ΑΚΑΔΗΜΙΑ ΠΕΡΙΦΕΡΕΙΑΣ ΑΝΑΤΟΛΙΚΗΣ ΜΑΚΕΔΟΝΙΑΣ ΘΡΑΚΗΣ 2017-2018

ΕΞΙΧΝΙΑΣΗ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

Βασικές Έννοιες

Βασίλης Χατζής
Δρ. Πληροφορικής
ΤΕΙ ΑΜΘ

Θα μιλήσουμε για...

- τις βασικές αρχές της ηλεκτρονικής εγκληματολογίας,
- τα είδη και τις μορφές των ηλεκτρονικών εγκλημάτων,
- την έννοια, τον τρόπο απόκτησης και διαχείρισης των ψηφιακών αποδεικτικών στοιχείων,
- τα λογισμικά και τα εργαλεία που βοηθάνε στην εξιχνίαση ηλεκτρονικών εγκλημάτων
- το κόστος των ηλεκτρονικών εγκλημάτων

Εγκληματολογική Επιστήμη

Η *Εγκληματολογική Επιστήμη* (*Forensic Science*), ασχολείται με την ανακάλυψη, ανάλυση και νομική τεκμηρίωση των αποδείξεων, που συνδέουν μια αξιόποινη πράξη με ένα πρόσωπο ή γενικότερα πρόσωπα και αποδεικτικά στοιχεία.

Η ανάλυση του DNA και η εξέταση των δακτυλικών αποτυπωμάτων είναι μερικές από τις δυνατότητες που χρησιμοποιεί η επιστήμη αυτή.

Ηλεκτρονική Εγκληματολογία

Ο πιο αποδεκτός ορισμός της *Ηλεκτρονικής Εγκληματολογίας* (*Digital Forensic*) προκύπτει από τον ορισμό της *εγκληματολογικής επιστήμης των υπολογιστών* (*Forensic Computing Science*).

Η εγκληματολογική επιστήμη υπολογιστών, είναι "η επιστήμη που ασχολείται με την αναγνώριση, διατήρηση, ανάλυση και παρουσίαση ψηφιακών αποδείξεων κατά τρόπο νομικά αποδεκτό"

Ηλεκτρονικό έγκλημα

- Έγκλημα είναι μια επιθετική πράξη εναντίον της κοινωνίας ή ενός ατόμου που παραβιάζει τουλάχιστον έναν νόμο και τιμωρείται.

- Ως ηλεκτρονικό έγκλημα μπορεί να θεωρηθεί *“μια εγκληματική πράξη στην οποία ο ηλεκτρονικός υπολογιστής χρησιμοποιείται ως το κυριότερο μέσο τέλεσής της”.*

Ηλεκτρονικό έγκλημα (2)

- Η Ευρωπαϊκή Ένωση, σύμφωνα με τη Συνθήκη κατά του Ηλεκτρονικού Εγκλήματος ορίζει το Ηλεκτρονικό Έγκλημα ως *"οποιαδήποτε εγκληματική ενέργεια διεπράχθη εναντίον ή με τη βοήθεια ενός ηλεκτρονικού υπολογιστή ή δικτύου ηλεκτρονικών υπολογιστών"*

- Βρετανική Αστυνομία αναφέρει ότι ηλεκτρονικό έγκλημα είναι "η χρήση ηλεκτρονικού υπολογιστή ή δικτύου ηλεκτρονικών υπολογιστών για την διάπραξη εγκλήματος"

Μορφές Ηλεκτρονικού Εγκλήματος

Στο ηλεκτρονικό έγκλημα η ηλεκτρονική συσκευή μπορεί :

- Να αποτελεί το στόχο κάποιας επίθεσης. Στην περίπτωση αυτή μπορούμε να πούμε ότι ο υπολογιστής είναι το "θύμα" της επίθεσης.

- Να αποτελεί το μέσο διάπραξης κάποιας επίθεσης, δηλαδή το εργαλείο που χρησιμοποιεί ο επιτιθέμενος για να πραγματοποιήσει τον εγκληματικό σκοπό του (π.χ. εισβάλλοντας σε κάποιο άλλο υπολογιστή).

- Να αποτελεί ένα βοηθητικό μέσο για τη διάπραξη του εγκλήματος, π.χ. να αποθηκεύονται σε αυτόν στοιχεία ή πληροφορίες που αφορούν άτομα τα οποία συμμετέχουν σε παράνομες δραστηριότητες.

Ηλεκτρονικά εγκλήματα σε σχέση με τα παραδοσιακά

- Οι οικονομικές απώλειες που προξενούνται στα “ψηφιακά” θύματα είναι πολύ μεγαλύτερες από εκείνες των θυμάτων των παραδοσιακών εγκλημάτων.
- Ένα μεγάλο μέρος δεν καταγγέλλεται και έτσι δεν καταγράφεται από καμία επίσημη αρχή.
- Ένα μεγάλο μέρος δεν γίνεται αντιληπτό από το θύμα.

Ηλεκτρονικά εγκλήματα σε σχέση με τα παραδοσιακά

- Διαπράττονται συνήθως από μακρινή απόσταση (τρίτες χώρες).
- Ο εντοπισμός του ηλεκτρονικού εγκληματία είναι τεχνολογικά περίπλοκος.
- Αποδίδουν μεγάλα κέρδη με μικρό κίνδυνο ανακάλυψης του δράστη.
- Ο αριθμός των θυμάτων τους συγκρινόμενος με εκείνο των παραδοσιακών εγκλημάτων είναι κατά πολύ μεγαλύτερος.

Κατηγορίες Ηλεκτρονικών Εγκλημάτων

- Κακόβουλες εισβολές σε δίκτυα φωνής και δεδομένων (π.χ. παρακολουθήσεις)
- Επιθέσεις Άρνησης Εξυπηρέτησης (DOS - denial of service - attacks)
- Επιθέσεις σε δικτυακούς τόπους
- Κακόβουλο λογισμικό (ιοί -viruses, σκουλήκια – worms, δούρειοι ίπποι -trojan horses)
- Ανεπιθύμητη Αλληλογραφία (Spamming)

Κατηγορίες Ηλεκτρονικών Εγκλημάτων (2)

- Ηλεκτρονικό ψάρεμα (Phising)
- Man in the middle
- Απάτες στο Διαδίκτυο
- Κλοπή ταυτότητας
- Ξέπλυμα χρήματος / Ηλεκτρονικο-οικονομικά εγκλήματα / Ψηφιακά νομίσματα
- Διακίνηση υλικού παιδικής πορνογραφίας

Κατηγορίες Ηλεκτρονικών Εγκλημάτων (3)

- Τρομοκρατία
- Επιθέσεις παρενόχλησης (cyberbulling)
- Κατασκοπεία (βιομηχανική, κρατική, πολιτική)
- Hacking / Cracking /Ethical Hacking
- Απώλεια Πνευματικών Δικαιωμάτων / Πειρατεία λογισμικού, ταινιών, αντιγραφές

Στατιστικά Στοιχεία

Καταγγελίες στο safeline.gr

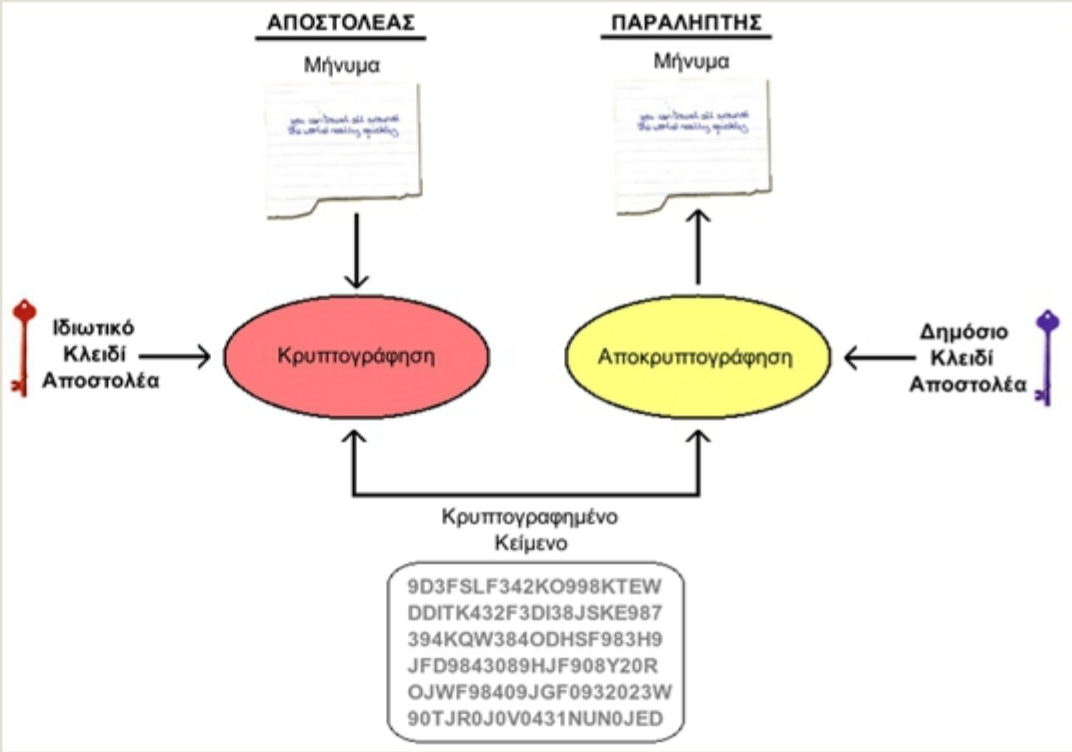
Τεχνολογίες Προστασίας

Passwords (π.χ. 123, qwerty, 15011975, apostolos)

Antivirus, Antimalware, Online & email protection κ.α.

Ασφαλή πρωτόκολλα επικοινωνίας (π.χ. https)

Κρυπτογράφηση



Σκοπός ηλεκτρονικής εγκληματολογίας

- Ο κύριος σκοπός της ηλεκτρονικής εγκληματολογίας είναι η ορθή εύρεση και η συγκέντρωση *ψηφιακών αποδεικτικών στοιχείων* (digital evidence).

Ψηφιακά αποδεικτικά στοιχεία

- Ψηφιακά αποδεικτικά στοιχεία μπορεί να είναι οποιαδήποτε πληροφορία, που αποθηκεύεται ή μεταφέρεται σε ψηφιακή μορφή.

- Διαφέρουν σε σχέση με τα συμβατικά αποδεικτικά στοιχεία αφού γεννάται το ερώτημα εάν τα ψηφιακά αποδεικτικά στοιχεία είναι πραγματικά ή εικονικά (virtual).

- Βασικό χαρακτηριστικό των ψηφιακών αποδεικτικών στοιχείων είναι ο μεγάλος βαθμός μεταβλητότητάς τους. Μπορούν πολύ εύκολα να τροποποιηθούν ή να καταστραφούν.

Ψηφιακά αποδεικτικά στοιχεία (2)

Τα ψηφιακά αποδεικτικά στοιχεία αποτελούνται από *ψηφιακά δεδομένα* (digital data) τα οποία διακρίνονται σε:

- *μεταβλητά δεδομένα* (volatile data): δεδομένα που αποθηκεύονται στην μνήμη του συστήματος (π.χ. μητρώο συστήματος, cache, μνήμη RAM) και χάνονται αν σταματήσει η τροφοδοσία της συσκευής με ρεύμα, αν γίνει τερματισμός της λειτουργίας της ή επανεκκίνηση

- *διαρκή δεδομένα* (persistent data): δεδομένα που είναι αποθηκευμένα στους σκληρούς δίσκους του συστήματος ή σε άλλες συσκευές μόνιμης αποθήκευσης, όπως σκληροί δίσκοι, USB, CDs και κάρτες μνήμης

Ψηφιακά αποδεικτικά στοιχεία (3)

- Παρ' όλο ότι τα ψηφιακά αποδεικτικά στοιχεία, λόγω της φύσης τους, είναι ευαίσθητα και μπορούν να αλλοιωθούν, να φθαρούν ή να καταστραφούν λόγω σφαλμάτων κατά την επεξεργασία ή την εξέτασή τους, μπορούν σχετικά εύκολα να ανακτηθούν με τα κατάλληλα ερευνητικά εργαλεία και μεθόδους

Ψηφιακά αποδεικτικά στοιχεία (4)

- Οργανισμοί όπως ο Scientific Working Group on Digital Evidence (www.swgde.org) και ο International Organization on Computer Evidence (www.ioce.org) καθορίζουν τα πρότυπα για την ανάκτηση, τη διατήρηση και την εξέταση ψηφιακών αποδεικτικών στοιχείων.

Κατηγορίες ψηφιακών αποδεικτικών στοιχείων

- ***Αντικείμενα δεδομένων (data objects)****:* Αντικείμενα ή πληροφορίες, που έχουν αποδεικτική αξία σε μια ποινική υπόθεση και σχετίζονται με φυσικά αντικείμενα.

- ***Ψηφιακές αποδείξεις (digital evidence)****:* Πληροφορίες, που έχουν αποδεικτική αξία σε μια ποινική υπόθεση και αποθηκεύονται ή μεταδίδονται σε ψηφιακή μορφή.

- ***Φυσικά αντικείμενα (physical items):*** Τα φυσικά μέσα όπου αποθηκεύονται ή μέσω των οποίων μεταδίδονται πληροφορίες και αντικείμενα δεδομένων.

Κατηγορίες ψηφιακών αποδεικτικών στοιχείων (2)

- ***Γνήσιες ψηφιακές αποδείξεις (original digital evidence):*** *Τα* φυσικά αντικείμενα και τα δεδομένα που σχετίζονται με αυτά τη στιγμή που συλλέγονται από τη σκηνή του εγκλήματος.

- ***Διπλότυπα ψηφιακών αποδείξεων (duplicate digital evidence):*** Μια ακριβής ψηφιακή αναπαραγωγή όλων των δεδομένων που περιέχονται σε ένα γνήσιο ψηφιακό αντικείμενο.

- ***Αντίγραφο (copy):*** Μια ακριβής αναπαραγωγή των πληροφοριών που περιέχονται σε ένα γνήσιο φυσικό αντικείμενο.

Υλικό για εντοπισμό στοιχείων Ηλεκτρονικών Εγκλημάτων

- Υπολογιστές
- Κινητές συσκευές
- Smart … συσκευές
- Δίκτυα (Internet / Κινητής / GPS)
- Βάσεις Δεδομένων (Cloud)

Ανάκτηση

Ηλεκτρονική Εγκληματολογία VS Ανάκτηση από καταστροφή

- Η ηλεκτρονική εγκληματολογία (Computer forensics) αναζητά στοιχεία που μπορούν να ανακτηθούν από αποθηκευτικά μέσα ενός ηλεκτρονικού συστήματος.
- Η δικτυακή ηλεκτρονική εγκληματολογία (Network forensics) παρέχει πληροφορίες για τον τρόπο με τον οποίον ο εισβολέας απέκτησε πρόσβαση στο δίκτυο.
- Ανάκτηση δεδομένων (Data recovery) είναι η διαδικασία της επαναφοράς δεδομένων που έχουν χαθεί από λάθος ή βλάβη.

Ανάκτηση

Ηλεκτρονική Εγκληματολογία VS Ανάκτηση από καταστροφή

- Στην ηλεκτρονική εγκληματολογία ανάκτηση είναι η διαδικασία κατά την οποία γίνεται προσπάθεια εύρεσης στοιχείων που ο χρήστης προσπάθησε να κρύψει.

- Ενώ η ανάκτηση από καταστροφή είναι η διαδικασία κατά την οποία γίνεται ανάκτηση χρήσιμων δεδομένων τα οποία ο χρήστης δεν θέλει να χάσει.

Λογισμικά Εξιχνίασης Ηλεκτρονικού Εγκλήματος

- EnCase
- Foremost
- FTK
- Registry Recon
- PTK Forensics
- The Sleuth Kit
- The Coroner's Toolkit
- COFEE
- Selective file dumper
- HashKeeper
- Xplico

Παραδείγματα

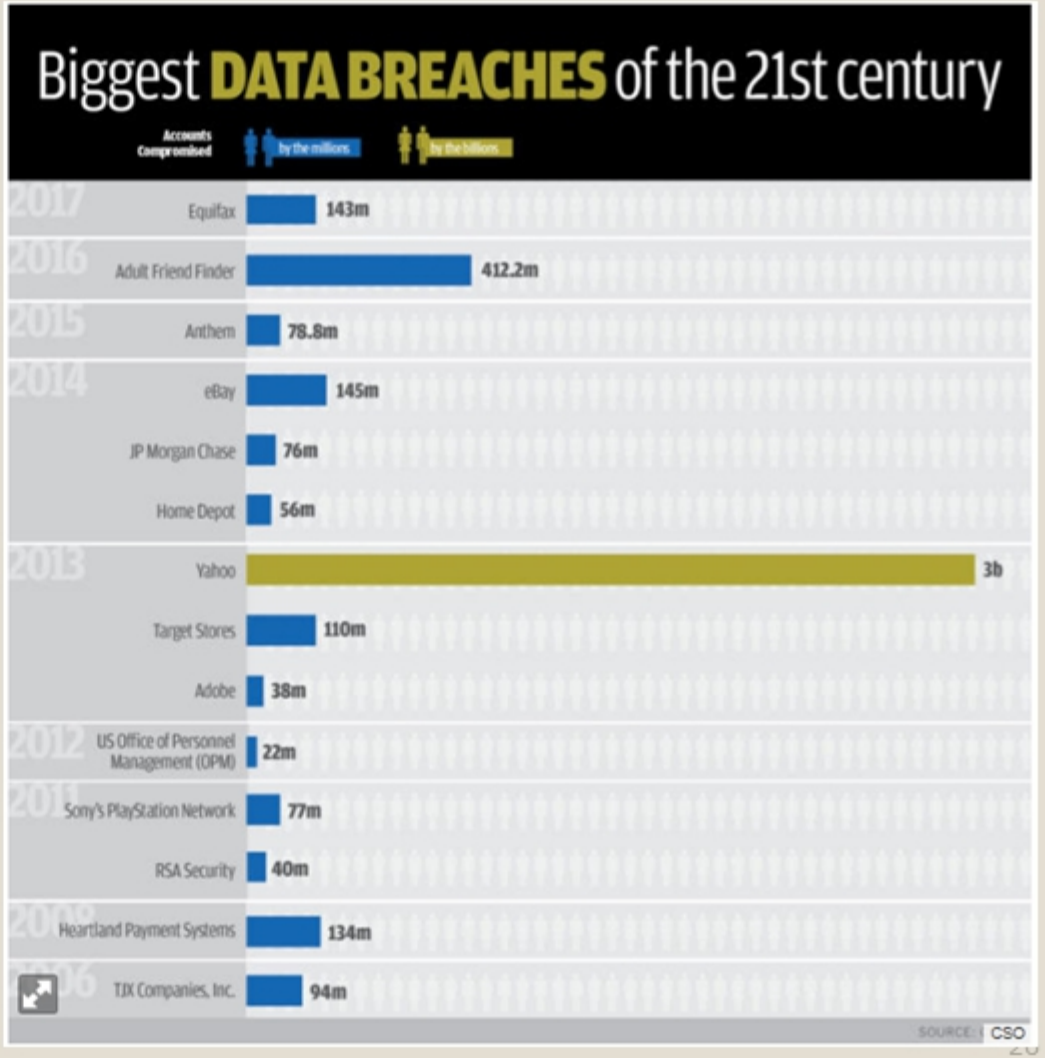
Wikileaks (2006)

Λίστα Lagarde (2010)

i - cloud (2014)

Panama papers (2016)

Paradise Papers (2017)



Στατιστικά Στοιχεία

Κόστος διαρροής πληροφοριών

Το κόστος του ηλεκτρονικού εγκλήματος θα φθάσει τα 2 τρισεκατομμύρια δολάρια μέχρι το 2019, δηλαδή τριπλάσια αύξηση από τις εκτιμήσεις των 500 δισεκατομμυρίων δολαρίων το 2015.

Σύμφωνα με το "The Global Risks Report 2016", από το Παγκόσμιο Οικονομικό Φόρουμ, σημαντικό μέρος του εγκλήματος στον κυβερνοχώρο δεν εντοπίζεται. Αυτό ισχύει ιδιαίτερα στην περίπτωση της βιομηχανικής κατασκοπείας και της βλάβης των ιδιωτικών μυστικών, επειδή είναι δύσκολο να εντοπιστεί η παράνομη πρόσβαση σε ευαίσθητα ή εμπιστευτικά έγγραφα και δεδομένα.

Σύμφωνα με την έκθεση "ITRC Data Breach Report" (ITRC), περισσότερα από 29 εκατομμύρια αρχεία έχουν εκτεθεί σε 858 δημοσιευμένες παραβιάσεις σε διάφορους τομείς, συμπεριλαμβανομένων των οικονομικών, της κυβέρνησης, της υγειονομικής περίθαλψης και της εκπαίδευσης.

Στατιστικά Στοιχεία

Κόστος διαρροής πληροφοριών

Σύμφωνα με το "2016 Cost of Data Breach Study: Global Analysis" του Ινστιτούτου Ponemon, το οποίο διερεύνησε 383 οργανισμούς που υπέστησαν τουλάχιστον μία παραβίαση το 2016, το μέσο κόστος ανά παραβίαση ήταν 4 εκατομμύρια δολάρια (7 εκατομμύρια δολάρια στις ΗΠΑ)

Η ίδια μελέτη διαπίστωσε ότι το κόστος ανά χαμένη εγγραφή ήταν κατά μέσο όρο 158 δολάρια παγκοσμίως (220 δολάρια στις ΗΠΑ)

Λόγω του νομικού πλαισίου συμμόρφωσης και των ισχυόντων κανονισμών, το κόστος ανά παραβίαση σε οργανισμούς στον τομέα της υγειονομικής περίθαλψης και των χρηματοπιστωτικών υπηρεσιών ξεπερνά όλες τις άλλες βιομηχανικές ομάδες.

Στατιστικά Στοιχεία

Κόστος διαρροής πληροφοριών

Οι οικονομικές απώλειες που προκύπτουν από την κλοπή εμπορικών μυστικών κυμαίνεται από 749 δισ. έως 2.2 τρισ. δολάρια ετησίως.

Πέρυσι, η IDG ανίχνευσε 38% περισσότερα περιστατικά στον κυβερνοχώρο από ό,τι το προηγούμενο έτος.

48% των παραβιάσεων ασφαλείας δεδομένων προκαλούνται από πράξεις κακόβουλης πρόθεσης. Ανθρώπινο σφάλμα ή βλάβη συστήματος για το υπόλοιπο.

Στατιστικά Στοιχεία

ΜΜΕ (έως 1000 άτομα) και διαρροή πληροφοριών

Οι ΜΜΕ είναι ιδιαίτερα ευάλωτες στο ηλεκτρονικό έγκλημα, ένα 50% ανέφεραν ότι υπέστησαν τουλάχιστον ένα cyberattack τους τελευταίους 12 μήνες.

Το μέσο κόστος μιας παραβίασης δεδομένων που συνεπάγεται κλοπή περιουσιακών στοιχείων ανήλθε σε 879.582 δολάρια για αυτές τις ΜΜΕ. Πλήρωσαν άλλα 955.429 δολάρια για να αποκαταστήσουν την κανονική τους επιχείρηση μετά από επιτυχείς επιθέσεις.

Για αυτές τις ΜΜΕ, το 60% των εργαζομένων χρησιμοποιούν τον ίδιο κωδικό πρόσβασης σε όλα όσα έχουν πρόσβαση.

Το 63% των επιβεβαιωμένων παραβιάσεων δεδομένων οφείλονται σε έναν αδύναμο, προεπιλεγμένο ή κλεμμένο κωδικό πρόσβασης.

Στατιστικά Στοιχεία

Επενδύσεις στην Ασφάλεια

Οι παγκόσμιες δαπάνες για την καταπολέμηση του εγκλήματος στον κυβερνοχώρο θα φτάσουν τα 80 δισεκατομμύρια δολάρια φέτος, ενώ οι οργανισμοί επικεντρώνονται ολοένα και περισσότερο στην ανίχνευση και την αντίδραση, επειδή η λήψη προληπτικών μέτρων δεν ήταν επιτυχής στον αποκλεισμό κακόβουλων επιθέσεων

Οι δαπάνες για την ασφάλεια στον κυβερνοχώρο έχουν διογκωθεί, κυρίως στις ΗΠΑ, από 1 δισεκατομμύριο δολάρια πριν από δύο χρόνια σε 2,5 δισεκατομμύρια δολάρια το 2016. Οι ειδικοί αναμένουν δραματική ανάπτυξη τα επόμενα πέντε χρόνια καθώς το ασφαλιστικό concept εξαπλώνεται παγκοσμίως.

Το 2016, 62% των οργανισμών χρησιμοποίησαν υπηρεσίες ασφαλείας για τουλάχιστον ένα μέρος της άμυνας στον κυβερνοεγκληματικό τομέα, σύμφωνα με την έκθεση της PwC «The Global State of Information Security».

Στατιστικά Στοιχεία

Ετοιμότητα και Αντίδραση

Μόνο το 38% των οργανισμών που συμμετείχαν στην έρευνα "2015 Global Cybersecurity Status Report" της ISACA πιστεύουν ότι είναι έτοιμοι να αντιμετωπίσουν μια επίθεση της εξειδικευμένης εγκληματικότητας στον κυβερνοχώρο.

Από τους 1.000 επαγγελματίες IT που συμμετείχαν στην έρευνα για την "2016 Cyberthreat Defense Report" της Invincea, το 75% ανέφερε ότι τα δίκτυά τους είχαν παραβιαστεί το τελευταίο έτος και το 62% δήλωσαν ότι αναμένουν να έχουν ένα επιτυχημένο cyberattack σε κάποιο σημείο αυτό το έτος.

Σύμφωνα με το Verizon DBIR, το 30% των ηλεκτρονικών μηνυμάτων ηλεκτρονικού "ψαρέματος" ανοίγονται και το 12% αυτών κάνουν κλικ στον σύνδεσμο ή το συνημμένο.

Μια έρευνα του Osterman Research σε 540 οργανισμούς στη Βόρεια Αμερική, τη Βρετανία και τη Γερμανία αποκάλυψε ότι σχεδόν οι μισοί είχαν υποστεί επιθέσεις ransomware το τελευταίο έτος.

Συμπεράσματα

Ραγδαία αύξηση στα ηλεκτρονικά εγκλήματα και στο κόστος αυτών για τις επιχειρήσεις και οργανισμούς

Λήψη μέτρων ασφαλείας - Εγρήγορση των επιχειρήσεων και εκπαίδευση των εργαζομένων

Προσοχή στη διαχείριση των ευαίσθητων δεδομένων από ιδιώτες και επιχειρήσεις

Δυσκολίες στην αντιμετώπιση / εξιχνίαση των ηλεκτρονικών εγκλημάτων - Διεθνείς συνεργασίες και συνεχή εκπαίδευση των επαγγελματιών του χώρου