

Ασφάλεια Πληροφοριακών Συστημάτων

Ιστορικά Στοιχεία για την Ασφάλεια Πληροφοριών

Με την ανάπτυξη του ανθρώπινου πολιτισμού έγινε κατανοητό το πόσο σημαντική είναι η αποστολή μηνυμάτων με **ασφάλεια**, χωρίς να κινδυνεύει δηλαδή να μαθευτεί αλλά και να μην τροποποιηθεί το περιεχόμενο των μηνυμάτων

- Κρυπτεία Σκυτάλη της αρχαίας Σπάρτης
- Κώδικα του Καίσαρα στην Ρωμαϊκή εποχή



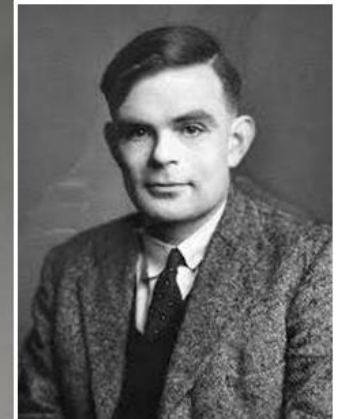
Telegraph



Carrier Pigeons

Ιστορικά Στοιχεία για την Ασφάλεια Πληροφοριών

- Στη σύγχρονη εποχή, κατά τον Β' Παγκόσμιο Πόλεμο, έγινε γνωστή η συσκευή Αίνιγμα (Enigma), με την οποία αποστέλλονταν κρυπτογραφημένα μηνύματα από το ναζιστικό Γερμανικό στρατό.
- Η αποκρυπτογράφηση (σπάσιμο) των μηνυμάτων της με τη συμμετοχή του Άλαν Τούριγκ (Alan Turing) βοήθησε στην τελική έκβαση του πολέμου.



Ιστορικά Στοιχεία για την Ασφάλεια Πληροφοριών

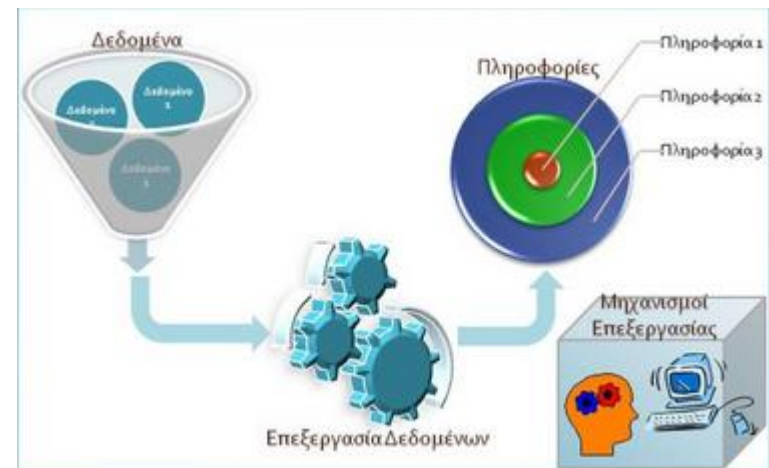
- 1988 ο Ρόμπερτ Μόρις (Robert Morris) δημιούργησε το πρώτο Σκουλήκι (worm)
- Εκείνη την εποχή φυλακίστηκε για πρώτη φορά και ένας από τους γνωστότερους μέχρι σήμερα χάκερς, ο Κέβιν Μίτνικ (Kevin Mitnick)
- Σήμερα μέσω του διαδικτύου μεταδίδονται πληροφορίες με διάφορους τρόπους, από ιδιώτες και οργανισμούς, ενώ ταυτόχρονα υπάρχουν σ' αυτό ανταγωνιστές αλλά και διάφορες ομάδες ατόμων που караδοκούν και συχνά το καταφέρνουν να υποκλέψουν δεδομένα και να τα εκμεταλλευτούν με διάφορους τρόπους

Πληροφοριακό Σύστημα

Είναι ένα σύνολο ανθρώπινου δυναμικού, υπολογιστών και διαδικασιών, τα οποία συνεργάζονται αρμονικά για να βοηθήσουν έναν οργανισμό ή μία επιχείρηση να πετύχει τους στόχους του

Υλικό + Λογισμικό + Δεδομένα + Άνθρωποι + Διαδικασίες

- TAXIsnet - Υπουργείο Οικονομικών
- mySchool – Υπουργείο Παιδείας



Ασφάλεια Πληροφοριακών Συστημάτων

- είναι ένας τομέας της επιστήμης της Πληροφορικής, ο οποίος ασχολείται με την **προστασία των δεδομένων** ενός Πληροφοριακού Συστήματος από άτομα χωρίς εξουσιοδότηση
- άτομο χωρίς εξουσιοδότηση είναι οποιοδήποτε δεν έχει άδεια πρόσβασης σε κάποιο τμήμα του πληροφοριακού συστήματος. (π.χ. ένας φάκελος αρχείων, μια Βάση Δεδομένων κ.α.)



Ηλεκτρονικό Έγκλημα

Είναι οι αξιόποινες εγκληματικές πράξεις που τελούνται με την βοήθεια ηλεκτρονικών υπολογιστών και που τιμωρούνται από τη νομοθεσία.

Ανάλογα με τον τρόπο που πραγματοποιούνται διαχωρίζονται σε:

- εγκλήματα που έγιναν με τη χρήση Ηλεκτρονικών Υπολογιστών (computer crime)
- κυβερνοεγκλήματα (cyber crime), εάν έγιναν μέσω του Διαδικτύου

Κυβερνοεγκλήματα

- Τροποποίηση δεδομένων - Κλοπή δεδομένων
- Παρεμπόδιση κυβερνοκυκλοφορίας
- Εισβολή σε δίκτυο - Σαμποτάζ σε δίκτυο
- Μη εξουσιοδοτημένη πρόσβαση
- Διασπορά ιών
- Πλαστογραφία - Απάτη
- Επιβλαβές περιεχόμενο



Δίωξη Ηλεκτρονικού Εγκλήματος

Υπηρεσία της ελληνικής Αστυνομίας
με αποστολή την πρόληψη, έρευνα και καταστολή
εγκλημάτων ή αντικοινωνικών συμπεριφορών, που
διαπράττονται μέσω διαδικτύου ή άλλων μέσων
ηλεκτρονικής επικοινωνίας

<https://cyberalert.gr/>



Χάκερς

- αυτά τα άτομα ή ομάδες ατόμων, εισβάλουν σε υπολογιστικά συστήματα
- είναι συνήθως εξαιρετικά μεγάλη απειλή για δικτυωμένα συστήματα γιατί εισβάλουν μέσω του διαδικτύου
- έχουν βαθιά γνώση Λειτουργικών Συστημάτων και γλωσσών προγραμματισμού



Χάκερς

Ανάλογα με τις ηθικές τους αρχές χωρίζονται στις εξής 3 κατηγορίες:

- Black Hat
- White Hat
- Gray Hat



Black hats hackers

- πολλές φορές λέγονται και κράκερς (Crackers)
- συνήθως εισβάλουν σε συστήματα με σκοπό να κλέψουν- καταστρέψουν δεδομένα
- δημιουργούν κακόβουλο λογισμικό
- σπάνε προγράμματα
- υποκλέπτουν κωδικούς κ.λπ.



White hats hackers

- ψάχνουν για «κενά» (vulnerabilities) ασφαλείας σε Λειτουργικά Συστήματα, εφαρμογές και τους λόγους υπάρξεως τους
- δεν έχουν σκοπό την καταστροφή δεδομένων και συνήθως ενημερώνουν τους υπεύθυνους για τα κενά ασφαλείας που βρίσκουν, ώστε να επιδιορθωθούν (ηθικό χάκινγκ)



Gray hats hackers

- είναι άτομα που χρησιμοποιούν τους υπολογιστές για να τιμωρήσουν υποτιθέμενους εγκληματίες του Κυβερνοχώρου (Cyberspace)
- ονομάζονται και χακτιβιστές (hacktivists) όταν μεταφέρουν πολιτικά μηνύματα μέσω διαδικτύου



Κοινωνική Μηχανική (social engineering)

- Στον χώρο της Πληροφορικής έχει την έννοια της εξαπάτησης διαφόρων ατόμων, με σκοπό την απόσπαση εμπιστευτικών πληροφοριών και μπορούν να χρησιμοποιηθούν, για παράδειγμα σε διαδικτυακές αγορές ή να πουληθούν σε τρίτους ή για εκφοβισμό και για εκβιασμό των ιδιοκτητών τους
- Οι πληροφορίες αυτές μπορεί να είναι προσωπικές, αλλά ενδέχεται να αφορούν και τον χώρο εργασίας
- Ονόματα, ημερομηνίες γεννήσεως, κωδικοί, αριθμοί τηλεφώνων, ταχυδρομικές διευθύνσεις, ηλεκτρονικές διευθύνσεις (πολλές φορές οι χρήστες δίνουν τέτοια στοιχεία μέσω ιστοσελίδων Κοινωνικής Δικτύωσης) και τραπεζικά στοιχεία είναι κάποιες από τις πληροφορίες που ίσως είναι στόχος των ενδιαφερομένων

Κοινωνική Μηχανική (social engineering)

- Η γνωστότερη τεχνική που χρησιμοποιούν για την απόσπαση πληροφοριών είναι το **ηλεκτρονικό ψάρεμα** (phishing), όπου συνήθως χρησιμοποιούνται πλαστά ηλεκτρονικά μηνύματα (πχ. από τράπεζες) και σύνδεσμοι προς πλαστές ιστοσελίδες και ζητούν την καταχώρηση των πληροφοριών που τους ενδιαφέρουν

