

# ***GDPR*** ***και*** ***Τεχνικά Μέτρα Ασφάλειας*** ***Πληροφοριακών Συστημάτων***



[www.altiusconsultants.gr](http://www.altiusconsultants.gr)

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

Copyright Altius Consultants 2018

# 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

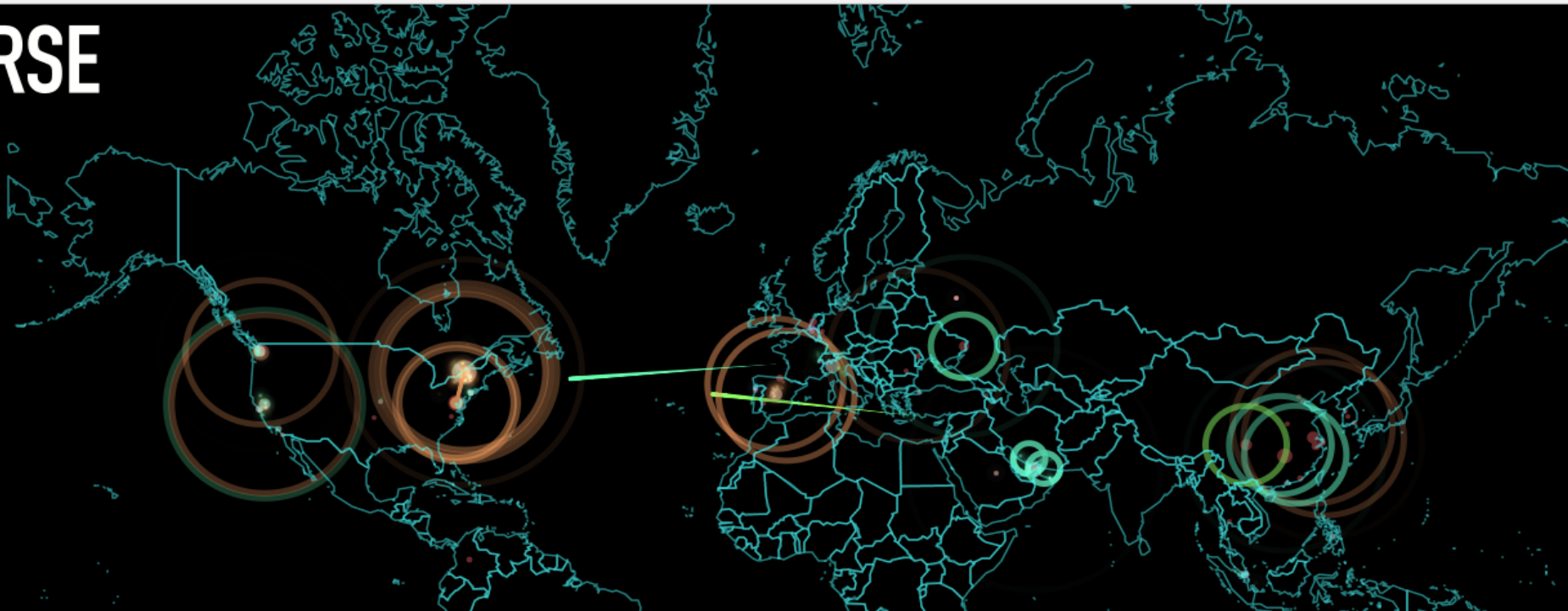
- **Εμπιστευτικότητα (Confidentiality):** Διασφάλιση ότι πρόσβαση στην πληροφορία έχουν μόνο όσοι έχουν κατάλληλη εξουσιοδότηση.
- **Ακεραιότητα (Integrity):** Διασφάλιση ότι η πληροφορία είναι πλήρης, ακριβής και έγκυρη.
- **Διαθεσιμότητα (Availability):** Διασφάλιση ότι η πληροφορία είναι διαθέσιμη 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.



### ATTACK ORIGINS

COUNTRY	#	PORT	SERVICE TYPE
United States	56	25	smtp
China	29	23	telnet
Ukraine	23	8080	http-alt
Netherlands	20	3389	ms-wbt-server
Spain	16	5900	rfb
South Korea	8	50864	xsan-filesystem
Moldova	5	3306	mysql
Colombia	2	21027	unknown
Turkey	1	52436	unknown
Thailand	1	49580	unknown

### ATTACK TYPES

### ATTACK TARGETS

#	COUNTRY
102	United States
28	United Arab Emirates
21	Italy
14	Spain
5	Singapore
1	Saudi Arabia
1	Russia
1	Portugal
1	Belgium

### LIVE ATTACKS

TIMESTAMP	ATTACKER	ATTACKER IP	ATTACKER GEO	TARGET GEO	ATTACK TYPE	PORT
13:31:35.324	Chinanet Guangdong Province Network	113.84.21.55	Guangzhou, CN	Lynnwood, US	xsan-filesystem	50864
13:31:35.123	Chinanet Hubei Province Network	116.211.0.90	Wuhan, CN	Dubai, AE	http-alt	8080
13:31:35.120	Chinanet Hubei Province Network	116.211.0.90	Wuhan, CN	Dubai, AE	http-alt	8080
13:31:34.994	Microsoft Corporation	65.55.169.253	Washington, US	De Kalb Junctio...	smtp	25
13:31:34.903	Microsoft Corporation	65.55.169.249	Washington, US	De Kalb Junctio...	smtp	25
13:31:34.525	Microsoft Corporation	157.56.111.252	Redmond, US	De Kalb Junctio...	smtp	25
13:31:34.365	Zhenjiang Sky Netbar	218.3.55.177	Zhenjiang, CN	Madrid, ES	telnet	23
13:31:34.364	Zhenjiang Sky Netbar	218.3.55.177	Zhenjiang, CN	Madrid, ES	telnet	23
13:31:33.967	Jsc Moldtelecom S.A.	109.185.205.84	Chisinau, MD	Roseville, US	telnet	23
13:31:33.773	Net For Ankas	46.161.40.120	Luhansk, UA	Roseville, US	ms-wbt-server	3389



- HOME
- EXPLORE
- WHY NORSE?

Copyright Altius Consultants 2018

<http://map.norsecorp.com>

### GREECE

# 67 MOST-ATTACKED COUNTRY

OAS	9263
ODS	21199
MAV	1752
WAV	9785
IDS	19342
VUL	499
KAS	1432
BAD	0

Detections discovered since 00:00 GMT

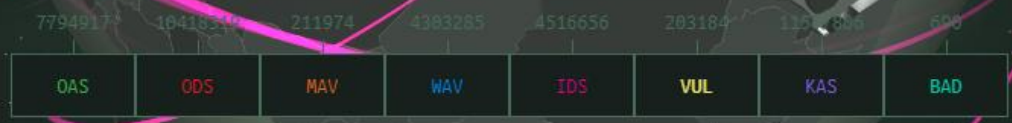
[More details](#)

Share data



  
  
  
  
DEMO OFF



# Αλληλουχία Μέτρων Προστασίας

Πρόληψη  
Prevention

Ανίχνευση  
Detection

Αντίδραση  
Reaction



# 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](mailto:n.doulos@altiusconsultants.gr)  
Web Site : [www.altiusconsultants.gr](http://www.altiusconsultants.gr)

