ΕΙΣΑΓΩΓΗ

- Νέες τεχνολογικές εξελίξεις – νέες εφαρμογές και συστήματα δικτύωσης: smart home, smart cars, smart business, smart cities, ολόκληροι τομείς υπηρεσιών, χρήση AI
- πανδημία COVID-19: εναλλακτικές μέσα στον ψηφιακό κόσμο: τηλεδιάσκεψη (teleconference, telco), βιντεο-κλήση (video call), απομακρυσμένη πρόσβαση (remote access), ηλεκτρονικό κατάστημα (e-shop), το ψηφιακό κράτος (digital state)
- Οι νέες τεχνολογίες+ τεχνολογίες νέφους (cloud computing) + δίκτυα 5ης γενιάς = εφαρμογή στους τομείς της υγείας (Internet of Medical Things - IoMT, ψηφιακό σύστημα υγείας, διασύνδεση υπηρεσιών παροχής υγείας και υγειονομικών πόρων), των μεταφορών (σε επίπεδο οχήματος, οδηγού, αλλά και υποδομής), τον κατασκευαστικό τομέα (Industry 4.0), τον αγροδιατροφικό τομέα, εθνική άμυνα (Internet of Military Things).
- Internet of Everything (IoE) - η διαδικτύωση των πάντων.

ΚΙΝΔΥΝΟΙ-ΠΡΟΚΛΗΣΕΙΣ:

Ψηφιακός κόσμος-νέος θαυμαστός κόσμος – μεγαλύτερο πεδίο για κακόβουλες και παράνομες ενέργειες.

-Νέες υπηρεσίες - νέοι κίνδυνοι για την εκμετάλλευση ή παραβίαση των προσωπικών μας δεδομένων. Πχ ιστότοποι κοινωνικής δικτύωσης (social networking).

Λύση: γνώση, κατανόηση των σύγχρονων τεχνολογικών εξελίξεων, πρόβλεψη ειδικών δικλείδων ασφαλείας, διαρκή ενημέρωση και ευαισθητοποίηση των χρηστών στο πλαίσιο της προαγωγής της κυβερνο-υγιεινής (cyber-hygiene).

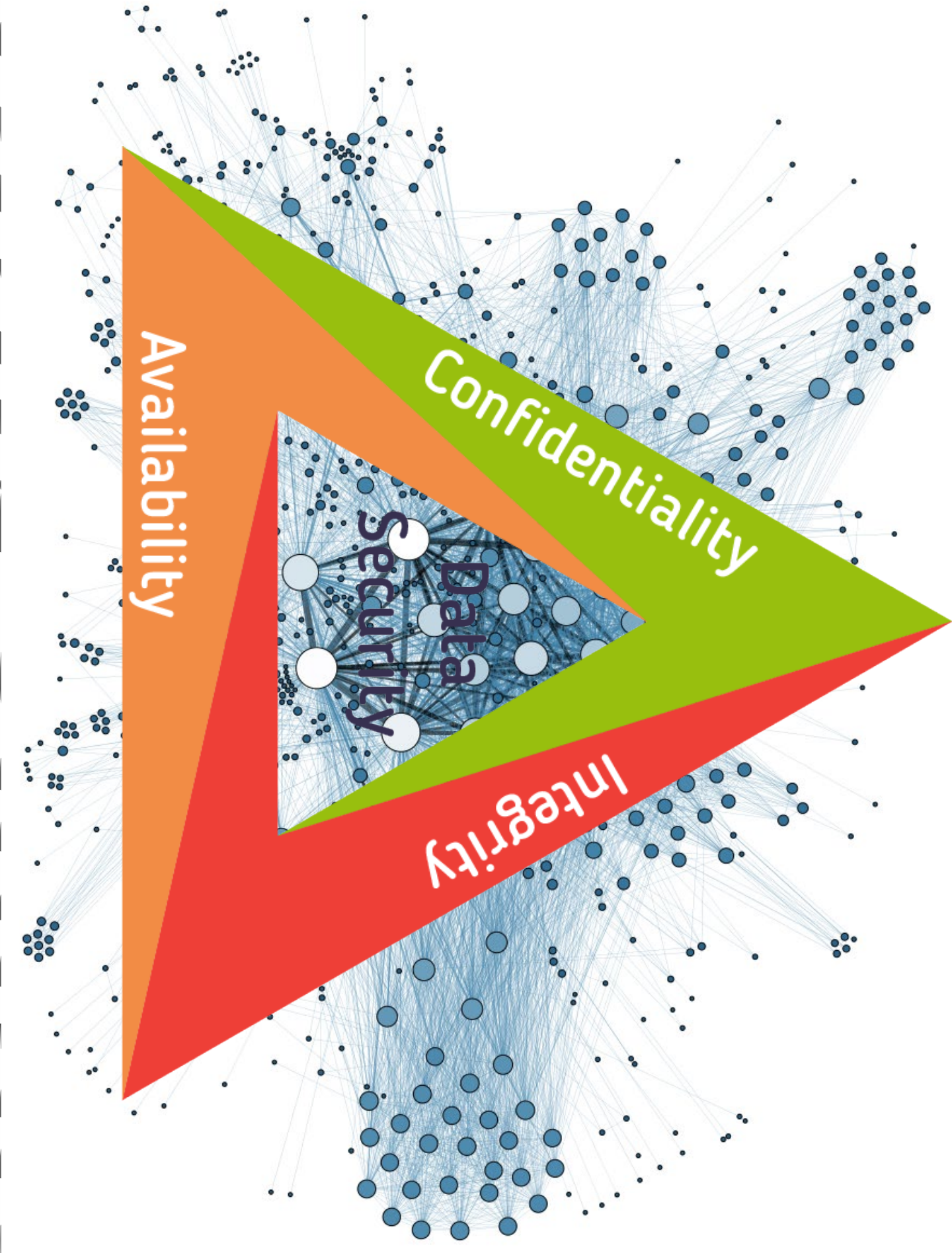
ΟΡΙΣΜΟΙ

- **Κυβερνοεπιθέσεις**:

Μπορεί να οδηγήσουν σε απώλεια δεδομένων και παραβίαση της εμπιστευτικότητας, διαθεσιμότητας και ακεραιότητας των πληροφοριών, υπηρεσιών και συστημάτων ενός φορέα με αποτέλεσμα σημαντικές οικονομικές και επιχειρηματικές επιπτώσεις (πχ στη φήμη εταιρείας).

- **Κυβερνοασφάλεια:**

Η προστασία των δεδομένων, των δικτύων, συσκευών και των προγραμμάτων ενός φορέα από μη εξουσιοδοτημένες προσβάσεις, επιθέσεις και την πιθανή διακοπή της λειτουργίας του από εσωτερικές και εξωτερικές απειλές.


Availability
Confidentiality
Integrity
Data
Security

ΚΟΙΝΕΣ ΒΑΣΙΚΕΣ ΕΝΝΟΙΕΣ

- **Confidentiality (Εμπιστευτικότητα):**

Η πρόσβαση στις πληροφορίες πρέπει να επιτρέπεται ανά πάσα στιγμή μόνο σε εξουσιοδοτημένα άτομα. Ένα βασικό στοιχείο της διατήρησης της εμπιστευτικότητας είναι να διασφαλιστεί ότι άτομα χωρίς την κατάλληλη εξουσιοδότηση εμποδίζονται να έχουν πρόσβαση σε πληροφορίες.

- **Integrity (Ακεραιότητα):**

Οι πληροφορίες πρέπει να προστατεύονται από μη εξουσιοδοτημένη τροποποίηση ή παραβίαση.

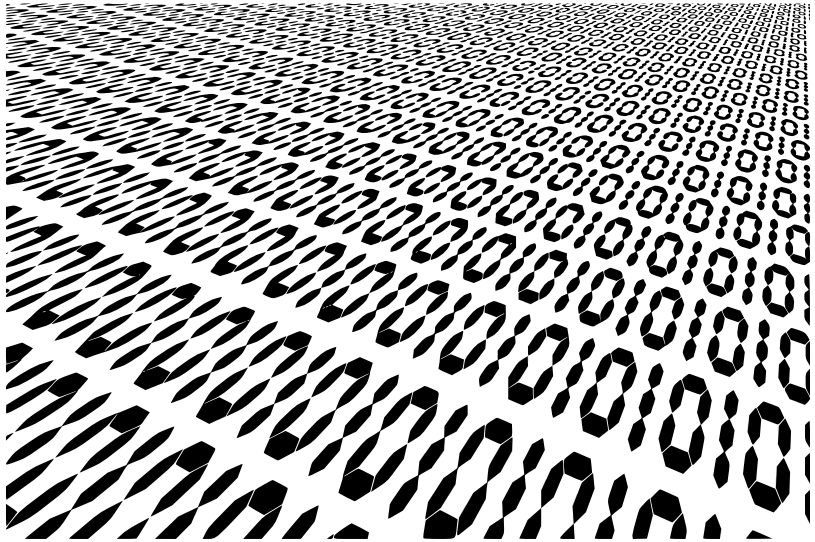
- **Availability (Διαθεσιμότητα):**

Οι πληροφορίες πρέπει να είναι άμεσα διαθέσιμες τη στιγμή που ο εκάστοτε χρήστης απαιτεί πρόσβαση σε αυτές.

Threat	Impact	Remedy
Confidentiality	Privacy of individuals, leaking credentials	Encryption, strong authentication, access control, data anonymization
Data Integrity	Invalid data	Strong identity verification (such as the use of certificates), encryption, checksum verification
Data Availability	Query performance, denial of service	Distributed data providers, intrusion detection and prevention

Ειδη κυβερνοαπειλων

DENIAL OF SERVICE ATTACKS



- **Malicious software**: κακόβουλο λογισμικό το οποίο έχει σχεδιαστεί ειδικά για να προκαλέσει ζημιά ή να αποκτήσει μη εξουσιοδοτημένη πρόσβαση σε ένα σύστημα υπολογιστή. Περιλαμβάνει ιούς (virus), worms, trojan horses, ransomware κλπ.

- **Web based attacks:** Πρόκειται για απειλές που στοχεύουν απευθείας στο χρήστη μέσω εκμετάλλευσης αδυναμιών στους φυλλομετρητές (browsers), καθώς και στα συστήματα διαχείρισης περιεχομένου (content management systems). Κυριότερα είδη επιθέσεων αυτής της κατηγορίας αποτελούν τα browser exploits, drive-by downolads, watering hole attacks κ.α.

- **Phising:** Κακόβουλα μηνύματα ηλεκτρονικού ταχυδρομείου ή τηλεφωνικές συνδιαλλαγές, οι οποίες αποσκοπούν στο να παραπλανήσουν τους χρήστες και να αποκαλύψουν εμπιστευτικές πληροφορίες.

- **Ανεπιθύμητα μηνύματα ηλεκτρονικού ταχυδρομείου- SPAM:** πρόκειται για αποστολή ανεπιθύμητης αλληλογραφίας σε χρήστες. Η εν λόγω αλληλογραφία χαρακτηρίζεται από το πολύ μικρό κόστος αποστολής των μηνυμάτων, την ενόχληση που προκαλεί στους χρήστες, αλλά και την εν δυνάμει μετεξέλιξη των μηνυμάτων σε απειλή phishing.

- **Dos attacks (denial of services)**: Επιθέσεις κατά τις οποίες μεγάλος όγκος διαδικτυακής κίνησης στοχεύει σε μια υπηρεσία, με σκοπό να καταστεί αδύνατο από τα συστήματα να εξυπηρετήσουν νόμιμα αιτήματα. Ουσιαστικά, εκμεταλλεύονται την πεπερασμένη χωρητικότητα συστημάτων και δικτύων, ώστε να καταστήσουν αδύνατη την παροχή υπηρεσιών (απώλεια διαθεσιμότητας).

- **Παραβάσεις προσωπικών δεομένων**: Επιθέσεις οι οποίες αποσκοπούν στη διαρροή, αλλοίωση ή μη διαθεσιμότητα προσωπικών δεδομένων. Σύμφωνα με τον Κανονισμό της Ε.Ε. 2016/679, τέτοιου είδους επιθέσεις νοούνται ως παραβιάσεις δεδομένων προσωπικού χαρακτήρα, οι οποίες χρήζουν άμεσης αντιμετώπισης.

- **Botnets**: Δίκτυα τα οποία αποτελούνται από υπολογιστικές συσκευές ανυποψίαστων χρηστών που έχουν μολυνθεί με κακόβουλο λογισμικό και ελέγχονται κεντρικά από κάποιον επιτιθέμενο, προκειμένου να χρησιμοποιηθούν ομαδικά στην αποστολή μηνυμάτων ανεπιθύμητης αλληλογραφίας, σε επιθέσεις άρνησης υπηρεσίας, σε cryptojacking, κλπ.

- **Διαρροή δεδομένων σε μη εξουσιοδοτημένους χρήστες:** Τα δεδομένα μπορεί να περιλαμβάνουν οικονομικά στοιχεία, πατέντες, δεδομένα με κατοχυρωμένα πνευματικά δικαιώματα, πλάνα στρατηγικής ανάπτυξης κλπ.

- **Identity theft:** Ο επιτιθέμενος αποκτά δεδομένα προσωπικού χαρακτήρα του χρήστη (passwords, social security numbers κ.α.), με αποτέλεσμα την ιδιοποίηση της ταυτότητας του χρήστη (impersonation) και με σκοπό το οικονομικό όφελος (αγορές προϊόντων μέσω πιστωτικών καρτών, παράνομη επιστροφή φόρου κ.λπ.) εις βάρος του.

- **Ransomware:** Κακόβουλο λογισμικό (malware) το οποίο κρυπτογραφεί τα δεδομένα του πληροφοριακού συστήματος, για την αποκρυπτογράφηση των οποίων ο επιτιθέμενος απαιτεί λύτρα (συνήθως σε μορφή κρυπτονομίσματος).

Web application attacks: Επιθέσεις που στοχεύουν σε διαδικτυακές εφαρμογές (web applications). Οι εν λόγω εφαρμογές λόγω της καθολικής χρήσης τους στην προσφορά περιεχομένου αποτελούν στόχο πολλαπλών ειδών επιθέσεων, με κυριότερες τα cross-site scripting (XSS), SQL injection, path traversal, local file inclusion κ.α.

Insider threats: Απειλές που προέρχονται από στελέχη και εξωτερικών συνεργατών που εργάζονται ή εργάζονταν σε έναν οργανισμό και κατέχουν εσωτερική πληροφόρηση για τις πρακτικές ασφάλειας, τα υπολογιστικά συστήματα και τα δεδομένα του Οργανισμού. Οι εν λόγω απειλές μπορούν να οδηγήσουν σε πλήθος επιθέσεων με πολύ μεγάλο αντίκτυπο για τον φορέα και είναι εξαιρετικά δύσκολο να διαγνωσθούν ή και αντιμετωπισθούν.

Ηλεκτρονική κατασκοπία: Κατασκοπία μέσω του κυβερνοχώρου, η οποία μπορεί να περιλαμβάνει χρήση εξειδικευμένων εργαλείων για την άντληση στοιχείων ή/και χρήση συνδυασμού των προαναφερθέντων απειλών. Συνήθως αυτή η μορφή επίθεσης αναφέρεται ως «στοχευμένη» (λόγω του ότι οι επιτιθέμενοι έχουν πολύ συγκεκριμένους στόχους) με απώτερο στόχο την υποκλοπή ευαίσθητων, για τον οργανισμό, πληροφοριών.

THE REVIEW OF THE ENISA FORESIGHT CYBER-SECURITY THREATS FOR 2030

enisa EUROPEAN UNION AGENCY FOR CYBERSECURITY 20 years!

THREAT AGENTS παράγοντες απειλών

- **cybercriminals**: ο κυβερνοέγκλημα (cybercrime): κάθε κακόβουλη ενέργεια που αποσκοπεί να επιφέρει αντίκτυπο στις επιχειρησιακές λειτουργίες ενός οργανισμού. Οι κυβερνοεγκληματίες μπορεί νσ είναι ομάδες ή μεμονωμένα φυσικά πρόσωπα που χρησιμοποιούν την τεχνολογία (ΤΠΕ) για την τέλεση κακόβουλων ενεργειών. Συχνά εμπλέκονται σε παράνομες δοσοληψίες στο επονομαζόμενο Dark Web, όπου προβαίνουν σε αγοροπωλησία κακόβουλων εφαρμογών ή πληροφοριών για πιθανούς στόχους.

Το κυβερνοέγκλημα δύναται να περιλαμβάνει:

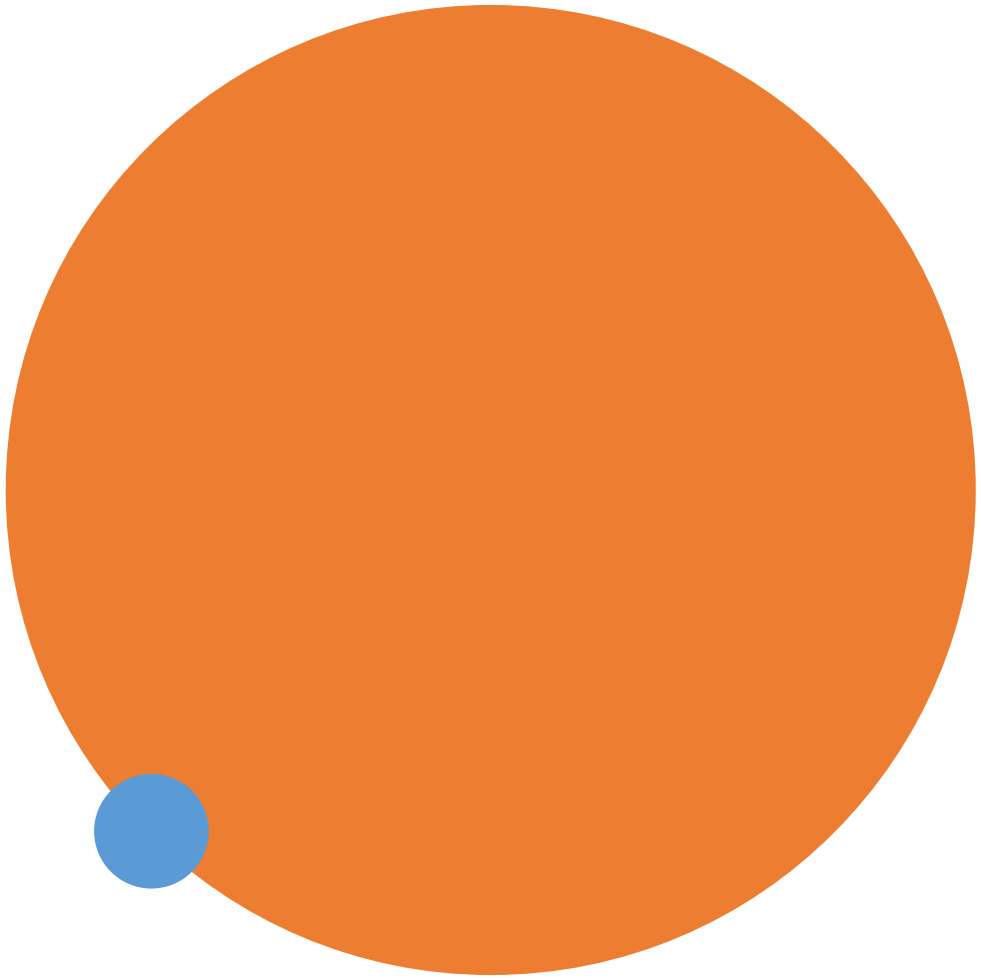
- Τρομοκρατικές ενέργειες (κυβερνο-τρομοκρατία).

- Επιθέσεις άρνησης υπηρεσίας (Denial of Service, DoS - cyber extortion).

- Κυβερνο-πόλεμο (cyber warfare).

- **Τρίτα κράτη**: ομάδες οι οποίες είτε ανήκουν, είτε χρηματοδοτούνται από κράτη και αποσκοπούν να εξαπολύσουν επιθέσεις που θα επιφέρουν μεγάλο αντίκτυπο στην παροχή βασικών / ουσιωδών υπηρεσιών από Φορείς. Τέτοιου είδους επιθέσεις έχουν ως κύριο στόχο τη διακοπή υπηρεσιών (π.χ. μέσω επιθέσεων άρνησης υπηρεσίας - DoS/DDoS) ή μη εξουσιοδοτημένης πρόσβασης σε διαβαθμισμένα δεδομένα. Ιδιαίτερη μνεία πρέπει να γίνει σε περιπτώσεις κυβερνο-κατασκοπείας, όπου διακρίνεται, τα τελευταία έτη, έξαρση επιθέσεων σε Φ.Ε.Β.Υ. (φορείς εκμετάλλευσης βασικών υπηρεσιών)

- **Ακτιβιστές**: Αυτό-αποκαλούμενοι ακτιβιστές ή αντίστοιχες ομάδες που προβαίνουν σε κακόβουλες ενέργειες όπως επιθέσεις άρνησης υπηρεσιών, αλλοίωση ιστοσελίδων, επιθέσεις/αντεπιθέσεις σε κράτη, κλπ. Στόχος των ακτιβιστών (συχνά αναφερόμενοι ως hacktivists) είναι η προώθηση κάποιας κοινωνικής αλλαγής ή πολιτικής ατζέντας ή αντεπίθεσης για την τόνωση του εθνικού φρονήματος, η οποία συχνά συνοδεύεται από προειδοποίηση για παύση της «γενεσιουργού αιτίας» υπό την απειλή της παράτασης ή/και επανάληψης ή/και κλιμάκωσης της επίθεσης.



- **Εσωτερικές απειλές**: αφορά σε υπαλλήλους οργανισμών που προβαίνουν, είτε εκούσια, είτε ακούσια, σε κακόβουλες ενέργειες. Λόγω της φύσης και του επιπέδου πρόσβασης σε συστήματα και πληροφορίες ενός Φορέα, καθώς και της προσέγγισης περιμετρικής ασφάλειας που υιοθετούν αρκετοί Φορείς, οι εσωτερικές απειλές αποτελούν τον μεγαλύτερο παράγοντα απειλών και έναν από τους πιο δύσκολους στην αναγνώριση και αντιμετώπισή τους.

Θεσμικό πλαίσιο cybersecurity

- Ν. 5160/2024 - οδηγία NIS II
- Οδηγία για την ανθεκτικότητα των κρίσιμων οντοτήτων (2022/2557)
- Κανονισμός DORA 2022/2554 για την ψηφιακή ανθεκτικότητα του χρηματοπιστωτικού τομέα
- Ν. 4961/2022 άρθρα 32-42 για τις συσκευές IoT (αφορά σε κατασκευαστές, εισαγωγείς, διανομείς και φορείς εκμετάλλευσης τέτοιων συσκευών-αναδυόμενες τεχνολογίες)
- Άρθρα 109-223 του Νόμου 4727/2020 για τον Ευρωπαϊκό Κώδικα Ηλεκτρονικών Επικοινωνιών, άρθρο 12 του Ν. 3471/2006 και 205/2013 Απόφαση της ΑΔΑΕ «Κανονισμός για την Ασφάλεια και την Ακεραιότητα Δικτύων και Υπηρεσιών Ηλεκτρονικών Επικοινωνωνιών= Εισαγωγή μέτρων ασφάλειας πληροφοριών για δίκτυα / υπηρεσίες ηλεκτρονικών επικοινωνιών – αφορά σε παρόχους δικτύων ή/και υπηρεσιών ηλεκτρονικών επικοινωνιών
- Κανονισμός (ΕΕ) 2019/881 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 17ης Απριλίου 2019 σχετικά με τον ENISA και με την πιστοποίηση της κυβερνοασφάλειας στον τομέα της τεχνολογίας πληροφοριών και επικοινωνιών
- Κοινή απόφαση ΑΠΔΠΧ/ΑΔΑΕ 01/2013 για την προστασία των προσωπικών δεδομένων στις ηλεκτρονικές υπηρεσίες

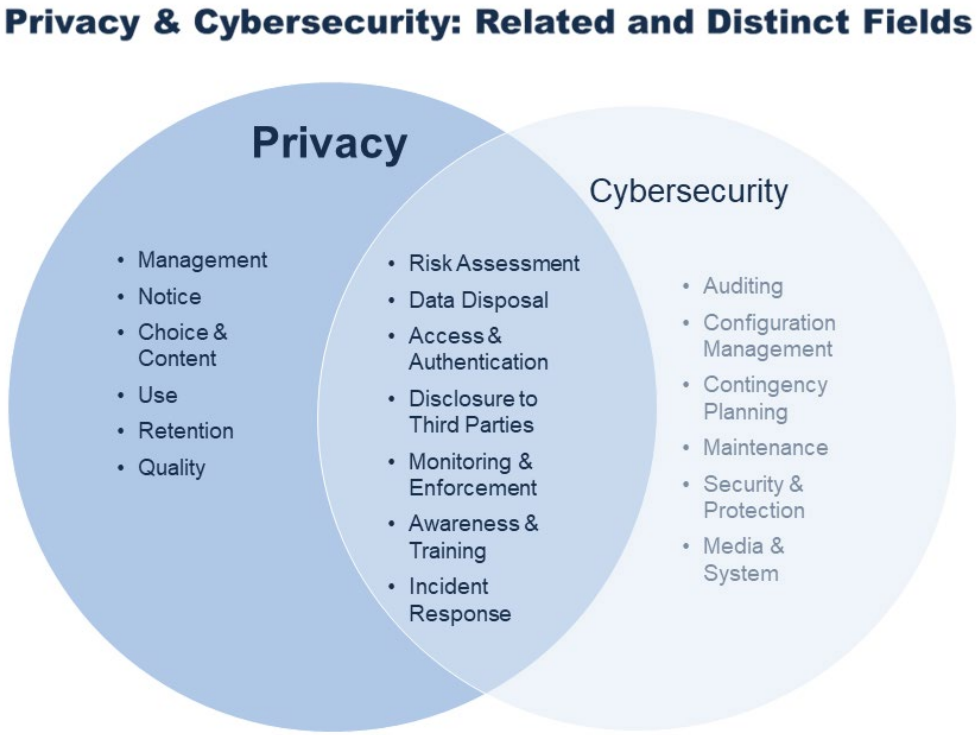
ΑΡΧΕΣ-stakeholders	ΑΡΜΟΔΙΟΤΗΤΕΣ
ENISA	Ο Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια, ENISA, είναι ο οργανισμός της Ένωσης αφιερωμένος στην επίτευξη ενός υψηλού κοινού επιπέδου ασφάλειας πληροφοριών σε όλη την Ευρώπη. Ο ENISA συμβάλλει στην πολιτική της ΕΕ στον κυβερνοχώρο, ενισχύει την αξιοπιστία των προϊόντων, υπηρεσιών και διαδικασιών ΤΠΕ με συστήματα πιστοποίησης κυβερνοασφάλειας, συνεργάζεται με κράτη μέλη και φορείς της ΕΕ και βοηθά την Ευρωπαϊκή Επιτροπή να προετοιμαστεί για τις αυριανές προκλήσεις ασφάλειας πληροφοριών.
ΚΕΜΕΑ (ΥπΠΡΟΠΟ)	Επιστημονικός, ερευνητικός και συμβουλευτικός φορέας, με σκοπό τη διεξαγωγή θεωρητικής και εφαρμοσμένης έρευνας και εκπόνησης μελετών, για θέματα που αφορούν την Πολιτική Ασφάλειας
Εθνική Αρχή Κυβερνοασφάλειας	- Έλεγχος και αξιολόγηση φορέων. - Συνολική διαχείριση της Εθνικής Στρατηγικής Κυβερνοασφάλειας. - Συλλογή και επεξεργασία πολιτικών ασφαλείας, σχεδίων αποκατάστασης και τήρηση μητρώου - Συντονισμός, εποπτεία, συνεργασίες, ενημέρωση

ΑΡΧΕΣ	ΑΡΜΟΔΙΟΤΗΤΕΣ
ΑΔΑΕ	- Εποπτεύει την εφαρμογή της νομοθεσίας περί απορρήτου των επικοινωνιών. - Επιβλέπει τη νόμιμη διαδικασία της άρσης του απορρήτου των επικοινωνιών. - Ρυθμίζει και εποπτεύει την ασφάλεια των επικοινωνιών στα διαθέσιμα στο κοινό δίκτυα και υπηρεσίες ηλεκτρονικών επικοινωνιών.
ΑΠΔΠΧ	- Παρακολουθεί και επιβάλλει την εφαρμογή του ΓΚΠΔ. - Ενημερώνει το κοινό, γνωμοδοτεί για νομοθετικά και διοικητικά μέτρα, καταρτίζει και διατηρεί κατάλογο σε σχέση με την απαίτηση για διενέργεια εκτίμησης αντικτύπου
ΔΝΣΗ Δίωξης Ηλεκτρονικού Εγκλήματος (Κυβερνοέγκλημα)	- Είναι υπεύθυνη για την επιβολή του νόμου κατά των κυβερνοεγκλημάτων και για την πρόληψη, την έρευνα και την καταστολή εγκλημάτων ή αντικοινωνικών συμπεριφορών, που διαπράττονται μέσω του διαδικτύου ή άλλων μέσων ηλεκτρονικής επικοινωνίας.
ΕΥΠ	- Ενεργεί ως αρχή αρμόδια για την ασφάλεια πληροφοριών στον δημόσιο τομέα. - Εθνική Αρχή Αντιμετώπισης Ηλεκτρονικών Επιθέσεων (CERT), CRYPTO (κρυπτασφάλεια), TEMPEST, INFOSEC (ασφάλεια εθνικών επικοινωνιών και συστημάτων τεχνολογίας πληροφοριών)

Σχέση κυβερνοασφάλειας-προσωπικών δεδομένων

- Προστασία κοινών «αγαθών» και αρχών
- Ορισμός υπευθύνου προσώπου
- Υποχρέωση λήψης μέτρων και διαδικασιών ασφαλείας
- Υποχρέωση αναφοράς περιστατικών
- Έλεγχος από αρμόδιες αρχές-κυρώσεις
- Ανάγκη ενημέρωσης και ευαισθητοποίησης κοινού
- Ανάγκη συλλογής, ανάλυσης και τεκμηρίωσης δεδομένων κυβερνοεπιθέσεων που ενέχουν παραβίαση της ιδιωτικότητας, με σκοπό την απόκτηση ολοκληρωμένης εικόνας για τα εν λόγω περιστατικά, καθώς και την πραγματοποίηση περαιτέρω δράσεων για την αντιμετώπισή τους.

Ασφαλεια και ιδιωτικοτητα στον κυβερνοχωρο



Ευχαριστούμε πολύ!

Λίνα Α. Δικαιάκου, Δ.Μ.Ε.
Δικηγόρος-Νομική Σύμβουλος
info@neolaw.gr