Τα πρότυπα ως εργαλεία για την θωράκιση των κρίσιμων υποδομών πληροφοριών

Αρχή Ψηφιακής Ασφάλειας (ΑΨΑ)

Αντρέας Ιακώβου, Επικεφαλής CSIRT-CY
Αρχή Ψηφιακής Ασφάλειας
https://dsa.cy | https://csirt.cy

ΕΠΙΤΡΟΠΟΣ ΕΠΙΚΟΙΝΩΝΙΩΝ

Αρχή Ψηφιακής Ασφάλειας

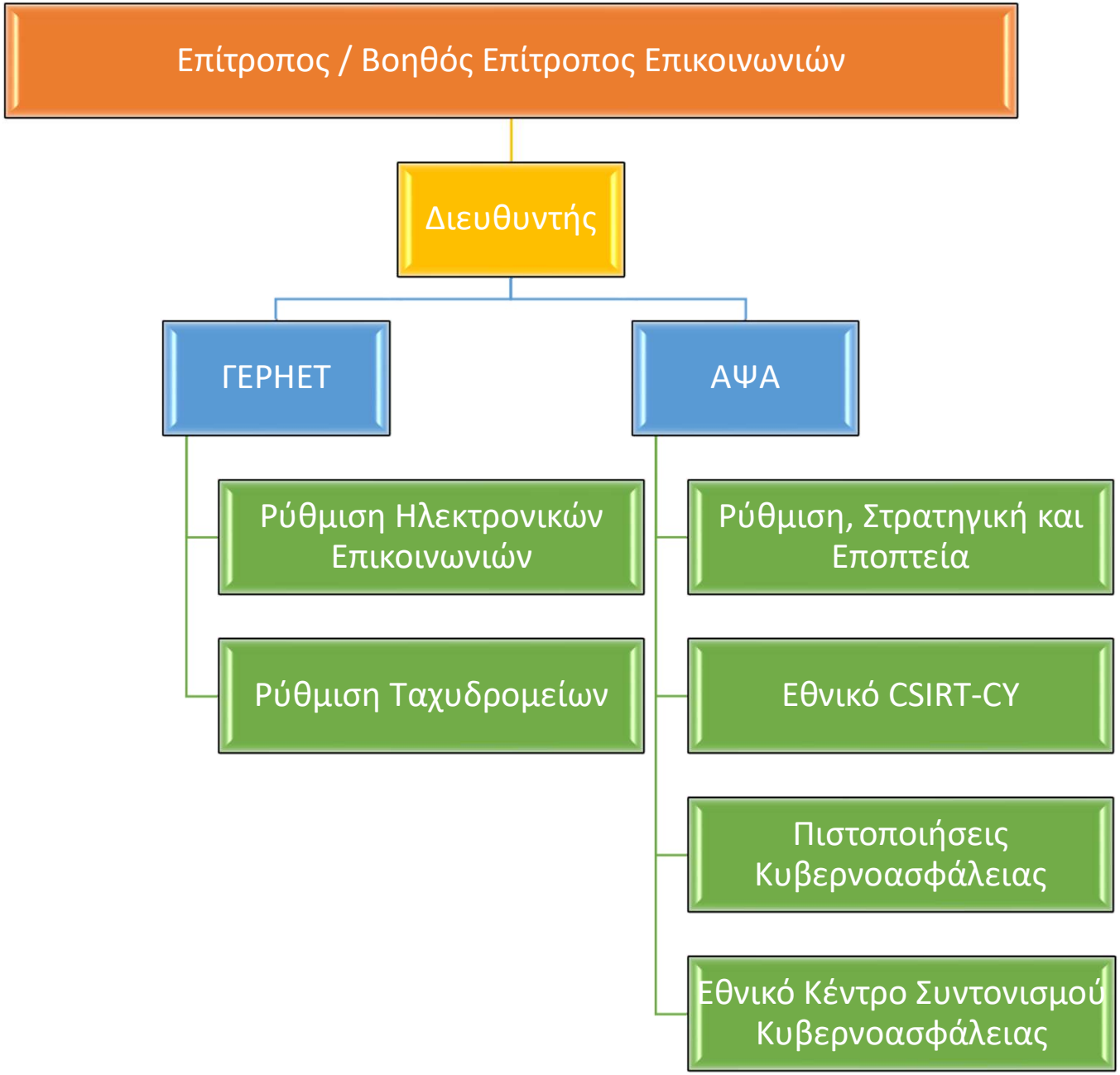
Βασικές Αρμοδιότητες & Δραστηριότητες

ΑΨΑ – Ποιοι είμαστε;

Συστατικά στοιχεία Εθνικής Ικανότητας Κυβερνοασφάλειας

- Αρχή Ψηφιακής Ασφάλειας
  - Υπό την εποπτεία του
- Υλοποίηση της Ευρωπαϊκής Οδηγίας NIS στην Επιτρόπου ΕπικοινωνιώνΚυπριακή Δημοκρατία
  - Ενιαίο Κέντρο Επαφής, Εθνική Αρμόδια Αρχή (για όλους τους τομείς), Εθνικό CSIRT
- Συντονισμός της υλοποίησης της Εθνικής Στρατηγικής Κυβερνοασφάλειας
  - Κυβερνοασφάλεια/NIS, Κυβερνοέγκλημα, **Κυβερνοάμυνα**, σχετικές Εξωτερικές Σχέσεις
- Εθνική Αρχή Πιστοποίησης Κυβερνοασφάλειας
  - Υλοποίηση του Ευρωπαϊκού Πλαισίου Πιστοποίησης Κυβερνοασφάλειας στην Κύπρο
- Εθνική Κέντρο Συντονισμού Κυβερνοασφάλειας
  - Παρέχει γνώση και διευκολύνει την πρόσβαση σε τεχνογνωσία για βιομηχανικά, τεχνολογικά και ερευνητικά θέματα κυβερνοασφάλειας

Οργανωτική Δομή



ΕΠΙΤΡΟΠΟΣ ΕΠΙΚΟΙΝΩΝΙΩΝ

Επίτροπος Επικοινωνιών / Βοηθός Επίτροπος

Διευθυντής Γραφείου Επιτρόπου Επικοινωνιών

Πρώτος Λειτουργός – Προϊστάμενος ΑΨΑ

Τομέας Ρύθμισης, Στρατηγικής και Εποπτείας	Εθνικό CSIRT-CY	Τομέας Πιστοποίησης	Εθνικό Κέντρο Συντονισμού Κυβερνοασφάλειας
- Εθνική Στρατηγική - Εθνική Αξιολόγηση Κινδύνων - Καθορισμός ΦΕΒΥ - Μέτρα Ασφάλειας - Κοινοποίηση Περιστατικών - Έλεγχοι και Εποπτεία - Διαχείριση Κρίσεων - Συντονισμός - Επικοινωνία - Συνεργασία - Επίγνωση	- Προειδοποιήσεις - Διαχείριση Περιστατικών - Χειρισμός Ευπαθειών - Χειρισμός Artifacts - Δικανική Ανάλυση - Δομικές Διείσδυσης - Διαχείριση Κρίσεων - Συντονισμός - Επικοινωνία - Συνεργασία - Επίγνωση	- Εποπτεία **και** Εφαρμογή Σχημάτων Πιστοποίησης - Συμμόρφωση Vendors / Service Providers - Βοήθεια στη διαπίστευση - Εξουσιοδότηση Οργανισμών Αξιολόγησης Συμμόρφωσης - Διαχείριση Καταγγελιών - Συμβολή στη δημιουργία Σχημάτων Πιστοποίησης - Ευρωπαϊκή Συνεργασία	- Εποπτεία και Εφαρμογή Σχημάτων Πιστοποίησης - **Συμμόρφωση** Vendors / Service Providers - Βοήθεια στη διαπίστευση - Εξουσιοδότηση Οργανισμών Αξιολόγησης Συμμόρφωσης - Διαχείριση Καταγγελιών - Συμβολή στη δημιουργία Σχημάτων Πιστοποίησης - Ευρωπαϊκή Συνεργασία

Τομέας Ρύθμισης, Στρατηγικής και Εποπτείας

Στόχος

ΕΘΝΙΚΗ ΑΣΦΑΛΕΙΑ

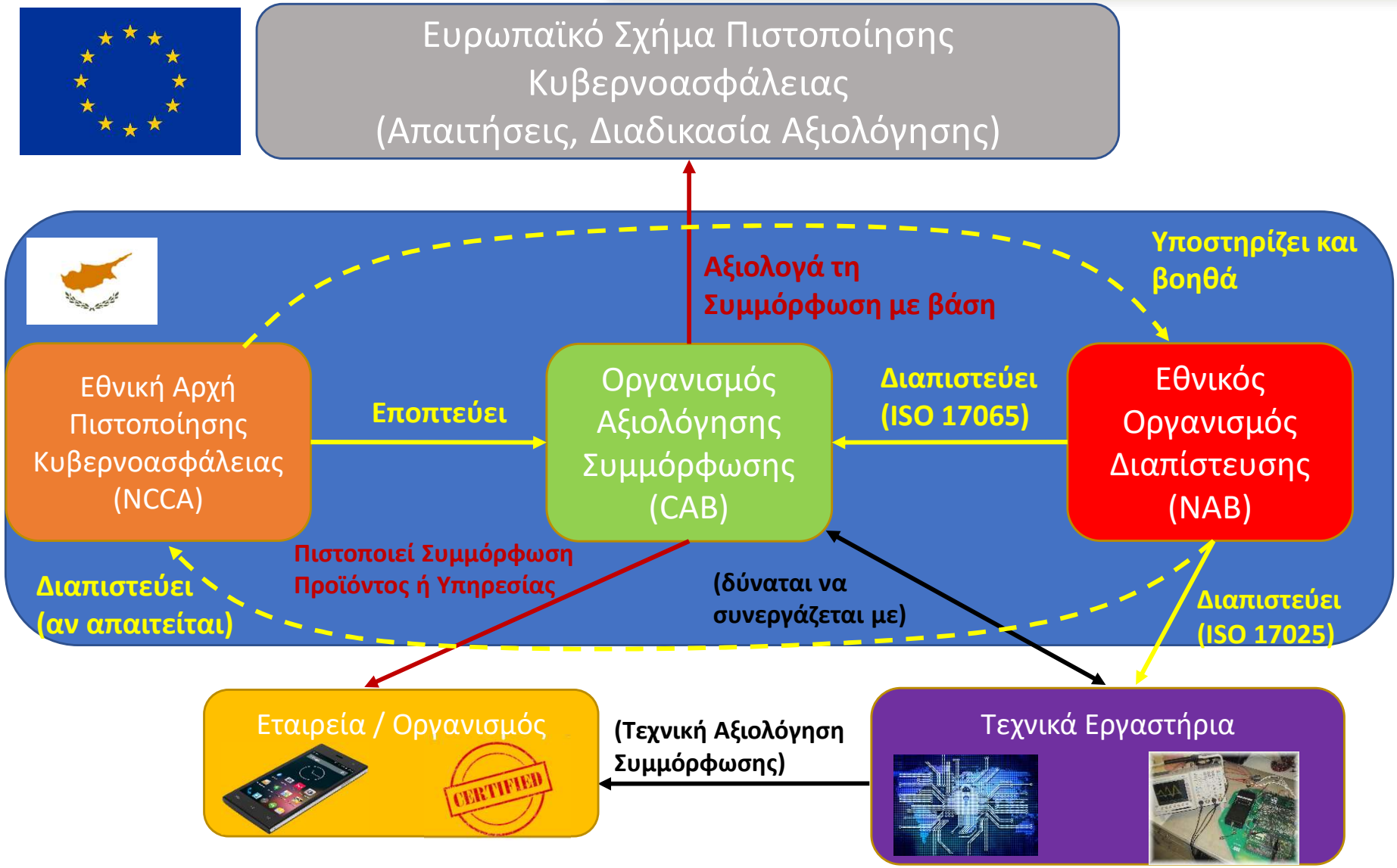
ΕΘΝΙΚΗ ΟΙΚΟΝΟΜΙΑ

ΑΣΦΑΛΕΙΑ ΚΑΙ ΥΓΕΙΑ

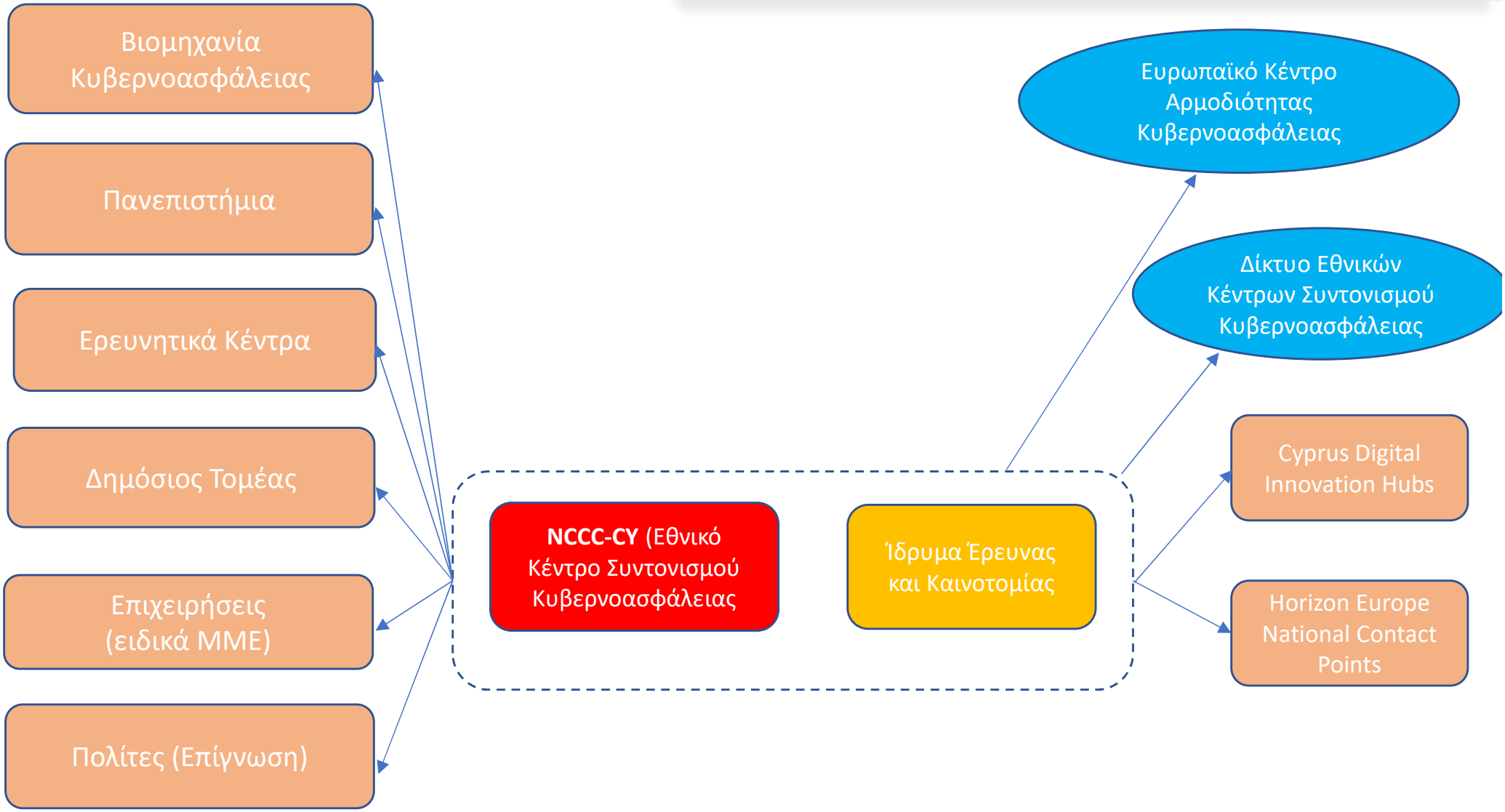
ΚΟΙΝΩΝΙΚΗ ΕΥΗΜΕΡΙΑ

ΠΕΡΙΒΑΛΛΟΝ

Πιστοποιήσεις Κυβερνοασφάλειας στην Κύπρο



Εθνικό Κέντρο Συντονισμού Κυβερνοασφάλειας



Βασικές Αρμοδιότητες & Δραστηριότητες

Αρχή Ψηφιακής Ασφάλειας (ΑΨΑ)

- Το Εθνικό CSIRT-CY είναι ο τεχνικός βραχίονας της ΑΨΑ.
- Το Εθνικό CSIRT-CY αποτελείται από 1 προϊστάμενο και 8 αναλυτές.

Στόχος

- Η Ενίσχυση του επιπέδου ασφάλειας της Κυπριακής Δημοκρατίας.
- Η προστασία των Κρίσιμων Πληροφοριακών Υποδομών, των Τραπεζών, των Παρόχων Ψηφιακών Υπηρεσιών και των Παρόχων Ηλεκτρονικών Επικοινωνιών.

Ίδρυση Εθνικού CSIRT-CY

- Το Υπουργικό Συμβούλιο της Κυπριακής Δημοκρατίας βασισμένο στην οδηγία της Ευρωπαϊκής Ένωσης περί ασφαλείας Δικτύων και Υπολογιστών (NISD – Αρ. Άρθρου 9) ενέκρινε την ίδρυση της Εθνικής ομάδας CSIRT-CY στις 22/10/16 με την απόφαση αριθμό 81/477.
- Το Υπουργικό Συμβούλιο στις 3/5/2017, ενέκρινε τον Πίνακα, με τις Κρίσιμες Πληροφοριακές Υποδομές της Κυπριακή Δημοκρατία (αρ. απόφασης 82.518).
- Η Βουλή των Αντιπροσώπων ψήφισε το νόμο περί ασφαλείας Δικτύων και Υπολογιστών στην Κύπρο, και με την οδηγία αριθμό 17(1)/2018 όρισαν την ΑΨΑ ως την αρμόδια αρχή με τεχνικό βραχίονα το Εθνικό CSIRT-CY.

Συνεργασίες

- Υπουργείο Άμυνας
- Cyprus Police (Cyber Crime Unit)
- Cyprus National Guard (Στρατιωτικό CSIRT)
- CSIRTs Network
- Trusted Introducer (TI)
- Forum of Incident Response and Security Teams (FIRST)
- European Union Agency for Network and Information Security (ENISA)
- International Telecommunication Union (ITU)
- CERT-EU
- CNCS (CERT Portugal)
- CERT-RO (CERT Romania)
- Memorandum of Understanding με
  - Ισραήλ
  - Ρουμανία
  - Πολωνία
- Στρατιωτική Σχολή Ευελπίδων

Ακαδημαϊκό CSIRT

Η Αρχή Ψηφιακής Ασφάλειας, όπως και το Εθνικό CSIRT-CY βρίσκονται από την πρώτη στιγμή δίπλα στον νεοσύστατο Ακαδημαϊκό CSIRT συμμετέχοντας ως συνεργάτης (Partner) στο Ευρωπαϊκό πρόγραμμα για την σύσταση και αναβάθμιση του, δίνοντας πάντοτε κατευθυντήριες γραμμές όπως και τεχνική υποστήριξη όπου χρειάζεται.

Για την επίτευξη των στόχων μας, την εύκολη επικοινωνία και στενή συνεργασία, αλλά και την εξοικονόμηση δημοσίων κονδυλίων συμφωνήθηκε όπως το Ακαδημαϊκό CSIRT συστεγαστεί με το Εθνικό CSIRT.

Από τις αρχές Σεπτεμβρίου 2019 οι δύο οργανισμοί συστεγάζονται και δουλεύουν στενά με κοινό στόχο την προστασία των κρίσιμων υποδομών του κάθε οργανισμού και την ολική προστασία του κυβερνοχώρου της Κυπριακής Δημοκρατίας.

Στρατιωτικό CSIRT

Η Αρχή Ψηφιακής Ασφάλειας, όπως και το Εθνικό CSIRT-CY βρίσκονται από την πρώτη στιγμή δίπλα στον σχεδιασμό και δημιουργία του Στρατιωτικού CSIRT.

Οι δύο οργανισμοί δουλεύουν στενά με κοινό στόχο την προστασία των κρίσιμων υποδομών και την ολική προστασία του κυβερνοχώρου της Κυπριακής Δημοκρατίας, συμμετέχοντας σε κοινές ασκήσεις και αναλύσεις περιστατικών.

Πιστοποιήσεις

- Full Member of FIRST (Forum of Incident Response and Security Teams) – April 2018.
- Accredited Trusted Introducer Team – Ready for Certification – June 2018.
- Advanced Maturity (ENISA CSIRT Maturity Assessment) – March 2019.

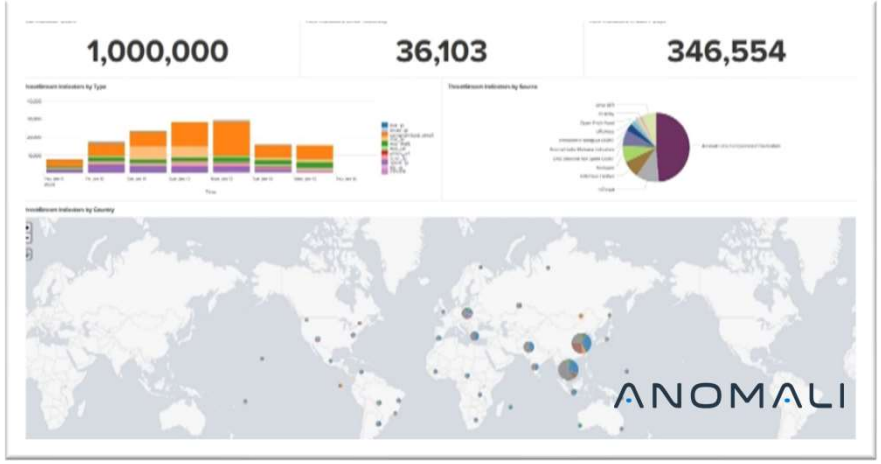
Σε ανακοίνωση της ENISA, σε συνάντηση ενώπιων όλων των Ευρωπαϊκών CSIRTs, το Εθνικό CSIRT-CY ονομάστηκε ως η πιο γρήγορα αναπτυσσόμενη και ώριμη ομάδα CSIRT.

Υπηρεσίες

- Πρόληψης
- Ανταπόκρισης

Threat Intelligence

- Πληροφορίες για απειλές (από εξωτερικούς συνεργάτες).
- Ενημερώσεις σε πραγματικό χρόνο.
- Φίλτρα βασισμένα σε δείκτες IoCs.
- Εντοπισμός ύποπτης δραστηριότητας.
- Ανάλυση κακόβουλής δραστηριότητας.
- Εξωτερικά κανάλια
  - AbuseHelper
  - Anomali
  - Shadowserver
  - Cymru
  - CERT-Bund
  - CERT-EU
  - CERTBr
  - MISP



Έλεγχοι ασφάλειας

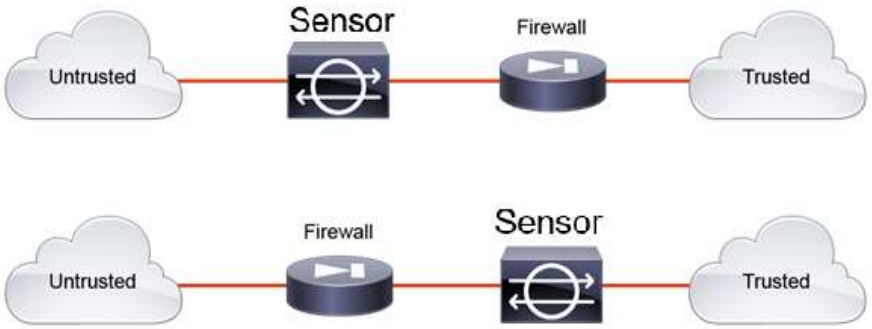
- Ανάλυση διαδικτυακών διακομιστών σε πραγματικό χρόνο.
- Ανάλυση διακομιστών ηλεκτρονικής αλληλογραφίας σε πραγματικό χρόνο.
- Εξασφαλίζει την ακεραιότητα και διαθεσιμότητα των διαδικτυακών υπηρεσιών που ανήκουν στους φορείς.

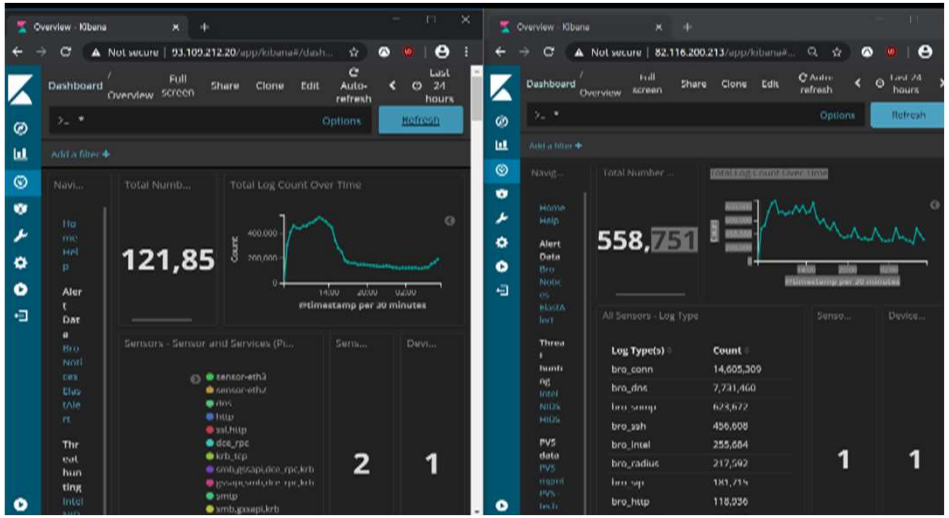
- Εργαλείο ασφάλειας που επιβλέπει συνεχώς την ασφάλεια και τη διαμόρφωση της ιστοσελίδας και του ηλεκτρονικού ταχυδρομείου ενός οργανισμού.
- Έλεγχος πιστοποιητικών εγκυρότητας.
- Έλεγχος πιστοποιητικών HTTP/HTTPs.
- Έλεγχος 530 domain names .cy, .gov.cy.

- Απομακρυσμένος έλεγχος ιστοσελίδων για ανεύρεση τρωτών σημείων.
- Μέχρι σήμερα κατόπιν επικοινωνίας έχουν γίνει ~50 έλεγχοι.

Έλεγχοι ασφάλειας (Αισθητήρες)

- Ανάλυση δικτύου σε πραγματικό χρόνο.
- Φίλτρα βασισμένα σε πρωτόκολλα δικτύου.
- Ανίχνευση ύποπτων ενεργειών.
- Ανάλυση κακόβουλων ενεργειών.



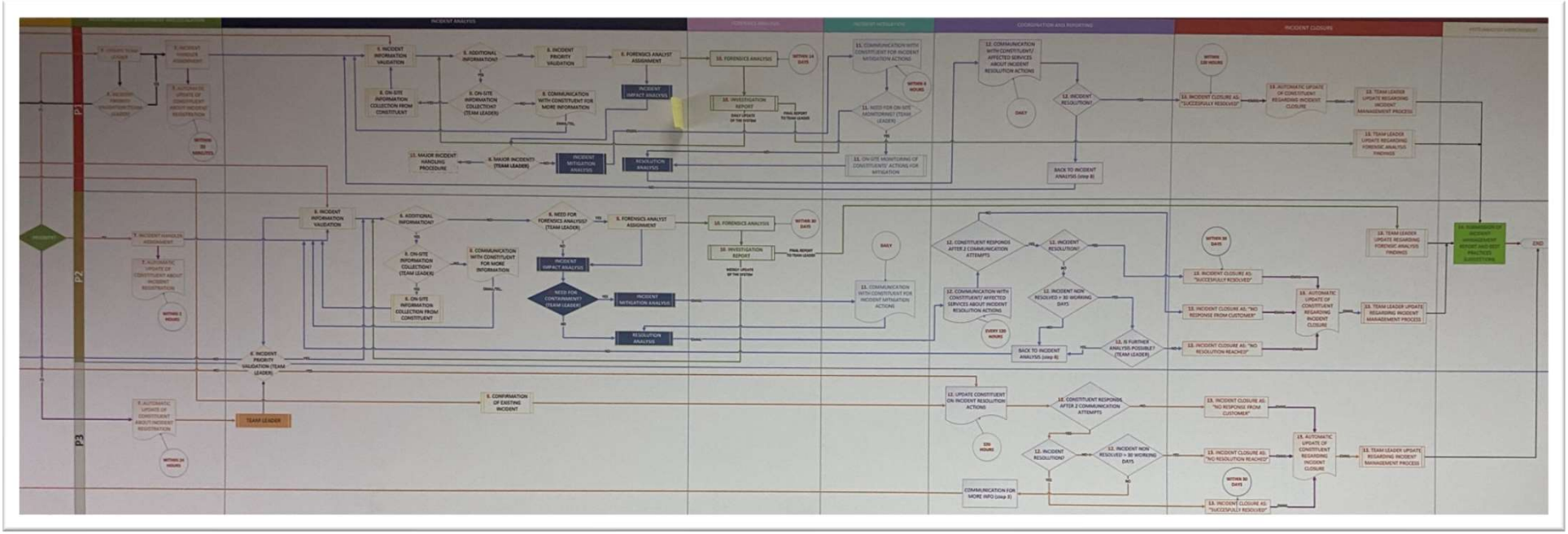


- **Εκπαιδεύσεις «Phishing Awareness» σε Κρίσιμες Υποδομές**
- **Τεχνικές Εκπαιδεύσεις σε Σχολεία**

CYBERANGE

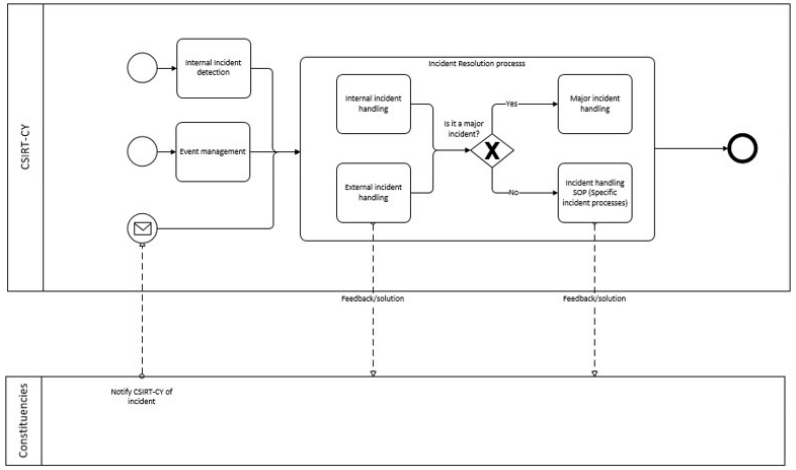
- Πλατφόρμα ασκήσεων
- Πλατφόρμα εκπαίδευσης
- Ρεαλιστικά σενάρια
- Τεχνικό επίπεδο
- Διοικητικό επίπεδο
- Πολιτικές
- Διαδικασίες

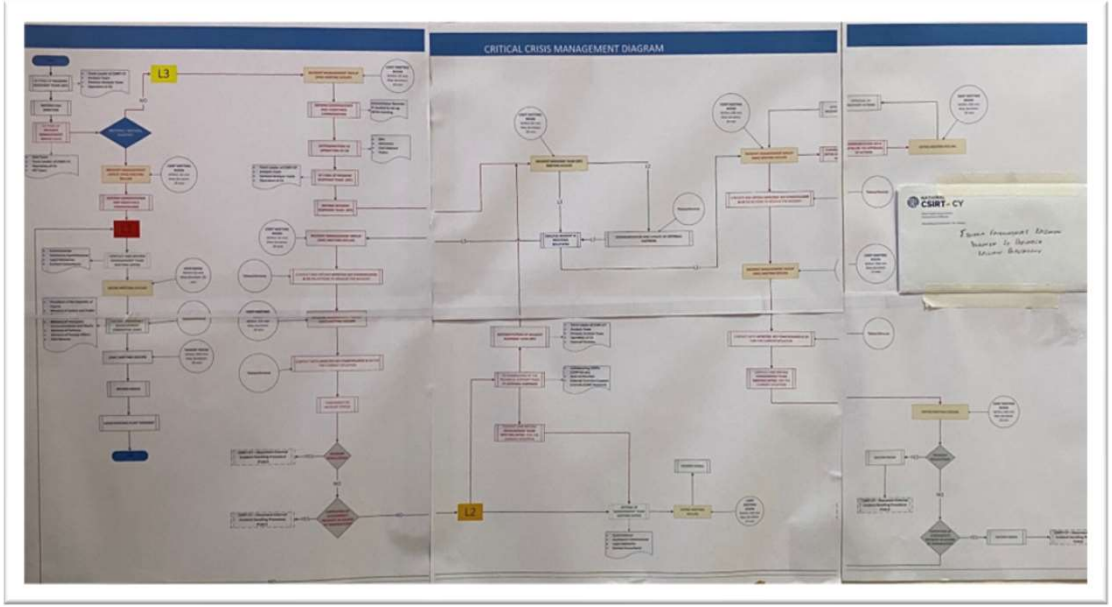
- Incident Management.
  - Χειρισμός Περιστατικών και Μετριασμός Προβλήματος.
  - Χειρισμός Περιστατικών Εθνικής Καταστροφής (Major Incident).
- Δικανική Ανάλυση.
- Αναφορές και Συστάσεις Επαναφοράς Υπηρεσιών.



Διαχείριση Περιστατικών

- Χειρισμός περιστατικών και μετριασμός προβλήματος.
- Περιστατικά χωρισμένα βάση κρισιμότητας και επικινδυνότητας P1, P2, P3.
- Ξεχωριστός χρόνος απόκρισης βάση της κατηγοριοποίησης του περιστατικού.
- Δυνατότητα για περισυλλογή στοιχείων στις εγκαταστάσεις του φορέα.
- Ειδικό δίκτυο – CSIRT-CY Lab – σε απομονωμένο δίκτυο για δικανική ανάλυση.





“DO WE HAVE INCIDENTS IN CYPRUS???”

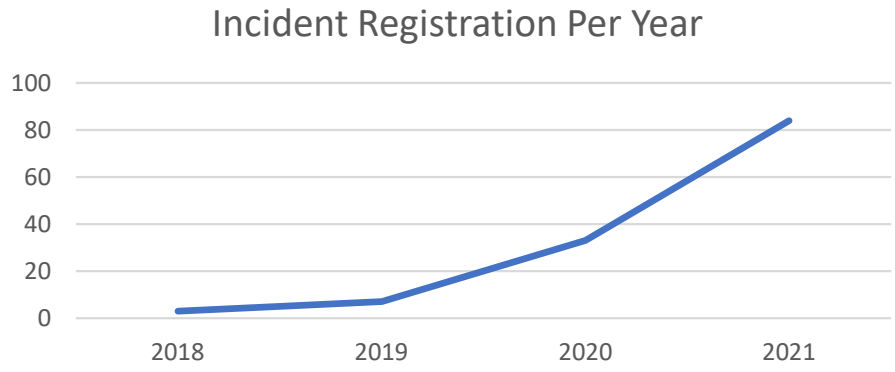
Dwell time is the number of days from first evidence of compromise that an attacker is present on a victim network before detection. (Gartner)

“Surely.. No one cares to attack Cyprus”

Numb3rs

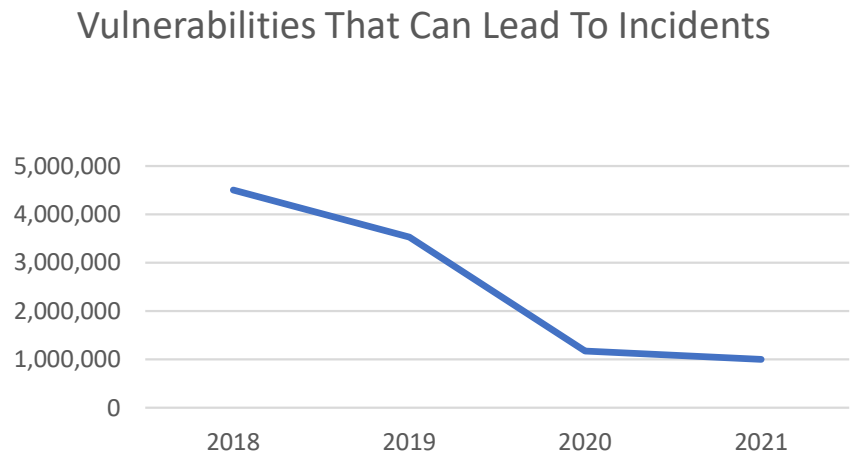
Incidents Registered To The National CSIRT

- 2018 = 3
- 2019 = 7
- 2020 = 33
- 2021 = 190
- 2022 = 225 (incl. 13/12/22)

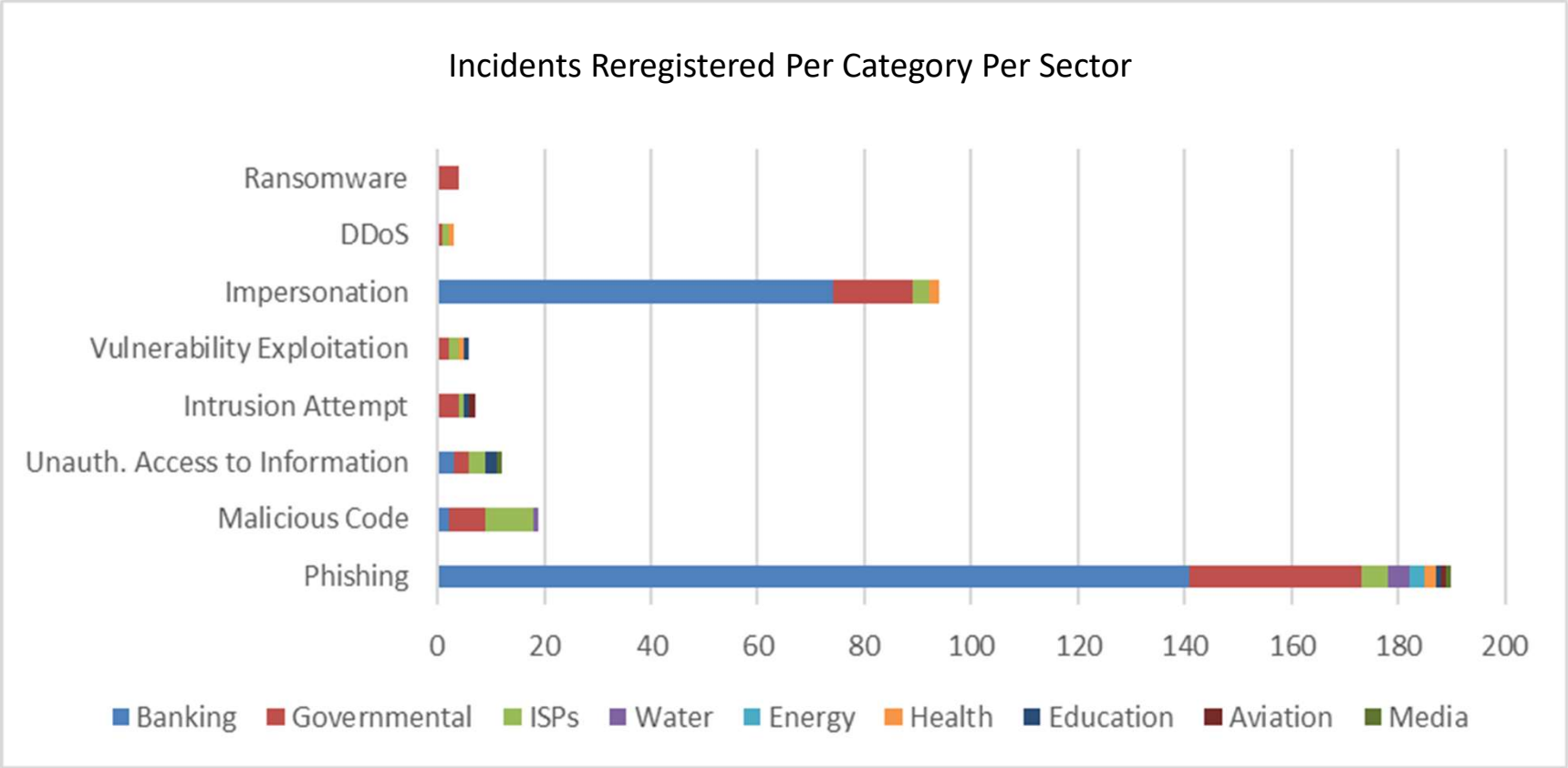


Vulnerability Notifications To The CNI

- 2018 = 4,500,268
- 2019 = 3,527,391
- 2020 = 1,175,797
- 2021 = ~ 1,000,000
- 2022 = ~ 900,000

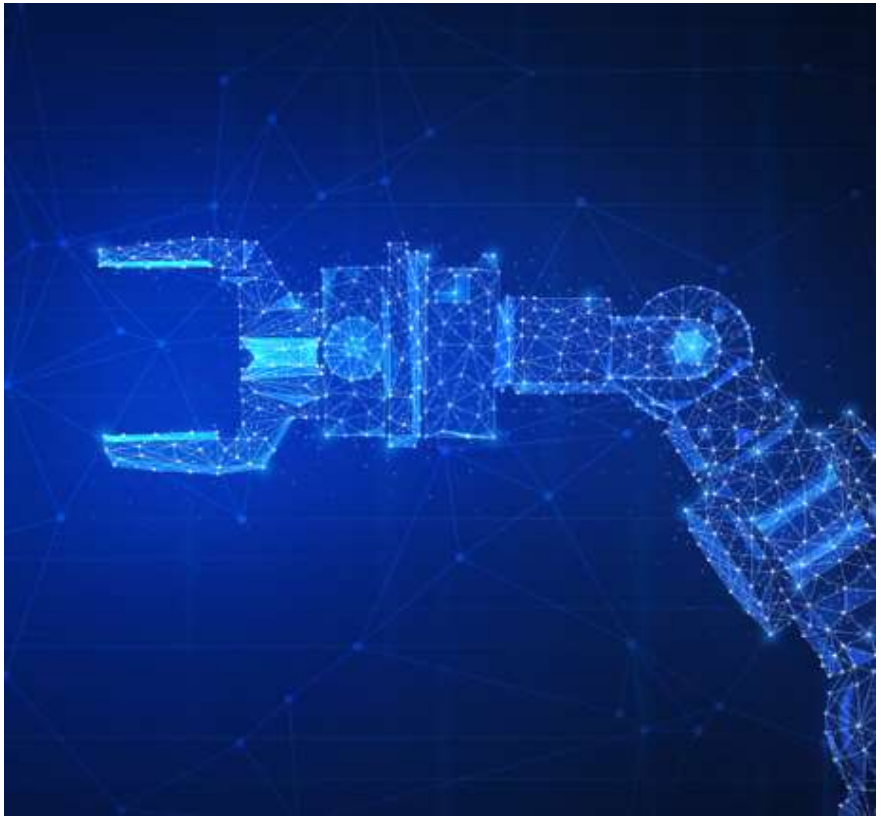


Numb3rs


Incidents Reregistered Per Category Per Sector
Ransomware
DDoS
Impersonation
Vulnerability Exploitation
Intrusion Attempt
Unauth. Access to Information
Malicious Code
Phishing
0
20
40
60
80
100
120
140
160
180
200
Banking
Governmental
ISPs
Water
Energy
Health
Education
Aviation
Media

Κίνδυνοι σε Εθνικό Επίπεδο

- Διακοπή παροχής υπηρεσιών των Κρίσιμων Υποδομών.
- Υποκλοπή προσωπικών στοιχείων.
- Δημιουργία αισθήματος ανασφάλειας στους πολίτες μέσω κακόβουλης αλλαγής των ιστοσελίδων Κυβερνητικών υπηρεσιών.
- Υποκλοπή διαβαθμισμένων εγγράφων/πληροφοριών από Κυβερνητικές υπηρεσίες.
- Παραβίαση βασικών κυβερνητικών συστημάτων.
- Μη εξουσιοδοτημένη πρόσβαση σε κυβερνητικά συστήματα.
- Παράνομη χρήση κυβερνητικών συστημάτων.
- Γενικευμένο Black-out.



Οι κυβερνο-επιθέσεις προηγούνται των λοιπών στρατιωτικών επιχειρήσεων και χρησιμοποιούνται κατά κόρον σε περίοδο κρίσεων και γεωπολιτικής αστάθειας.

NATIONAL CSIRT-CY

ΕΠΙΤΡΟΠΟΣ ΕΠΙΚΟΙΝΩΝΙΩΝ

Αρχή Ψηφιακής Ασφάλειας

Feedback
Planning & Direction
Collection
Processing
Analysis
Dissemination

Εκπαιδεύσεις με θεματολογία την ζωή στο διαδίκτυ

- Τι είναι η κυβερνοασφάλεια;
- Κίνδυνοι και απειλές στο κυβερνοχώρο
- Πραγματικά παραδείγματα
- Καλές πρακτικές
- Βήματα μετριασμού / Στοιχεία επικοινωνίας

Ε.Ε. Παρ. III(I)
Αρ. 5342, 21.8.2020
Αριθμός 389

Ο ΠΕΡΙ ΑΣΦΑΛΕΙΑΣ ΔΙΚΤΥΩΝ ΚΑΙ ΣΥΣΤΗΜΑΤΩΝ ΠΛΗΡΟΦΟΡΙΩΝ ΝΟΜΟΣ ΤΟΥ 2020

Απόφαση δυνάμει των άρθρων 17(ιζ), 17(ιη), 17(ιθ), 17(κβ), 17(κγ), 19(1)(β), 19(1)(γ), 20(1)(α), 20(1)(β), 20(1)(γ), 46(1), 46(4) και 46(5)

Η Αρχή Ψηφιακής Ασφάλειας (στο εξής «η Αρχή»),

Οι φορείς οφείλουν να συμμορφωθούν με το ακόλουθο πρόγραμμα ενεργειών:

(α) Μέχρι 31 Δεκεμβρίου 2020
- Αποστολή έκθεσης στην Αρχή στην οποία θα καταγράφεται η παρούσα κατάσταση ασφάλειας δικτυών και συστημάτων πληροφοριών στον φορέα

(β) Μέχρι 31 Δεκεμβρίου 2021
- Υποβολή των εγγράφων και πληροφοριών σύμφωνα με τις απαιτήσεις του άρθρου 13 της παρούσας Απόφασης

(γ) Μέχρι 31 Δεκεμβρίου 2022
- Ολοκλήρωση της υλοποίησης και εφαρμογής των μέτρων ασφάλειας που αντιμετωπίζουν τους υψηλότερους σε κρισιμότητα, κινδύνους που έχουν εντοπιστεί
- Πρόγραμμα υλοποίησης του συνόλου του Πλαισίου

(δ) Μέχρι 31 Δεκεμβρίου 2023 και μετέπειτα, σε ετήσια βάση
- Ολοκλήρωση της υλοποίησης του υπόλοιπου Πλαισίου
- Υποβολή των εγγράφων και πληροφοριών σύμφωνα με τις απαιτήσεις του άρθρου 13 της παρούσας Απόφασης

ΠΑΡΑΡΤΗΜΑ Ι : ΠΛΑΙΣΙΟ ΑΞΙΟΛΟΓΗΣΗΣ ΚΙΝΔΥΝΩΝ

ΠΑΡΑΡΤΗΜΑ ΙΙ: ΣΧΕΔΙΟ ΕΠΙΧΕΙΡΗΣΙΑΚΗΣ ΣΥΝΕΧΕΙΑΣ ΚΑΙ ΣΧΕΔΙΟ ΑΠΟΚΑΤΑΣΤΑΣΗΣ ΑΠΟ ΚΑΤΑΣΤΡΟΦΕΣ

ΠΑΡΑΡΤΗΜΑ ΙΙΙ: ΠΛΑΙΣΙΟ ΜΕΤΡΩΝ ΑΣΦΑΛΕΙΑΣ

1.ΜΕΤΡΑ ΑΣΦΑΛΕΙΑΣ

1.2 ΠΡΟΣΤΑΣΙΑ ΚΑΙ ΕΝΤΟΠΙΣΜΟΣ (PROTECT AND DETECT)

1.3 ΑΝΤΑΠΟΚΡΙΣΗ (RESPOND)

Κατηγορία	#	Μέτρο	Στόχος Μέτρου	Περιγραφή Μέτρου
Στρατηγική	STR1	Στρατηγική για την ασφάλεια πληροφοριών	Να θεσπιστεί στρατηγική ασφάλειας πληροφοριών στην οποία να αναλύονται οι στόχοι και η προσέγγιση υψηλού επιπέδου με σκοπό τον μετριασμό των κινδύνων για την ασφάλεια πληροφοριών.	Καθορισμός του οράματος και της δέσμευσης για την ασφάλεια πληροφοριών σε μια στρατηγική που θα περιγράφει λεπτομερώς συγκεκριμένους στόχους αναφορικά με την ασφάλεια, καθώς και την προσέγγιση για την ασφάλεια και τη διαχείριση του κινδύνου, και τα μέσα για την επικύρωση της αποτελεσματικότητας της στρατηγικής με την υποστήριξη από βασικούς δείκτες επιδόσεων. Η στρατηγική ασφάλειας πληροφοριών αντικατοπτρίζεται στην πολιτική ασφάλειας πληροφοριών, όπως περιγράφεται στο μέτρο [GOV3]. Τα στελέχη γνωρίζουν τη στρατηγική και την πολιτική ασφάλειας πληροφοριών, όπως περιγράφεται στο μέτρο [TA1].
Διακυβέρνηση	GOV1	Ρόλοι και αρμοδιότητες σχετικά με την ασφάλεια πληροφοριών	Να καθοριστούν οι ρόλοι και οι αρμοδιότητες σχετικά με την ασφάλεια πληροφοριών εντός του οργανισμού.	Καθορισμός των ρόλων και των αρμοδιοτήτων όσον αφορά την ασφάλεια δικτύων και πληροφοριών για όλα τα στελέχη που ασχολούνται με την επεξεργασία πληροφοριών ή έχουν πρόσβαση σε συστήματα επεξεργασίας πληροφοριών. Οι καθορισμένοι ρόλοι και αρμοδιότητες αντικατοπτρίζονται στην πολιτική ασφάλειας των πληροφοριών [GOV3]. Τα στελέχη πρέπει να είναι επαρκώς ενημερωμένα και να έχουν επίγνωση των ρόλων και των ευθυνών τους όσον αφορά την ασφάλεια δικτύων και πληροφοριών, όπως ορίζεται στα μέτρα [TA1, TA2]. Οι ρόλοι και οι αρμοδιότητες που σχετίζονται με την ασφάλεια των πληροφοριών θα πρέπει να καθορίζονται από τη διοίκηση, ώστε να εξασφαλίζεται η υπευθυνότητα για τις αποφάσεις της διοίκησης που σχετίζονται με την ασφάλεια δικτύων και συστημάτων πληροφοριών.

3.ΠΡΟΣΑΡΤΗΜΑ Β: ΟΔΗΓΙΕΣ ΕΦΑΡΜΟΓΗΣ: ISO/IEC 27001 AND NIST SP800-53

Το παρόν παράρτημα περιλαμβάνει αναφορές στις οδηγίες εφαρμογής ανά μέτρο ασφάλειας. Οι οδηγίες εφαρμογής στον παρακάτω πίνακα αναφέρονται σε δύο διεθνή πρότυπα: ISO / IEC 27001 και NIST SP800-53 Rev. 4, και παρέχονται για υποβοήθεια στην κατανόηση του περιεχόμενου των μέτρων ασφάλειας από τους φορείς.

Ref.	Control	ISO/IEC 27001	NIST SP800-53 Rev. 4
AM1	Asset lifecycle management	A.8	CM-8, PL-4, PS-4, PS-5, RA-2, MP-2, MP-3, MP-4, MP-5, MP-6, MP7, PE-16, PE-18, PE-20, SC-8, SC-28
AM2	Inventory of assets and ownership	A.8.1.1, A.8.1.2	CM-8
AM3	Asset monitoring	A.12.4	PE-20
AM4	Availability management	A.11.2.4, A.17.2	SC-5, SC-36
AM5	Cryptographic controls	§10, A.18.1.5	SC-12, SC-13
AM6	Capacity management	A.12.1.3	AU-4, CP-2, SC-5
AS1	Secure software development lifecycle	A.14.2	SA-8, SA-10, SA-11
BCR 1	Business impact analysis	A.16.1.1, A.17.1.1, A.17.1.2	RA-2, RA-3, PM-9
BCR 2	Business continuity plan	A.16.1.1, A.17.1.1, A.17.1.2	CP-2, CP-6, CP-7, CP-8, CP-9, CP-10, CP-11, CP-13, IR-8
BCR 3	Business continuity exercises and simulations	A.17.1.3	CP-4, IR-2, IR-3, PM-14
BCR 4	Disaster recovery plan	A.16.1.1, A.17.1.1, A.17.1.2, A.17.1.3	CP-2, IR-8, CP-4, IR-3, PM-14
CM1	Change management	A.12.1.2	CM-3, CM-5, SA-10
CM2	Configuration management	A.5.1.1, A.5.1.2, A.6.1.1, A.8.1.1, A.8.1.2, A.9.2.3, A.9.4.5, A.12.1.1, A.12.1.2, A.12.1.4, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4, A.18.1.1, A.18.1.2; A.18.2.2	CM-1, CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-8, CM-9, CM-10, CM-11
DS1	Information lifecycle management	§8.1, A.8.1, A.8.2, A.8.3	SA-1, SA-3, SA-4, SA-5, SA-8, SA-9, SA-11, SA-12, MP-1, MP-2, MP-3, MP-4, MP-5, MP-6, MP-7, MP-8

Ευχαριστώ!

Andreas Iacovou
Team Leader, National CSIRT-CY
www.dsa.cy/ | www.csirt.cy/

ΕΠΙΤΡΟΠΟΣ ΕΠΙΚΟΙΝΩΝΙΩΝ

Αρχή Ψηφιακής Ασφάλειας