SysteCom

MEMBER OF QNR GROUP

# ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ

# &

# NIS2

ΠΣΒΑΚ

ΠΑΝΕΛΛΗΝΙΟΣ ΣΥΝΔΕΣΜΟΣ
ΒΙΟΜΗΧΑΝΩΝ & ΑΝΤΙΠΡΟΣΩΠΩΝ
ΚΑΛΛΥΝΤΙΚΩΝ & ΑΡΩΜΑΤΩΝ

QUALITY & RELIABILITY
GROUP

SysteCom

MEMBER OF QNR GROUP

# Hello Everyone!

**Nikos Niskopoulos**

SysteCom Chief Operations Director

COO | CISO | DPO

MSc OSCP ISO 27K

# Περιεχόμενα

SysteCom
MEMBER OF QNR GROUP

# Σκοπός της Παρουσίασης

SysteCom
MEMBER OF QNR GROUP

**Στόχος:**

Να κατανοήσουμε τις απειλές, να γνωρίσουμε καλύτερα την οδηγία NIS2 και να υιοθετήσουμε πρακτικά βήματα προστασίας!

## Γιατί μας αφορά;

Ο κλάδος καλλυντικών διαχειρίζεται δεδομένα πελατών, συνταγές, εμπορικά μυστικά και είναι μέρος της αλυσίδας εφοδιασμού.

## Τι μας είπατε εσείς;

Εφαρμόζουμε βασικά μέτρα χωρίς στρατηγική, χαμηλή εξοικείωση προσωπικού, ανησυχία για **διακοπή λειτουργίας** και **απώλεια δεδομένων**.

## Ποιους αφορά;

Η κυβερνοασφάλεια αφορά **ΟΛΟΥΣ** — ιδιοκτήτες, στελέχη, εργαζομένους.
Η οδηγία NIS2 καθιστά τη διοίκηση **προσωπικά υπεύθυνη**.

# Στατιστικά Κυβερνοεγκλήματος

SysteCom
MEMBER OF QNR GROUP

Καθημερινά σημειώνονται κυβερνοεπιθέσεις που μπορούν να προκαλέσουν σοβαρές απώλειες δεδομένων.

Ο κίνδυνος υπάρχει αλλά η δική μας προσοχή, ενημέρωση και σωστές πρακτικές είναι αυτά που κάνουν τη διαφορά.

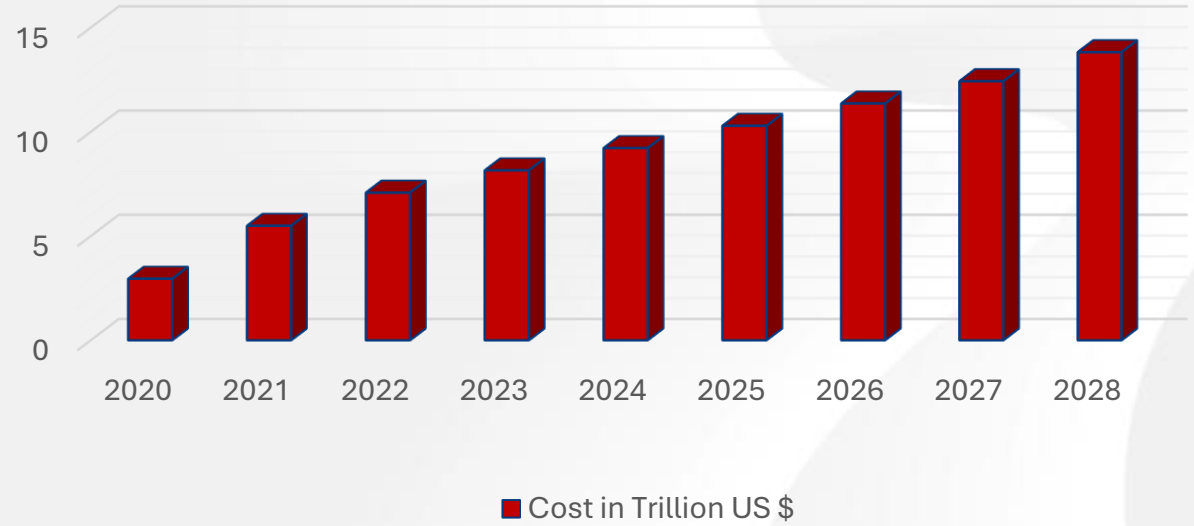
**101**

Ο συνολικός αριθμός ημερών για να εντοπισθεί μια κυβερνοεπίθεση.

**30%** αύξηση των επιθέσεων χρόνο με τον χρόνο τα τελευταία 5 χρόνια[1].

Η παγκόσμια ζημία από το κυβερνοέγκλημα προβλέπεται να φτάσει τα **11,36 τρισεκατομμύρια** δολάρια ετησίως μέχρι το 2026.

Αν μετρούταν ως GDP χώρας, τότε το κυβερνοέγκλημα θα ήταν η τρίτη μεγαλύτερη οικονομία στον κόσμο μετά τις Η.Π.Α. και την Κίνα[2].




Πηγή 1 : Checkpoint report [1]https://blog.checkpoint.com/research/a-closer-look-at-q3-2024-75-surge-in-cyber-attacks-worldwide/
Πηγή 2 : Cybercrime Magazine: 'https://cybersecurityventures.com//top-5-cybersecurity-facts-figures-predictions-and-statistics-for-2021-to-2025'

# Απειλές στον Κυβερνοχώρο

SysteCom
MEMBER OF QNR GROUP

Foresight

Cyber/Physical ecosystems exploited

Threats against data

Disinformation

Cross border SPOF

Hybrid Threats

Internet threats

Rise of surveillance

Ransomware

Threats Against Data

Complex Environments

Skills shortage

Targeted attacks

AI abuse

Space-based infrastructure

Supply-chain attacks

Social Engineering

Denial of Service

Malware

Πηγή: ENISA Threat Landscape 2024

# Ανερχόμενοι Κίνδυνοι Τεχνητής Νοημοσύνης

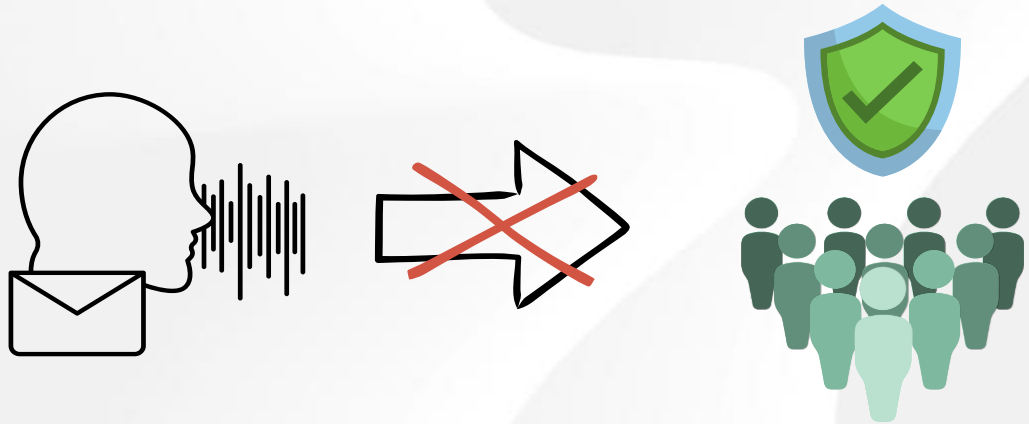
SysteCom
MEMBER OF QNR GROUP

- **Deepfakes ηχητικά ή βίντεο μηνύματα** που μιμούνται στελέχη ή συνεργάτες.
- **Απατηλά μηνύματα,** χωρίς λάθη και με φυσική γλώσσα.
- **Αυτοματοποιημένες απάτες,** όπου ένας επιτιθέμενος μπορεί να στοχεύσει πολλά άτομα ταυτόχρονα.
- **Ψεύτικες τηλεφωνικές κλήσεις ή chat υποστήριξης,** που φαίνονται πραγματικές.

## Γιατί είναι σημαντικό;

Επειδή όσο πιο πειστικές γίνονται οι επιθέσεις, τόσο πιο εύκολα μπορεί κάποιος να ξεγελαστεί.

Η προσοχή, η επιβεβαίωση και η τήρηση διαδικασιών είναι η **ΚΑΛΥΤΕΡΗ ΑΜΥΝΑ ΜΑΣ**.



# Ενδεικτικά Περιστατικά Ασφάλειας

SysteCom
MEMBER OF QNR GROUP

## Περιστατικό 1

Μεγάλος γαλλικός Όμιλος Καλλυντικών – από τους μεγαλύτερους παγκοσμίως - δέχθηκε επίθεση **ransomware**.

Η παραγωγή σταμάτησε πλήρως, οι εργαζόμενοι επέστρεψαν σπίτι.

## Τι είχε συμβεί;

Γνωστό hacking group κρυπτογράφησε τα συστήματα και ζήτησε λύτρα **$25 εκατ.** (τα οποία διπλασιάστηκαν σε $50 εκατ. μετά από μερικές μέρες).

Η παραγωγή επανήλθε σταδιακά μετά από σχεδόν **4 εβδομάδες**.

## Γιατί μας αφορά;

- ✓ Εταιρεία του **κλάδου** - καλλυντικά/φαρμακευτικά
- ✓ Κόστος: εβδομάδες **χαμένης παραγωγής**, ζημιά στη φήμη, κλοπή δεδομένων

# Ενδεικτικά Περιστατικά Ασφάλειας

SysteCom
MEMBER OF QNR GROUP

## Περιστατικό 2

Πολυεθνική Εταιρεία Καλλυντικών δέχθηκε **κυβερνοεπίθεση** που οδήγησε σε διαρροή εσωτερικών δεδομένων.

Αναγκάστηκε να κλείσει μέρος του δικτύου της.

## Τι είχε συμβεί;

Χάκερ **απέκτησαν πρόσβαση** στα εσωτερικά συστήματα και έκλεψαν εμπιστευτικά δεδομένα. Η εταιρεία αναγκάστηκε να **κλείσει τμήματα** του δικτύου, διακόπτοντας τη λειτουργία της.

## Γιατί μας αφορά;

- ✓ Ακόμα και οι **μεγαλύτεροι όμιλοι** ομορφιάς είναι ευάλωτοι
- ✓ Κλοπή δεδομένων = **ζημιά στο brand**, απώλεια εμπιστοσύνης πελατών
- ✓ Αν συμβεί σε εσάς: **πόσο γρήγορα θα ανακάμπτατε;**

# Ενδεικτικά Περιστατικά Ασφάλειας

SysteCom
MEMBER OF QNR GROUP

## Περιστατικό 3

Ο CFO γερμανικής εταιρείας δέχθηκε βιντεοκλήση **deepfake** - φαινομενικά από τον CEO - που ζητούσε επείγουσα μεταφορά κεφαλαίων.

Αποτέλεσμα: απώλεια **$$ εκατ.**

## Τι είχε συμβεί;

Με χρήση **AI**, οι επιτιθέμενοι αναπαρήγαγαν τη φωνή και την εικόνα του CEO σε πραγματικό χρόνο. Ο CFO πίστεψε ότι μιλούσε με τον πραγματικό διευθυντή και ενέκρινε τη συναλλαγή.

## Γιατί μας αφορά;

- ✓ Τα **deepfakes** κάνουν το **CEO Fraud** πιο πειστικό από ποτέ
- ✓ Πάντα **επιβεβαιώνουμε** μέσω 2ου καναλιού επικοινωνίας
- ✓ Μικρές εταιρείες = πιο εύκολος στόχος λόγω **λιγότερων ελέγχων**

# Οδηγία NIS2 & ν. 5160/2024

SysteCom
MEMBER OF QNR GROUP

## Τι είναι η NIS2 και γιατί αφορά τον κλάδο μας;

Η οδηγία **NIS2**, έχει ενσωματωθεί στο ελληνικό δίκαιο με τον **ν. 5160/2024**, επεκτείνει τους τομείς κυβερνοασφάλειας σε **χημικά, τρόφιμα, manufacturing** και εφοδιαστική αλυσίδα.

### Βασικοί Πυλώνες:

- **Διαχείριση κινδύνων** κυβερνοασφάλειας
- Αναφορά περιστατικών: **24 ώρες / 72 ώρες**
- Ασφάλεια **εφοδιαστικής αλυσίδας**
- **Ευθύνη διοίκησης** — προσωπική ευθύνη CEO

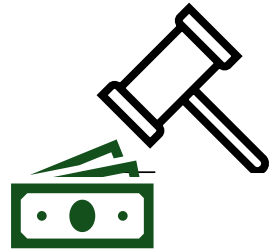

Πρόστιμα: **€10.000.000** ή 2% του ετήσιου τζίρου.
**Η Εθνική Αρχή Κυβερνοασφάλειας (NCSA) εποπτεύει και μπορεί να αναστείλει προσωρινά τη διοίκηση σε περίπτωση μη συμμόρφωσης.**

# Πυλώνες NIS2 & Υποχρεώσεις

SysteCom
MEMBER OF QNR GROUP

## Τι απαιτεί ο ν. 5160/2024

**Υπεύθυνος Ασφαλείας (ΥΑΣΠΕ):**
Ορισμός υπεύθυνου κυβερνοασφάλειας.
**Πολιτική Κυβερνοασφάλειας:**
Εγκεκριμένη από τη Διοίκηση εντός 3 μηνών.
**22 Ελεγκτικά Μέτρα:**
Τεχνικοί και οργανωτικοί έλεγχοι ασφαλείας.
**Ετήσια Εκπαίδευση:**
Υποχρεωτική για διοίκηση και εργαζομένους.



## Κυρώσεις & Ευθύνη

**Πρόστιμα:**
Έως €10 εκατ. ή 2% του τζίρου (Βασικές οντότητες κ 1,4% για Σημαντικές).
**Προσωπική Ευθύνη Διοίκησης:**
CEO/νόμιμος εκπρόσωπος ευθύνεται προσωπικά. Δυνατότητα προσωρινής απαγόρευσης άσκησης καθηκόντων.
**Εποπτεία NCSA:**
Η Εθνική Αρχή Κυβερνοασφάλειας διενεργεί ελέγχους και επιβάλλει κυρώσεις.

# Πρακτικά Βήματα για την Συμμόρφωση

SysteCom
MEMBER OF QNR GROUP

Πρακτικό **NIS2 Checklist** — Αυτά πρέπει να «απαιτήσετε» αύριο το πρωί:

**Ο σκοπός είναι διττός: Ασφάλεια & Κανονιστική Συμμόρφωση**

- Ορισμός Υπευθύνου Κυβερνοασφάλειας (ΥΑΣΠΕ / CISO)
- Πολιτικές Κυβερνοασφάλειας Εγκεκριμένες από την Διοίκηση
- Risk Assessment και εγκεκριμένο πλάνο περιορισμού των κινδύνων
- Τεχνικά μέτρα προστασίας
  - ✓ MFA παντού (ιδίως email, VPN, admin accounts)
  - ✓ Endpoint protection (EDR / όχι απλό antivirus)
  - ✓ Patch management (critical updates)
  - ✓ Backup (offline / immutable αν γίνεται)
  - ✓ Vulnerability Scan (Εσωτερικό & Εξωτερικό) / Ιδανικά και Τακτικό PenTest
- Διαχείριση Προμηθευτών & Έλεγχος πρόσβασης τρίτων (IT/ Εξωτερικοί)
- Ετήσια εκπαίδευση κυβερνοασφάλειας (Υποχρεωτική NIS2)
- Απόκριση σε περιστατικά & Reporting
- Security Monitoring (Managed SOC)

# Συμπεράσματα

SysteCom
MEMBER OF QNR GROUP

Η **κυβερνοασφάλεια** δεν είναι πολυτέλεια - είναι **επιχειρηματική αναγκαιότητα** και νομική υποχρέωση.

Το NIS2 φέρνει **πρόστιμα, ευθύνη διοίκησης** και υποχρεωτική αναφορά περιστατικών.

Εφαρμόζουμε άμεσα τα **8 πρακτικά βήματα.**

Η προστασία δεν ξεκινά από την τεχνολογία.
**Ξεκινά από Εμάς.**
***www.psvak.gr***

SysteCom
MEMBER OF QNR GROUP

# ΕΥΧΑΡΙΣΤΟΥΜΕ!

ΠΣΒΑΚ
ΠΑΝΕΛΛΗΝΙΟΣ ΣΥΝΔΕΣΜΟΣ
ΒΙΟΜΗΧΑΝΩΝ & ΑΝΤΙΠΡΟΣΩΠΩΝ
ΚΑΛΛΥΝΤΙΚΩΝ & ΑΡΩΜΑΤΩΝ

**Επικοινωνήστε μαζί μας:**

technology@systecom.gr 211 1809000