# NIS Directive

# Ενσωμάτωση στην Ελληνική Νομοθεσία Απαιτήσεις Συμμόρφωσης

PRIORITY Consultants

# Νομικό και κανονιστικό πλαίσιο

## 2016

**Οδηγία 2016/1148 ΕΕ**

Το 2016 εκδίδεται από την ΕΕ Οδηγία σε σχέση με τις υποχρεώσεις των παρόχων βασικών υπηρεσιών και ψηφιακών υπηρεσιών

## 2018

**Νόμος 4577/2018**

Το 2018 εκδίδεται από το Ελληνικό κράτος ο νόμος 4577 μέσω του οποίου ενσωματώνεται η οδηγία 2016/1148

**Εκτελεστικός κανονισμός ΕΕ 2018/151**

Το 2018 εκδίδεται από την ΕΕ εκτελεστικός κανονισμός που θεσπίζει οδηγίες για την εφαρμογή της ΕΕ 2016/148

## 2019

**Απόφαση 1027/2019**

Το 2019 εκδίδεται η απόφαση 1027 μέσω της οποίας προσδιορίζονται οι βασικές απαιτήσεις Ασφάλειας

**Σκοπός νομοθετικού πλαισίου**

Διασφάλιση της ομαλής λειτουργίας των Φορέων Εκμετάλλευσης Βασικών Υπηρεσιών και των Παρόχων Ψηφιακών Υπηρεσιών και εξασφάλιση της συνέχειας των υπηρεσιών που παρέχουν

# Βασικές απαιτήσεις της Ευρωπαϊκής οδηγίας

**Εθνική Στρατηγική**

Δημιουργία εθνικής στρατηγικής για την ασφάλεια δικτύων και πληροφοριών. Η στρατηγική θα πρέπει να αποτυπωθεί στην εθνική νομοθεσία του κράτους μέλους

**Οργανωτικό πλαίσιο**

Δημιουργία οργανωτικού πλαισίου για την υλοποίησης της στρατηγικής

**Παρακολούθηση υλοποίησης**

Καθορισμός των αρμόδιων οργανισμών που σκοπό θα έχουν την παρακολούθηση της υλοποίησης των οριζόμενων στην οδηγία

**Αντιμετώπιση κυβερνοεπιθέσεων**

Ανάπτυξη μίας ή περισσότερων ομάδων αντιμετώπισης κυβερνοεπιθέσεων (CSIRT)

# Φορείς εκμετάλλευσης βασικών υπηρεσιών
## Κριτήρια προσδιορισμού

**01**

Ο φορέας να παρέχει υπηρεσία ουσιώδη για τη διατήρηση κρίσιμων κοινωνικών ή και οικονομικών δραστηριοτήτων

**02**

Η παροχή της υπηρεσίας αυτής να στηρίζεται σε συστήματα δικτύου και πληροφοριών

**03**

Η πρόκληση σοβαρής διατάραξης της παροχής της εν λόγω υπηρεσίας από τυχόν συμβάν

# Ψηφιακές υπηρεσίες

**01**

Υπηρεσίες επιγραμμικής αγοράς (online marketplace)*

**02**


Υπηρεσίες Online search

**03**


Υπηρεσίες cloud computing

*Οι επιγραμμικές αγορές επιτρέπουν στους καταναλωτές και στους εμπόρους να συνάπτουν επιγραμμικές συμβάσεις πώλησης ή παροχής υπηρεσιών με εμπόρους, και αποτελούν τον τελικό προορισμό για τη σύναψη των εν λόγω συμβάσεων.

# Σκοπός της απόφασης

# Γενικοί όροι και υποχρεώσεις

**Συνεργάτες είναι φυσικά ή νομικά πρόσωπα που χρησιμοποιούνται για την κατασκευή, συντήρηση ή λειτουργία συστημάτων δικτύου και πληροφοριών για την παροχή των βασικών υπηρεσιών**

Κάθε ΦΕΒΥ ή ΠΨΥ οφείλει να λαμβάνει όλα τα κατάλληλα τεχνικά και οργανωτικά μέτρα

**Τεχνικά και οργανωτικά μέτρα**

Κάθε ΦΕΒΥ ή ΠΨΥ ευθύνεται για το σύνολο των πράξεων οποιουδήποτε συνεργάτη

**Ευθύνες πράξεων συνεργατών**

Κάθε ΦΕΒΥ ή ΠΨΥ οφείλει να συνεργάζεται με τις αρμόδιες αρχές για την επίλυση περιστατικών και τον περιορισμό του αντικτύπου των επιπτώσεών τους

**Επίλυση περιστατικών**

ΦΕΒΥ: Φορέας Εκμετάλλευσης Βασικών Υπηρεσιών
ΠΨΥ : Πάροχος Ψηφιακών Υπηρεσιών
Οργανισμός : ΦΕΒΥ ή ΠΨΥ

# Ενιαία Πολιτική Ασφάλειας

- Κάθε Οργανισμός θεσπίζει, υλοποιεί και διατηρεί επίκαιρη και καταγεγραμμένη Πολιτική Ασφαλείας σχετικά με την ασφάλεια των συστημάτων δικτύου και πληροφοριών
- Η Πολιτική Ασφάλειας του Οργανισμού οφείλει να καλύπτει τουλάχιστον όσα ορίζει η Ενιαία Πολιτική Ασφάλειας*

* Η Ενιαία Πολιτική Ασφάλειας ορίζεται από την Εθνική Αρχή Κυβερνοασφάλειας

# Βασικές Απαιτήσεις Ασφάλειας

## Επιλογή μέτρων ασφάλειας

Προκειμένου να επιλεγούν και να εφαρμοστούν μέτρα που ικανοποιούν τις βασικές απαιτήσεις ασφάλειας, ενθαρρύνεται η **χρήση διεθνώς αποδεκτών προτύπων**, προδιαγραφών και οδηγών που σχετίζονται με την ασφάλεια των συστημάτων δικτύων και πληροφοριών

# Υπεύθυνος Ασφάλειας Πληροφοριών και Δικτύων

- Κάθε Οργανισμός οφείλει να ορίσει Υπεύθυνο Ασφάλειας Πληροφοριών και Δικτύων

- Ο Υπεύθυνος Ασφάλειας Πληροφοριών και Δικτύων
  - Αποτελεί το σημείο επαφής με την Εθνική Αρχή Κυβερνοασφάλειας και το αρμόδιο CSIRT
  - Συνεργάζεται με την Εθνική Αρχή Κυβερνοασφάλειας και με το αρμόδιο CSIRT
  - Συντονίζει και επιβλέπει τον Οργανισμό ως προς τις υποχρεώσεις που απορρέουν από τον ν. 4577/2018
  - Εποπτεύει την υλοποίηση της Ενιαίας Πολιτικής Ασφάλειας
  - Εποπτεύει την εκπαίδευση και ευαισθητοποίηση των υπαλλήλων του Οργανισμού σε θέματα ασφάλειας πληροφοριών και δικτύων
  - Εποπτεύει τη σύνταξη της αναφοράς αυτοαξιολόγησης του Οργανισμού που αποστέλλεται στην Εθνική Αρχή Κυβερνοασφάλειας
  - Παρίσταται στους ελέγχους που πραγματοποιεί η Ομάδα Επιθεώρησης Ελέγχου, όπως αυτή ορίζεται από την Εθνική Αρχή Κυβερνοασφάλειας

## Κριτήρια προσδιορισμού σοβαρής διατάραξης για ΦΕΒΥ

- Κάθε συμβάν κατά το οποίο η συνέχεια της υπηρεσίας που παρέχεται από τον φορέα επηρεάζεται για πάνω από 100.000 χρηστοώρες
- Κάθε συμβάν που επηρεάζει πληθυσμό τουλάχιστον 50.000 χρηστών
- Απειλή σε ανθρώπινη ζωή. Σε περίπτωση απώλειας ανθρώπινης ζωής το συμβάν κρίνεται αυτομάτως κοινοποιήσιμο
- Το συμβάν έχει προκαλέσει υλικές ζημιές στον ίδιο τον φορέα ή σε άλλους φορείς που υπερβαίνουν το 1.000.000 ευρώ

## Κριτήρια προσδιορισμού σοβαρής διατάραξης για ΠΨΥ

- Η υπηρεσία που παρέχεται από πάροχο ψηφιακών υπηρεσιών δεν ήταν διαθέσιμη για περισσότερες από 5.000.000 χρηστοώρες (ο όρος χρηστοώρα αναφέρεται στο πλήθος των θιγόμενων χρηστών στην Ένωση επί χρονικό διάστημα εξήντα λεπτών)

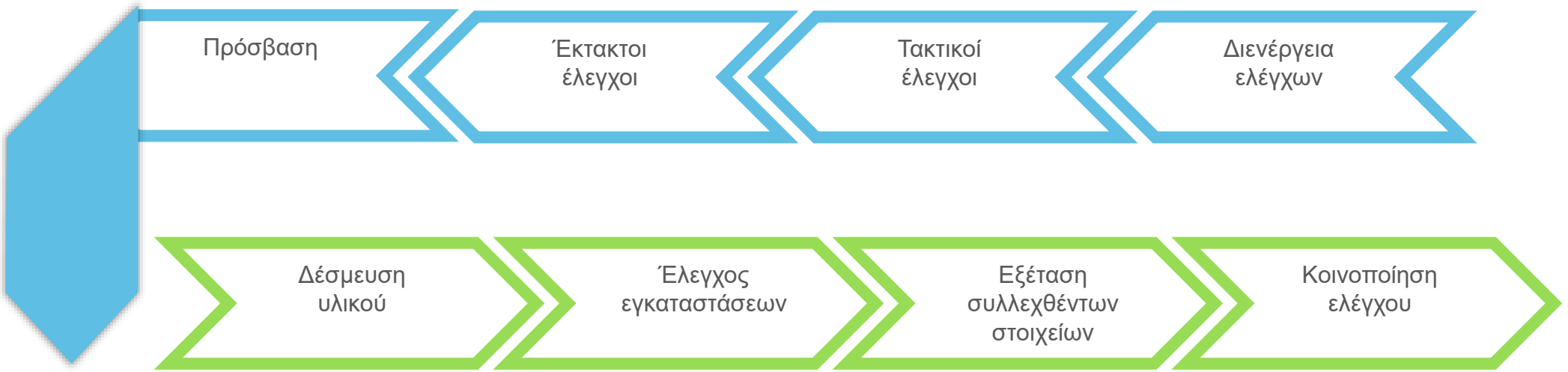
- Το συμβάν είχε ως αποτέλεσμα την απώλεια της ακεραιότητας, της αυθεντικότητας, ή της εμπιστευτικότητας των αποθηκευμένων ή μεταδοθέντων ή των επεξεργασμένων δεδομένων ή τις συναφείς υπηρεσίες που προσφέρονται ή είναι προσβάσιμες μέσω συστήματος δικτύου και πληροφοριών του παρόχου ψηφιακών υπηρεσιών, επηρεάζοντας περισσότερους από 100.000 χρήστες εντός της Ένωσης

- Το συμβάν προκάλεσε κίνδυνο για τη δημόσια ασφάλεια, τη δημόσια προστασία ή κίνδυνο απώλειας ανθρώπινων ζωών

- Το συμβάν έχει προκαλέσει υλικές ζημίες σε τουλάχιστον έναν χρήστη στην Ένωση, εφόσον η ζημία που προκλήθηκε στον εν λόγω χρήστη υπερβαίνει το 1.000.000 ευρώ

# Κοινοποίηση συμβάντος ασφάλειας

# Διαδικασία ελέγχου



# Κυρώσεις

Οι διοικητικές κυρώσεις που είναι δυνατόν να επιβληθούν είναι:

- Σύσταση προς τον Οργανισμό ή τον νόμιμο εκπρόσωπό τους, σε περίπτωση που, κατόπιν διενέργειας ελέγχου ή συνδρομή συμβάντος ασφαλείας, αναγνωριστεί ότι δεν τηρούνται τα απαιτούμενα από το νόμο μέτρα ασφαλείας

- Επίπληξη προς τον Οργανισμό ή τον νόμιμο εκπρόσωπό τους, σε περίπτωση που κατόπιν διενέργειας ελέγχου ή συνδρομή συμβάντος ασφαλείας, αναγνωριστεί ότι παρά την πρότερη σύσταση της αρχής δεν συμμορφώθηκαν με τις υποδείξεις της ΕΑΚ

- Στην περίπτωση μη συμμόρφωσης του Οργανισμού με την διαδικασία σύστασης η επίπληξης, επιβάλλεται διοικητικό πρόστιμο στον Οργανισμό σύμφωνα με τις διατάξεις του άρθρου 15 του ν. 4577/2018

# Κυρώσεις

| Απουσία κοινοποίησης ή κοινοποίηση με αδικαιολόγητη καθυστέρηση συμβάντος με σοβαρό αντίκτυπο | Απουσία εφαρμογής κατάλληλων και αναλογικών τεχνικών και οργανωτικών, προληπτικών μέτρα για τη διαχείριση κινδύνων ασφάλειας | Σε περίπτωση που φυσικό ή νομικό πρόσωπο δεν παρέχει ή παρέχει με αδικαιολόγητη καθυστέρηση πληροφορίες που ζητούνται κατά τη διενέργεια ελέγχου ή διερεύνηση περιστατικού |
|---|---|---|
| • Πρόστιμο μέχρι του ποσού των 15.000€ με σύσταση για συμμόρφωση και προειδοποίηση επιβολής περαιτέρω κυρώσεων<br>• Πρόστιμο μέχρι του ποσού των 200.000€ σε περίπτωση υποτροπής | • Πρόστιμο μέχρι του ποσού των 50.000€ με σύσταση για συμμόρφωση και προειδοποίηση επιβολής περαιτέρω κυρώσεων<br>• Πρόστιμο μέχρι του ποσού των 200.000€ σε περίπτωση υποτροπής | • Πρόστιμο μέχρι του ποσού των 50.000€ με σύσταση για συμμόρφωση και προειδοποίηση επιβολής περαιτέρω κυρώσεων<br>• Πρόστιμο μέχρι του ποσού των 200.000€ σε περίπτωση υποτροπής |

# Επιθέσεις σε κρίσιμες υποδομές

## 2010 Stuxnet Worm on Iranian Nuclear Centrifuges

| | |
|---|---|
| **Description & Event Timeline** | ▪ Targeted Iranian nuclear facility Siemens PLCs<br>▪ Increased centrifuge speed causing component damage<br>▪ Inadvertently spread outside facility network |
| **Adversary Sophistication** | Very High |
| **Corruption Vector** | USB drive exploiting Zero-Day flaw in Windows Operating system |
| **Effected Technology & Components** | 1. Corrupted USB flash drive introduced<br>2. Worm executes attack payload<br>3. Link file executes and propagates copies of worm<br>4. Rootkit hides malicious files/processes to prevent detection<br>5. Centrifuges over spin & tear themselves apart |
| **Consequences** | Destroyed ~20% of Iran's nuclear centrifuges |

# Επιθέσεις σε κρίσιμες υποδομές

## 2011-13 Port of Antwerp Drug Smuggling Hack

| | |
|---|---|
| **Description & Event Timeline** | Used combination of software & hardware hacks to obtain shipping containers' schedules and access PINs |
| **Adversary Sophistication** | High: professional hackers |
| **Corruption Vector** | Email, Physical ports |
| **Effected Technology & Components** | 1. Phishing emails<br>2. pwnies (Linux computer running Metasploit software, connected to cellular network, disguised as power strip)<br>3. Key-logging devices to capture keystrokes and screen grabs |
| **Consequences** | ▪ Drug traffickers obtained schedules and PINs to access shipping containers containing drugs<br>▪ Extracted drugs before container transportation |

# Επιθέσεις σε κρίσιμες υποδομές

## 2017 Maersk Ransomware

| | |
|---|---|
| **Description & Event Timeline** | Petya/NotPetya/Nyetyea family of ransomware/malware affecting numerous corporate networks globally, including company A.P. Moller-Maersk |
| **Adversary Sophistication** | High: Russia (unconfirmed) using leaked NSA |
| **Corruption Vector** | Flaw in Windows OS |
| **Effected Technology & Components** | 1. Ransomware/ malware (IT software targeting operating system)<br>2. Virus embedded in Ukrainian accounting software update<br>3. Used flaw in Windows OS to lock systems & demand ransome |
| **Consequences** | ▪ $300M<br>▪ 2000 computers affected worldwide<br>▪ 17 Maersk shipping container terminals closed for 48 hours |

# Πλαίσιο Διακυβέρνησης

| | IT | IT & OT | OT |
|---|---|---|---|
| Standard | **ISO**<br>ISO 27001: Information Security Management Standard<br><br>**COBIT**<br>A Business Framework for the Governance & Management of Enterprise. | **NIST**<br>SP 800-160 Systems Security Engineering<br><br>**NIST**<br>SP 800-53 Security & Privacy Controls for Federal Information Systems & Organizations | **ISA/IEC**<br>ISA/IEC 62443 Industrial Network & System Security<br><br>**NIST**<br>SP 800-82 Guide to Industrial Control Systems Security |
| Best Practice | **CIS**<br>Top 20 Critical Security Controls<br><br>**ISF**<br>Standard of Good Practice for Information Security | **NIST**<br>Maritime Bulk Liquids Transfer Cybersecurity Framework Profile<br>**BIMCO**<br>Guidelines on Cyber Security Onboard Ships<br>**IMO**<br>Interim Guidelines on Maritime Cyber Risk Management | **ABS**<br>Cybersecurity Principles to Marine & Offshore Operations |

# Αντιμετώπιση Κινδύνων

# Διασφάλιση Επιχειρησιακής Συνέχειας


THANK
YOU