GDPR
και
Τεχνικά Μέτρα Ασφάλειας Πληροφοριακών Συστημάτων

www.altiusconsultants.gr

Εισηγητής
Νικόλαος Δούλος
IT & Business Development Consultant
n.doulos@altiusconsultants.gr
Mobile : 6936 733 950 tel : 210 60 46 340

Ασφάλεια Πληροφοριών

Το οργανωμένο πλαίσιο από έννοιες, αντιλήψεις, αρχές, πολιτικές, διαδικασίες, τεχνικές και **ΜΕΤΡΑ** , που απαιτούνται για να προστατευτούν οι πληροφορίες, από κάθε σκόπιμη ή τυχαία απειλή.

Κύριες Ιδιότητες της Ασφάλειας Πληροφοριών

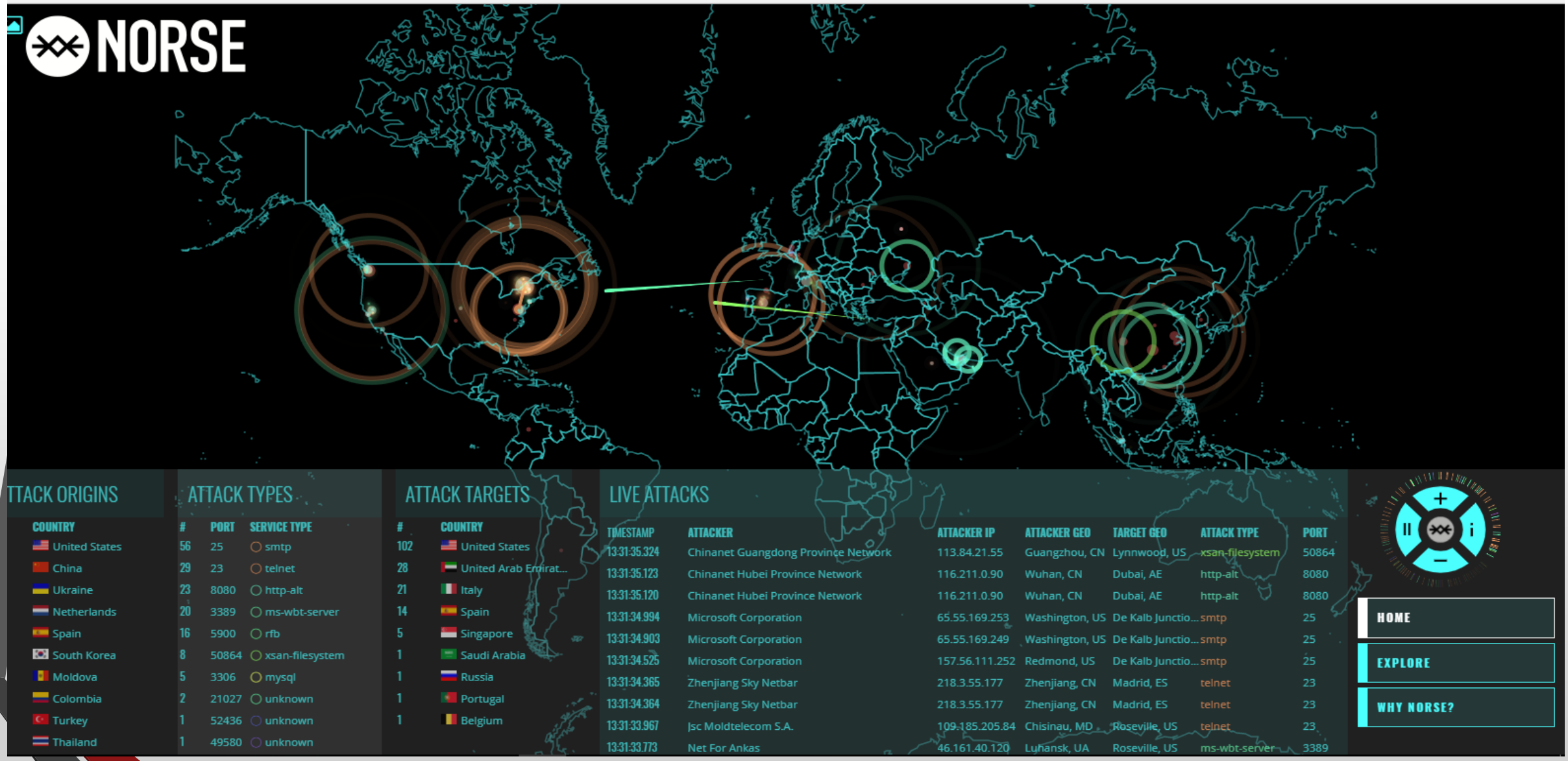
- **Εμπιστευτικότητα (Confidentiality):** Διασφάλιση ότι πρόσβαση στην πληροφορία έχουν μόνο όσοι έχουν κατάλληλη εξουσιοδότηση.
- **Ακεραιότητα (Integrity):** Διασφάλιση ότι η πληροφορία είναι πλήρης, ακριβής και έγκυρη.
- **Διαθεσιμότητα (Availability):** Διασφάλιση ότι η πληροφορία είναι διαθέσιμη κάθε στιγμή που ένας εξουσιοδοτημένος χρήστης επιχειρεί να αποκτήσει πρόσβαση σε αυτή.

Ασφάλεια Πληροφοριών & Συστημάτων

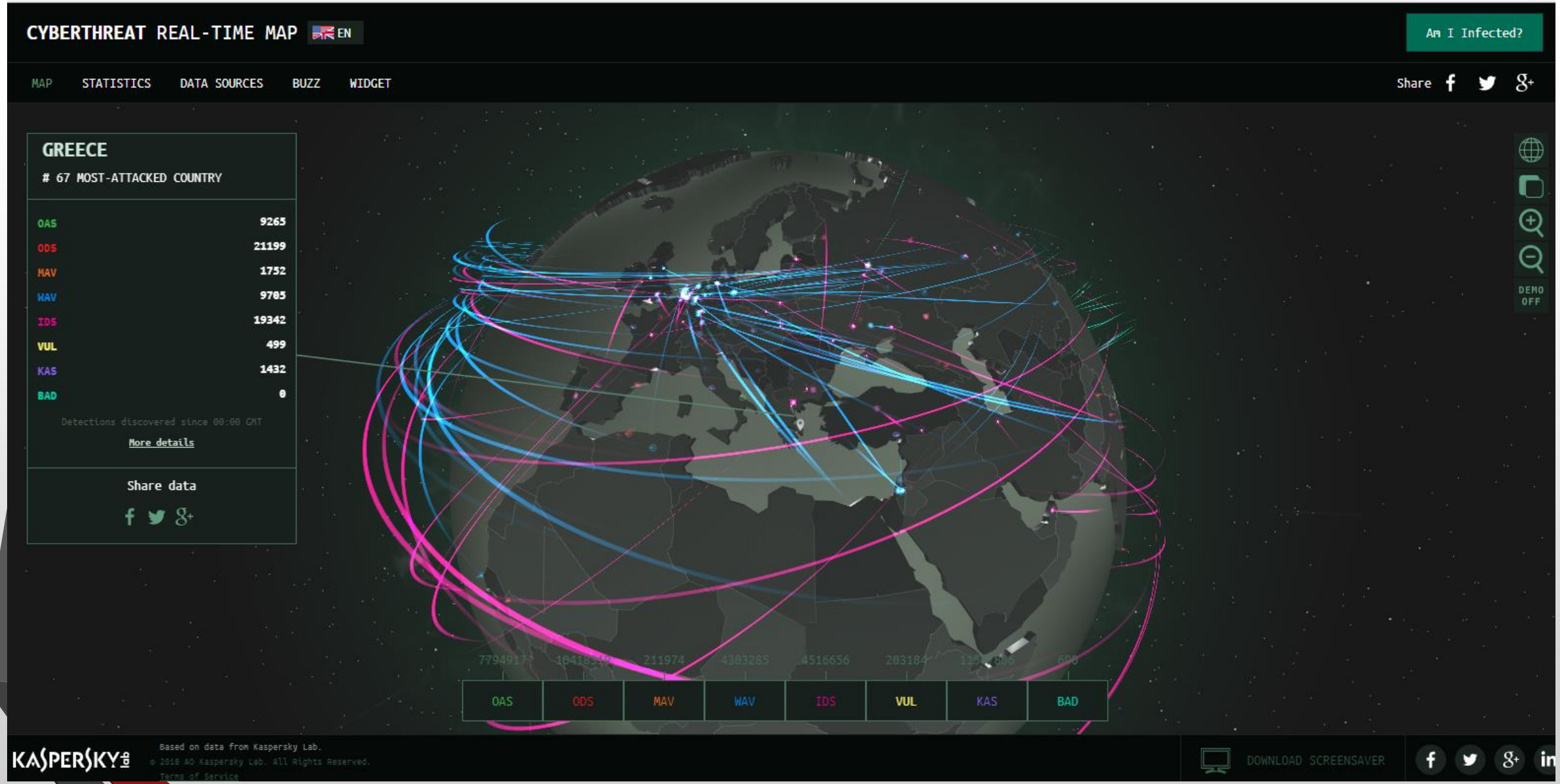
- **Ασφάλεια πληροφοριών:** διατήρηση της εμπιστευτικότητας, της ακεραιότητας και διαθεσιμότητας.
- **Ασφάλεια πληροφοριακών συστημάτων:** προστασία των στοιχείων που συνιστούν ένα πληροφοριακό σύστημα (hardware, software, πληροφορία, άνθρωποι, διαδικασίες).
- Η ασφάλεια **δεν είναι μόνο** τεχνικό ζήτημα! Είναι **ΚΑΙ** τεχνικό ζήτημα!

Μέτρα Ασφάλειας και Σχέδιο Ασφάλειας

- Οι οδηγίες και οι διαδικασίες που περιλαμβάνονται στην Πολιτική Ασφάλειας **υλοποιούνται με την εφαρμογή των μέτρων προστασίας ή ασφάλειας** (security measures, security controls , αντίμετρα - counter measures).
- Η Πολιτική Ασφάλειας μαζί με το σύνολο των μέτρων προστασίας αποτελούν το Σχέδιο Ασφάλειας (Security Plan) για τα πληροφοριακά συστήματα ενός οργανισμού.



http://map.norsecorp.com



http://cybermap.kaspersky.com

Αλληλουχία Μέτρων Προστασίας

Πρόληψη - Prevention

- Penetration Test
- Data Loss Prevention Software (DLP)
- Audit
- GAP Analysis
- Πιστοποίηση
- Ορισμός Πολιτικών και Διαδικασιών
- Επικαιροποίηση Πολιτικών και Διαδικασιών
- Business Continuity Plan – Disaster Recovery Plan (BCP – DRP)

Κατηγορίες Μέτρων Προστασίας Πληροφοριακών Συστημάτων

Κατηγορίες Μέτρων Προστασίας πληροφοριακών Συστημάτων

- Διοικητικά
- Φυσικής Ασφάλειας
- Τεχνικά

Διοικητικά Μέτρα

- Οργάνωση και διαχείριση της Ασφάλειας του ΠΣ
  - Ρόλοι και οι αρμοδιότητες του προσωπικού
  - Ο τρόπος διαχείρισης πληροφοριών
  - Κώδικας δεοντολογίας (εσωτερικών κανόνων)
  - Διαδικασία πρόσληψης και αποχώρησης υπαλλήλου (πχ δέσμευση εμπιστευτικότητας)
  - Διαβάθμιση πληροφοριών
  - Δημιουργία <<κουλτούρας>>
  - Η εκπαίδευση

Παραδείγματα Διοικητικών Μέτρων

- Ορισμός Πολιτικών και Διαδικασιών
- Συμβάσεις Εμπιστευτικότητας και Non Disclosure Agreement (NDA)
  - Με προσωπικό
  - Με εξωτερικούς Προμηθευτές – Συνεργάτες , κυρίως αν έχουν πρόσβαση σε πληροφορίες ή στο ΠΣ (π.χ. εξωτερικοί μηχανογράφοι, διαφημιστικά γραφεία κτλ)
- Εγχειρίδιο οδηγιών ασφάλειας πληροφοριών

Μέτρα Φυσικής Ασφάλειας

- από φυσικές καταστροφές
- ασφάλεια πρόσβασης στις κτιριακές εγκαταστάσεις
- ασφάλεια πρόσβασης υπολογιστικού και δικτυακού εξοπλισμού

Παραδείγματα Μέτρων Φυσικής Ασφάλειας

- Συναγερμός
- Κάμερες / Καταγραφικό.
- Κλειδαριές (με κωδικό ή όχι) για ντουλάπες , συρτάρια κτλ
- Πυρασφάλεια

Παραδείγματα Μέτρων Φυσικής Ασφάλειας

- Διαδικασίες για :
  - Χρήση συσκευών USB εντός του οργανισμού
  - Πρόσβαση στο δίκτυο του οργανισμού.
  - Χρήση wifi
  - Clear Desk – Clear Monitor
- Γενικό Access Control για την πρόσβαση στην εταιρεία.
  - Συσκευές βιομετρικών ελέγχων (δακτυλικό αποτύπωμα, ίριδα ματιού, χαρακτηριστικών προσώπου, φωνής).
  - Μαγνητικές Κάρτες

Παραδείγματα Μέτρων Φυσικής Ασφάλειας

- Server Room με ελεγχόμενη πρόσβαση και προδιαγραφές ασφαλείας.
  - Access Control
  - Σύστημα Ειδοποίησης για Πρόσβαση στο χώρο
  - Σύστημα Ειδοποίησης Περιβαλλοντικών Συνθηκών (θερμοκρασία , υγρασία κτλ)
  - Ειδικό Σύστημα Πυρόσβεσης
- Ορισμός Περιοχών Ελεγχόμενης Πρόσβασης
  - Σήμανση
  - Access Control

Τεχνικά Μέτρα Ασφάλειας

- **Κάλυψη Ευπαθειών.**
- **<<Απόκρουση>> Απειλών.**
- **Κυβερνο-επιθέσεις.**
- **Ηλεκτρονικό Έγκλημα.**
- **Ταυτοποίηση και αυθεντικοποίηση:** Διασφάλιση ότι ο χρήστης που επιχειρεί να αποκτήσει πρόσβαση σε πληροφορία/ σύστημα/ εφαρμογή είναι αυτός που ισχυρίζεται ότι είναι.

Τεχνικά Μέτρα Ασφάλειας

- **Έλεγχος πρόσβασης:** Διασφάλιση ότι ο χρήστης που επιχειρεί να αποκτήσει πρόσβαση σε πληροφορία/ σύστημα/ εφαρμογή είναι εξουσιοδοτημένος γι᾽ αυτή την ενέργεια.
- **Έλεγχος και παρακολούθηση (audit & monitoring):** Παρακολούθηση και καταγραφή των ενεργειών των χρηστών.

Τεχνικά Μέτρα Ασφάλειας

- **Προστασία προσωπικών δεδομένων:** Προστασία των δεδομένων προσωπικού χαρακτήρα και των ευαίσθητων δεδομένων του ατόμου από μη εξουσιοδοτημένη συλλογή, αποθήκευση και επεξεργασία, σύμφωνα με την κείμενη νομοθεσία.
- **Μη αποποίηση ευθύνης:** Διασφάλιση ότι ένας χρήστης δεν μπορεί να αρνηθεί ότι εκτέλεσε μία ενέργεια σχετική με πρόσβαση/ επεξεργασία σε πληροφορία/ σύστημα / εφαρμογή.

Παραδείγματα Τεχνικών Μέτρων Ασφάλειας

- Password Policy
- Anti-virus, Anti-Malware, Anti-Spyware
- Active Directory
- Δικαιώματα Χρηστών στους πόρους του ΠΣ

Παραδείγματα Τεχνικών Μέτρων Ασφάλειας

- Κλείδωμα θυρών USB
- Backup
- Τείχος Προστασίας - Firewalls

Παραδείγματα Τεχνικών Μέτρων Ασφάλειας

- Software Updates
  - Antivirus
  - Operation Systems
  - Applications
- Log Files
- Σύστημα Ανίχνευσης Εισβολής (Intrusion Detection System – IDS)

Παραδείγματα Τεχνικών Μέτρων Ασφάλειας

- Εικονικό Ιδιωτικό Δίκτυο (Virtual Private Network – VPN)
  - Απομακρυσμένη Πρόσβαση.
- Ψηφιακές Υπογραφές
- Cryptography
- Πρωτόκολλα SSL
- Monitoring Software


Copyright Altius Consultants 2018

Σας Ευχαριστώ.

Νικόλαος Δούλος
IT & Business Development Consultant
Email : n.doulos@altiusconsultants.gr
Web Site : www.altiusconsultants.gr