessing
    - Dictionary attacks

SQL injection attack

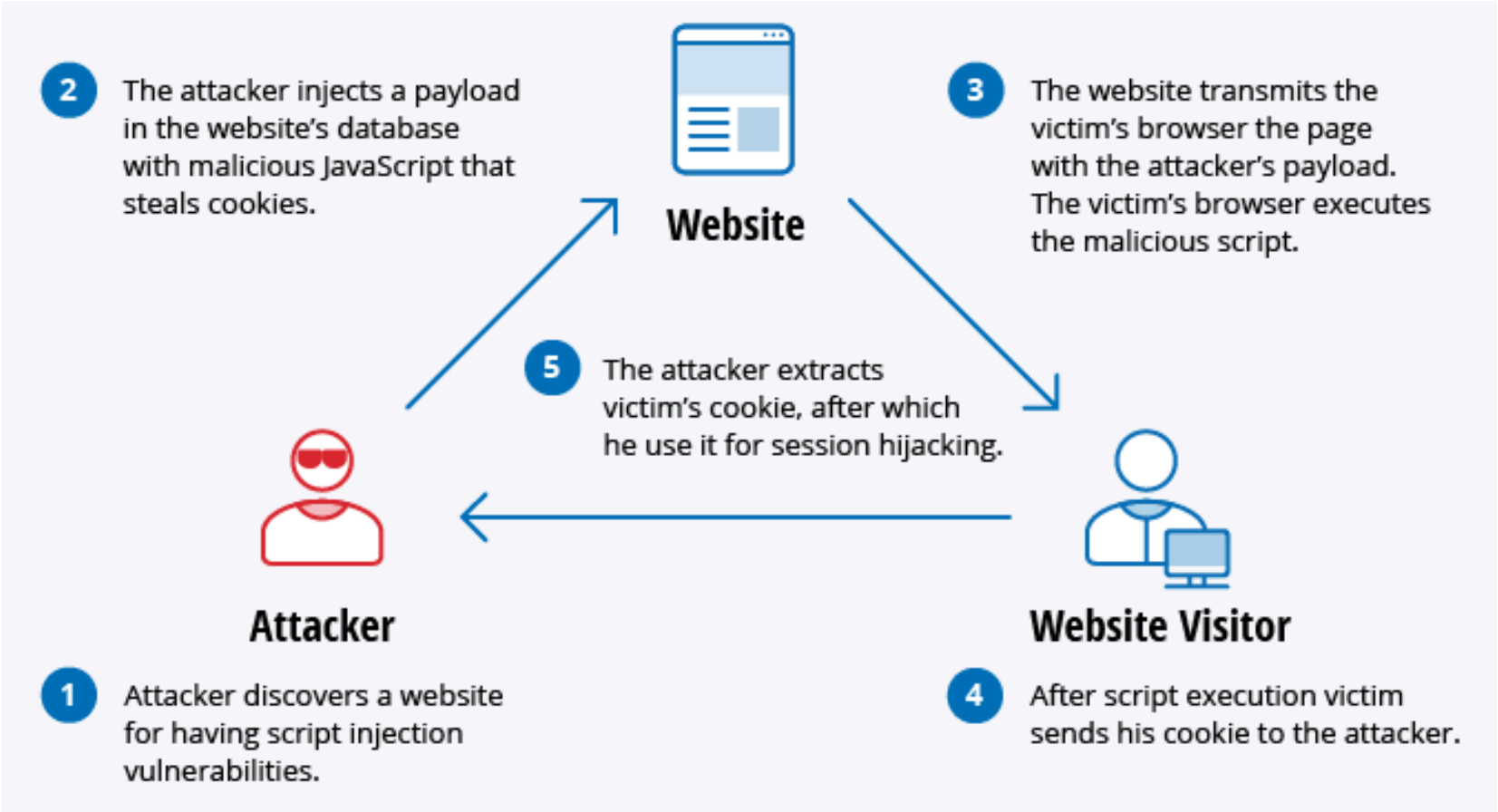
- SQL – Structured Query Language
  - Γλώσσα διαχείρισης δεδομένων στις Βάσεις Δεδομένων
- Η είσοδος που παρέχεται από τον χρήστη (π.χ. μέσω μίας φόρμας σε μία ιστοσελίδα) έχει σκοπό τη δημιουργία και εκτέλεση ενός SQL ερωτήματος με σκοπό την ανάκτηση πληροφοριών από μία βάση δεδομένων
  - "SELECT * FROM users WHERE account = '" + userProvidedAccountNumber +"';"
  - "SELECT * FROM users WHERE account = '' or '1' = '1';"
- Μια επιτυχημένη εκμετάλλευση SQL injection μπορεί να διαβάσει ευαίσθητα δεδομένα από τη βάση δεδομένων, να τροποποιήσει (να εισαγάγει, να ενημερώσει ή να διαγράψει) δεδομένα βάσης δεδομένων, να εκτελέσει λειτουργίες διαχείρισης (όπως shutdown) στη βάση δεδομένων, να ανακτήσει το περιεχόμενο ενός συγκεκριμένου αρχείου και, εκδίδει εντολές στο λειτουργικό σύστημα.

Cross-site scripting (XSS) attack

- Οι επιθέσεις XSS χρησιμοποιούν πόρους ιστότοπους για την εκτέλεση σεναρίων στο πρόγραμμα περιήγησης ιστού του θύματος.
  - Ο εισβολέας εισάγει ένα λογισμικό (payload) με κακόβουλο JavaScript στη βάση δεδομένων ενός ιστότοπου. Όταν ο θύμα ζητήσει μια σελίδα από τον ιστότοπο, ο ιστότοπος μεταδίδει τη σελίδα, με το payload του εισβολέα ως μέρος του σώματος HTML, στον browser του θύματος, ο οποίος εκτελεί το κακόβουλο σενάριο.

- Οι πιο επικίνδυνες συνέπειες συμβαίνουν όταν το XSS χρησιμοποιείται για την εκμετάλλευση πρόσθετων ευπαθειών. Αυτά τα τρωτά σημεία μπορούν να επιτρέψουν σε έναν εισβολέα όχι μόνο να κλέψει τα cookies, αλλά και να καταγράψει τα πλήκτρα, να καταγράψει στιγμιότυπα οθόνης, να ανακαλύψει και να συλλέξει πληροφορίες δικτύου και να αποκτήσει πρόσβαση και να ελέγξει από απόσταση την μηχανή του θύματος.

Cross-site scripting (XSS) attack



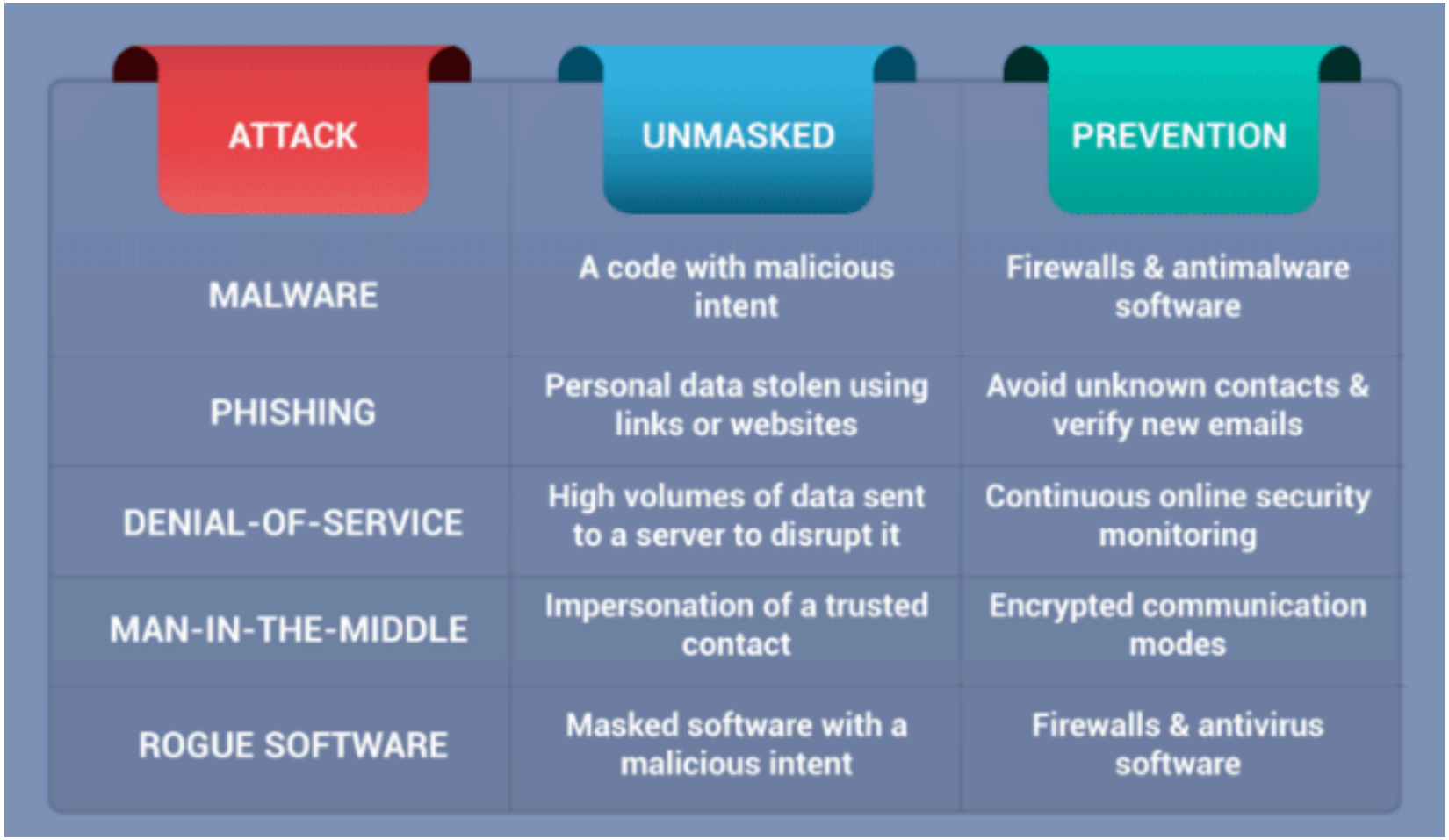
Malware attack

- Virus / Worms / Trojans / Logic bombs
- Ransomware
  - Τύπος κακόβουλου λογισμικού που αποκλείει την πρόσβαση στα δεδομένα του θύματος και απειλεί να το δημοσιεύσει ή να το διαγράψει εκτός και αν πληρωθεί λύτρα.
  - Ενώ μερικά απλά ransomware ηλεκτρονικών υπολογιστών μπορούν να κλειδώσουν το σύστημα με τρόπο που δεν είναι δύσκολο για ένα έμπειρο άτομο να αντιστραφεί, το πιο προηγμένο κακόβουλο λογισμικό χρησιμοποιεί μια τεχνική που ονομάζεται cryptoviral extortion, η οποία κρυπτογραφεί τα αρχεία του θύματος με τρόπο που τους καθιστά σχεδόν αδύνατο να ανακάμψουν χωρίς κλειδί αποκρυπτογράφησης.

Zero-day exploit

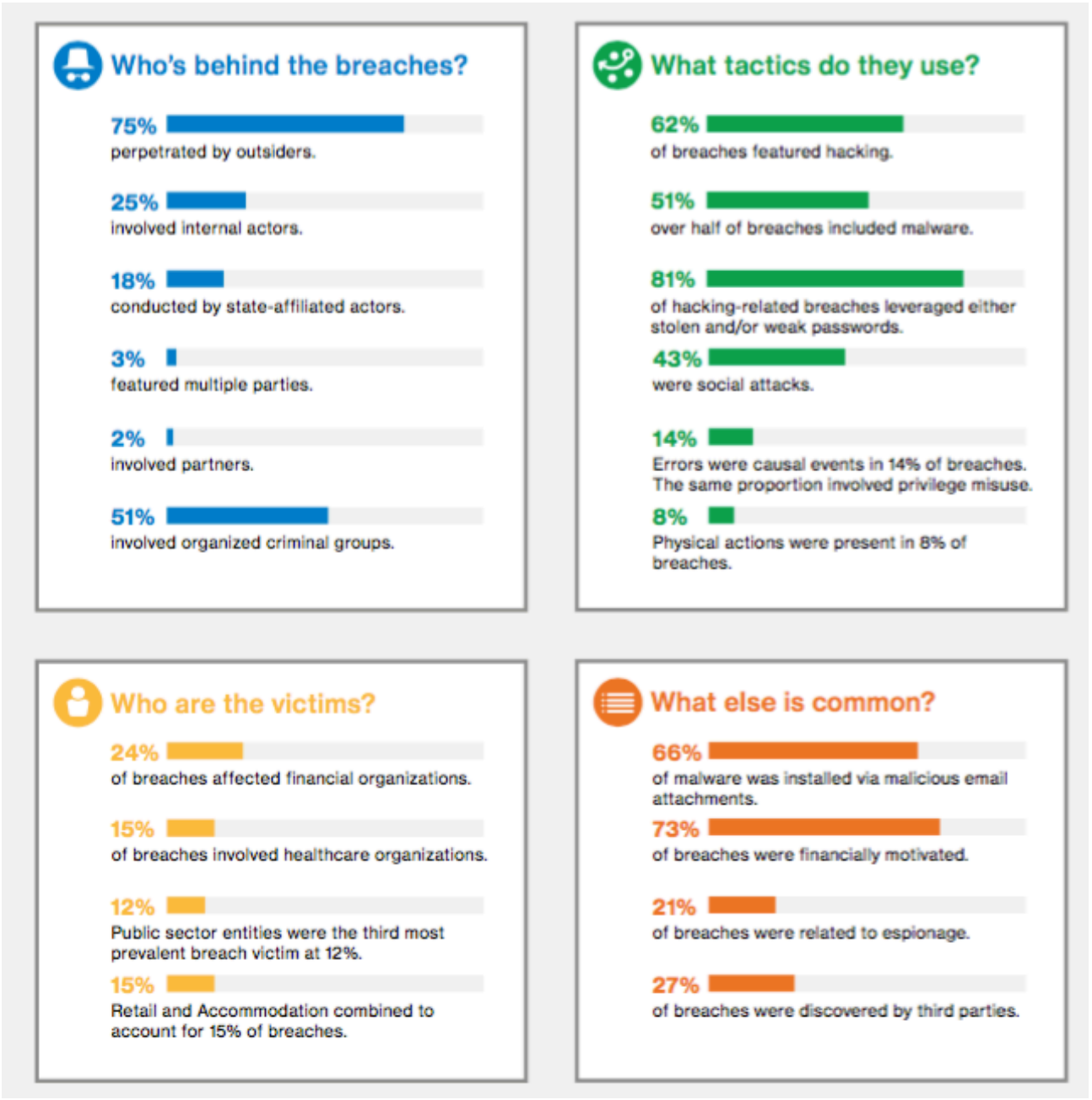
- Μία zero-day exploit επιτυγχάνεται μετά την ανακοίνωση μιας ευπάθειας ενός συστήματος/λειτουργικού/λογισμικού/δικτύου αλλά πριν από την εφαρμογή μιας ενημερωμένης έκδοσης κώδικα ή μιας λύσης.
- Οι επιτιθέμενοι στοχεύουν στην αποκαλυπτόμενη ευπάθεια κατά τη διάρκεια αυτού του χρονικού διαστήματος.

Συνοψίζοντας…



ATTACK	UNMASKED	PREVENTION
MALWARE	A code with malicious intent	Firewalls & antimalware software
PHISHING	Personal data stolen using links or websites	Avoid unknown contacts & verify new emails
DENIAL-OF-SERVICE	High volumes of data sent to a server to disrupt it	Continuous online security monitoring
MAN-IN-THE-MIDDLE	Impersonation of a trusted contact	Encrypted communication modes
ROGUE SOFTWARE	Masked software with a malicious intent	Firewalls & antivirus software

Κατηγοριοποίηση κυβερνοεπιθέσεων



Verizon Data Breach Investigations Report (2017)

Κριτήριο
προέλευση του δράστη

- Εξωτερικές
- Εσωτερικές

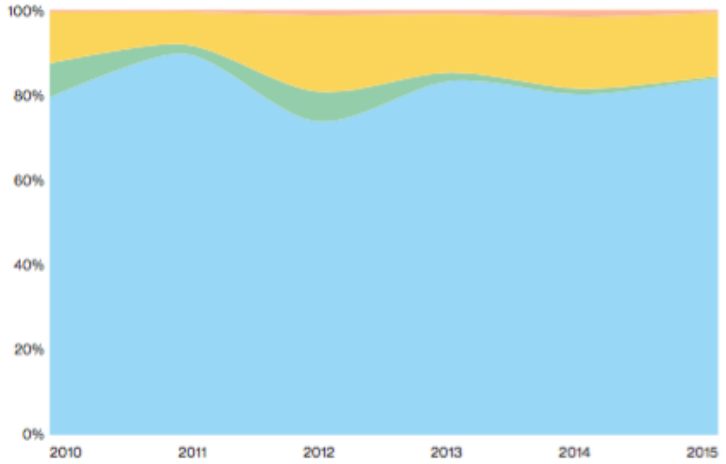


Figure 2.
Percent of breaches per threat actor category over time, (n=8,158)

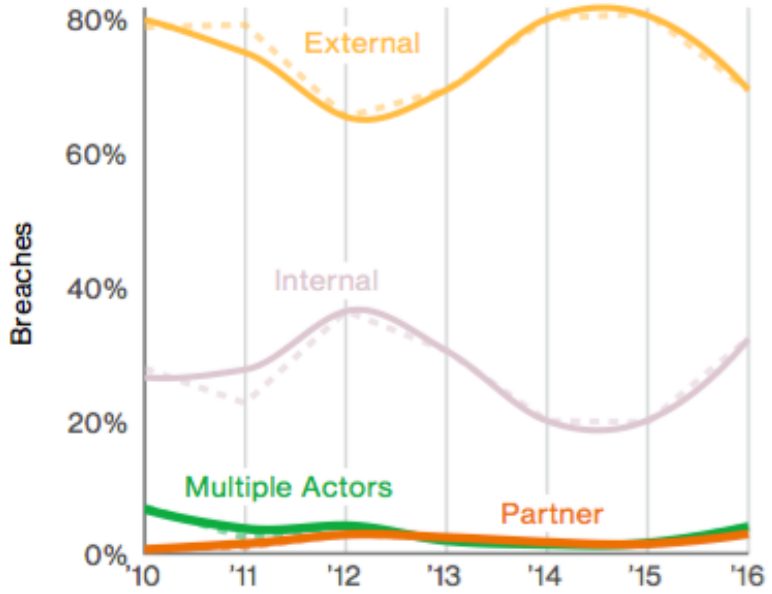


Figure 2: Threat actor categories over time

Κριτήριο – πρόθεση του δράστη

- Εγκληματικές πράξεις (cyber crimes)
  - *κυβερνοεγκληματίας (cyber criminal)*: οικονομικά ή ψυχολογικά οφέλη, κλοπή χρημάτων/δεδομένων, απόκτηση προσωπικής δόξας
- Τρομοκρατικές πράξεις (cyber terrorism)
  - *κυβερνοτρομοκράτης (cyber terrorist)*: πολιτικά ή κοινωνικά κίνητρα, εξαναγκασμός ενός συγκεκριμένου αποδέκτη(επίσημες αρχές ενός κράτους) εκφοβίζοντας τον με πράξεις ή με απειλές βίας
- Εχθροπραξίες (cyberwar/cyber warfare)
  - *κυβερνοπολεμιστής (cyber warrior/combatant)*: επίτευξη συγκεκριμένων στρατιωτικών στόχων στα πλαίσια μιας γενικευμένης διακρατικής αντιπαράθεσης

Κριτήριο *κίνητρο*

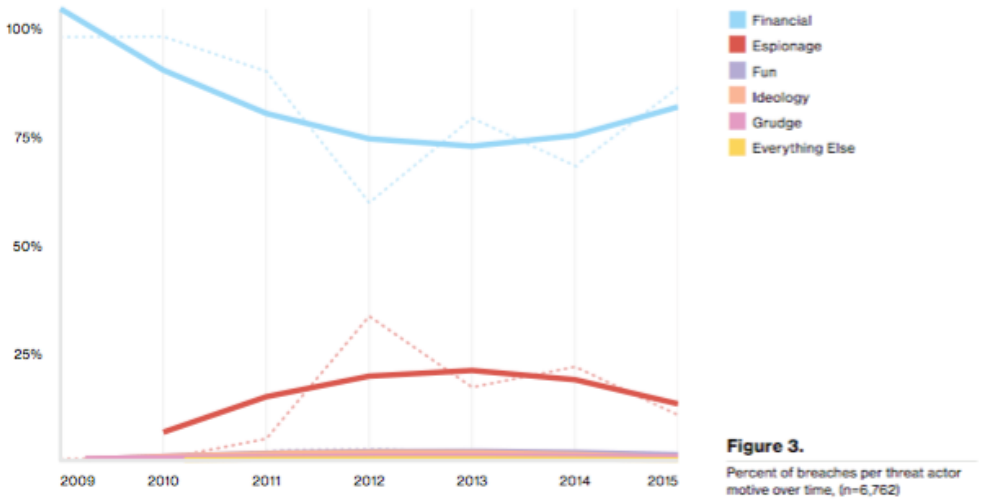


Figure 3.
Percent of breaches per threat actor motive over time, (n=6,762)

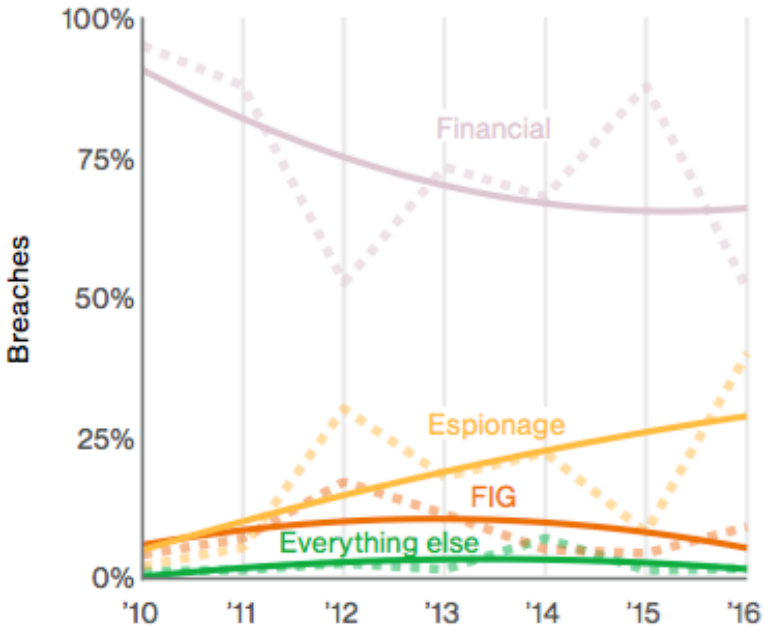


Figure 3: Threat actor motives over time

Κριτήριο - στόχος

- Μη-στοχευμένες επιθέσεις
  - ο στόχος δεν είναι συγκεκριμένος: όσο πιο πολλοί χρήστες, συσκευές, υπηρεσίες είναι δυνατό
    - phishing - sending emails to large numbers of people asking for sensitive information (such as bank details) or encouraging them to visit a fake website
    - water holing - setting up a fake website or compromising a legitimate one in order to exploit visiting users
    - ransomware - which could include disseminating disk encrypting extortion malware
    - scanning - attacking wide swathes of the Internet at random
- Στοχευμένες επιθέσεις
  - ο στόχος είναι συγκεκριμένος: πιο καταστροφικές
    - spear-phishing - sending emails to targeted individuals that could contain an attachment with malicious software, or a link that downloads malicious software
    - deploying a botnet - to deliver a DDOS (Distributed Denial of Service) attack
    - subverting the supply chain - to attack equipment or software being delivered to the organisation

Κριτήριο
στόχος (assets)

Server

User Device (POS)

Person

Media

Network

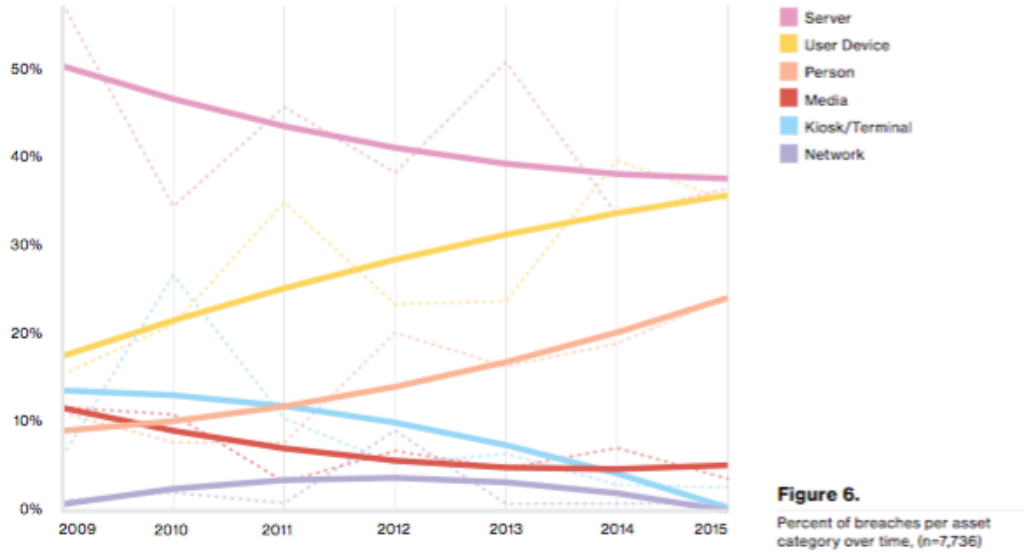


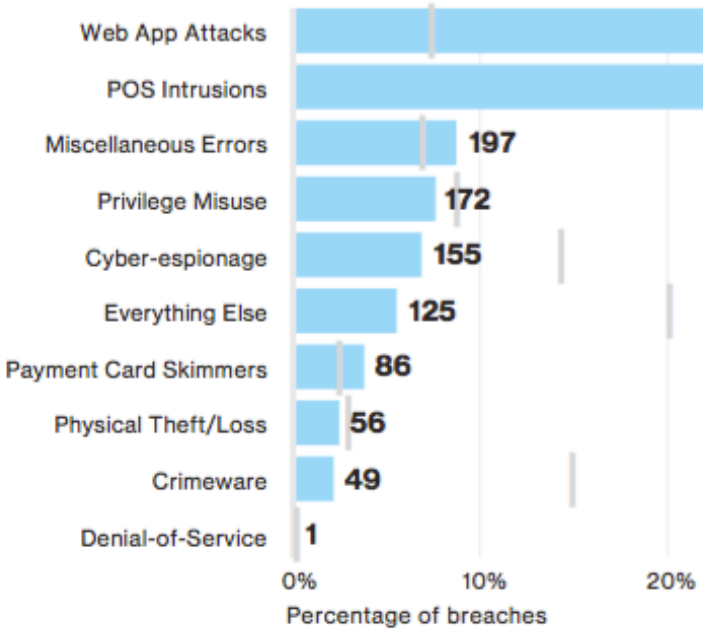
Figure 6.
Percent of breaches per asset category over time, (n=7,736)

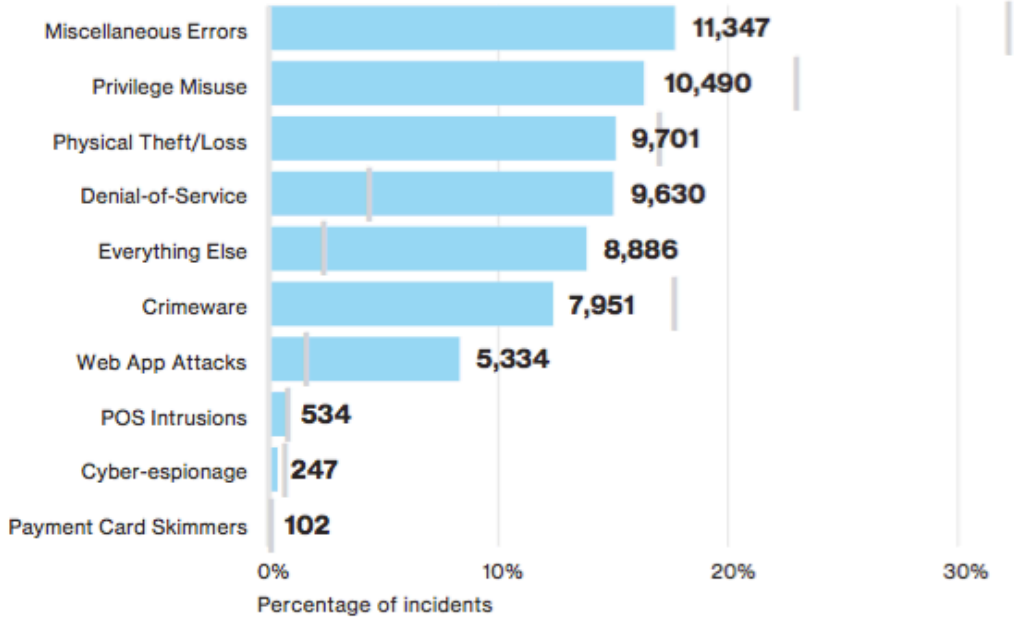
Κριτήριο – συνέπειες/αποτέλεσμα

- Έκθεση συσκευής (Device Compromise)
  - απόκτηση πλήρους ελέγχου μίας συσκευής
- Διακοπή υπηρεσίας (Service Disruption)
  - να εμποδίσει μία υπηρεσία να εκτελεί τα καθηκοντά της
- Εξαγωγή δεδομένων (Data Exfiltration)
  - κλοπή ευαίσθητων πληροφοριών από ένα στόχο
- Έγχυση «κακών» δεδομένων (Bad Data Injection)
  - ενσωμάτωση λανθασμένων δεδομένων σε ένα σύστημα χωρίς να ανιχνευθούν
- Advanced Persistent Threat (APT)
  - απόκτηση εκτεταμένης πρόσβασης σε μία συσκευή

9 incident classification patterns

combine who (actors), what (assets), how (actions) and why (motive)





9 incident classification patterns

combine who (actors), what (assets), how (actions) and why (motive)

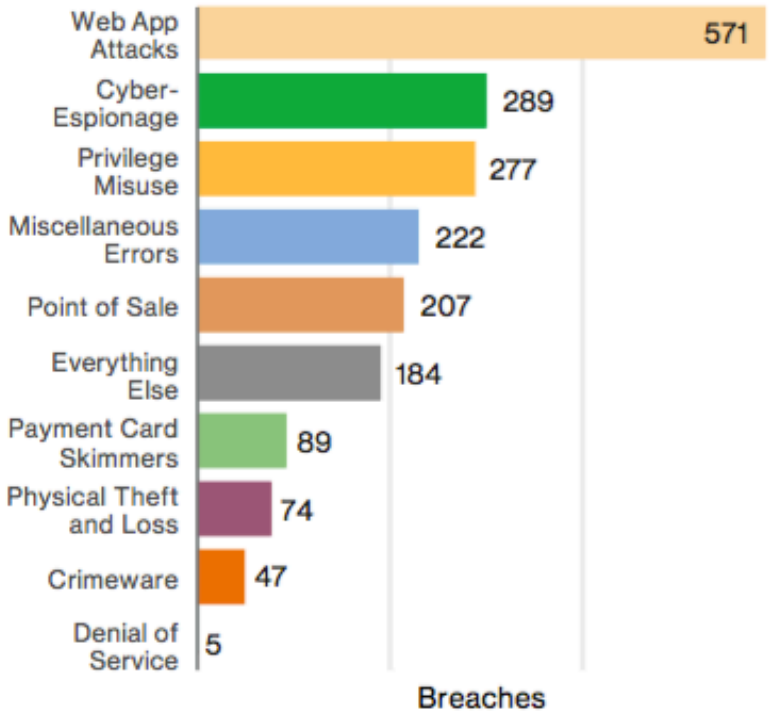


Figure 33: Percentage and count of breaches per pattern (n=1,935)

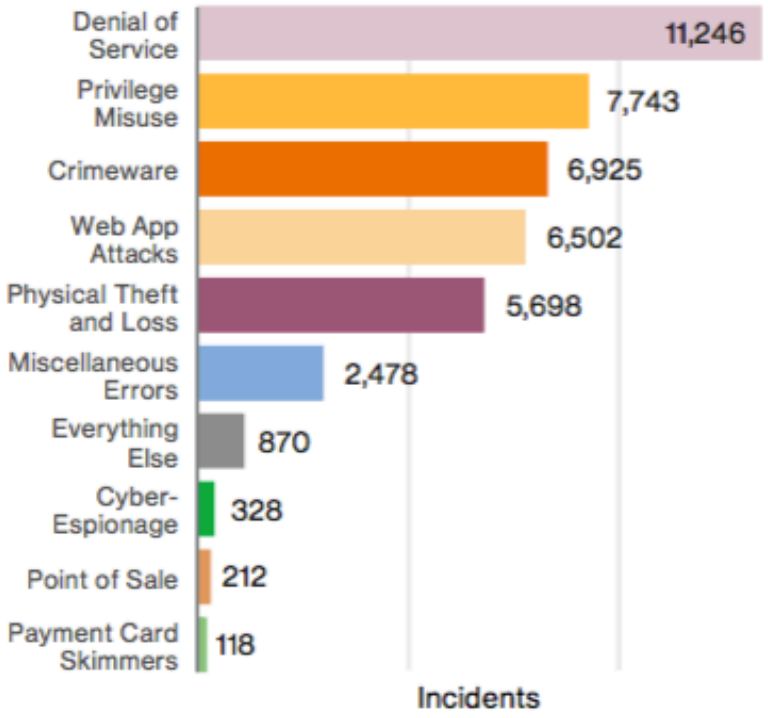


Figure 34: Percentage and count of incidents per pattern (n=42,068)

9 incident classification patterns

- Crimeware
  - αφορά χρήση κακόβουλου λογισμικού (malware) και δεν εντάσσεται σε άλλο πρότυπο
  - οικονομικά κίνητρα και ευκαιριακού χαρακτήρα
  - malware infections: έχουν σταλεί μέσω email ή web server
  - Ransomware
    - είδος malware το οποίο μολύνει το σύστημα και κρυπτογραφεί τα δεδομένα μέχρι να πληρωθούν τα λύτρα (ransom) που απαιτούνται για να «επιστραφούν» τα δεδομένα
- Cyber-Espionage (κυβερνο-κατασκοπεία)
  - μη εξουσιοδοτημένη πρόσβαση στο δίκτυο ή το σύστημα στα πλαίσια της κυβερνο-κατασκοπείας
  - συλλογή απόρρητων πληροφοριών
  - spear-phishing

9 incident classification patterns

- Denial of Service (άρνηση παροχής υπηρεσίας)
  - θέτει σε κίνδυνο τη διαθεσιμότητα δικτύων και συστημάτων
  - επιθέσεις στα δίκτυα και στις εφαρμογές σχεδιασμένες έτσι ώστε να κατακλύσουν τα συστήματα (υπερφόρτωση) με αποτέλεσμα να υποβαθμιστεί η απόδοσή τους ή να διακοπεί η υπηρεσία
  - Botnet
- Insider and Privilege Misuse (Κακή χρήση προνομίων και εκ των έσω)
  - οποιαδήποτε μη εγκεκριμένη ή κακόβουλη χρήση των πόρων ενός οργανισμού
  - κατά κυρίο λόγο αφορά εκ των έσω κακή χρήση, αλλά μπορεί να αφορά και εταίρους ή συνεργάτες

9 incident classification patterns

- Miscellaneous Errors
  - ακούσιες πράξεις έβλαψαν άμεσα ένα χαρακτηριστικό ενός αγαθού (asset)
  - π.χ. λανθασμένη αποστολή ή δημοσίευση πληροφοριών
- Physical Theft and Loss (φυσική κλοπή και απώλεια)
  - όταν ένα αγαθό χάθηκε είτε λόγω λάθος τοποθέτησης είτε κακόβουλης πράξης

9 incident classification patterns

- Payment Card Skimmers (σαρωτές καρτών πληρωμής)
  - φυσική τοποθέτηση συσκευών σάρωσης (skimming device) σε ένα «αγαθό» το οποίο διαβάζει τα δεδομένα των μαγνητικών ταινίων των καρτών πληρωμής (π.χ. ATMs, τερματικά POS, αντλίες καυσίμων, κ.α.)
- Point of Sale Intrusions (εισβολές στα σημεία πώλησης POS)
  - απομακρυσμένες επιθέσεις εναντίον των περιβαλλόντων όπου διεξάγονται συναλλαγές λιανικής πώλησης με κάρτα
  - τα τερματικά POS και οι ελεγκτές POS είναι τα αγαθά στόχος
  - χρήση κλεμμένων πιστοποιητικών και brute force πράξεις
  - RAM scraping, keylogging/spyware malware

9 incident classification patterns

- Web Application Attacks (επιθέσεις σε web εφαρμογές)
  - στόχος μία web εφαρμογή
  - εκμετάλλευση αδυναμιών σε επίπεδο κώδικα
  - παρεμπόδιση μηχανισμών αυθεντικοποίησης
  - SQL injections (SQLi)
- Everything Else
  - social engineering
  - information gathering
  - network footprinting

Κριτήριο *εργαλεία/ενέργειες*

Hacking

Malware

Social Engineering

Error

Physical

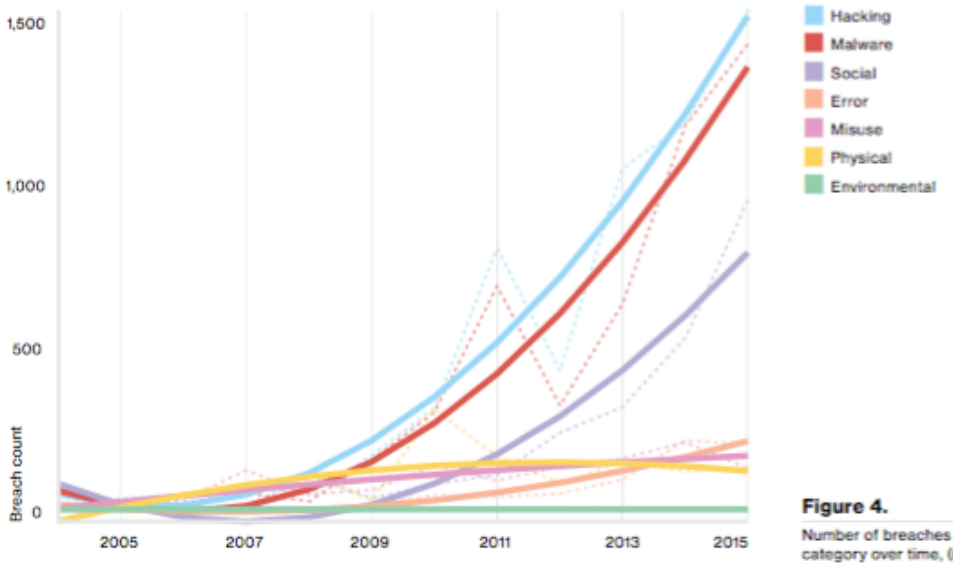


Figure 4.
Number of breaches per threat action category over time, (n=9,009)

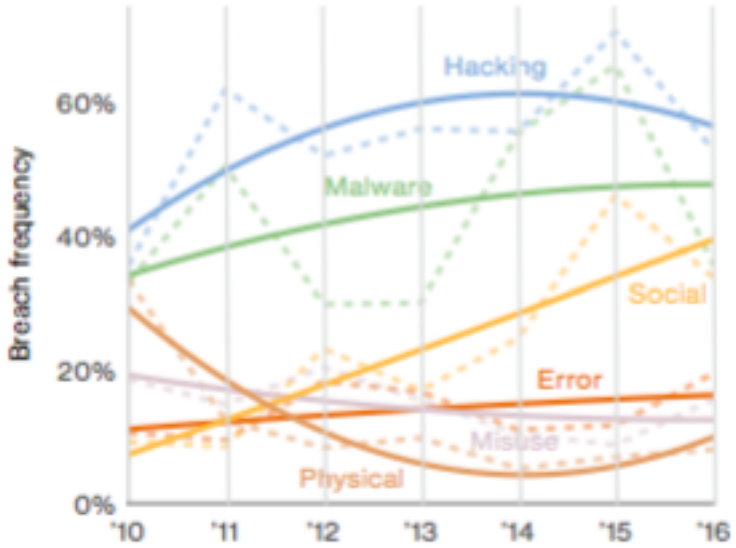


Figure 4: Percentage of breaches per threat action category over time

Ενέργειες

- Hacking
  - σκόπιμη πρόσβαση ή πρόκληση βλάβης σε πληροφοριακά αγαθά χωρίς εξουσιοδότηση παρακάμπτοντας ή αποτρέποντας μηχανισμούς ασφαλείας
- Malware
  - οποιοδήποτε κακόβουλο λογισμικό, script ή κώδικας που εκτελείται σε μια συσκευή, η οποία αλλάζει την κατάσταση ή τη λειτουργία της, χωρίς τη συναίνεση του ιδιοκτήτη
- Social
  - εξαπάτηση, χειραγώγηση, εκφοβισμός για την εκμετάλλευση πληροφοριακών αγαθών
- Error
  - ο,τιδήποτε έχει γίνει εσφαλμένα ή ακούσια
- Misuse
  - η χρήση προνομίων και πόρων με τρόπο αντίθετο προς το σκοπό τους
- Physical
  - σκόπιμες απειλές που περιλαμβάνουν εγγύτητα, κατοχή ή βία
- • Environmental
  - φυσικά γεγονότα και κινδύνους που σχετίζονται με το άμεσο περιβάλλον ή την υποδομή

Malware (κακόβουλα λογισμικά)

- Κακόβουλος κώδικας με σκοπό να κλέψει δεδομένα ή να καταστρέψει κάτι σε έναν υπολογιστή
  - Ιοί (viruses): προσκολλάται σ' ένα πρόγραμμα ή σ' ένα αρχείο και εκτελείται όταν το πρόγραμμα αυτό τεθεί σε λειτουργία. Αναπαράγεται μολύνοντας κι άλλα προγράμματα ή αρχεία.
  - Σκουλήκια (worms): επιφέρει τις συνέπειες του άμεσα χωρίς να χρειάζεται να προηγηθεί η εκτέλεση άλλου προγράμματος ή να υπάρξει ανθρώπινη παρέμβαση. Διαδίδεται μέσω του Διαδικτύου και μπορεί να προσβάλει όλα τα συστήματα στα οποία είναι συνδεδεμένος ο υπολογιστής που έχει μολύνει.
  - Δούρειοι Ίπποι (Trojan Horses): δεν αναπαράγεται, αλλά κρύβεται μέσα σε αθώα προγράμματα, μπορεί να αποκτήσει απομακρυσμένη πρόσβαση ή και έλεγχο (Drive-by Download)
  - Spyware: καταγράφει/ κατασκοπεύει δραστηριότητες του χρήστη, π.χ. να βλέπει κωδικούς πρόσβασης
- Πρόσβαση
  - Επισυναπτόμενα στα email
  - Λήψεις λογισμικού
  - Αδυναμίες λειτουργικών συστημάτων

Cross-Platform Malware & Metamorphic and Polymorphic Malware

- Πολλαπλής-πλατφόρμας κακόβουλα προγράμματα (CPM – Cross-Platform Malware)
  - κακόβουλα προγράμματα για διάφορες πλατφόρμες/λειτουργικά συστήματα (Windows/iOS)
- Μεταμορφικά και Πολυμορφικά Κακόβουλα Προγράμματα (Metamorphic and Polymorphic Malware)
  - κακόβουλα προγράμματα που συνεχίζουν να αλλάζουν τον κώδικά τους έτσι ώστε μία επιτυχής έκδοσή τους να διαφέρει από τις προηγούμενες
  - δεν εντοπίζονται/εμποδίζονται εύκολα από προγράμματα εντοπισμού και αντιικά
  - απειλούν διαδικτυακές εφαρμογές ανοιχτού κώδικα

Password Attacks - Brute-Force Attacks - Dictionary Attacks

- παραβίαση του κωδικού πρόσβασης του θύματος
- ο επιτιθέμενος αποκτά πρόσβαση σε ένα ασφαλές σύστημα
- *πρόταση*: δημιουργία καλών κωδικών πρόσβασης
- Επίθεση ωμής βίας
  - ο εισβολέας χρησιμοποιεί όλους τους πιθανούς συνδυασμούς γραμμάτων, αριθμών και συμβόλων για να εισάγει το σωστό κωδικό πρόσβασης. Όσο μεγαλύτερος και πολυπλοκότερος είναι ένας κωδικός πρόσβασης, τόσο περισσότερο χρόνο απαιτούν οι πιθανοί συνδυασμοί του.
- Επίθεση λεξικού
  - ο εισβολέας χρησιμοποιεί ένα λεξικό σε μία προσπάθεια να σπάσει έναν κωδικό πρόσβασης. Προτείνεται να μη γίνεται η χρήση απλών λέξεων που μπορούν να βρεθούν σε ένα λεξικό στους κωδικούς πρόσβασης.

DDoS - Botnet

- Denial of Service Attack (DoS): γίνεται από έναν υπολογιστή
- Distributed DoS (DDoS): εμπεριέχονται πολλαπλοί υπολογιστές, οι οποίοι στέλνουν φορτίο στο δίκτυο-στόχο
- Botnet: σύνολο υπολογιστών του οποίου ο επιτιθέμενος έχει πάρει τον έλεγχο για κακόβουλους σκοπούς
  - ο χρήστης του υπολογιστή δεν συνειδητοποιεί ότι ο υπολογιστής του αποτελεί μέρος του botnet
  - οι υπολογιστές που συνεισφέρουν, χαρακτηρίζονται ως bots ή zombies
  - ο επιτιθέμενος έχει την απαραίτητη υπολογιστική ισχύ που απαιτείται για τη διεξαγωγή μιας DDoS επίθεσης

Social Engineering
(Κοινωνική Μηχανική)

- η τέχνη της απόσπασης, με ποικίλες μεθόδους, καίριων πληροφοριών από ανθρώπους και της άνομης χρησιμοποίησής τους

- στο πλαίσιο κοινωνικής επαφής
  - π.χ. φιλίες σε δίκτυα κοινωνικής δικτύωσης όπου ο hacker κερδίζει την εμπιστοσύνη του θύματος και αποσπά απ' αυτόν πληροφορίες - λ.χ. ημερομηνία γέννησης – οι οποίες μπορεί να τον οδηγήσουν στο να ανακαλύψει κάποιον κωδικό)

Phishing

- ο hacker εμφανίζεται ως ένα φαινομενικά έμπιστο πρόσωπο (p.x. με e-mail) και προσπαθεί να παραπλανήσει το θύμα προκειμένου να αποσπάσει τα στοιχεία ηλεκτρονικής ταυτότητας του θύματος (όνομα χρήστη, κωδικό πρόσβασης και άλλα στοιχεία ταυτότητας)
- η αποστολή ηλεκτρονικών μηνυμάτων (e-mails) που σκοπό έχουν να προκαλέσουν την κλοπή εμπιστευτικών στοιχείων που ανήκουν στον παραλήπτη του ηλεκτρονικού μηνύματος
  - τα ηλεκτρονικά αυτά μηνύματα δίνουν την εντύπωση πως προέρχονται από κάποια τράπεζα είτε από ιστοσελίδα που έχει κερδίσει την εμπιστοσύνη των χρηστών του διαδικτύου και ζητούν από τον παραλήπτη την αποκάλυψη δεδομένων
- spear-phishing: αποστολή στοχευμένων email τα οποία περιέχουν επισυναπτόμενο malicious software ή link προς αυτό
- water holing: δημιουργία ενός «ψεύτικου» website ή η «έκθεση» ενός νόμιμου με σκοπό την εκμετάλλευση των επισκεπτών

Μόνιμη Προηγμένη Απειλή (APT – Advanced Persistent Threat)

- εξεζητημένες, συγχρονισμένες και συντεταγμένες προσπάθειες προς ένα μόνο στόχο
  - socially engineered Trojans ή phishing attacks
- η διείσδυση σε ένα ευαίσθητο σύστημα, παραμένοντας μη ανιχνεύσιμο για όσο το δυνατόν περισσότερο, και αφήνοντας ελάχιστα ίχνη
- απόκτηση ευαίσθητων και διαβαθμισμένων πληροφοριών
- σχετίζεται συχνά με επιθέσεις κυβερνο-κατασκοπείας

Ο ενδιάμεσος άνθρωπος (Man-in-the-middle MITM)

- ο επιτιθέμενος υποδύεται το τερματικό σημείο ενός συστήματος online ανταλλαγής πληροφοριών (π.χ. internet banking)
- αποκτά πρόσβαση μέσω ενός μη κρυπτογραφημένου ασύρματου σημείο εισόδου (που δε χρησιμοποιεί WAP, WPA, WPA2)
- έχει πρόσβαση σε ό,τι πληροφορία στέλνει ο χρήστης

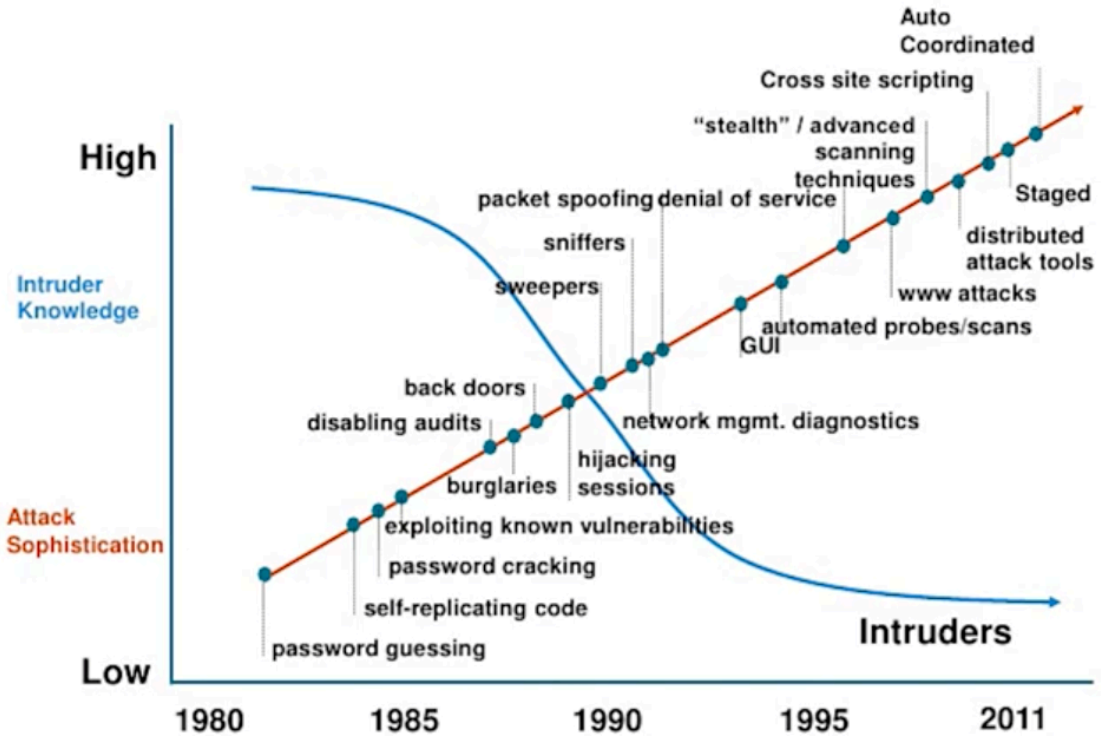
Αδυναμίες

- Υπερχείλιση προσωρινής μνήμης (buffer overflow)
  - τοποθετούνται περισσότερα δεδομένα σε ένα buffer) από όσα μπορεί να διατηρήσει αντικαθιστώντας άλλα δεδομένα.
  - περιέχουν κώδικα για να προκαλέσουν επιβλαβή δράση

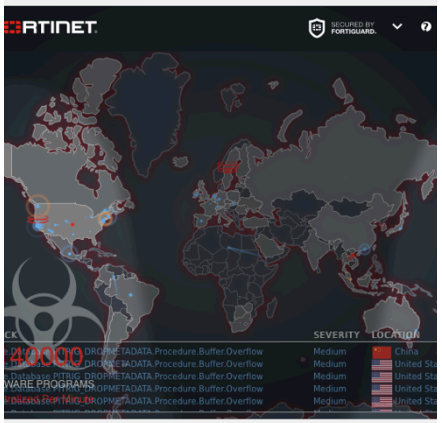
- SQL Injection
  - τα δεδομένα που δίνει ο χρήστης χρησιμοποιούνται για τη δημιουργία SQL ερωγημάτων με σκοπό την ανάκτηση πληροφοριών από τη ΒΔ
  - ο επιτιθέμενος δημιουργεί SQL εντολές με σκοπό να παρακάμψει τη διαδικασία επαλήθευσης του χρήστη

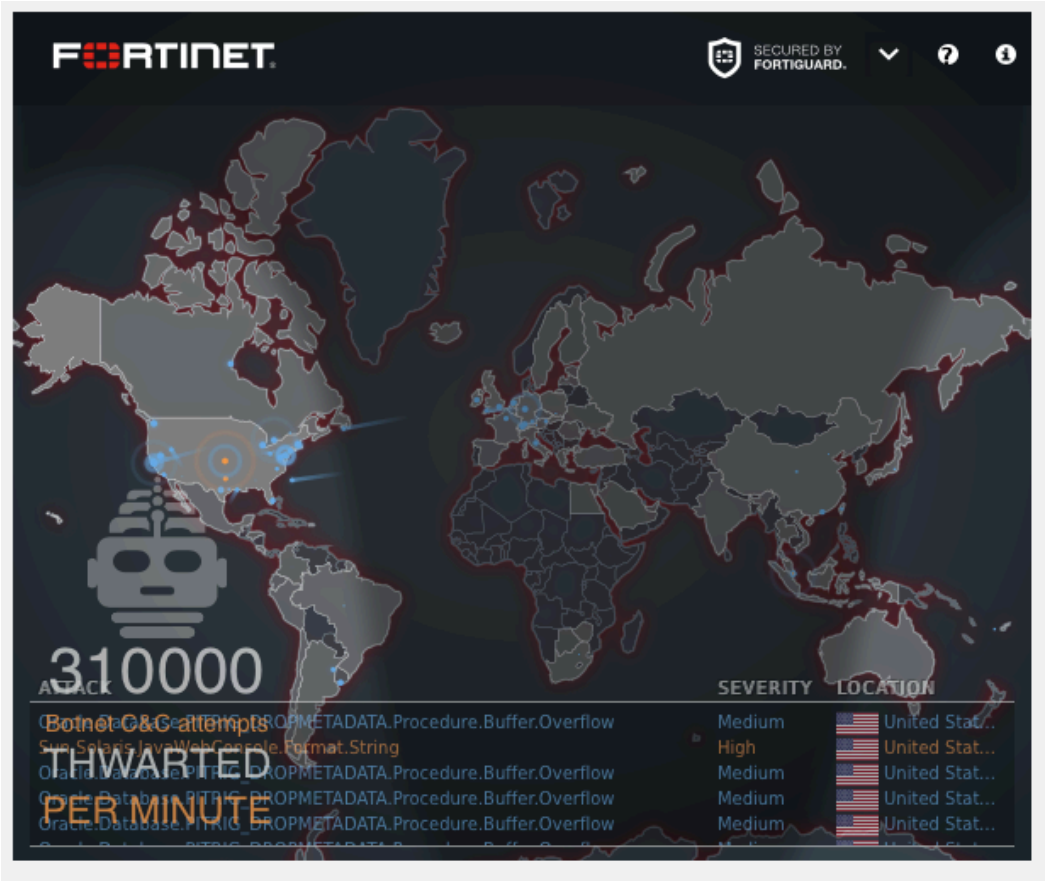
Attack Sophistication vs. Intruder Technical Knowledge

Courtesy Emil on security



Cyberthreat Maps





Fortinet Threat Map

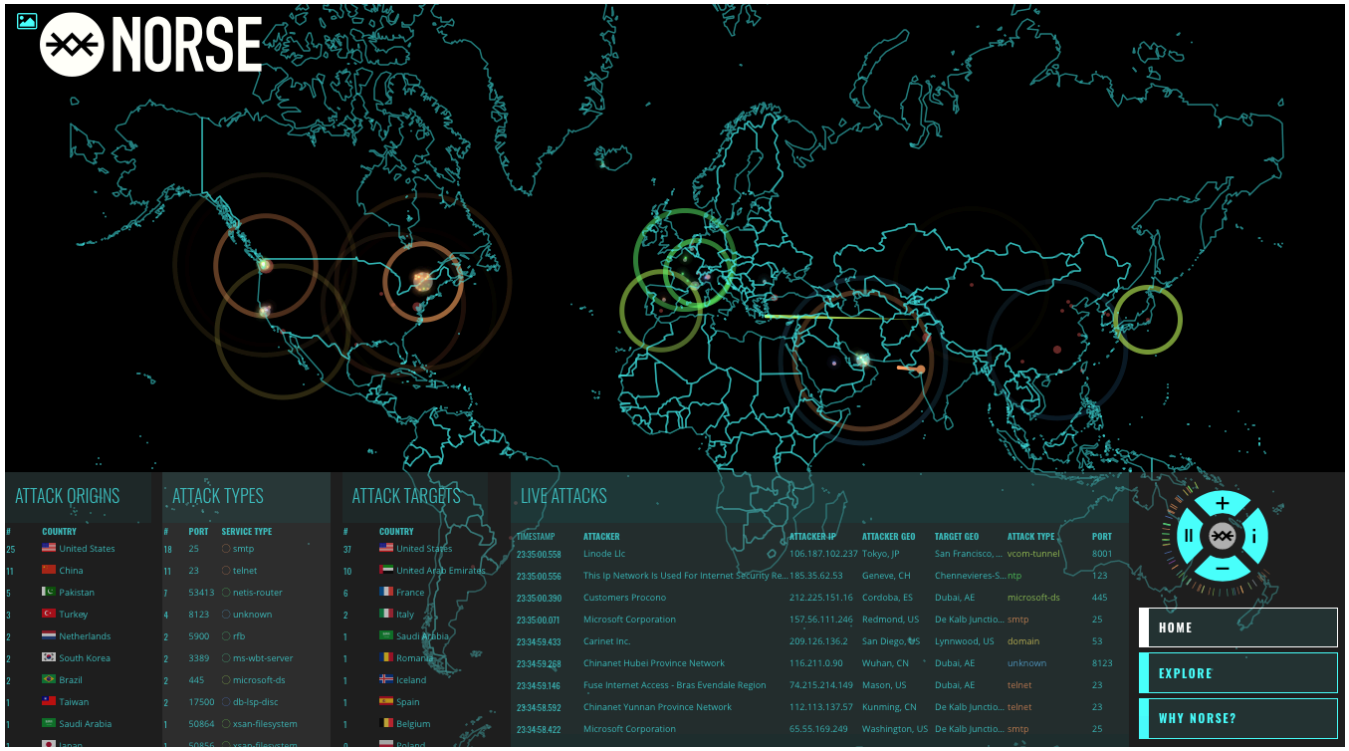
http://threatmap.fortiguard.com

FireEye Cyber Threat Map, FireEye, Inc.

https://www.fireeye.com/cyber-map/threat-map.html

Cyberthreat Real-Time Map, Kaspersky Lab

https://cybermap.kaspersky.com



Norse Corporation

http://map.norsecorp.com/

Μελέτες Περίπτωσης

1. Προσδιορίστε εάν το περιστατικό απειλούσε την Εμπιστευτικότητα, την Ακεραιότητα ή / και τη Διαθεσιμότητα
2. Δηλώστε την κύρια αιτία του συμβάντος
3. Προσδιορίστε την πραγματική ή πιθανή ζημία του συμβάντος

Μελέτες Περίπτωσης

HE-2: Hacktivist Attack – the Epluribus Enum, σελ. 19

HE-3: Partner Misuse – the Indignant Mole, σελ.24

HE-4: Disgruntled Employee – the Absolute Zero, σελ. 29

CD-3: IoT Calamity – the Panda Monium, σελ. 46

CE-2: DDoS attack – the 12000 Monkeyz, σελ. 61

- https://www.slideshare.net/EdurekaIN/8-most-common-cybersecurity-threats-types-of-cyber-attacks-cybersecurity-for-beginners-edureka