Το τοπίο των κυβερνοαπειλών: αναγκαιότητα η πολυτέλεια;

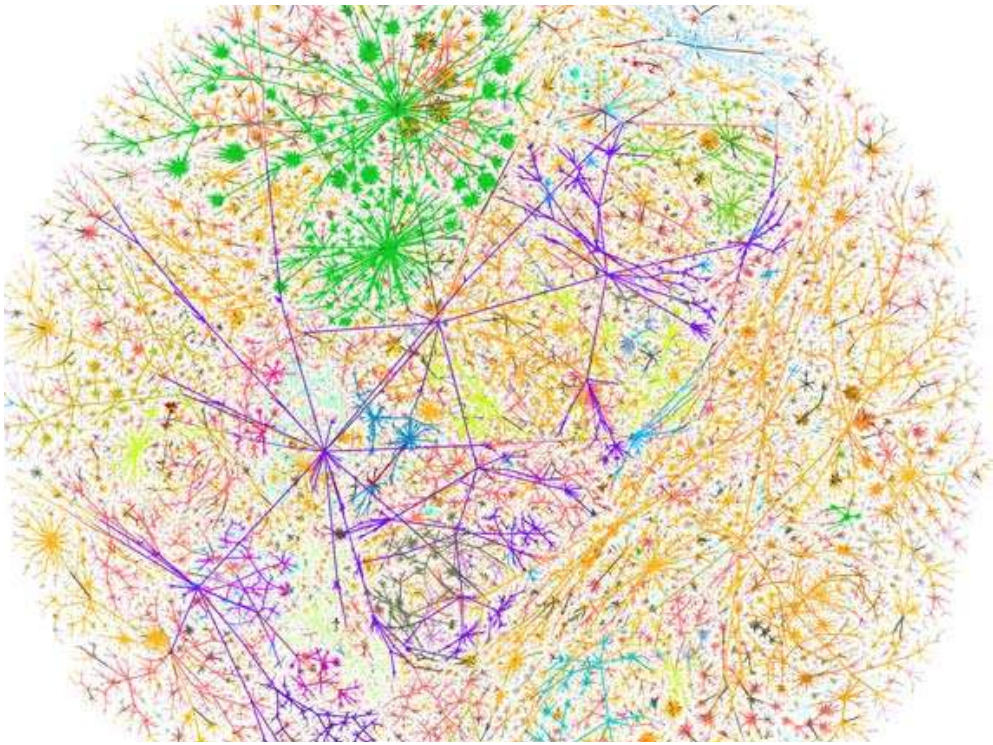
Λ. Μαρίνος | ENISA

Απόρρητο των επικοινωνιών : σύγχρονες προκλήσεις, 8 Μαΐου 2018

European Union Agency for Network and Information Security

Τι είναι ο κυβερνοχώρος?

Όχι μόνο Υπολογιστές, Τηλεπικοινωνίες, Λογισμικό, κ.λπ.



..αλλά η δυνατότητα της δυναμικής διασύνδεσης τους με σκοπό την ανταλλαγή δεδομένων.

Ο κυβερνοχώρος τόπος εγκλημάτων..

… κυβερνοχώρος αναγνωρίζεται σαν χώρος για εγκληματικές πράξεις, πεδίο επιχειρήσεων, πεδίο μάχης..

….. μόνο που….

τα άλλα πεδία έχουν συγκεκριμένα σύνορα/οριοθέτηση…

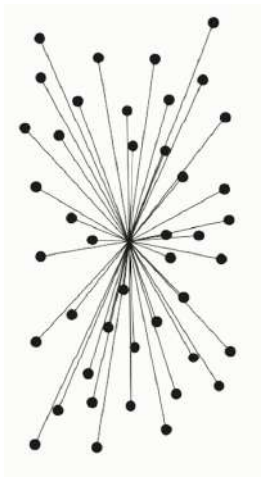
στον κυβερνοχώρο σύνορο είναι **Κάθε IP** (κάθε μια συσκευή)!!!

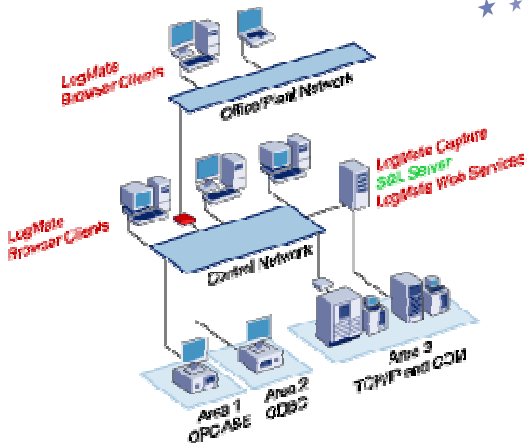
Το επίπεδο κινδύνου στον κυβερνοχώρο

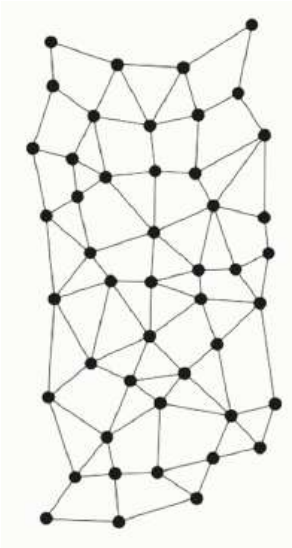
Ποιος επιτίθεται σε ποιον/σε τι?

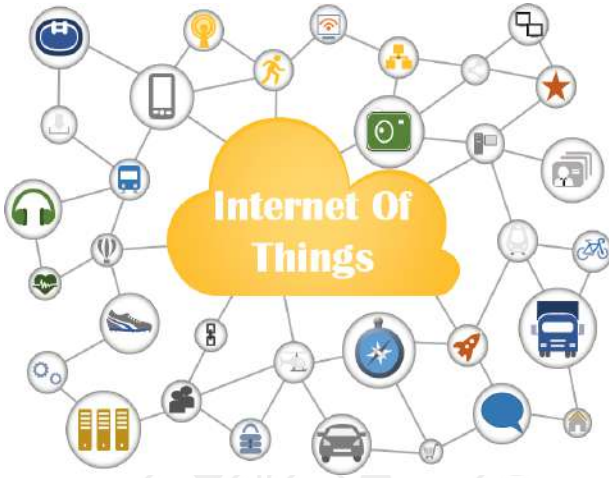
Με κύριο ενδιαφέρον χρήση, αντιγραφή, αποθήκευση, σβήσιμο, ανταλλαγή πληροφοριών

… αλλαγές στην αρχιτεκτονική…









Τα “συστατικά” των κυβερνοαπειλών..

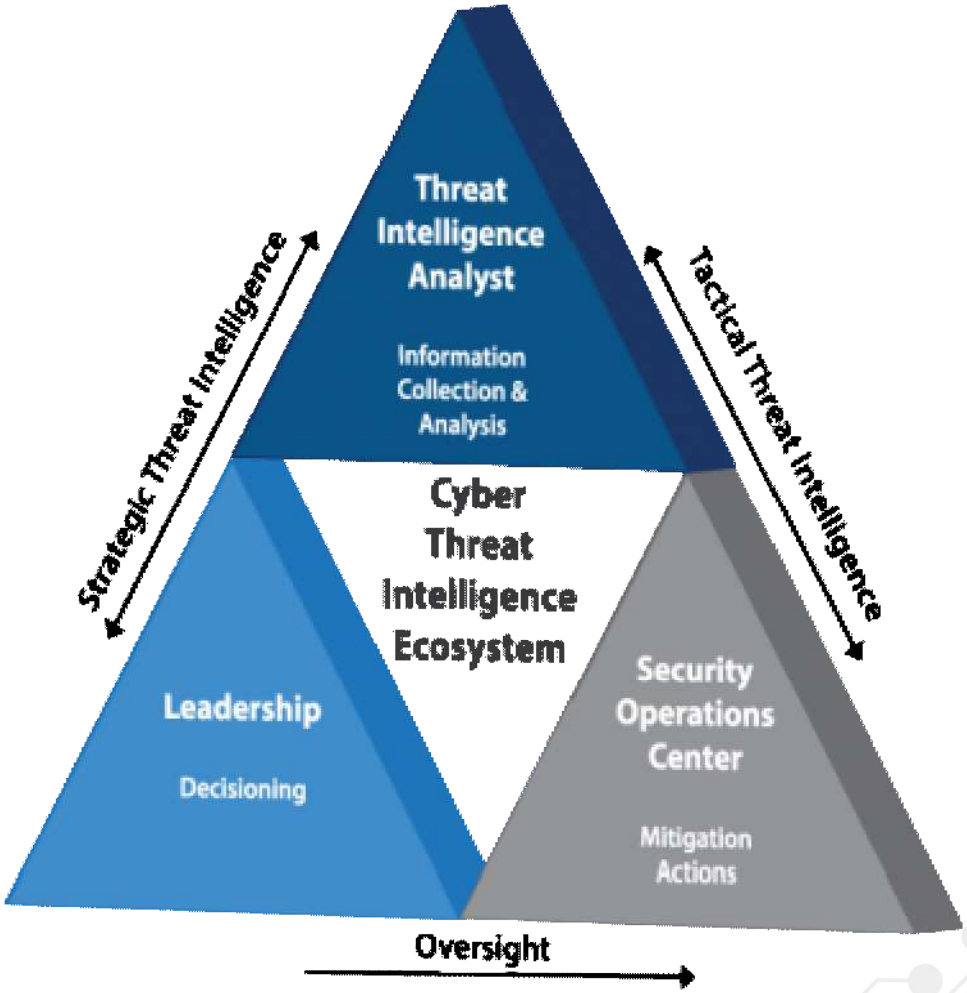
- Τα εργαλεία επίθεσης
- Τα τρωτά/ασθενή σημεία του θύματος
- Η στρατηγική εκτέλεσης της επίθεσης
- Ο τελικός σκοπός της επίθεσης
- Τα κίνητρα του επιτιθέμενου
- Το επίπεδο ικανοτήτων του επιτιθέμενου

Ποια είναι τα “εργαλεία” των επιθέσεων?

Πολλαπλά και πολυποίκιλα

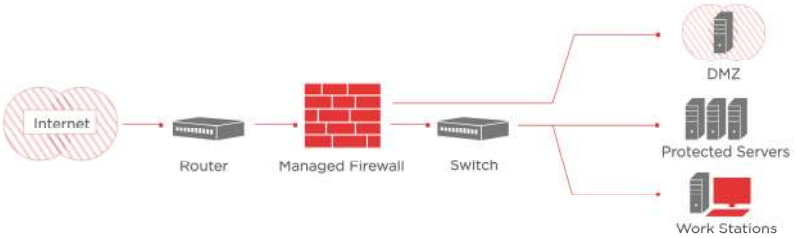
Top Threats 2017	Assessed Trends 2017	Change in ranking
1. Malware	→	→
2. Web based attacks	↑	→
3. Web application attacks	↑	→
4. Phishing	↑	↑
5. Spam	↑	↑
6. Denial of service	↑	↓
7. Ransomware	↑	↑
8. Botnets	↑	↓
9. Insider threat	→	→
10. Physical manipulation/damage/ theft/loss	→	→

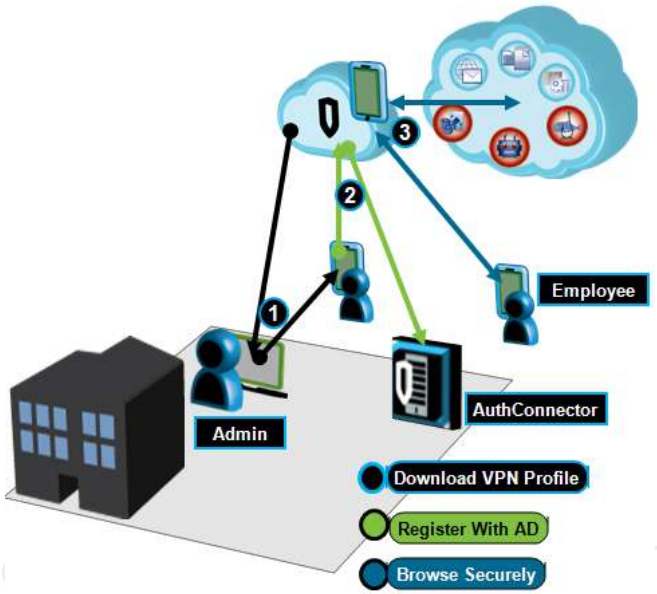
Ο σκοπός του οικοσυστήματος



https://www.nuspire.com/technologies/threat-intelligence/

Χρήση πληροφορίας κυβερνοαπειλών...





Η ανάλυση κυβερνοαπειλών είναι αναγκαιότητά

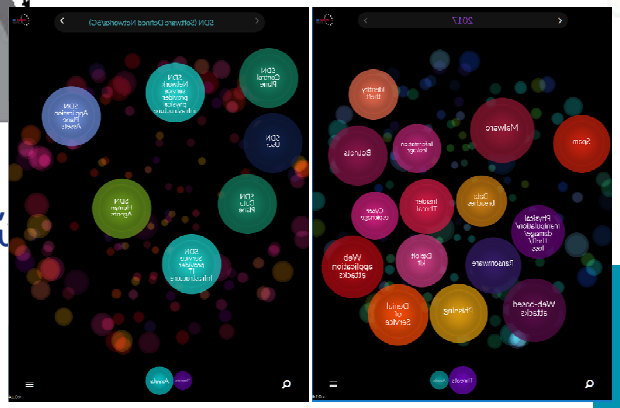
Για να προσαρμόσουμε την ταχύτητα αντίδρασης …

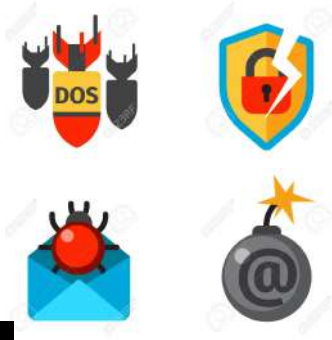
στα αναγκαία για την εποχή επίπεδα…

Το τοπίο κυβερνοαπειλών του ENISA..

Τεχνικές στην ανάλυση απειλώ

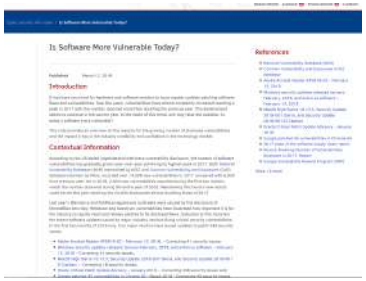
Εργαλείο online



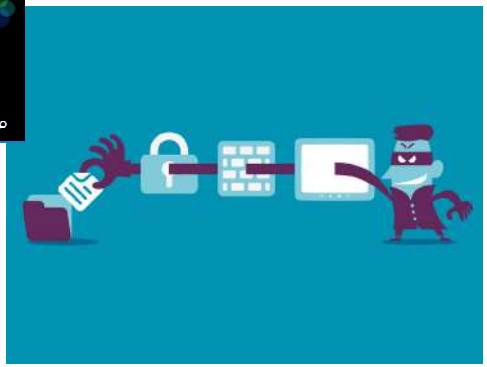


15 βασικές κυβερνοαπειλές

Κακόβουλοι παράγοντες



15θημερο δελτίο επίκαιρων απειλών



Μέθοδοι επιθέσεων

Τι λένε οι στατιστικές?

Από τα καταγεγραμμένα κυβερνο-περιστατικά:

- Κυβερνοέγκλημα 75%
- Δράση μυστικών υπηρεσιών 20%
- Υπόλοιπα 5% (εμπεριέχει κυβερνοπόλεμο)

Πιστεύεται ότι μόλις 25-50% των συμβάντων δηλώνονται η γίνονται γνωστά!

Σπουδαιότερες αναδυόμενες κυβερνοαπειλές….

- Διαφορές ταχυτήτων μεταξύ επιθέσεων και άμυνας
  - Έλλειψη επενδύσεων
  - Έλλειψη ανθρωπ. δυναμικού
  - Έλλειψη ικανοτήτων
- Εμπορικοποίηση των τρωτών/ασθενών σημείων
  - “Θεσμικοί επενδυτές”
  - Κυβερνοέγκλημα
- Απειλές των εκάστοτε δημοκρατιών
  - Απόκτηση εμπιστευτικών δεδομένων
  - Επιρροή στα μέσα κοινωνικής δικτύωσης
- Απειλές των κρίσιμων υποδομών
  - Αντιμετώπιση μόνιμων απειλών (APT)
  - Διασφάλιση πολύπλοκων υποδομών

Η ανάλυση κυβερνοαπειλών είναι βασικό εργαλείο...

.. σίγουρα ήρθε για να μείνει

Ευχαριστώ για την προσοχή σας!

PO Box 1309, 710 01 Heraklion, Greece

Tel: +30 28 14 40 9710

info@enisa.europa.eu

www.enisa.europa.eu

Χρήσιμοι σύνδεσμοι

ENISA Threat Landscape:

https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2017

ENISA online tool:

https://etl.enisa.europa.eu

ENISA Infonotes:

https://www.enisa.europa.eu/publications/info-notes#c5=2008&c5=2018&c5=false&c2=infonote_publication_date&reversed=on&b_start=0

CTI EU:

https://www.enisa.europa.eu/events/cti-eu-event

ENISA NIS Summer School:

https://nis-summer-school.enisa.europa.eu/

EU NIS Directive:

https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive

EU takes action on fake news:

http://europa.eu/rapid/press-release_MEMO-18-3371_en.htm