ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ

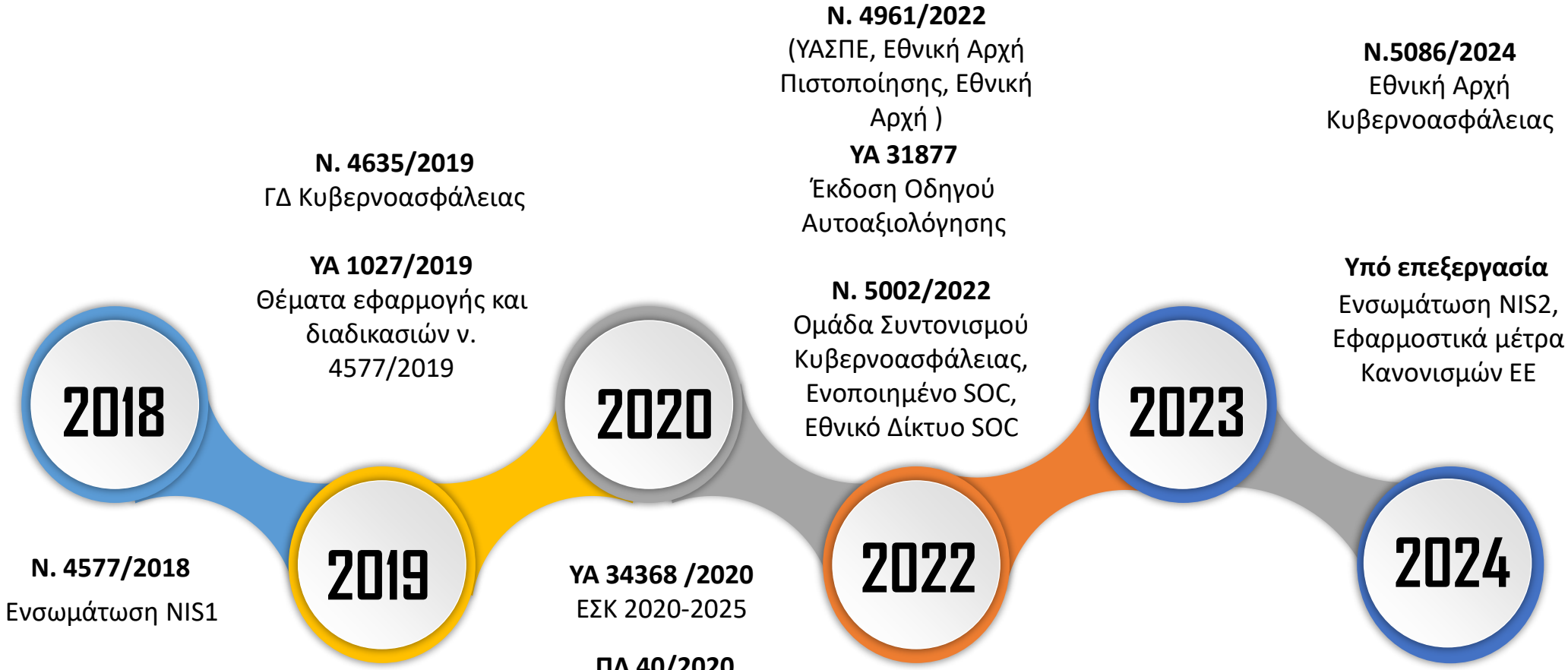
ΕΘΝΙΚΗ ΑΡΧΗ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ

Διακυβέρνηση Κυβερνοασφάλειας: προειδοποίηση, ανίχνευση και αντιμετώπιση κυβερνοεπιθέσεων

Θωμάς Δομπρίδης

03 Ιουλίου, 2024

Εθνικό θεσμικό πλαίσιο κυβερνοασφάλειας



National Cyber Security Authority
N.5086/2024

Άρθρο 3 - Σύσταση Εθνικής Αρχής Κυβερνοασφάλειας

Συστήνεται νομικό πρόσωπο δημοσίου δικαίου (Ν.Π.Δ.Δ.) με την επωνυμία **«Εθνική Αρχή Κυβερνοασφάλειας»** (Αρχή). Για τις σχέσεις της με την αλλοδαπή, η Αρχή χρησιμοποιεί την επωνυμία «National Cybersecurity Authority (NCSA)». Η Αρχή εποπτεύεται από τον **Υπουργό Ψηφιακής Διακυβέρνησης** και εδρεύει στην **Αθήνα**.

Άρθρο 4 - Σκοπός και αρμοδιότητες

Σκοπός της Αρχής είναι η οργάνωση, ο συντονισμός, η εφαρμογή και ο έλεγχος ενός ολοκληρωμένου πλαισίου στρατηγικών, μέτρων και δράσεων για την επίτευξη υψηλού επιπέδου κυβερνοασφάλειας στη χώρα, σε επίπεδο πρόληψης, προστασίας, αποτροπής, εντοπισμού, αντιμετώπισης, αποκατάστασης και ανάκαμψης από κυβερνοεπιθέσεις.

Άρθρο 5 - Όργανα διοίκησης

Η Αρχή διοικείται από τον **Διοικητή** και τους **Υποδιοικητές**.

National Cyber Security Authority
N.5086/2024

Άρθρο 4 - Σκοπός και αρμοδιότητες

2. Για την εκπλήρωση του σκοπού της η Αρχή ιδίως:

θ) Λαμβάνει, ιδίως, τεχνικά μέτρα αποτροπής και αντιμετώπισης του κυβερνοεγκλήματος σε συνεργασία με άλλες αρμόδιες αρχές και υπηρεσίες, και ιδίως με την Ελληνική Αστυνομία.

ιβ) Παρακολουθεί το συνολικό επίπεδο ασφάλειας του κυβερνοχώρου στη χώρα και προλαμβάνει, προστατεύει, συντονίζει και συμβάλλει στην αντιμετώπιση απειλών και κυβερνοεπιθέσεων, καθώς και στη διαχείριση περιστατικών ασφαλείας, μεταξύ άλλων, με τη λειτουργία του Ενοποιημένου SOC, του Εθνικού Δικτύου SOC και της Ομάδας Απόκρισης συμβάντων στον κυβερνοχώρο (CSIRT), σε συνεργασία με τις συναρμόδιες για την κυβερνοασφάλεια αρχές σε εθνικό, ενωσιακό και διεθνές επίπεδο για την επίτευξη των εθνικών στόχων για τη διασφάλιση υψηλού επιπέδου ασφαλείας, καθώς και για την προάσπιση των ατομικών δικαιωμάτων στον κυβερνοχώρο.

National Cyber Security Authority
N.5086/2024

Άρθρο 4 - Σκοπός και αρμοδιότητες

2. Για την εκπλήρωση του σκοπού της η Αρχή ιδίως:

ιγ) Καταρτίζει το Εθνικό Σχέδιο Έκτακτης Ανάγκης, συμβάλλει στην εκπόνηση του Εθνικού Σχεδίου Αποτίμησης Κινδύνων Συστημάτων Τεχνολογίας Πληροφορικής και Επικοινωνιών, τα οποία προβλέπονται στην περ. γ) του άρθρου 22 και στο άρθρο 29 του ν. 5002/2022 (Α' 228) αντίστοιχα, και καταρτίζει το Εθνικό Σχέδιο Αντιμετώπισης Περιστατικών και Κρίσεων στον Κυβερνοχώρο, τα οποία υποβάλλει προς έγκριση στην Επιτροπή Συντονισμού για θέματα Κυβερνοασφάλειας.

ιδ) Αποτελεί το ενιαίο σημείο αναφοράς σχετικά με απειλές και συμβάντα στον κυβερνοχώρο, συλλέγοντας και διαμοιράζοντας πληροφορίες προς άλλους δημόσιους και ιδιωτικούς φορείς, σε συνεργασία με άλλες αρχές, σε εθνικό, ευρωπαϊκό και διεθνές επίπεδο, για την ανίχνευση, συγκέντρωση και ανάλυση δεδομένων που σχετίζονται με απειλές και περιστατικά στον κυβερνοχώρο.

National Cyber Security Authority
N.5086/2024

Άρθρο 4 - Σκοπός και αρμοδιότητες

2. Για την εκπλήρωση του σκοπού της η Αρχή ιδίως:

ιε) Παρέχει κατευθυντήριες γραμμές και δεσμευτικές οδηγίες για την αντιμετώπιση κυβερνοαπειλών σε δημόσιους και ιδιωτικούς φορείς, σε συνεργασία με τις κατά περίπτωση αρμόδιες αρχές και την Επιτροπή Συντονισμού για θέματα κυβερνοασφάλειας.

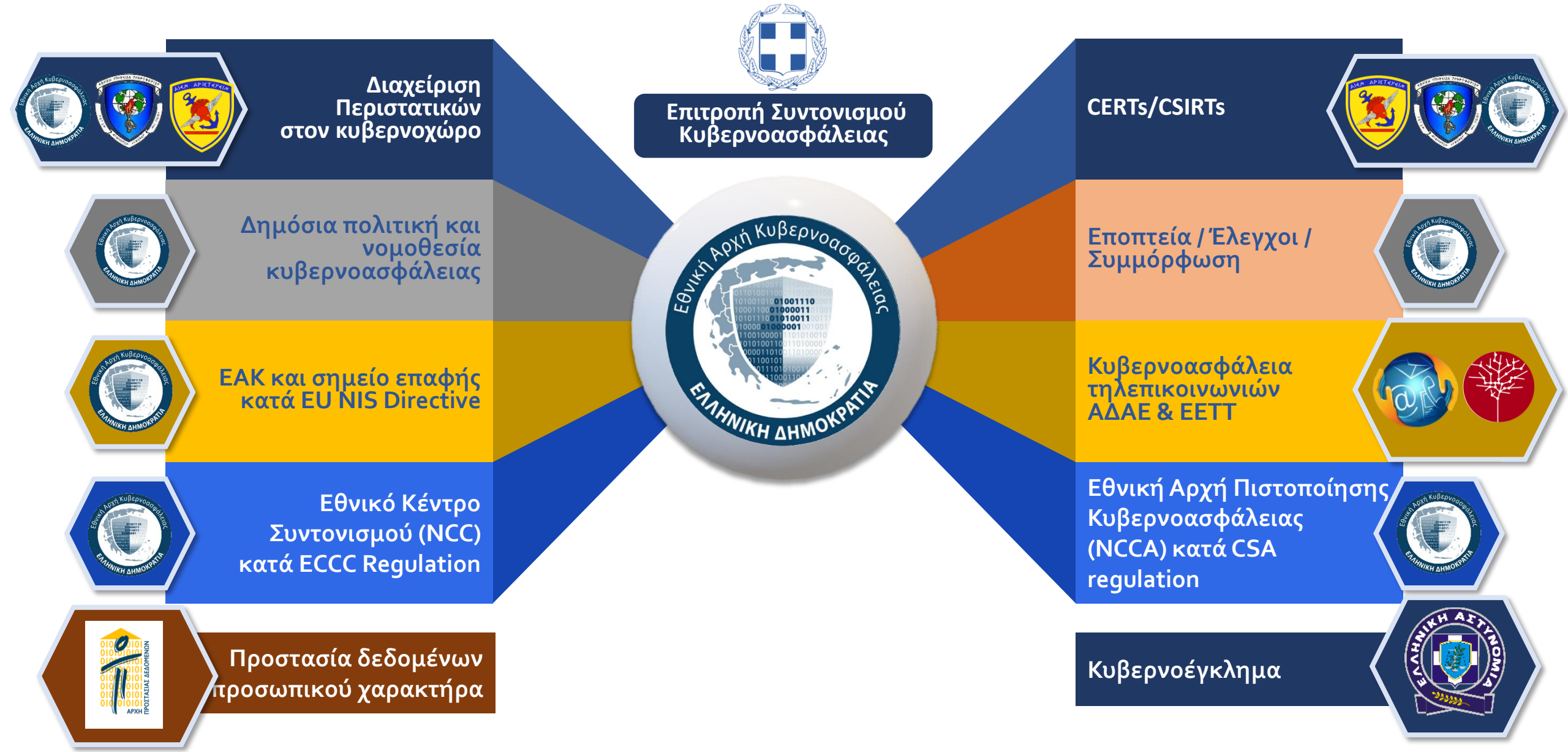
ιστ) Ενημερώνει, χωρίς καθυστέρηση, την Επιτροπή Συντονισμού για θέματα κυβερνοασφάλειας σε περίπτωση εξαιρετικού συμβάντος που ενέχει στρατηγικό κίνδυνο.

National Cyber Security Authority
N.5086/2024

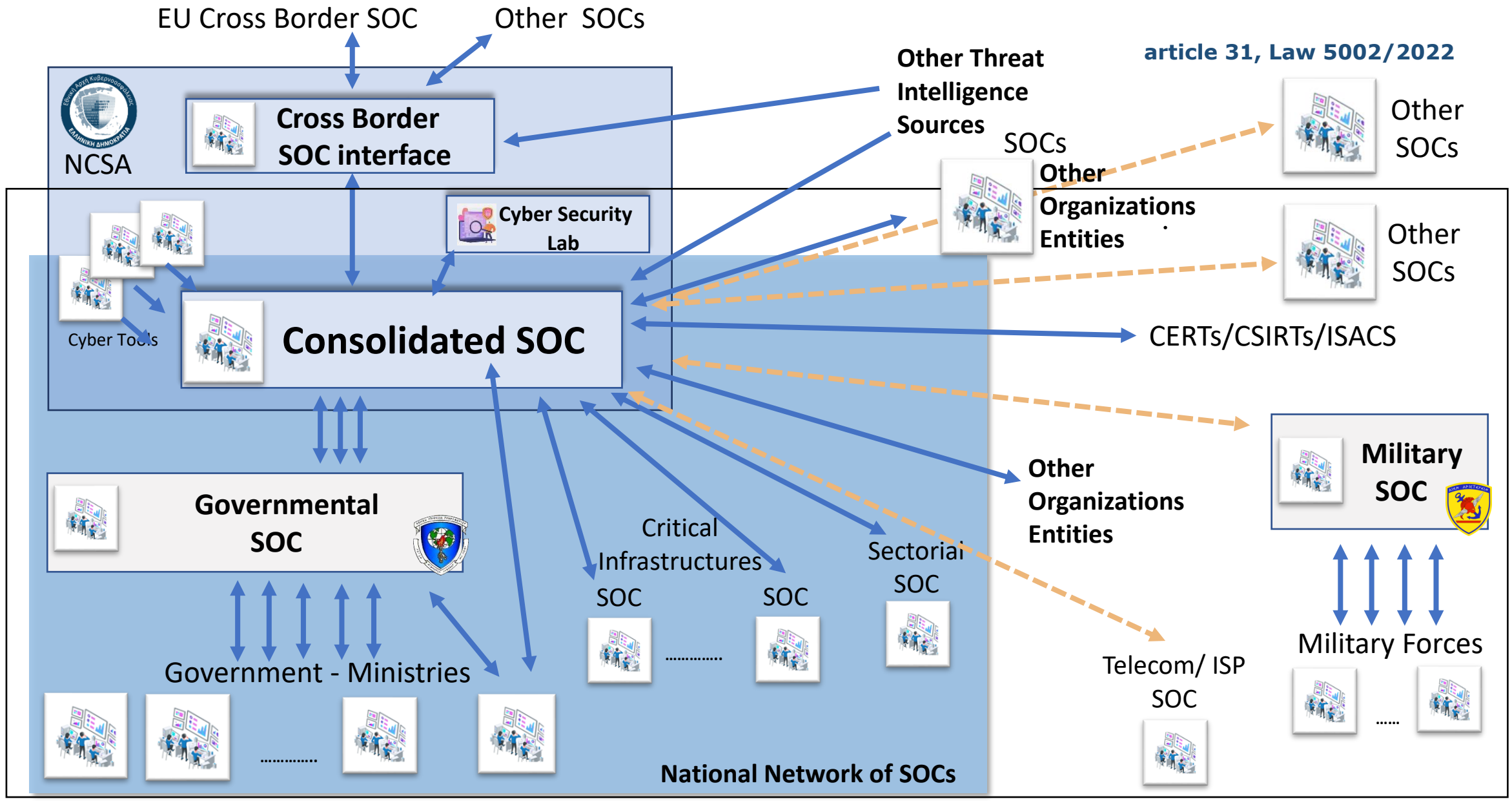
Άρθρο 10 - Οργάνωση και διάρθρωση

2. Στην Αρχή λειτουργούν
Κέντρο Επιχειρήσεων Κυβερνοασφάλειας (**Security Operations Centre**),
Ομάδα Απόκρισης Συμβάντων στον Κυβερνοχώρο (**CSIRT**), καθώς και
Εργαστήριο Αναλύσεων, Δοκιμών και Ερευνών (**Forensics & Testing Lab**).

Διακυβέρνηση κυβερνοασφάλειας στην Ελλάδα



Ενοποιημένο Κέντρο Αναφοράς Κυβερνοασφάλειας (SOC)
Εθνικό Δίκτυο SOCs

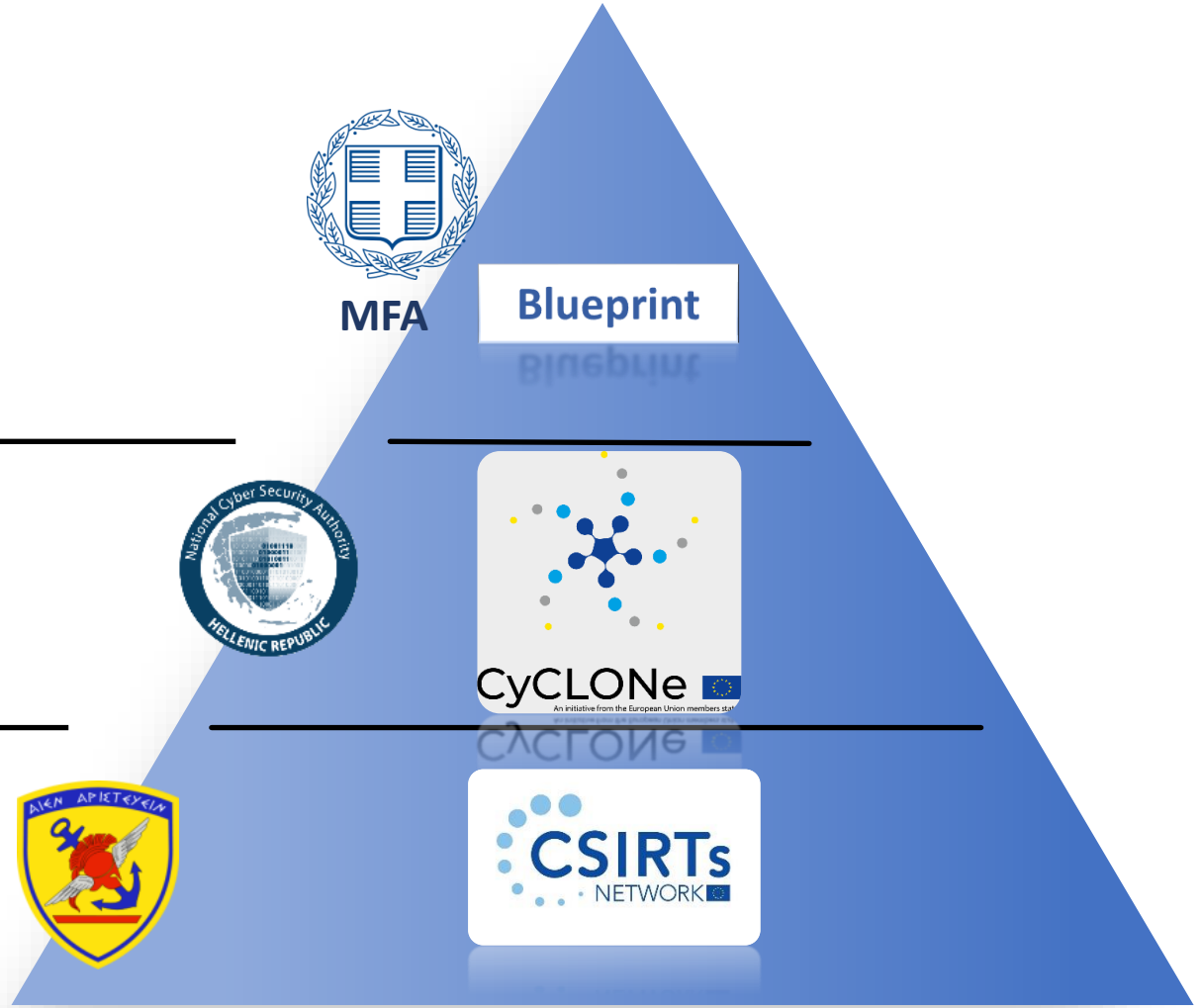


EU Coordinated Response to Large Scale Cyber Incidents

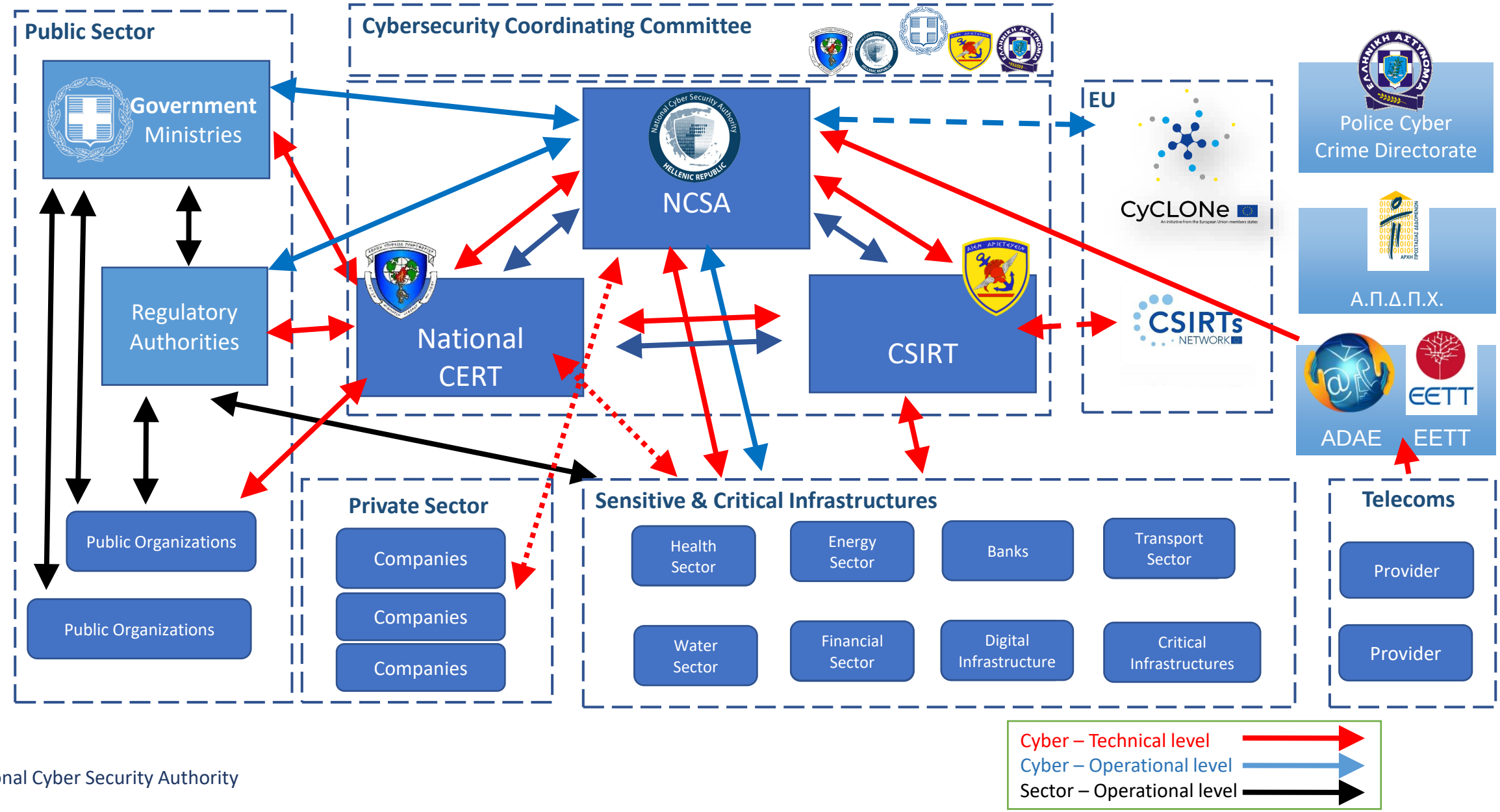
Political Level
Blueprint for coordinated response to major cyber-attacks

Operational Level
Cyber Crisis Liaison Organisation Network (CyCLONe)

Technical Level
CSIRTs Network



National Cybersecurity Incident Management



Cyber Threat Landscape

Threat Landscape
Incidents

Threat Landscape Overview

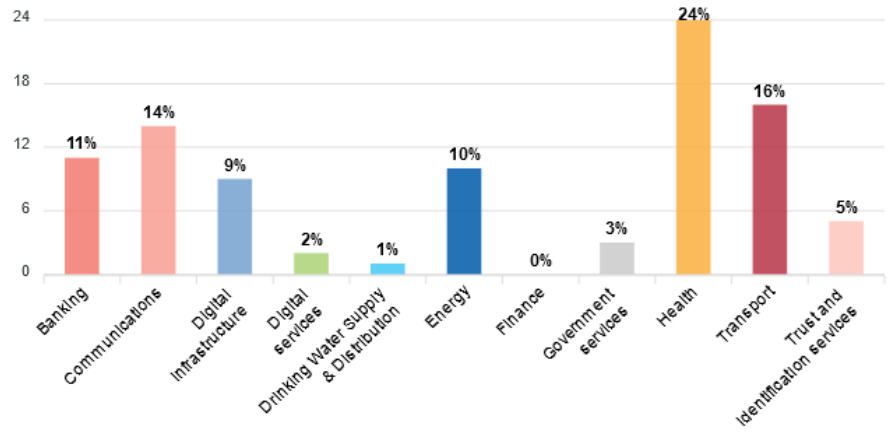
Overall | Trend

- [ ] All
- [x] Energy
- [x] Transport
- [x] Banking
- [x] Finance
- [x] Health
- [x] Drinking Water Supply & Distribution
- [x] Digital infrastructure
- [x] Communications
- [x] Trust and identification services
- [x] Digital services
- [x] Government services

2024	2023	2022	2021	2020	2019	2018	2017	2016	2015	2014	2013	2012
1	1268	1083	555	483	185	175	183	159	138	146	95	77
Reported incidents	Reported incidents	Reported incidents	Reported incidents	Reported incidents	Reported incidents	Reported incidents	Reported incidents	Reported incidents	Reported incidents	Reported incidents	Reported incidents	Reported incidents

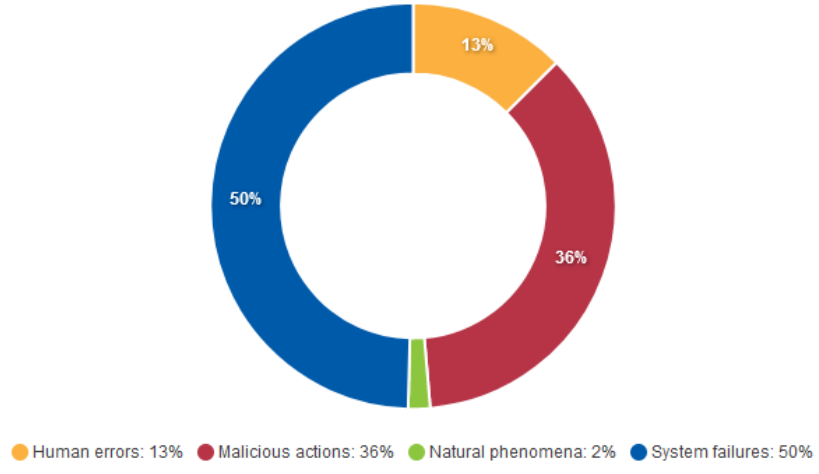
Year: 2023
№ Incidents: 1268 (100% of total)

Impact per sector



Year: 2023
№ Incidents: 1268 (100% of total)

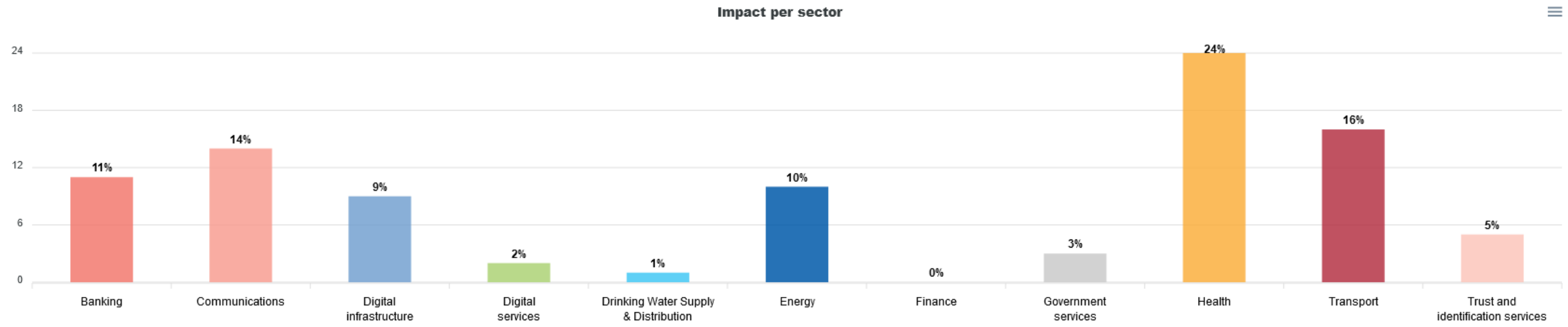
Nature of the incident



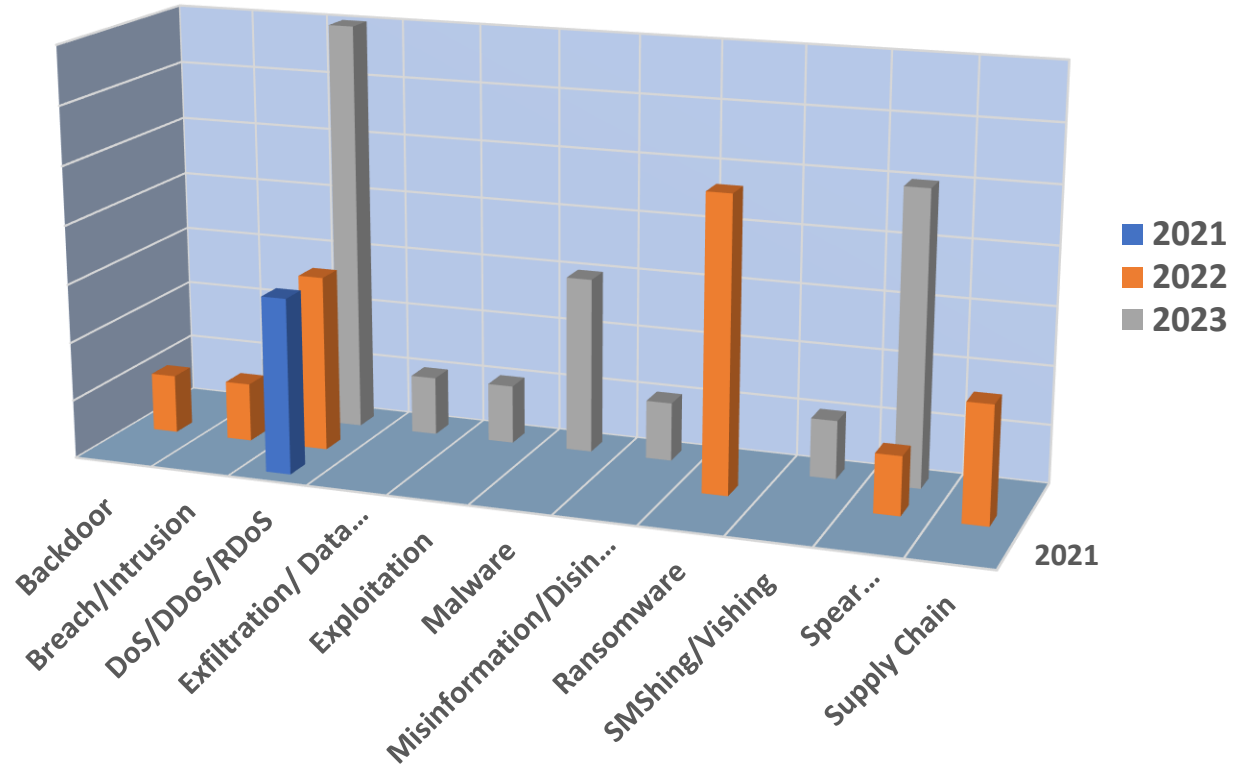
Overall / Trend	2024	2023	2022	2021	2020	2019	2018	2017	2016	2015	2014	2013	2012
EECC Article 40 Electronic communications (formerly Article 13a)	0 Reported incidents	156 Reported incidents	155 Reported incidents	168 Reported incidents	170 Reported incidents	153 Reported incidents	157 Reported incidents	169 Reported incidents	158 Reported incidents	138 Reported incidents	146 Reported incidents	95 Reported incidents	77 Reported incidents
EIDAS Article 19 Trust services	0 Reported incidents	63 Reported incidents	35 Reported incidents	45 Reported incidents	36 Reported incidents	32 Reported incidents	18 Reported incidents	14 Reported incidents	1 Reported incidents	0 Reported incidents	0 Reported incidents	0 Reported incidents	0 Reported incidents
EIDAS Article 10 e-ID systems	1 Reported incidents	0 Reported incidents	0 Reported incidents	0 Reported incidents	0 Reported incidents	0 Reported incidents	0 Reported incidents	0 Reported incidents	0 Reported incidents	0 Reported incidents	0 Reported incidents	0 Reported incidents	0 Reported incidents
NISD Article 14 and 16 Essential and Digital services	0 Reported incidents	1049 Reported incidents	880 Reported incidents	341 Reported incidents	283 Reported incidents	0 Reported incidents	0 Reported incidents	0 Reported incidents	0 Reported incidents	0 Reported incidents	0 Reported incidents	0 Reported incidents	0 Reported incidents

Impact per sector

Year: 2023
№ Incidents: 1268 (100% of total)



Cyber incidents in Hellenic CRITICAL INFRASTRUCTURE (last 3 years)

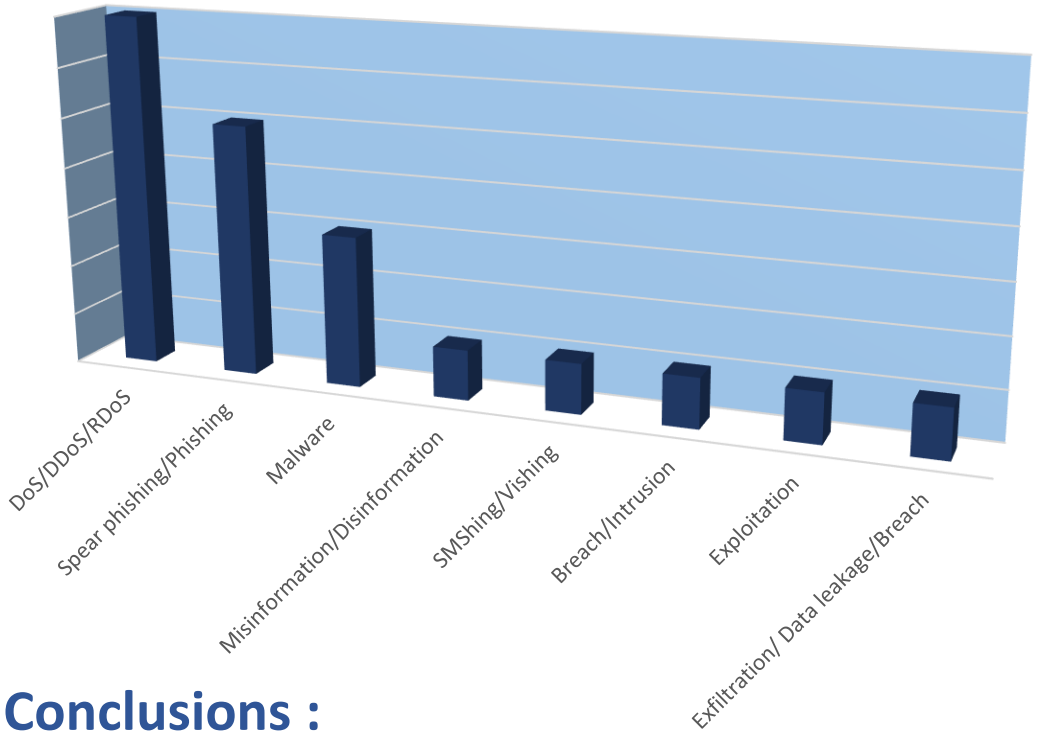


Characteristics and trends:

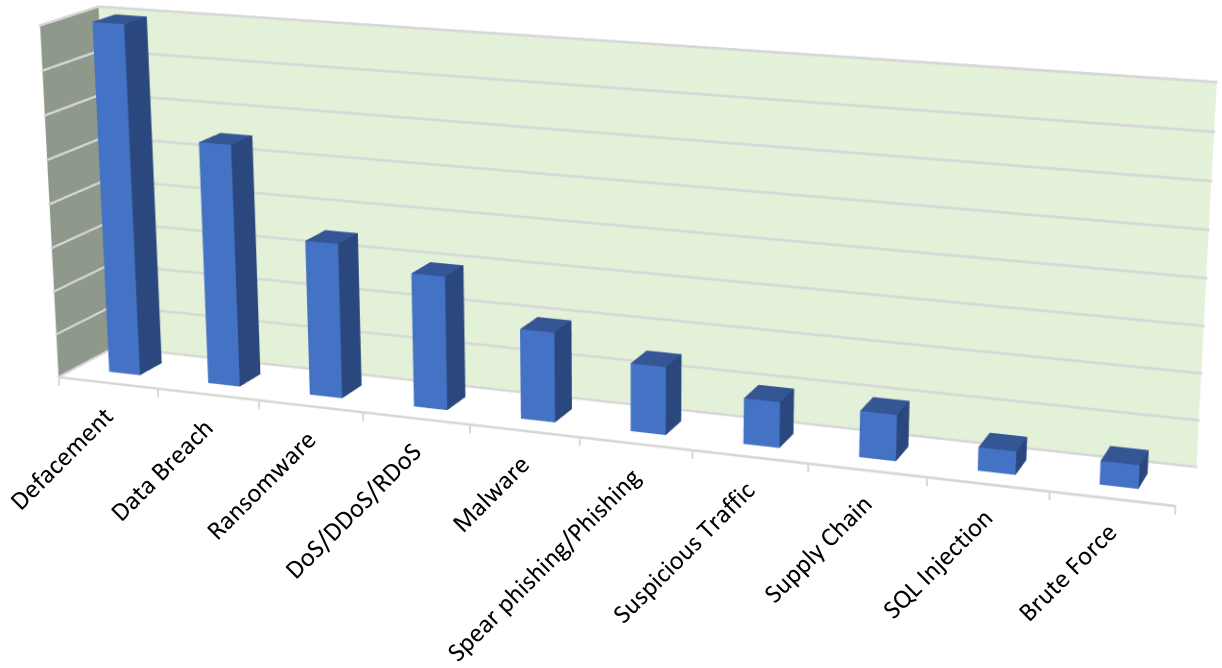
- ✓ 2022 reported incidents were **quadrupled** compared to 2021 incidents
- ✓ The **energy sector** was at the center of cyber attacks in 2022, due to geopolitical instability
- ✓ 2023 reported incidents are **almost doubled** compared to 2023 incidents
- ✓ The **transportation sector** is at the center of cyber attacks in 2023

Cyber incidents in Critical Infrastructure & Public Sector (2023)

Critical Infrastructure incidents (NCSA)



Public Sector Incidents (National CERT)



Conclusions :

- ✓ Double reported incidents in the public sector than in the critical infrastructures for the current year
- ✓ **DDOS, Phishing and Malware** most common in **Critical Infrastructures**
- ✓ **Defacements, Data Breach and Ransomware** most common in the **Hellenic Public Sector**

NIS2

EU Directive for Networks and Information Systems

Security Measures

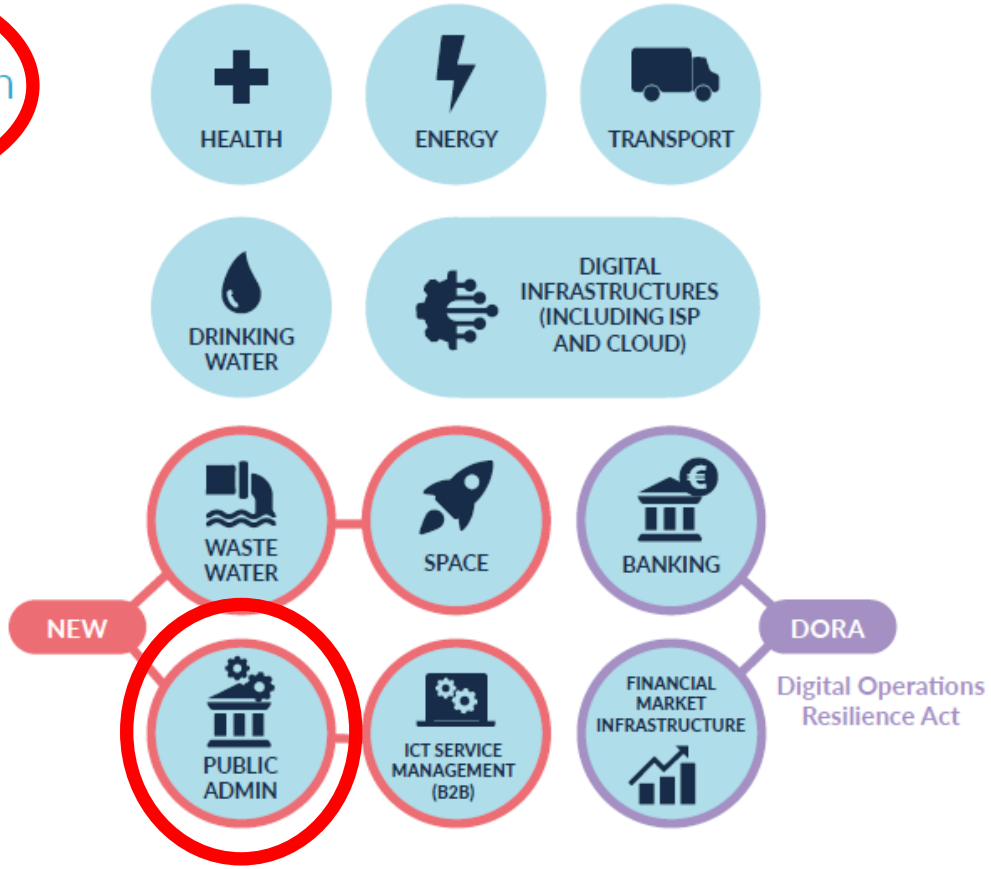
Η Οδηγία 2022/2555 (NIS 2)

Εισαγωγικές παρατηρήσεις

- Σημαντική ενίσχυση απαιτήσεων για:
  - Τις αρμόδιες Εθνικές Αρχές
  - Τους υπόχρεους Οργανισμούς
    - Υποχρεώσεις λήψης μέτρων
    - Υποχρεώσεις αναφοράς περιστατικών
- Σημαντική ενδυνάμωση του πλαισίου ελέγχων, εποπτείας και επιβολής
  - Βασικές οντότητες: ex ante & ex post έλεγχοι
  - Σημαντικές οντότητες: μόνο ex post έλεγχοι
- Έμφαση στην ανταλλαγή πληροφοριών και την επικοινωνία μεταξύ Οργανισμών και Εθνικών Αρχών, καθώς και διευρωπαϊκής συνεργασίας
- Εφαρμογή: 18 Οκτωβρίου 2024

NIS2 - Sectors

Annex 1 - Sectors of High Criticality



Annex 2 - Other Critical Sectors

NIS2 - Security Measures

1. Top Management Commitment and Accountability (Δέσμευση και Υπευθυνότητα της ανώτατης διοίκησης)
2. Network and information security policy (Πολιτική ασφάλειας δικτύων και πληροφοριών)
3. Risk management Policy (Πολιτική διαχείρισης κινδύνων)
4. Asset Management (Διαχείριση περιουσιακών στοιχείων)
5. Human Resources Security (Ασφάλεια Ανθρώπινου Δυναμικού)
6. Basic cyber hygiene practices and security training (Βασικές πρακτικές υγιεινής στον κυβερνοχώρο και εκπαίδευση ασφάλειας)
7. Access Control (Έλεγχος πρόσβασης)
8. Supply Chain Security (Ασφάλεια Εφοδιαστικής Αλυσίδας)
9. Security in network and information systems acquisition, development, and maintenance (Ασφάλεια δικτύου και απόκτηση, ανάπτυξη και συντήρηση πληροφοριακών συστημάτων)
10. Cryptography (Κρυπτογράφηση)
11. Incident Handling (Χειρισμός Περιστατικών)
12. Business Continuity and crisis management (Επιχειρησιακή συνέχεια και διαχείριση κρίσεων)
13. Environmental and physical security (Περιβαλλοντική και φυσική ασφάλεια)

❖ Cyber hygiene measures

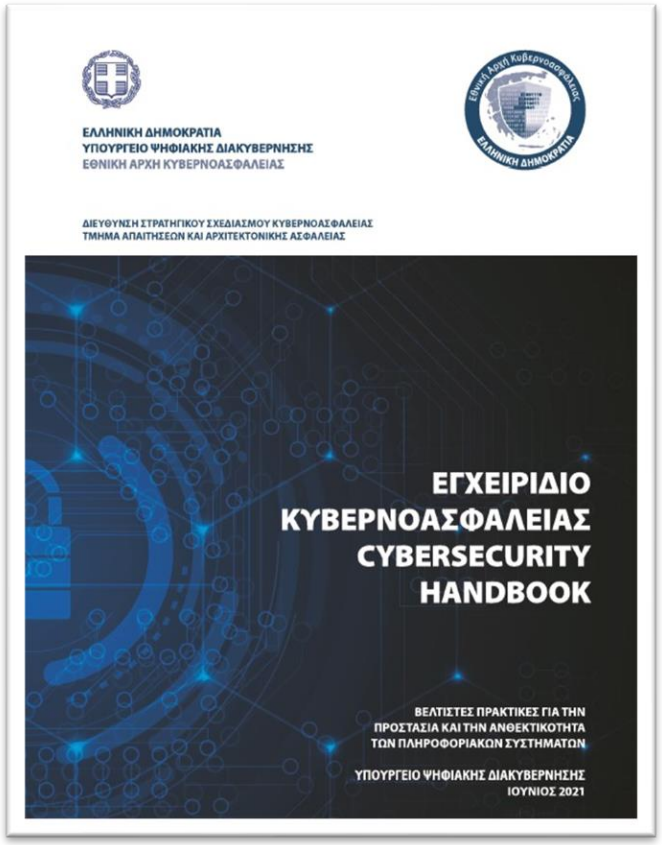
National Cyber Security Authority

Tools

Platforms

National Cyber Security Authority

Cybersecurity Handbook



7. Προστασία από κακόβουλο λογισμικό

Υλοποιείστε τεχνολογίες που ανιχνεύουν και εμποδίζουν την εγκατάσταση, εκτέλεση και μετάδοση κακόβουλου λογισμικού ή εντολών στις συσκευές και στο δίκτυο του Οργανισμού.

Ποιοι είναι οι κίνδυνοι;

Το κακόβουλο λογισμικό συνιστά μία από τις βασικότερες απειλές για τα πληροφοριακά συστήματα και οι κίνδυνοι που απορρέουν από τη δράση του είναι πολυποίκιλοι:

- κλοπή κωδικών πρόσβασης,
- κλοπή δεδομένων,
- εντοπισμός πρόσβετων στόχων εντός του δικτύου,
- κρυπτογράφηση και αλλοίωση δεδομένων.

Ο κακόβουλος κώδικας μπορεί να μολύνει τα συστήματα με διάφορους τρόπους, συμπεριλαμβανομένων του email, μολυσμένων ιστοσελίδων και φορητών μέσων αποθήκευσης (USB, εξωτερικοί σκληροί δίσκοι). Η εξάπλωσή του στηρίζεται σε ευπάθειες στα συστήματα αλλά και σε απρόσεκτη συμπεριφορά του τελικού χρήστη, όπως είναι το άνοιγμα συνημμένων αρχείων και συνδέσεων (links), η εγκατάσταση προγραμμάτων και η εισαγωγή μολυσμένου USB. Προκειμένου το κακόβουλο λογισμικό να ανιχνευθεί και να αφαιρεθεί, οι μηχανισμοί προστασίας θα πρέπει να εφαρμοστούν σε όλα τα σημεία εισόδου και εξόδου των συστημάτων (σταθμοί εργασίας, web servers, mail servers, proxy servers, remote access servers, firewalls).

Μέτρα προστασίας (sub-controls)
7.1 Αναπτύξτε και καταγράψτε: - πολιτική προστασίας από κακόβουλο λογισμικό, που θα περιγράφει σκοπό, πεδίο εφαρμογής, ρόλους και ευθύνες, - διαδικασίες υλοποίησης της πολιτικής και των σχετικών μέτρων προστασίας.
7.2 Υλοποιείστε λογισμικό προστασίας από κακόβουλα προγράμματα (anti-malware software) σε κάθε σταθμό εργασίας και server, το οποίο θα λειτουργεί με αυτοματοποιημένο τρόπο μέσω κεντρικής διαχείρισης. Το λογισμικό θα ώρα συνεχώς, ενώ η βάση δεδομένων των υπογραφών του (signature database) θα ενημερώνεται σε τακτική βάση.
7.3 Ρυθμίστε ώστε να διενεργείται αυτόματη σάρωση για κακόβουλο λογισμικό (anti-malware scanning) σε φορητά μέσα αποθήκευσης (USB, εξωτερικούς σκληρούς δίσκους, CD, DVD), όταν αυτά συνδέονται σε συσκευές.
7.4 Διασφαλίστε ότι οι εκδόσεις των web browsers και e-mail clients που είναι εγκατεστημένοι στα συστήματα του Οργανισμού είναι οι πλέον πρόσφατες, ενημερώνονται αυτόματα και είναι πλήρως υποστηριζόμενες.
7.5 Προβείτε σε απενεργοποίηση ή απεγκατάσταση κάθε μη εγκεκριμένου plug-in ή add-on σε web browsers και e-mail clients.
7.6 Χρησιμοποιείστε την υπηρεσία DNS filtering για την παρεμπόδιση πρόσβασης σε γνωστά κακόβουλα domains.

7.7 Επιβάλλετε φιλτράρισμα του URL σε επίπεδο δικτύου για να περιοριστεί η δυνατότητα σύνδεσης σε ιστοσελίδες μη εγκεκριμένες από την πολιτική ασφαλείας του Οργανισμού.

7.8 Εφαρμόστε την τεχνική φιλτραρίσματος περιεχομένου (content filtering) για τον έλεγχο των κακόβουλων εισερχόμενων e-mails.

7.9 Εγκαταστήστε συστήματα ανίχνευσης και πρόληψης εισβολών (host-based intrusion detection / prevention systems) σε κάθε server κρίσιμης σημασίας (web, email, DNS κ.α.).

7.10 Εγκαταστήστε συστήματα ανίχνευσης και πρόληψης εισβολών (host-based intrusion detection / prevention systems) σε κάθε σταθμό εργασίας.

Σχήμα 7

Παράδειγμα μόλυνσης και διασποράς κακόβουλου λογισμικού

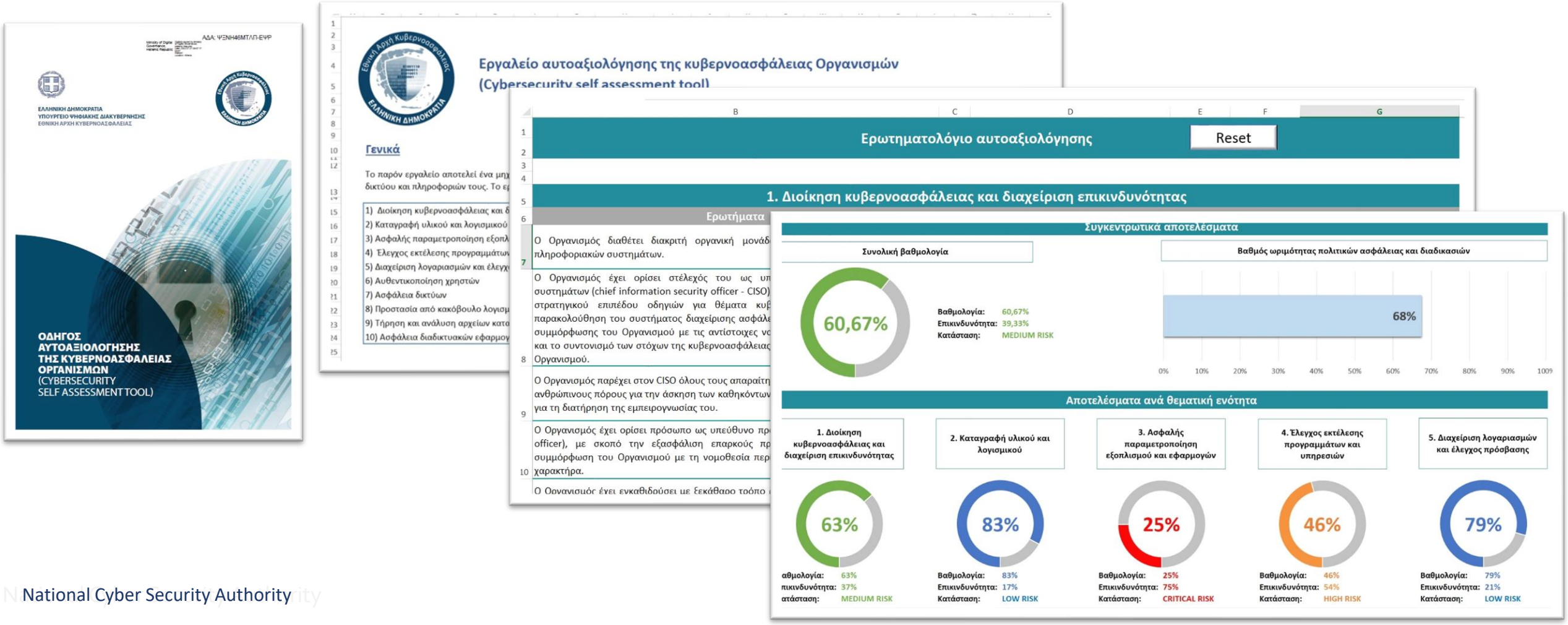
Πηγή: https://www.spambrella.com/what-is-emotet-malware-and-how-is-it-delivered/

Στο σχήμα απεικονίζεται μία από τις παραλλαγές του Emotet, ενός από τα πλέον επικίνδυνα malware των τελευταίων ετών που η δράση του διέκοπη μόλις πρόσφατα[13]. Αφού μολύνει τον υπολογιστή του θύματος, το Emotet κλέβει συνθηματικά που είναι αποθηκευμένα στο σύστημα και στον browser του χρήστη, ενώ από τον κατάλογο των επαφών του Outlook λογαριασμού του συλλέγει ονόματα και emails για να στείλει νέα spam emails. Εκτός από τα παραπάνω, το Emotet κατεβάζει στον υπολογιστή του θύματος και άλλα malware, κυρίως banking trojans που έχουν στόχο την κλοπή των κωδικών πρόσβασης στο web banking. Είναι χαρακτηριστικό ότι στις περισσότερες των περιπτώσεων η αρχική μόλυνση ξεκινά χάρη σε ένα απλό κλικ που έκανε το θύμα για να ανοίξει ένα κακόβουλο word αρχείο που εστάλη μέσω email. Εδώ φαίνεται πόσο σημαντική είναι η εκπαίδευση και ευαισθητοποίηση των χρηστών σε βασικά θέματα κυβερνοασφάλειας, όπως είναι οι επιθέσεις κοινωνικής μηχανικής μέσω phishing emails.

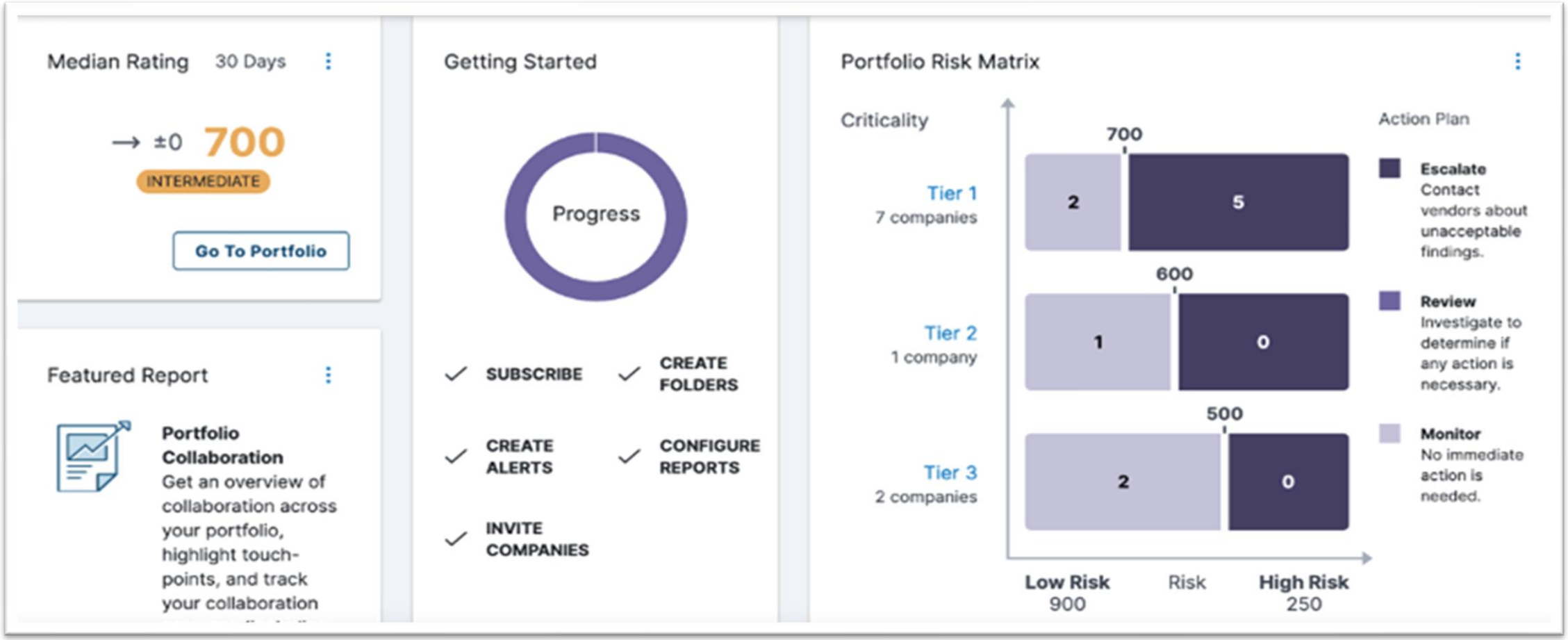
13 βλ. https://www.europol.europa.eu/newsroom/news/worldwide-takedown-hits-most-dangerous-malware-emotet-disrupted-through-global-action

National Cyber Security Authority

Cybersecurity Self-Assessment Tool

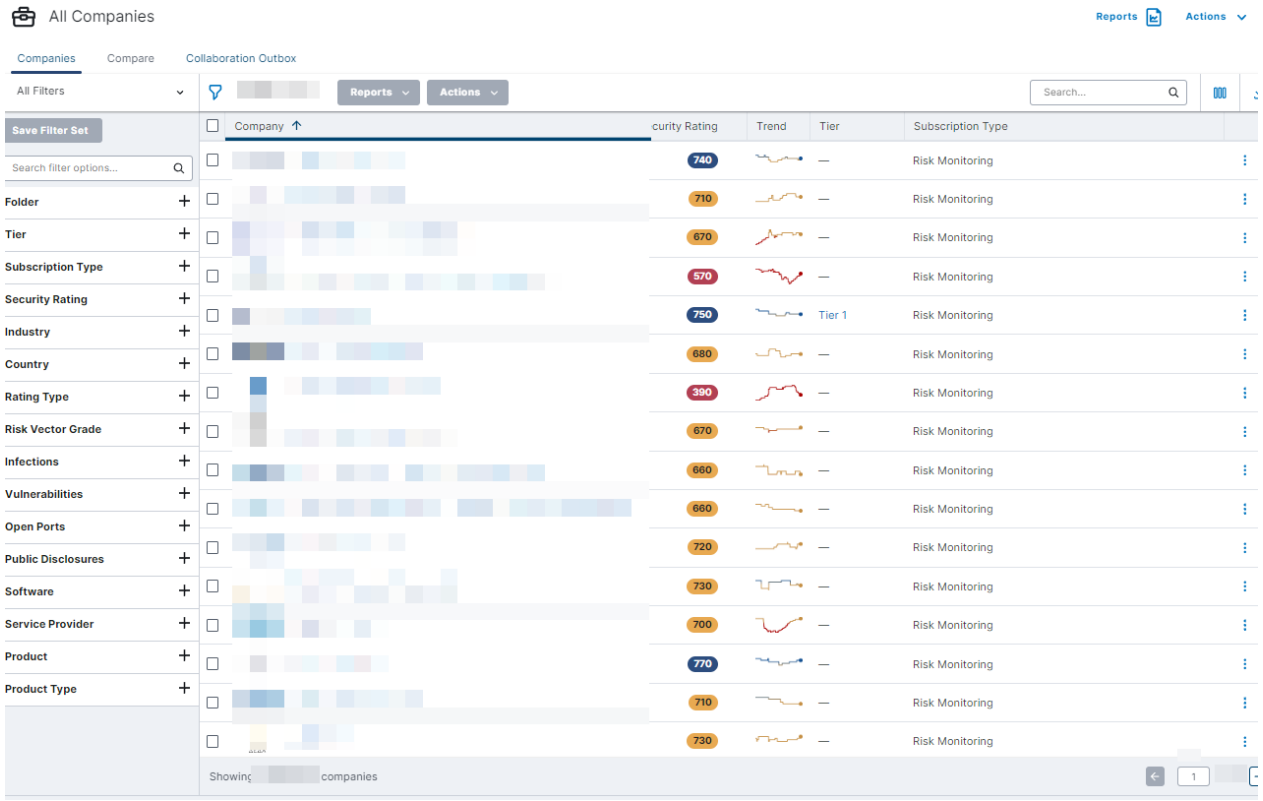


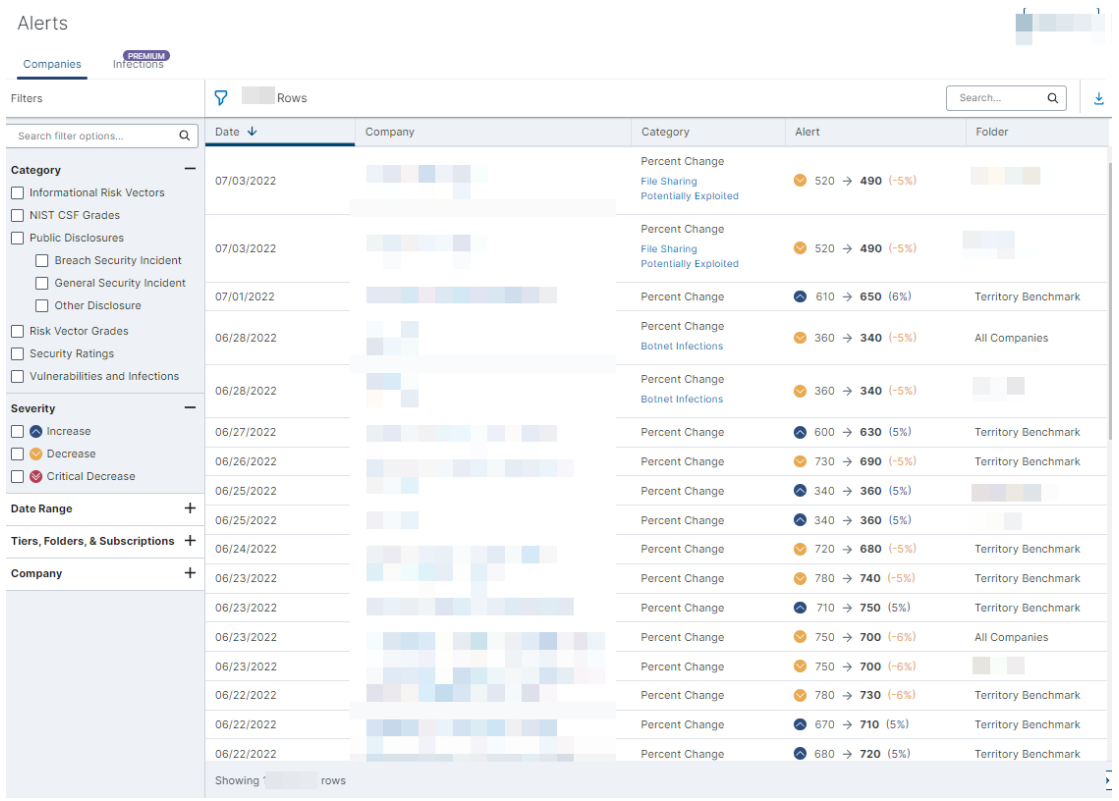
National Cyber Security Authority
Πλατφόρμα Αξιολόγησης Επιπέδου Κυβερνοασφάλειας



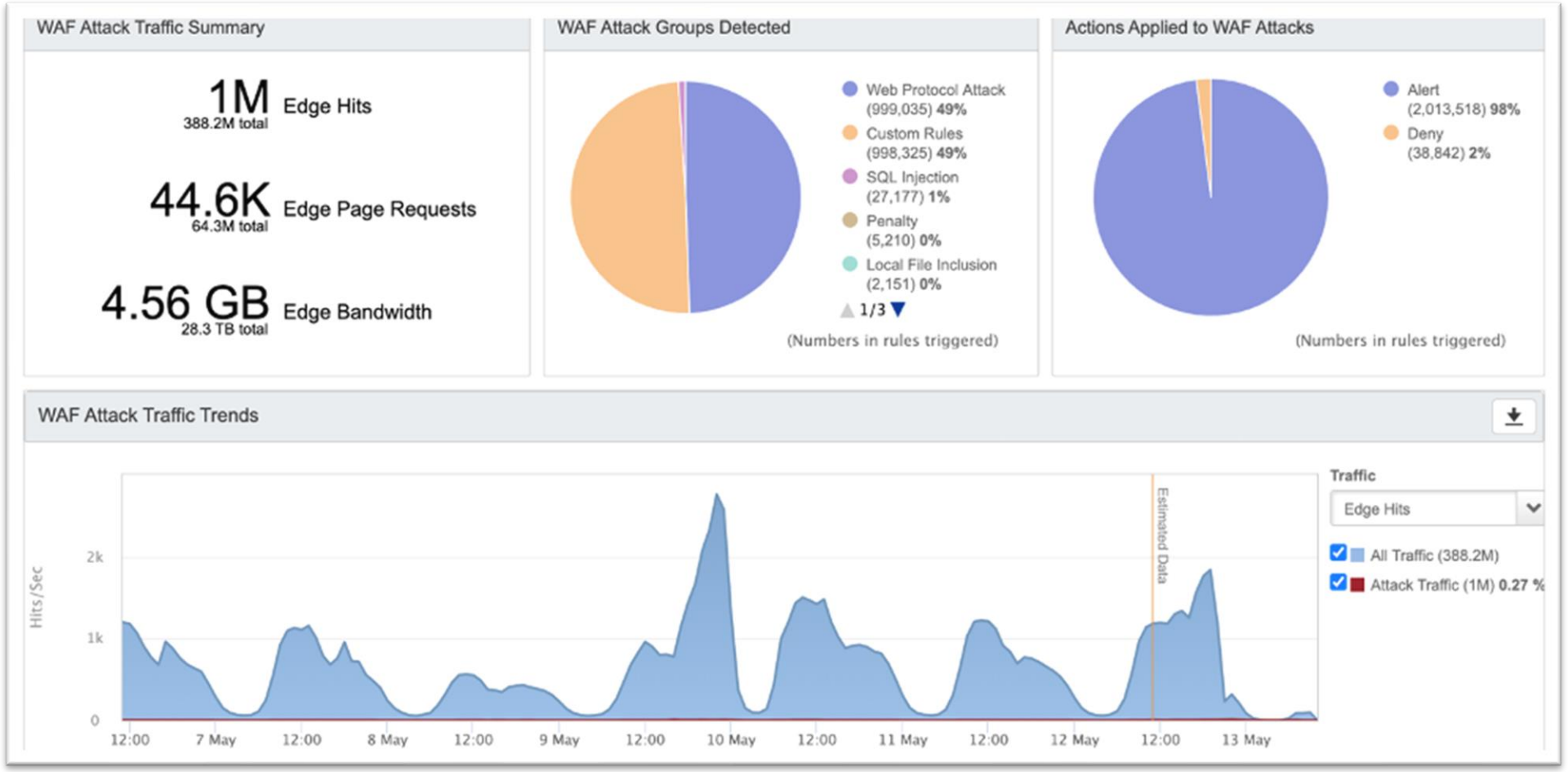
National Cyber Security Authority

Πλατφόρμα Αξιολόγησης Επιπέδου Κυβερνοασφάλειας

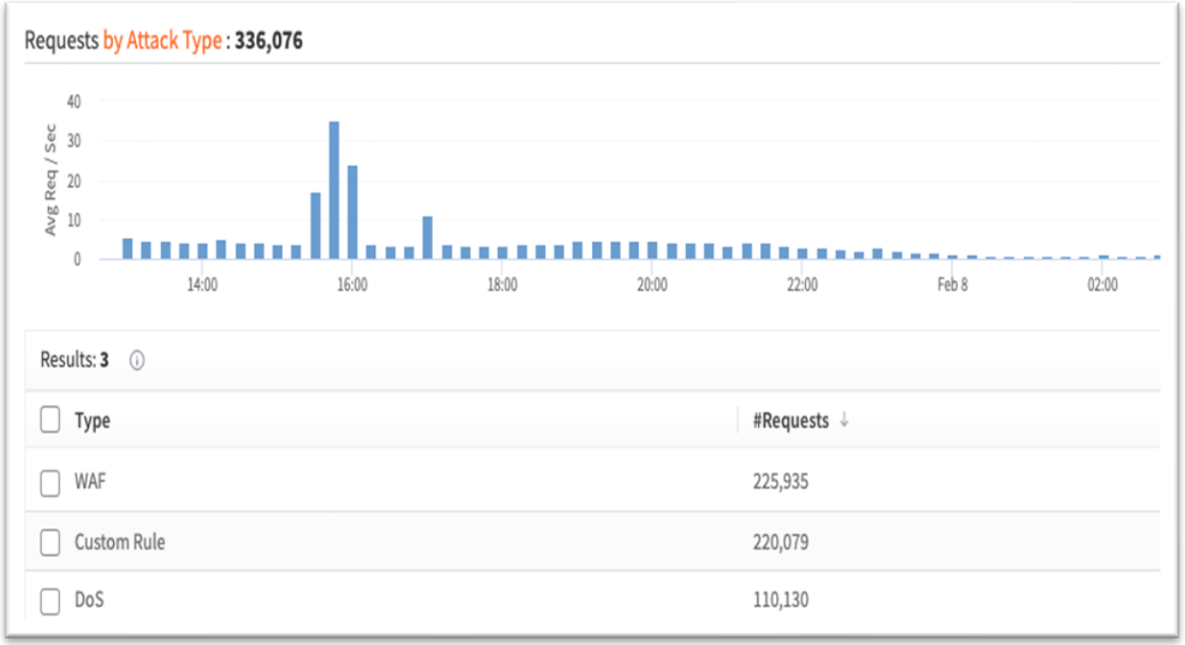


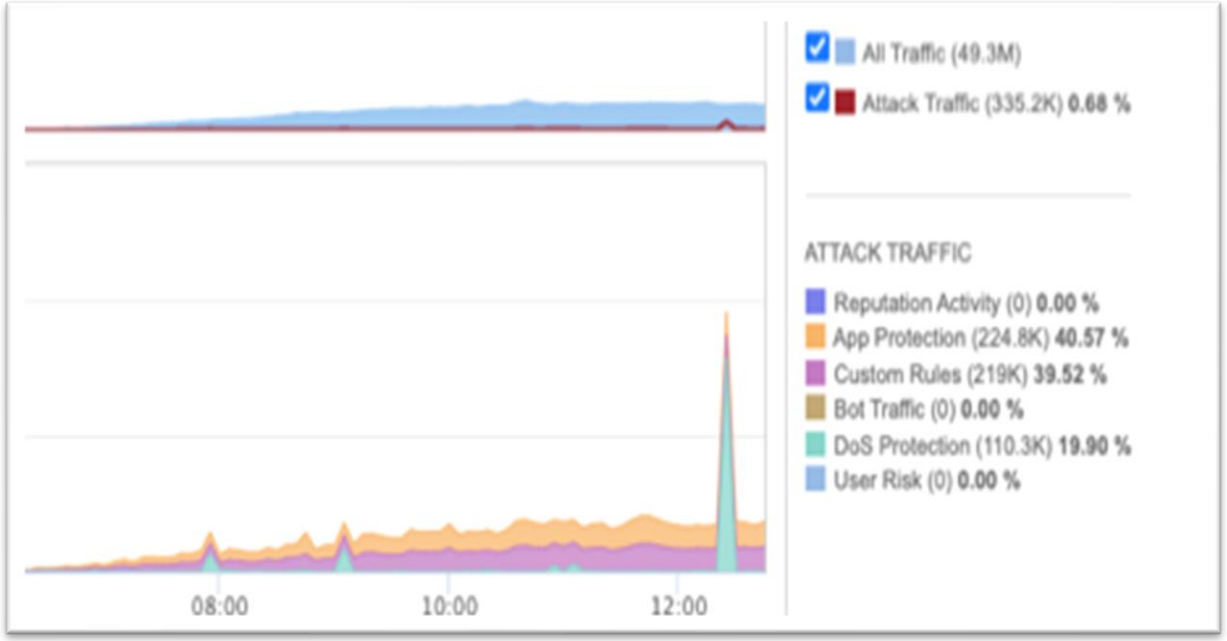


National Cyber Security Authority
Κυβερνητική Υπηρεσία Προστασίας Ιστοσελίδων

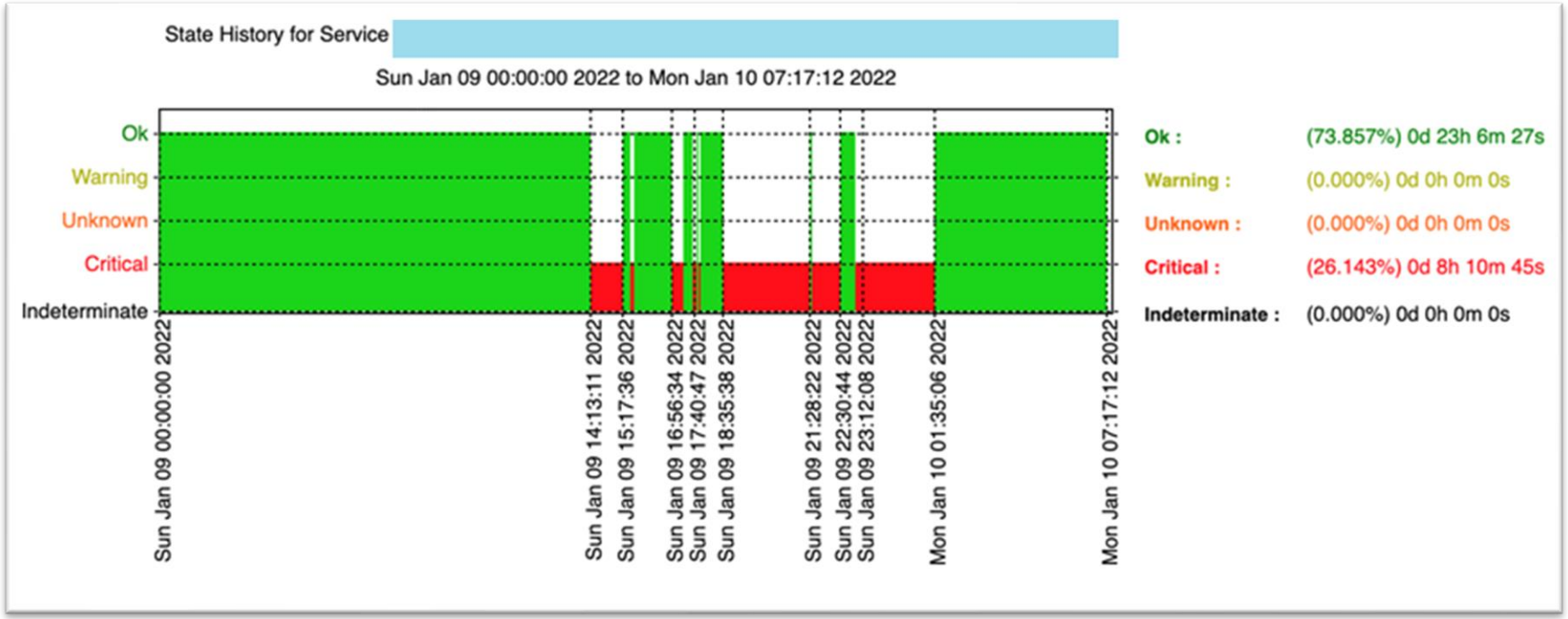


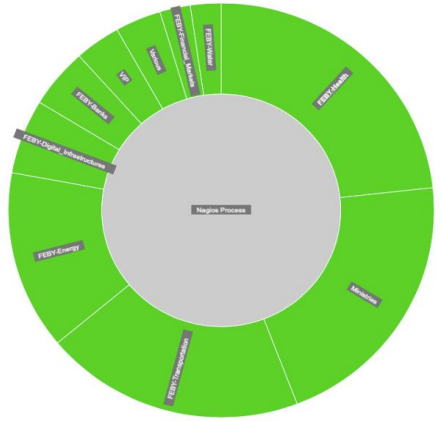
National Cyber Security Authority
Κυβερνητική Υπηρεσία Προστασίας Ιστοσελίδων





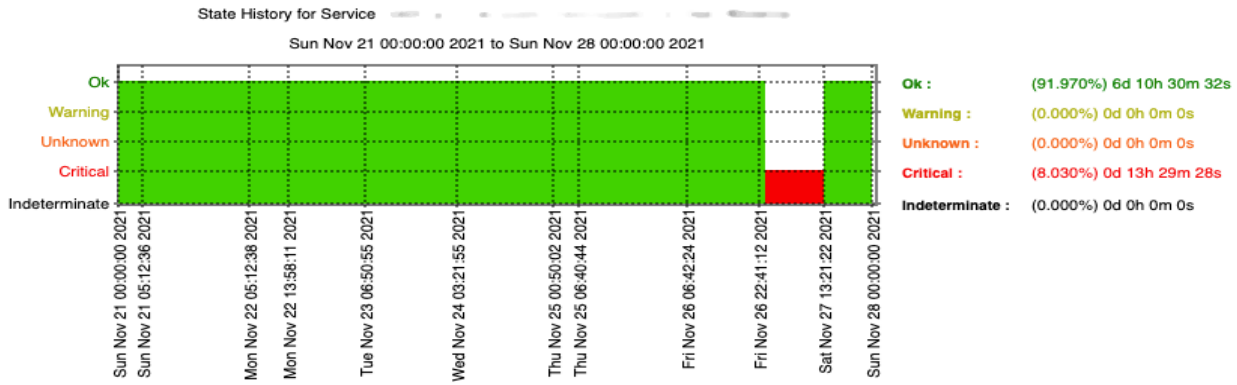
National Cyber Security Authority
Σύστημα επίβλεψης διαθεσιμότητας ιστοτόπων

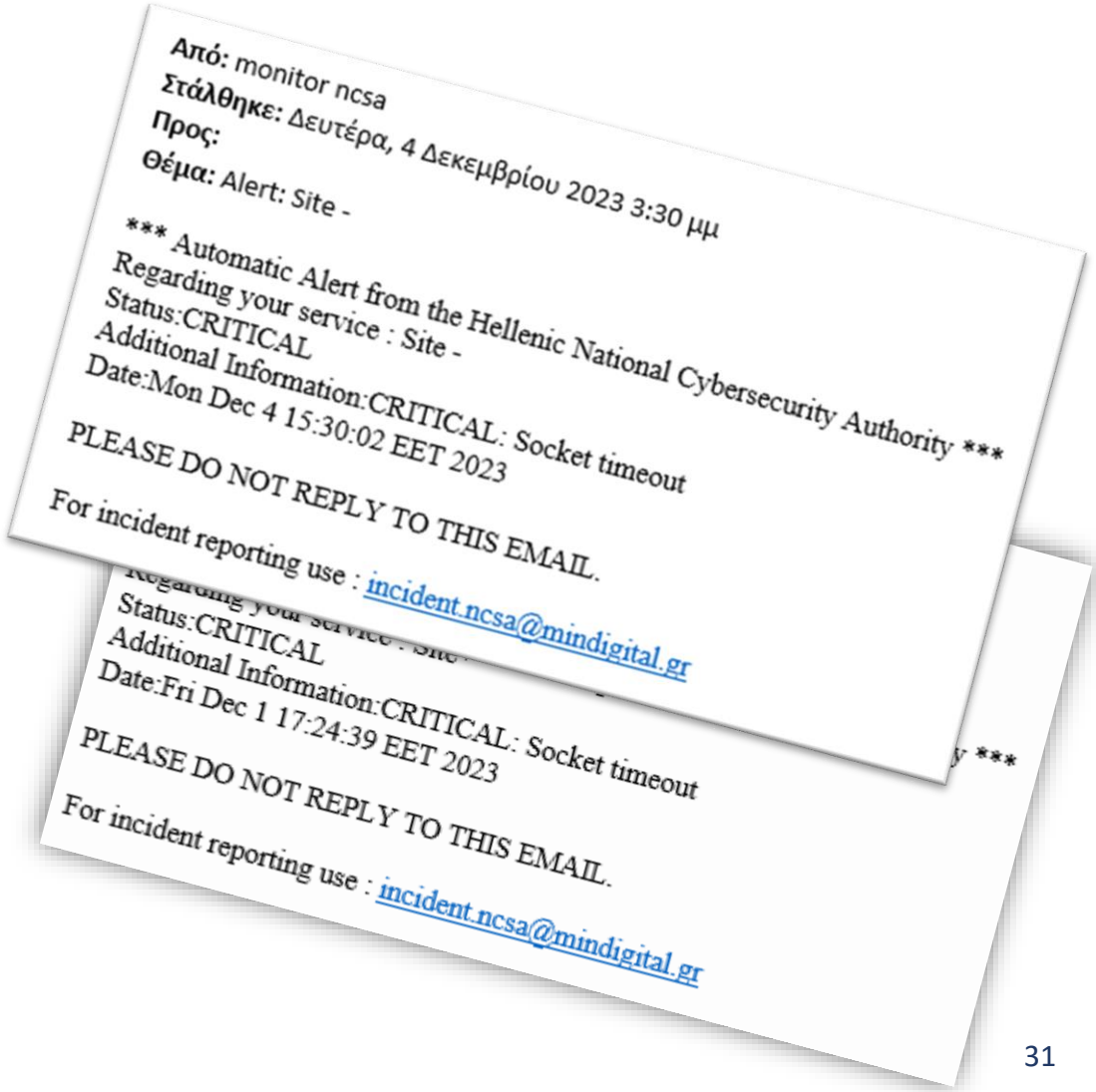




National Cyber Security Authority
Σύστημα επίβλεψης διαθεσιμότητας ιστοτόπων

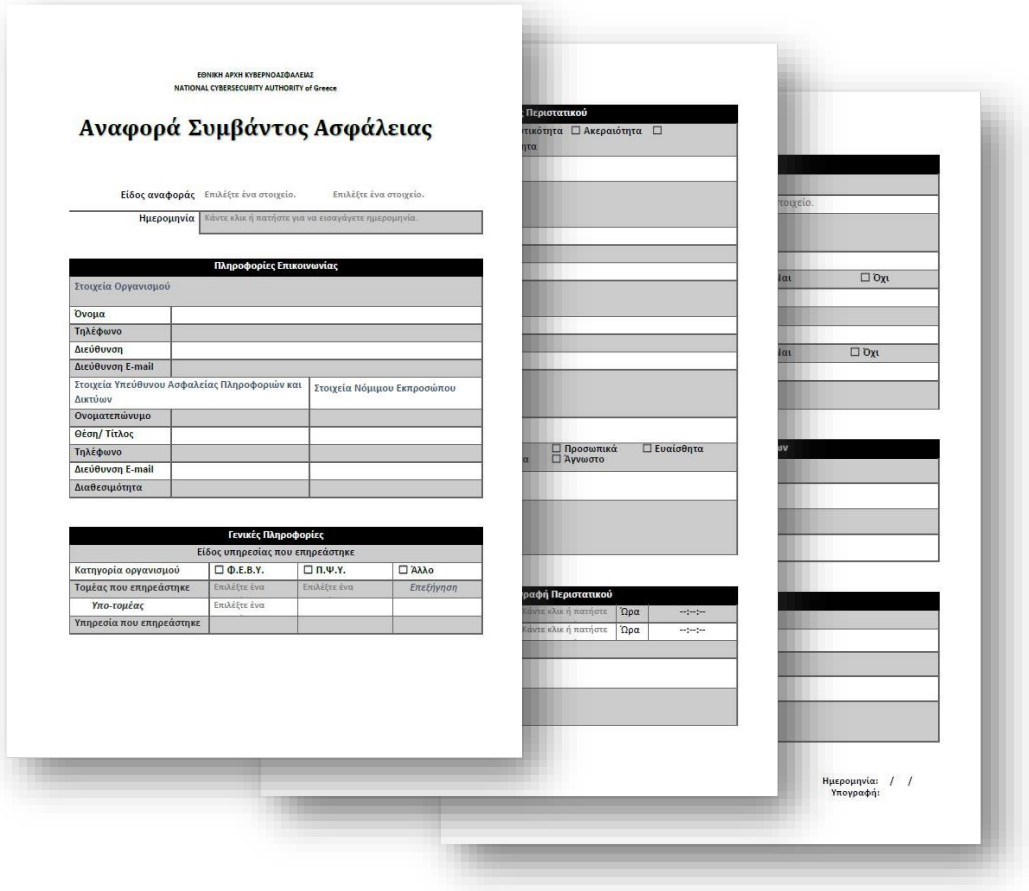
Host	Service	Status
Ministries	[redacted]	CRITICAL
FEBY-	[redacted]	OK
	[redacted]	OK
	[redacted]	OK
	[redacted]	OK
FEBY-	[redacted]	OK
	[redacted]	OK
	[redacted]	OK
	[redacted]	OK
	[redacted]	OK





National Cyber Security Authority
Incident Reporting

incident.ncsa@mindigital.gr


ΕΘΝΙΚΗ ΑΡΧΗ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ
NATIONAL CYBERSECURITY AUTHORITY of Greece

Αναφορά Συμβάντος Ασφάλειας

Είδος αναφοράς Επιλέξτε ένα στοιχείο. Επιλέξτε ένα στοιχείο.

Ημερομηνία Κάντε κλικ ή πατήστε για να εισαγάγετε ημερομηνία.

Πληροφορίες Επικοινωνίας		
Στοιχεία Οργανισμού		
Όνομα		
Τηλέφωνο		
Διεύθυνση		
Διεύθυνση E-mail		
Στοιχεία Υπεύθυνου Ασφαλείας Πληροφοριών και Δικτύων		Στοιχεία Νόμιμου Εκπροσώπου
Ονοματεπώνυμο		
Θέση/ Τίτλος		
Τηλέφωνο		
Διεύθυνση E-mail		
Διαθεσιμότητα		

Γενικές Πληροφορίες			
Είδος υπηρεσίας που επηρεάστηκε			
Κατηγορία οργανισμού	☐ Φ.Ε.Β.Υ.	☐ Π.Ψ.Υ.	☐ Άλλο
Τομέας που επηρεάστηκε	Επιλέξτε ένα	Επιλέξτε ένα	Επεξήγηση
Υπο-τομέας	Επιλέξτε ένα		
Υπηρεσία που επηρεάστηκε			

Περιστατικού
☐ Ακεραιότητα ☐
☐ Προσωπικά ☐ Ευαίσθητα ☐ Άγνωστο
☐ Όχι
☐ Όχι
Περιστατικού
Ώρα --:--:--
Ώρα --:--:--
Ημερομηνία: / /
Υπογραφή:

Thomas Dompridis

General Director of Operational Planning
National Cyber Security Authority
Ministry of Digital Governance

t.dompridis@mindigital.gr

https://mindigital.gr/kyvernoasfaleia