

Security of Network & Information Systems (NIS 2) – Πολιτικές Ασφαλείας

Δρ. Φώτιος Γκιουλέκας

Μεταδιδάκτορας Πληροφορικής ΑΠΘ

Μέλος της Εθελοντικής Ομάδας ENISA E-Health Security Experts



ARISTOTLE
UNIVERSITY
OF THESSALONIKI

GOOGLE.ORG
CYBERSECURITY
SEMINARS

Σύνοψη

- Ενσωμάτωση της Οδηγίας NIS2 στην Ελληνική Νομοθεσία
 - Ν. 5160/2024 – NIS2
 - ΥΑ 1899/2025 – Προσόντα, Καθήκοντα & Ασυμβίβαστο του ΥΑΣΠΕ
 - KYA 1689/2025 - Εθνικό Πλαίσιο Απαιτήσεων Κυβερνοασφάλειας
- Διαδικασία Συμμόρφωσης Οντότητας ως προς NIS2
- Οργάνωση Πολιτικών Ασφαλείας, Οδηγοί & Πρακτικές
 - Παραδείγματα Εφαρμογής και Πρακτικές Συμβουλές
- Διαχείριση Περιστατικού Κυβερνοασφάλειας – Κύκλος Ζωής

Κάθε συμβάν ασφαλείας (event) δεν αποτελεί πάντα ένα περιστατικό (incident)!

Ελληνική Νομοθεσία

N. 4577, ΦΕΚ Α'
199/03.12.2018 -
NIS 1: Ενσωμάτωση
στην Ελληνική
νομοθεσία της
Οδηγίας
2016/1148/EE ([link](#))

N. 5160/2024, ΦΕΚ Α'
195/27.11.2024 - NIS 2:
Ενσωμάτωση στην
Ελληνική νομοθεσία της
Οδηγίας 2022/2555/ΕΕ
([link](#))

KYA 1689/2025, ΦΕΚ Β'
2186/06.05.2025: Εθνικό
Πλαίσιο Απαιτήσεων
Κυβερνοασφάλειας Βασικών
και Σημαντικών Οντοτήτων
([link](#))

KYA 1990 /2025, ΦΕΚ Β' 4241/04.08.2025 :
Δημιουργία Ψηφιακής
πλατφόρμας για την
εγγραφή των βασικών και
των σημαντικών οντοτήτων
([link](#))

ΥΑ 1899/2025, ΦΕΚ Β'
4250/05.08.2025:
Καθορισμός προσόντων,
καθηκόντων,
ασυμβιβάστων και
υποχρεώσεων των
Υπεύθυνων Ασφαλείας
Συστημάτων
Πληροφορικής και
Επικοινωνιών ([link](#))

Τι είναι η NIS2 τελικά; Πως Προέκυψε;

- Η Οδηγία NIS2 (ΕΕ 2022/2555) για μέτρα υψηλού κοινού επιπέδου κυβερνοασφάλειας σε ολόκληρη την Ένωση) αποτελεί τη βασική νομοθεσία της Ευρωπαϊκής Ένωσης για την κυβερνοασφάλεια, εστιάζοντας στην προστασία κρίσιμων υποδομών
- Καθορίζει νομικά μέτρα για την ενίσχυση της ασφάλειας με ένα αυξημένο επίπεδο κυβερνοασφάλειας στην ΕΕ
- Τα κράτη μέλη την ενσωμάτωσαν στο εθνικό τους δίκαιο έως την 17^η Οκτωβρίου 2024

▪ Προέκυψε γιατί:

- Η NIS1 είχε περιορισμένο πεδίο εφαρμογής και ασάφειες, με αποτέλεσμα να υπάρχουν ανισότητες στην εφαρμογή της μεταξύ των κρατών μελών
- Η ολοένα αυξανόμενες επιθέσεις σε κρίσιμες υποδομές με ιδιαίτερα εξελιγμένους τρόπους (π.χ. ransomware) οριοθετούν ενιαία και αυστηρότερα πρότυπα προστασίας.
- Οι αλυσίδες εφοδιασμού & οι ψηφιακές υπηρεσίες είναι πλέον διεθνείς και διασυνδεδεμένες. Ένα πρόβλημα σε ένα σημείο σε μια χώρα μπορεί να επηρεάσει ολόκληρη την ΕΕ



Η Οδηγία NIS2 στην Ελλάδα μέσα από τη Νομοθεσία - Γενικές Διατάξεις

- Αντικείμενο (Αρθ. 1 της Οδηγίας NIS2):
- Ορίζεται η Εθνική Αρχή Κυβερνοασφάλειας – **EAK**:
 - Διαχείριση κυβερνοκρίσεων
 - Ενιαίο σημείο επαφής για την κυβερνοασφάλεια & ομάδων απόκρισης για συμβάντα που αφορούν στην ασφάλεια υπολογιστών (**Computer Security Incident Response Team - CSIRT**)
 - Κατάρτιση Εθνικού Σχεδίου αντιμετώπισης
- Καθορίζονται μέτρα διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας και η **υποχρέωση υποβολής αναφορών**
- Προβλέπει κανόνες και υποχρεώσεις σχετικά με την **ανταλλαγή πληροφοριών** για την κυβερνοασφάλεια
- Θέσπιση διατάξεων για την εν γένει εποπτεία και επιβολή μέτρων και κυρώσεων για την εφαρμογή της NIS2

The screenshot shows the official website of the Greek National Cybersecurity Authority (ΕΑΚ). The top navigation bar includes links for the Greek Parliament (ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ), the Law (Οδηγία NIS2), Alerts (Alerts), NCC/ECCC, EL CSIRT, Test Υπηρεγίας NIS2, and Αναφορά Συμβάντος. Below the navigation is the logo of the National Cybersecurity Authority (ΕΘΝΙΚΗ ΑΡΧΗ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ) and a menu with links for Αρχική, ΕΑΚ, Κυβερνοπιθέσεις, Αντιμετώπιση Απειλών – Συστάσεις, Νομοθεσία, and Νέα – Πληροφορίες.

The main content area features a large banner for "NIS2" (Ενσωμάτωση της Ευρωπαϊκής Οδηγίας 2022/2555 για την Κυβερνοασφάλεια). To the right of the banner is a list of key points:

- Ο νέος εφαρμοστικός νόμος για την κυβερνοασφάλεια στην Ελλάδα
- Εθνικό πλαίσιο απαιτήσεων κυβερνοασφάλειας για βασικές & σημαντικές οντότητες
- Πολιτικές κυβερνοασφάλειας
- Πεδίο εφαρμογής και Εργαλείο καθοδήγησης
- Συγκέντρωσης

Below the banner are three blue boxes with links:

- Εγγραφή Οντοτήτων στο Μητρώο ΕΑΚ** (Εγγραφή Βασικών και Σημαντικών Οντοτήτων μέσω του gov.gr)
- Η Οδηγία NIS2 στην Ελλάδα** (ΕΝΗΜΕΡΩΤΙΚΟ ΦΥΛΛΑΔΙΟ: Οδηγός Αναφοράς ν.5160/2024 για την κυβερνοασφάλεια)
- Εργαλείο Καθοδήγησης** (ΤΕΣΤ ΥΠΑΓΟΥΜΕΝΗΣ: Μάθετε εάν ο φορέας σας, εμπίπτει στο πεδίο εφαρμογής της Οδηγίας NIS2)

<https://www.cyber.gov.gr/>

Πεδίο εφαρμογής: Άρθρο 2 της NIS2 - I

- Εφαρμόζεται σε Δημόσιες ή Ιδιωτικές Οντότητες
 - Οι κρίσιμες υποδομές, επιχειρήσεις, φορείς και οργανισμοί αναφέρονται ως «οντότητες»
 - παρέχουν τις υπηρεσίες τους ή ασκούν τις δραστηριότητές τους εντός της Ένωσης
- Αφορά μεγάλες και μεσαίες επιχειρήσεις που δραστηριοποιούνται σε κρίσιμους τομείς όπως οι Δημόσιοι οργανισμοί & οι Φορείς παροχής ψηφιακών υπηρεσιών (cloud, data centers, DNS, υπηρεσίες social media)
- Εισάγονται οι όροι «Βασικές Οντότητες (Essential Entities) - παρέχουν υπηρεσίες ζωτικής σημασίας για τη λειτουργία της κοινωνίας & της οικονομίας» και «Σημαντικές Οντότητες (Important Entities) – μη κρίσιμες αλλά με σημαντική επίδραση» για να οριοθετήσει:
 - τον βαθμό κρισιμότητας των υπηρεσιών που προσφέρουν
 - την επίπτωση που μπορεί να έχει ένα κυβερνοπεριστατικό
 - την προτεραιότητα εποπτείας από τις αρμόδιες αρχές (ΕΑΚ)

Πεδίο εφαρμογής: Άρθρο 2 της NIS2 - II

Βασικές Οντότητες			
 Ενέργεια	 Υγεία	 Διαχείριση υπηρεσιών ΤΠΕ (μεταξύ επιχειρήσεων)	
 Μεταφορές	 Πόσιμο νερό	 Οντότητες δημόσιας διοίκησης	
 Τράπεζες	 Λύματα	 Διάστημα	
 Υποδομές χρηματοπιστωτικών αγορών	 Ψηφιακές υποδομές		

Σημαντικές Οντότητες			
 Ταχυδρομικές υπηρεσίες και υπηρεσίες ταχυμεταφορών	 Παραγωγή, μεταποίηση και διανομή τροφίμων	 Έρευνα	
 Διαχείριση αποβλήτων	 Κατασκευαστικός τομέας		ΟΤΑ α' και β' βαθμού
 Παρασκευή, παραγωγή και διανομή χημικών προϊόντων	 Ψηφιακοί πάροχοι		

Παραρτήματα I & II του Ν. 5160/2024

Πηγή: [Οδηγός Αναφοράς v.5160/2024 για την κυβερνοασφάλεια](#)

Πεδίο εφαρμογής: Άρθρο 2 της NIS2 - II

- Αφορά οργανισμούς που χαρακτηρίζονται ως μεσαίες επιχειρήσεις σύμφωνα με την παρ. 1 του άρθρου 2 του Παραρτήματος της Σύστασης 2003/361/ΕΚ της Επιτροπής, της 6ης Μαΐου 2003, σχετικά με τον ορισμό των πολύ μικρών, των μικρών και των μεσαίων επιχειρήσεων (L 124), ή υπερβαίνουν τα ανώτατα όρια για τις μεσαίες επιχειρήσεις και οι οποίες είναι εγκατεστημένες ή παρέχουν τις υπηρεσίες τους ή ασκούν τις δραστηριότητές τους εντός της ελληνικής επικράτειας

Κατηγορία Επιχείρησης	Αριθμός απασχολούμενων	Ετήσιος κύκλος εργασιών	<ή>	Ετήσιος συνολικός Ισολογισμός
Μεσαία 	<250	KAI $\leq \text{€ 50 εκατ.}$	<ή>	$\leq \text{€ 43 εκατ.}$
Μικρή 	<50	$\leq \text{€ 10 εκατ.}$	<ή>	$\leq \text{€ 10 εκατ.}$
Πολύ Μικρή 	<10	$\leq \text{€ 2 εκατ.}$	<ή>	$\leq \text{€ 2 εκατ.}$

- Οι Μικρές επιχειρήσεις γενικά εξαιρούνται, εκτός αν παρέχουν υπηρεσίες ζωτικής σημασίας ή κρίσιμες τεχνολογίες. Αν μια εταιρεία παρέχει υποδομή σε άλλες οντότητες NIS2 (π.χ. cloud provider για Πληροφοριακό Σύστημα Νοσοκομείου), τότε υπάγεται και αυτή στη NIS2.

Πεδίο εφαρμογής: Άρθρο 2 της NIS2 - III

- Καθορισμός Υπαγωγής στη NIS2 σε 3 Βήματα

Είναι η επιχείρηση
μεσαία ή μεγάλη;

Ανήκει η
επιχείρηση σε
τομέα που
καλύπτει η NIS2
(Βασική ή
Σημαντική
Οντότητα);

Που είναι
εγκατεστημένη η
επιχείρηση (Έδρα
στην ΕΕ ή παροχή
υπηρεσιών στην
ΕΕ);

«Έλεγχος υπαγωγής στο
πεδίο εφαρμογής της NIS2
στην Ιστοσελίδα της ΕΑΚ»

Η εφαρμογή του νόμου εκκινεί από την 27^η Νοεμβρίου
2026 για τους ΟΤΑ Α' βαθμού [KYA B' 5472/14.10.2025](#)

Η ΕΑΚ κοινοποιεί στην Ευρωπαϊκή Επιτροπή
τα ονόματα των βασικών και σημαντικών
οντοτήτων ανά 2 έτη μέσω της ψηφιακή της
πλατφόρμα καταλόγου οντοτήτων (Όνομα, IP
range, email, phone number, Domain Name)!

Υπαγωγή στη NIS2

- Ανεξαρτήτως μεγέθους, βασικές οντότητες αποτελούν οι:
 - πάροχοι υπηρεσιών εμπιστοσύνης και μητρώα ονομάτων τομέα ανωτάτου επιπέδου, καθώς και πάροχοι υπηρεσιών συστήματος ονομάτων τομέα (DNS)
 - πάροχοι δημόσιων δικτύων ηλεκτρονικών επικοινωνιών ή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών που χαρακτηρίζονται ως μεσαίες επιχειρήσεις
 - οντότητες δημόσιας διοίκησης που εντάσσονται στους φορείς της κεντρικής κυβέρνησης
 - οντότητες που προσδιορίζονται ως κρίσιμες οντότητες βάσει της Οδηγίας (ΕΕ) 2022/2557 (Δήμοι, Ψηφιακές υποδομές, Πάροχοι Ενέργειας, κτλ.)
 - οντότητες που αναγνωρίστηκαν, σύμφωνα με το ν. 4577/2018, ως φορείς εκμετάλλευσης βασικών Υπηρεσιών (NIS1) (Νοσοκομεία, ΕΥΔΑΘ, κτλ.)

Εξαιρέσεις Υπαγωγής στην Οδηγία NIS2

- Δεν εφαρμόζεται σε οντότητες δημόσιας διοίκησης που ασκούν τις δραστηριότητές τους στους τομείς της εθνικής ασφάλειας, της δημόσιας τάξης, της άμυνας ή της επιβολής του νόμου, συμπεριλαμβανομένων της πρόληψης, της διακρίβωσης, της διαπίστωσης και της δίωξης ποινικών αδικημάτων
- Όταν μια οντότητα ενεργεί ως πάροχος υπηρεσιών εμπιστοσύνης (π.χ. πιστοποιητικά για ηλεκτρονικές υπογραφές, για ηλεκτρονικές σφραγίδες, γνησιότητας ιστοτόπων ή για την παροχή άλλων υπηρεσιών εμπιστοσύνη - <https://digital-strategy.ec.europa.eu/el/faqs/questions-answers-trust-services-under-european-digital-identity-regulation> - αυστηρότερες υποχρεώσεις μέσω του Κανονισμού eIDAS – EE 910/2014- electronic IDentification, Authentication and trust Services)
- Δεν εφαρμόζεται σε οντότητες τις οποίες η Ελλάδα εξαιρεί από το πεδίο εφαρμογής του Κανονισμού της NIS2 οργανισμούς σχετικά με την ψηφιακή επιχειρησιακή ανθεκτικότητα του χρηματοοικονομικού τομέα (π.χ. πιστωτικά ιδρύματα), οι οποίες όμως επιβάλουν τουλάχιστον ισοδύναμες απαιτήσεις με τη NIS2 για την Κυβερνοασφάλεια & CSIRT (Κανονισμός DORA - Digital Operational Resilience Act - ΕΕ 2022/2554)
- Γενικά δεν εφαρμόζονται σωρευτικά οι διατάξεις του νόμου εφόσον υπάρχει ισοδύναμη τομεακή νομοθεσία της ΕΕ και αντίστοιχη εθνική εναρμόνιση. Πρόκειται για πρόβλεψη που αποσκοπεί στην αποφυγή επικάλυψης ρυθμίσεων και περιπτών διοικητικών βαρών.

Ορισμοί: Άρθρο 6 της Οδηγίας NIS2 (Συνοπτικά) - I

- **Δικτυακό και Πληροφοριακό Σύστημα:**
 - I. **Δίκτυο ηλεκτρονικών επικοινωνιών:** τα συστήματα μετάδοσης και, κατά περίπτωση, ο εξοπλισμός μεταγωγής ή δρομολόγησης και οι λοιποί πόροι που επιτρέπουν τη μεταφορά σημάτων, με τη χρήση καλωδίου, ραδιοσημάτων, οπτικού ή άλλου ηλεκτρομαγνητικού μέσου, συμπεριλαμβανομένων των δορυφορικών δικτύων, των σταθερών (μεταγωγής δεδομένων μέσω κυκλωμάτων και πακετομεταγωγής, συμπεριλαμβανομένου του διαδικτύου) και κινητών επίγειων δικτύων, των συστημάτων ηλεκτρικών καλωδίων, εφόσον χρησιμοποιούνται για τη μετάδοση σημάτων, των δικτύων που χρησιμοποιούνται για ραδιοτηλεοπτικές εκπομπές, καθώς και των δικτύων καλωδιακής τηλεόρασης, ανεξάρτητα από το είδος των μεταφερόμενων πληροφοριών
 - II. **κάθε συσκευή ή ομάδα διασυνδεδεμένων ή συναφών συσκευών, μία ή περισσότερες από τις οποίες, σύμφωνα με ένα πρόγραμμα, διενεργούν αυτόματη επεξεργασία ψηφιακών δεδομένων**
 - III. **ψηφιακά δεδομένα που αποθηκεύονται, υποβάλλονται σε επεξεργασία, ανακτώνται ή μεταδίδονται από στοιχεία που καλύπτονται για τους σκοπούς της λειτουργίας, χρήσης, προστασίας και συντήρησής τους**
- **Ασφάλεια συστημάτων δικτύου και πληροφοριακών συστημάτων:** η ικανότητα των συστημάτων δικτύου και πληροφοριακών συστημάτων να ανθίστανται, σε δεδομένο επύπεδο εμπιστοσύνης, σε κάθε συμβάν που ενδέχεται να θέσει σε κίνδυνο τη διαθεσιμότητα, την αυθεντικότητα, την ακεραιότητα ή την εμπιστευτικότητα των αποθηκευμένων, διαβιβαζόμενων ή επεξεργασμένων δεδομένων ή των υπηρεσιών που προσφέρονται από τα εν λόγω συστήματα δικτύου και πληροφοριακών συστημάτων ή είναι προσβάσιμες μέσω αυτών
- **Κυβερνοασφάλεια:** οι δραστηριότητες που απαιτούνται για την προστασία των συστημάτων δικτύου και πληροφοριών, των χρηστών των εν λόγω συστημάτων και άλλων επηρεαζόμενων από κυβερνοαπειλές προσώπων (άρθρ. 2 του Κανονισμού ΕΕ 2019/881)

Ορισμοί: Άρθρο 6 της Οδηγίας NIS2 (Συνοπτικά) - II

- **Εθνική Στρατηγική Κυβερνοασφάλειας:** συνεκτικό πλαίσιο το οποίο παρέχει στρατηγικούς στόχους και προτεραιότητες στον τομέα της κυβερνοασφάλειας και τη διακυβέρνηση για την επίτευξή τους
- **Παρ' ολίγον Περιστατικό:** συνεκτικό περιστατικό, το οποίο θα μπορούσε να έχει θέσει σε κίνδυνο τη διαθεσιμότητα, την αυθεντικότητα, την ακεραιότητα ή την εμπιστευτικότητα των αποθηκευμένων, διαβιβαζόμενων ή υφιστάμενων επεξεργασία δεδομένων ή των υπηρεσιών που προσφέρονται ή είναι προσβάσιμες μέσω συστημάτων δικτύου και πληροφοριακών συστημάτων, αλλά **το οποίο εμποδίστηκε ή δεν υλοποιήθηκε επιτυχώς**
- **Περιστατικό:** Κάθε συμβάν που θέτει σε κίνδυνο τη διαθεσιμότητα, την αυθεντικότητα, την ακεραιότητα ή το απόρρητο των δεδομένων που αποθηκεύονται, μεταδίδονται ή υποβάλλονται σε επεξεργασία ή των υπηρεσιών που προσφέρονται ή είναι προσβάσιμες μέσω συστημάτων δικτύου και πληροφοριακών συστημάτων
- **Περιστατικό μεγάλης κλίμακας στον τομέα της κυβερνοασφάλειας:** περιστατικό το οποίο προκαλεί διατάραξη που υπερβαίνει την ικανότητα της χώρας να ανταποκριθεί σε αυτή ή το οποίο έχει σημαντικό αντίκτυπο σε τουλάχιστον δύο κράτη μέλη της ΕΕ

Ορισμοί: Άρθρο 6 της Οδηγίας NIS2 (Συνοπτικά) - III

- **Χειρισμός περιστατικών:** κάθε ενέργεια και διαδικασία που αποσκοπεί στην πρόληψη, τη διαπίστωση, την ανάλυση και τον περιορισμό ή την αντίδραση σε περιστατικό και την ανάκαμψη από αυτό
- **Κίνδυνος:** η πιθανότητα απώλειας ή διατάραξης που προκαλείται από περιστατικό και εκφράζεται ως συνδυασμός του μεγέθους της εν λόγω απώλειας ή διατάραξης και της πιθανότητας επέλευσης του εν λόγω περιστατικού
- **Ευπάθεια:** αδυναμία, ευαισθησία ή ελάττωμα προϊόντων ΤΠΕ ή υπηρεσιών ΤΠΕ που μπορεί να αποτελέσει αντικείμενο εκμετάλλευσης από κυβερνοαπειλή
- **Πάροχος διαχειριζόμενων υπηρεσιών ασφάλειας:** πάροχος διαχειριζόμενων υπηρεσιών που εκτελεί ή παρέχει υποστήριξη για δραστηριότητες που σχετίζονται με τη διαχείριση κινδύνων κυβερνοασφάλειας, συμπεριλαμβανομένων της αντιμετώπισης περιστατικών, των δοκιμών διείσδυσης και των ελέγχων ασφάλειας
- **Σύστημα ονομάτων χώρου ή DNS:** ιεραρχικό κατανεμημένο σύστημα ονοματοδοσίας που επιτρέπει τον προσδιορισμό των διαδικτυακών υπηρεσιών και πόρων, επιτρέποντας στις συσκευές των τελικών χρηστών να χρησιμοποιούν υπηρεσίες δρομολόγησης και συνδεσιμότητας στο διαδίκτυο για την πρόσβαση στις εν λόγω υπηρεσίες και πόρους

Ορισμοί: Άρθρο 6 της Οδηγίας NIS2 (Συνοπτικά) - IV

- **«Εκπρόσωπος»:** φυσικό ή νομικό πρόσωπο εγκατεστημένο στην Ελλάδα που έχει οριστεί ρητά να ενεργεί εξ ονόματος παρόχου υπηρεσιών Domain Name System (DNS), μητρώου ονομάτων top-level domain (TLD), οντότητας που παρέχει υπηρεσίες καταχώρισης ονομάτων τομέα, παρόχου υπηρεσιών υπολογιστικού νέφους, παρόχου υπηρεσιών κέντρου δεδομένων, παρόχου δικτύου διανομής περιεχομένου, κτλ. που δεν είναι εγκατεστημένος στην Ευρωπαϊκή Ένωση, στον οποίο μπορεί να απευθύνεται η Εθνική Αρχή Κυβερνοασφάλειας ή CSIRT αντί της ίδιας της οντότητας όσον αφορά τις υποχρεώσεις της εν λόγω οντότητας
- **Οντότητα:** φυσικό ή νομικό πρόσωπο που έχει συσταθεί και αναγνωρίζεται ως τέτοιο βάσει του εθνικού δικαίου του τόπου εγκατάστασής του ή του τόπου παροχής υπηρεσιών και άσκησης δραστηριοτήτων, το οποίο μπορεί, ενεργώντας για ίδιο λογαριασμό, να ασκεί δικαιώματα και να υπόκειται σε υποχρεώσεις
- **Οντότητα Δημόσιας Διοίκησης:** οντότητα που αναγνωρίζεται ως τέτοια σύμφωνα με το εθνικό δίκαιο, μη συμπεριλαμβανομένων των δικαστηρίων, των κοινοβουλίων ή της κεντρικής τράπεζας

Συντονισμένα Κανονιστικά Πλαίσια

Άρθρο 7: Εθνική Στρατηγική Κυβερνοασφάλειας

- Η Εθνική Αρχή Κυβερνοασφάλειας διαμορφώνει την Εθνική Στρατηγική Κυβερνοασφάλειας (Ε.Σ.Κ.) που προβλέπει τους στρατηγικούς στόχους, τους πόρους που απαιτούνται για την επίτευξη των εν λόγω στόχων και κατάλληλα μέτρα πολιτικής και ρυθμιστικά μέτρα, με σκοπό την επίτευξη και τη διατήρηση υψηλού επιπέδου Κυβερνοασφάλειας
- Αποσαφηνίζει τους ρόλους και τις αρμοδιότητες των σχετικών ενδιαφερόμενων μερών σε εθνικό επίπεδο
- Υποστηρίζει τη συνεργασία και τον συντονισμό σε εθνικό επίπεδο μεταξύ των αρμόδιων αρχών μεταξύ των αρμόδιων αρχών, του ενιαίου σημείου επαφής και των CSIRTS
- Θεσπίζονται πολιτικές για:
 - εμπέδωση της κυβερνοασφάλειας στην αλυσίδα εφοδιασμού προϊόντων τεχνολογιών πληροφοριών και επικοινωνίας (ΤΠΕ) και υπηρεσιών ΤΠΕ, που χρησιμοποιούνται από οντότητες για την παροχή των υπηρεσιών τους & τη διατήρηση της γενικής διαθεσιμότητας, της ακεραιότητας και της εμπιστευτικότητας του δημόσιου πυρήνα του διαδικτύου
 - Η Εθνική Αρχή Κυβερνοασφάλειας κοινοποιεί την Ε.Σ.Κ. στην Ευρωπαϊκή Επιτροπή εντός τριών (3) μηνών από την έγκρισή της και Ε.Σ.Κ. αξιολογείται σε τακτική βάση και τουλάχιστον ανά πέντε (5)
 - Το Σχέδιο Δράσης για την υλοποίηση της Ε.Σ.Κ. αξιολογείται και, εφόσον είναι αναγκαίο, επικαιροποιείται τουλάχιστον ανά δύο (2) έτη

Άρθρο 8: Αρμόδια αρχή & ενιαίο σημείο επαφής: Εθνική Αρχή Κυβερνοασφάλειας

Άρθρο 9: Εθνικό πλαίσιο διαχείρισης κυβερνοκρίσεων

- Αναπόσπαστο μέρος της Στρατηγικής Εθνικής Ασφάλειας του ΚΥ.Σ.Ε.Α.
- Θέτει Στόχους & μέτρα για όλους τους τομείς της NIS2
- Εκτίμηση κινδύνων & απόκριση σε περιστατικά
- Πιστοποίηση ΤΠΕ προϊόντων σε δημόσιες συμβάσεις
- Συντονισμένη γνωστοποίηση ευπαθειών
- Κατάρτιση & ευαισθητοποίηση πολιτών & στελεχών
- Έχει την εποπτεία και τον έλεγχο για τη συμμόρφωση ως προς NIS2
- Επιβάλει μέτρα εποπτείας και πρόστιμα σε περιπτώσεις μη συμμόρφωσης στις οντότητες
- Σε απευθείας συνεργασία με την Αρχή Προστασίας Προσωπικών Δεδομένων
- Μπορεί να απαγορεύει προσωρινά σε κάθε φυσικό πρόσωπο που είναι υπεύθυνο για την άσκηση διευθυντικών καθηκόντων σε επίπεδο διευθύνοντος συμβούλου ή νόμιμου εκπροσώπου στη βασική οντότητα να ασκεί διευθυντικά καθήκοντα
- Ορίζεται ως αρμόδια αρχή για κρίσεις μεγάλης κλίμακας & περιστατικών
- Καταρτίζεται εθνικό σχέδιο αντιμετώπισης περιστατικών μεγάλης κλίμακας και κρίσεων στον κυβερνοχώρο
- Συμμετέχει στο Ευρωπαϊκό Δίκτυο οργανώσεων διασύνδεσης για κρίσεις στον κυβερνοχώρο (EU-CyCLONe)

Άρθρο 10: Ομάδες απόκρισης για συμβάντα που αφορούν στην ασφάλεια υπολογιστών (CSIRTs)

- ✓ Η Εθνική Αρχή Κυβερνοασφάλειας ορίζεται ως αρμόδια ομάδα απόκρισης για συμβάντα που αφορούν στην ασφάλεια υπολογιστών (Computer Security Incident Response Team - CSIRT)
- ✓ Για τους **Φορείς της Κεντρικής Κυβέρνησης τους Οργανισμούς Τοπικής Αυτοδιοίκησης** α' βαθμού & β' βαθμού ως αρμόδια ομάδα απόκρισης για συμβάντα που αφορούν στην ασφάλεια υπολογιστών (CSIRT) ορίζεται η Ομάδα Αντιμετώπισης Ηλεκτρονικών Επιθέσεων (**Εθνικό CERT**) της Διεύθυνσης Κυβερνοχώρου της Εθνικής Υπηρεσίας Πληροφοριών (Ε.Υ.Π.) **Παρατήρηση:** Για τα περιστατικά κυβερνοασφάλειας οφείλει να ενημερώνει και την ΕΑΚ λόγω του συντονιστικού της χαρακτήρα!
- ✓ Υφίσταται και το CSIRT του Γενικού Επιτελείου Εθνικής Άμυνας
- ✓ Για την αντιμετώπιση συμβάντων στον τομέα της κυβερνοασφάλειας, δύνανται να συστήνονται ειδικές ομάδες απόκρισης σε Εθνικό Επίπεδο
- ✓ **Τα άρθρα 11, 12, 13 καθορίζουν τον τρόπο λειτουργίας των CSIRT και το συντονισμό με CSIRT της ΕΕ**



Μέτρα Διαχείρισης Κινδύνων & Υποχρεώσεις Αναφορέας Περιστατικών - I

❖ Άρθ. 14: Διακυβέρνηση (άρ. 20 της NIS2)

- Τα όργανα διοίκησης των βασικών και σημαντικών οντοτήτων πρέπει να εγκρίνουν **εντός τριών (3) μηνών από την έναρξη ισχύος του νόμου τα μέτρα διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας**
- Επιβλέπουν την εφαρμογή των μέτρων και είναι υπεύθυνα για παραβιάσεις των υποχρεώσεων
- Η ευθύνη αυτή δεν θίγει τους ισχύοντες κανόνες περί ευθύνης δημόσιων υπαλλήλων και αιρετών ή διορισμένων αξιωματούχων
- Τα μέλη των οργάνων διοίκησης παρακολουθούν εκπαίδευση και διασφαλίζουν ότι οι οντότητες παρέχουν ετήσια κατάρτιση στους υπαλλήλους
- Στόχος η απόκτηση γνώσεων και δεξιοτήτων για τον εντοπισμό κινδύνων και την αξιολόγηση πρακτικών διαχείρισης στον τομέα της κυβερνοασφάλειας

❖ Άρθ. 15: Μέτρα διαχείρισης κινδύνων (άρ. 21 & παρ. 1 του άρ. 24 της NIS2)

- Βασικές και σημαντικές οντότητες λαμβάνουν τεχνικά, επιχειρησιακά και οργανωτικά μέτρα για τη διαχείριση της ασφάλειας σε δίκτυα και πληροφοριακά συστήματα, έχοντας υπόψη έκθεση σε κίνδυνο, μέγεθος οντότητας, σοβαρότητα & κοινωνικές/οικονομικές επιπτώσεις:
 - ✓ Πολιτικές και διαδικασίες ανάλυσης κινδύνου
 - ✓ Διαχείριση περιστατικών
 - ✓ Επιχειρησιακή συνέχεια και αποκατάσταση μετά από καταστροφή
 - ✓ Ασφάλεια αλυσίδας εφοδιασμού
 - ✓ Ασφάλεια στην απόκτηση, ανάπτυξη και συντήρηση συστημάτων
 - ✓ Αξιολόγηση της αποτελεσματικότητας των μέτρων
 - ✓ Πρακτικές κυβερνοϋγιεινής και κατάρτισης
 - ✓ Πολιτικές σχετικά με κρυπτογραφία
 - ✓ Ασφάλεια ανθρώπινων πόρων, έλεγχος πρόσβασης, διαχείριση πάγιων στοιχείων
 - ✓ Χρήση πολυπαραγοντικής επαλήθευσης ταυτότητας και ασφαλών επικοινωνιών έκτακτης ανάγκη

Μέτρα Διαχείρισης Κινδύνων & Υποχρεώσεις Αναφορέας Περιστατικών - II

- ❖ **Άρ. 15: Μέτρα διαχείρισης κινδύνων (άρ. 21 & παρ. 1 του άρ. 24 της NIS2)**
 - Ορίζεται Υπεύθυνος Ασφάλειας Συστημάτων Πληροφορικής και Επικοινωνιών (**Υ.Α.Σ.Π.Ε.**) με εξουσιοδοτήσεις και πόρους
 - Τηρείται **ενιαία πολιτική κυβερνοασφάλειας**, η οποία εγκρίνεται τουλάχιστον **ετησίως** από την **Εθνική Αρχή Κυβερνοασφάλειας**
 - Τηρείται η **συνολική καταγραφή** των υλικών και άυλων πληροφοριακών και επικοινωνιακών αγαθών, τα οποία ιεραρχούνται βάσει της κρισιμότητάς τους
 - Υποστηρίζεται η **χρήση πιστοποιημένων** προϊόντων και υπηρεσιών ΤΠΕ βάσει ευρωπαϊκών προτύπων που θεσπίζονται σύμφωνα με το άρθρο 49 του Κανονισμού (ΕΕ) 2019/881 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου
- ❖ **Άρ. 16 – Υποχρεώσεις αναφοράς περιστατικών (άρ. 23 της NIS2)**
 - Οι βασικές και σημαντικές οντότητες κοινοποιούν αμελλητί στην ομάδα απόκρισης συμβάντων CSIRT της Εθνικής Αρχής Κυβερνοασφάλειας κάθε περιστατικό με σημαντικό αντίκτυπο στην παροχή υπηρεσιών τους
 - **Οι Φορείς της Κεντρικής Κυβέρνησης τους Οργανισμούς Τοπικής Αυτοδιοίκησης α' βαθμού & β' βαθμού κοινοποιούν περιστατικά στην CSIRT της Εθνικής Υπηρεσίας Πληροφοριών, με ταυτόχρονη ενημέρωση της Εθνικής Αρχής Κυβερνοασφάλειας**
 - Οι οντότητες ενημερώνουν και τους αποδέκτες των υπηρεσιών τους για σημαντικά περιστατικά που μπορεί να επηρεάσουν την παροχή υπηρεσιών χωρίς αδικαιολόγητη καθυστέρηση.
 - Κάθε κοινοποίηση πρέπει να περιλαμβάνει πληροφορίες για πιθανές διασυνοριακές επιπτώσεις του περιστατικού
 - Η απλή κοινοποίηση δεν συνεπάγεται ευθύνη για την οντότητα.

Μέτρα Διαχείρισης Κινδύνων & Υποχρεώσεις Αναφορέας Περιστατικών - III

- ❖ **Άρ. 16 – Υποχρεώσεις αναφοράς περιστατικών (άρ. 23 της NIS2)**
 - Ένα περιστατικό θεωρείται **σημαντικό** αν προκαλεί ή μπορεί να προκαλέσει **είτε** σοβαρή λειτουργική διατάραξη ή οικονομική ζημία στην **οντότητα είτε** σημαντική υλική/μη υλική ζημία σε **τρίτους**
 - Οι οντότητες πρέπει να καταθέτουν:
 - α) Έγκαιρη προειδοποίηση εντός **24 ωρών** από την αναγνώριση περιστατικού
 - β) Κοινοποίηση περιστατικού εντός **72 ωρών** με αρχική αξιολόγηση
 - γ) Ενδιάμεσες ενημερώσεις κατόπιν αιτήματος της ΕΑΚ
 - δ) Τελική αναφορά εντός **ενός (1) μηνός** με λεπτομέρειες περιστατικού και μέτρων μετριασμού
 - Η Εθνική Αρχή Κυβερνοασφάλειας παρέχει γρήγορη ανταπόκριση, καθοδήγηση, τεχνική υποστήριξη και εκκινεί διαδικασίες εφόσον απαιτείται (π.χ. αναφορά στις αρχές).
 - Σε διασυνοριακά περιστατικά, ενημερώνονται συναρμόδιοι φορείς της ΕΕ και ο ENISA
 - Υπάρχει δυνατότητα ενημέρωσης του κοινού για την πρόληψη ή αντιμετώπιση σημαντικών περιστατικών μετά από διαβούλευση
 - Η Εθνική Αρχή Κυβερνοασφάλειας ως ενιαίο σημείο επαφής υποβάλλει στον **ENISA**, **ανά τρεις (3) μήνες**, συνοπτική έκθεση, η οποία περιλαμβάνει ανωνυμοποιημένα και συγκεντρωτικά δεδομένα σχετικά με τα περιστατικά
-
- ❖ **Άρ. 17 – Τυποποίηση (άρ. 25 της NIS2)**
 - Η ΕΑΚ για την αποτελεσματική εφαρμογή των μέτρων διαχείρισης κινδύνων **μπορεί να θεσπίσει μέτρα βάσει προτύπων & τεχνικών προδιαγραφών λαμβάνοντας υπόψη τις κατευθύνσεις του ENISA όχι όμως συγκεκριμένες τεχνολογίες**

Δικαιοδοσία & Καταχώριση - I

❖ Άρ. 18 – Δικαιοδοσία και εδαφικότητα (άρ. 26 της NIS2)

- Οι οντότητες που είναι εγκατεστημένες ή παρέχουν υπηρεσίες ή ασκούν δραστηριότητα στη χώρα υπόκεινται στη δικαιοδοσία της ΕΑΚ - **Εξαιρούνται:**
 - i. Πάροχοι δημόσιων δικτύων & υπηρεσιών ήλ. επικοινωνιών που παρέχουν υπηρεσίες σε **άλλο κράτος μέλος**
 - ii. Πάροχοι DNS, μητρώα ονομάτων top-level domain (TLD), υπηρεσίες καταχώρισης ονομάτων τομέα, υπολογιστικού νέφους, κέντρων δεδομένων, δικτύων διανομής περιεχομένου, και παρόχοι υπηρεσιών ασφαλείας και πλατφορμών κοινωνικής δικτύωσης που **εμπίπτουν στη δικαιοδοσία του κράτους μέλους όπου έχουν την κύρια εγκατάστασή τους**
 - iii. Οντότητες δημόσιας διοίκησης που ανήκουν σε **άλλο κράτος μέλος**
- Η κύρια **εγκατάσταση** ορίζεται με βάση το σημείο λήψης αποφάσεων για μέτρα διαχείρισης κινδύνων, επιχειρήσεις κυβερνοασφάλειας ή τη **μεγαλύτερη βάση εργαζομένων** στην Ελλάδα
- Οντότητες εκτός ΕΕ που παρέχουν υπηρεσίες εντός αυτής οφείλουν να ορίσουν εκπρόσωπο στην ΕΕ, ο οποίος υπόκειται στη δικαιοδοσία της χώρας εγκατάστασής του
- Η Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών ορίζεται ως τομεακό σημείο επαφής και συνεργασίας σε εθνικό επίπεδο με την Εθνική Αρχή Κυβερνοασφάλειας (National Sectorial Focal Point, NSFP) αναφορικά με τους παρόχους δημόσιων δικτύων ηλεκτρονικών επικοινωνιών ή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών

Δικαιοδοσία & Καταχώριση - II

❖ Άρ. 19 – Μητρώο οντοτήτων (άρ. 27 της NIS2)

▪ Υπόχρεοι:

- Πάροχοι DNS, TLD, υπηρεσιών καταχώρισης ονομάτων τομέα
- Πάροχοι cloud, data centers, CDN, διαχειριζόμενων υπηρεσιών & ασφάλειας
- Επιγραμμικές αγορές (π.χ. Skroutz, Bestprice) , μηχανές αναζήτησης, πλατφόρμες κοινωνικής δικτύωσης

▪ Υποχρέωση υποβολής έως 30-09-2025 προς την ΕΑΚ:

- Επωνυμία & τύπος οντότητας
- Διεύθυνση εγκατάστασης ή εκπροσώπου στην ΕΕ
- Στοιχεία επικοινωνίας (email, τηλέφωνο)
- Κράτη μέλη όπου παρέχονται υπηρεσίες
- Εύρος IP της οντότητας

▪ Ενημέρωση μεταβολών:

- Εντός 3 μηνών από την αλλαγή
- Η ΕΑΚ διαβιβάζει τα στοιχεία (εκτός IP) στον ENISA

❖ Άρ. 20 – Βάση δεδομένων καταχώρισης ονομάτων τομέα (άρ. 28 της NIS2)

- Για την ασφάλεια, τη σταθερότητα και την ανθεκτικότητα του DNS, τα μητρώα ονομάτων TLD & οι οντότητες που παρέχουν υπηρεσίες καταχώρισης ονομάτων τομέα συλλέγουν και διατηρούν ακριβή και πλήρη δεδομένα καταχώρισης σε ειδική βάση δεδομένων, σύμφωνα με τον Κανονισμό Γ.Κ.Π.Δ. με α) το όνομα τομέα, β) την ημερομηνία καταχώρισης, γ) το όνομα, την ηλεκτρονική διεύθυνση & τον αριθμό τηλεφώνου του καταχωρίζοντος, δ) στοιχεία επικοινωνίας του σημείου επαφής που διαχειρίζεται το όνομα τομέα, αν διαφέρει από τον καταχωρίζοντα

▪ Διαφάνεια & πρόσβαση:

- Δημοσιοποίηση μη προσωπικών δεδομένων
- Παροχή πρόσβασης σε νόμιμα αιτήματα εντός 72 ωρών
- Δημοσίευση πολιτικών γνωστοποίησης



govgr Εγγραφή Οντοτήτων του ν.5160/2024

<https://nis2register.cyber.gov.gr/app/home>

Ανταλλαγή Πληροφοριών - I

- ❖ **Άρ. 21 – Ρυθμίσεις για την ανταλλαγή πληροφοριών στον τομέα της κυβερνοασφάλειας (άρ. 29 της NIS2)**
- **Σκοπός:** Ενίσχυση της πρόληψης, ανίχνευσης, ευαισθητοποίησης, αντιμετώπισης και ανάκαμψης από περιστατικά κυβερνοασφάλειας μέσω εθελοντικής συνεργασίας μεταξύ οντοτήτων
- **Αντικείμενο Ανταλλαγής Πληροφοριών:**
 - Κυβερνοαπειλές & παρ' ολίγον περιστατικά
 - Ευπάθειες & ενδείξεις παραβίασης
 - Κακόβουλες τακτικές, τεχνικές & διαδικασίες Πληροφορίες για παράγοντες απειλής
 - Προειδοποιήσεις και συστάσεις παραμετροποίησης εργαλείων ασφάλειας
- **Πλαίσιο Υλοποίησης:**
 - Πραγματοποιείται εντός κοινοτήτων βασικών και σημαντικών οντοτήτων
 - Συμμετέχουν, κατά περίπτωση, προμηθευτές και πάροχοι υπηρεσιών
 - Λαμβάνεται υπόψη ο ευαίσθητος χαρακτήρας των πληροφοριών
- Οι βασικές & σημαντικές οντότητες **ενημερώνουν άμεσα την ΕΑΚ** για τη συμμετοχή ή απόσυρσή τους από πλαίσια ανταλλαγής πληροφοριών

Information Sharing and Analysis Centers (ISACs) – supported by ENISA

μη κερδοσκοπικοί, αξιόπιστοι κόμβοι που έχουν σχεδιαστεί για τη βελτίωση της ανθεκτικότητας στην ασφάλεια στον κυβερνοχώρο

<https://enisa.europa.eu/topics/cybersecurity-of-critical-sectors/information-sharing-and-analysis-centers-isacs>



Ανταλλαγή Πληροφοριών - II

- ❖ **Άρ. 22 – Εθελούσια κοινοποίηση των σχετικών πληροφοριών (άρ. 30 της ΝΙΣ2)**
- Οι κοινοποιήσεις μπορούν να υποβάλλονται στην Εθνική Αρχή Κυβερνοασφάλειας σε εθελοντική βάση, από:
 - βασικές και σημαντικές οντότητες όσον αφορά περιστατικά, κυβερνοαπειλές και παρ' ολίγον περιστατικά,
 - οντότητες ανεξαρτήτως του αν εμπίπτουν στο πεδίο εφαρμογής του παρόντος νόμου, όσον αφορά σημαντικά περιστατικά, κυβερνοαπειλές και παρ' ολίγον περιστατικά
- Η ΕΑΚ επεξεργάζεται τις κοινοποιήσεις **δίνοντας προτεραιότητα στην επεξεργασία των υποχρεωτικών κοινοποιήσεων**
- Η ΕΑΚ διασφαλίζει την **εμπιστευτικότητα** και την κατάλληλη προστασία των πληροφοριών
- Με την επιφύλαξη της πρόληψης, της διερεύνησης, της διακρίβωσης και της δίωξης ποινικών αδικημάτων, η εθελούσια αναφορά δεν συνεπάγεται την επιβολή πρόσθετων υποχρεώσεων στην κοινοποιούσα οντότητα, τις οποίες δεν θα υπείχε αν δεν είχε υποβάλει την κοινοποίηση

Εποπτεία & Κυρώσεις - I

- ❖ **Άρ. 23 – Γενικές πτυχές που αφορούν την εποπτεία και την επιβολή (παρ. 5 άρ. 8, παρ. 1 άρ. 9, παρ. 2 άρ. 10, παρ. 2 άρ. 11 και άρ.31 της NIS2)**
 - Η ΕΑΚ ασκεί **εποπτεία και έλεγχο βασικών και σημαντικών οντοτήτων** & Εποπτεύει μέσω **επιθεωρητών, πιστοποιημένων ελεγκτών και τεχνικών εμπειρογνωμόνων (SMEs)**
 - Επιβάλλεται αναλογικό παράβολο εποπτείας & τέλος ελέγχου, ανάλογα με το μέγεθος της οντότητας και την πολυπλοκότητα του ελέγχου
 - Συνεργάζεται με την **Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα** για περιστατικά που αφορούν **παραβίαση δεδομένων προσωπικού χαρακτήρα**
 - Οι εντεταλμένοι υπάλληλοι μπορούν να:
 - Πραγματοποιούν **επιτόπιους ελέγχους** με ή χωρίς προειδοποίηση.
 - **Συλλέγουν δεδομένα & πληροφορίες** από συσκευές, servers και cloud.
 - **Ενεργούν έρευνες** σε γραφεία & εγκαταστάσεις.
 - **Κατάσχουν ή αντιγράφουν** επαγγελματικά έγγραφα και ηλεκτρονικά δεδομένα.
 - **Σφραγίζουν χώρους ή αρχεία,** στο μέτρο που απαιτείται για τον έλεγχο
 - Τα όργανα της ΕΑΚ απολαμβάνουν **λειτουργική ανεξαρτησία** έναντι των εποπτευόμενων φορέων της δημόσιας διοίκησης

Εποπτεία & Κυρώσεις - II

- Οι βασικές οντότητες υπόκεινται σε πλήρες εκ των προτέρων & εκ των υστέρων καθεστώς εποπτείας, ενώ οι σημαντικές οντότητες υπόκεινται σε απλοποιημένο, μόνο εκ των υστέρων, εποπτικό καθεστώς
- Εκ των προτέρων (**ex ante**) εποπτικό καθεστώς εννοείται ο έλεγχος και εποπτεία που πραγματοποιείται περιοδικά ή εκτάκτως, χωρίς να έχει λάβει χώρα περιστατικό κυβερνοασφάλειας
- Εκ των υστέρων (**ex post**) εποπτικό καθεστώς, εννοείται ο έλεγχος και εποπτεία που πραγματοποιείται μετά την εκδήλωση περιστατικού
- Κατά τους ελέγχους (**ex post και ex ante**), παρέχονται αποδεικτικά στοιχεία, ενδείξεις ή πληροφορίες από την οικεία οντότητα από τα οποία αποδεικνύεται η συμμόρφωσή της με τις απαιτήσεις, ιδίως των άρθρων 15 και 16 αρχή της λογοδοσίας

Πηγή: [Οδηγός Αναφοράς v.5160/2024 για την κυβερνοασφάλεια](#)

Εποπτεία & Κυρώσεις - III

- ❖ **Άρ. 24 – Μέτρα εποπτείας και επιβολής σε σχέση με βασικές οντότητες (άρ. 32 της ΝΙΣ2)**
 - **Στόχος:** Εξασφάλιση αποτελεσματικής, αναλογικής και αποτρεπτικής εποπτείας για τη συμμόρφωση με τις υποχρεώσεις κυβερνοασφάλειας από την ΕΑΚ
 - Τα μέτρα εποπτείας και επιβολής που ασκούνται σε βασικές οντότητες πρέπει να είναι αποτελεσματικά, αναλογικά και αποτρεπτικά, λαμβάνοντας υπόψη τις περιστάσεις κάθε περίπτωσης
 - Η ΕΑΚ δύναται να διενεργεί:
 - **Επιτόπιες επιθεωρήσεις & δειγματοληπτικούς ελέγχους**
 - **Τακτικούς & στοχευμένους ελέγχους ασφάλειας** (βάσει εκτίμησης κινδύνου)
 - **Έκτακτους ειδικούς ελέγχους** σε περίπτωση περιστατικού ή καταγγελίας
 - **Σαρώσεις ασφαλείας** με δίκαια & διαφανή κριτήρια
 - **Αιτήματα παροχής πληροφοριών**, δεδομένων & αποδεικτικών στοιχείων
 - Η ΕΑΚ εκδίδει προειδοποιήσεις, δεσμευτικές οδηγίες, επιβάλλει προθεσμίες, εντέλλει διακοπή παράνομων συμπεριφορών και επιβάλλει διοικητικά πρόστιμα
 - Σε περίπτωση μη συμμόρφωσης, έχει τη δυνατότητα **προσωρινής αναστολής πιστοποιήσεων** ή **απαγόρευσης** άσκησης διοικητικών καθηκόντων σε υπεύθυνα πρόσωπα
 - Προβλέπεται δικαίωμα άσκησης αίτησης ακύρωσης ενώπιον του Συμβουλίου της Επικρατείας για τις αποφάσεις
 - Οι υπεύθυνοι φυσικά πρόσωπα θεωρούνται προσωπικά υπεύθυνοι για τη συμμόρφωση της οντότητας
 - Η ΕΑΚ συνεργάζεται με άλλες εθνικές αρχές και ευρωπαϊκά όργανα για τη διασφάλιση της συμμόρφωσης

Εποπτεία & Κυρώσεις - IV

- ❖ **Άρ. 25 – Μέτρα εποπτείας και επιβολής σε σχέση με σημαντικές οντότητες (άρ. 33 της ΝΙΣ2)**
- Η ΕΑΚ είναι η αρμόδια αρχή για την εποπτεία και τον έλεγχο της συμμόρφωσης με τις διατάξεις του νόμου για την κυβερνοασφάλεια
- Σε περίπτωση υποψίας **μη συμμόρφωσης σημαντικής οντότητας**, η ΕΑΚ λαμβάνει αποτελεσματικά, αναλογικά και αποτρεπτικά κατασταλτικά μέτρα:
 - Επιτόπιες επιθεωρήσεις και εποπτεία εντός και εκτός εγκαταστάσεων
 - Στοχευμένους ελέγχους ασφάλειας και σαρώσεις με αντικειμενικά και διαφανή κριτήρια
 - Αιτήματα για παροχή πληροφοριών, πρόσβαση σε δεδομένα, και αποδεικτικά πολιτικών κυβερνοασφάλειας
- Εκδίδει **προειδοποιήσεις**, δεσμευτικές οδηγίες και διατάζει την αποκατάσταση παραβάσεων ή τη διακοπή παραβατικής συμπεριφοράς
- Μπορεί να **επιβάλλει διοικητικά πρόστιμα** και, αν χρειαστεί, προσωρινά μέτρα όπως **αναστολή πιστοποιήσεων** ή **απαγόρευση άσκησης διοικητικών καθηκόντων**, διατάσσει **δημοσιοποίηση παραβιάσεων** κατά περίπτωση
- **Συνεργάζεται με άλλες αρχές και διασφαλίζει τη λειτουργική ανεξαρτησία των οργάνων της κατά την άσκηση των καθηκόντων της**

Εποπτεία & Κυρώσεις - V

ΒΑΣΙΚΕΣ ΟΝΤΟΤΗΤΕΣ	ΣΗΜΑΝΤΙΚΕΣ ΟΝΤΟΤΗΤΕΣ
επιτόπιες επιθεωρήσεις και εποπτεία εκτός των εγκαταστάσεων, συμπεριλαμβανομένων δειγματοληπτικών ελέγχων, που διεξάγονται από τους επιθεωρητές	επιτόπιες επιθεωρήσεις και κατασταλτική εποπτεία εντός και εκτός των εγκαταστάσεων
τακτικοί και στοχευμένοι έλεγχοι ασφάλειας που διενεργούνται από την Εθνική Αρχή Κυβερνοασφάλειας,	στοχευμένοι έλεγχοι ασφάλειας που διενεργούνται από την Εθνική Αρχή Κυβερνοασφάλειας
έκτακτοι ειδικοί έλεγχοι	σαρώσεις ασφαλείας βάσει αντικειμενικών, αμερόληπτων, δίκαιων και διαφανών κριτηρίων αξιολόγησης του κινδύνου
σαρώσεις ασφαλείας βάσει αντικειμενικών, αμερόληπτων, δίκαιων και διαφανών κριτηρίων αξιολόγησης του κινδύνου	αιτήματα παροχής αναγκών πληροφοριών για την αξιολόγηση των μέτρων διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας που λαμβάνει η οικεία οντότητα
αιτήματα παροχής αναγκών πληροφοριών για την εκ των υστέρων αξιολόγηση των μέτρων διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας που λαμβάνει η οικεία οντότητα	αιτήματα για πρόσβαση σε δεδομένα, έγγραφα ή πληροφορίες που είναι αναγκαίες για την εκτέλεση των εποπτικών καθηκόντων
αιτήματα πρόσβασης σε δεδομένα, έγγραφα και πληροφορίες που απαιτούνται για την εκτέλεση των εποπτικών καθηκόντων	αιτήματα για αποδεικτικά στοιχεία που αφορούν στην εφαρμογή των πολιτικών κυβερνοασφάλειας
αιτήματα για αποδεικτικά στοιχεία που αφορούν στην εφαρμογή των πολιτικών κυβερνοασφάλειας	

I A I
εκδίδει προειδοποιήσεις σχετικά με παραβάσεις από τις οικείες οντότητες

I B I
εκδίδει δειμευτικές οδηγίες και κατευθύνσεις, μεταξύ άλλων δύον αφορά στα μέτρα που είναι αναγκαία για την πρόληψη ή την αποκατάσταση περιστατικού, και τάσσει προθεσμίες για την εφαρμογή των εν λόγω μέτρων και για την υποβολή εκθέσεων σχετικά με την εφαρμογή τους, ή εντέλλει τις οικείες οντότητες να αποκαταστήσουν τις έλλειμμες ή τις παραβάσεις που εντοπίστηκαν

I C I
εντέλλει τις οικείες οντότητες να ενημερώσουν τα φυσικά ή νομικά πρόσωπα, σε αέστη με τα οποία παρέχουν υπηρεσίες ή ασκούν δραστηριότητες που ενδέχεται να επηρεαστούν από σημαντική κυβερνοαπειλή, σχετικά με τη φύση της απειλής, καθώς και σχετικά με τυχόν μέτρα προστασίας ή αποκατάστασης που μπορούν να λάβουν τα εν λόγω φυσικά ή νομικά πρόσωπα για την αντιμετώπιση της εν λόγω απειλής

I D I
εντέλλει τις οικείες οντότητες να διασφαλίσουν ότι τα μέτρα διαχείρισης κινδύνων που τομέα της κυβερνοασφάλειας εναρμονίζονται με το άρθρο 15 ή να εκπληρώσουν τις υποχρέωσης υποβολής εκθέσεων που ορίζονται στο άρθρο 16, με συγκεκριμένο τρόπο και εντός ορισμένου χρονικού διαστήματος

I E I
εντέλλει τις οικείες οντότητες να ενημερώσουν τα φυσικά ή νομικά πρόσωπα, σε αέστη με τα οποία παρέχουν υπηρεσίες ή ασκούν δραστηριότητες που ενδέχεται να επηρεαστούν από σημαντική κυβερνοαπειλή, σχετικά με τη φύση της απειλής, καθώς και σχετικά με τυχόν μέτρα προστασίας ή αποκατάστασης που μπορούν να λάβουν τα εν λόγω φυσικά ή νομικά πρόσωπα για την αντιμετώπιση της εν λόγω απειλής

I F I
εντέλλει τις οικείες οντότητες να ενημερώσουν τα φυσικά ή νομικά πρόσωπα, σε αέστη με τα οποία παρέχουν υπηρεσίες ή ασκούν δραστηριότητες που ενδέχεται να επηρεαστούν από σημαντική κυβερνοαπειλή, σχετικά με τη φύση της απειλής, καθώς και σχετικά με τυχόν μέτρα προστασίας ή αποκατάστασης που μπορούν να λάβουν τα εν λόγω φυσικά ή νομικά πρόσωπα για την αντιμετώπιση της εν λόγω απειλής

I G I
εντέλλει τις οικείες οντότητες να πάσχουν συμπεριφορά που παραβάζει τις απαγόρευσις και να απόσχουν από την επανάληψη της εν λόγω συμπεριφοράς

I H I
επιπλέον των λοιπών μέτρων, επιβάλλει διοικητικά πρόστιμα

Παραβιάσεις & Πρόστιμα: Άρ. 26 - Γενικοί όροι για την επιβολή διοικητικών προστίμων σε βασικές και σημαντικές οντότητες Κυρώσεις (άρ. 34 & 36 NIS2)

Άρ. 15 Μέτρα διαχείρισης κινδύνων, Άρ. 16 Αναφορά περιστατικών

Παραβίαση των άρθρων 15 ή 16



πρόστιμο έως 10.000.000€
(βασικές οντότητες)

ή κατ' ανώτατο όριο δύο τοις εκατό (2%) του κατά το προηγούμενο οικονομικό έτος συνολικού παγκόσμιου επίσιου κύκλου εργασιών της επιχείρησης στην οποία ανήκει η σημαντική οντότητα, ανάλογα με το ποιο είναι υψηλότερο.

Παραβίαση των άρθρων 15 ή 16



πρόστιμο έως 7.000.000€
(σημαντικές οντότητες)

ή κατ' ανώτατο όριο ένα κόμμα τέσσερα τοις εκατό (1,4%) του κατά το προηγούμενο οικονομικό έτος συνολικού παγκόσμιου επίσιου κύκλου εργασιών της επιχείρησης στην οποία ανήκει η σημαντική οντότητα, ανάλογα με το ποιο είναι υψηλότερο.

Παραβιάσεις των παρ. του Άρ. 24 & 25

Κλιμάκωση διοικητικών προστίμων



πρόστιμο έως 1.000.000€

για παράδειγμα: για την παράβαση εκ μέρους βασικών οντοτήτων δεσμευτικών οδηγιών και κατευθύνσεων, μεταξύ άλλων όσον αφορά τα μέτρα που είναι αναγκαία για την πρόληψη ή την αποκατάσταση περιστατικού επιβάλλεται πρόστιμο ύψους κατ' ανώτατο όριο ενός εκατομμυρίου (1.000.000) ευρώ ενώ για την παράβαση εκ μέρους σημαντικών οντοτήτων δεσμευτικών οδηγιών ή εντολών για την αποκάταση διαιτωμένων ελλείψεων, κατ' ανώτατο όριο επτακοσίων χιλιάδων (700.000) ευρώ.

Διοικητικά πρόστιμα σε οντότητες δημόσιας διοίκησης



πρόστιμο 20.000€-500.000€

Παραβίαση παρ. 1 του άρθρου 14



πρόστιμο έως 200.000€

Διακυβέρνηση- Ευθύνες Διοίκησης



πρόστιμο έως 100.000€

Παραβίαση του άρθρου 19



πρόστιμο έως 200.000€

Μητρώο οντοτήτων

Παραβίαση του άρθρου 20



πρόστιμο έως 800.000€

Βάση δεδομένων καταχώρισης ονομάτων τομέα

Παραβίαση παρ. 3 του άρθρου 21



πρόστιμο έως 100.000€

Ενημέρωση για ανταλλαγή Πληροφοριών μεταξύ Οντοτήτων

Παραβίαση παρ. 2 και 4 του άρθρου 24



πρόστιμο έως 500.000€

Εποπτικά μέτρα και έλεγχοι σε βασικές Οντότητες από την ΕΑΚ

Παραβίαση παρ. 2 του άρθρου 25



πρόστιμο έως 350.000€

Εποπτικά μέτρα και έλεγχοι σε σημαντικές Οντότητες από την ΕΑΚ

Παραβίαση παρ. 6 του άρθρου 15



πρόστιμο έως 300.000€

Πιστοποίηση των προϊόντων ΤΠΕ που χρησιμοποιούνται για τη συμμόρφωση

Άρ. 26 Παραβάσεις που συνεπάγονται παραβίαση δεδομένων προσωπικού χαρακτήρα- (άρ. 35 NIS2)

- Αν διαπιστωθεί από την ΕΑΚ στο πλαίσιο της εποπτείας ή της επιβολής κυρώσεων, ότι η παράβαση από βασική ή σημαντική οντότητα των υποχρεώσεων που ορίζονται στα άρθρα 15 και 16 μπορεί να συνεπάγεται παραβίαση δεδομένων προσωπικού χαρακτήρα (GDPR) ενημερώνει χωρίς αδικαιολόγητη καθυστέρηση την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΔΠΧ)
- Όταν η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα ή άλλος εποπτικός οργανισμός επιβάλλει διοικητικό πρόστιμο σε Οντότητα για παραβιάσεις του GDPR, η Εθνική Αρχή Κυβερνοασφάλειας δεν επιβάλλει διοικητικό πρόστιμο αλλά δύναται να εφαρμόσει ανάλογα μέτρα επιβολής
- Σε περίπτωση που επιβληθεί διοικητικό πρόστιμο για παραβίαση του GDPR από άλλη εποπτική αρχή, η ΕΑΚ ενημερώνει την ΑΔΠΧ

Άρ. 26 Αμοιβαία συνδρομή (άρ. 37 NIS2)

- Όταν μια οντότητα παρέχει υπηρεσίες σε περισσότερα του ενός κράτη μέλη ή παρέχει υπηρεσίες σε ένα ή περισσότερα κράτη μέλη της Ευρωπαϊκής Ένωσης και τα συστήματα δικτύου και πληροφοριών της βρίσκονται σε ένα ή περισσότερα άλλα κράτη μέλη, εφόσον ένα εκ των μελών είναι η Ελλάδα, η ΕΑΚ συνεργάζεται με τις αρμόδιες αρχές των λοιπών ενδιαφερόμενων κρατών μελών και παρέχεται αμοιβαία συνδρομή, ανάλογα με τις ανάγκες
- Κατά περίπτωση και με κοινή συμφωνία, οι αρμόδιες αρχές των κρατών μελών μπορούν να αναλαμβάνουν κοινές εποπτικές ενέργειες
- Η ΕΑΚ δεν απορρίπτει το αίτημα συνδρομής από άλλη αρχή, εκτός εάν διαπιστωθεί ότι δεν είναι αρμόδια να παράσχει τη ζητούμενη συνδρομή, ότι η ζητούμενη συνδρομή δεν είναι ανάλογη προς τα εποπτικά της καθήκοντα ή ότι το αίτημα αφορά πληροφορίες ή συνεπάγεται δραστηριότητες οι οποίες, εάν κοινοποιηθούν ή εκτελεστούν, θα ήταν αντίθετες προς τα βασικά συμφέροντα εθνικής ασφάλειας, δημόσιας ασφάλειας ή άμυνας της Ελλάδας. Πριν απορρίψει το εν λόγω αίτημα, η Εθνική Αρχή Κυβερνοασφάλειας διαβουλεύεται με τις άλλες οικείες αρμόδιες αρχές, καθώς και, κατόπιν αιτήματος ενός από τα ενδιαφερόμενα κράτη μέλη, με την Ευρωπαϊκή Επιτροπή και τον ENISA.

Βασικές Διαφορές μεταξύ NIS1 & NIS2, GDPR & ISO 27001

Κατηγορία	NIS1	NIS2	GDPR	ISO 27001
Σκοπός	Προστασία κρίσιμων υποδομών από κυβερνοαπειλές	Αυστηρότερος έλεγχος κυβερνοασφάλειας για κρίσιμους & σημαντικούς φορείς	Προστασία προσωπικών δεδομένων ατόμων	Διαχείριση κινδύνων ασφάλειας πληροφοριών
Πεδίο εφαρμογής	Κάποιοι κρίσιμοι τομείς	Διευρυμένο, περισσότερες οντότητες & τομείς	Όλες οι επιχειρήσεις που επεξεργάζονται δεδομένα ευρωπαίων πολιτών	Όλες οι οργανώσεις ανεξαρτήτως τομέα
Νομικό πλαίσιο	Ευρωπαϊκή Οδηγία, βασικές απαιτήσεις	Οδηγία με αυστηρές νομικές επιβολές και ποινές	Κανονισμός ΕΕ, με αυστηρές ποινές μη συμμόρφωσης	Πρότυπο χωρίς νομικές ποινές/ρήτρες
Αναφορά περιστατικών	Ναι, με περιορισμούς	Υποχρεωτική, αυστηρά χρονοδιαγράμματα	Με αναφορά μόνο σε παραβιάσεις προσωπικών δεδομένων	Δεν προβλέπει αναφορά περιστατικών
Ευκολία συμμόρφωσης	Πιο γενικό πλαίσιο	Πιο συγκεκριμένο με λεπτομερείς απαιτήσεις	Εστιάζει στα προσωπικά δεδομένα	Παρέχει ολοκληρωμένο σύστημα διαχείρισης ασφάλειας
Ευθύνη Διοίκησης	Όχι συγκεκριμένη	Ρητά επιβάλλεται ευθύνη Διοίκησης και τιμωρίες	Ευθύνη για επεξεργασία δεδομένων	Ευθύνη για υλοποίηση και διαρκή βελτίωση συστήματος
Στόχος	Ανθεκτικότητα δικτύων και πληροφοριών	Υψηλότερο επίπεδο κυβερνοασφάλειας με ελέγχους	Προστασία προσωπικών δεδομένων	Ολοκληρωμένη προστασία πληροφοριών μέσω βέλτιστων πρακτικών

✓ Η συμμόρφωση με το πρότυπο ISO 27001 συνδράμει στην κάλυψη πολλών απαιτήσεων της NIS2, **δεν υποκαθιστά όμως** την υποχρέωση συμμόρφωσης με τον νόμο και τις νομικές υποχρεώσεις που θέτει η νομοθεσία για τον κανονισμό NIS2

✓ Ο κανονισμός GDPR διέπει κυρίως τις πλευρές **προσωπικών δεδομένων** που μπορεί να εμπλέκονται σε περιστατικά κυβερνοασφάλειας

ΥΑ 1899/2025 – Καθορισμός προσόντων, καθηκόντων, ασυμβιβάστων και υποχρεώσεων των Υπεύθυνων Ασφαλείας Συστημάτων Πληροφορικής και Επικοινωνιών –’Έναρξη Ισχύος του Νόμου 01.11.2025

- Επιλογή Υ.Α.Σ.Π.Ε. – Βασικές Αρχές (Άρθ. 3)
- ✓ Ορίζεται στέλεχος της Οντότητας με κατάλληλα προσόντα και εμπειρία στους τομείς:
 - Ασφάλεια πληροφοριών & δικτύων
 - Κυβερνοασφάλεια
- ✓ Κριτήρια επιλογής:
 - Εμπειρία και γνώση στους σχετικούς τομείς
 - Ακεραιότητα & ευσυνειδησία
 - Ικανότητες διαχείρισης κρίσεων, λήψης αποφάσεων & συντονισμού
 - Κατανόηση της σημασίας του ρόλου για την ασφάλεια κρίσιμων συστημάτων και δεδομένων
- ✓ Κατ' εξαίρεση: μπορεί να οριστεί στέλεχος άλλης Οντότητας του ίδιου ομίλου επιχειρήσεων.
- ✓ Τακτική επανεξέταση της καταλληλότητας του ΥΑΣΠΕ, & αντικατάστασή του αν δεν πληροί πλέον τις απαιτήσεις



Άρθ. 4 - Προσόντα, κωλύματα και ασυμβίβαστα του ΥΑΣΠΕ - I

✓ Να διαθέτει επαρκή γνώση των επιχειρηματικών διαδικασιών της Οντότητας & τα κάτωθι ελάχιστα προσόντα:

- Προπτυχιακό ή μεταπτυχιακό τίτλο ετήσιας τουλάχιστον διάρκειας σε συναφές με τους τομείς της ασφάλειας πληροφοριών και δικτύων ή της κυβερνοασφάλειας γνωστικό αντικείμενο

ή

- Εμπειρογνωσία στους τομείς της ασφάλειας πληροφοριών και δικτύων ή της κυβερνοασφάλειας τουλάχιστον 5 ετών

ή

- Πιστοποιημένη γνώση μεθοδολογιών, διαδικασιών, τεχνικών, εργαλείων και προτύπων ασφάλειας πληροφοριών και ψηφιακών συστημάτων και εμπειρογνωσία στους τομείς της ασφάλειας πληροφοριών και δικτύων ή της κυβερνοασφάλειας τουλάχιστον 2 ετών

✓ Κωλύματα για τον ορισμό:

- Προηγούμενη αμετάκλητη καταδίκη του για την τέλεση ενός ή περισσότερων από τα κακουργήματα ή πλημμελήματα του Π.Κ. περί εγκλημάτων κατά των τηλεπικοινωνιών και άλλων κοινωφελών εγκαταστάσεων & περί προσβολών ατομικού απορρήτου και επικοινωνίας

- Οι Οντότητες οφείλουν να ζητούν από τον υποψήφιο ΥΑΣΠΕ αντίγραφο ποινικού μητρώου. Η ΕΑΚ δύναται να ζητεί οποτεδήποτε να της επιδειχθεί από την Οντότητα το αντίγραφο ποινικού μητρώου του ορισθέντος ΥΑΣΠΕ



Άρθ. 4 - Προσόντα, κωλύματα και ασυμβίβαστα του ΥΑΣΠΕ - II

- ✓ Τα καθήκοντα του ΥΑΣΠΕ είναι **ασυμβίβαστα** με αυτά του Υπευθύνου Προστασίας Δεδομένων (DPO) του άρθρου 37 του GDPR, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων
- ✓ Τα καθήκοντα του ΥΑΣΠΕ είναι **ασυμβίβαστα** με αυτά του Υπευθύνου για τα αντικείμενα των τεχνολογιών πληροφορικής και επικοινωνίας (ΤΠΕ) και της ηλεκτρονικής διακυβέρνησης της Οντότητας
- ✓ Η παράλειψη ορισμού ΥΑΣΠΕ από τις υπόχρεες οντότητες συνιστά σοβαρή παράλειψη συμμόρφωσης και αντιμετωπίζεται ανάλογα από την ΕΑΚ – Οφείλει η Οντότητα να δηλώσει τον ΥΑΣΠΕ στην Ψηφιακή Πλατφόρμα της ΕΑΚ
- ✓ Στους φορείς της κεντρικής κυβέρνησης ορίζεται υπάλληλος κατηγορίας ΠΕ κλάδου Πληροφορικής οποιασδήποτε ειδικότητας ή κατηγορίας ΤΕ κλάδου Πληροφορικής (SOFTWARE ή HARDWARE) με τον αναπληρωτή του. Ελλείφει υπαλλήλου κατηγορίας ΠΕ ή ΤΕ κλάδου Πληροφορικής, ορίζεται υπάλληλος οποιουδήποτε κλάδου κατηγορίας ΠΕ ή ΤΕ βάσει της εμπειρίας του



Άρθ. 5 - Υποχρεώσεις προηγούμενου ελέγχου ιστορικού του ΥΑΣΠΕ

- ✓ Οι Οντότητες υποχρεούνται να διασφαλίζουν ότι ο **ΥΑΣΠΕ**:
 - υποβάλλεται σε κατάλληλους ελέγχους ιστορικού προτού αναλάβει καθήκοντα, βασιζόμενες στα προσόντα και τις δεξιότητες του
- ✓ Προηγούμενος έλεγχος ιστορικού απαιτείται ανάλογα με:
 - Ρόλους και επίπεδα πρόσβασης
 - Ιδιαιτερότητες των καθηκόντων
 - Επίπεδο πρόσβασης σε συστήματα και πληροφορίες
 - Κατηγοριοποίηση πληροφοριών και επιχειρηματικοί κίνδυνοι
- ✓ Πολιτική ελέγχων αναθεωρείται περιοδικά και προσαρμόζεται στις μεταβαλλόμενες ανάγκες και το περιβάλλον
- ✓ Αρχές διενέργειας ελέγχων κατά τη διενέργεια προηγούμενων ελέγχων ιστορικού του ΥΑΣΠΕ:
 - Πριν την ανάληψη καθηκόντων
 - Αναλόγως της ευαισθησίας της θέσης
 - Εξέταση επαγγελματικής πορείας και ηθικής του υποψηφίου
 - Συμμόρφωση με ευρωπαϊκές και εθνικές διατάξεις προστασίας δεδομένων (GDPR)
 - Δεοντολογικές αρχές: διακριτικότητα, εχεμύθεια, διαφάνεια, καλής πίστης και χρηστών ηθών
 - Έλεγχος ανάλογος με τον επιχειρηματικό κίνδυνο της θέσης

Άρθ. 6 - Καθήκοντα και υποχρεώσεις του ΥΑΣΠΕ - I

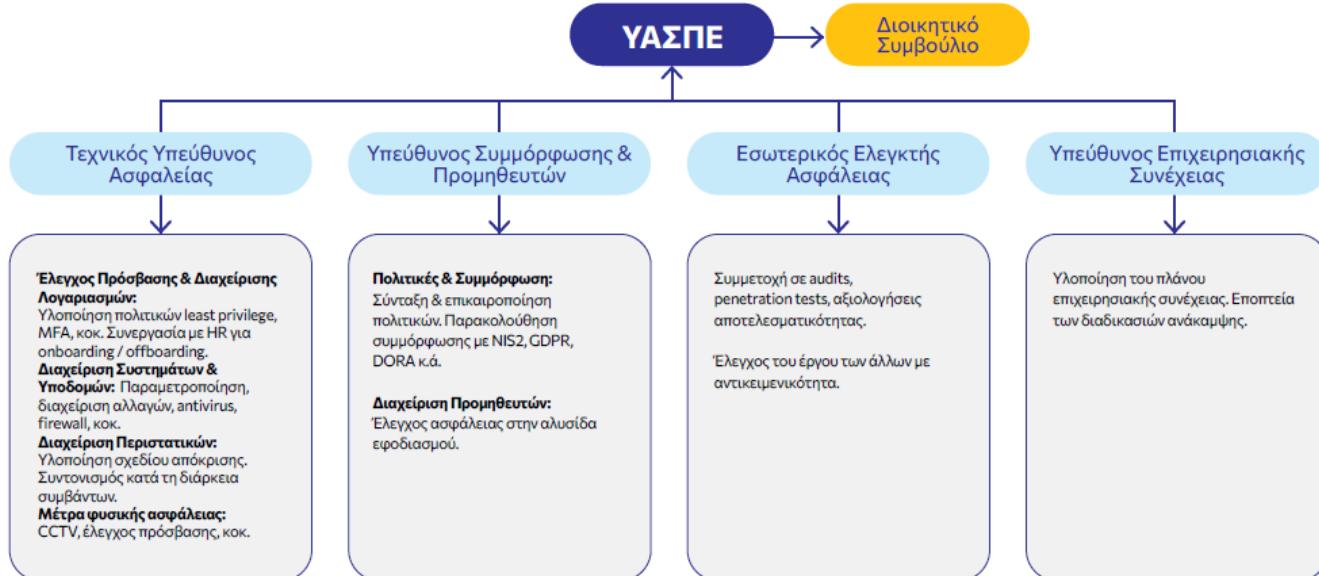
- Η διαρκής μέριμνα για την **ασφάλεια των συστημάτων δικτύου και πληροφοριών** της Οντότητας και η εποπτεία της υλοποίησης των μέτρων κυβερνοασφάλειας
- Η διαχείριση των **πάσης φύσεως επικοινωνιών** και επαφών με την ΕΑΚ
- Η ανάπτυξη **επαφών με εξειδικευμένα fora ασφάλειας** και **ομάδες ειδικού ενδιαφέροντος στον κυβερνοχώρο**, καθώς και επαγγελματικές **ενώσεις** με συναφή δραστηριότητα
- Η επιμέλεια & ο συντονισμός για τη **συμμόρφωση** της Οντότητας με τις **απαιτήσεις** του άρθρου 15 του ν. 5160/2024 και της KYA 1689/30.04.2025 για **μέτρα διαχείρισης κινδύνων κυβερνοασφάλειας**
- **Εκπαίδευση & ευαισθητοποίηση** των μελών των οργάνων διοίκησης και των λοιπών στελεχών της Οντότητας
- Η επιμέλεια & ο συντονισμός αναφορικά με την **κοινοποίηση σημαντικών περιστατικών** και κυβερνοαπειλών **στο αρμόδιο CSIRT**
- Η εποπτεία της **τήρησης & ο συντονισμός της εφαρμογής της ενιαίας πολιτικής κυβερνοασφάλειας** της Οντότητας με τη χρήση κατάλληλων προτύπων και διεθνών πρακτικών
- Η συνεργασία με τις λοιπές αρμόδιες αρχές για θέματα κυβερνοασφάλειας και η εφαρμογή των κατευθυντήριων οδηγιών, απαιτήσεων και μέτρων ασφαλείας που εκδίδουν
- **Υπολογισμό του συνολικού κινδύνου, ως συνδυασμού της πιθανότητας πραγματοποίησης των απειλών**
- Η παρουσίαση **της στρατηγικής και της πολιτικής κυβερνοασφάλειας στα όργανα διοίκησης της Οντότητας για έγκριση** και η ενημέρωση αυτών σχετικά με τις κυβερνοαπειλές και τους κινδύνους

Άρθ. 6 - Καθήκοντα και υποχρεώσεις του ΥΑΣΠΕ - II

- Μέτρα ασφάλειας της αλυσίδας εφοδιασμού κατά την εκκίνηση των διαδικασιών προμήθειας εξοπλισμού και ανάθεσης παροχής υπηρεσιών ΤΠΕ
- Καθορισμό, έγκριση και εφαρμογή διαδικασιών για την ανάλυση κινδύνων, την επιχειρησιακή συνέχεια και την ανάκαμψη της Οντότητας από καταστροφές
- Τήρηση μητρώου της Οντότητας με τις υποδομές πληροφορικής και επικοινωνιών, το λογισμικό και τα πληροφοριακά αγαθά
- Συμμετοχή στη διενέργεια ελέγχων και επιτόπιων επιθεωρήσεων από πιστοποιημένους επιθεωρητές και τεχνικούς εμπειρογνώμονες ή αρμόδια όργανα της ΕΑΚ
- Δύναται να ασκεί και άλλα καθήκοντα, εφόσον η άσκησή τους δεν παρακωλύει την αποτελεσματική εκπλήρωση του έργου του και δεν προκαλείται σύγκρουση συμφερόντων
- Τα όργανα διοίκησης της διασφαλίζουν ότι ο ΥΑΣΠΕ διαθέτει κατάλληλο και επαρκές επίπεδο αυτονομίας στη λήψη αποφάσεων. Ο ΥΑΣΠΕ λογοδοτεί απευθείας στο ανώτατο διοικητικό επίπεδο της Οντότητας
- Συνεργασία με τους πιστοποιημένους επιθεωρητές και τεχνικούς Εμπειρογνώμονες και τα αρμόδια όργανα της ΕΑΚ για τη διενέργεια σαρώσεων ασφαλείας
- Απόκριση επί αιτημάτων παροχής πληροφοριών, πρόσβασης σε δεδομένα και αποστολής αποδεικτικών στοιχείων
- Παρακολούθηση & αξιοποίηση νέων τεχνολογιών και εργαλείων ασφάλειας συστημάτων ΤΠΕ για την ενίσχυση του επιπέδου κυβερνοασφάλειας
- Δεσμεύεται, κατά την εκτέλεση των καθηκόντων του, από την τήρηση της εμπιστευτικότητας και του απορρήτου
- Αν στα συστήματα ΤΠΕ λαμβάνει χώρα επεξεργασία δεδομένων προσωπικού χαρακτήρα απευθύνεται στο DPO για οδηγίες
- Αν στα συστήματα ΤΠΕ λαμβάνει χώρα επεξεργασία Διαβαθμισμένων Πληροφοριών και Υλικού, σύμφωνα με τον Εθνικό Κανονισμό Ασφάλειας (B'683/2018) ή τον Εθνικό Κανονισμό Βιομηχανικής Ασφάλειας (B'4071/2020), ο Υ.Α.Σ.Π.Ε. απευθύνεται αμελλητί στην ΕΑΚ ή τις λοιπές αρμόδιες εθνικές αρχές

Ομάδα Κυβερνοασφάλειας - Παράδειγμα

- Διατομεακό όργανο με επικεφαλής τον ΥΑΣΠΕ, επανδρωμένο με στελέχη των τμημάτων πληροφορικής, διαχείρισης κινδύνου, νομικών υποθέσεων, προστασίας δεδομένων προσωπικού χαρακτήρα, κοκ. Η σύνθεσή της εξαρτάται από το μέγεθος, τις ανάγκες και λειτουργίες της επιχείρησης



Πηγή: [Οδηγός για τη Συμμόρφωση των Επιχειρήσεων](#)

KYA 1689/2025 - Εθνικό Πλαίσιο Απαιτήσεων Κυβερνοασφάλειας Βασικών & Σημαντικών Οντοτήτων

- **Στόχος:** Ο καθορισμός του εθνικού πλαισίου απαιτήσεων κυβερνοασφάλειας, το οποίο περιλαμβάνει τα τεχνικά, επιχειρησιακά και οργανωτικά μέτρα διαχείρισης των κινδύνων κυβερνοασφάλειας της παρ. 2 του άρ. 15 του Ν. 5160/2024 (NIS2)
- Οι απαιτήσεις & τα μέτρα διαχείρισης των κινδύνων κυβερνοασφάλειας βασίζονται σε ολιστική προσέγγιση του κινδύνου (*all hazards approach*), που αποσκοπεί στην προστασία των συστημάτων δικτύου & πληροφοριών και του φυσικού περιβάλλοντος των εν λόγω συστημάτων από περιστατικά, εξασφαλίζοντας επίπεδο ασφάλειας ανάλογο προς τον εκάστοτε κίνδυνο
- Γενικές αρχές εφαρμογής με βάση την αρχή της αναλογικότητας (*proportionality principle*) λαμβάνοντας υπ' όψιν:
 - ✓ Το μέγεθος και η πολυπλοκότητα των επιχειρησιακών λειτουργιών
 - ✓ Το είδος και η κρισιμότητα των δεδομένων επεξεργάζονται
 - ✓ Το βαθμό έκθεσης της οντότητας σε κινδύνους
 - ✓ Την πιθανότητα εμφάνισης περιστατικών και τη σοβαρότητά τους
 - ✓ Τις κοινωνικές και οικονομικές επιπτώσεις από την εμφάνιση περιστατικών
 - ✓ Το κόστος υλοποίησης του μέτρου σε σχέση με τα προσδοκώμενα οφέλη

Τεκμηρίωση



- Έγγραφα ψηφιακής ή φυσικής μορφής:
 - ✓ πολιτικές ασφάλειας & διαδικασίες
 - ✓ πρακτικά διοικητικού συμβουλίου
 - ✓ οικονομικά στοιχεία
 - ✓ Συμβάσεις
 - ✓ βεβαιώσεις εκπαίδευσης
 - ✓ διαγράμματα δικτύου
 - ✓ πλάνα επιχειρησιακής συνέχειας
 - ✓ έγγραφα περιοδικής αξιολόγησης μέτρων και διαδικασιών
 - ✓ αναφορές ελέγχων ασφάλειας
 - ✓ μηνύματα ηλεκτρονικού ταχυδρομείου)
- Τα τηρούμενα αποδεικτικά στοιχεία πρέπει να είναι επαρκή για την τεκμηρίωση συμμόρφωσης με τις οικείες υποχρεώσεις
- Στοιχεία τεκμηρίωσης που προκύπτουν μέσω της φυσικής παρατήρησης κατάλληλου δείγματος πληροφοριακών συστημάτων και εξέτασης των εφαρμοσμένων μέτρων ασφάλειας και διαδικασιών. Ενδεικτικά:
 - ✓ Τεχνολογίες ασφάλειας δικτύων
 - ✓ Μέτρα ασφάλειας σε συσκευές τελικού χρήστη και διακομιστές
 - ✓ κατανομή δικαιωμάτων πρόσβασης
 - ✓ μέτρα φυσικής ασφάλειας
- Στοιχεία τεκμηρίωσης που προκύπτουν μέσω συνεντεύξεων με κατάλληλο δείγμα μελών της διοίκησης και εργαζομένων της οντότητας

Υποχρεώσεις και ευθύνη των ανωτάτων οργάνων διοίκησης

- ❖ Η NIS2 δίνει έμφαση στις υποχρεώσεις & τη λογοδοσία της Ανώτατης Διοίκησης
- ❖ Η συμμόρφωση προϋποθέτει την ενεργή συμμετοχή των διοικούντων

- Ευθύνη του κατά περίπτωση ανώτατου οργάνου διοίκησης αποτελεί η διαμόρφωση & υλοποίηση ολοκληρωμένου προγράμματος διαχείρισης των κινδύνων κυβερνοασφάλειας που περιλαμβάνει:
 - ✓ Πολιτικές & Διαδικασίες
 - ✓ Ανάθεση ρόλων, αρμοδιοτήτων και ευθυνών
 - ✓ Σύνολο τεχνικών, οργανωτικών & επιχειρησιακών μέτρων για την ασφάλεια των συστημάτων δικτύου & πληροφοριών

- Εγκρίνει, επιβλέπει, αξιολογεί & εποπτεύει το πρόγραμμα διαχείρισης των κινδύνων κυβερνοασφάλειας
- Παρέχει τους απαραίτητους πόρους για την υλοποίηση του προγράμματος και τη διαχείριση των κινδύνων
- Εξασφαλίζει ότι το σύνολο του προσωπικού ενημερώνεται για τις υποχρεώσεις και τις ευθύνες του όσον αφορά στην τήρηση και εφαρμογή της πολιτικής ασφάλειας κτλ.
- Η οικεία οντότητα τηρεί τα στοιχεία τεκμηρίωσης
- Παρακολουθεί σε περιοδική βάση πρόγραμμα εκπαίδευσης για θέματα κυβερνοασφάλειας και διασφαλίζει ότι παρέχεται αντίστοιχο πρόγραμμα και στο προσωπικό της

Πλαίσιο Διαχείρισης Κινδύνων



- **Πλαίσιο για τη διαχείριση των κινδύνων:**
 - Ανάπτυξη και τήρηση πλαισίου διαχείρισης κινδύνων κυβερνοασφάλειας
 - Ευθυγράμμιση με τη συνολική στρατηγική διαχείρισης επιχειρηματικών κινδύνων
 - Συνεκτίμηση σχέσεων με τρίτα μέρη, προμηθευτές και παρόχους υπηρεσιών
- **Εκτίμηση Κινδύνων (Risk Assessment):**
 - Περιοδική και αναλογική εκτίμηση κινδύνων
 - Διαδικασίες αναγνώρισης, ανάλυσης και αξιολόγησης κινδύνων
 - Μεθοδολογίες βάσει διεθνών προτύπων ή βέλτιστων πρακτικών
- **Πρόσθετες Υποχρεώσεις για Βασικές Οντότητες:**
 - Εμπεριστατωμένες εκτιμήσεις κινδύνων
 - Χρήση πληροφοριών **Cyber Threat Intelligence** από αξιόπιστες πηγές
 - Αξιολόγηση ευπαθειών (**Vulnerability Assessment**) των συστημάτων
- **Πλάνο Αντιμετώπισης Κινδύνων (Risk Treatment Plan):**
 - Αποτελέσματα risk assessment
 - Αξιολόγηση αποτελεσματικότητας μέτρων
 - Κόστος – όφελος
 - Ταξινόμηση Αγαθών & Δεδομένων (Υλισμικό & Λογισμικό)
 - Ανάλυση επιχειρηματικών επιπτώσεων
- **Επικαιροποίηση:**
 - Περιοδική αναθεώρηση risk assessment & treatment plan ή μετά από:
 - Σοβαρά περιστατικά κυβερνοασφάλειας
 - Οργανωτικές/λειτουργικές αλλαγές
 - Μεταβολές στο περιβάλλον κυβερνοαπειλών



Πολιτικές και Διαδικασίες Ασφάλειας Πληροφοριών

▪ Γενική Πολιτική Ασφάλειας:

- Γραπτή πολιτική, εγκεκριμένη από το ανώτατο όργανο διοίκησης
- Καθορίζει τη στρατηγική προσέγγιση για τη διαχείριση της ασφάλειας των συστημάτων δικτύου και πληροφοριών της οντότητας

▪ Θεματικές Πολιτικές Ασφάλειας

- Καλύπτουν ειδικές πτυχές κυβερνοασφάλειας (ανθρώπινο δυναμικό, διαδικασίες, τεχνολογίες)
- **Εγκρίνονται επίσης από το ανώτατο όργανο διοίκησης**



▪ Ελάχιστες Θεματικές Πολιτικές Ασφάλειας:

- Έλεγχος πρόσβασης
- Διαχείριση αγαθών
- Ορθή χρήση αγαθών & δεδομένων
- Αφαιρούμενα μέσα αποθήκευσης
- Διαχείριση περιστατικών κυβερνοασφάλειας
- Ασφάλεια εφοδιαστικής αλυσίδας
- Ασφάλεια δικτύων
- Διενέργειας Ελέγχων Κυβερνοασφάλειας
- Αντίγραφα ασφαλείας
- Κρυπτογράφηση δεδομένων & επικοινωνιών
- Φυσική & περιβαλλοντική ασφάλεια

▪ Αξιολόγηση & Επικαιροποίηση:

- Περιοδική ή μετά από:
 - Σοβαρά περιστατικά κυβερνοασφάλειας
 - Οργανωτικές/λειτουργικές αλλαγές

Ρόλοι, αρμοδιότητες & εξουσίες - Ανεξάρτητος έλεγχος ασφάλειας πληροφοριών



- **Καθορισμός Αρμοδιοτήτων & Ρόλων:**
 - Οι ρόλοι ανατίθενται βάσει επιχειρηματικών αναγκών ή θεσμικών αρμοδιοτήτων
 - Ανάλογα με το μέγεθος και την κρισιμότητα, δύνανται να ορίζονται επιπρόσθετοι ρόλοι πέραν του ΥΑΣΠΕ
- **Ο ΥΑΣΠΕ αναφέρεται απευθείας στο ανώτατο όργανο διοίκησης για όλα τα θέματα κυβερνοασφάλειας**
- **Αξιολόγηση & Επικαιροποίηση:**
 - Περιοδική ή μετά από:
 - Σοβαρά περιστατικά κυβερνοασφάλειας
 - Οργανωτικές/λειτουργικές αλλαγές

- **Περιοδικοί Ανεξάρτητοι Έλεγχοι (Independent Audits):**
 - Στο σύνολο των παραμέτρων του προγράμματος διαχείρισης ασφάλειας πληροφοριών της, συμπεριλαμβανομένων του προσωπικού, των πολιτικών, των διαδικασιών και των τεχνολογιών που χρησιμοποιεί
 - Η οντότητα εγγυάται την αμεροληφία των προσώπων που διεξάγουν τους ελέγχους ασφάλειας πληροφοριών
 - Εφόσον προκύψει ανεπαρκής υλοποίηση μέτρων κυβερνοασφάλειας, το ανώτατο όργανο διοίκησης διαδικασίες διορθωτικών ενεργειών
 - Οι έλεγχοι πραγματοποιούνται:
 - Σε προγραμματισμένα χρονικά διαστήματα
 - Όταν προκύπτουν σοβαρά περιστατικά κυβερνοασφάλειας
 - Όταν συμβαίνουν σημαντικές λειτουργικές αλλαγές
 - Όταν μεταβάλλεται το διεθνές περιβάλλον κυβερνοαπειλών

Διαδικασίες παρακολούθησης της συμμόρφωσης - Ασφάλεια ανθρώπινου δυναμικού

- **Διαδικασίες Παρακολούθησης Συμμόρφωσης:**
 - Εφαρμόζονται διαδικασίες παρακολούθησης & αξιολόγησης της συμμόρφωσής με τις κανονιστικές υποχρεώσεις κυβερνοασφάλειας
 - Τα αποτελέσματα της παρακολούθησης υποβάλλονται περιοδικά στο ανώτατο όργανο διοίκησης
 - **Αντιμετώπιση Μη Συμμόρφωσης:**
 - Το ανώτατο όργανο διοίκησης εκκινεί διαδικασίες διορθωτικών ενεργειών για την αποκατάσταση της συμμόρφωσης
 - **Χρονοπρογραμματισμός Παρακολούθησης:**
 - Σε προγραμματισμένα χρονικά διαστήματα
 - Όταν υπάρχουν μεταβολές στο σχετικό κανονιστικό πλαίσιο
 - Όταν υφίστανται σημαντικές αλλαγές στις λειτουργίες της οντότητας
- Η οντότητα εφαρμόζει διαδικασίες ελέγχου καταληλότητας για το υποψήφιο προσωπικό
 - Καθορίζονται και κοινοποιούνται οι ευθύνες που εξακολουθούν να ισχύουν μετά τη λήξη ή αλλαγή απασχόλησης
 - Υλοποιούνται διαδικασίες πειθαρχικού ελέγχου για προσωπικό που παραβιάζει τη γενική ή θεματικές πολιτικές ασφάλειας της οντότητας
 - Διενεργούνται έλεγχοι επαλήθευσης ιστορικού (background checks) του υποψήφιου προσωπικού
 - Εξετάζονται ζητήματα αμεροληψίας και ακεραιότητας όπου απαιτείται
 - Τα μέτρα αφορούν προσωπικό με ρόλους και αρμοδιότητες κυβερνοασφάλειας, με σκοπό τη διασφάλιση της διαρκούς καταληλότητας, ικανότητας και αξιοπιστίας του

Διαχείριση Υλισμικού και Λογισμικού

- **Κατάλογος Αγαθών Πληροφορικής:**
 - Υλισμικό, λογισμικό, συστήματα, κατηγορίες δεδομένων, υπηρεσίες
 - Συμπεριλαμβάνονται και τα αγαθά επιχειρησιακής τεχνολογίας (OT), εφόσον υπάρχουν
 - Για κάθε αγαθό ορίζεται ιδιοκτήτης (owner), υπεύθυνος για τη διαχείριση και συντήρησή του
- **Ταξινόμηση Δεδομένων & Αγαθών σε διακριτά επίπεδα βάσει:**
 - Εμπιστευτικότητας, Ακεραιότητας, Διαθεσιμότητας
 - Η αντιστοίχιση κάθε αγαθού και συνόλου δεδομένων με ένα επίπεδο ταξινόμησης γίνεται ανάλογα με την ευαισθησία, κρισιμότητα και επιχειρηματική τους αξία
- **Πολιτική Ορθής Χρήσης Αγαθών & Δεδομένων:**
 - Εκπονείται γραπτή πολιτική και οδηγίες για την ορθή χρήση των αγαθών καθ' όλη τη διάρκεια του κύκλου ζωής τους
 - Προμήθεια → Χρήση → Αποθήκευση → Μεταφορά → Ασφαλής απομάκρυνση / διαγραφή
- **Πολιτική Διαχείρισης Αφαιρούμενων Μέσων:**
 - Καθορίζεται πολιτική ασφαλούς διαχείρισης αφαιρούμενων μέσων αποθήκευσης σύμφωνα με το σύστημα ταξινόμησης αγαθών και δεδομένων



Διαχείριση κινδύνων από τις σχέσεις με προμηθευτές και παρόχους υπηρεσιών ΤΠΕ - I



- **Βασικές Απαιτήσεις:**
- **Πολιτική & Διαδικασίες:** Καθορισμός πολιτικών για τη διαχείριση κινδύνων από προμηθευτές και παρόχους ΤΠΕ
- **Κατάλογος Προμηθευτών:** Τήρηση ενημερωμένου μητρώου με στοιχεία επαφής, παρεχόμενα προϊόντα/υπηρεσίες και ταξινόμηση κρισιμότητας Ενδεικτικά:
 - παραγωγοί/κατασκευαστές προϊόντων υλικού & λογισμικού
 - πάροχοι υπηρεσιών νεφοϋπολογιστικής
 - πάροχοι διαχειριζόμενων υπηρεσιών
 - πάροχοι διαχειριζόμενων υπηρεσιών ασφάλειας
- **Διαδικασίες Διαχείρισης Κινδύνων που σχετίζονται με την απόκτηση εξοπλισμού και την παροχή υπηρεσιών σε Όλο τον Κύκλο Ζωής):**
 - Εφαρμογή διαδικασιών για την απόκτηση, χρήση και διαχείριση εξοπλισμού & υπηρεσιών Τ.Π.Ε.
 - Περιλαμβάνει και χρήση υπηρεσιών νεφοϋπολογιστικής (cloud).
 - Ελάχιστα περιλαμβανόμενα:
 - **Αξιολόγηση & επιλογή προμηθευτών:** επίπεδο κυβερνοασφάλειας, πιστοποιήσεις, δυνατότητα ελέγχου, αξιολογήσεις πελατών
 - **Καθορισμός απαιτήσεων ασφάλειας** για τις υποδομές και τεχνολογίες που χρησιμοποιούν οι πάροχοι
 - **Καθορισμός απαιτήσεων ασφάλειας** για τα προς απόκτηση προϊόντα, συστήματα και υπηρεσίες

Διαχείριση κινδύνων από τις σχέσεις με προμηθευτές και παρόχους υπηρεσιών ΤΠΕ - II

- **Διαδικασίες Διαχείρισης Κινδύνων που σχετίζονται με την απόκτηση εξοπλισμού και την παροχή υπηρεσιών σε Όλο τον Κύκλο Ζωής):**
- **Συμβάσεις Προμηθειών και Παροχής Υπηρεσιών ΤΠΕ περιλαμβάνουν τουλάχιστον:**
 - Απαιτήσεις κυβερνοασφάλειας για προϊόντα & υπηρεσίες
 - Περιγραφή συστημάτων και δεδομένων στα οποία υπάρχει πρόσβαση
 - Δικαιώμα ελέγχου ή απαίτηση για αναφορές/αποτελέσματα ελέγχων
 - Υποχρεώσεις για ασφαλή λήξη: διαγραφή προσβάσεων, ασφαλής διαγραφή δεδομένων, εμπιστευτικότητα
- **Περιοδική Αξιολόγηση & Επικαιροποίηση**
- **Τακτική αναθεώρηση πολιτικών και διαδικασιών βάσει:**
 - Άλλαγές πρακτικών προμηθευτών
 - Περιστατικά κυβερνοασφάλειας

- **Πρόσθετα μέτρα για βασικές οντότητες:**
 - Θέσπιση ενισχυμένων απαιτήσεων κυβερνοασφάλειας για κρίσιμους προμηθευτές/παρόχους (λόγω επιπτώσεων σε εθνική ασφάλεια, δημόσια υγεία, οικονομική σταθερότητα)
 - **Επέκταση της διαχείρισης κινδύνων σε όλη την εφοδιαστική αλυσίδα, με καθορισμό απαιτήσεων και για υπεργολάβους των αναδόχων προμηθευτών και παρόχων υπηρεσιών ΤΠΕ**



Διαχείριση λογαριασμών και έλεγχος πρόσβασης



■ Έλεγχος Πρόσβασης (Logical Access Control):

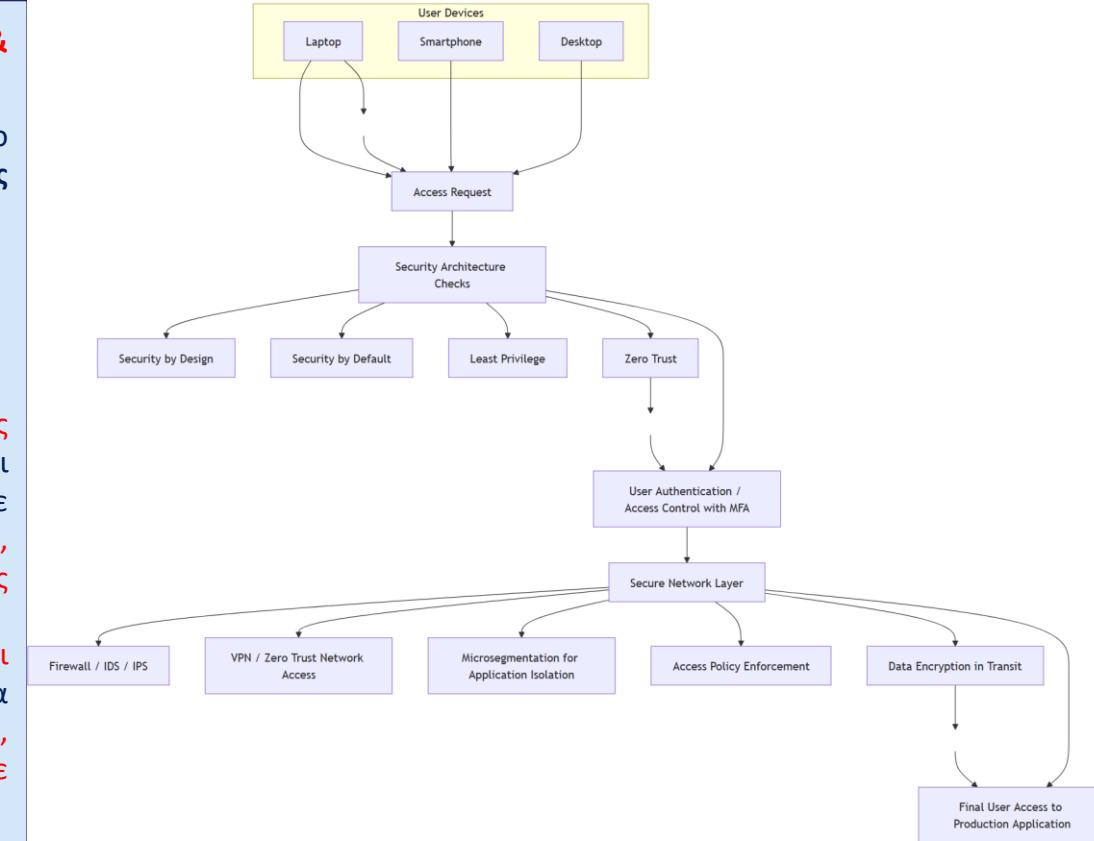
- Πολιτικές & Διαδικασίες Ασφαλούς Πρόσβασης στα Συστήματα ΤΠΕ:
- Εκπόνηση **πολιτικής και διαδικασιών** για τον **λογικό έλεγχο πρόσβασης**, με βάση τις επιχειρηματικές ανάγκες, τις αρμοδιότητες και τις απαιτήσεις ασφάλειας & **εφαρμόζεται** σε **προσωπικό και εξωτερικούς συνεργάτες / παρόχους ΤΠΕ**
- Χορήγηση **μοναδικής ταυτότητας (ID)** σε κάθε χρήστη ή σύστημα για **διασφάλιση λογοδοσίας** ενεργειών
- Ανάθεση & ανάκληση δικαιωμάτων βάσει:
 - Ελάχιστων προνομίων (**least privilege**)
 - Ανάγκης γνώσης (**need to know**)
 - Διαχωρισμού καθηκόντων (**separation of duties**)
- Περιορισμός προνομιούχων λογαριασμών μόνο όπου είναι απολύτως απαραίτητο, σύμφωνα με την κρισιμότητα λειτουργιών και δεδομένων
- Άμεση **τροποποίηση** ή **αφαίρεση δικαιωμάτων** σε περίπτωση αλλαγής ή αποχώρησης προσωπικού
- Εφαρμογή **ισχυρών μεθόδων αυθεντικοποίησης**, όπως:
 - Ισχυρά συνθηματικά, ψηφιακά πιστοποιητικά, έξυπνες κάρτες, βιομετρικά μέσα
- Ενεργοποίηση **πολυπαραγοντικής αυθεντικοποίησης (MFA)** όπου απαιτείται ανάλογα με την κρισιμότητα συστημάτων και δεδομένων
- **Περιοδική αξιολόγηση & επικαιροποίηση** πολιτικών ελέγχου πρόσβασης μετά από σημαντικές αλλαγές ή περιστατικά κυβερνοασφάλειας

Ασφαλής παραμετροποίηση υλισμικού, λογισμικού, υπηρεσιών και δικτύων - Διαχείριση αλλαγών

- **Διαδικασίες & Εργαλεία Ελέγχου Ρυθμίσεων:**
- Ανάπτυξη διαδικασιών & εργαλείων για επιβολή ρυθμίσεων/παραμετροποίησεων του υλικού, του λογισμικού των υπηρεσιών και του δικτύου' συμπεριλαμβανομένων και αυτών της ασφάλειας
- **Υλοποίηση Ασφαλούς Παραμετροποίησης (Secure Configuration):**
- Εφαρμογή προκαθορισμένων προτύπων (κατασκευαστών ή ανεξάρτητων οργανισμών)
- Υιοθέτηση γενικών αρχών κυβερνοασφάλειας:
 - Αρχή της ελάχιστης λειτουργικότητας (**Least Functionality**)
 - Αρχή των ελάχιστων προνομίων (**Least Privilege**)
- **Τα προεπιλεγμένα συνθηματικά (default passwords) τροποποιούνται κατά την εγκατάσταση κάθε νέου προϊόντος, συστήματος ή εφαρμογής**
- **Περιοδική Αξιολόγηση & Αναθεώρηση διαδικασιών ασφαλούς παραμετροποίησης:**
- Με την εμφάνιση νέων απειλών ή ευπαθειών
- Με την εισαγωγή νέων εκδόσεων υλικού ή λογισμικού
- **Διαδικασίες για αλλαγές, επισκευές και συντήρηση:**
- **Αξιολόγηση αντικτύπου:** Εκτίμηση πιθανών επιπτώσεων των αλλαγών
- **Κατηγοριοποίηση & προτεραιοποίηση:** Ορισμός κριτηρίων για ταξινόμηση των αλλαγών
- **Υλοποίηση με πλάνο:** Εκτέλεση αλλαγών βάσει συγκεκριμένου σχεδίου
- **Δοκιμές & αποδοχή:** Δοκιμή αλλαγών και έγκριση αποτελεσμάτων
- **Αξιολόγηση & Επικαιροποίηση της διαδικασίας αλλαγών:**
- Περιοδική ανασκόπηση διαδικασιών
- Αναθεώρηση σε περιπτώσεις σοβαρών περιστατικών κυβερνοασφάλειας ή σημαντικών αλλαγών στις λειτουργίες της οντότητας

Αρχές ασφαλούς ανάπτυξης εφαρμογών

- **Καθορισμός Απαιτήσεων Ασφάλειας Αρχές & Πρακτικές:**
- Ορισμός απαιτήσεων ασφάλειας από το στάδιο σχεδιασμού και προδιαγραφών βάσει κρισιμότητας εφαρμογών και ανάλυσης κινδύνων
- Εφαρμογή στην Αρχιτεκτονική των:
 - Ασφάλεια από το σχεδιασμό (*Security by Design*)
 - Ασφάλεια εξ ορισμού (*Security by Default*)
 - Ελάχιστα προνόμια (*Least Privilege*)
 - Μηδενική εμπιστοσύνη (*Zero Trust*)
- Τα περιβάλλοντα ανάπτυξης, δοκιμών και παραγωγής των εφαρμογών που αποκτά ή αναπτύσσει είναι διαχωρισμένα μεταξύ τους και προστατευμένα με κατάλληλα μέτρα ασφάλειας (διαχωρισμός δικτύων, ασφαλής διαμόρφωση συστημάτων, έλεγχος πρόσβασης)
- Υλοποιούνται διαδικασίες διενέργειας δοκιμών και τεχνικών ελέγχων ασφάλειας σε διάφορα στάδια ανάπτυξης των εφαρμογών που αποκτά ή αναπτύσσει, και, σε κάθε περίπτωση, προ της θέσης τους σε παραγωγική λειτουργία



Διαχείριση και γνωστοποίηση ευπαθειών

- **Πολιτικές και Διαδικασίες:** Ορισμός και εφαρμογή διαδικασιών για εντοπισμό, αξιολόγηση και αντιμετώπιση ευπαθειών στα συστήματα **δικτύου και πληροφορικής**
- **Τακτική παρακολούθηση συλλογή & ανάλυση πληροφοριών για τεχνικές ευπάθειες μέσω:** Αρμόδιων αρχών
 - Ερευνητικών οργανισμών, Προμηθευτών / Παρόχων υπηρεσιών, CSIRTs
- Εγκατάσταση **security patches** σε **κρίσιμα συστήματα** εντός εύλογου διαστήματος (Εξαιρέσεις επιτρέπονται με τεκμηρίωση και αντισταθμιστικά μέτρα)
- **Δοκιμή ενημερώσεων σε ελεγχόμενο περιβάλλον** πριν την εγκατάσταση σε παραγωγικά συστήματα, εφόσον απαιτείται
- **Περιοδικές αυτοματοποιημένες σαρώσεις (vulnerability scanning)** και καταγραφή αποτελεσμάτων
- Εφαρμογή σχεδίου **προτεραιοποίησης** για **αποκατάσταση ευπαθειών** με βάση σοβαρότητα και κρισιμότητα δεδομένων (**Τεκμηρίωση** για ευπάθειες που δεν απαιτούν αποκατάσταση)
- Ορισμός & υλοποίηση διαδικασίας **για τη γνωστοποίηση μη δημόσια γνωστών ευπαθειών (zero-day vulnerabilities)** που αφορούν στα συστήματα **δικτύου και πληροφοριών** προς το αρμόδιο CSIRT

Αξιολόγηση της αποτελεσματικότητας των μέτρων διαχείρισης κινδύνων κυβερνοασφάλειας



- **Εκπόνηση πολιτικής και διαδικασιών για διενέργεια ελέγχων κυβερνοασφάλειας στα συστήματα δικτύου και πληροφοριών της με στόχο την αξιολόγηση της αποτελεσματικότητας των μέτρων διαχείρισης κινδύνων κυβερνοασφάλειας που έχουν υλοποιηθεί σε αυτά. Οι εν λόγω διαδικασίες περιλαμβάνουν το πεδίο εφαρμογής, τη συχνότητα και το είδος των ελέγχων ασφάλειας**
- **Εξωτερικοί έλεγχοι παρείσδυσης (External Penetration Tests) τουλάχιστον μία φορά ετησίως ή μετά από σοβαρό περιστατικό**
- **Αποκατάσταση ελλείψεων και επικύρωση διορθωτικών ενεργειών με βάση πλάνο προτεραιοποίησης και κρισιμότητα ευρημάτων**
- **Αυτοξιολόγηση:** Ετήσια ή μετά από σοβαρό περιστατικό, με χρήση Οδηγού ΕΑΚ. Αποστολή αποτελεσμάτων και πλάνου διορθωτικών ενεργειών στην Εθνική Αρχή Κυβερνοασφάλειας
- **Επιπλέον μέτρα για βασικές οντότητες:**
 - Εσωτερικοί έλεγχοι παρείσδυσης (Internal Penetration Tests) μία φορά ετησίως ή μετά από σοβαρό περιστατικό με βάση το σχήμα ταξινόμησης των αγαθών και των δεδομένων
 - **Αποκατάσταση ελλείψεων και επικύρωση διορθωτικών μέτρων** μετά τον εσωτερικό έλεγχο παρείσδυσης με σαφές πλάνο προτεραιοποίησης

Ο Οδηγός Αυτοξιολόγησης Κυβερνοασφάλειας της ΕΑΚ



- <https://cyber.assessments.hcaa.gov.gr/>
- <https://cyber.gov.gr/wp-content/uploads/2025/03/Cybersecurity-Self-Assessment-Tool-Greek-version-4.zip>
- [Οδηγός Αυτοξιολόγησης Έγγραφο](#)

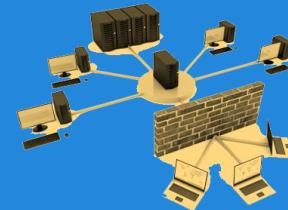


Microsoft Excel
ro-Enabled Works|

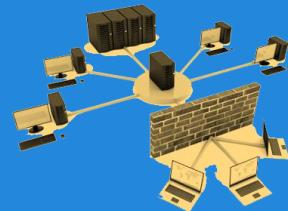
Περιέχει 234 Σημεία Ελέγχου χωρισμένα σε 19 Θεματικές Ενότητες

- | | |
|-----------------------------------------------------------------|----------------------------------------------------------------------|
| 1) Διοίκηση κυβερνοασφάλειας και διαχείριση επικινδυνότητας | 11) Απομακρυσμένη εργασία |
| 2) Καταγραφή υλικού και λογισμικού | 12) Χρήση κρυπτογραφίας |
| 3) Ασφαλής παραμετροποίηση εξοπλισμού και εφαρμογών | 13) Εκπαίδευση και ευαισθητοποίηση σε θέματα κυβερνοασφάλειας |
| 4) Έλεγχος εκτέλεσης προγραμμάτων και υπηρεσιών | 14) Διαχείριση κινδύνων στην εφοδιαστική αλυσίδα |
| 5) Διαχείριση λογαριασμών και έλεγχος πρόσβασης | 15) Υλοποίηση τεχνικών ελέγχων κυβερνοασφάλειας |
| 6) Αυθεντικοποίηση χρηστών | 16) Μέτρα φυσικής ασφάλειας εγκαταστάσεων |
| 7) Ασφάλεια δικτύων | 17) Λήψη αντιγράφων ασφαλείας (backup) |
| 8) Προστασία από κακόβουλο λογισμικό | 18) Αντιμετώπιση περιστατικών κυβερνοασφάλειας |
| 9) Τήρηση και ανάλυση αρχείων καταγραφής συμβάντων (event logs) | 19) Διασφάλιση επιχειρησιακής συνέχειας και ανάκαμψης από καταστροφή |
| 10) Ασφάλεια διαδικτυακών εφαρμογών | |

Ασφάλεια Δικτύων - I



- **Εκπόνηση γραπτής πολιτικής και διαδικασιών για την προστασία των δικτύων και δικτυακών συσκευών**
- **Τείχη προστασίας και προηγμένες τεχνολογίες**
 - περιορίζουν και φιλτράρουν τις δικτυακές συνδέσεις, για την προστασία του δικτύου της από μη εξουσιοδοτημένη πρόσβαση
 - Επιπλέον μέτρα ανάλογα με την επικινδυνότητα: intrusion detection/prevention systems (**IDS/IPS**), web application firewalls (**WAF**)
- **Έλεγχος Πρόσβασης**
 - Ασφαλής σύνδεση, αυθεντικοποίηση και εξουσιοδότηση χρηστών
 - Αποτροπή σύνδεσης μη εξουσιοδοτημένων συσκευών
 - Ισχυρά μέτρα για απομακρυσμένες συνδέσεις (συμπεριλαμβανομένων προμηθευτών/παρόχων)



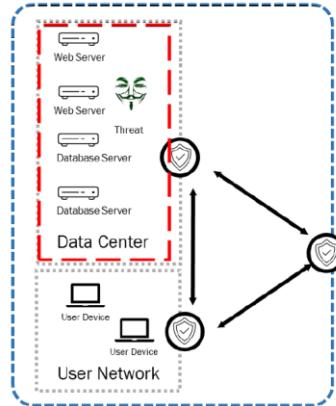
Ασφάλεια Δικτύων - II

- **Διαχείριση δικτυακής αρχιτεκτονικής**
 - Διαχωρισμός δικτύου σε διακριτά υποδίκτυα/ζώνες (network segmentation) ανάλογα με κρισιμότητα και ευαισθησία
 - Φιλτράρισμα δικτυακής κίνησης μεταξύ ζωνών.
 - Περιορισμός ανοιχτών θυρών, πρωτοκόλλων και υπηρεσιών στο απαραίτητο επίπεδο
- **Προστασία κρίσιμων υπηρεσιών και DNS**
 - Μέτρα για διαθεσιμότητα κρίσιμων υπηρεσιών και συνεχής λειτουργία
 - Βέλτιστες πρακτικές ασφάλειας DNS και ασφαλής δρομολόγηση δικτυακής κίνησης
 - τροπή σύνδεσης μη εξουσιοδοτημένων συσκευών
 - Ισχυρά μέτρα για απομακρυσμένες συνδέσεις (συμπεριλαμβανομένων προμηθευτών/παρόχων)
- **Τακτική αξιολόγηση και επικαιροποίηση πολιτικών & διαδικασιών** με αναπροσαρμογή σε σοβαρά περιστατικά κυβερνοασφάλειας, αλλαγές λειτουργιών ή μεταβολές διεθνούς περιβάλλοντος απειλών

Ασφάλεια Δικτύων - III

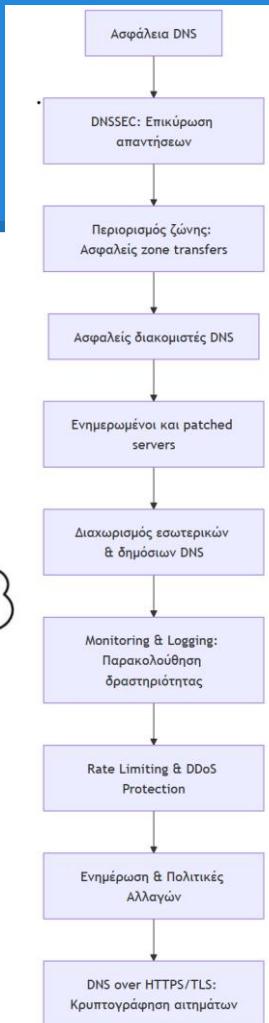
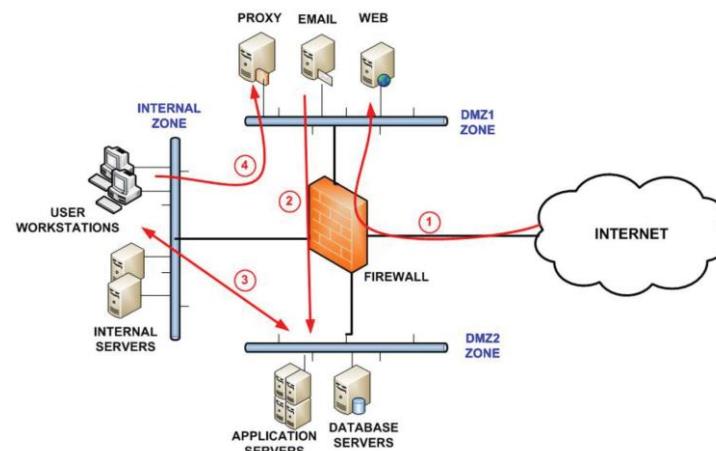
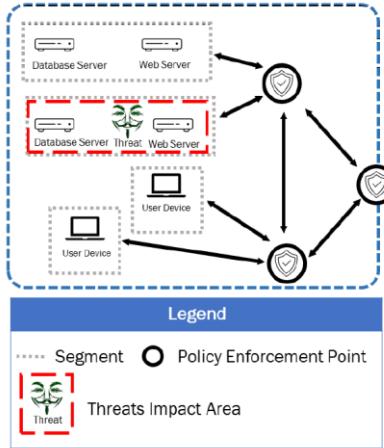
Allow by default

Traditional Segmentation



Deny by default

Microsegmentation



Πηγές: 1) https://www.cisa.gov/sites/default/files/2025-07/ZT-Microsegmentation-Guidance-Part-One_508c.pdf,

2) [Εγχειρίδιο-Κυβερνοασφάλειας](#),

Προστασία από Κακόβουλο Λογισμικό



- **Μέτρα:**
- Ύλοποίηση τεχνολογιών σε σταθμούς εργασίας, διακομιστές και δικτυακές συσκευές για ανίχνευση και εξουδετέρωση κακόβουλου λογισμικού
- Αυτόματες ενημερώσεις για όλες τις σχετικές τεχνολογίες
- **Έλεγχος εφαρμογών και λογισμικού:**
- Κανόνες και τεχνολογίες για περιορισμό εκτέλεσης μη εξουσιοδοτημένου λογισμικού
- Παρακολούθηση σταθμών εργασίας, διακομιστών και δικτυακών συσκευών
- **Προστασία από κακόβουλους ιστότοπους:**
- Φιλτράρισμα συνδέσεων με γνωστά κακόβουλα domains και ιστοτόπους

- **Φιλτράρισμα ηλεκτρονικού ταχυδρομείου:**
- Τεχνολογίες ανίχνευσης και απόρριψης κακόβουλων ή ανεπιθύμητων μηνυμάτων
- **Ασφαλείς φυλλομετρητές (web browsers):**
- Χρήση μόνο υποστηριζόμενων φυλλομετρητών
- Τακτικές ενημερώσεις και περιορισμός μη εξουσιοδοτημένων επεκτάσεων

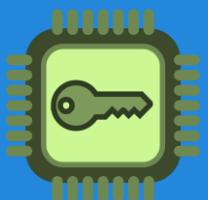
Εκπαίδευση και ευαισθητοποίηση σε θέματα κυβερνοασφάλειας



- **Προγράμματα για όλο το προσωπικό:**
- Περιοδικά προγράμματα εκπαίδευσης για όλο το προσωπικό και μέλη διοίκησης
- Παρέχουν βασικές πρακτικές κυβερνοϋγιεινής:
 - Ασφαλής χρήση email & αντιμετώπιση phishing/social engineering
 - Δημιουργία και διαχείριση ισχυρών κωδικών πρόσβασης
 - Πολυπαραγοντική αυθεντικοποίηση (MFA)
 - Ασφαλής πλοιήγηση στο διαδίκτυο
 - Ρυθμίσεις ασφάλειας για τηλεργασία και απομακρυσμένη πρόσβαση
 - Λήψη αντιγράφων ασφαλείας
 - Αναγνώριση και αναφορά συμβάντων κυβερνοασφάλειας

- **Προγράμματα για ειδικούς ρόλους:**
- Εκπαίδευση με βάση ρόλο και αρμοδιότητες στη διαχείριση συστημάτων και δικτύων:
 - Οδηγίες για ασφαλή παραμετροποίηση & λειτουργία συστημάτων και εφαρμογών
 - Ανάλυση γνωστών απειλών και κινδύνων
 - Διαχείριση και απόκριση σε περιστατικά κυβερνοασφάλειας

Τα προγράμματα εκπαίδευσης και ευαισθητοποίησης στην κυβερνοασφάλεια αξιολογούνται, επικαιροποιούνται βάσει αλλαγών σε κανονιστικές απαιτήσεις, μεταβολές στο τρέχον διεθνές περιβάλλον κυβερνοαπειλών, καθώς και τις τεχνολογικές εξελίξεις.



Χρήση Κρυπτογραφίας

- **Εκπόνηση γραπτής πολιτικής και διαδικασιών** για την εμπιστευτικότητα, αυθεντικότητα και ακεραιότητα των δεδομένων - συμμόρφωση με το σχήμα ταξινόμησης δεδομένων και αποτίμηση επικινδυνότητας
- **Κρυπτογράφηση δεδομένων αυξημένης κρισιμότητας:**
 - **At rest:** Δεδομένα σε υπολογιστές, διακομιστές, αφαιρούμενα μέσα, εφαρμογές και βάσεις δεδομένων
 - **In transit:** Δεδομένα κατά τη μεταφορά μέσω δικτύου
- **Διαδικασίες κρυπτογραφίας:**
 - Επιλογή τρόπων κρυπτογράφησης, πρωτοκόλλων και αλγορίθμων ανάλογα με την κατηγορία δεδομένων και το επίπεδο προστασίας
 - Διαχείριση κλειδιών και ψηφιακών πιστοποιητικών: Δημιουργία, διανομή, αποθήκευση, αλλαγή και ανάκληση

Αξιολόγηση και επικαιροποίηση διαδικασιών σε περιοδική βάση, λαμβάνοντας υπόψη τις εξελίξεις στις μεθόδους & τεχνολογίες κρυπτογράφησης



Φυσική και Περιβαλλοντική Ασφάλεια

- **Πολιτική & Διαδικασίες:** Εκπόνηση γραπτής πολιτικής και διαδικασιών που αφορούν στον φυσικό έλεγχο πρόσβασης (physical access control) στην υποδομή της και στους χώρους που φιλοξενούν πληροφοριακά της συστήματα, καθώς και στην προστασία τους από **φυσικούς** και **περιβαλλοντικούς** κινδύνους
- **Μέτρα Φυσικής Ασφάλειας:** Υλοποίηση επαρκών μέτρων ασφαλείας και επίβλεψης στην περίμετρο των εγκαταστάσεων και καθιέρωση διακριτών εσωτερικών ζωνών προστασίας, ανάλογα με τις απαιτήσεις κάθε περιοχής
- **Έλεγχος Πρόσβασης:** Περιορισμένη πρόσβαση σε κρίσιμους χώρους μόνο σε εξουσιοδοτημένο προσωπικό, με χρήση μεθόδων ταυτοποίησης, καταγραφής και επίβλεψης
- **Προστασία από Κινδύνους:** Εφαρμογή μέτρων προστασίας έναντι πυρκαγιάς, πλημμύρας, εγκληματικών ενεργειών και άλλων φυσικών ή περιβαλλοντικών απειλών
- **Υποστηρικτικά Συστήματα:** Προστασία και παρακολούθηση των μηχανισμών υποστήριξης της συνεχούς λειτουργίας των πληροφοριακών της συστημάτων, ιδίως όσον αφορά στα μέσα παροχής ηλεκτρισμού, νερού, εξαερισμού και κλιματισμού, από συμβάντα αστοχίας ή σοβαρής διατάραξης της λειτουργίας τους
- **Αξιολόγηση & Επικαιροποίηση:** σε προγραμματισμένα χρονικά διαστήματα και όταν λαμβάνουν χώρα σοβαρά περιστατικά φυσικής και περιβαλλοντικής ασφάλειας ή σημαντικές αλλαγές στις λειτουργίες της οντότητας

Διαχείριση περιστατικών κυβερνοασφάλειας



- **Ανάπτυξη Πολιτικής:**
- Γραπτή πολιτική διαχείρισης περιστατικών κυβερνοασφάλειας που περιλαμβάνει:
 - Ρόλους και διαδικασίες αναφοράς περιστατικών σε αρμόδιες αρχές
 - Πλάνο ανίχνευσης, ανάλυσης, απόκρισης, ανάκαμψης και επαναφοράς συστημάτων
- **Υπεύθυνος Διαχείρισης Περιστατικών:**
- Ορίζεται τουλάχιστον ένας υπάλληλος για τον συντονισμό της απόκρισης. Σε περίπτωση εξωτερικού αναδόχου, προβλέπεται υπάλληλος με ρόλο επίβλεψης
- **Καταγραφή Δραστηριοτήτων (Event Logging):**
- Τα πληροφοριακά συστήματα παραμετροποιούνται ώστε να καταγράφουν δραστηριότητες, ιδίως εκείνες που αφορούν **ευαίσθητα δεδομένα και λογαριασμούς αυξημένων προνομίων**

- **Διατήρηση & Προστασία Καταγραφών:**
- Οι καταγραφές συμβάντων τηρούνται για προκαθορισμένο χρονικό διάστημα, με **ασφαλή αποθήκευση** και **προστασία από μη εξουσιοδοτημένη πρόσβαση ή αλλοίωση**
- **Έλεγχος & Παρακολούθηση:**
- Οι καταγραφές ελέγχονται τακτικά για **ανίχνευση ύποπτων ενεργειών**. Σε περίπτωση αυτοματοποιημένης παρακολούθησης, έχουν οριστεί **όρια και ειδοποιήσεις** για έγκαιρη ανίχνευση περιστατικών

Αξιολόγηση & Επικαιροποίηση: Περιοδικά ή προκύψουν σοβαρά περιστατικά, αλλάζουν οι λειτουργίες της οντότητας, ή μεταβληθεί το διεθνές περιβάλλον κυβερνοαπειλών

Επιχειρησιακή Συνέχεια & Διαχείριση Κρίσεων



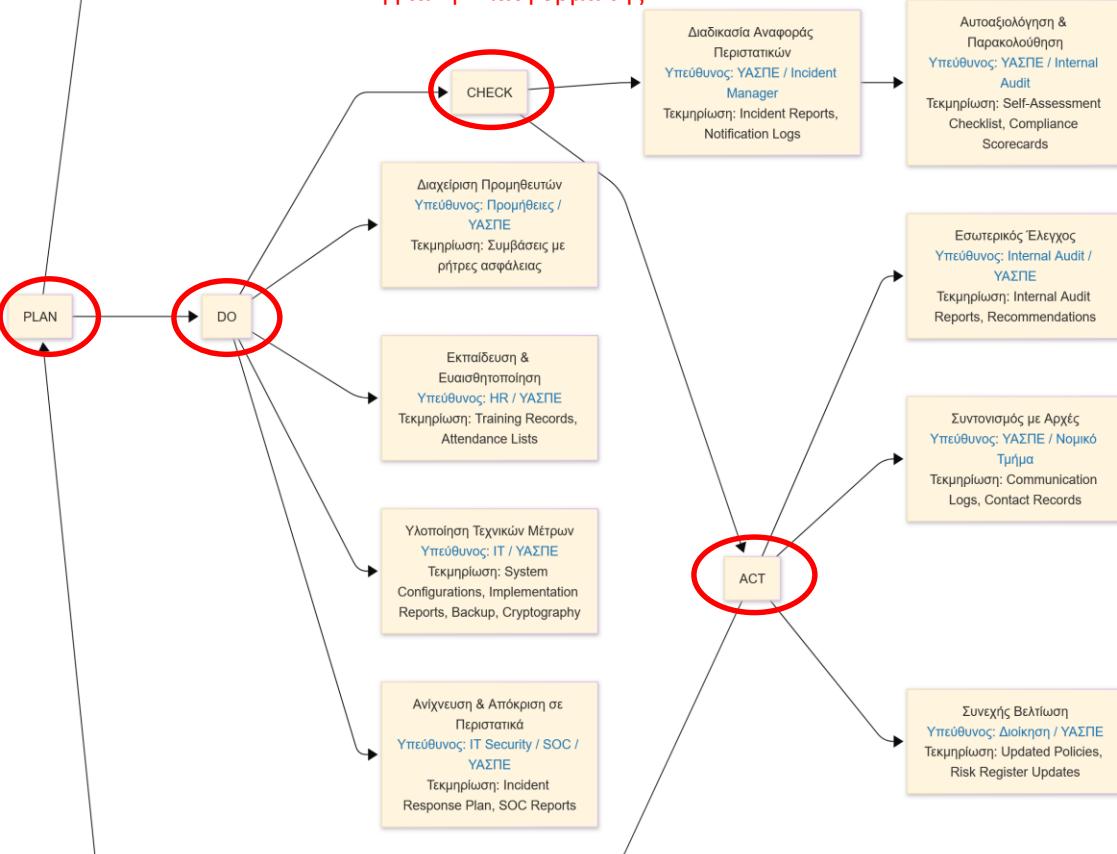
- **Πλάνο Επιχειρησιακής Συνέχειας & Ανάκαμψης από Καταστροφή (BCP/DRP):**
- βασίζεται στην **αποτίμηση κινδύνων** και περιλαμβάνει: **Σκοπό & πεδίο εφαρμογής, Ρόλους & αρμοδιότητες, Σημεία επαφής & κανάλια επικοινωνίας, Συνθήκες ενεργοποίησης του πλάνου, Δραστηρότητες ανάκαμψης ανά λειτουργία, Απαιτούμενους πόρους**
- **Ανάλυση Επιχειρηματικών Επιπτώσεων (Business Impact Analysis):**
- Αναγνώριση και αξιολόγηση επιπτώσεων από διαταράξεις· ανάπτυξη απαιτήσεων επιχειρησιακής συνέχειας για κρίσιμα συστήματα
- Το **πλάνο** επανεξετάζεται περιοδικά ή όταν προκύψουν σοβαρά περιστατικά ή αλλαγές στο περιβάλλον απειλών
- **Πολιτική & Διαδικασίες Αντιγράφων Ασφαλείας (Backups):** Καθορισμός τρόπου λήψης και ασφαλούς διαχείρισης αντιγράφων
- **Αυτοματοποιημένα Αντίγραφα Ασφαλείας:** Λήψη και τήρηση backups συστημάτων, εφαρμογών και δεδομένων με βάση την κρισιμότητά τους
- **Έλεγχος Πρόσβασης στα Αντίγραφα Ασφαλείας:** Εφαρμογή φυσικών και λογικών ελέγχων σύμφωνα με την ταξινόμηση των δεδομένων
- **Δοκιμές Επαναφοράς (Restoration Tests):** Τακτική δοκιμή επαναφοράς δειγματοληπτικών αντιγράφων για επαλήθευση αξιοπιστίας
- **Οι Βασικές οντότητες επιπλέον εφαρμόζουν:**
- Κατάρτιση και τήρηση διαδικασιών για τη διαχείριση κρίσεων σε περιπτώσεις ιδιαίτερα σοβαρών περιστατικών
- Με ανάθεση **Ρόλων & ευθυνών** στο προσωπικό, διαύλους **επικοινωνίας** με αρχές, οργανισμούς και κοινό και **Θέσπιση** μέτρων διατήρησης ασφάλειας των συστημάτων κατά τη διάρκεια της κρίσης
- Οι διαδικασίες κρίσεων επανεξετάζονται περιοδικά ή όταν αλλάζει το επιχειρησιακό ή το τρέχον διεθνές περιβάλλον κυβερνοαπειλών.

Διαδικασία Συμμόρφωσης

Η συμμόρφωση με τη
Νομοθεσία & την οδηγία NIS2
απαιτεί οργανωτικά, τεχνικά και
διοικητικά βήματα



Gap Analysis Tool (EAK)



Δεν ξεχνώ την Περιοδική ή Έκτακτη Αξιολόγηση & Επικαιροποίηση για το κάθε στάδιο όπως ορίζεται από την KYA και Συνεργασία με DPO όπου απαιτείται!

Μητρώο Υπηρεσιών & Συστημάτων βάσει της οδηγίας NIS2 (Asset Management)

A/A	Υπηρεσία/Σύστημα	Κατηγορία Υπηρεσίας	Κρίσιμη Περιγραφή Υπηρεσία (Ναι/Οχι)	Owner	Ευπάθειες ή Απειλές	Τεχνολογία/Πλατφόρμα	Αξιολόγηση Ασφάλειας (Περίοδος)	Πολιτική Αναφορών Ασφαλείας (Περιγραφή)	Αξιολόγηση Κρίσιμου Κινδύνου	Δικτυακές Πληροφορίες (IP/Υποδίκτυο)	Πολιτική Ασφάλειας	
1	Διακομιστής Ιστοσελίδας	Web Server	Φιλοξενία ιστοσελίδας e- commerce	A.A.	DDoS, SQL Injection	Apache, Nginx, Linux	Ετήσια Αξιολόγηση	Αναφορά εντός 24 ωρών	Κίνδυνος παραβιασης δεδομένων χρηστών.	IP: 192.168.1.10 Υποδίκτυο: 192.168.1.0/24	Πολιτική Συστήματος: Χρήση ισχυρών κωδικών, εγκατάσταση WAF, περιορισμός πρόσβασης ανά IP. Αντίδραση σε Επιθέσεις: Μόνιμο logging, ενεργοποίηση του DDoS protection	
2	Βάση Δεδομένων Πελατών	Database Server	Αποθήκευση προσωπικών δεδομένων	Nαι	A.A.	SQL Injection,	MySQL, MariaDB	Ετήσια Αξιολόγηση	Αναφορά εντός 48 ωρών	Κίνδυνος διαρροής προσωπικών δεδομένων.	IP: 192.168.1.20 Υποδίκτυο: 192.168.1.0/24	Πολιτική Συστήματος: Ενίσχυση κρυπτογράφησης, περιορισμός πρόσβασης με βάση ρόλους, τακτική αναβάθμωση. Αντίδραση σε Επιθέσεις: Ενεργοποίηση αναφορών για μη εξουσιοδοτημένη πρόσβαση, αμέσως αποκατάσταση.
3	FIREWALL	Δίκτυο	Προστασία από μη εξουσιοδοτη- μένη πρόσβαση	Nαι	A.A.	TCP Flood, DoS	Fortinet, Palo Alto	Ετήσια Αξιολόγηση	Αναφορά εντός 12 ωρών	Κίνδυνος παρακάμψης του firewall.	IP: 192.168.100.1 Υποδίκτυο: 192.168.100.0/24	Πολιτική Συστήματος: Διαχείριση κανόνων πρόσβασης, ενεργοποίηση logging, περιορισμός συνδέσεων από άγνωστες IP. Αντίδραση σε Επιθέσεις: Ενεργοποίηση αναφορών και άμεση ανάλυση για οποιαδήποτε παραβίαση των κανόνων.
4	Υπηρεσία Παροχής Ενέργειας	Κρίσιμη Υποδομή	Παροχή ενέργειας για λειτουργία οργανισμού	Nαι	A.A.	Στατική Διακοπή, Cyber-Physical Attacks	SCADA, PLCs, IoT	Ετήσια Αξιολόγηση	Αναφορά εντός 12 ωρών	Κίνδυνος διακοπής ενεργειακής τροφοδοσίας ή υποδομών.	IP: 192.168.10.10 Υποδίκτυο: 192.168.10.0/2 4	Πολιτική Συστήματος: Χρήση προστασίας από επιθέσεις σε SCADA, κρυπτογράφηση των επικοινωνιών, παρακολούθηση συνεχών των ενεργειακών συστημάτων για πιθανές αναμνησες. Αντίδραση σε Επιθέσεις: Άμεση αποσύνδεση από το δίκτυο σε περιπτώσεις αναγνωρισμένων επιθέσεων. Εφαρμογή στρατηγικής "Air Gap" (φυσική ή λογική απομόνωση) για κρίσιμα συστήματα ενέργειας.

Ανάλυση και Εκτίμηση Κινδύνου

1

- Εντοπίζονται οι πηγές απειλών που σχετίζονται με τον Οργανισμό (κακόβουλες ομάδες, ανταγωνιστές, άλλα κράτη, φυσικές απειλές, λάθη κ.λπ.).

2

- Εντοπίζονται οι ενέργειες / γεγονότα (*threat events*) που θα μπορούσαν να συμβούν από τις παραπάνω πηγές (κυβερνοεπιθέσεις, φυσικές καταστροφές, βλάβη υλικού κ.λπ.).

3

- Εντοπίζονται οι ευπάθειες του Οργανισμού που θα μπορούσε κάποια πηγή να τις εκμεταλλευτεί μέσω συγκεκριμένων ενεργειών / γεγονότων

4

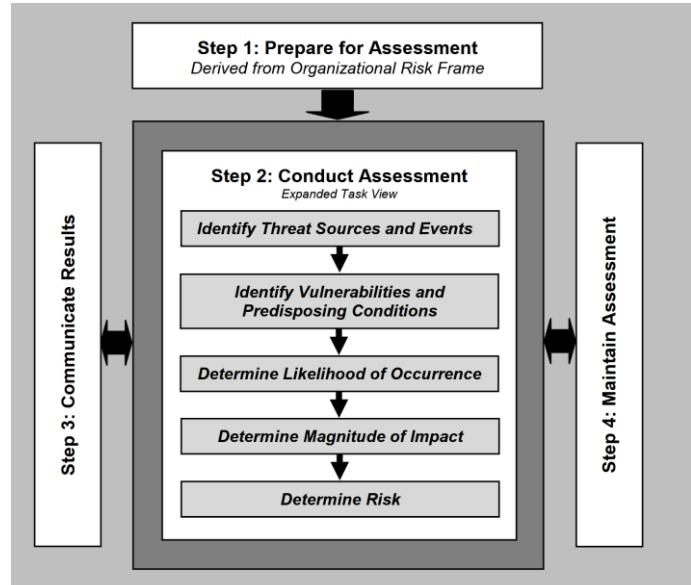
- Εκτιμάται η πιθανότητα ότι οι αναγνωρισμένες πηγές θα ξεκινήσουν συγκεκριμένες ενέργειες και η πιθανότητα επιτυχούς πραγματοποίησης των γεγονότων

5

- Εκτιμούνται οι δυσμενείς επιπτώσεις (στις λειτουργίες και συστήματα του Φορέα, σε πρόσωπα, σε άλλους Οργανισμούς ή στην ίδια την εθνική ασφάλεια) εάν οι ενέργειες / γεγονότα πραγματοποιηθούν

6

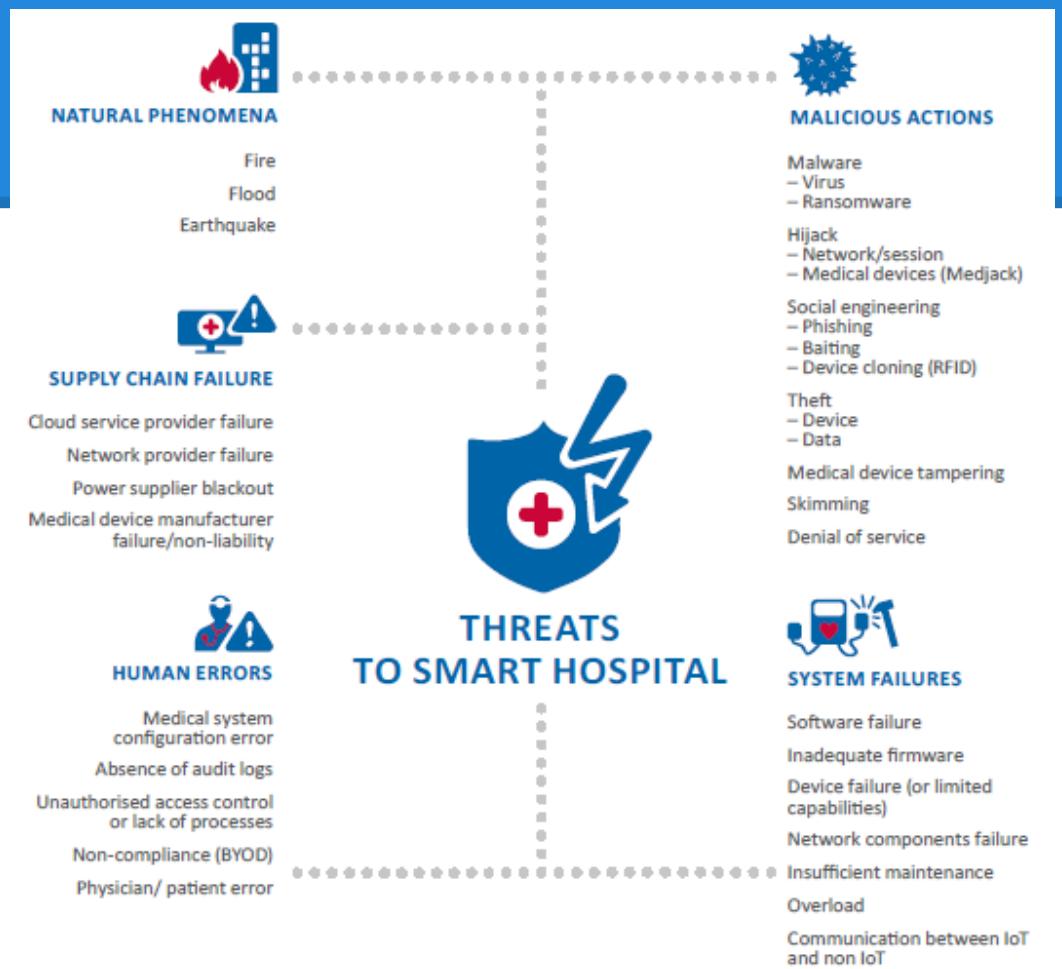
- Καθορίζεται ο κίνδυνος για την ασφάλεια του Οργανισμού, ως συνδυασμός (i) της πιθανότητας πραγματοποίησης των γεγονότων και (ii) των δυσμενών επιπτώσεων εάν τα γεγονότα πραγματοποιηθούν



NIST- Guide for Conducting Risk Assessments
<https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf>

Ταξινόμηση Απειλών σε Νοσοκομείο

- <https://www.enisa.europa.eu/sites/default/files/publications/Smart%20Hospitals.pdf>



Εργαλείο Αξιολόγησης Συμμόρφωσης (Gap Analysis) Οντοτήτων με τον ν. 5160/2024 (NIS2) της ΕΑΚ

- Παρέχει τη δυνατότητα να εντοπίσει με ακρίβεια τα κενά συμμόρφωσης, να αποτιμήσει την ωριμότητα των τεχνικών και οργανωτικών του μέτρων και να σχεδιάσει στοχευμένες παρεμβάσεις βελτίωσης
 - Ο χρήστης καλείται να αξιολογήσει και να επιλέξει την **τρέχουσα κατάσταση υλοποίησης** για κάθε επιμέρους σημείο ελέγχου του εργαλείου. Η επιλογή γίνεται μέσα από προκαθορισμένες τιμές (π.χ. Δεν έχει ξεκινήσει, Σε εξέλιξη, Ολοκληρωμένο, κ.λπ.)
 - Με την ολοκλήρωση των επιλογών, το εργαλείο προχωρά σε αυτόματο υπολογισμό:
 - **Του ποσοστού υλοποίησης**
 - **Του συνολικού ποσοστού υλοποίησης**
 - Βοηθάει στη διάγνωση των σημείων που παρουσιάζουν **ελλείψεις** ή υστερούν σε εφαρμογή & **στη χάραξη ενός στοχευμένου σχεδίου δράσης**
- **Ιστοσύνδεσμοι (Εκδόθηκε 10/09/2025):**
- <https://cyber.gov.gr/wp-content/uploads/2025/09/EAK-Gap-Analysis-Tool-FINAL.xlsx>
 - <https://cyber.gov.gr/wp-content/uploads/2025/09/10.09-%CE%95%CE%91%CE%9A-GAP-ANALYSIS FINAL-1.pdf>
 - <https://cyber.gov.gr/se-ischy-to-neo-ergaleio-axiologisis-symmorfosis-ontotiton-me-ton-n-5160-2024-m-mpletsas-thespizoyme-to-kanonistiko-plaisio-enischysis-tis-kyvernoanthektitikotitas/>

Gap Analysis Tool – EAK - I

Περιγραφή Κατάστασης	Ποσοστό Υλοποίησης	Οδηγία Ερμηνείας
Δεν εφαρμόζεται	"Εξαρτείται"	Δεν εφαρμόζεται, καθώς η απαίτηση αναφέρεται σε περιπτώσεις/υλοποιήσεις που δεν υφίστανται στο Οργανισμό
Δεν έχει ξεκινήσει	0%	Καμία ενέργεια ή τεκμηρίωση δεν υπάρχει
Σχεδιάζεται	25%	Έχει γίνει αναγνώριση, αλλά όχι ακόμα υλοποίηση
Μερική υλοποίηση	50%	Υπάρχει υλοποίηση, αλλά λείπουν βασικά στοιχεία ή διαδικασίες
Σχεδόν ολοκληρωμένο	75%	Η πλειοψηφία έχει υλοποιηθεί, εκκρεμούν μικρές λεπτομέρειες
Πλήρως υλοποιημένο	100%	Πλήρης συμμόρφωση με τεκμηρίωση και εφαρμογή
Κάθε σημείο ελέγχου συνοδεύεται από αναλυτική περιγραφή της απαίτησης, την κατάσταση υλοποίησης, η οποία επιλέγεται από προκαθορισμένες επιλογές (π.χ. «Δεν έχει ξεκινήσει», «Σχεδιάζεται», «κατάστασης, καθώς και τη βαρύτητα του κάθε σημείου ελέγχου.		
Με βάση τη βαρύτητα και το ποσοστό υλοποίησης, υπολογίζεται το επίπεδο συμμόρφωσης για κάθε σημείο, σύμφωνα με τον τύπο:		
Επίπεδο Συμμόρφωσης = Ποσοστό Υλοποίησης × Βαρύτητα.		
Π.χ., εάν ένα σημείο έχει βαρύτητα 5 και ποσοστό υλοποίησης 50%, τότε η συμμόρφωση υπολογίζεται ως: $0,5 \times 5 = 2,5$ μονάδες.		
Η Συνολική Συμμόρφωση (%) υπολογίζεται με βάση τον συνολικό βαθμό επίτευξης σε σχέση με τη μέγιστη δυνατή βαθμολογία όλων των σημείων ελέγχου. Ο τύπος είναι ο εξής: Συνολική Συμμόρφωση (%) = $(\text{Συνολική Επιτευχθείσα Βαθμολογία}) / (\text{Μέγιστη Δυνατή Βαθμολογία}) \times 100$.		
Ο υπολογισμός αυτός παρέχει μια συνολική εικόνα του επιπέδου συμμόρφωσης του οργανισμού με τις απαιτήσεις, λαμβάνοντας υπόψη τόσο την πρόοδο υλοποίησης όσο και τη σχετική σημασία (βαρύτητα) των σημείων ελέγχου.		
Για να υπολογιστεί η Μέγιστη Δυνατή Βαθμολογία, λαμβάνεται το άθροισμα των τιμών της στήλης «Βαρύτητα» (στήλη F) για όλα τα σημεία ελέγχου. Το άθροισμα αυτό αντιπροσωπεύει τη συνολική βαρύτητα των σημείων ελέγχου. Συνεπώς, ο υπολογισμός γίνεται ως εξής: Μέγιστη Δυνατή Βαθμολογία = ΣΥΝΟΛΟ(Βαρύτητα).		

Gap Analysis Tool – EAK - II

Απαιτήσεις Συμμορφωσης						Σύνολικη Συμμορφωση: 0.00%
#	Μετρα	Κατασταση	Ποσοστο Υλοποιηση (%)	Βαρυτητα (1-5)	Επιπεδο Συμμορφωσης	
10	Διαχείριση Ταυτότητας, Αυθεντικοποίηση και Έλεγχος Πρόσβασης	Δεν έχει ξεκινήσει	0%	Μέγιστη Δυνατή Βαθμολογία: 50	Επιτευχθείσα Βαθμολογία: 0	
10.1	Η οντότητα χρηγεί πολιτική και διαδικασίες που αφορούν στο λογικό έλεγχο πρόσβασης (logical access control) στα συστήματα δικτύου και πληροφοριών της, με βάση τις επιχειρηματικές της ανάγκες ή τις αρμοδιότητές της, εφόσον πρόκειται για οντότητα της περ. στ' της παρ. 2 του άρθρου 3 του ν. 5160/2024, καθώς και τις απαιτήσεις ασφάλειας. Οι ως άνω πολιτικές και διαδικασίες αφορούν στο προσωπικό της οντότητας και σε προσωπικό άλλων οντοτήτων, όπως είναι προμηθευτές και πάροχοι υπηρεσιών Τ.Π.Ε..	Δεν έχει ξεκινήσει	0%	5	0	
10.2	Η οντότητα χρηγεί μοναδική ταυτότητα (identity) σε κάθε χρήστη και σύστημα που αποκτά πρόσβαση στα συστήματα δικτύου και πληροφοριών της, με σκοπό τη διασφάλιση λογοδοσίας για ενέργειες που εκτελούνται με τη συγκεκριμένη ταυτότητα.	Δεν έχει ξεκινήσει	0%	5	0	
10.3	Η οντότητα χρηγεί και ανακαλεί δικαιώματα πρόσβασης στα συστήματα δικτύου και πληροφοριών της με βάση τις αρχές των ελάχιστων προνομίων (least privilege), της ανάγκης γνώσης (need to know) και του διαχωρισμού καθηκόντων (separation of duties).	Δεν έχει ξεκινήσει	0%	5	0	
10.4	Η οντότητα διασφαλίζει ότι η χρήση «προνομιούχων» (privileged) λογαριασμών και δικαιωμάτων διαχείρισης περιορίζονται στον απόλυτα απαραίτητο βαθμό, με βάση την κρισιμότητα των επιχειρηματικών λειτουργιών της ή των αρμοδιοτήτων της, κατά περίπτωση, καθώς και το αγήμα ταξινόμησης των αγαθών και των δεδομένων.	Δεν έχει ξεκινήσει	0%	5	0	
10.5	Η οντότητα διασφαλίζει ότι στις περιπτώσεις μεταβολής ή διακοπής της απασχόλησης του προσωπικού, τα δικαιώματα πρόσβασης τροποποιούνται ανάλογα και εγκαίρως ανάλογα με την κρισιμότητα της πρόσβασης.	Δεν έχει ξεκινήσει	0%	5	0	
10.6	Η οντότητα διασφαλίζει ότι αξιολογεί και επικαιροποιεί περιοδικά (προτείνεται σε ετήσια βάση) τα δικαιώματα πρόσβασης στα συστήματα δικτύου και πληροφοριών με βάση τις επιχειρηματικές της ανάγκες.	Δεν έχει ξεκινήσει	0%	4	0	
10.7	Η οντότητα διασφαλίζει ότι οι τοπικοί διαχειριστικοί λογαριασμοί χρηστών (local administrator rights) στα τερματικά τους (PCs, laptops) είναι απενεργοποιούνται και ενεργοποιούνται μόνο σε περιπτώσεις που απαιτείται λόγω επιχειρησιακής ανάγκης.	Δεν έχει ξεκινήσει	0%	4	0	
10.8	Η οντότητα διασφαλίζει ότι ο εφαρμόζονται ισχυρές μέθοδοι και τεχνολογίες ασφαλούς αυθεντικοποίησης, ανάλογες με την ταξινόμηση της κρισιμότητας των αγαθών και των δεδομένων. Οι μέθοδοι αυθεντικοποίησης μπορεί να περιλαμβάνουν ισχυρά συνήθειατικά, ψηφιακά πιστοποιητικά, έξυπνες κάρτες, συσκευές ή βιομετρικά μέσα.	Δεν έχει ξεκινήσει	0%	5	0	
10.9	Η οντότητα διασφαλίζει ότι εφαρμόζονται μέθοδοι και τεχνολογίες πολυπαραγοντικής αυθεντικοποίησης (multi-factor authentication) για τις υπηρεσίες VPN και νέφους.	Δεν έχει ξεκινήσει	0%	5	0	
10.10	Η οντότητα διασφαλίζει ότι εφαρμόζονται μέθοδοι και τεχνολογίες πολυπαραγοντικής αυθεντικοποίησης (multi-factor authentication) με ιδιαίτερη έμφαση στους χρήστες με υψηλά προνόμια (privileged users), και ειδικά για την πρόσβαση σε κρίσιμα εσωτερικά δίκτυα, διαχειριστικά συστήματα και ευαίσθητα δεδομένα, σύμφωνα με την ταξινόμηση της κρισιμότητας των πληροφοριακών αγαθών.	Δεν έχει ξεκινήσει	0%	3	0	
10.11	Η οντότητα αξιολογεί και επικαιροποιεί περιοδικά (προτείνεται σε ετήσια βάση) το σύνολο των πολιτικών και διαδικασιών που αφορούν στον έλεγχο πρόσβασης, ίδιως όταν λαμβάνουν χώρα σημαντικές αλλαγές στις λειτουργίες της οντότητας ή σοβαρά περιστατικά κυβερνοασφάλειας.	Δεν έχει ξεκινήσει	0%	4	0	
11	Ασφαλή Παραμετροποίηση Υλικού, Λογισμικού, Υπηρεσιών και Δικτύων	Δεν έχει ξεκινήσει	0%	Μέγιστη Δυνατή Βαθμολογία: 16	Επιτευχθείσα Βαθμολογία: 0	
11.1	Η οντότητα αναπτύσσει διαδικασίες και εργαλεία για την επιβολή ρυθμίσεων και παραμετροποίησεων του υλικού, του λογισμικού, των υπηρεσιών και του δικτύου της, συμπεριλαμβανομένων των ρυθμίσεων και παραμετροποίησεων ασφάλειας.	Δεν έχει ξεκινήσει	0%	4	0	
11.2	Η οντότητα υλοποιεί διαδικασίες ασφαλούς παραμετροποίησης (secure configuration), κατά περίπτωση, στα πληροφοριακά της συστήματα, εφαρμόζοντας βέλτιστες διεθνείς πρακτικές ή προκαθορισμένα πρότυπα κατασκευαστών ή ανεξάρτητων ερευνητικών οργανισμών.	Δεν έχει ξεκινήσει	0%	4	0	

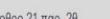
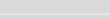
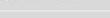
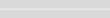
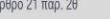
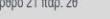
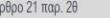
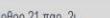
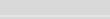
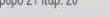
Gap Analysis Tool – EAK - III

ΑΠΑΙΤΗΣΕΙΣ ΣΥΜΜΟΡΦΩΣΗΣ		ΣΤΟΙΧΕΙΑ ΤΕΚΜΗΡΙΩΣΗΣ/ΥΛΟΠΟΙΗΣΗΣ			ΠΡΟΤΕΙΝΟΜΕΝΕΣ ΕΝΕΡΓΕΙΕΣ
#	ΜΕΤΡΑ	ΤΟΠΙΝΗ ΚΑΤΑΣΤΑΣΗ/ ΠΑΡΑΤΗΡΗΣΗ	ΤΕΚΜΗΡΙΑ	ΚΕΝΟ ΣΥΜΜΟΡΦΩΣΗΣ	
10	Διαχείριση Ταυτότητας, Αυθεντικοποίηση και Έλεγχος Πρόσβασης				
10.1	Η οντότητα έχει εκπονήσει πολιτική και διαδικασίες που αφορούν στο λογικό έλεγχο πρόσβασης (logical access control) στα συστήματα δικτύου και πληροφοριών της, με βάση τις επιχειρηματικές της ανάγκες ή τις αρμοδιότητές της, εφόσον πρόκειται για οντότητα της περ. στ' της παρ. 2 του άρθρου 3 του ν. 5160/2024, καθώς και τις απατήσεις ασφάλειας. Οι ωντες πολιτικές και διαδικασίες αφορούν στο προσωπικό της οντότητας και σε προσωπικό άλλων οντοτήτων, όπως είναι προμηθευτές και πάροχοι υπηρεσιών Τ.Π.Ε..				
10.2	Η οντότητα χορηγεί μοναδική ταυτότητα (identity) σε κάθε χρήστη και σύστημα που αποκτά πρόσβαση στα συστήματα δικτύου και πληροφοριών της, με σκοπό τη διασφάλιση λογοδοσίας για ενέργειες που εκτελούνται με τη συγκεκριμένη ταυτότητα.				
10.3	Η οντότητα χορηγεί και ανακαλεί δικαιώματα πρόσβασης στα συστήματα δικτύου και πληροφοριών της με βάση τις αρχές των ελάχιστων προνομίων (least privilege), της ανάγκης γνώσης (need to know) και του διαχωρισμού καθηκόντων (separation of duties).				
10.4	Η οντότητα διασφαλίζει ότι η χορήγηση «τριπομόνυμα» (privilege) λογαριασμών και δικαιώματων διαχείρισης περιορίζεται στον απόλυτα απαραίτητο θαρρό, με βάση την κρισιμότητα των επιχειρηματικών λειτουργιών της ή των αρμοδιοτήτων της, κατά περίπτωση, καθώς και το σχήμα ταξινόμησης των αγαθών και των δεδομένων.				
10.5	Η οντότητα διασφαλίζει ότι στις περιπτώσεις μεταβολής ή διακοπής της απασχόλησης του προσωπικού, τα δικαιώματα πρόσβασης τροποποιούνται ανάλογα και εγκαίρως ανάλογα με την κρισιμότητη της πρόσβασης.				
10.6	Η οντότητα διασφαλίζει ότι αξιολογία και επικαρποτητή περιοδικά (προτείνεται σε ετήσια βάση) τα δικαιώματα πρόσβασης στα συστήματα δικτύου και πληροφοριών με βάση τις επιχειρηματικές της ανάγκες.				
10.7	Η οντότητα διασφαλίζει ότι οι τοπικοί διαχειριστικοί λογαριασμοί χρηστών (local administrator rights) στα τερματικά τους (PCs, laptops) είναι απενεργοποιημένα και ενεργοποιούνται μόνο σε περιπτώσεις που απαιτείται λόγω επιχειρηματικής ανάγκης.				
10.8	Η οντότητα διασφαλίζει ότι εφαρμόζονται ιαχυρές μέθοδοι και τεχνολογίες ασφαλισμούς αυθεντικοποίησης, ανάλογες με την ταξινόμηση της κρισιμότητας των αγαθών και των δεδομένων. Οι μέθοδοι αυθεντικοποίησης μπορεί να περιλαμβάνουν ιαχυρά συνθηματικά, ψηφιακά πιστοποιητικά, έξυπνες κάρτες, συσκευές ή βιομετρικά μέσα.				
10.9	Η οντότητα διασφαλίζει ότι εφαρμόζονται μέθοδοι και τεχνολογίες πολυπαραγοντικής αυθεντικοποίησης (multi-factor authentication) για τις υπηρεσίες VPN και νέφους.				
10.10	Η οντότητα διασφαλίζει ότι εφαρμόζονται μέθοδοι και τεχνολογίες πολυπαραγοντικής αυθεντικοποίησης (multi-factor authentication) με ιδιαίτερη έμφαση στους χρήστες με υψηλά προνόμια (privileged users), και ειδικά για την πρόσβαση σε κρίσιμα εσωτερικά δικτύα, διαχειριστικά συστήματα και ευαίσθητα δεδομένα, σύμφωνα με την ταξινόμηση της κρισιμότητας των πληροφοριακών αγαθών.				
10.11	Η οντότητα αξιολογεί και επικαρποτεί περιοδικά (προτείνεται σε ετήσια βάση) το σύνολο των πολιτικών και διαδικασιών που αφορούν στον έλεγχο πρόσβασης, ίδιως σταν λαμβανόντα χώρα σημαντικές αλλαγές στις λειτουργίες της οντότητας ή σεβαρά περιστατικά κυβερνοασφάλειας.				
11	Ασφαλής Παραμετροποίηση Υλικού, Λογισμικού, Υπηρεσιών και Δικτύων				
11.1	Η οντότητα αναπτύσσει διαδικασίες και εργαλεία για την επιβολή ρυθμίσεων και παραμετροποίησεων των υλικού, του λογισμικού, των υπηρεσιών και του δικτύου της, συμπεριλαμβανομένων των ρυθμίσεων και παραμετροποίησεων ασφάλειας.				
11.2	Η οντότητα υλοποιεί διαδικασίες ασφαλούς παραμετροποίησης (secure configuration), κατά περίπτωση, στα πληροφοριακά της συστήματα, εφαρμόζοντας βέλτιστες διεθνείς πρακτικές ή προκαθορισμένα πρότυπα κατασκευαστών ή ανεξάρτητων ερευνητικών οργανώσων.				

Gap Analysis Tool – EAK - IV

ΑΠΑΙΤΗΣΕΙΣ ΣΥΜΜΟΡΦΩΣΗΣ		ΠΛΑΝΟ ΔΙΟΡΘΩΤΙΚΩΝ/ΒΕΛΤΙΩΤΙΚΩΝ ΕΝΕΡΓΕΙΩΝ			
#	ΜΕΤΡΑ	ΠΡΟΤΕΙΝΟΜΕΝΕΣ ΕΝΕΡΓΕΙΕΣ	ΠΡΟΤΕΡΑΙΟΤΗΤΑ	ΚΑΤΑΛΗΚΤΙΚΗ ΗΜΕΡΟΜΗΝΙΑ	ΥΠΕΥΘΥΝΟΣ
10	Διαχείριση Ταυτότητας, Αυθεντικοποίηση και Έλεγχος Πρόσβασης				
10.1	Η αντότητα έχει εκπονήσει πολιτική και διαδικασίες που αφορούν στο λογικό έλεγχο πρόσβασης (logical access control) στα συστήματα δικτύου και πληροφοριών της, με βάση τις επιχειρησιακές της ανάγκες και τις αρμοδιότητες της, εφόσον πρόκειται για αντότητα της περ. στ' της παρ. 2 του άρθρου 3 του ν. 5160/2024, καθώς και τις απαιτήσεις ασφαλείας. Οι ως άνω πολιτικές και διαδικασίες αφορούν στο προσωπικό τηςς αντότητας και σε προσωπικό άλλων αντιστητών, όπως είναι προμηθεύτες και πάροχοι υπηρεσιών Τ.Π.Ε..	Select...			
10.2	Η αντότητα χρηγεί μοναδική ταυτότητα (identity) σε κάθε χρήστη και σύστημα που αποκτά πρόσβαση στα συστήματα δικτύου και πληροφοριών της, με σκοπό τη διασφάλιση λογόδοσσας για ενέργειες που εκτελούνται με τη συγκεκριμένη ταυτότητα.		Select...		
10.3	Η αντότητα χρηγεί και ανακαλεί δικαιώματα πρόσβασης στα συστήματα δικτύου και πληροφοριών της με βάση τις αρχές των ελάχιστων προνομίων (least privilege), της ανάγκης γνώσης (need to know) και του διαχωρισμού καθηκόντων (separation of duties).		Select...		
10.4	Η αντότητα διασφαλίζει ότι η χορήγηση «προνομίου» (privilege) λογαριασμών και δικαιώματων διαχείρισης περιορίζονται στον απόλυτα απαραίτητο ρεμβό, με βάση την κριματότητα των επιχειρηματικών λεπτομεριών της, ή των αρμοδιοτήτων της, κατά περίττωση, καθώς και το σχήμα ταξινόμησης των αγαθών και των δεδομένων.		Select...		
10.5	Η αντότητα διασφαλίζει ότι στις περιπτώσεις μεταβολής ή διακοπής της απασχόλησης του προσωπικού, τα δικαιώματα πρόσβασης τροποποιούνται ανάλογα και εγκαίρως ανάλογα με την κριματότητα της πρόσβασης.		Select...		
10.6	Η αντότητα διασφαλίζει ότι αρμόδιοι και επικαρποτοί περιοδικά (προτείνεται σε ετήσια βάση) τα δικαιώματα πρόσβασης στα συστήματα δικτύου και πληροφοριών με βάση τις επιχειρησιακές της ανάγκες.		Select...		
10.7	Η αντότητα διασφαλίζει ότι οι τοπικοί διαχειριστικοί λογαριασμοί χρηστών (local administrator rights) στα τερματικά τους (PCs, laptops) είναι απενεργοποιημένοι και ενεργοποιούνται μόνο σε περιπτώσεις που απαιτείται λόγω επιχειρησιακής ανάγκης.		Select...		
10.8	Η αντότητα διασφαλίζει ότι εφαρμόζονται ισχυρές μέθοδοι και τεχνολογίες ασφαλούς αυθεντικοποίησης, ανάλογες με την ταξινόμηση της κριματότητας των αγαθών και των δεδομένων. Οι μέθοδοι αυθεντικοποίησης μπορεύ να περιλαμβάνουν ισχυρά συνθηματικά, ψηφιακά πιστοποιητικά, έξυπνες κάρτες, συσκευές ή βιομετρικά μέσα.		Select...		
10.9	Η αντότητα διασφαλίζει ότι εφαρμόζονται μέθοδοι και τεχνολογίες πολυπαραγοντικής αυθεντικοποίησης (multi-factor authentication) για τις υπηρεσίες VPN και νέφους.		Select...		
10.10	Η αντότητα διασφαλίζει ότι εφαρμόζονται μέθοδοι και τεχνολογίες πολυπαραγοντικής αυθεντικοποίησης (multi-factor authentication) με ιδιαίτερη έμφαση στους χρήστες με υψηλά προνόμια (privileged users), και ειδικά για την πρόσβαση σε κρίσιμα εισιτηριακά δίκτυα, διαχειριστικά συστήματα και ευαίσθητα δεδομένα, σύμφωνα με την ταξινόμηση της κριματότητας των πληροφοριακών αγαθών.		Select...		
10.11	Η αντότητα αξιολογεί και επικαρποτεί περιοδικά (προτείνεται σε ετήσια βάση) το σύνολο των πολιτικών και διαδικασιών που αφορούν στον έλεγχο πρόσβασης, ίδιως όταν λαμβάνουν χώρα σημαντικές αλλαγές στις λεπτομεριές της αντότητας ή ασφαρά περιστατικά κυβερνοασφάλειας.		Select...		
11	Ασφαλής Παραμετροποίηση Υλικού, Λογισμικού, Υπηρεσιών και Δικτύων				
11.1	Η αντότητα αναπτύσσει διαδικασίες και εργαλεία για την επιβολή ρυθμίσεων και παραμετροποίησεων του υλικού, του λογισμικού, των υπηρεσιών και του δικτύου της, συμπεριλαμβανομένων των ρυθμίσεων και παραμετροποίησεων ασφαλείας.		Select...		
11.2	Η αντότητα μπορεί διαδικασίες ασφαλούς παραμετροποίησης (secure configuration), κατά περίπτωση, στα πληροφοριακά της συστήματα, εφαρμόζοντας βέλτιστες διεύθυνσης πρακτικές ή προκαθορισμένα πρότυπα κατασκευαστών ή ανεξάρτητων ερευνητικών οργανισμών.		Select...		

Gap Analysis Tool – EAK - V

ΑΠΑΙΤΗΣΕΙΣ ΣΥΜΜΟΡΦΩΣΗΣ				ΑΝΑΦΟΡΑ		
#	ΜΕΤΡΑ	ΚΑΤΑΣΤΑΣΗ	ΣΧΟΛΙΑ	N.5160/2024	KYΑ 1689/2025	ΟΔΗΓΙΑ NIS2
10	Διαχείριση Ταυτότητας, Αυθεντικοποίηση και Ελέγχος Πρόσβασης			 Άρθρο 15 Μέτρα διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας παρ. 29 & παρ. 2t	 Άρθρο 13	 Άρθρο 21 παρ. 26 & παρ. 2t της Οδηγίας
10.1	Η αντότητα έχει εκπονήσει πολιτική και διαδικασίες που αφορούν στο λογικό έλεγχο πρόσβασης (logical access control) στα συστήματα δικτύου και πληροφοριών της, με βάση τις επιχειρηματικές της ανάγκες ή τις αρμοδιότητές της, εφόσον πρόκειται για αντότητα της περ. στ' της παρ. 2 του άρθρου 3 του ν. 5160/2024, καθώς και τις αποτελέσεις ασφάλειας. Οι ως άνω πολιτικές και διαδικασίες αφορούν στο προσωπικό της αντότητας και σε προσωπικό άλλων οντοτήτων, όπως είναι προμηθευτές και πάροχοι υπηρεσιών Τ.Π.Ε.	Σε εξέλιξη		 Άρθρο 15 Μέτρα διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας παρ. 29	 Άρθρο 13 παρ. α	 Άρθρο 21 παρ. 29
10.2	Η αντότητα χορηγεί μοναδική ταυτότητα (identity) σε κάθε χρήστη και σύστημα που αποκτά πρόσβαση στα συστήματα δικτύου και πληροφοριών της, με σκοπό τη διασφάλιση λογόδοσσας για ενέργειες που εκτελούνται με τη συγκεκριμένη ταυτότητα.	Select...		 Άρθρο 15 Μέτρα διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας παρ. 2t	 Άρθρο 13 παρ. β	 Άρθρο 21 παρ. 2i
10.3	Η αντότητα χορηγεί και ανακαλεί δικαιώματα πρόσβασης στα συστήματα δικτύου και πληροφοριών της με βάση τις αρχές των ελάχιστων προνομίων (least privilege), της ανάγκης γνώσης (need to know) και του διαχωρισμού καθηκόντων (separation of duties).	Select...		 Άρθρο 15 Μέτρα διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας παρ. 29	 Άρθρο 13 παρ. γ	 Άρθρο 21 παρ. 28
10.4	Η αντότητα διασφαλίζει ότι η χορήγηση «προνομίων» (privileged) λογαριασμών και δικαιωμάτων διαχείρισης περιορίζεται στον απλύτα απαραίτητο ρυθμό, με βάση την κρισιμότητα των επιχειρηματικών λειτουργιών της ή των αρμόδιετων της, κατά περίπτωση, καθώς και το σχήμα ταξινόμησης των αγαθών και των δεδουλεύμαντων.	Δεν έχεινήσει		 Άρθρο 15 Μέτρα διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας παρ. 29	 Άρθρο 13 παρ. δ	 Άρθρο 21 παρ. 28
10.5	Η αντότητα διασφαλίζει ότι στις περιπτώσεις μεταβολής ή διακοπής της απασχόλησης του προσωπικού, τα δικαιώματα πρόσβασης τροποποιούνται απλώς και εγκαυμάτων απλώς με την κρισιμότητα της πρόσβασης.	Select...		 Άρθρο 15 Μέτρα διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας παρ. 29	 Άρθρο 13 παρ. ε	 Άρθρο 21 παρ. 28
10.6	Η αντότητα διασφαλίζει ότι αξιολογεί και επικαιριόποιει περιοδικά (προτείνεται σε ετήσια βάση) τα δικαιώματα πρόσβασης στα συστήματα δικτύου και πληροφοριών με βάση τις επιχειρηματικές της ανάγκες.	Select...		 Άρθρο 15 Μέτρα διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας παρ. 29	 Άρθρο 13 παρ. η	 Άρθρο 21 παρ. 28
10.7	Η αντότητα διασφαλίζει ότι οι τοπικοί διαχειριστικοί λογαριασμοί χρηστών (PCs, laptops) είναι απενεργοποιημένοι και ενεργοποιούνται μόνο σε περιπτώσεις που απαιτείται λόγω επιχειρηματικής ανάγκης.	Select...		 Άρθρο 15 Μέτρα διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας παρ. 29	 Άρθρο 13 παρ. δ	 Άρθρο 21 παρ. 28
10.8	Η αντότητα διασφαλίζει ότι εφαρμόζονται ισχυρές μέθοδοι και τεχνολογίες ασφαλούς αυθεντικοποίησης, ανάλογες με την ταξινόμηση της κρισιμότητας των αγαθών και των δεδουλεύμαντων. Οι μέθοδοι αυθεντικοποίησης μπορεί να περιλαμβάνουν ιχυρά συνθηματικά, ψηφιακά πιστοποιητικά, έξυπνες κάρτες, συσκευές ή βιομετρικά μέσα.	Select...		 Άρθρο 15 Μέτρα διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας παρ. 29	 Άρθρο 13 παρ. στ	 Άρθρο 21 παρ. 28
10.9	Η αντότητα διασφαλίζει ότι εφαρμόζονται μέθοδοι και τεχνολογίες πολυταραγωνικής αυθεντικοποίησης (multi-factor authentication) για τις υπηρεσίες VPN και νέφους.	Select...		 Άρθρο 15 Μέτρα διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας παρ. 2t	 Άρθρο 13 παρ. ζ	 Άρθρο 21 παρ. 2i
10.10	Η αντότητα διασφαλίζει ότι εφαρμόζονται μέθοδοι και τεχνολογίες πολυταραγωνικής αυθεντικοποίησης (multi-factor authentication) με ίδιατερη έμφαση στους χρήστες με υψηλά προνόμια (privileged users), και ειδικά για την πρόσβαση σε κρίσιμα εσωτερικά δίκτυα, διαχειριστικά συστήματα και ευαίσθητα δεδομένα, σύμφωνα με την ταξινόμηση της κρισιμότητας των πληροφορικών αγαθών.	Select...		 Άρθρο 15 Μέτρα διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας παρ. 2t	 Άρθρο 13 παρ. ζ	 Άρθρο 21 παρ. 2i
10.11	Η αντότητα αξιολογεί και επικαιριόποιει περιοδικά (προτείνεται σε ετήσια βάση) το σύνολο των πολιτικών και διαδικασιών που αφορούν στον έλεγχο πρόσβασης, ιδίως όταν λαμβάνουν χώρα σημαντικές αλλαγές στις λειτουργίες της αντότητας ή σοβαρά περιστατικά κυβερνοασφάλειας.	Select...		 Άρθρο 15 Μέτρα διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας παρ. 29	 Άρθρο 13 παρ. η	 Άρθρο 21 παρ. 28
11	Ασφαλής Παραμετροποίηση Υλικού, Λογισμικού, Υπηρεσιών και Δικτύων			 Άρθρο 15 Μέτρα διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας παρ. 2t	 Άρθρο 14	 Άρθρο 21 παρ. 2i της Οδηγίας
11.1	Η αντότητα αναπτύσσει διαδικασίες και εργαλεία για την επιβολή ρυθμίσεων και παραμετροποίησης του υλικού, του λογισμικού, των υπηρεσιών και του δικτύου της, συμπεριλαμβανομένων των ρυθμίσεων και παραμετροποίησης ασφάλειας.	Select...		 Άρθρο 15 Μέτρα διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας παρ. 2t	 Άρθρο 14 παρ. α	 Άρθρο 21 παρ. 2i
11.2	Η αντότητα υλοποιεί διαδικασίες ασφαλούς παραμετροποίησης (secure configuration), κατά περίπτωση, στα πληροφοριακά της συστήματα, εφαρμόζοντας βέλτιστες δεινές πρακτικές ή πρακτικούμενά πρότυπα κατασκευώντας ή ανεξάρτητους ερευνητικούς οργανισμούς.	Select...		 Άρθρο 15 Μέτρα διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας παρ. 2t	 Άρθρο 14 παρ. β	 Άρθρο 21 παρ. 2i

Gap Analysis Tool – EAK - VI

ΣΥΝΟΛΙΚΗ ΣΥΜΜΟΡΦΩΣΗ

ΕΠΙΠΕΔΟ ΣΥΝΟΛΙΚΗΣ ΣΥΜΜΟΡΦΩΣΗΣ: 0,00%
ΕΠΙΚΙΝΔΥΝΟΤΗΤΑ: 100,00%
ΚΑΤΑΣΤΑΣΗ: ΚΡΙΣΙΜΟΣ ΚΙΝΔΥΝΟΣ

0%

ΕΠΙΠΕΔΟ ΣΥΜΜΟΡΦΩΣΗΣ: 0,00%
ΕΠΙΚΙΝΔΥΝΟΤΗΤΑ: 100,00%
ΚΑΤΑΣΤΑΣΗ: ΚΡΙΣΙΜΟΣ ΚΙΝΔΥΝΟΣ

0%

13. Διαχείριση Αλλαγών

ΕΠΙΠΕΔΟ ΣΥΜΜΟΡΦΩΣΗΣ: 0,00%
ΕΠΙΚΙΝΔΥΝΟΤΗΤΑ: 100,00%
ΚΑΤΑΣΤΑΣΗ: ΚΡΙΣΙΜΟΣ ΚΙΝΔΥΝΟΣ

0%

14. Διαχείριση και Γνωστοποίηση Ευπαθειών

ΕΠΙΠΕΔΟ ΣΥΜΜΟΡΦΩΣΗΣ: 0,00%
ΕΠΙΚΙΝΔΥΝΟΤΗΤΑ: 100,00%
ΚΑΤΑΣΤΑΣΗ: ΚΡΙΣΙΜΟΣ ΚΙΝΔΥΝΟΣ

0%

15. Αξιολόγηση της Αποτελεσματικότητας των Μέτρων Διαχείρισης

ΕΠΙΠΕΔΟ ΣΥΜΜΟΡΦΩΣΗΣ: 0,00%
ΕΠΙΚΙΝΔΥΝΟΤΗΤΑ: 100,00%
ΚΑΤΑΣΤΑΣΗ: ΚΡΙΣΙΜΟΣ ΚΙΝΔΥΝΟΣ

0%

17. Προστασία από Κακόβουλο Λογισμικό

ΕΠΙΠΕΔΟ ΣΥΜΜΟΡΦΩΣΗΣ: 0,00%
ΕΠΙΚΙΝΔΥΝΟΤΗΤΑ: 100,00%
ΚΑΤΑΣΤΑΣΗ: ΚΡΙΣΙΜΟΣ ΚΙΝΔΥΝΟΣ

0%

18. Εκπαίδευση και Εναισθητοποίηση σε Θέματα Κυβερνοασφάλειας

ΕΠΙΠΕΔΟ ΣΥΜΜΟΡΦΩΣΗΣ: 0,00%
ΕΠΙΚΙΝΔΥΝΟΤΗΤΑ: 100,00%
ΚΑΤΑΣΤΑΣΗ: ΚΡΙΣΙΜΟΣ ΚΙΝΔΥΝΟΣ

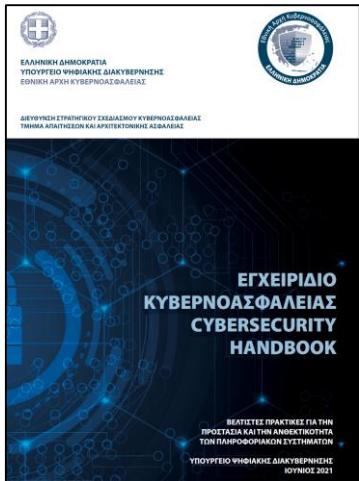
0%

19. Χρήση Κρυπτογραφίας

ΕΠΙΠΕΔΟ ΣΥΜΜΟΡΦΩΣΗΣ: 0,00%
ΕΠΙΚΙΝΔΥΝΟΤΗΤΑ: 100,00%
ΚΑΤΑΣΤΑΣΗ: ΚΡΙΣΙΜΟΣ ΚΙΝΔΥΝΟΣ

0%

Οργάνωση Πολιτικών Ασφαλείας, Οδηγοί & Πρακτικές



Εγχειρίδιο
Κυβερνοασφάλειας της ΕΑΚ



NIST Cybersecurity
Framework Policy
Template Guide



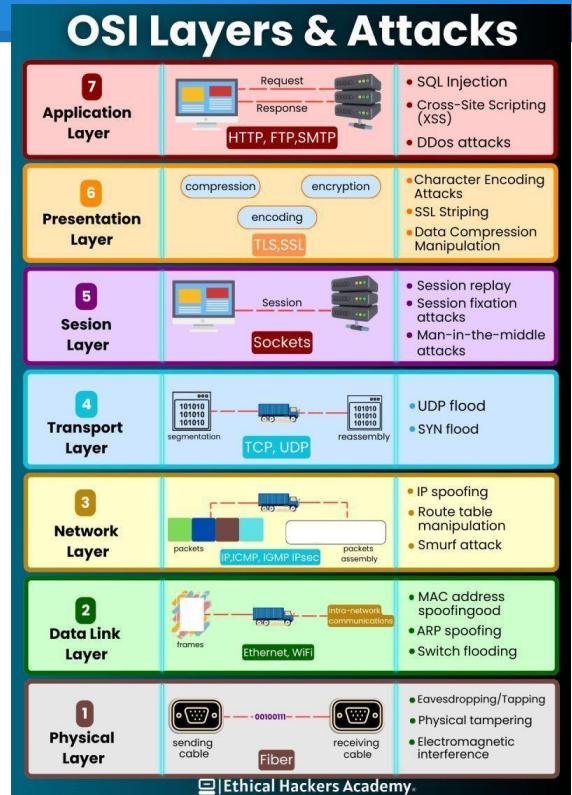
Οδηγός
για τη Συμμόρφωση
των Επιχειρήσεων



NIS2 Technical Implementation
Guidance

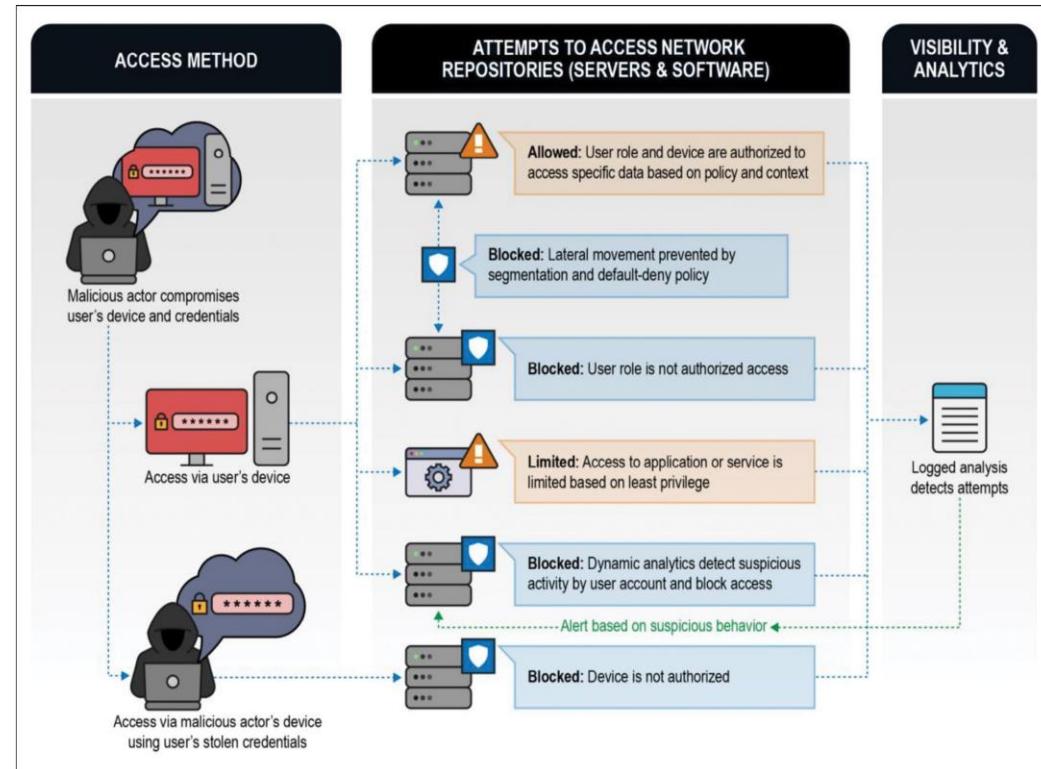
Κυβερνοϋγιεινή, Απειλές & Πολιτικές Ασφαλείας - I

- **Κυβερνοϋγιεινή (Cyber hygiene): πρακτικές & καθημερινές ενέργειες που εφαρμόζουν οργανισμοί και φυσικά πρόσωπα με στόχο την καλή λειτουργία και online ασφάλεια των συστημάτων, εφαρμογών και υπολογιστών τους**
- Ενδεικτικά, περιλαμβάνει: τακτικές ενημερώσεις του λογισμικού (updates), ισχυρούς κωδικούς, τακτικά backups των δεδομένων, εγκατάσταση λογισμικών προστασίας (antivirus, antimalware, κοκ), διαδικασίες κρυπτογράφησης (encryption), διαμερισματοποίηση του εταιρικού δικτύου, ...

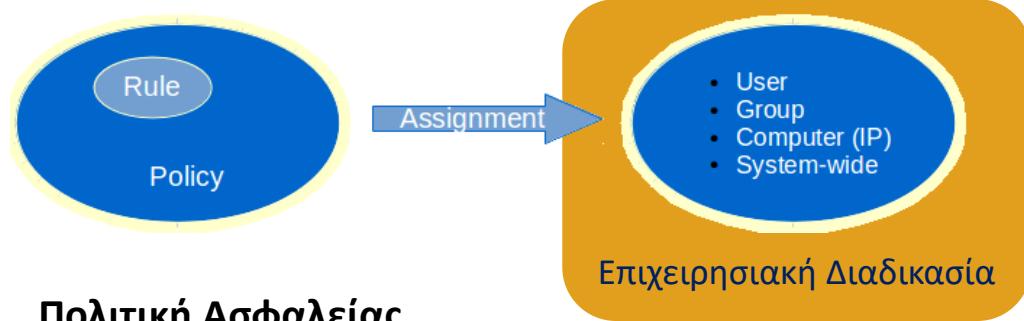


Κυβερνοϋγιεινή, Απειλές & Πολιτικές Ασφαλείας - III

- Παράδειγμα εφαρμογής του zero trust, όπου ο επιτιθέμενος **έχει παραβιάσει τους κωδικούς πρόσβασης** ενός νόμιμου χρήστη και **αποπειράται να αποκτήσει πρόσβαση** σε συστήματα του Οργανισμού, ο οποίος όμως **έχει εφαρμόσει μέτρα** βάσει των γραπτών **πολιτικών ασφαλείας**



Τί είναι οι Πολιτικές Ασφαλείας



- **Πολιτική Ασφαλείας**
- Σύνολο κανόνων που διασφαλίζουν την:
 - **Ακεραιότητα:** διατήρηση των δεδομένων ενός πληροφοριακού συστήματος
 - **Εμπιστευτικότητα:** ευαίσθητες πληροφορίες που δεν πρέπει να αποκαλύπτονται σε μη εξουσιοδοτημένα άτομα
 - **Διαθεσιμότητα:** εξασφάλιση ότι τα δεδομένα, οι Η/Υ και οι υπηρεσίες δικτύου θα είναι στη διάθεση των χρηστών όποτε και όταν απαιτείται η χρήση τους
- Εφαρμόζονται σε επίπεδο χρηστών, συστήματος (τομέα), Η/Υ, ομάδες χρηστών

- **Ελάχιστες Γραπτές Θεματικές Πολιτικές Ασφάλειας:**

- Έλεγχος πρόσβασης
- Διαχείριση αγαθών
- Ορθή χρήση αγαθών & δεδομένων
- Αφαιρούμενα μέσα αποθήκευσης
- Διαχείριση περιστατικών κυβερνοασφάλειας
- Ασφάλεια εφοδιαστικής αλυσίδας
- Ασφάλεια δικτύων
- Διενέργειας Ελέγχων Κυβερνοασφάλειας
- Αντίγραφα ασφαλείας
- Κρυπτογράφηση δεδομένων & επικοινωνιών
- Φυσική & περιβαλλοντική ασφάλεια

Πολιτικές Ασφαλείας & Κανόνες Εφαρμογής (Μέτρα)

Στοιχείο Πολιτικής Ασφάλειας	Μέτρα / Κανόνες Εφαρμογής	NIST Function: Govern	NIST Function: Identify	NIST Function: Protect	NIST Function: Detect	NIST Function: Respond	NIST Function: Recover
<p>Η πολιτική ασφαλείας είναι το σύνολο των αρχών και κατευθυντήριων γραμμών που καθορίζουν πώς προστατεύονται τα περιουσιακά στοιχεία (δεδομένα, υποδομές, προσωπικό).</p> <p>Εξαπομίκευση ανά τμήμα ή λειτουργία (π.χ. διαφορετική πολιτική για το τμήμα ΙΤ και για το HR)</p> <p>Προσαρμογή ανά επίπεδο ευαισθησίας δεδομένων (π.χ. αυστηρότεροι κανόνες για απόρρητα δεδομένα)</p> <p>Ευθυγράμμιση με νομικές και κανονιστικές απαιτήσεις (π.χ. GDPR, NIS2)</p> <p>Περιοδική αναθεώρηση ανάλογα με νέες απειλές ή τεχνολογικές αλλαγές</p>	<p>Τα μέτρα ασφαλείας είναι οι συγκεκριμένες ενέργειες ή τεχνικά μέσα που εφαρμόζονται για την υλοποίηση της πολιτικής ασφαλείας.</p> <p>Περιλαμβάνουν:</p> <ul style="list-style-type: none">Τεχνικά μέτρα: διαφορετικά επίπεδα κρυπτογράφησης, firewall κανόνες, έλεγχος πρόσβασης)Οργανωτικά μέτρα: διαδικασίες ελέγχου ταυτότητας, εκπαίδευση προσωπικούΦυσικά μέτρα: κάρτες πρόσβασης, κάμερες, φύλακες <p>Προσαρμογή στην ανάλυση κινδύνου: τα μέτρα ποικίλλουν ανάλογα με τη σοβαρότητα και την πιθανότητα των απειλών</p>	<p>Govern: Organizational Context (GV.OC) 2</p> <p>Govern: Risk Management Strategy (GV.RM) 3</p> <p>Govern: Roles, Responsibilities, and Authorities (GV.RR) 4</p> <p>Govern: Policy (GV.PO) 5</p> <p>Govern: Oversight (GV.OV) 5</p> <p>Govern: Cybersecurity Supply Chain Risk Management (GV.SC) 6</p>	<p>Identify: Asset Management (ID.AM) 8</p> <p>Identify: Risk Assessment (ID.RA) 9</p> <p>Identify: Improvement (ID.IM) 11</p>	<p>Protect: Identity Management and Access Control (PR.AA) 13</p> <p>Protect: Awareness and Training (PR.AT) 14</p> <p>Protect: Data Security (PR.DS) 15</p> <p>Protect: Platform Security (PR.PS) 16</p> <p>Protect: Technology Infrastructure Resilience (PR.IR) 17</p>	<p>Detect: Adverse Event Analysis (DE.AE) 18</p> <p>Detect: Continuous Monitoring (DE.CM) 19</p>	<p>Respond: Incident Management (RS.MA) 21</p> <p>Respond: Incident Response Reporting and Communication (RS.CO) 22</p> <p>Respond: Incident Analysis (RS.AN) 22</p> <p>Respond: Incident Mitigation (RS.MI) 23</p>	<p>Recover: Incident Recovery Plan Execution (RC.RP) 24</p> <p>Recover: Incident Recovery Communication (RC.CO) 25</p>
<p>Προστασία πρόσβασης σε συστήματα.</p> <p>Όλες οι προσωπικές πληροφορίες των χρηστών πρέπει να προστατεύονται από μη εξουσιοδοτημένη πρόσβαση.</p>	<p>Χρήση ισχυρών κωδικών πρόσβασης και πολυπαραγοντικής αυθεντικοποίησης (2FA ή ΜΦΑ). Εφαρμογή κρυπτογράφησης για τις βάσεις δεδομένων, έλεγχος & πρόσβαση στους διακομιστές μόνο από συγκεκριμένους χρήστες.</p>						

Παράδειγμα: Identification-and-Authentication-Policy (NIST) - I

NIST FUNCTION:

Protect

Protect: Identity Management and Access Control (PR-AA)

- PR-AA-01 Identities and credentials for authorized users, services, and hardware are managed by the organization
- Access Control Policy
 - Account Management/Access Control Standard
 - Configuration Management Policy
 - **Identification and Authentication Policy**
 - Sanitization Secure Disposal Standard
 - Secure Configuration Standard
 - Secure System Development Life Cycle Standard
- PR-AA-02 Identities are proofed and bound to credentials based on the context of interactions
- Access Control Policy
 - Account Management/Access Control Standard
 - Authentication Tokens Standard
 - Configuration Management Policy
 - Identification and Authentication Policy
- PR-AA-03 Users, services, and hardware are authenticated
- Remote Access Standard
- PR-AA-04 Identity assertions are protected, conveyed, and verified
- Access Control Policy
 - Account Management/Access Control Standard
 - Authentication Tokens Standard
 - Configuration Management Policy
 - Identification and Authentication Policy

Policy #:	Title:	Effective Date:
XXX	Identification and Authentication Policy	MM/DD/YY

PURPOSE

To ensure that only properly identified and authenticated users and devices are granted access to Information Technology (IT) resources in compliance with IT security policies, standards, and procedures.

REFERENCE

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53a – Identification and Authentication (IA), NIST SP 800-12, NIST SP 800-63, NIST SP 800-73, NIST SP 800-76, NIST SP 800-78, NIST SP 800-100, NIST SP 800-116; Homeland Security Presidential Directive (HSPD) 12 Policy for a Common Identification Standard for Federal Employees and Contractors; Federal Information Processing Standards (FIPS): FIPS 201, FIPS 140

POLICY

This policy is applicable to all departments and users of IT resources and assets.

1. IDENTIFICATION AND AUTHENTICATION

IT Department shall:

- a. Ensure that information systems uniquely identify and authenticate users or processes acting on behalf of [entity] users.
- b. Ensure that information systems implement multifactor authentication for network access to privileged accounts.
- c. Ensure that information systems implement multifactor authentication for network access to non-privileged accounts.
- d. Ensure that information systems implement multifactor authentication for local access to privileged accounts.
- e. Ensure that information systems implement replay-resistant authentication mechanisms for network access to privileged accounts.
- f. Ensure that information systems implement multifactor authentication for remote access to privileged and non-privileged accounts such that one of the factors is provided by a device separate from the system gaining access and the device utilizes a cryptographic strength mechanisms that protects the primary authentication token (secret key, private key or one-time password)

against compromise by protocol threats including: eavesdropper, replay, online guessing, verifier impersonation and man-in-the-middle attacks.

- g. Ensure that information systems accept and electronically verify Personal Identity Verification (PIV) credentials.
2. DEVICE IDENTIFICATION AND AUTHENTICATION
IT Department shall:
 - a. Ensure that information systems uniquely identify and authenticate all devices before establishing a network connection.
 3. IDENTIFIER MANAGEMENT
IT Department, through department information systems owners, shall:
 - a. Ensure that the [entity] manages information system identifiers by receiving authorization from [entity defined personnel or roles] to assign an individual, group, role, or device identifier.
 - b. Select an identifier that identifies an individual, group, role, or device.
 - c. Assign the identifier to the intended individual, group, role, or device.
 - d. Prevent reuse of identifiers for 90 days.
 - e. Disable the identifier after 30 days of inactivity.
 4. AUTHENTICATOR MANAGEMENT
IT Department shall:
 - a. Manage information system authenticators by verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, or device receiving the authenticator.
 - b. Establish initial authenticator content for authenticators defined by the organization.
 - c. Ensure that authenticators have sufficient strength of mechanism for their intended use.
 - d. Establish and implement administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators.
 - e. Change default content of authenticators prior to information system installation.

Παράδειγμα: Identification-and-Authentication-Policy (NIST) - II

- f. Establish minimum and maximum lifetime restrictions and reuse conditions for authenticators.
- g. Change/refresh authenticators every 90 days.
- h. Protect authenticator content from unauthorized disclosure and modification.
- i. Require individuals and devices to implement specific security safeguards to protect authenticators.
- j. Change authenticators for group/role accounts when membership to those account changes.
- k. Ensure that information systems, for password-based authentication enforce minimum password complexity that must not contain the user's entire Account Name value or entire Full Name value.
- l. Ensure passwords must contain characters from three of the following five categories:
 - i. Uppercase characters of European languages (A through Z, with diacritic marks, Greek and Cyrillic characters);
 - ii. Lowercase characters of European languages (a through z, sharp-s, with diacritic marks, Greek and Cyrillic characters);
 - iii. Base 10 digits (0 through 9);
 - iv. Non-alphanumeric characters ~@#\$%^&* _+=|\()0[];"<>,.?; and
 - v. Any Unicode character that is categorized as an alphabetic character, but is not uppercase or lowercase. This includes Unicode characters from Asian languages.
- m. Require passwords to have a minimum length of 8 characters.
- n. Enforce at least one changed character when new passwords are created.
- o. Store and transmit only cryptographically-protected passwords.
- p. Enforce password minimum and maximum lifetime restrictions of one day and 120 days respectively.
- q. Prohibit password reuse for 12 generations.

- r. Allow the use of a temporary password for system logons with an immediate change to a permanent password.
- s. Ensure that information system, for PKI-based authentication, validates certifications by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information.
- t. Enforce authorized access to the corresponding private key.
- u. Map the authenticated identity to the account of the individual or group.
- v. Implement a local cache of revocation data to support path discovery and validation in case of inability to access revocation information via the network.
- w. Require that the registration process to receive [entity defined types of and/or specific authenticators] be conducted in person or by a trusted third party before [entity defined registration authority] with authorization by [entity defined personnel or roles].
- x. Ensure that the information system, for hardware token-based authentication, employs mechanisms that satisfy [entity defined token quality requirements].

AUTHENTICATOR FEEDBACK

IT Department shall:

- a. Ensure that information systems obscure feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.

CRYPTOGRAPHIC MODULE AUTHENTICATION

IT Department shall:

- a. Ensure that information systems implement mechanisms for authentication to a cryptographic module that meet the requirements of applicable state and federal laws, directives, policies, regulations, standards, and guidance for such authentication.

IDENTIFICATION AND AUTHENTICATION

IT Department shall:

- a. Ensure that information systems uniquely identify and authenticate non-entity users or processes acting on behalf of non-entity users.
- b. Ensure that information systems accept and electronically verify Personal Identity Verification (PIV) credentials from other government agencies.

- c. Ensure that information systems accept only Federal Identity, Credential, and Access Management (FICAM) Trust Framework Solutions initiative approved third-party credentials.
- d. Ensure that the organization employs only FICAM-approved information system components in [entity defined information systems] to accept third-party credentials.

COMPLIANCE

Employees who violate this policy may be subject to appropriate disciplinary action up to and including discharge as well as both civil and criminal penalties. Non-employees, including, without limitation, contractors, may be subject to termination of contractual agreements, denial of access to IT resources, and other actions as well as both civil and criminal penalties.

POLICY EXCEPTIONS

Requests for exceptions to this policy shall be reviewed by the Chief Information Security Officer (CISO) and the Chief Information Officer (CIO). Departments requesting exceptions shall provide such requests to the CIO. The request should specifically state the scope of the exception along with justification for granting the exception, the potential impact or risk attendant upon granting the exception, risk mitigation measures to be undertaken by the IT Department, initiatives, actions and a time-frame for achieving the minimum compliance level with the policies set forth herein. The CIO shall review such requests; confer with the requesting department.

RESPONSIBLE DEPARTMENT

Chief Information Office and Information System Owners

DATE ISSUED/DATE REVIEWED

Date Issued:	MM/DD/YYYY
Date Reviewed:	MM/DD/YYYY

Οργάνωση των Επιχειρησιακών Διαδικασιών βάσει των Καταγεγραμμένων Πολιτικών Ασφαλείας (Control Document)

Name	Description	Required audit evidence	Questions			
Managing information security in the ICT supply chain	<p>Measure Processes and procedures should be established and implemented to manage the information security risks associated with the ICT product and service supply chain.</p> <p>Purpose To maintain an agreed level of information security in supplier relationships.</p>		<ul style="list-style-type: none"> * What is done to find out which other suppliers are in the ICT supply chain? * How are products/services that are critical to maintaining functionality identified in the ICT supply chain? * How can it be ensured that critical components and their origin are tracked through the entire ICT supply chain? * How is it ensured that the security requirements also apply to other service providers (sub-service providers)? * How is this compliance guaranteed? * How is this compliance checked (pentest, third-party certificates, ...)? 			
Name	Control Types	security properties	Cybersecurity concepts	Governance	Operational capabilities	Security domains
Managing information security in the ICT supply chain	Preventive Detective Corrective	Confidentiality Integrity Availability	Identity Protect Detect Respond Recover	Asset_management Information_protection Human_resource_security Physical_security System_and_network_security	Application_security Secure_configuration Identity_and_access_management Threat_and_vulnerability_management Continuity Supplier_relationships_security Legal_and_compliance Information_security_event_management Information_security_assurance	Governance_and_Ecosystem Protection Defence Resilience
Managing information security in the ICT supply chain	X	X X X	X		X	X X

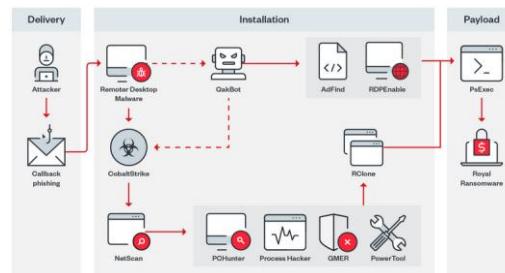
Περιπτώσεις Επιθέσεων & Εφαρμογή Μέτρων

- Επίθεση απόσπασης credential από Domain Controller



Πηγή: <http://www.criticalstart.com/2014/08/target-of-choice-your-windows-domain-controllers-2/#more-2787/>

- Ransomware Attack (π.χ. Royal Ransomware)



Tactic	Technique or Sub-technique
TA0005: Discovery	T1083: File and Directory Discovery
TA0007: Discovery	T1016: System Network Configuration Discovery
TA0007: Discovery	T1046: Network Service Discovery
TA0007: Discovery	T1057: Process Discovery
TA0007: Discovery	T1082: System Information Discovery
TA0007: Discovery	T1135: Network Share Discovery
TA0040: Impact	T1486: Data Encrypted for Impact
TA0040: Impact	T1489: Service Stop
TA0040: Impact	T1490: Inhibit System Recovery
TA0002: Execution	T1059: Command and Scripting Interpreter

Πηγές: https://www.trendmicro.com/en_us/research/22/l/conti-team-one-splinter-group-resurfaces-as-royal-ransomware-wit.html, <https://www.cybereason.com/blog/royal-ransomware-analysis>

Μοντέλο Ελάχιστης Απαιτούμενης πρόσβασης - Least privileged administrative model

- Εφαρμογή της **Αρχής του Least Privilege**: Κάθε χρήστης, λογαριασμός ή σύστημα πρέπει να διαθέτει μόνο τα απολύτως απαραίτητα δικαιώματα για να εκτελέσει τις εργασίες του — ούτε περισσότερα, ούτε λιγότερα
 - **Χρήση λογαριασμών 2 κατηγοριών:**
 - ✓ **Κανονικός λογαριασμός**: Για καθημερινές εργασίες, χωρίς δικαιώματα διαχειριστή
 - ✓ **Διαχειριστής (Administrator)**: Μόνο για διοικητικές ενέργειες στον Τομέα (domain) (π.χ. επεξεργασία Active Directory, Εγκαταστάσεις Εφαρμογών & group policies,...)
 - **Μείωση κινδύνου κακόβουλων ενεργειών ή λαθών**
 - **Καλύτερος έλεγχος πρόσβασης και διαφάνεια ενεργειών**
- ✓ Απενεργοποίηση του Τοπικού Λογαριασμού Διαχειριστή (Local Administrator) σε όλους τους Υπολογιστές της Οντότητας
- 

Regular User Account

Only has permissions to:
Read / Send emails
Browse the Web
Access files
Print
Using applications
etc..



Administrator Account

Only use account for admin tasks:
Making changes to devices (e.g network settings)
Editing Active Directory
Creating Hyper-V / Vmware VMs
Installing software
Creating GPOs

Λήψη Αντιγράφων Ασφαλείας (backups) με τη μέθοδο 3-2-1

- Εφαρμογή Μεθόδου 3-2-1:
 - ✓ 3 πλήρη αντίγραφα δεδομένων
 - ✓ 2 αποθηκευμένα τοπικά σε διαφορετικά μέσα
 - ✓ 1 αποθηκευμένο εκτός τοποθεσίας (off-site ή cloud)
 - ✓ Integrity Check
- Καθορισμός RTOs (Recovery Time Objectives)
- Καθορισμός RPOs (Recovery Point Objectives)
- Ιεράρχηση κρίσιμων συστημάτων & αύξηση της συχνότητας λήψης backup τους
- Ελεγχόμενη, περιορισμένη και καταγραφόμενη πρόσβαση στα backups
- Τακτικός έλεγχος διαδικασιών ανάκτησης (τουλάχιστον 1 φορά/έτος)
- Όχι τοπική αποθήκευση σε προσωπικά τερματικά
- Χρήση secure protocol για λήψη backup μέσω δικτυακών πόρων:
 - ✓ Encrypted SMB 3.x backup share (AES-128 ή AES-256)
 - ✓ HTTPS / WebDAV
 - ✓ iSCSI (with IPsec ή isolated VLAN)
 - ✓ NFSv4 (krb5p = Kerberos authentication + integrity + privacy)



Οδηγοί & Συμβουλές από ΕΑΚ

- ✓ **Βέλτιστες Πρακτικές για τη διασφάλιση των Συστημάτων Υγείας**
 - Καταγραφή υλικού και λογισμικού
 - Αντίγραφα Ασφαλείας και Ανάκαμψης Δεδομένων
 - Πολυπαραγοντικός Έλεγχος Ταυτότητας (MFA) και Διαχείριση Προνομιακής Πρόσβασης (PAM)
 - Τακτικές Αναβαθμίσεις Λογισμικού και Ενημερώσεις – Διαχείριση ευπαθειών
 - Κατακερματισμός Δικτύου
 - Ανίχνευση και Ανταπόκριση σε Σημεία Τερματικών (EDR)
 - Εκπαίδευση Ευαισθητοποίησης για Phishing
 - Φίλτράρισμα Email και Ανίχνευση Απειλών
 - Ασφαλής Διαμόρφωση και Θωράκιση Συστημάτων Καταγραφή και παρακολούθηση συμβάντων (event logs monitoring Security Information & Event Management)
 - Σχέδιο Απόκρισης σε Περιστατικά (Incident Response Plan)
 - Υλοποίηση ελέγχων παρείσδυσης (penetration tests)
- ✓ **Οδηγός 15 σημείων ενίσχυσης της κυβερνοασφάλειας και αποτροπής λυτρωσικών επιθέσεων (ransomware) για τα Πανεπιστημιακά Ιδρύματα**
 - Αντίγραφα Ασφαλείας και Ανάκαμψης Δεδομένων
 - Καταγραφή υλικού και λογισμικού
 - Πολυπαραγοντικός Έλεγχος Ταυτότητας (MFA)
 - Ανίχνευση και Ανταπόκριση σε Σημεία Τερματικών (EDR)
 - Εκπαίδευση Ευαισθητοποίησης για Phishing
 - Κατακερματισμός Δικτύου
 - Διαχείριση Προνομιακής Πρόσβασης (PAM)
 - Φίλτράρισμα Email και Ανίχνευση Απειλών
 - Ασφαλής Διαμόρφωση και Θωράκιση Συστημάτων (Security Information & Event Management)
 - Καταγραφή και παρακολούθηση συμβάντων (event logs monitoring, SIEM)
 - Αποφυγή Χρήσης Πειρατικού Λογισμικού
 - Παρακολούθηση για Μη Εξουσιοδοτημένο Crypto Mining, Tor και Υπηρεσίες Torrent
 - Υλοποίηση ελέγχων παρείσδυσης (penetration tests)

Penetration Test

Τύπος Δοκιμής	Σκοπός / Σχέση με NIS2	Ενδεικτικά Αποδεικτικά / Τεκμηρίωση	Συχνότητα
Εξωτερική Διείσδυση Υποδομής (Internet-facing)	Επιδεικνύει την προστασία των περιμετρικών συστημάτων και τη μείωση της επιφάνειας επίθεσης, όπως απαιτεί η NIS2 για πρόληψη περιστατικών.	Λίστα IP/ονομάτων host, ευρήματα επαθειών, screenshots/logs, αλυσίδες εκμετάλλευσης (σε υψηλό επίπεδο), CVSS/μέτρα μετριασμού, αποτελέσματα επανελέγουχου.	Τουλάχιστον 1 φορά/έτος ή μετά από σημαντική αλλαγή συστήματος.
Εσωτερικός Έλεγχος Δικτύου	Επαληθεύει την ικανότητα εντοπισμού και μετριασμού κινδύνων από εσωτερικούς χρήστες ή παραβιασμένα endpoints.	Σενάριο προσομοιώμενης επίθεσης, αρχεία καταγραφής host, χάρτινης βημάτων σε MITRE ATT&CK, εισιτήρια αποκατάστασης, αποτελέσματα επανελέγουχου.	Ετησίως ή ανά 6 μήνες για περιβάλλοντα υψηλού κινδύνου.
Έλεγχος Web Εφαρμογών & APIs	Εξασφαλίζει ότι κρίσιμες εφαρμογές προστατεύονται από ευπάθειες OWASP (Open Web Application Security Project) Top 10, όπως απαιτείται για ασφαλεία υπηρεσιών και δεδομένων.	Λίστα επαθειών, PoC (ανωνυμοποιημένο), traces αιτήσεων/απαντήσεων, οδηγίες επιδόρθωσης, αποδείξεις επανελέγουχου.	Με κάθε νέα έκδοση ή ανά τρίμηνο για κρίσιμες εφαρμογές.
Έλεγχος με Διαπιστευτήρια (Authenticated Testing)	Διασφαλίζει προστασία σε περίπτωση παραβιάσης λογαριασμού χρήστη και ορθή διαχείριση προνομίων.	Λογαριασμοί/ρόλοι που χρησιμοποιήθηκαν, εύρηματα και επιδόρθωση, αποδείξη επανελέγουχου.	Μετά από αλλαγές σε ρόλους/διαχείριση ταυτότητας ή νέα λειτουργικότητα.
Έλεγχος Ρυθμίσεων & Υποδομής Cloud	Επαληθεύει σωστές ρυθμίσεις IAM, περιορισμού πρόσβασης και ασφαλείας δεδομένων – κρίσιμες απαιτήσεις NIS2 για διαχείριση κινδύνου.	Screenshots ρυθμίσεων, αποτελέσματα επαλέγουχου πρόσβασης, αποδείξεις διορθώσεων και επανελέγουχου.	Τριμηνιαία ή μετά από σημαντικές αλλαγές σε περιβάλλον cloud.
Έλεγχος Εφαρμογών Κινητών Συσκευών	Διασφαλίζει ότι οι εφαρμογές κινητών δεν εκθέτουν δεδομένα μέσω κακής αποθήκευσης ή API.	Απόσπασμα κώδικα (με απόκρυψη), ευρήματα API, οδηγίες επιδόρθωσης, επανελέγουχος.	Με κάθε νέα έκδοση εφαρμογής.
Έλεγχος Ασύρματης & Απομακρυσμένης Πρόσβασης	Επιβεβαιώνει ασφάλεια Wi-Fi, VPN και μηχανισμών τηλεργασίας, όπως απαιτείται για την ασφαλεία πρόσβασης.	Δοκιμές σύνδεσης, ευρήματα ρυθμίσεων, αποδεικτικά αποκατάστασης.	Ετησίως ή μετά από αλλαγές υποδομής δικτύου.
Κοινωνική Μηχανική (Phishing/Vishing)	Αξιολογεί την ανθεκτικότητα προσωπικού σε επιθέσεις κοινωνικής μηχανής και την αποτελεσματικότητα εκπαίδευσης/αναφοράς.	Μετρικά εκστρατείας, αναφορές click rate, ενέργειες εκπαίδευσης/αποκατάστασης.	Ανά εξάμηνο ή μετά από εκπαιδευση προσωπικού.
Red Team (Προσομοίωση Αντιπάλου)	Αξιολογεί την ικανότητα ανίχνευσης και απόκρισης (SOC/IR), σύμφωνα με τις απαιτήσεις NIS2 για "detect and respond".	Χρονολόγιο ενεργειών, ανιχνεύσεις επιτυχημένες/ανεπιτυχείς, lessons learned, επικαιροποίηση playbook IR.	Ετησίως ή ανά 12–18 μήνες ανάλογα με την ωριμότητα.
Δοκιμές Denial-of-Service (DoS/DDoS)	Ελέγχει την ανθεκτικότητα και τα σχέδια μετριασμού επιθέσεων διαθεσμότητας.	Μετρήσεις κυκλοφορίας, καταγραφή επιπτώσεων, αναφορές απόδοσης μηχανισμών αύμνας.	Μόνο εφόσον υπάρχει ασφαλές περιβάλλον δοκιμών και ρητή έξουσιοδότηση.
Έλεγχος OT / ICS (Βιομηχανικά Συστήματα)	Διασφαλίζει την ασφάλεια κρίσιμων λειτουργικών τεχνολογιών, με έμφαση στη μη παρεμβατική αξιολόγηση.	Σχέδιο ασφάλειας, υπογραφή μηχανικών, logs δοκιμών, ενέργειες αποκατάστασης.	Ετησίως ή σύμφωνα με κύκλο συντήρησης
Αξιολόγηση Τρίτων & Εφοδιαστικής Αλυσίδας	Αποδεικνύει διαχείριση κινδύνου συνεργατών/προμηθευτών όπως ορίζει η NIS2.	Ερωτηματολόγια ασφαλείας, αποδεικτικά δοκιμών, κοινά ευρήματα, ρήτρες SOW.	Ετησίως ή με κάθε νέο κρίσιμο προμηθευτή

Penetration Testing Tool	Description
Password Crackers	Password cracking tools are often referred to as password recovery tools and can be used to crack or recover a password. This is accomplished either by removing the original password, after bypassing the data encryption, or by outright discovery of the password. Password crackers repeatedly make guesses in order to crack the password. Examples of password cracking tools include John the Ripper, Ophcrack, L0phtCrack, THC Hydra, RainbowCrack, and Medusa.
Wireless Hacking Tools	Wireless hacking tools are used to intentionally hack into a wireless network to detect security vulnerabilities. Examples of wireless hacking tools include Aircrack-ng, Kismet, InSSIDer, KisMAC, Firesheep, and NetStumbler.
Network Scanning and Hacking Tools	Network scanning tools are used to probe network devices, servers, and hosts for open TCP or UDP ports. Examples of scanning tools include Nmap, SuperScan, Angry IP Scanner, and NetScanTools.
Packet Crafting Tools	These tools are used to probe and test a firewall's robustness using specially crafted forged packets. Examples include Hping, Scapy, Socat, Yersinia, Netcat, Nping, and Nemesis.
Packet Sniffers	These tools are used to capture and analyze packets within traditional Ethernet LANs or WLANs. Tools include Wireshark, Tcpdump, Ettercap, Dsniff, EtherApe, Paros, Fiddler, Ratproxy, and SSLstrip.
Rootkit Detectors	This is a directory and file integrity checker used by white hats to detect installed root kits. Example tools include AIDE, Netfilter, and PF: OpenBSD Packet Filter.
Fuzzers to Search Vulnerabilities	Fuzzers are tools used by threat actors to discover a computer's security vulnerabilities. Examples of fuzzers include Skipfish, Wapiti, and W3af.
Forensic Tools	These tools are used by white hats to hackers to sniff out any trace of evidence existing in a computer. Example of tools include Sleuth Kit, Helix, Maltego, and Encase.
Debuggers	These tools are used by black hats to reverse engineer binary files when writing exploits. They are also used by white hats when analyzing malware. Debugging tools include GDB, WinDbg, IDA Pro, and Immunity Debugger.
Hacking Operating Systems	These are specially designed operating systems preloaded with tools optimized for hacking. Examples of specially designed hacking operating systems include Kali Linux, Knoppix, BackBox Linux.
Encryption Tools	Encryption tools use algorithm schemes to encode the data to prevent unauthorized access to the encrypted data. Examples of these tools include VeraCrypt, CipherShed, OpenSSH, OpenSSL, Tor, OpenVPN, and Stunnel.
Vulnerability Exploitation Tools	These tools identify whether a remote host is vulnerable to a security attack. Examples of vulnerability exploitation tools include Metasploit, Core Impact, Sqlmap, Social Engineer Toolkit, and Nmapspider.
Vulnerability Scanners	These tools scan a network or system to identify open ports. They can also be used to scan for known vulnerabilities and scan VMs, BYOD devices, and client databases. Examples of tools include Nmap, Secunia PSI, Core Impact, Nessus v6, SAINT, and Open VAS.

Σύνοψη Πολιτικών & Μέτρων - I

1. Access Control and Authentication

Role-based Access: Limit access to sensitive data and systems based on users' roles and responsibilities.

Strong Authentication: Implement multi-factor authentication (MFA) to prevent unauthorized access.

Principle of Least Privilege: Ensure users only have the minimum level of access necessary to perform their duties.

2. Data Protection and Privacy

Data Encryption: Ensure all data in transit and at rest is encrypted using industry-standard encryption protocols.

Data Minimization: Share only the necessary amount of data between organizations to reduce exposure.

Compliance with Regulations: Follow relevant laws and regulations (e.g., GDPR) regarding data privacy and security.

3. Incident Reporting and Response

Timely Reporting: Establish clear procedures for reporting any security incidents or breaches within the collaboration tool.

Collaboration on Response: Define how the organizations will collaborate in responding to incidents, ensuring transparency and coordination.

Root Cause Analysis: Work together to investigate the causes of incidents and implement measures to prevent recurrence.

4. Acceptable Use and Behavior

Respectful Communication: Maintain professional and respectful communication among members to avoid misunderstandings or conflicts.

Prohibited Activities: Clearly outline prohibited behaviors, such as the use of the platform for malicious activities, spreading malware, or sharing inappropriate content.

Content Moderation: Implement mechanisms to prevent and report inappropriate or offensive content.

Σύνοψη Πολιτικών & Μέτρων - II

5. Security Hygiene Practices

Regular Software Updates: Ensure that all collaboration tools are up-to-date with the latest security patches and updates.

Vulnerability Scanning: Periodically scan shared tools for vulnerabilities and resolve any discovered issues.

Password Management: Encourage strong password policies and, where applicable, the use of password managers to prevent weak passwords.

6. Third-party Integrations and Vendor Risk Management

Due Diligence: Ensure that any third-party integrations with the collaboration tool meet the same cybersecurity standards as internal systems.

Security Audits: Conduct regular security audits of third-party tools and services integrated with the collaboration platform.

7. Transparency and Accountability

Audit Trails: Maintain logs and records of all user activities to ensure accountability and traceability.

Regular Reviews: Perform periodic audits of user permissions and activities to ensure compliance with security policies.

Clear Accountability: Define clear responsibilities for security, data management, and incident response.

8. Training and Awareness

Cybersecurity Training: Regularly train all users on the risks, best practices, and tools they will use to collaborate securely.

Awareness Campaigns: Promote awareness around common threats like phishing, social engineering, and insider threats.

Collaboration Etiquette: Provide guidelines on the proper use of communication tools, including how to share information securely.

Σύνοψη Πολιτικών & Μέτρων - III

9. Collaboration and Information Sharing

Secure Information Sharing: Establish protocols for securely sharing sensitive information between organizations.

Threat Intelligence Sharing: Encourage sharing threat intelligence to improve overall security across all collaborating organizations.

Clear Data Ownership: Define who owns the data, including intellectual property and sensitive information, shared across platforms.

10. Dispute Resolution

Conflict Management: Provide clear procedures for handling disputes or disagreements between organizations or individuals using the collaboration tools.

Escalation Procedures: Define a process for escalating unresolved security or operational issues.

11. End-of-Life and Exit Strategy

Data Retention and Deletion: Establish clear guidelines for the retention and secure deletion of data when collaborations end or when a participant leaves the platform.

Access Termination: Define procedures for promptly revoking access to collaboration tools upon termination of roles or relationships.

12. Continuous Improvement

Regular Review and Updates: Continuously review and update the Code of Conduct in response to evolving threats, new tools, and organizational changes.

Feedback Mechanisms: Encourage feedback from participants to improve the collaboration process and security posture.

Διαχείριση Περιστατικού Κυβερνοασφάλειας

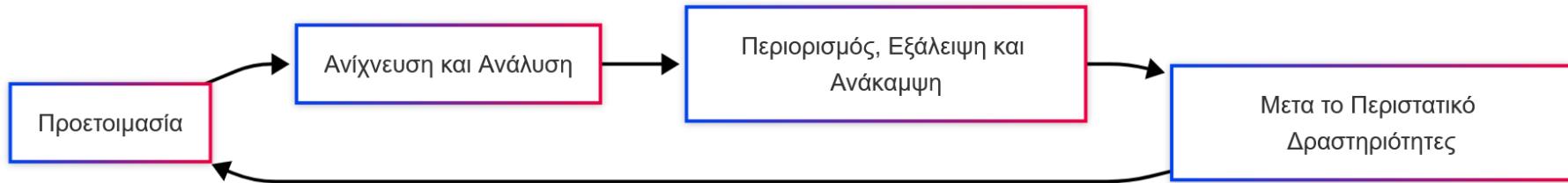
- **Συμβάν:** Ύποπτη ή ανώμαλη δραστηριότητα που δεν έχει αποδειχτεί ακόμα ότι είναι κακόβουλη ή επιβλαβής
- π.χ. Χρήστης Συνδέθηκε εκτός προβλεπόμενου ωραρίου ή μαζικό upload πολλών εγγραφών σε κάποια ιστοσελίδα
- **Περιστατικό:** Μια σοβαρή παραβίαση ασφαλείας που έχει ήδη προκαλέσει βλάβη ή κινδύνους στην ασφάλεια
- π.χ. κλείδωμα αρχείων μετά από ransomware (παραβίαση διαθεσιμότητας)
- **Ως περιστατικό** νοείται κάθε συμβάν που θέτει σε κίνδυνο τη διαθεσιμότητα, την ακεραιότητα ή την εμπιστευτικότητα των δεδομένων που αποθηκεύονται, μεταδίδονται ή υποβάλλονται σε επεξεργασία ή των υπηρεσιών που προσφέρονται ή είναι προσβάσιμες μέσω συστημάτων δικτύου και πληροφοριακών συστημάτων καθώς και την αυθεντικότητα

**Ένα περιστατικό
θεωρείται
σημαντικό αν:**

α) έχει προκαλέσει ή μπορεί να προκαλέσει σοβαρή λειτουργική διατάραξη των υπηρεσιών ή οικονομική ζημία για την οικεία οντότητα,

β) έχει επιπρεάσει ή μπορεί να επιπρεάσει άλλα φυσικά ή νομικά πρόσωπα προκαλώντας σημαντική υλική ή μη υλική ζημία.

Διαχείριση Περιστατικού Κυβερνοασφάλειας – Κύκλος Ζωής



- ✓ Κύκλος ζωής απόκρισης περιστατικών NIST (<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf>)

I. Προετοιμασία (Preparation):

Δημιουργία σχεδίου απόκρισης σε περιστατικά, την εκπαίδευση του προσωπικού, την ανάπτυξη εργαλείων και την εγκατάσταση πολιτικών ασφαλείας

II. Ανίχνευση και Ανάλυση (Detection and Analysis):

Περιλαμβάνει την ανίχνευση ύποπτων δραστηριοτήτων μέσω εργαλείων και την ανάλυση των δεδομένων για να κατανοηθεί αν πρόκειται για πραγματικό περιστατικό και ποιο είναι το μέγεθός του. Η αναγνώριση του περιστατικού είναι κρίσιμη για την αποτελεσματική αντίδραση.

III. Περιορισμός, Εξάλειψη και Ανάκαμψη (Containment, Eradication, and Recovery):

Όταν το περιστατικό εντοπιστεί, το πρώτο βήμα είναι να περιοριστεί η διάδοση ή η εξάπλωσή του (π.χ. απομόνωση μολυσμένων συστημάτων). Στη συνέχεια, το κακόβουλο λογισμικό ή η απειλή εξαλείφεται, αποκαθίστανται τα συστήματα και οι υπηρεσίες στην κανονική τους λειτουργία. Η αποκατάσταση μπορεί να περιλαμβάνει ανάκτηση δεδομένων και επαναφορά των συστημάτων σε ασφαλή κατάσταση.

IV. Μετά το Περιστατικό Δραστηριότητες (Post-Incident Activity):

Η Οντότητα αναλύει το περιστατικό για να μάθει από αυτό και να ενισχύσει την ασφάλεια στο μέλλον. Αυτό περιλαμβάνει την αναφορά του περιστατικού, τη διερεύνηση της αιτίας του, την αξιολόγηση των διαδικασιών και την εφαρμογή βελτιώσεων στο σχέδιο απόκρισης. Στόχος είναι να μειωθεί ο κίνδυνος για μελλοντικά περιστατικά και να ενισχυθεί η ασφάλεια.

Υποβολή Αναφορών σε Περίπτωση Περιστατικού

Πότε υποβάλλονται αναφορές



**Έγκαιρη προειδοποίηση
εντός 24 ωρών** από τη στιγμή που
αντιλήφθηκαν το περιστατικό



**Κοινοποίηση περιστατικού
εντός 72 ωρών** από τη στιγμή που
αντιλήφθηκαν το περιστατικό



Ενδιάμεση έκθεση, αν αιτηθεί από την
Εθνική Αρχή Κυβερνοασφάλειας



Τελική έκθεση το αργότερο σε 1 μήνα
μετά την υποβολή της κοινοποίησης

Τι περιέχουν οι αναφορές

- Προκαταρκτική αξιολόγηση (είδος περιστατικού, πιθανός αντίκτυπος).

- Πλήρη αναφορά με επικαιροποίηση πληροφοριών.
- Αρχική αξιολόγηση (σοβαρότητα, αντίκτυπος, ενδείξεις παραβίασης, κοκ).

- Επικαιροποίηση της κατάστασης.

- Λεπτομερή περιγραφή του περιστατικού (σοβαρότητα, αντίκτυπος, κοκ).
- Είδος απειλής ή βασική αιτία που ενδεχομένως προκάλεσε το περιστατικό.
- Μέτρα αντιμετώπισης που εφαρμόζονται.

Υποβάλλεται από τον ΥΑΣΠΕ στην ΕΑΚ

(Οι Δημόσιες οντότητες, της Κεντρικής Κυβέρνησης και των Οργανισμών Τοπικής Αυτοδιοίκησης Α' και Β' βαθμού, κοινοποιούν τα περιστατικά στην CSIRT της Εθνικής Υπηρεσίας Πληροφοριών με ταυτόχρονη ενημέρωση της Εθνικής Αρχής Κυβερνοασφάλειας)

https://cyber.gov.gr/kyvernoepithes_eis/anafora-symvanton/

Φόρμα Υποβολής Αναφοράς Περιστατικού

Αντίκτυπος Περιστατικού	
Παραβίαση αρχών ασφάλειας πληροφοριών	<input type="checkbox"/> Εμπιστευτικότητα <input type="checkbox"/> Ακεραιότητα <input type="checkbox"/> Διαθεσιμότητα
Πλήθος επηρεασμένων χρηστών	
Έκταση διατάραξης της λειτουργίας / Διάρκεια μη διαθεσιμότητας της υπηρεσίας (σε χρηστώρων)	
Γεωγραφική έκταση	
Πόροι που επηρεάστηκαν	
Εξαρτώμενες οντότητες	
Έκταση επιπτώσεων σε κινητικές/ οικονομικές δραστηριότητες	
Εκτιμώμενη Ήμερη	
Υλικές ζημιές	
Επιπτώσεις φήμης	
Επιπτώσεις στην Υγεία, τη δημόσια ασφάλεια & προστασία/ πυθανές ανθρώπινες απώλειες	
Απώλεια/ Παραβίαση Δεδομένων	<input type="checkbox"/> Δημόσια <input type="checkbox"/> Προσωπικά <input type="checkbox"/> Ευαίσθητα <input type="checkbox"/> Απόρρητα <input type="checkbox"/> Άγνωστο
Τόπος δεδομένων που τέθηκαν σε κίνδυνο	
Διασυνοριακός αντίκτυπος	
Σύντομη Περιγραφή	Επιλέξτε ένα στοιχείο.

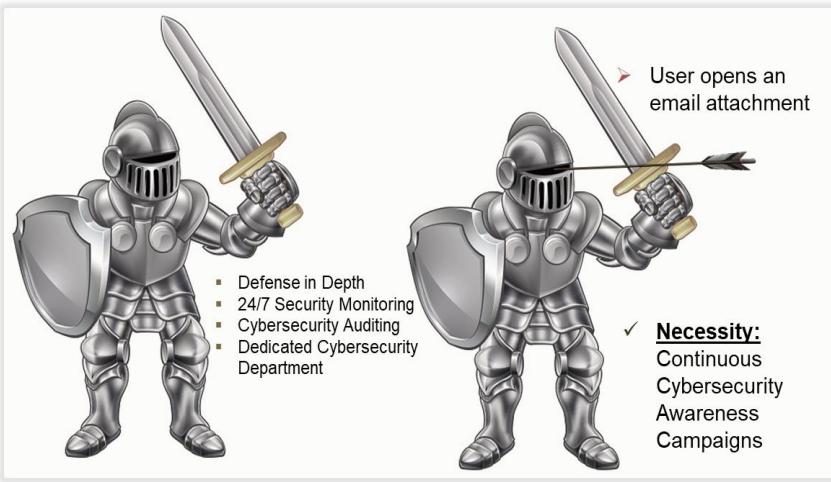
Αναλυτική Περιγραφή Περιστατικού				
Χρόνος συμβάντος	Ημερομηνία	Κάντε κλικ ή πατήστε	Ώρα	--::--
Χρόνος εντοπισμού	Ημερομηνία	Κάντε κλικ ή πατήστε	Ώρα	--::--
Διάρκεια				
Αναλυτικά αίτια περιστατικού				
Αναλυτικά στοιχεία πόρων που επηρεάστηκαν				

Τρέχουσα Κατάσταση	
Μετριασμός επιπτώσεων	
Κατάσταση περιστατικού	Επιλέξτε ένα στοιχείο.
Ενέργειες που έχουν ληφθεί για τον μετριασμό/ περιορισμό του αντικύτου που περιστατικού	
Επίπεδο μετριασμού επιπτώσεων	
Ενεργοποίηση BCP/ DRPs	<input type="checkbox"/> Ναι <input type="checkbox"/> Όχι
Κατάσταση σχεδίου	
Προγραμματισμένες ενέργειες	
Χρόνος αποκατάστασης	
Ανάγκη ενίσχυσης από CSIRT	<input type="checkbox"/> Ναι <input type="checkbox"/> Όχι
Ανάγκη ενίσχυσης από άλλες Αρχές	
Σημειώσεις	

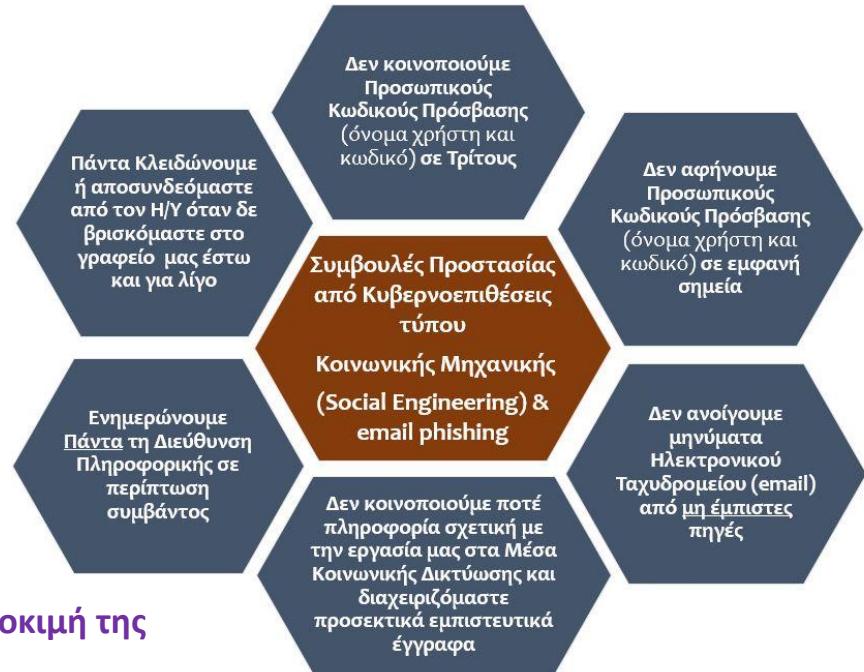
Ενημέρωση Εμπλεκομένων	
Χρήστες που επηρεάστηκαν	
Αρμόδιες (Εθνικές) Αρχές	
Διασυνοριακή ενημέρωση	
Ενημέρωση κοντού	

Η επόμενη μέρα	
Συμπεράσματα	
Κύρια αίτια	
Προκλήσεις	
Προτάσεις	
Μακροπρόθεσμα μέτρα ασφάλειας	

Απαραίτητη η Εκστρατεία Ευαισθητοποίησης Κυβερνοασφάλειας στο Προσωπικό των Οντοτήτων



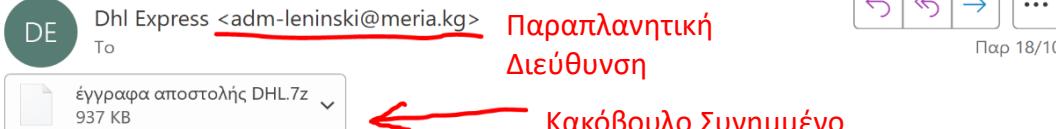
- <https://zeroday.im/> (Online Threat Heat Map)
- ✓ **Πλαίσιο phishing ανοιχτού κώδικα που διευκολύνει τη δοκιμή της έκθεσης του οργανισμού σας σε επιθέσεις phishing:**
<https://getgophish.com/> , <https://github.com/trustedsec/social-engineer-toolkit> ,
<https://github.com/rsmusllp/king-phisher>



Πώς αναγνωρίζουμε αν κάποιο Ηλ. Μήνυμα είναι Phishing;

Τίτλος: Επείγον: παραλήφθηκε νέο πακέτο - έγγραφα αποστολής **DHL**

Αποστολέας:



Αγαπητέ πελάτη,

Αριθμός παρακολούθησης: Προστέθηκε στο συνημμένο τιμολόγιο

Τύπος συσκευασίας: Standard

Αριθμός τεμαχίων: τεμάχια

Βάρος: 70,40 kg. Επισυνάπτουμε αντίγραφα των εγγράφων για αναφορά σας. Επικοινωνήστε μαζί μας. Εξυπηρέτηση πελατών (CS) για περισσότερες πληροφορίες

Πάντα σε εξυπηρετεί καλύτερα!

DHL EXPRESS

Αυτό είναι ένα αυτοματοποιημένο email, μην απαντήσετε απευθείας. Εάν έχετε οποιεσδήποτε ερωτήσεις, επικοινωνήστε μαζί μας επίσημα.

DHL Express (Hellas) SA
44, Alimou Ave.
174 55, Alimos
Greece
Tel: +30 2109890860

Πώς αναγνωρίζουμε αν κάποιο Ηλ. Μήνυμα είναι Phishing;

Τίτλος: Παρακαλούμε Ολοκληρώστε την Επικύρωση Στοιχείων σας

Αποστολέας:



Αγαπητέ χρήστη,

Για να διατηρήσετε την πρόσβασή σας στις υπηρεσίες μας, παρακαλούμε να ενημερώσετε τα δεδομένα σας μέσω του eGov-KYC. Αυτή η διαδικασία είναι απαραίτητη για την συμμόρφωση με τις απαιτήσεις του GDPR.

Ενημέρωση μέχρι 11 Νοεμβρίου 2024

Κάντε κλικ στο παρακάτω κουμπί για να επικαιροποιήσετε τα δεδομένα σας.



Για περισσότερες πληροφορίες, επισκεφτείτε το gov.gr.

Πώς αναγνωρίζουμε αν κάποιο Ηλ. Μήνυμα είναι Phishing;

Τίτλος: Δικαστικές Εντολές.

Αποστολέας:



Ελληνική Αστυνομία <www.astynomia.gr@gmail.com>

To undisclosed-recipients:



Αντιστράτηγος..pdf
263 KB

Γεια σας,
Παρακαλώ διαβάστε τη συνημμένη κλήση που σας αφορά και απαντήστε μου.

Με τους καλύτερους χαιρετισμούς

Δημήτριος Μάλλιος.

Αντιστράτηγος Αστυνομίας

Αρχηγός της Ελληνικής Αστυνομίας

Παραπλανητική Διεύθυνση Email

Reply

Reply All

Forward

...

Σαβ 9/11/2024 12:22 πμ

Πιθανός Ιός!

Ερωτήσεις;



ARISTOTLE
UNIVERSITY
OF THESSALONIKI

GOOGLE.ORG
CYBERSECURITY
SEMINARS