«Αρμοδιότητες ΔΙ.Δ.Η.Ε. σε Περιστατικά Ασφάλειας ICT – Ενέργειες πρώτων ανταποκριτών"

Βασίλειος Παπακώστας

Διευθυντής Διεύθυνσης Δίωξης Ηλεκτρονικού Εγκλήματος

Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος

- Αυτοτελής Κεντρική Υπηρεσία
- Υπαγωγή απευθείας στον κ. Αρχηγό της Ελληνικής Αστυνομίας
- Έδρα: Αθήνα
- Υποδιεύθυνση Βορείου Ελλάδος – Θεσσαλονίκη
- Προσωπικό γενικών & ειδικών καθηκόντων

Συνεργασίες

Εθνικό επίπεδο

- Λοιπές Υπηρεσίες ΕΛ.ΑΣ.
- Δικαστικές Αρχές
- Εθνική Αρχή Κυβερνοασφάλειας
- ΓΕΕΘΑ (ΔΙ.ΚΥΒ.)
- Ε.Υ.Π. / Δνση Κυβερνοχώρου
- Ανεξάρτητες Αρχές
- Ακαδημαϊκά Ιδρύματα

Ευρωπαϊκό & Διεθνές Επίπεδο

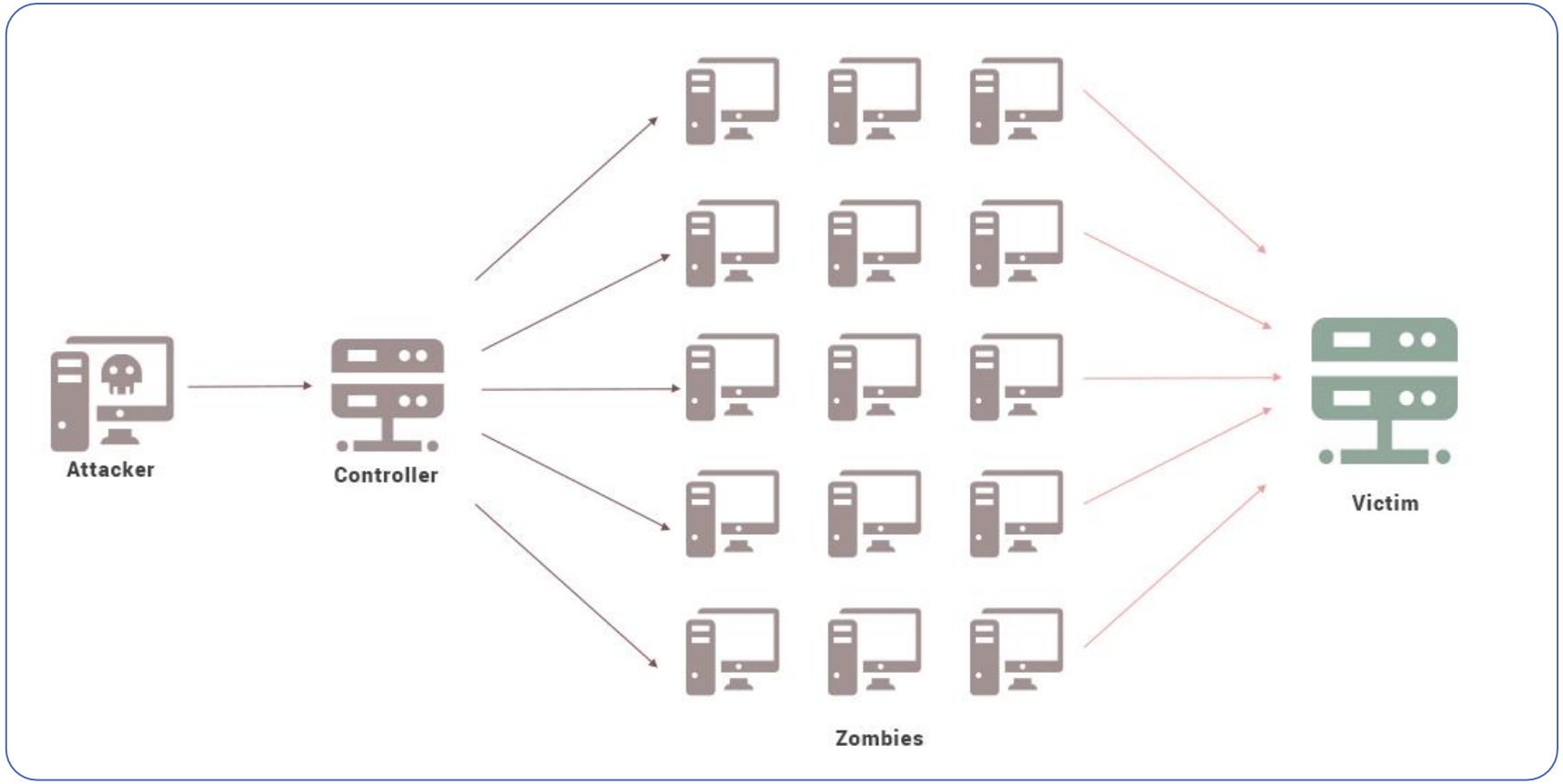
- SELEC
- Europol & European Cybercrime Centre (EC3)
- INTERPOL
- NCMEC

Επιθέσεις σε πληροφοριακά συστήματα

- Αρμοδιότητα για ποινική διερεύνηση, σύμφωνα με άρθρο 31 του Π.Δ. 178/2014
- Τμήμα Ασφάλειας Ηλεκτρονικών και Τηλεφωνικών Επικοινωνιών & Προστασίας Λογισμικού & Πνευματικών Δικαιωμάτων
- Συνεργασία με Εθνική Αρχή Κυβερνοασφάλειας, ΓΕΕΘΑ (CSIRT), Διεύθυνση Κυβερνοχώρου της Ε.Υ.Π.
- Εσωτερικά: Ομάδα Άμεσης Ανταπόκρισης
- Ομάδα Ασφαλείας IT του φορέα - στόχου

Τρέχουσες Απειλές για τους Οργανισμούς

Europol – European Cybercrime Centre



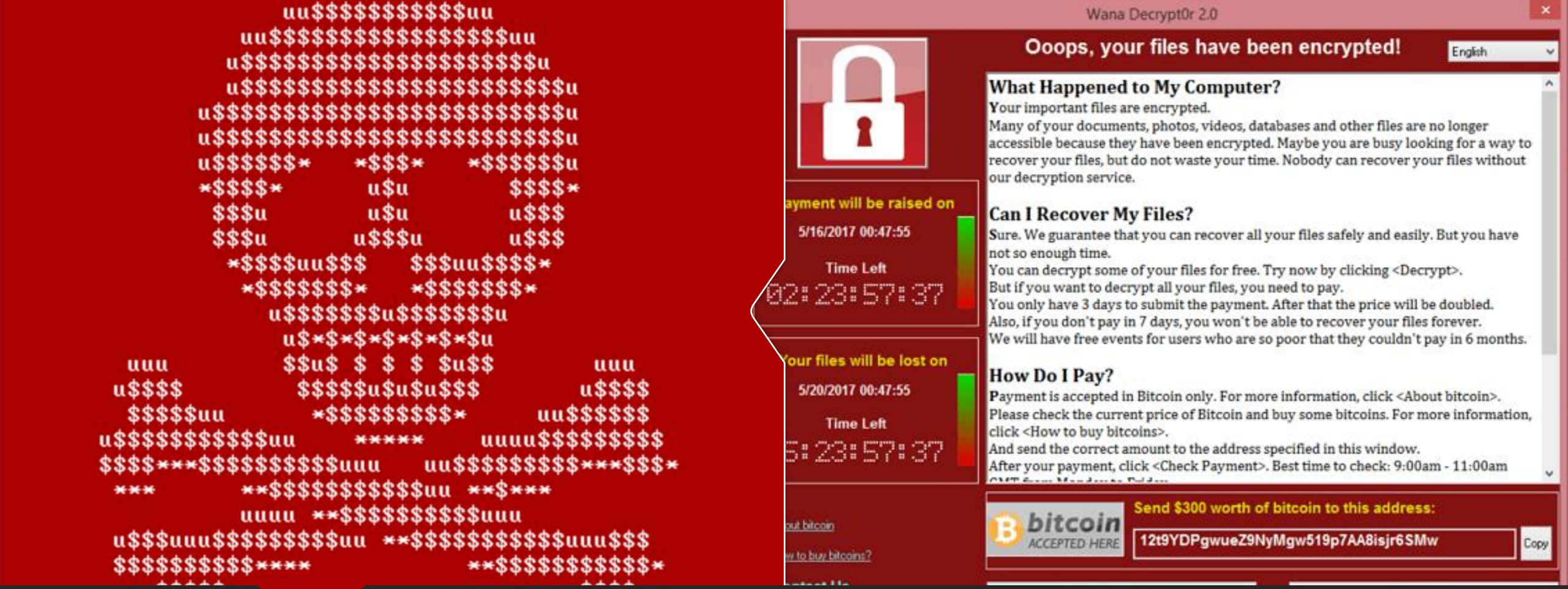
Επιθέσεις τύπου DDOS

Op. POWER OFF

- Cybercrime-as-a-service
- Εργαλεία διαθέσιμα για «ενοικίαση»
- Πραγματοποίηση επιθέσεων χωρίς ιδιωτικό εξοπλισμό ή εξειδικευμένες τεχνικές γνώσεις
- Εμπλεκόμενοι χρήστες στην Ελλάδα


AYYILDIZ TİM - 2
CUMHURİYET ;
Fikren, İlmen Ve Bedenen Kuvvetli Ve Yüksek Karakterli Muhafızlar İster
CEDKAN BİR YAFES | LEDÜN ABDAL | KEREM SAH NOYAN
İNTEGRAL | EFRAİM | TOPALOSMANAĞA | ŞAHPAŞA | DENGİZER | AKBELŞAH
YILDIRIM ORDULARI BIRIM KOMUTANLIĞI

Defacement


Wana Decrypt0r 2.0
Ooops, your files have been encrypted!
English
What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.
Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.
How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am
ayment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37
our files will be lost on
5/20/2017 00:47:55
Time Left
5:23:57:37
Send $300 worth of bitcoin to this address:
bitcoin ACCEPTED HERE
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
Copy

Ransomware

Κακόβουλο Λογισμικό

Social Engineering

Ζητήματα Νομοθεσίας

Ισχύον πλαίσιο

- Σύμβαση του Συμβουλίου της Ευρώπης για το Έγκλημα στον Κυβερνοχώρο (Βουδαπέστη, 2001)
- Οδηγία 2013/40/ΕΕ για τις επιθέσεις κατά συστημάτων πληροφοριών
- Κυρώθηκαν με νόμο 4411/2016 και προστέθηκαν σχετικά άρθρα στον Ποινικό Κώδικα
- Ωστόσο, από το νέο Ποινικό Κώδικα (Ν. 4619/2019) απουσιάζει σημαντικός αριθμός αδικημάτων

Σημείο Επαφής 24/7

Για την καταπολέμηση του εγκλήματος στον κυβερνοχώρο, απαιτείται διεθνής συνεργασία μεταξύ δικαστικών αρχών και αρχών επιβολής του νόμου. Κάθε Χώρα θα πρέπει:

- Να έχει λειτουργικό εθνικό σημείο επαφής
- Να χρησιμοποιεί το υπάρχον δίκτυο των σημείων επαφής που είναι διαθέσιμο σε 24ωρη βάση και τις επτά ημέρες της εβδομάδας
- Να ανταποκρίνεται σε επείγοντα αιτήματα για βοήθεια εντός 8 ωρών προκειμένου να δηλώσουν αν και πότε θα μπορέσουν να απαντήσουν
- Να διασφαλίζει την παροχή άμεσης συνδρομής σε περιπτώσεις έρευνας ή δίωξης αναφορικά με ποινικά αδικήματα σχετιζόμενα με συστήματα και δεδομένα υπολογιστή ή με σκοπό τη συλλογή αποδεικτικών στοιχείων.

Ευρωπαϊκή Εντολή Έρευνας

- Επίσπευση διαδικασιών δικαστικής συνδρομής
- Άμεση συνεργασία μεταξύ Κρατών – Μελών της Ε.Ε.
- Αιτήματα για ανακριτικές πράξεις που αφορούν θύματα ή δράστες σε άλλες χώρες

Άρθρο 38 - ΚΠΔ – Υποχρέωση ανακοίνωσης αξιόποινης Πράξης

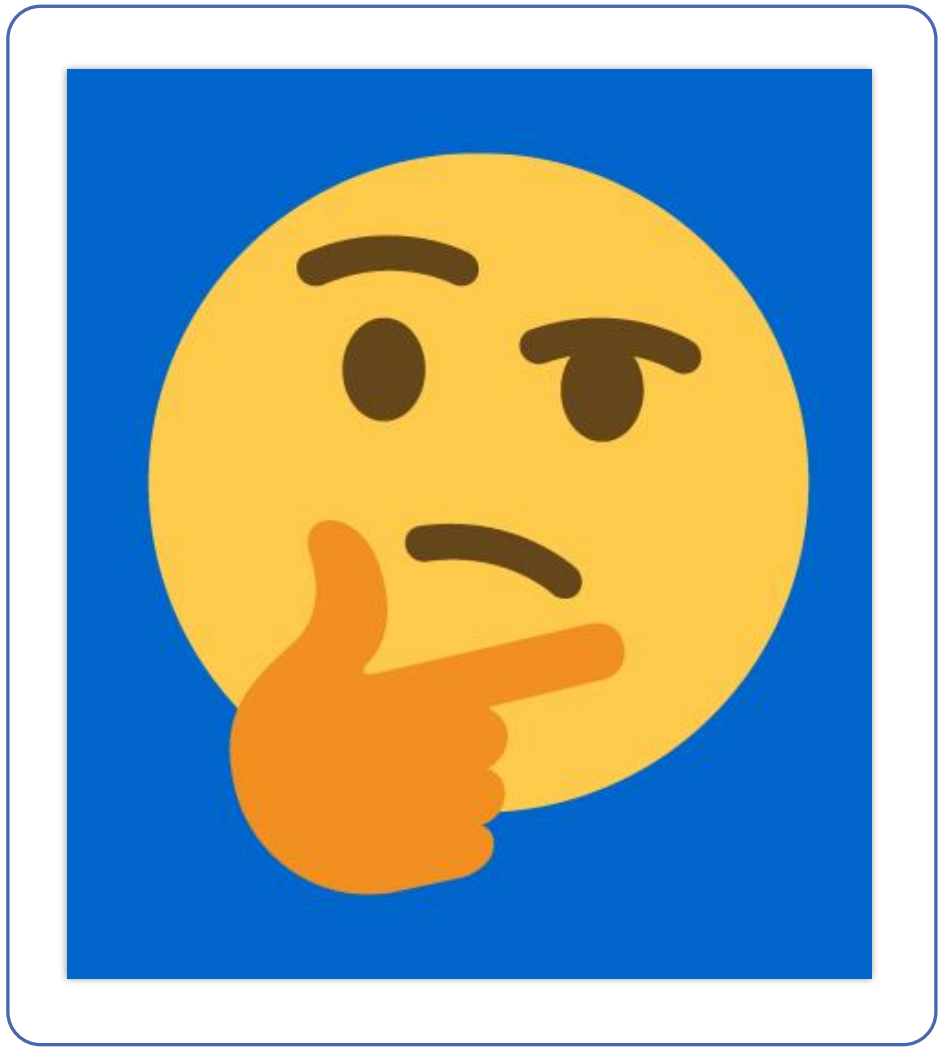
- 1. Οι ανακριτικοί υπάλληλοι οφείλουν να ανακοινώσουν χωρίς χρονοτριβή στον αρμόδιο εισαγγελέα οτιδήποτε πληροφορούνται με κάθε τρόπο για αξιόποινη πράξη που διώκεται αυτεπαγγέλτως.
- 2. **Οι υπόλοιποι δημόσιοι υπάλληλοι**, καθώς και εκείνοι στους οποίους ανατέθηκε προσωρινά δημόσια υπηρεσία, έχουν την ίδια υποχρέωση για τις αξιόποινες πράξεις της παρ. 1, αν πληροφορήθηκαν γι' αυτές κατά την εκτέλεση των καθηκόντων τους.
- 3. Η ανακοίνωση γίνεται **γραπτώς και πρέπει να περιέχει όλα τα στοιχεία** που υπάρχουν και αφορούν την αξιόποινη πράξη, τους δράστες και τις αποδείξεις

Το πρόβλημα

- Δεν υπάρχουν συγκεκριμένες νομικές διατάξεις σχετικά με τη συλλογή, το χειρισμό και την εγκυρότητα των ψηφιακών μέσων και των ψηφιακών αποδείξεων στην ανακριτική – δικαστική διαδικασία.
- Η ποικιλομορφία και ανομοιογένεια των υποδομών (υλικό και λογισμικό) στον δημόσιο τομέα.
- Το μεγάλο εύρος των τεχνικών που χρησιμοποιούν οι κακόβουλοι χρήστες για να εκτελέσουν κυβερνοεπιθέσεις εναντίον των πληροφοριακών μας συστημάτων
- Η ευρηματικότητα των κακόβουλων χρηστών

Συνέπειες

- Έλλειψη προτυποποίησης και αδυναμία δημιουργίας ενός πλαισίου έγκυρων και αποδεκτών τρόπων ενεργειών.
- Το προσωπικό ενεργεί κατά το δοκούν
- Χρήση αυτοσχέδιων εργαλείων



Πρώτοι Ανταποκριτές – Ενέργειες - Συλλογή ψηφιακών Αποδείξεων

Προσέγγιση

- Προετοιμασία του οργανισμού για την αντιμετώπιση των απειλών.
- Υιοθέτηση τεχνικών και οργανωτικών μέτρων
- Συλλογή και ανάλυση πληροφοριών από ανοιχτές πηγές του διαδικτύου
- Εκπαίδευση – Ενημέρωση Προσωπικού
- Αντιμετώπιση περιστατικών ασφαλείας από:
  - **Υπεύθυνοι πληροφοριακών συστημάτων**
  - Ομάδες αντιμετώπισης περιστατικών ασφαλείας - Computer Emergency Response Teams (CERTs) – Computer Security Incident Response Teams (CSIRTs) σε κυβερνητικό ή εταιρικό επίπεδο
  - Διωκτικές Αρχές (Law Enforcement)

Ομάδες CSIRT

- Οι ομάδες CSIRT θα πρέπει να αποτελούνται από ειδικούς σε Digital Forensics
- Για τη συλλογή των δεδομένων θα πρέπει να χρησιμοποιούνται εργαλεία – λογισμικά που είναι έγκυρα (validated), να μπορούν να αναπαραχθούν (reproducible) και να επαναληφθούν (repeatable). Δηλαδή η χρήση τους να οδηγεί στο ίδιο αποτέλεσμα αν χρησιμοποιηθούν με την ίδια μέθοδο, πάνω στα ίδια αντικείμενα, από ένα άτομο.
- Να διασφαλίζεται η ακεραιότητα (integrity) και η αποδεκτότητα (admissibility) των δεδομένων σε κάθε περίπτωση και σε κάθε στάδιο συλλογής τους.
- Δεν επιτρέπεται σε κανένα τρίτο πρόσωπο εκτός της ομάδας CSIRT να επεμβαίνει στο σύστημα και στα δεδομένα προς συλλογή όταν υπάρχει περιστατικό ασφαλείας.

Ομάδες CSIRT

- Να ενημερώνονται για νέες βέλτιστες πρακτικές από ευρωπαϊκούς οργανισμούς (π.χ. ENISA)
- Να ακολουθούν διεθνή πρότυπα (Computer Security Incident Handling Guide από NIST – National Institute Standards and Technology)
- Οι ομάδες CSIRT να βρίσκονται σε στενή συνεργασία με τις Αρχές Επιβολής του Νόμου.

Αντιμετώπιση Περιστατικών Ασφαλείας (Incident Response) (1/3)

- **Όσοι εμπλέκονται στην αντιμετώπιση των περιστατικών ασφαλείας πρέπει να ενεργούν προς την διαφύλαξη των κατωτέρω αρχών:**
- Άμεση ενημέρωση αρμόδιων Αρχών και στελεχών του Οργανισμού
- Περιορισμός επιπλέον ζημίας από το συγκεκριμένο περιστατικό
- Διαφύλαξη των αποδεικτικών στοιχείων και ενδείξεων που σχετίζονται με τις οντότητες που ευθύνονται για το περιστατικό ασφαλείας (κακόβουλοι χρήστες και λογισμικά, ελλιπή μέτρα ασφαλείας, εσωτερικές απειλές)
- Ενέργειες προς Ανίχνευση, Αντιμετώπιση και Ανάκαμψη των πόρων από το περιστατικό ασφαλείας

Αντιμετώπιση Περιστατικών Ασφαλείας (Incident Response) (2/3)

- Να αποφεύγεται η αλλοίωση των δεδομένων κατά τη διάρκεια της συλλογής τους, σε διαφορετική περίπτωση να αναγράφεται σε σχετική αναφορά.
- Να χρησιμοποιούνται εργαλεία συλλογής που αφήνουν όσο το δυνατόν λιγότερα ίχνη στο σύστημα (portable εργαλεία).
- Να λαμβάνονται αντίγραφα των αρχείων καταγραφής του συστήματος ή και των λογισμικών διαχείρισης δεδομένων και να συνοδεύονται από σχετικό ψηφιακό αποτύπωμα (hash value).

Αντιμετώπιση Περιστατικών Ασφαλείας (Incident Response) (3/3)

- Να καταγράφονται όλες οι ενέργειες που πραγματοποιούνται και να παραδίδονται μαζί με τα υπό εξέταση πειστήρια στις υπηρεσίες επιβολής του Νόμου (LEA).
- Είναι σημαντικό να αποδεικνύεται η αντικειμενικότητα, η λογική αλληλουχία και η ακεραιότητα των αποδεικτικών στοιχείων.
- Είναι, επίσης, απαραίτητη η λεπτομερής παρουσίαση της διαδικασίας απόκτησης των στοιχείων αυτών, επιδεικνύοντας όλες τις διεργασίες μέσω των οποίων αυτά αποκτήθηκαν.

Ευχαριστώ για την προσοχή σας!

Βασίλειος Παπακώστας – ccu@cybercrimeunit.gov.gr