NCC
ΕΘΝΙΚΟ ΚΕΝΤΡΟ ΣΥΝΤΟΝΙΣΜΟΥ
ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ
ΚΥΠΡΟΥ

# ΓΛΩΣΣΑΡΙΟ

# ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ

## ΟΔΗΓΟΣ ΒΑΣΙΚΗΣ ΟΡΟΛΟΓΙΑΣ

ΕΠΙΤΡΟΠΟΣ ΕΠΙΚΟΙΝΩΝΙΩΝ | Αρχή Ψηφιακής Ασφάλειας

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

www.ncc.cy

# Ποιοι είμαστε

Την 21η Δεκεμβρίου 2021, με απόφαση του Υπουργικού Συμβουλίου η Αρχή Ψηφιακής Ασφάλειας (ΑΨΑ) , οντότητα του ευρύτερου δημόσιου τομέα, ορίστηκε ως το Εθνικό Κέντρο Συντονισμού Κυβερνοασφάλειας (NCC-CY) στην Κυπριακή Δημοκρατία.

Το NCC-CY λειτουργεί συντονισμένα ως μέλος του Δικτύου των Εθνικών Κέντρων Συντονισμού (NCCs) και υποστηρίζει το Ευρωπαϊκό Κέντρο Αρμοδιότητας Κυβερνοασφάλειας (ECCC) στην εκπλήρωση της αποστολής και των στόχων του.

**www.ncc.cy**

NCC

ΕΘΝΙΚΟ ΚΕΝΤΡΟ ΣΥΝΤΟΝΙΣΜΟΥ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ

ΚΥΠΡΟΥ

# Κύριοι Στόχοι

### ΕΠΙΧΟΡΗΓΗΣΕΙΣ

Παροχή επιχορηγήσεων για επένδυση στην Κυβερνοασφάλεια

### ΚΟΙΝΟΤΗΤΑ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ

Αναγνώριση, δημιουργία και διασύνδεση της Εθνικής Κοινότητας Κυβερνοασφάλειας με την Ευρωπαϊκή

### ΕΥΑΙΣΘΗΤΟΠΟΙΗΣΗ

Προάγουμε την ευαισθητοποίηση, παρέχουμε ενημέρωση και εκπαίδευση για θέματα κυβερνοασφάλειας

NCC

ΕΘΝΙΚΟ ΚΕΝΤΡΟ ΣΥΝΤΟΝΙΣΜΟΥ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ ΚΥΠΡΟΥ

**Κυβερνοασφάλεια (Cybersecurity):** Είναι η πρακτική προστασίας συστημάτων, δικτύων και προγραμμάτων από ψηφιακές επιθέσεις. Αυτές οι κυβερνοεπιθέσεις συνήθως στοχεύουν στην πρόσβαση, την αλλαγή ή την καταστροφή ευαίσθητων πληροφοριών. Εκβίαση/ Απόσπαση χρημάτων από χρήστες μέσω ransomware ή διακόπτοντας τις συνήθεις επιχειρηματικές διαδικασίες.

**Κυβερνο- Απειλές (Cyber Threads)**: Πιθανοί κίνδυνοι που μπορεί να απειλήσουν την κυβερνοασφάλεια (π.χ Ransomware, Malware)

**Τρωτά σημεία (Vulnerabilities)**: Σημεία σε συστήματα υπολογιστών ή δίκτυα που μπορούν να εκμεταλλευτούν οι επιτιθέμενοι για να προκαλέσουν προβλήματα ή να αποκτήσουν πρόσβαση

**Κυβερνο-επίθεση (Cyber Attack)**: Είναι κάθε σκόπιμη προσπάθεια κλοπής, έκθεσης, αλλαγής, απενεργοποίησης ή καταστροφής δεδομένων, εφαρμογών ή άλλων περιουσιακών στοιχείων μέσω μη εξουσιοδοτημένης πρόσβασης σε δίκτυο, σύστημα υπολογιστή ή ψηφιακή συσκευή.

www.ncc.cy

NCC

ΕΘΝΙΚΟ ΚΕΝΤΡΟ ΣΥΝΤΟΝΙΣΜΟΥ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ

ΚΥΠΡΟΥ

**Ανίχνευση Απειλών (Threat Detection)**: Η διαδικασία ανίχνευσης και αντιμετώπισης ανεπιθύμητων δραστηριοτήτων ή προσπαθειών εισβολής.

**Ευαίσθητες Πληροφορίες (Sensitive Information)**: Πληροφορία που, εάν διαρρεύσει ή καταστεί προσβάσιμη σε μη εξουσιοδοτημένα πρόσωπα, μπορεί να προκαλέσει ζημιά σε άτομα, οργανισμούς ή συστήματα.

**Κυβερνοεπίθεση (Cyber Attack)**: Επιθέσεις που πραγματοποιούνται μέσω του διαδικτύου με σκοπό την παραβίαση, την καταστροφή, τον έλεγχο ή την κλοπή ευαίσθητων δεδομένων.

**Κακόβουλο Λογισμικό (Malware)**: Λογισμικό σχεδιασμένο για να προκαλεί ζημιά σε έναν υπολογιστή, δίκτυο ή χρήστη, όπως ιοί (viruses), και κακόβουλα προγράμματα.

NCC
ΕΘΝΙΚΟ ΚΕΝΤΡΟ ΣΥΝΤΟΝΙΣΜΟΥ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ ΚΥΠΡΟΥ

**Ηλεκτρονικό Ψάρεμα (Phishing)**: Μια επίθεση όπου ο επιτιθέμενος προσπαθεί να αποκτήσει ευαίσθητες πληροφορίες, όπως κωδικούς πρόσβασης ή πιστωτικές κάρτες, παριστάνοντας ότι είναι αξιόπιστη πηγή (π.χ. ηλεκτρονικό ταχυδρομείο [email] ή website [ιστοσελίδα]).

**Pharming**: Το pharming στην κυβερνοασφάλεια είναι ένας τύπος κυβερνοεπίθεσης που ανακατευθύνει την κυκλοφορία του ιστότοπου από έναν νόμιμο ιστότοπο σε έναν ψεύτικο ιστότοπο, με σκοπό την κλοπή ευαίσθητων πληροφοριών, όπως κωδικούς πρόσβασης και πιστωτικές κάρτες.

**Vishing**: Συνδυασμός των λέξεων voice (φωνή) και phishing (απάτη). Αναφέρεται σε μια μορφή όπου κακόβουλος επιτιθέμενος χρησιμοποιεί την φωνητική επικοινωνία μέσω φωνητικών κλήσεων για να εξαπατήσει τα θύματα του. Στόχος του απατεώνα είναι να αποκτήσει ευαίσθητες πληροφορίες, όπως αριθμό πιστωτικής κάρτας, κωδικό πρόσβασης, ή άλλες προσωπικές πληροφορίες.

**Smishing**: Το smishing είναι μια άλλη μορφή απάτης που συνδυάζει τις λέξεις SMS (Short Message Service) και phishing (απάτη). Στο smishing, ο κακόβουλος επιτιθέμενος χρησιμοποιεί μηνύματα κειμένου (SMS) για να εξαπατήσει τα θύματά του. Συνήθως, τα ανεπιθύμητα μηνύματα περιέχουν ψευδείς ή παραπλανητικές πληροφορίες με σκοπό να πείσουν τα θύματα να αποκαλύψουν προσωπικές πληροφορίες, όπως αριθμούς πιστωτικών καρτών, κωδικούς πρόσβασης ή άλλες ευαίσθητες πληροφορίες.

NCC
ΕΘΝΙΚΟ ΚΕΝΤΡΟ ΣΥΝΤΟΝΙΣΜΟΥ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ ΚΥΠΡΟΥ

**Τείχος Προστασίας (Firewall)**: Ένα υλικό ή λογισμικό σύστημα που χρησιμοποιείται για τον έλεγχο της εισόδου και εξόδου της κυκλοφορίας δεδομένων μεταξύ δικτύων.

**Ενημέρωση Ασφαλείας (Patch Management)**: Ένα πρόγραμμα ή ένα σύνολο προγραμμάτων που ενημερώνει ένα σύστημα για να κλείσει ενδεχόμενες ευπάθειες ασφαλείας.

**Έλεγχος Ταυτότητας δύο παραγόντων/ Έλεγχος ταυτότητας Πολλαπλών Παραγόντων(2 Factors Authentication/ Multi Factor Authentication)**: Είναι μια μέθοδος επαλήθευσης ταυτότητας στην οποία οι χρήστες πρέπει να παρέχουν δύο ή περισσότερα αποδεικτικά στοιχεία, όπως έναν κωδικό πρόσβασης και έναν κωδικό πρόσβασης μίας χρήσης, για να αποδείξουν την ταυτότητά τους και να αποκτήσουν πρόσβαση σε έναν διαδικτυακό λογαριασμό.

**Πολιτικές Ασφαλείας (Security Policies)**: Ένα σύνολο κανόνων που ισχύουν για δραστηριότητες στον υπολογιστή και τους πόρους επικοινωνιών που ανήκουν σε έναν οργανισμό. Αυτοί οι κανόνες περιλαμβάνουν τομείς όπως την φυσική ασφάλεια, ασφάλεια προσωπικού και η ασφάλεια δικτύου.

www.ncc.cy

NCC
ΕΘΝΙΚΟ ΚΕΝΤΡΟ ΣΥΝΤΟΝΙΣΜΟΥ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ
ΚΥΠΡΟΥ

**Επιθετική Ανίχνευση (Intrusion Detection)**: Σύστημα που παρακολουθεί το δίκτυο ή τα συστήματα για ανιχνεύσεις επιθέσεων ή παραβιάσεων.

**Επιθετική Πρόληψη (Intrusion Prevention)**: Σύστημα που ανιχνεύει και αποτρέπει επιθέσεις ή ανεπιθύμητες ενέργειες σε πραγματικό χρόνο.

**Κρυπτογράφηση (Cryptography)**: Η κωδικοποίηση πληροφοριών για την προστασία της εμπιστευτικότητας και της ακεραιότητας των δεδομένων.

**Δίκτυο Μηδενικής Εμπιστοσύνης (Zero Trust Network)**: Μια αρχή ασφαλείας που υποστηρίζει ότι δεν πρέπει να υπάρχει προκαταρκτική εμπιστοσύνη για κανένα χρήστη ή συσκευή στο δίκτυο.

NCC
ΕΘΝΙΚΟ ΚΕΝΤΡΟ ΣΥΝΤΟΝΙΣΜΟΥ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ ΚΥΠΡΟΥ

**Ανάκτηση Δεδομένων (Data Recovery)**: Η διαδικασία ανάκτησης δεδομένων μετά από μια καταστροφή, όπως επίθεση ransomware (κακόβουλα λογισμικά με απώτερο σκοπό την εξασφάλιση λύτρων) ή φυσική ζημιά.

**Εκπαίδευση Εργαζομένων (Employee Training)**: Η διαδικασία κατάρτισης του προσωπικού για την αναγνώριση και αντιμετώπιση κινδύνων ασφαλείας.

**Διακυβέρνηση κυβερνοασφάλειας (Cybersecurity Governance)** Η διακυβέρνηση της κυβερνοασφάλειας είναι μια ολοκληρωμένη στρατηγική κυβερνοασφάλειας που ενσωματώνεται στις οργανωτικές λειτουργίες και αποτρέπει τη διακοπή των δραστηριοτήτων λόγω απειλών ή επιθέσεων στον κυβερνοχώρο.

**Ευάλωτη Προσβασιμότητα (Vulnerability Disclosure)**: Η αποκάλυψη ευπάθειας αναφέρεται στη διαδικασία εντοπισμού, αναφοράς και επιδιόρθωσης αδυναμιών λογισμικού, υλικού ή υπηρεσιών που μπορούν να αξιοποιηθούν.

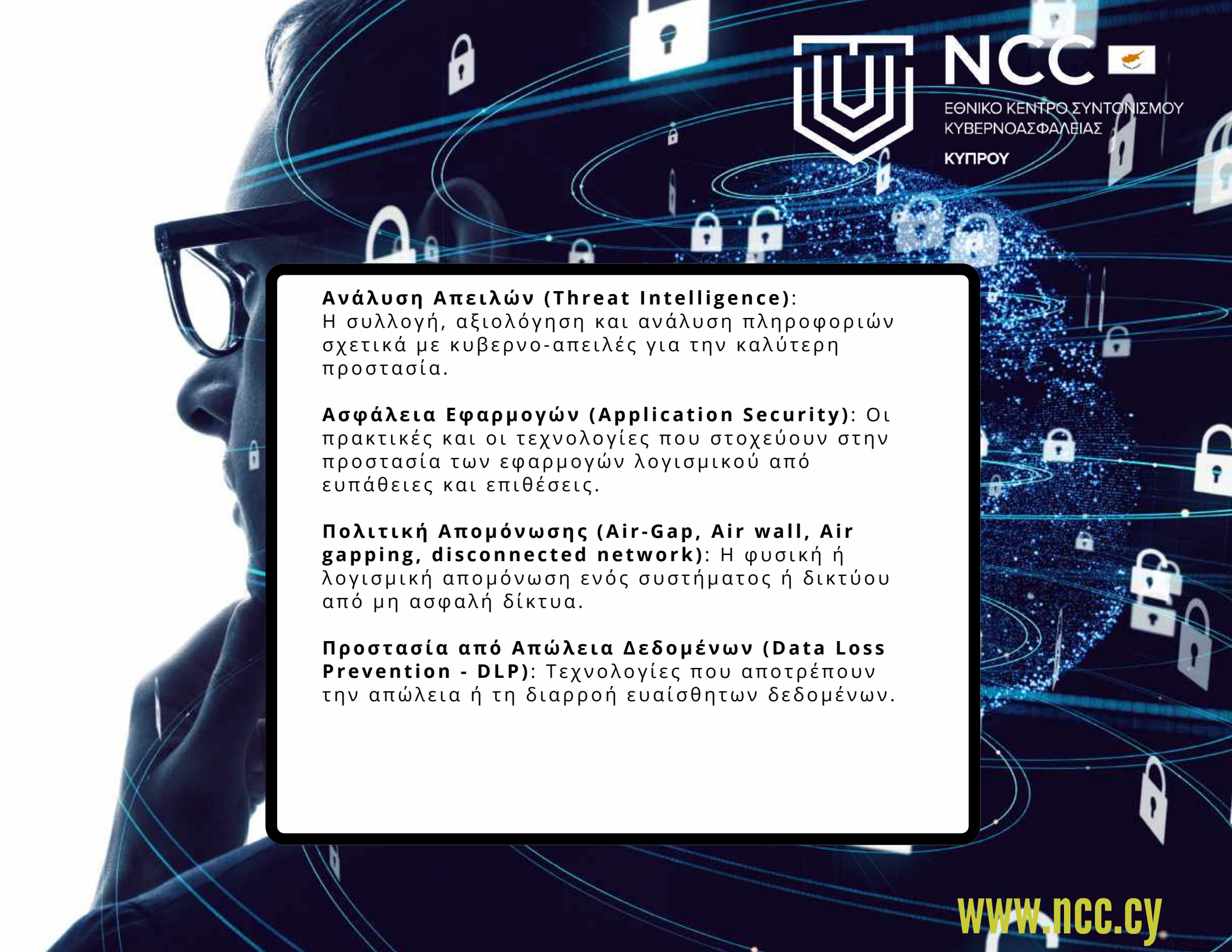

**Προηγμένες Απειλές Κινδύνου (Advanced Persistent Threats - APTs)**: Συνεχείς και εξελιγμένες κυβερνοεπιθέσεις που στοχεύουν συγκεκριμένους οργανισμούς για μεγάλο χρονικό διάστημα.

**Συμμόρφωση (Compliance)**: Η συμμόρφωση με κυβερνονομικές προδιαγραφές, νόμους και κανονιστικά πλαίσια που σχετίζονται με την κυβερνοασφάλεια.

**Ανίχνευση και Αντιμετώπιση Περιστατικών (Incident Detection and Response)**: Οι διαδικασίες και οι τεχνολογίες που χρησιμοποιούνται για τον εντοπισμό και την αντιμετώπιση κυβερνοεπιθέσεων και παραβιάσεων.

**Κυβερνοασφάλεια του Διαδικτύου των Πραγμάτων (IoT Security)**: Οι πρακτικές και οι τεχνολογίες που αφορούν την ασφάλεια των συσκευών που συνδέονται στο Διαδίκτυο.

www.ncc.cy



NCC

ΕΘΝΙΚΟ ΚΕΝΤΡΟ ΣΥΝΤΟΝΙΣΜΟΥ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ ΚΥΠΡΟΥ

**Ανάλυση Απειλών (Threat Intelligence)**: Η συλλογή, αξιολόγηση και ανάλυση πληροφοριών σχετικά με κυβερνο-απειλές για την καλύτερη προστασία.

**Ασφάλεια Εφαρμογών (Application Security)**: Οι πρακτικές και οι τεχνολογίες που στοχεύουν στην προστασία των εφαρμογών λογισμικού από ευπάθειες και επιθέσεις.

**Πολιτική Απομόνωσης (Air-Gap, Air wall, Air gapping, disconnected network)**: Η φυσική ή λογισμική απομόνωση ενός συστήματος ή δικτύου από μη ασφαλή δίκτυα.

**Προστασία από Απώλεια Δεδομένων (Data Loss Prevention - DLP)**: Τεχνολογίες που αποτρέπουν την απώλεια ή τη διαρροή ευαίσθητων δεδομένων.

www.ncc.cy

NCC
ΕΘΝΙΚΟ ΚΕΝΤΡΟ ΣΥΝΤΟΝΙΣΜΟΥ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ
ΚΥΠΡΟΥ

**Ευαισθητοποίηση σε θέματα Κινδύνων (Risk Awareness)**: Η αναγνώριση και η κατανόηση των κινδύνων από μια οργάνωση ή ένα άτομο σχετικά με την κυβερνοασφάλεια.

**Ανθεκτικότητα στον Κυβερνοχώρο (Cyber Resilience)**: Η ικανότητα ενός οργανισμού να αντιμετωπίζει και να ανακάμπτει από κυβερνοεπιθέσεις.

**Κυβερνοπόλεμος (Cyber Warfare)**: Ο πόλεμος που διεξάγεται στον κυβερνοχώρο, συχνά με στόχο τα δίκτυα και τα συστήματα πληροφοριών.

**Υποκλοπή Κίνησης Δεδομένων (Data Interception)**: Η μη εξουσιοδοτημένη ή κρυφή υποκλοπή δεδομένων που μεταδίδονται μέσω δικτύου ή καναλιού επικοινωνίας.

www.ncc.cy

NCC
ΕΘΝΙΚΟ ΚΕΝΤΡΟ ΣΥΝΤΟΝΙΣΜΟΥ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ
ΚΥΠΡΟΥ

**Breach**: Παραβίαση δεδομένων είναι κάθε περιστατικό ασφαλείας κατά το οποίο μη εξουσιοδοτημένα μέρη αποκτούν πρόσβαση σε ευαίσθητα δεδομένα ή εμπιστευτικές πληροφορίες.

**Περιμετρική Ασφάλεια (Perimeter Security)**: Τα μέτρα που λαμβάνονται για την προστασία των εξωτερικών συνόρων ενός δικτύου ή συστήματος.

**Ανάλυση κίνησης δικτύου (Network Traffic Analysis)**:Η μέθοδος παρακολούθησης της διαθεσιμότητας και της δραστηριότητας του δικτύου για τον εντοπισμό ανωμαλιών, συμπεριλαμβανομένων ζητημάτων ασφάλειας και λειτουργίας.

**Ανάλυση Συμβάντων (Security Event Analysis)**: Η αξιολόγηση και ερμηνεία των γεγονότων που καταγράφονται από συστήματα ασφαλείας για την ανίχνευση ενδεχόμενων προβλημάτων.

NCC
ΕΘΝΙΚΟ ΚΕΝΤΡΟ ΣΥΝΤΟΝΙΣΜΟΥ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ ΚΥΠΡΟΥ

**Διαχείριση Κινδύνων (Risk Management)**: Η διαδικασία αναγνώρισης, αξιολόγησης και διαχείρισης των κινδύνων που σχετίζονται με την κυβερνοασφάλεια.

**Ασφάλεια Κινητών Συσκευών (Mobile Device Security)**: Οι πρακτικές και οι τεχνολογίες που αφορούν την ασφάλεια των κινητών συσκευών, όπως smartphone και tablet.

**Ανάλυση Αναγνώρισης Στοιχείων (Identity Recognition Analysis)**: Η χρήση τεχνολογίας για τον εντοπισμό και τον έλεγχο της ταυτότητας χρηστών.

**Ανίχνευση και απόκριση απειλών (Threat detection and response)**: Η πρακτική του εντοπισμού οποιασδήποτε κακόβουλης δραστηριότητας που θα μπορούσε να θέσει σε κίνδυνο το δίκτυο και, στη συνέχεια, η σύνθεση μιας κατάλληλης απόκρισης για τον μετριασμό ή την εξουδετέρωση της απειλής πριν αυτή μπορέσει να εκμεταλλευτεί τυχόν υπάρχουσες ευπάθειες.

www.ncc.cy

NCC
ΕΘΝΙΚΟ ΚΕΝΤΡΟ ΣΥΝΤΟΝΙΣΜΟΥ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ
ΚΥΠΡΟΥ

Βιβλιογραφία


https://www.cisa.gov

https://www.cisco.com

https://www.cloudflare.com

https://csrc.nist.gov

https://www.enisa.europa.eu

https://www.ibm.com

https://innovationatwork.ieee.org

https://www.kaspersky.com

# Επικοινωνία

NCC
ΕΘΝΙΚΟ ΚΕΝΤΡΟ ΣΥΝΤΟΝΙΣΜΟΥ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ
ΚΥΠΡΟΥ

ΑΝΔΡΕΑ ΧΑΛΙΟΥ 1, 2408 ΕΓΚΩΜΗ, ΛΕΥΚΩΣΙΑ

1447

info@ncc.cy

www.ncc.cy

ΕΠΙΤΡΟΠΟΣ ΕΠΙΚΟΙΝΩΝΙΩΝ | Αρχή Ψηφιακής Ασφάλειας

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE