ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΑΤΡΩΝ
UNIVERSITY OF PATRAS

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΑΤΡΩΝ

ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΗΛΕΚΤΡΟΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ & ΠΛΗΡΟΦΟΡΙΚΗΣ

ΕΡΓΑΣΙΑ ΕΞΑΜΗΝΟΥ

ΓΙΑ ΤΟ ΜΑΘΗΜΑ

Δίκτυα Δημόσιας Χρήσης

ΑΣΦΑΛΕΙΑ ΣΤΟ INTERNET

ΠΕΤΡΟΠΟΥΛΟΥ ΚΩΝΣΤΑΝΤΙΝΑ

4602

ΔΙΔΑΣΚΩΝ: ΧΡΗΣΤΟΣ ΜΠΟΥΡΑΣ **ΠΑΤΡΑ 2014**

ΠΕΡΙΕΧΟΜΕΝΑ

5. Κρυπτογραφία

5.1 Ιστορική αναδρομή κρυπτογραφίας
5.2 Βασική ορολογία κρυπτογραφίας
5.3 Κρυπτογραφία σε συμμετρικά κλειδιά
5.4 Επιθέσεις σε συμμετρικά κλειδιά
5.5 Κρυπτογραφία Δημόσιου κλειδιού
5.6. Επιθέσεις σε Δημόσιου κλειδιού
5.6 Συμμετρικό κλειδί vs. Κρυπτογραφία δημόσιου κλειδιού

6. Η ασφάλεια στο διαδίκτυο

6.1 SSL Error
6.2 Αδυναμίες – Μειονεκτήματα του Πρωτοκόλλου SSL
6.3 Επιθέσεις και Ανθεκτικότητα του πρωτοκόλλου SSL
6.4 Σχέση του Πρωτοκόλλου SSL και του Μοντέλου OSI

7. Αντιμετώπιση

7.1 Συστήματα ανίχνευσης επιθέσεων
7.2 Εργαλεία παρακολουθήσεις συστήματος
7.3 Πιστοποίηση
7.4 Ανιχνευτές ιών
7.5 Λογισμικό ελέγχου ασφαλείας *(Malware)*
7.6 Τεχνικές τοπολογίας δικτύου

ΚΕΦΑΛΑΙΟ 1: ΕΙΣΑΓΩΓΗ

1. Εισαγωγή

Ο σκοπός της δημιουργίας των δικτύων ήταν η ανάγκη μετάδοση της πληροφορίας από έναν πομπό σε ένα δέκτη με τη βοήθεια της ηλεκτρικής ενέργειας και του ηλεκτρικού ρεύματος.

Το δίκτυο δίνει τη δυνατότητα σε ένα συνδρομητή του να επικοινωνήσει με οποιονδήποτε άλλον συνδρομητή που διαθέτει την κατάλληλη διάταξη πρόσβασης σε κάποιο οριακό σύστημα του δικτύου που ονομάζεται κόμβος ή κέντρο.

Η χρήση του διαδικτύου είναι αναπόσπαστο κομμάτι της καθημερινότητας μας πλέον. Μέσω του διαδικτύου εισαγόμαστε σένα είδος παγκόσμιου και πολύμορφου διαλόγου χωρίς όρια και περιορισμούς εκτός από αυτούς που εμείς οι ίδιοι επιβάλουμε στους εαυτούς μας. Οι δυνατότητες που μας προσφέρει το Internet είναι πάρα πολλές από ομαδικές συσκέψεις, συζητήσεις μέσω φόρουμ γύρω από οποιοδήποτε θέμα κ.α, ωστόσο αυτή ακριβώς η ανωνυμία και η δυνατή πρόσβαση σε οποιοδήποτε χώρο και θέμα δημιουργεί και τους κινδύνους.

Στο πλαίσιο μιας παγκόσμιας κινητοποίησης κυβερνητικών και μη οργανισμών για την ασφαλή χρήση του Διαδικτύου και κυρίως για την προστασία των παιδιών, το Ευρωπαϊκό Κοινοβούλιο προχωρεί στην υλοποίηση μιας ευρωπαϊκής εκστρατείας και ενός προγράμματος δράσης πληροφόρησης και συνειδητοποίησης, για να πληροφορηθούν οι γονείς και όλοι όσοι ασχολούνται με παιδιά (δάσκαλοι, κοινωνικοί λειτουργοί κ.λπ.) για τον καλύτερο τρόπο προστασίας των ανηλίκων από την έκθεση σε περιεχόμενο που θα μπορούσε να είναι βλαβερό για την ανάπτυξή τους, έτσι ώστε να εξασφαλιστεί η ευημερία τους.

Κατά την πλοήγηση στους χώρους του Διαδικτύου είναι καλό να έχουμε υπόψη μας τα παρακάτω:

- Το Διαδίκτυο είναι κυρίως μια κοινωνία ανθρώπων και κρύβει τους ίδιους κινδύνους που κρύβει κάθε κοινωνία, ιδιαίτερα όταν διευκολύνεται στο έπακρο ο τρόπος επικοινωνίας των ανθρώπων μεταξύ τους.
- Οι πληροφορίες που παρουσιάζονται στο Διαδίκτυο δεν είναι πάντα έγκυρες.

- Η κοινοποίηση των προσωπικών στοιχείων του χρήστη *(ονοματεπώνυμο, διεύθυνση, τηλέφωνο, φωτογραφία, κωδικοί πρόσβασης, αριθμός πιστωτικών καρτών, e-mail κ.λπ.)* είναι καλό να αποφεύγεται.
- Η τοποθέτηση του υπολογιστή *(εάν είναι δυνατόν)* σε κοινόχρηστο χώρο και όχι αποκλειστικά στο παιδικό δωμάτιο ενθαρρύνει τη χρήση του Διαδικτύου σε οικογενειακό περιβάλλον και βοηθά στην επίβλεψη των ιστοσελίδων τις οποίες επισκέπτονται τα παιδιά.
- Η καλή επικοινωνία με τα παιδιά είναι απαραίτητη ώστε να ενθαρρύνονται να μιλάνε για αυτούς με τους οποίους επικοινωνούν, ανταλλάσσουν μηνύματα και να ενημερώνουν εάν ποτέ γίνονται θύματα απειλών, εκφοβισμού ή παρενόχλησης οποιασδήποτε μορφής.
- Η χρήση του υπολογιστή ως μέσου απασχόλησης του παιδιού χωρίς την παρουσία ενηλίκου είναι καλό να αποφεύγεται. Ο υπολογιστής δεν πρέπει να χρησιμοποιείται ως ηλεκτρονική ¨babysitter¨
- Η δημιουργία ενός συνόλου από κανόνες χρήσης του Η/Υ αποδεκτών από όλους και η ανάρτηση τους σε εμφανές σημείο δίπλα στον υπολογιστή συντελεί στην προστασία όλων των χρηστών.

1.1 Ιστορική αναδρομή

Το Σεπτέμβριο του 1997 κάποιοι σταμάτησαν την κανονική λειτουργία του Web site της Coca-Cola και αντικατέστησαν τις κανονικές σελίδες της εταιρείας με σελίδες οι οποίες περιείχαν μηνύματα εναντίον της.

Εκείνη τη χρονιά, δυο μεγάλες εταιρείες πιστωτικών καρτών δέχθηκαν μια σημαντική επίθεση όταν κάποιος hacker κατάφερε να κλέψει μια μεγάλη ποσότητα στοιχείων κατόχων πιστωτικών καρτών και αριθμών πιστωτικών καρτών. Στη συνέχεια ο hacker έστειλε e-mail στους κατόχους πιστωτικών καρτών των οποίων τα στοιχεία έκλεψε, λέγοντας τους πως η εταιρεία τους εμπιστεύθηκε την ασφάλεια των δεδομένων τους σε μια άλλη εταιρεία η οποία όμως δεν υπήρξε αρκετά προσεκτική.

Την ίδια χρονιά, ο Carlos Salgado εγκατέστησε ένα πρόγραμμα, γνωστό ως *sniffer***,** σε μια εταιρεία πιστωτικών καρτών. Το πρόγραμμα *sniffer* παρακολουθούσε τη λειτουργία και τελικά κατάφερε να αποθηκεύσει τα στοιχεία για πάνω από 10.0000 πιστωτικές κάρτες.

Το 1996 ο Dan Farmer, ένας σύμβουλος ασφαλείας και προγραμματιστής, χρησιμοποίησε ένα εργαλείο γνωστό με το όνομα *Satana* για να ελέγξει την ασφάλεια ενός αριθμού ιστοχώρων. Έλεγξε 2.200 ιστόχωρους και ανακάλυψε ότι περίπου το 65% από αυτά ήταν ευάλωτα σε διάφορα είδη γνωστών επιθέσεων, αυτό είναι ένα αρκετά σημαντικό στατιστικό στοιχείο.

Αυτό που το κάνει πιο σημαντικό είναι ότι ο Farmer επικεντρώθηκε σε ιστόχωρους τα οποία θα έπρεπε να είναι ιδιαίτερα ασφαλή:

- Τραπεζικά
- Ασφαλιστικών εταιρειών
- Εταιρειών πιστωτικών καρτών
- Κυβερνητικών υπηρεσιών.

1.2 Γιατί δεν είναι ασφαλές το Internet

Το δίκτυο *(κόμβος ή κέντρο)* είναι ένα απλό μοντέλο που δημιουργήθηκε για να καλύψει τις ανάγκες επικοινωνίας πολλών συνδρομητών.

Έτσι άρχισαν να εμφανίζονται πολλές μορφές δικτύων όπως το:

1. *ARPANET (Advanced Research Project Agency Network)* το οποίο μετονομάστηκε από το αμερικάνικο υπουργείο Άμυνας το 1972 σε DARPANET *(Defense Advanced Research Project Agency Network)* και χρησιμοποίησε το πρωτόκολλο TCP *(Transmission Control Protocol)*, το οποίο είναι αυτό που κατέστησε δυνατή την δημιουργία του Internet αφού ήταν η βάση για ένα σύνολο από πρωτόκολλα γνωστά ως TCP/IP.
2. *CYBERNET*
3. *DCS (Distributed Computing System)*
4. *CYCLADES*

Μετά εμφανίστηκε το Internet, το οποίο συνεχώς εξαπλωνόταν και απορροφούσε άλλα μικρότερα δίκτυα όπως το BITNET *(δίκτυο της IBM που είχε κατασκευάσει για ένα σύνολο πανεπιστημίων)*. Αρχικά γινόταν χρήση του Internet μόνο για ανάγνωση του ηλεκτρονικού ταχυδρομείου *(e-mail)* και για κοινή χρήση κάποιων εκτυπωτών. Έτσι δεν έδιναν τότε ιδιαίτερη σημασία για την ασφάλεια του δικτύου.

Στη σημερινή εποχή, που τεράστιο ποσοστό ανθρώπων χρησιμοποιούν τα δίκτυα για τραπεζικές συναλλαγές, αγορές και υποβολή φορολογικών δηλώσεων, η ασφάλεια των δικτύων είναι ένα πάρα πολύ μεγάλο πρόβλημα, που συνιστά την προσοχή όλων μας . Έχει γίνει απαραίτητη ανάγκη και πρωτεύων στόχος η προστασία των δικτύων.

Τα τελευταία χρόνια έχουν γίνει πολλές επιθέσεις σε δίκτυα κυρίως από άτομα που έχουν σκοπό να βλάψουν *(Hackers)*.

Είναι εξαιρετικά εύκολο κάποιος να προσπελάσει ένα δίκτυο το οποίο δεν έχει εξοπλιστεί με τα είδη προστασίας και να μην γίνει αντιληπτός. Έτσι έχοντας περάσει

αυτό το στάδιο μπορεί σχετικά εύκολα να υποκλέψει στοιχεία, προσωπικά δεδομένα, λογαριασμούς καρτών και οτιδήποτε άλλο ,στο οποίο μπορεί εύκολα να έχει πρόσβαση.

ΚΕΦΑΛΑΙΟ 2 ΕΙΔΗ ΕΠΙΘΕΣΕΩΝ

2.1. Ιοί

Η ιστορία των ιών ξεκινάει στης αρχές της δεκαετίας του ΄70 όπου ανιχνεύθηκε για πρώτη φορά στο *ARPANET*, τον πρόδρομο του Διαδικτύου. Διαδόθηκε μέσω του λειτουργικού συστήματος *TENEX*, που χρησιμοποιούσε τότε το *ARPANET* και θα μπορούσε να χρησιμοποιήσει όποια σύνδεση γινόταν με το δίκτυο για να μολύνει τους συνδεδεμένους υπολογιστές.

- Το **1981** με την άφιξη του πρώτου προσωπικού ηλεκτρονικού υπολογιστή ευρείας αγοράς με την μορφή της APPLE II ,οι πρώτοι computer viruses άρχισαν να εμφανίζονται. Οι ιοί είναι κομμάτια του «malicious code» που συνδέονται με τα προγράμματα οικοδεσποτών και διαδίδουν ένα μολυσμένο πρόγραμμα όταν εκτελείται. Έχουν παρατηρηθεί διάφορες χαρακτηριστικές επιθέσεις ιών σε διάφορα συστήματα. Ο Elk Cloner του Rich Skrenta είναι ο πρώτος επίσημα αναγνωρισμένος ιός υπολογιστή.

- Το **1986** δύο προγραμματιστές ο Amjad και ο Basit Farook Alvi χρησιμοποιούν το boot sector μιας floopy disk για να μολύνουν κάθε υπολογιστή με τον οποίο η δισκέτα έρχεται σε επαφή. Κάνοντας αυτό, δημιουργούν τον πρώτο ιό που μόλυνε τον IBM PC.

- Το **1988** ο Jerusalem virus εξαπολύεται ,μολύνοντας .exe και .com αρχεία , ο ιός αυτός είναι σχεδιασμένος να ενεργοποιείται κάθε παρασκευή και 13 και να διαγράψει κάθε πρόγραμμα που έχει εκτελεστεί εκείνη την ημέρα.

- Το **1991** ο πρώτος πολυμορφικός ιός εμφανίζεται. Αυτό το είδος είναι πολύ δύσκολο να ανιχνευθεί ,επειδή αλλάζει η εμφάνιση τους με κάθε νέα μόλυνση.

- Το **1992** εμφανίζεται η DAME *(Dark Avenger Mutation Engine),* σκοπός της είναι να μετατρέπει ένα απλό ιό σε πολυμορφικό.

- Το **1995** ο ιός Word concept γίνεται ένας από τους κυρίαρχους ιούς στη δεκαετία του 90,γιατί διαδίδεται μέσω των μακροεντολών σε έγγραφα Word.

Με λίγα λόγια θα μπορούσαμε να πούμε ότι οι ιοί είναι ένα είδους κακόβουλου προγράμματος υπολογιστή, το οποίο μπορεί να αντιγραφεί χωρίς παρέμβαση του χρήστη και να "μολύνει" τον υπολογιστή χωρίς τη γνώση ή την άδεια του χρήστη του και μπορούν να χρησιμοποιηθούν για μια ποικιλία διαφορετικών επιθέσεων.

Ένας Ιός είναι ένα πρόγραμμα το οποίο επισυνάπτει τον εαυτό του σε αρχεία τα οποία υπάρχουν στον υπολογιστή αυτή η διαδικασία είναι γνωστή ως μόλυνση. Αφού ένας ιός εγκατασταθεί σε έναν υπολογιστή, μπορεί να αντιγράψει τον εαυτό του και σε άλλα αρχεία στον υπολογιστή.

2.1.1 Κατηγορίες ιών

Υπάρχουν τρεις κύριες κατηγορίες ιών. Τους αναφέρουμε ονομαστικά εδώ και τους αναλύουμε λίγο ποιο κάτω :

- Εκτελέσιμοι ιοί
- Ιοί δεδομένων
- Ιοί οδηγών συσκευών

- Ένας εκτελέσιμος ιός: → Είναι ένας ιός ο οποίος προστίθεται σε ένα εκτελέσιμο αρχείο, το οποίο όταν εκτελεστεί θα έχει ως αποτέλεσμα να εκτελεστεί και ο κώδικας του ιού. Αυτός ο κώδικας στη συνέχεια θα κάνει κάποια κακόβουλη ενέργεια όπως να διαγράψει κάποια σημαντικά αρχεία.
- Ένας ιός δεδομένων: → Είναι ένας ιός ο οποίος μολύνει ένα αρχείο που περιέχει δεδομένα αντί για εκτελέσιμο κώδικα. Συχνά τα δεδομένα αυτά είναι συνδεδεμένα με κάποιο πρόγραμμα, το οποίο χρειάζεται τα δεδομένα για να εκτελέσει τη λειτουργία του.

Για παράδειγμα:

Πολλά προγράμματα χρειάζονται ένα startup αρχείο το οποίο αρχικοποιεί το πρόγραμμα και ορίζει βασικές παραμέτρους της λειτουργίας του. Ένας ιός δεδομένων θα μπορούσε να μολύνει ένα τέτοιο αρχείο και να αλλάξει τα δεδομένα σε ένα τέτοιο αρχείο ώστε το πρόγραμμα δεν θα μπορεί να λειτουργήσει ή η λειτουργία του θα τεθεί σε κίνδυνο.

Ένας άλλος τύπος ιού δεδομένων θα μπορούσε να προσθέσει μια καταχώρηση σε ένα αρχείο με password κι έτσι θα επέτρεπε πρόσβαση σε ένα εισβολέα.

Άλλο ένα παράδειγμα είναι:

Ενός ιού δεδομένων για έναν επεξεργαστή κειμένου, που θα μπορούσε επίσης να γραφτεί και εύκολα και που θα μπορούσε να αλλάζει τα περιεχόμενα κάθε αρχείου που ανοίγει από τον επεξεργαστή κειμένου ή ακόμη χειρότερα να το σβήνει.

- Ένας ιός οδηγών συσκευών: →Αυτοί επηρεάζουν τους οδηγούς συσκευών ενός λειτουργικού συστήματος που χρησιμοποιούνται για τον χειρισμό

διαφόρων στοιχείων του υπολογιστή όπως δίσκος. *(Ευτυχώς αυτός ο τύπος ιού εμφανιζόταν κυρίως σε παλιότερα λειτουργικά συστήματα όπως το MSDOS.)*

2.1.2. Δημιουργείς Ιών

Πριν από μερικά χρόνια η έλευση της visual basic, έκανε τον προγραμματισμό πολύ πιο εύκολο για εκατομμύρια ανθρώπους. Δυστυχώς με αυτό τον τρόπο έγινε ευκολότερη και η δημιουργία ιών, ενώ χάρη στο Internet η ταχύτητα διάδοσής τους μειώθηκε από μερικούς μήνες σε μερικές ημέρες ή ακόμη και ώρες.

Σήμερα η πλειοψηφία των συγγραφέων ιών αποτελείται από νεαρούς με μικρές τεχνικές γνώσεις, οι οποίοι αντιγράφουν παλαιότερους ιούς και τους διαδίδουν τροποποιημένους, χωρίς πολλές φορές να καταλαβαίνουν και οι ίδιοι ακριβώς με ποιο τρόπο το επιτυγχάνουν.

Παράδειγμα τέτοιου ιού ήταν:

Ο ILOVE YOU, ο οποίος βασίστηκε σε παλιότερο κώδικα και διαδόθηκε τόσο γρήγορα αποκλειστικά και μόνο χάρη στην εξαιρετική ψυχολογική του προσέγγιση ένα μήνυμα αγάπης είναι πολύ δύσκολο να παραβλεφθεί.

Οι σύγχρονοι δημιουργοί ιών αντιμετωπίζουν τα δημιουργήματά τους όπως και τα graffiti. Αντί όμως να αφήσουν το αποτύπωμά τους σε έναν τοίχο γράφοντας ένα σύνθημα, εκείνοι δημιουργούν έναν ιό και τον αφήνουν να διαδοθεί, λαμβάνοντας ικανοποίηση από το θόρυβο ο οποίος προκαλείται.

2.1.3. Ένας τυπικός ιός

Ο πιο πρόσφατος στον κόσμο των ιών των υπολογιστών είναι: Ο ιός που μεταδίδεται με την ηλεκτρονική αλληλογραφία (e-mail virus)

Ένας τέτοιος ιός ήτανε ο ιός *Melissa* που εμφανίσθηκε τον Μάρτιο του 1999, ήταν θεαματική κατά την επίθεση της. Ο ιός Melissa εξαπλώθηκε με έγγραφα του Microsoft Word που στάλθηκαν μέσω e-mail.

Λειτουργούσε ως εξής :

Κάποιος δημιούργησε τον ιό ως ένα έγγραφο του Word που φορτώθηκε *(uploaded)* σε μια ομάδα ειδήσεων *(newsgroup)* του Internet. Όποιος κατέβαζε το έγγραφο και το άνοιγε θα ενεργοποιούσε τον ιό, ο οποίος θα έστελνε το έγγραφο *(και συνεπώς και τον εαυτό του)* μ' ένα μήνυμα e-mail στους πρώτους 50 χρήστες που υπήρχαν στο βιβλίο διευθύνσεων *(address book)* του μολυσμένου υπολογιστή. Το μήνυμα αυτό του e-mail περιείχε ένα φιλικό σημείωμα που εμφάνιζε το όνομα του ατόμου από το οποίο έφευγε και έτσι ο αποδέκτης θα άνοιγε το μήνυμα νομίζοντας ότι είναι αβλαβές.
Ο ιός θα δημιουργούσε μετά 50 καινούργια μηνύματα από το μηχάνημα του παραλήπτη. Ως αποτέλεσμα ο ιός *Melissa* ήταν ο πιο γρήγορα διαδεδομένος ιός που εμφανίσθηκε ποτέ και ανάγκασε μάλιστα πολλές μεγάλες εταιρείες να διακόψουν να κλείσουν το σύστημα email για να μπορέσει να ελεγχθεί η εξάπλωση.

2.2. Λογικές ηλεκτρονικές βόμβες *(e-bomb)*

Μικρά προγράμματα που προστίθενται σε κάποιο υπάρχον πρόγραμμα ή ακόμα τροποποιούν κάποιον υπάρχοντα κώδικα

Καλούνται έτσι διότι είναι προγραμματισμένες να εκραγούν ηλεκτρονικά κάτω από κάποιες προϋποθέσεις.

Για να κατανοήσουμε τον όρο μπορούμε να την παρομοιάσουμε με τις τρομοκρατικές επιθέσεις σε αεροπλάνα με πυροδοτούμενες βόμβες υπό πίεση, όπου εξαιτίας της ατμοσφαιρικής πίεσης η βόμβα εκρήγνυται όταν πέσει η πίεση στο απαιτούμενο επίπεδο.

Έτσι λοιπόν και η λογική βόμβα προστίθεται στο πρόγραμμα από κάποιον που έχει εύκολη πρόσβαση στο σύστημα και εννοείται και την απαιτούμενη γνώση για να την εγκαταστήσει. Η πρόσβαση πάλι μπορεί να αποκτηθεί και με κάποιον τρόπο υποκλοπής

Τρόπος Λειτουργίας:

Η Ηλεκτρονική λογική βόμβα *(e-bomb)* όσο τρέχει το πρόγραμμα που τη συγκρατεί να μην εκραγεί μένει άνεργη όταν σταματήσει και για κάποιο λόγο το πρόγραμμα δεν τρέξει τότε η βόμβα πυροδοτείται και γίνεται ηλεκτρονική έκρηξη.

Για παράδειγμα*:*

Ένας προγραμματιστής που δουλεύει σε μια εταιρία για όσο ο προγραμματιστής τροφοδοτεί με τα στοιχεία του το σύστημα και κάνει boot *ένα πρόγραμμα τότε δεν υπάρχει φόβος, όταν όμως για κάποιο λόγο δε γίνει αυτό τότε η βόμβα μετρώντας αντίστροφα κάποιο χρονικό διάστημα που δεν έχει δεχθεί το αναγνωριστικό τότε εκρήγνυται με αποτέλεσμα να γίνει εκκαθάριση δίσκων, διαγραφή αρχείων ή κρυπτογράφηση τους*

2.3 Ανιχνευτές

Ονομάζονται ανιχνευτές δικτυακής κίνησης

Είναι προγράμματα που χρησιμοποιούνται για τον έλεγχο της ασφάλειας των συστημάτων. Λέγονται ανιχνευτές γιατί έχουν την γνώση και τον εξοπλισμό να γνωρίζουν όλα τα εξωτερικά σημεία από τα οποία θα μπορούσε κάποιος hacker να διαπεράσει την ασφάλεια του συστήματος και να έχει πρόσβαση σε αυτό.

Αρχικά δημιουργήθηκαν από τους διαχειριστές ασφαλείας του συστήματος, αλλά τελικά χρησιμοποιήθηκαν από hackers για να βρίσκουν και να προσδιορίζουν τους πιθανούς επόμενους στόχους επίθεσής τους

Τέτοια προγράμματα είναι :

- *ISS*
- το *TCP dump*
- ο *NMAP*
- ο *SATAN* και πολλά άλλα.

2.4 Δούρειοι Ίπποι *(trojan horses)*

Στην πληροφορική, ο δούρειος ίππος *(trojan horse ή απλά trojan)* είναι:

Ένα κακόβουλο πρόγραμμα που ξεγελάει τον χρήστη και τον κάνει να πιστεύει ότι εκτελεί κάποια χρήσιμη λειτουργία ενώ στα κρυφά εγκαθιστά στον υπολογιστή του άλλα κακόβουλα προγράμματα.

Το όνομά του προκύπτει από την Ιλιάδα του Ομήρου, όπου αναγράφεται ότι ο Οδυσσέας εμπνεύστηκε την κατασκευή ενός ξύλινου αλόγου, στην κοιλιά του οποίου κρύβονταν Αχαιοί πολεμιστές. Με τον τρόπο αυτό ξεγέλασε τους κάτοικους της Τροίας, εισήγαγε τον στρατό των Αχαιών μέσα στην πόλη και την κυρίευσε. Η τακτική που χρησιμοποιούν οι δούρειοι ίπποι είναι παρόμοια με την τακτική που χρησιμοποίησε ο Οδυσσέας, οπότε πήραν και αυτήν την ονομασία.

Τρόπος Λειτουργίας

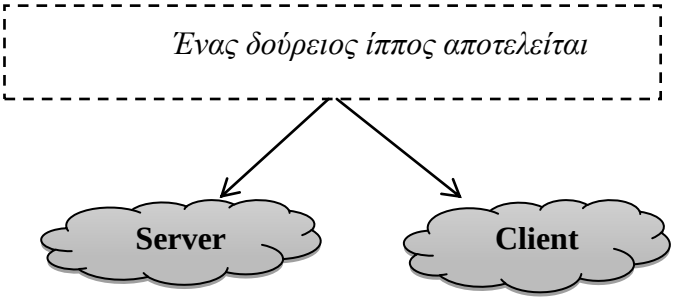
Εξωτερικά μοιάζουν με προγράμματα τα οποία εκτελούν χρήσιμες λειτουργίες, είναι ενδιαφέροντα και δίνουν την εντύπωση στον χρήστη ότι είναι ακίνδυνα. Όταν όμως ο χρήστης εκτελέσει αυτό το πρόγραμμα, τότε ενεργοποιείται ο κακόβουλος κώδικας με αποτέλεσμα ο υπολογιστής να μολυνθεί. Συνήθως αποτέλεσμα της μόλυνσης από δούρειο ίππο είναι η εγκατάσταση κάποιου προγράμματος που επιτρέπει σε μη εξουσιοδοτημένους χρήστες να έχουν πρόσβαση στον μολυσμένο υπολογιστή και να τον χρησιμοποιούν για να ξεκινήσουν άλλες επιθέσεις προς άλλους υπολογιστές του διαδικτύου. Σε αντίθεση με τους ιούς, οι δούρειοι ίπποι δε μεταδίδονται μολύνοντας αρχεία.

Συνήθεις «κρυψώνες» ενός *Δούρειου Ίππου* είναι

- κάποιο νέο δωρεάν παιχνίδι στο Διαδίκτυο,
- κάποιο τραγούδι σε μορφή *MP3 ή MP4*
- κάποιο εξειδικευμένο πρόγραμμα αρκετά δελεαστικό ώστε να το κατεβάσουν οι χρήστες.

Όταν εκτελεστεί το εν λόγω «ύποπτο» πρόγραμμα, καλείται η διαδικασία του *Δούρειου Ίππου*, η οποία επιτελεί ανεπιθύμητες λειτουργίες:

- Η τροποποίηση,
- Η διαγραφή,
- Η κρυπτογράφηση,
- Η αντιγραφή αρχείων χρηστών σε σημείο όπου ο διαρρήκτης μπορεί να τις ανακτήσει αργότερα ή να τις αποστείλει στον εαυτό του ή σε κάποια ασφαλή κρυψώνα μέσω ηλεκτρονικού ταχυδρομείου ή *FTP*.



Για να μπορέσει να μολυνθεί ένας υπολογιστής από ένα πρόγραμμα δούρειου ίππου, θα πρέπει με κάποιον τρόπο να εγκατασταθεί και να εκτελεσθεί σ' αυτόν το μέρος Server. Μετά, αφού εκτελεσθεί το μέρος Client στον υπολογιστή του εισβολέα και δοθεί η IP διεύθυνση του υπολογιστή που έχει προσβληθεί, ο έλεγχός του θα είναι πλέον πολύ εύκολος.

Οι δούρειοι ίπποι επικοινωνούν με τον Client μέσω των διαφόρων θυρών *(ports)* του υπολογιστή, τις οποίες μπορούμε να απενεργοποιήσουμε με τη χρήση κάποιου firewall *(τείχους προστασίας)*.

Τα προγράμματα μέσω των οποίων μεταφέρονται οι δούρειοι ίπποι στον υπολογιστή μας αποκαλούνται *droppers*.

Μια περίπτωση Δούρειων Ίππων είναι γνωστές με το όνομα *dialers*

Ο τρόπος λειτουργίας είναι η απενεργοποίηση του ήχου του μόντεμ και η εν συνεχεία κλήση κάποιου διεθνούς αριθμού με ιδιαίτερα υψηλό κόστος. Συνήθως επιλέγονται μακρινές χώρες της πρώην Σοβιετικής Ένωσης *(π.χ. Μολδαβία κ.λπ.)* ή χώρες του Ειρηνικού, όπου επιλέγεται κάποιος πολύ ακριβός παροχέας Διαδικτύου, ώστε ο χρήστης να μην αντιληφθεί τίποτα ύποπτο και να συνεχίζει να δουλεύει ώρες.

Ένα παράδειγμα της ποιο πάνω λειτουργίας:

Μία ανάλογη περίπτωση, στην οποία τα «θύματα» ξόδεψαν περίπου 800.000 λεπτά χρόνου σύνδεσης πριν η Ομοσπονδιακή Επιτροπή Εμπορικών Αδικημάτων των ΗΠΑ κατορθώσει να ανακαλύψει τους τρεις υπευθύνους στο Long Island και να τους μήνυση.

Η ποινή που επιβλήθηκε στους δράστες ήταν η επιστροφή 2.74 εκατομμυρίων δολαρίων σε 38.000 θύματα

Σύμφωνα με τις πρώτες εκτιμήσεις του Τμήματος Δίωξης Ηλεκτρονικού Εγκλήματος

Περιοχή	**θύματα της απάτης**
Ασφάλειας Αττικής και του ΟΤΕ	>= 10.000
στην Ελλάδα	>= 1.000

Η απάτη λειτουργεί ως εξής

Μια ιστοσελίδα δελεάζει τον επισκέπτη, συνήθως με ανακοινώσεις για γυμνές φωτογραφίες επώνυμων γυναικών ή για καυτά videos on-line ή και με κάτι άλλο, οι οποίες υπηρεσίες μάλιστα διαφημίζονται έντονα και τονίζεται ότι παρέχονται δωρεάν. Μόλις ο χρήστης κάνει κλικ σ' ένα συγκεκριμένο σημείο, εγκαθίσταται αυτόματα στον υπολογιστή του και χωρίς αυτός να το γνωρίζει, ένα ειδικό πρόγραμμα *(πρόγραμμα-τσούχτραα)* με αποτέλεσμα αντί για αστική κλήση στον τοπικό provider *(ο γνωστός ΕΠΑΚ,)* να γίνεται εκτροπή και διεθνής κλήση σύνδεσης και μάλιστα υπερπόντια, με πολλαπλάσιο φυσικά κόστος.

Για παράδειγμα
Ο χρήστης αντί για 0,17 – 0,35 € την ώρα, χρεώνεται με 2,50 € ανά λεπτό.

Οι δημιουργοί παρόμοιων ιστοσελίδων έχουν κάνει συμβάσεις με τους τηλεπικοινωνιακούς οργανισμούς των χωρών αυτών και μοιράζονται τα κέρδη από τις υπέρογκες χρεώσεις των ανυποψίαστων χρηστών. Οι τηλεφωνικές εταιρείες ισχυρίζονται ότι δεν φέρουν καμία ευθύνη για τις υποθέσεις αυτές και ότι η μόνη παραχώρηση που μπορούν να κάνουν προς τους παθόντες είναι να αποπληρώσουν οι τελευταίοι τα χρέη τους σε δόσεις. Η μόνη αντιμετώπιση και πρόληψη της μάστιγας αυτής που χρεώνει υπέρογκα τους λογαριασμούς των ανυποψίαστων χρηστών είναι η προσοχή και η εγρήγορση των ίδιων των χρηστών.

Η καλύτερη προστασία από την απάτη αυτή είναι η εγκατάσταση φραγής των διεθνών τηλεφωνικών κλήσεων ή η προμήθεια και εγκατάσταση ειδικής συσκευής *AntiDialer,* η οποία παρεμβάλλεται ανάμεσα στην τηλεφωνική γραμμή και την συσκευή modem του υπολογιστή του χρήστη και επιτρέπει να γίνονται κλήσεις μόνο προς συγκεκριμένο αριθμό ΕΠΑΚ.

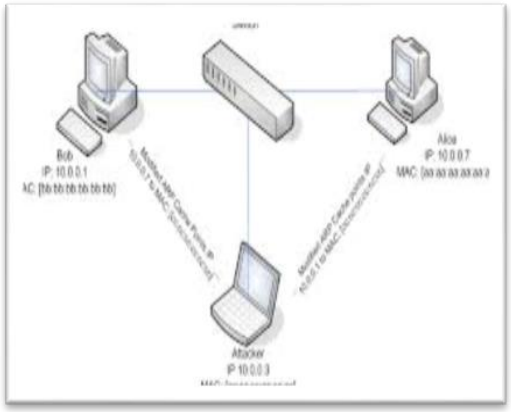
Για τις υπερβολικές αυτές χρεώσεις, ο ΟΤΕ δεν φέρει καμία ευθύνη και συμβουλεύει τους dial-up χρήστες για τα εξής :

- Να μην κατεβάζουν *(download)* προγράμματα στους υπολογιστές τους από άγνωστης και αμφίβολης προέλευσης ιστοσελίδες.
- Να αποσυνδέονται από το Internet όταν δεν το χρησιμοποιούν.
- Να χρησιμοποιούν την υπηρεσία φραγής των εξερχόμενων διεθνών τηλεφωνικών κλήσεων.
- Να μην επιτρέπουν τη χρήση του υπολογιστή για σύνδεση στο Internet από τρίτους, στο σπίτι ή τον χώρο εργασίας τους.

Για χρήστες που χρησιμοποιούν *Unix-Linux:*ένας Δούρειος Ίππος θα μπορούσε να τοποθετηθεί σε κάποιο συχνά χρησιμοποιούμενο φάκελο και να του δοθεί κάποιο όνομα παραπλήσιο με κάποιο υπάρχον αρχείο.

Είναι πιθανό, ακόμη και αν ο Δούρειος Ίππος τοποθετηθεί σε πολύπλοκους καταλόγους, που δε χρησιμοποιούνται συχνά, να υπάρξουν λάθη πληκτρολόγησης που θα οδηγήσουν στην εκτέλεση καταστροφικού κώδικα. Μπορεί, επίσης, ο επικίνδυνος κώδικας να έχει τοποθετηθεί σε φάκελο υπερχρήστη, όπως για παράδειγμα ο /bin και κάποιο λάθος να οδηγήσει πάλι σε ολέθρια αποτελέσματα.

2.5. Spoofing



Spoofing είναι ο όρος ο οποίος χρησιμοποιείται για να περιγράψει την κατάσταση κατά την οποία ένας εισβολέας χρησιμοποιεί κάποιο υπολογιστή προσποιούμενος στο σύστημα στο οποίο επιτίθεται ότι ο υπολογιστής που χρησιμοποιεί είναι κάποιος άλλος τον οποίο το σύστημα εμπιστεύεται και συνεπώς μπορεί να εκτελέσει λειτουργίες που κανονικά δεν θα επιτρεπόταν.

Το spoofing δεν απαιτεί πολλές γνώσεις σχετικά με password και μεθόδους πιστοποίησης χρηστών όπως οι προηγούμενες μέθοδοι. Έχει σχέση μόνο με το να νομίζει το δίκτυο ότι ο υπολογιστής που χρησιμοποιεί ο εισβολέας είναι κάποιος άλλος υπολογιστής που το δίκτυο εμπιστεύεται.

Τρόπος Λειτουργίας:

Για να καταλάβουμε πως λειτουργεί το spoofing μπορούμε να δούμε μια συγκεκριμένη μορφή της τεχνικής αυτής που λέγεται *IP spoofing.*

Η *IP spoofing* είναι αναπόσπαστο μέρος πολλών επιθέσεων στο δίκτυο και αποτελεί βέβαια αποτέλεσμα της *(blind spoofing).* Μια κοινή παρανόηση είναι ότι η IP Spoofing μπορεί να χρησιμοποιηθεί για να αποκρύψει την IP διεύθυνσή σας ενώ σερφάρετε στο διαδίκτυο, μιλάτε online, στέλνετε e-mail και ούτω καθεξής. Αυτό γενικά δεν ισχύει γιατί φτιάχνοντας την διεύθυνση της IP προέλευσης *(IP destination)* προκαλούνται αντιδράσεις όταν είναι σε λάθος κατεύθυνση κάτι που σημαίνει ότι δεν μπορείτε να δημιουργήσετε κανονική σύνδεση με το δίκτυο.

Ορισμένες απ' τις πιο διαδεδομένες δραστηριότητες του spoofing είναι

- το e-mail spoofing,
- mac-address spoofing,
- DNS spoofing,
- ενώ σχετικά νέα τεχνολογία είναι το spoofing μέσω sms.

2.6. Ηλεκτρονικό ψάρεμα *(phishing)*

Phishing ή πλαστογράφηση μάρκα ή *το* λανάρισμα *είναι* μια παραλλαγή του "ψαρέματος".

1ο ορισμός:

Η ιδέα είναι ότι πετάνε ένα δόλωμα με τις ελπίδες ότι ενώ οι περισσότεροι θα αγνοήσουν το δόλωμα, μερικοί θα μπουν στον πειρασμό να το δαγκώσουν.

2ο ορισμός:

Είναι μια μέθοδος ηλεκτρονικής εξαπάτησης από κοινούς απατεώνες που έχουν ωστόσο βαθιά γνώση της τεχνολογίας. Και γίνεται μέσω αποστολής μηνυμάτων email.

Τρόπος Λειτουργίας

Το ηλεκτρονικό ψάρεμα ξεκίνησε, με το phone phreaking, όταν ακόμα οι hackers έκαναν επιθέσεις στα τηλεφωνικά δίκτυα, επεμβαίνοντας στις γραμμές και αποσπώντας κρίσιμες πληροφορίες από προσωπικές συζητήσεις.

Στην διαδικτυακή του μορφή πρωτοεμφανίστηκε το 1995 μέσω της υπηρεσίας e-mail, και στη συνέχεια με άμεσο μήνυμα *(instant messaging).* Ο hacker στέλνει ένα e-mail ή άμεσο μήνυμα στο 'θύμα', στο οποίο συστήνεται ως αξιόπιστο πρόσωπο που ανήκει σε κάποια εταιρία ή οργανισμό, πολλές φορές και την ίδια την υπηρεσία του e-mail, και ζητά από το θύμα κάποια προσωπικά στοιχεία.

Βασικό εργαλείο του ηλεκτρονικού ψαρέματος είναι οι αποπλανητικοί σύνδεσμοι δλδ ο χρήστης βρίσκεται σε μία ιστοσελίδα, e-mail ή άμεσο μήνυμα, και τον παραπέμπουν σε έναν σύνδεσμο επιφανειακά αξιόπιστο, αλλά είναι φτιαγμένος έτσι ώστε να τον οδηγεί σε διαφορετική ιστοσελίδα από αυτή που προβλέπεται. Αυτό είναι κάτι πολύ κρίσιμο αλλά ταυτόχρονα και πολύ εύκολο στη δημιουργία του, αφού σε έναν απλό html κώδικα δίνεται η δυνατότητα να μετατρέψει κανείς τον τίτλο του συνδέσμου όπως θέλει και κάπως έτσι λειτουργούν και οι ψεύτικες ιστοσελίδες, που μέσω παραπλανητικών συνδέσμων, οδηγούν τους χρήστες σε σελίδες οπτικά πανομοιότυπες με τις αυθεντικές ιστοσελίδες, που ανήκουν όμως στον server του hacker.

Το «Phishing» μπορεί να γίνει ακόμα πιο επίφοβο, όταν χρησιμοποιούνται μέθοδοι ακόμα πιο δύσκολοι στην ανίχνευση τους:

Ένα από αυτούς είναι το λεγόμενο *«IDN spoofing»,* μέσω του οποίου με κακό χειρισμό των International Domain Names (IDN), πανομοιότυπα URL μπορούν να οδηγούν σε διαφορετικές ιστοσελίδες, δεν λύνεται ούτε με τα υπάρχοντα πιστοποιητικά αφού είναι πλέον πολύ εύκολο ακόμα και για τους hackers να αποκτήσουν πιστοποιητικό αυθεντικότητας.

Πολλές φορές οι phishers εξαπατούν ακόμα και τα anti-phishing προγράμματα ή καλύπτουν τα ίχνη τους με χρήση φίλτρων, όπως εικόνες ή flashplayer αντί για κείμενο ή την αξιοποίηση JavaScript για την κάλυψη του URL με κάποιο άλλο.

Στη δεύτερη περίπτωση είτε τοποθετείται μία εικόνα πάνω στο πραγματικό URL, η οποία δείχνει το πλαστό, είτε το πραγματικό URL κρύβεται πλήρως και στη θέση του μπαίνει το ψεύτικο. Ο θύτης μπορεί επίσης να εκμεταλλευτεί προβλήματα στον κώδικα της αυθεντικής ιστοσελίδας και προκαλέσει την επίθεση μέσω αυτής.

Άλλες τεχνικές Phishing χρησιμοποιούν αναδυόμενα παράθυρα «pop-up windows», πολλαπλές καρτέλες «tab-nabbing» ή ακόμα και τη δημιουργία ψεύτικων δημοσίων δικτύων σε αεροδρόμια, ξενοδοχεία και καφετέριες.

Για παράδειγμα

Το 2003 είδε τον πολλαπλασιασμό μιας απάτης phishing στο οποίο οι χρήστες έλαβαν e-mails δήθεν από eBay υποστηρίζοντας ότι ο λογαριασμός του χρήστη ήταν έτοιμος να

διακοπεί εκτός εάν έκανε κλικ στον παρεχόμενο σύνδεσμο και να ενημερώνονται τα στοιχεία της πιστωτικής κάρτας ότι η πραγματική eBay είχε ήδη.

Επειδή είναι σχετικά απλό να κάνει μια ιστοσελίδα να μοιάζει με ένα νόμιμο χώρο οργανώσεις που μιμούνται τον «HTML κώδικα» , η απάτη υπολογίζονται σε ανθρώπους που παρασυρθήκαν ώστε να σκέφτονται ότι μπορούν όντως να ενημερώνονται από το eBay και στη συνέχεια να πηγαίνουν στην ιστοσελίδα του eBay να ενημερώνουν τα στοιχεία του λογαριασμού τους .

Για να προστατευτούμε από το phishing, πρέπει να ακολουθήσουμε τις παρακάτω βασικές οδηγίες.

1. Να είστε ιδιαίτερα προσεκτικοί με τα email που ζητούν προσωπικές, εμπιστευτικές πληροφορίες ιδιαίτερα οικονομικής φύσης.

   Οι νόμιμες, αξιόπιστες εταιρείες δεν θα ζητήσουν ποτέ ευαίσθητες προσωπικές πληροφορίες μέσω email.

2. Μην υποκύψετε στις πιέσεις *να δώσετε άμεσα τις προσωπικές* πληροφορίες που σας ζητούνται.

   Οι απατεώνες χρησιμοποιούν συνήθως εκφοβιστικές τακτικές απειλώντας ότι εάν ο χρήστης δεν προβεί άμεσα στην ενημέρωση συγκεκριμένων πληροφοριών θα απενεργοποιηθεί ο λογαριασμός του ή θα καθυστερήσει η παροχή ορισμένων υπηρεσιών. Αυτό που πρέπει να κάνετε είναι να απευθυνθείτε απευθείας στον αποστολέα και να επιβεβαιώσετε τη γνησιότητα του μηνύματος.

3. Εξοικειωθείτε με την πολιτική προστασίας απορρήτου της ιστοσελίδας που χρησιμοποιείτε.

4. Μάθετε να ξεχωρίζετε τα γενικού χαρακτήρα μηνύματα *που ζητούν* πληροφορίες.

   Τα παραπλανητικά μηνύματα συνήθως δεν είναι προσωποποιημένα, σε αντίθεση με τα γνήσια στα οποία συνήθως η τράπεζά σας αναφέρεται στον αριθμό λογαριασμού που διατηρείτε σε αυτήν.

5. Μην συμπληρώνετε ποτέ τα προσωπικά στοιχεία σας σε φόρμες ενσωματωμένες σε μηνύματα email.

6. Μην χρησιμοποιείτε ποτέ τους συνδέσμους ενός email για πρόσβαση σε μια τοποθεσία web. Αντίθετα, ανοίξτε ένα νέο παράθυρο στο πρόγραμμα περιήγησης και πληκτρολογήστε απευθείας στη γραμμή διεύθυνσης το URL της τοποθεσίας.

7. Έχετε εγκατεστημένο αξιόπιστο λογισμικό για την καταπολέμηση του phishing.

   Το *Norton Internet Security εντοπίζει και μπλοκάρει αυτόματα τις πλαστές τοποθεσίες web. Επίσης, επαληθεύει τη γνησιότητα των γνωστότερων ιστοσελίδων τραπεζών και ηλεκτρονικών αγορών.*

ΚΕΦΑΛΑΙΟ3: ΚΑΚΟΒΟΥΛΕΣ ΕΠΙΘΕΣΕΙΣ ΣΤΟ ΔΙΑΔΥΚΤΙΟ

3.1 Εισαγωγή

Ένα δίκτυο συνίσταται από τη διασύνδεση δυο ή περισσοτέρων υπολογιστικών συστημάτων κατά τέτοιο τρόπο ώστε να παρέχεται η δυνατότητα στους χρήστες να επωφελούνται από ολόκληρο το υπολογιστικό δυναμικό.

Αυτό πραγματοποιείται μέσω της ανταλλαγής πληροφοριών μεταξύ των χρηστών και της κοινής χρήσης των διαθέσιμων υπολογιστικών πόρων.

Ένα εύλογο ερώτημα που απασχολεί τον σύγχρονο άνθρωπο ο οποίος βλέπει την τεχνολογία των ηλεκτρονικών υπολογιστών να καλπάζει και να αναπτύσσεται με γρήγορους ρυθμούς, είναι το γιατί οι υπολογιστές είναι ανασφαλείς.

3.2. Είδη επιθέσεων στο διαδίκτυο

Θα δούμε και θα αναλύσουμε τις διάφορες τεχνικές που χρησιμοποιούν συνήθως οι «εισβολείς» με στόχο να μπορέσουν να αποκτήσουν πρόσβαση σε υπολογιστικά συστήματα, να έχουν την δυνατότητα του πλήρη ελέγχου απομακρυσμένων συστημάτων και την πρόκληση ζημιών ή «τρώση» ενός συστήματος ανεξάρτητα των επιδόσεών αυτού.

1. Ανίχνευση δικτυακών υπηρεσιών συστημάτων *(probes, scans)*

   Μια ανίχνευση ενός συστήματος χαρακτηρίζεται από ασυνήθιστες προσπάθειες για να αποκτήσει κάποιος πρόσβαση ή να ανακαλύψει πληροφορίες για το σύστημα αυτό. Το συνηθέστερο είναι το δεύτερο διότι αν κάποιος καταφέρει να ανακαλύψει πληροφορίες για ένα σύστημα είναι αρκετά πιθανό να καταφέρει να παραβιάσει την ασφάλειά του εκμεταλλευόμενος τις αδυναμίες που είναι ήδη γνωστές για το συγκεκριμένο σύστημα.

Σαν παραδείγματα ανίχνευσης:

Η προσπάθεια για είσοδο στο σύστημα σε λογαριασμό χρήστη που δεν χρησιμοποιείται (όπως κάποιοι λογαριασμοί που υπάρχουν απλά για τις λειτουργίες των υπηρεσιών του συστήματος) και η σάρωση θυρών. Πρόκειται για μια διαδικασία αποστολής ερωτημάτων σε διακομιστές, με σκοπό να ληφθούν πληροφορίες για τις υπηρεσίες που προσφέρουν, καθώς και για το χρησιμοποιούμενο επίπεδο ασφαλείας

Από τη στιγμή που ο επίδοξος εισβολέας μάθει ποιες υπηρεσίες προσφέρει το μηχάνημα-στόχος, μπορεί στη συνέχεια να σχεδιάσει την επίθεσή του βασιζόμενος σε γνωστές αδυναμίες των υπηρεσιών.

Αξίζει να σημειωθεί ότι χρησιμοποιούνται και αυτοματοποιημένα εργαλεία για ανίχνευση συστημάτων που μπορούν να πραγματοποιήσουν ένα πολύ μεγαλύτερο αριθμό ανιχνεύσεων. Τέτοια εργαλεία εκτός από εισβολείς χρησιμοποιούνται και από διαχειριστές δικτύων για να μπορέσουν να διαπιστώσουν τυχόν αδυναμίες που παρουσιάζουν τα συστήματά τους.

2. Ανιχνευτές δικτυακών πακέτων *(packet sniffers)*

Ένας ανιχνευτής πακέτων *(packet sniffer)* είναι μια εφαρμογή λογισμικού που μπορεί να συλλάβει όλα τα πακέτα που κυκλοφορούν στο δίκτυο. Αν τα πακέτα δεν είναι κρυπτογραφημένα μια τέτοια εφαρμογή μπορεί να δώσει χρήσιμες πληροφορίες σε εισβολείς, όπως στοιχεία και συνθηματικά λογαριασμών χρηστών, αριθμούς πιστωτικών καρτών, και διάφορα άλλα προσωπικά στοιχεία χρηστών. Τα πακέτα περιέχουν απλό κείμενο δηλ: η πληροφορία που στέλνεται στο δίκτυο δεν είναι κρυπτογραφημένη. Αφού τα πακέτα δεν είναι κρυπτογραφημένα μπορούν να επεξεργαστούν από οποιαδήποτε εφαρμογή που τα πιάνει από το δίκτυο.

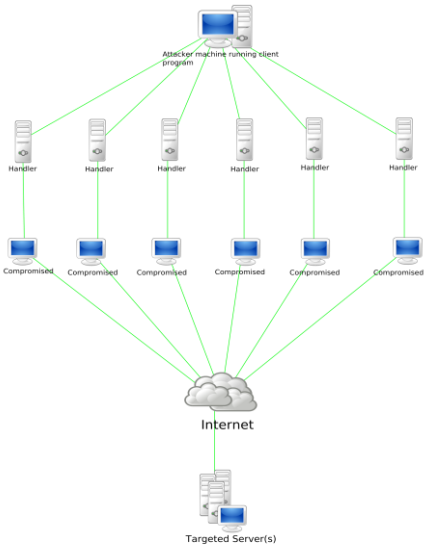
Τώρα οι ανιχνευτές πακέτων μπορούν να δώσουν πληροφορίες σχετικά και με τις τοπολογίες δικτύων πράγμα που οι εισβολείς βρίσκουν ιδιαίτερα χρήσιμο. Τέτοιες πληροφορίες μπορεί να είναι:

- ποιοι υπολογιστές παρέχουν συγκεκριμένες δικτυακές υπηρεσίες,
- πόσοι υπολογιστές βρίσκονται στο τοπικό δίκτυο,
- ποιοι υπολογιστές έχουν πρόσβαση σε άλλους κλπ.

Όλα αυτά μπορούν να εξαχθούν από τα πακέτα που κυκλοφορούν στο δίκτυο λόγω των καθημερινών λειτουργιών.

3. Προσποίηση διεύθυνσης IP *(IP Spoofing)*

Ο όρος **IP spoofing** στην επιστήμη των υπολογιστών αναφέρεται στην δημιουργία πακέτων IP με ψεύτικη διεύθυνση προέλευσης ούτως ώστε να συγκαλυφθεί η ταυτότητα του αποστολέα του πακέτου και ο παραλήπτης να νομίζει ότι προήλθε από άλλον υπολογιστή.



Μια επίθεση τέτοιου είδους συμβαίνει όταν κάποιος εισβολέας έξω από το δίκτυο που θέλουμε να προστατέψουμε προσποιείται ότι είναι μηχάνημα με διεύθυνση μέσα στο εύρος των διευθύνσεων που εμπιστευόμαστε *(εσωτερικές του δικτύου ή κάποιες από εξωτερικές)*.

Χρησιμοποιώντας διευθύνσεις που βρίσκονται σε εύρος που εμπιστευόμαστε ο επιτιθέμενος μπορεί να κερδίσει πρόσβαση σε δικτυακές υπηρεσίες που προορίζονται για έμπιστους χρήστες του δικτύου. Ο εισβολέας αποστέλλει μηνύματα με διευθύνσεις IP που υποδεικνύουν ότι αυτά προέρχονται από ένα "έμπιστο" port.

Ο επίδοξος εισβολέας αρχικά καταφεύγει σε ένα πλήθος τεχνικών για να βρει μια διεύθυνση IP που αντιστοιχεί σε ένα τέτοιο port. Στη συνέχεια, τροποποιεί τα περιεχόμενα της κεφαλής των πακέτων που θα αποστείλει, ώστε να φαίνεται ότι προέρχονται από ένα έμπιστο port.

Για παράδειγμα:

Ο εισβολέας μπορεί να μιμηθεί κάποιον από τους εσωτερικούς χρήστες ενός φορέα με τρόπο που εκθέτει τον οργανισμό στον οποίο αυτός βρίσκεται (π.χ. αποστολή ενοχλητικού ηλεκτρονικού ταχυδρομείου).

Τέτοιες επιθέσεις είναι πιο εύκολες όταν ο εισβολέας γνωρίζει κωδικό και συνθηματικό ενός έγκυρου χρήστη αλλά είναι δυνατές απλά και μόνο με τη γνώση των πρωτοκόλλων επικοινωνίας.

4. Κατανεμημένη επίθεση άρνηση Υπηρεσίας*(Denial of Service – DoS)*

Είναι μια από τις πλέον διάσημες αποτελεσματικές μεθόδους που χρησιμοποιούν οι εισβολείς για να θέτουν εκτός λειτουργίας δικτυωμένους υπολογιστές.

Στην πληροφορική, ένα denial-of-service (DoS) ή κατανεμημένη επίθεση άρνησης υπηρεσίας (DDoS) είναι μια προσπάθεια να κάνει μια μηχανή ή ένα δίκτυο πόρων μη διαθέσιμο στους προβλεπόμενους του χρήστες.

Θα πρέπει να αναφέρουμε ότι για τους περισσότερους ειδικούς οι επιθέσεις«Denial of Service (DoS)» ως μέσο εισβολής σε ένα σύστημα θεωρούνται πολύ ενοχλητικές, αλλά όχι θανάσιμα επικίνδυνες για ένα σύστημα.

Ο επιτιθέμενος μπορεί ίσως να διακόψει τη λειτουργία ενός μηχανήματος για μερικές ώρες, αλλά δεν έχει τη δυνατότητα να αποκτήσει πρόσβαση σε αυτό και να τροποποιήσει δεδομένα σε κάποιο από τα άλλα μηχανήματα τα οποία μοιράζονται το ίδιο δίκτυο. Δυστυχώς, αυτό δεν είναι αλήθεια. Μια καλή και δοκιμασμένη τεχνική χρησιμοποιήθηκε από τον *Kevin Mitnick* για να εισβάλει στο σύστημα του διώκτη του *κ. Tsutomu Shinomura* είναι η εισβολή σε ένα δίκτυο μέσω επίθεσης DoS σε έναν από τους servers' του.

Όταν το μηχάνημα αυτό πάψει να λειτουργεί, τότε ο επιτιθέμενος επικοινωνεί με άλλα μηχανήματα του ίδιου δικτύου "υποκρινόμενος" ότι τα πακέτα που στέλνει προέρχονται από το αχρηστεμένο και εκτός λειτουργίας πλέον μηχάνημα. Με τον τρόπο αυτό αυξάνονται σημαντικά οι πιθανότητες να επιτευχθεί πρόσβαση στα άλλα μηχανήματα του δικτύου, καθώς η εντολή πρόσβασης δεν δίνεται από έναν τρίτο, αλλά από μια έμπιστη πηγή (ένα μηχάνημα εντός του δικτύου)

Οι πιο συνηθισμένοι τύποι Denial Of Service Επιθέσεων είναι :

- Οι επιθέσεις που εκμεταλλεύονται αδυναμίες του πρωτοκόλλου **TCP/IP**
- Οι επιθέσεις που εκμεταλλεύονται αδυναμίες του **IPv4**
- Οι επιθέσεις που προσπαθούν να **εξαντλήσουν όλους τους πόρους** *(resources)* – μνήμη, CPU, Bandwidth - του συστήματος στόχου με αποτέλεσμα την διακοπή της λειτουργίας του.

Ας δούμε μερικές D.O.S. επιθέσεις που σχετίζονται με το πρωτόκολλο TCP/IP. Οι πιο γνωστές: είναι οι Ping of Death, Teardrop, SYN Attack, Land Attack και Smurf Attack.

- Ping of Death :Αυτή η επίθεση είναι πολύ γνωστή και χρησιμοποιούταν παλαιότερα για να κάνει απομακρυσμένα συστήματα να "παγώνουν" ή ακόμα και να κάνουν αυτόματη επανεκκίνηση *(reboot)*, έτσι ώστε οι χρήστες να μην μπορούν να τα χρησιμοποιήσουν.

Αυτό πλέον δεν είναι εφικτό μια και στις μέρες μας σχεδόν όλοι οι Διαχειριστές των Συστημάτων *(Systems Administrators)* έχουν αναβαθμίσει τα συστήματά τους κάνοντάς τα ασφαλή από τέτοιες επιθέσεις.

Ο τρόπος για να γίνει αυτή η επίθεση είναι: Να στείλει κάποιος ένα πακέτο data *(data packet)* που υπερβαίνει το μέγιστο επιτρεπόμενο όριο bytes του πρωτοκόλλου TCP/IP, που είναι **65536**. Στέλνοντας ένα πακέτο data *(data packet)* μεγαλύτερο από αυτό, αμέσως το σύστημα/στόχος πάθαινε κατάρρευση *(crash)* ή και "πάγωνε" *(hang)* ή και έκανε επανεκκίνηση *(reboot).*

Το Ping Of Death έγινε πολύ δημοφιλές λόγω της ευκολίας στην υλοποίηση του. Επίσης αυτού του τύπου η επίθεση ήταν και είναι ακόμα πολύ δημοφιλής στο IRC *(Internet Relay Chat)*

- Teardrop: Αυτή η επίθεση εκμεταλλεύεται την αδυναμία του πρωτοκόλλου TCP/IP στην επανασύνδεση *(reassembly)* των πακέτων δεδομένων *(data packets)* κατά την λήψη τους.

Όταν στέλνονται data στο Internet αυτά κατανέμονται σε μικρότερα κομμάτια στην υπολογιστή που κάνει την μετάδοση και συναρμολογούνται πάλι στον υπολογιστή που λαμβάνει. Ας υποθέσουμε ότι θέλουμε να στείλουμε 8000 bytes από έναν υπολογιστή σε έναν άλλον. Δεν θα τα στείλουμε όλα μαζί με μία μετάδοση *(transmission)* αλλά θα κοπούν σε μικρότερα πακέτα data *(data packets)* και κάθε πακέτο θα έχει συγκεκριμένο κομμάτι από τα 8000 bytes όπως :

- $1^{ο}$ πακέτο θα έχει byte 1 έως byte 1500,
- $2^{ο}$ πακέτο θα έχει byte 1501 έως byte 3000,
- $3^{ο}$ πακέτο θα έχει byte 3001 έως byte 4000 κ.λ.π.

Αυτά τα πακέτα έχουν στο αρχικό τους κομμάτι *(TCP header)* ένα πεδίο *(offset)* που περιγράφει πως θα γίνει η συναρμολόγηση στο σύστημα που θα λάβει τα πακέτα.

Στην επίθεση αυτή τα πακέτα που στέλνονται υπερκαλύπτουν το ένα το άλλο με αποτέλεσμα όταν το σύστημα που τα λαμβάνει προσπαθεί να τα συναρμολογήσει (reassembly) παθαίνει κατάρρευση (crash) ή/και "πάγωμα" (hang) ή/και επανεκκίνηση

- SYN Attack/Land Attack: Αυτές οι δύο επιθέσεις είναι ίδιες με τη διαφορά ότι:

Η *«SYN attack»* χρησιμοποιεί ανύπαρκτες διευθύνσεις IP για να αναγκάσει το σύστημα στόχο να περιμένει για πάντα για μια απάντηση από ανύπαρκτη IP διεύθυνση ενώ

Η *«Land Attack»* αντί για ανύπαρκτες IP διευθύνσεις χρησιμοποιεί την IP του συστήματος-στόχου και αυτό έχει ως αποτέλεσμα μια ατελείωτη σειρά *(endless loop)* επεξεργασίας για το σύστημα.

Και οι δύο επιθέσεις έχουν ως αποτέλεσμα, όταν γίνονται μαζικά, κατάρρευση *(crash)* ή/και "πάγωμα" *(hang)* ή/και επανεκκίνηση *(reboot).*

- Smurf Attack: Η «Smurf attack» είναι μια επίθεση όπου στέλνεται ένας υπέρογκος αριθμός από ping requests συνήθως στον router του δικτύου, χρησιμοποιώντας ψεύτικες *(spoofed)* IP διευθύνσεις μέσα από το ίδιο το δίκτυο.

Κάθε φορά που ο router δέχεται ένα Ping request θα το διανείμει *(route it)* ή θα απαντήσει σε αυτό *(echo back)*, με αποτέλεσμα την υπερφόρτωση *(flood)* του δικτύου με πακέτα και την διακοπή της λειτουργίας του.

- Άλλοι τύποι απειλών: Κάποιοι άλλοι τύποι απειλών για την ασφάλεια, την ιδιωτικότητα και την ανωνυμία περιλαμβάνουν:

1. Επιθέσεις Αντίστροφης Πορείας *(Trace Back Attack)*

Σε μία «επίθεση αντίστροφης πορείας», ένας επιτεθείς ξεκινά από ένα γνωστό ανταποκριτή και ιχνηλατεί το μονοπάτι προς τον ιδρυτή είτε κατά το μονοπάτι προώθησης είτε κατά το αντίστροφο μονοπάτι.

2. Επιθέσεις από Εχθρικούς Συνεργάτες, *(Malicious Collaborators)*

Είναι επιθετικά σε πρωτόκολλα που επικοινωνούν μεταξύ τους για να ανακαλύψουν την ταυτότητα κάποιου ιδρυτή.

3. Επιθέσεις Κωδικοποίησης Μηνυμάτων, *(Message Coding Attack)*

4. Επιθέσεις Χρονοσήμανσης, *(Timing Attack)*

Η απειλή των «επιθέσεων χρονοσήμανσης» περιγράφει την ανάλυση των πακέτων που μεταδίδονται και ανιχνεύει την πηγή τους εξαιτίας των συσχετισμένων χρόνων.

5. Επιθέσεις Υπερφόρτωσης Μηνυμάτων, *(Flooding Attack)*

6. Επιθέσεις Περιόδων Σύνδεσης,*(Connection Period Attacks)*

Ο τύπος αυτής της επίθεσης αναφέρεται στην απώλεια της ιδιωτικότητας μιας ομάδας και του επιπέδου ανωνυμίας της, με βάση το γεγονός ότι οι περισσότεροι χρήστες εγκαθιστούν έναν περιορισμένο αριθμό συνδέσεων και έχουν ένα συνήθη τύπο συμπεριφοράς στον ιστό.

7. Επιθέσεις από Αξιοποίηση Cookies

Όπως είναι γνωστό, τα cookies αποτελούν αρχεία δεδομένων που τοποθετούνται στο σύστημα ενός χρήστη με σκοπό να παρέχουν προσωπικές πληροφορίες σε εξυπηρετητές, τους οποίους επισκέπτονται οι χρήστες

8. Επιθέσεις σε Υπηρεσίες Προσωποποίησης.

Οι υπηρεσίες προσωποποίησης προσφέρονται κατά τη διαδικασία προσέλκυσης νέων χρηστών σε ένα περιβάλλον. Υπάρχει πάντοτε η απειλή αποκάλυψης προσωπικών πληροφοριών κατά τη διάρκεια της διαδικασίας εγγραφής.

3.3 Κίνδυνοι της ασφάλειας σε ένα δίκτυο

Η έννοια της ασφάλειας Δικτύου Υπολογιστών σχετίζεται με την ικανότητα μιας επιχείρησης ή ενός οργανισμού να προστατεύει τις πληροφορίες του από τυχόν αλλοιώσεις και καταστροφές, καθώς και από μη εξουσιοδοτημένη χρήση των πόρων του.

Εκτός αυτού μια άλλη έννοια για την Ασφάλεια Δικτύου Υπολογιστών, θεωρείται ως η δυνατότητα ενός δικτύου ή συστήματος πληροφοριών να αντισταθεί, σε δεδομένο επίπεδο αξιοπιστίας, σε τυχαία συμβάντα ή κακόβουλες ενέργειες που θέτουν σε κίνδυνο τη διάθεση, την επαλήθευση ταυτότητας, την ακεραιότητα και την τήρηση του απορρήτου των δεδομένων που έχουν αποθηκευτεί ή μεταδοθεί καθώς και τις συναφείς υπηρεσίες που παρέχονται είτε είναι προσβάσιμες μέσω των δικτύων και συστημάτων αυτών.

Οι κυριότεροι κίνδυνοι που συνεπάγονται από τη χρήση του Διαδικτύου είναι: *(αρχικά θα αναφερθούμε αναφορικά σε αυτούς και στην συνέχεια θα τους αναλύσουμε εκτενέστερα)*:

1. Ακατάλληλο Περιεχόμενο
2. Ανεπιθύμητα Μηνύματα *(Spam)*
3. Αποξένωση
4. Αποπλάνηση *(Grooming)*
5. Βίαια Παιχνίδια
6. Εθισμός *(Internet Addiction)*
7. Εκφοβισμός *(Cyberbullying)*
8. Επιβλαβείς Συμπεριφορές
9. Ηλεκτρονικός Τζόγος
10. Ιοί
11. Παιδική Πορνογραφία
12. Παραβίαση Ιδιωτικότητας
13. Παραπληροφόρηση *(Misinformation)*
14. Παραποίηση Γλώσσας
15. Υποκλοπή Προσωπικών στοιχείων *(Phising)*
16. Φυσικές Παθήσεις

Για την ανάλυση κάθε ενός κινδύνου θα δώσουμε μια μικρή περιγραφή του όρου, που μπορεί να συμβεί αυτός ο κίνδυνος και το σημαντικότερο τον τρόπο για την αντιμετώπιση του.

1. Ακατάλληλο Περιεχόμενο:

Ο όρος ακατάλληλο περιεχόμενο είναι υποκειμενικός σε σχέση με την ηλικία ή και την ψυχική κατάσταση του κάθε ατόμου.

Συνήθως με τον όρο ακατάλληλο περιεχόμενο, αναφερόμαστε σε περιεχόμενο, το οποίο μπορεί να περιλαμβάνει ρατσιστικό ή ξενοφοβικό περιεχόμενο, προώθηση επιβλαβών συμπεριφορών, προώθηση τυχερών παιχνιδιών, παρουσίαση πορνογραφικού υλικού, προώθηση βίας κ.λ.π.

Για παράδειγμα:

Ένα περιεχόμενο μπορεί να θεωρηθεί μη αποδεκτό για ένα μικρό παιδί εάν αυτό περιέχει ακατάλληλο υλικό, το οποίο μπορεί να προκαλέσει ψυχικές διαταραχές, να σοκάρει ή ακόμα να προωθήσει λάθος συμπεριφορές. Το ίδιο περιεχόμενο μπορεί όμως να θεωρηθεί κατάλληλο για ένα μεγαλύτερο σε ηλικία άτομο.

Μπορεί να συμβεί σε:

- Ιστοσελίδες αμφίβολου προέλευσης
- Μέσα από τα διαδικτυακά παιχνίδια *(online games)*
- Μέσω του ηλεκτρονικού ταχυδρομείου
- Μέσω του κινητού τηλεφώνου

Τρόποι Αντιμετωπίσεις:

1. Καταγγέλλουμε ιστοσελίδες με ακατάλληλο περιεχόμενο ή στο τηλέφωνο 22674747 *(Γραμμή Καταγγελιών HotLine).*
2. Αυτά που διαβάζουμε ή βλέπουμε στο Διαδίκτυο δεν είναι πάντοτε ορθά. Ρωτάμε άτομα που εμπιστευόμαστε, εάν έχουμε αμφιβολίες.
3. Αξιολογούμε τις πληροφορίες που βρίσκουμε στο Διαδίκτυο και ελέγχουμε το συγγραφέα, την προέλευση της σελίδας, τη βιβλιογραφία της πληροφορίας.

4. Χρησιμοποιούμε πολλαπλές πηγές πληροφοριών και διασταυρώνουμε τις πληροφορίες που βρίσκουμε στο Διαδίκτυο.
5. Εγκαθιστούμε λογισμικό φιλτραρίσματος πληροφοριών σε υπολογιστές που χρησιμοποιούνται από παιδιά.
6. Εάν κάτι μας κάνει να νιώθουμε άβολα ή αμήχανα, κλείνουμε το φυλλομετρητή μας και το αναφέρουμε αμέσως σε κάποιο ενήλικα.
7. Χρησιμοποιούμε τη δυνατότητα του φυλλομετρητή μας που ονομάζεται "Αγαπημένα" για να τοποθετήσουμε τις ιστοσελίδες που είναι ασφαλείς και επισκεπτόμαστε συχνά.
8. Ως γονείς ενημερωνόμαστε για τα είδη περιεχομένου που υπάρχουν και συζητάμε με τα παιδιά για το θέμα αυτό.
9. Εάν τα παιδιά μας είναι μικρότερα των 10 ετών μια καλή πρακτική θα ήταν να καθόμαστε μαζί τους, όταν αυτά χρησιμοποιούν το Διαδίκτυο.
10. Ως γονείς μπορούμε να αλλάξουμε την σελίδα του φυλλομετρητή που χρησιμοποιούν τα παιδιά μας σε μία ασφαλή σελίδα ειδικά σχεδιασμένη για την ηλικία τους *(π.χ. το Yahoo!Kids, www.imeakia.gr, Discovery Kids).*
11. Ως γονείς μπορούμε να ελέγχουμε και να καταγράφουμε την πλοήγηση των παιδιών μας, χρησιμοποιώντας ειδικά λογισμικά που καταγράφουν τη δραστηριότητα του υπολογιστή του παιδιού στο δικό μας υπολογιστή *(π.χ. το Parental Software και το Web Watcher)*

2. Ανεπιθύμητα Μηνύματα *(Spam)*

Ανεπιθύμητα Μηνύματα θεωρούνται τα μηνύματα εκείνα που υπό κανονικές συνθήκες οι χρήστες δεν θα επέλεγαν να δουν και τα οποία διανέμονται σε μεγάλο αριθμό παραληπτών.

Παραδείγματα ανεπιθύμητων μηνυμάτων είναι:

α) Μηνύματα που περιέχουν διαφημιστικά για αμφίβολα προϊόντα, **b)** μηνύματα με περιεχόμενο που συσχετίζεται με ψευδοτυχερά παιχνίδια, ψευδονομικές υπηρεσίες,

πορνογραφικό υλικό κτλ. **c)** Πολύ συχνό φαινόμενο είναι και η λήψη αλυσιδωτών μηνυμάτων *(chain e-mails).* Δλδ τα μηνύματα αυτά είναι, συνήθως ανεπιθύμητα και ο αποστολέας ζητά από τον παραλήπτη να προωθήσει το μήνυμα σε άλλα άτομα, τα οποία γνωρίζει.

Ο κίνδυνος εδώ, είναι ότι κάθε φορά που προωθούμε ένα μήνυμα, αν δεν είμαστε προσεχτικοί, μαζί με αυτό εμφανίζεται και η ηλεκτρονική διεύθυνση όλων των προηγούμενων ατόμων που προώθησαν το ίδιο μήνυμα. Έτσι δεν γνωρίζουμε ποιος θα παραλάβει το μήνυμα και τι θα κάνει με τις ηλεκτρονικές διευθύνσεις, οι οποίες θα εμφανίζονται σε αυτό.

Πού μπορεί να συμβεί:

- Στο ηλεκτρονικό ταχυδρομείο
- Λίστες ομάδων πληροφόρησης
- Στο κινητό τηλέφωνο

Τρόποι Αντιμετωπίσεις:

1. Είμαστε προσεχτικοί όταν δίνουμε την ηλεκτρονική μας διεύθυνση.
2. Ρυθμίζουμε την υπηρεσία φιλτραρίσματος του ηλεκτρονικού μας ταχυδρομείου, ώστε να σταματά ανεπιθύμητα μηνύματα.
3. Όταν το μήνυμα είναι από άγνωστο αποστολέα να μην παραπλανόμαστε ώστε να κάνουμε κλικ σε συνδέσμους παρόμοιους με: «Κάνε κλικ εδώ, εάν δεν θέλεις να παίρνεις τέτοια μηνύματα», γιατί αυτό επιβεβαιώνει στον αποστολέα ότι η ηλεκτρονική διεύθυνσή μας είναι σωστή. Έτσι, ο αποστολέας θα συνεχίσει να την χρησιμοποιεί ή θα μπορέσει πιο εύκολα να την πουλήσει σε άλλους.
4. Είμαστε προσεχτικοί όταν δίνουμε τον αριθμό του κινητού μας τηλεφώνου. Ανεπιθύμητα μηνύματα μπορούμε να πάρουμε και στο κινητό *(sms spam).* Χρησιμοποιούμε την κρυφή κοινοποίηση*(Bcc)* στο ηλεκτρονικό ταχυδρομείο, εάν θέλουμε να προωθήσουμε κάποιο μήνυμα σε πολλούς παραλήπτες, ούτως ώστε να προστατεύσουμε τις ηλεκτρονικές διευθύνσεις των παραληπτών.
5. Όταν δεχόμαστε ανεπιθύμητα μηνύματα, τα διαγράφουμε χωρίς να τα διαβάζουμε.
6. Είναι καλό να χρησιμοποιούμε δύο διευθύνσεις:
   Η 1η μια για να επικοινωνούμε με φίλους, συγγενείς, συναδέλφους και
   Η 2η για εγγραφές σε υπηρεσίες στο Διαδίκτυο, συμμετοχή σε forum κ.ά.
   Έτσι, αν παίρνουμε πολλά ανεπιθύμητα μηνύματα στη δεύτερη διεύθυνση μπορούμε εύκολα να τη διαγράψουμε και να δημιουργήσουμε μια καινούρια Επίσης μπορούμε να κρύψουμε την ηλεκτρονική μας διεύθυνση από προγράμματα ανίχνευσης ηλεκτρονικών διευθύνσεων.

Αυτό μπορούμε να το κάνουμε, δηλώνοντάς την μέσα σε αρχείο εικόνας ή περιγράφοντας την με κείμενο αντί πληκτρολογώντας την ως έχει *(π.χ. αντί για dog@home.cy πληκτρολογούμε dog at home τελεία cy*)

3. Αποξένωση

Αποξένωση είναι η αλόγιστη και πολύωρη χρήση του Διαδικτύου, δημιουργεί συναισθηματική απόσταση και αλλοιώνει την ποιότητα επικοινωνίας ανάμεσα στους ανθρώπους, κάτι το οποίο τους οδηγεί στην Αποξένωσή τους από τον Πραγματικό Κόσμο

Αρκετοί είναι αυτοί οι οποίοι ξοδεύουν άπειρες ώρες μπροστά στον υπολογιστή παίζοντας διαδικτυακά παιχνίδια, σερφάροντας στο Διαδίκτυο ή ακόμα και επικοινωνώντας με φίλους τους μέσω του Διαδικτύου αναπτύσσουν Διαδικτυακές *(on-line)* σχέσεις χωρίς να εγκαταλείπουν τα σπίτια τους.

Όλα αυτά γίνονται σε βάρος του χρόνου που διαφορετικά μπορούν να έχουν διαθέσιμο για τη συμμετοχή σε άλλες δραστηριότητες με φίλους, γείτονες ή ομάδες ανθρώπων με κοινά ενδιαφέροντα.

Ως αποτέλεσμα, κάποιοι άνθρωποι δεν μπορούν να ταυτιστούν με τους άλλους νιώθοντας αποκλεισμένοι στην εντός του Διαδικτύου κοινωνική τους ζωή.

Πού μπορεί να συμβεί:

- Γενικά στο Διαδίκτυο *(π.χ. διαδικτυακά παιχνίδια, κοινωνικά δίκτυα, δωμάτια συνομιλίας)*

Τρόποι Αντιμετωπίσεις

1. Χρησιμοποιούμε το Διαδίκτυο με μέτρο, συμπεριλαμβάνοντας στο πρόγραμμά μας εναλλακτικές δραστηριότητες που περιλαμβάνουν ενασχόληση με ομαδικά αθλήματα, χορωδίες, χορό και άλλες.
2. Ως γονείς ελέγχουμε και περιορίζουμε το χρόνο που τα παιδιά μας ξοδεύουν στο Διαδίκτυο.
3. Ως γονείς μπορούμε να ελέγχουμε το χρόνο που περνούν τα παιδιά μας στο Διαδίκτυο εγκαθιστώντας ειδικά λογισμικά *(π.χ. KidsWatch Time Control και WatchDog).*
4. Ανάλογα με την ηλικία των παιδιών μας, ως γονείς, μπορούμε να δημιουργήσουμε και να χρησιμοποιήσουμε κανόνες χρήσης του Διαδικτύου.

4. Αποπλάνηση

Αποπλάνηση συμβαίνει όταν άγνωστοι κακόβουλα εκμεταλλεύονται το στοιχείο της ανωνυμίας στο Διαδίκτυο για να προσεγγίσουν ανήλικα παιδιά με στόχο τη σεξουαλική παρενόχληση.

Πού μπορεί να συμβεί:

- Δωμάτια συνομιλίας *(chat rooms)*

Είναι ένας δημοφιλής τρόπος επικοινωνίας μεταξύ των νέων αλλά και δημοφιλές μέσο αποπλάνησης *(Shannon, 2008).*

- Σελίδες κοινωνικών δικτύων

Τρόποι Αντιμετωπίσεις:

1. Δεν δίνουμε τα προσωπικά μας στοιχεία σε ένα δωμάτιο συνομιλίας. Ποτέ δεν μπορούμε να είμαστε σίγουροι για την ταυτότητα του συνομιλητή μας.
2. Δεν συναντούμε κάποιο ξένο, τον οποίο γνωρίσαμε σε ένα δωμάτιο συνομιλίας. Αν μάς ζητηθεί κάτι τέτοιο το συζητάμε αμέσως με κάποιο ενήλικα.
3. Μπορούμε να αποθηκεύουμε τις ηλεκτρονικές μας συνομιλίες. Αν μια συνομιλία μας έκανε να νιώσουμε άβολα ή μας έφερε σε δύσκολη θέση, κρατάμε αντίγραφο. Αυτό θα μας βοηθήσει να καταγγείλουμε τον επιτήδειο που προσπάθησε να μας παραπλανήσει.
4. Διαβάζουμε τους όρους χρήσης, τον κώδικα επικοινωνίας και τη δήλωση απορρήτου στη διαδικτυακή τοποθεσία συνομιλίας, προτού αρχίσουμε τη συνομιλία.
5. Ως γονείς μπορούμε να μάθουμε τη γλώσσα του Διαδικτύου η οποία χρησιμοποιείται από τα νεαρά άτομα.
6. Ως γονείς ενημερωνόμαστε για τις διαδικτυακές γνωριμίες των παιδιών μας και αν παρατηρήσουμε κάτι ύποπτο, τα συμβουλεύουμε ανάλογα.

5. Βίαια Παιχνίδια

Σύμφωνα με έρευνες, εκατομμύρια άτομα αφιερώνουν χρόνο σε καθημερινή βάση σε ηλεκτρονικά παιχνίδια.

Η πιο δημοφιλής κατηγορία παιχνιδιών είναι η κατηγορία παιχνιδιών δράσης η οποία χωρίζεται σε άλλες υποκατηγορίες, όπως:

a. Παιχνίδια πολεμικών τεχνών *(Beat'em up)*
b. Λαβυρίνθων *(maze)*
c. Πλατφόρμας *(platform)*
d. Βολών *(shooters):* Θεωρείται η πλέον βίαια κατηγορία παιχνιδιών και έχει κατακριθεί ιδιαίτερα για τα κακά πρότυπα και τις αρνητικές επιδράσεις που πιθανότατα να έχει, ειδικά σε νεαρά άτομα . Όπως λέει και το όνομα, σκοπός είναι να χρησιμοποιήσουμε όπλα, ώστε να εξοντώσουμε τους αντιπάλους και να ολοκληρώσουμε τις αποστολές του παιχνιδιού.

Πού μπορεί να συμβεί:

- Διαδικτυακά παιχνίδια
- Αυτόνομα παιχνίδια τα οποία μπορούμε να παίξουμε με άλλους παίκτες μέσω δικτύου
- Παιχνίδια κονσόλας

Τρόποι Αντιμετωπίσεις:

1. Ενημερωνόμαστε για τον τρόπο αξιολόγησης του Πανευρωπαϊκού Συστήματος Πληροφόρησης για τα Ηλεκτρονικά Παιχνίδια *(Pan European Game Information - PEGI).*Κοιτάζοντας τη σήμανση PEGI στο κουτί του παιχνιδιού ή στην ιστοσελίδα από την οποία αυτό είναι διαθέσιμο, μπορούμε να προσδιορίσουμε αν ένα παιχνίδι είναι κατάλληλο για μας.
2. Ως γονείς επιτρέπουμε στα παιδιά μας να παίξουν ένα παιχνίδι, μόνο αφού εντοπίσουμε την ειδική PEGI σήμανση του παιχνιδιού που το αξιολογεί σε σχέση

με την ηλικία του χρήστη και είμαστε σίγουροι ότι είναι κατάλληλο για τα παιδιά μας.

3. Ως γονείς παροτρύνουμε τα παιδιά μας να κάνουν συχνά διαλείμματα κατά τη διάρκεια του παιχνιδιού.
4. Ως γονείς παροτρύνουμε τα παιδιά μας να εμπλέκονται σε εναλλακτικές δραστηριότητες *(π.χ. αθλήματα, παιχνίδια στο φυσικό περιβάλλον)*.

6. Εθισμός *(Internet Addiction)*

Σύμφωνα με στατιστικά στοιχεία της Μονάδας Εφηβικής Υγείας (Μ.Ε.Υ.) στην Ελλάδα, το φαινόμενο είναι συχνότερο σε αγόρια, σε δυσλειτουργικές οικογένειες και σε παιδιά με καταθλιπτικά συναισθήματα ή σύνδρομο υπερκινητικότητας.

Εθισμός στο Διαδίκτυο μπορεί να προκύψει με την πολύωρη ενασχόληση ατόμων σε διαδικτυακές δραστηριότητες όπως είναι: τα παιχνίδια, δωμάτια συζητήσεων, ηλεκτρονικός τζόγος και άλλα.

Μπορούμε να καταλάβουμε ότι ένα άτομο είναι εθισμένο όταν χαρακτηρίζεται από τουλάχιστο τρία από τα πιο κάτω:

a. Χρήση του Διαδικτύου για μεγαλύτερο χρονικό διάστημα από το προτιθέμενο
b. Κατανάλωση υπερβολικού χρόνου ή/και χρήματος σε δραστηριότητες σχετικές με το Διαδίκτυο
c. Συμπτώματα Συνδρόμου Απόσυρσης: Όπως για παράδειγμα άγχος, έμμονη σκέψη για το Διαδίκτυο, όνειρα για το Διαδίκτυο Χρήση Διαδικτύου προκειμένου να αποφευχθούν συμπτώματα απόσυρσης
d. Μείωση λειτουργικότητας του ατόμου: Συνήθως παραμελούν την προσωπική τους υγεία, γευματίζουν ανθυγιεινά, σταματούν τα αγαπημένα τους ενδιαφέροντα, εγκαταλείπουν το σχολείο, συγκρούονται έντονα στο σπίτι με τους γονείς τους, έχουν μεγάλη ένταση και θυμό που οδηγεί ακόμα και στη βία *(Chakraborty, 2010)*
e. Συνέχιση χρήσης του Διαδικτύου παρά τη γνώση της παραπάνω δυσλειτουργίας

Πού μπορεί να συμβεί:

- Συνήθως οι έφηβοι εθίζονται παίζοντας διαδικτυακά παιχνίδια ή/και τζόγο
- Σε ιστοσελίδες κοινωνικής δικτύωσης

Τρόποι Αντιμετωπίσεις:

1. Ευαισθητοποιούμαστε και ενημερωνόμαστε για το φαινόμενο του εθισμού.
2. Χρησιμοποιούμε το Διαδίκτυο με μέτρο, συμπεριλαμβάνοντας στο πρόγραμμά μας εναλλακτικές δραστηριότητες που περιλαμβάνουν ενασχόληση με ομαδικά αθλήματα, χορωδίες, χορό και άλλες.
3. Καλλιεργούμε ορθές στάσεις αξιοποίησης του Διαδικτύου από μικρές ηλικίες.
4. Ως γονείς ελέγχουμε και περιορίζουμε το χρόνο που τα παιδιά μας ξοδεύουν στο Διαδίκτυο. Μπορούμε να ελέγχουμε το χρόνο που περνούν τα παιδιά μας στο Διαδίκτυο εγκαθιστώντας ειδικά *λογισμικά (π.χ. KidsWatch Time Control, WatchDog).*
5. Ως γονείς συζητάμε με τα παιδιά μας από νεαρή ηλικία κανόνες χρήσης του Διαδικτύου και δίνουμε εναλλακτικές επιλογές απασχόλησης.
6. Εάν παρατηρήσουμε υπερβολική χρήση ή/και συμπεριφορές εθισμού αναζητούμε βοήθεια στην ιστοσελίδα «www.cyberethics.info »ή στο τηλέφωνο «22674747».

7. Εκφοβισμός *(Cyberbullying)*

Εκφοβισμός είναι η εσκεμμένη, επαναλαμβανόμενη και εχθρική συμπεριφορά απέναντι σε άτομο ή ομάδα ατόμων με σκοπό την πρόκληση συναισθηματικής και ψυχολογικής βλάβης.

Έχει τη μορφή ενός εκφοβιστικού, ρατσιστικού, προσβλητικού ή πρόστυχου ηλεκτρονικού μηνύματος, φωτογραφίας ή βίντεο. Κάποιες φορές ο εκφοβισμός μπορεί να οδηγήσει στο να περιθωριοποιηθούν και να αποκλειστούν άτομο ή άτομα από άλλους.

Πού μπορεί να συμβεί:

- Μέσω ηλεκτρονικού ταχυδρομείου *(e-mail)*
- Στα δωμάτια συναντήσεων *(chat rooms)*
- Σε σελίδες διαμοιρασμού και προβολής βίντεο
- Σε ιστολόγια *(blogs)*

- ή άλλες ιστοσελίδες που στοχεύουν να βλάψουν άτομα

Τρόποι Αντιμετωπίσεις:

1. Εάν πέσουμε θύμα εκφοβισμού, σταματάμε αμέσως την επικοινωνία με το θύτη.
2. Εμπιστευόμαστε στους γονείς μας ή σε κάποιο ενήλικα τον εκφοβισμό που έχουμε δεχθεί.
3. Δεν προωθούμε εκφοβιστικά μηνύματα.
4. Αν γνωρίζουμε κάποιο φίλο που είναι θύτης τον συμβουλεύουμε να σταματήσει.
5. Φιλτράρουμε ηλεκτρονικά μηνύματα από άτομα που μάς παρενοχλούν και μπλοκάρουμε την πρόσβασή τους στο ιστολόγιο μας.
6. Ως γονείς εάν γνωρίζουμε παιδιά στο σχολείο του παιδιού μας που παρενοχλούν να το αναφέρουμε στη διεύθυνση του σχολείου και το σχολικό σύμβουλο και, αν χρειαστεί, στην αστυνομία.
7. Ως γονείς οφείλουμε να είμαστε κοντά στο παιδί μας και να δημιουργούμε κλίμα αμοιβαίας εμπιστοσύνης.

8. Ηλεκτρονικός Τζόγος

Η ευκολία πρόσβασης σε ιστοσελίδες ηλεκτρονικού τζόγου αυξάνει τους κινδύνους εμπλοκής παιδιών και εφήβων σε τέτοιες δραστηριότητες.

Με τον όρο Ηλεκτρονικός Τζόγος εννοούμε τη δραστηριότητα κατά την οποία δύο ή περισσότερα άτομα συναντώνται διαδικτυακά με σκοπό την ανταλλαγή στοιχημάτων.

Μια τέτοια δραστηριότητα περιλαμβάνει το ρίσκο της πραγματικής οικονομικής απώλειας ή του κέρδους.

Πού μπορεί να συμβεί:

- Σε ιστοσελίδες ειδικά κατασκευασμένες για ηλεκτρονικό τζόγο

- Μέσα από ανεπιθύμητα μηνύματα που προσκαλούν τους χρήστες να παίξουν σε ηλεκτρονικά καζίνα, να ασχοληθούν με αθλητικά στοιχήματα και άλλα.

Τρόποι Αντιμετωπίσεις:

1. Αποφεύγουμε σελίδες που αφορούν ηλεκτρονικό τζόγο.
2. Αγνοούμε ανεπιθύμητα μηνύματα τα οποία μας προσκαλούν να παίξουμε σε ηλεκτρονικά καζίνα, να ασχοληθούμε με στοιχήματα και άλλα.
3. Ως γονείς μιλάμε με τα παιδιά μας και περνούμε περισσότερο χρόνο μαζί τους, συμβουλεύοντάς τα να μην σπαταλούν το χρόνο και τα χρήματά τους σε τέτοιες σελίδες.
4. Προστατεύουμε τα παιδιά από επισκέψεις σε τέτοιες ιστοσελίδες με το να χρησιμοποιούμε προγράμματα που τις φιλτράρουν και τις εμποδίζουν από το να εμφανίζονται στα αποτελέσματα μηχανών αναζήτησης, ακόμα και αν τα παιδιά τις ζητήσουν.
5. Ελέγχουμε και καταγράφουμε την πλοήγηση των παιδιών μας χρησιμοποιώντας ειδικό λογισμικό (*π.χ. Parental Software, Web Watcher)* που καταγράφει τη δραστηριότητα του υπολογιστή του παιδιού στο δικό μας υπολογιστή.

9. Ιοί

Ιός είναι: κακόβουλο πρόγραμμα, το οποίο εγκαθίσταται στον υπολογιστή, συνήθως εν αγνοία του χρήστη, και ενεργοποιείται είτε κάποια προκαθορισμένη χρονική στιγμή είτε ύστερα από κάποια συγκεκριμένη ενέργεια.

Πού μπορεί να συμβεί:

- Μέσω του ηλεκτρονικού ταχυδρομείου όπου λαμβάνουμε μολυσμένα συνημμένα αρχεία *(attachments)* ηλεκτρονικών μηνυμάτων *(e-mail)*, τα οποία όταν τα ανοίξουμε ενεργοποιούμε άθελά μας τους ιούς.

- Κατά την εγκατάσταση μολυσμένων προγραμμάτων κάποιες φορές εκτελούμε εν αγνοία μας μολυσμένα προγράμματα με αποτέλεσμα να ενεργοποιούμε τους ιούς.
- Κατά την πλοήγηση μας σε μολυσμένες σελίδες: ιστοσελίδες που έχουν δημιουργηθεί με τέτοιο τρόπο ώστε να μεταδίδουν ιούς στον υπολογιστή μας, όταν τις επισκεφτούμε ή όταν κατεβάσουμε ένα αρχείο.
- Κατά την ανταλλαγή αρχείων εν αγνοία μας παίρνουμε/ανοίγουμε αρχεία, τα οποία είναι μολυσμένα.

Τρόποι Αντιμετωπίσεις:

1. Δεν ανοίγουμε ηλεκτρονικά μηνύματα που έχουν σταλεί από άγνωστους αποστολείς.
2. Αποφεύγουμε ύποπτες ιστοσελίδες και, αν μπούμε κατά λάθος σε κάποια, την εγκαταλείπουμε αμέσως. Αν εμφανιστούν παράθυρα που ζητούν να συμφωνήσουμε σε οτιδήποτε τα κλείνουμε αμέσως και δεν πατούμε τυχόν κουμπιά μέσα σε αυτά
3. Έχουμε στον υπολογιστή μας εγκατεστημένο και ενημερωμένο πρόγραμμα εναντίον των ιών *(antivirus software).*
4. Επιτρέπουμε έλεγχο του υπολογιστή μας για ιούς δια μέσου του Διαδικτύου, μόνο εάν εμείς το έχουμε ζητήσει από έμπιστη ιστοσελίδα.
5. Χρησιμοποιούμε firewall, λογισμικό που αποτρέπει μη εξουσιοδοτημένα άτομα να αποκτήσουν πρόσβαση στον υπολογιστή μας.
6. Δημιουργούμε εφεδρικά αρχεία ασφαλείας, τα οποία αποθηκεύουμε σε μονάδα αποθήκευσης εκτός του ηλεκτρονικού υπολογιστή ή ακόμα και σε άλλο φυσικό χώρο από αυτόν που βρίσκεται ο υπολογιστής μας.
7. Αποφεύγουμε την εγκατάσταση εκτελέσιμων αρχείων, αρχείων με κατάληξη .exe, εκτός και αν γνωρίζουμε και εμπιστευόμαστε την προέλευσή τους.

10. Παιδική πορνογραφία

Παιδική πορνογραφία ορίζεται ως οι αναπαραστάσεις ανηλίκων που συμμετέχουν σε σεξουαλικές πράξεις ή καταστάσεις που υποδηλώνουν σεξουαλικές δραστηριότητες.

Μερικές φορές ο ορισμός περιλαμβάνει εικόνες που έχουν υποστεί επεξεργασία από ηλεκτρονικό υπολογιστή. Η παιδική πορνογραφία θεωρείται έγκλημα και υπόκειται σε ποινικές κυρώσεις.

Η παιδική πορνογραφία ορίζεται διαφορετικά από τη νομοθεσία της κάθε χώρας. Σύμφωνα με τη Σύμβαση για τα Διαδικτυακά Εγκλήματα του Συμβουλίου της Ευρώπης, η παιδική πορνογραφία έχει τις εξής μορφές:

- Ένας ανήλικος που συμμετέχει σε σεξουαλική δραστηριότητα
- Ένα άτομο που συμμετέχει σε σεξουαλική δραστηριότητα προσποιούμενο ότι είναι ανήλικο.
- Ρεαλιστικές εικόνες που αναπαριστούν ένα ανήλικο να συμμετέχει σε σεξουαλικές δραστηριότητες.

Η εξάπλωση των κυκλωμάτων παιδοφιλίας είναι ανησυχητική. Τα κυκλώματα αυτά είναι ομάδες ατόμων, τα οποία εργάζονται μαζί μέσω του Διαδικτύου με στόχο τη συλλογή και διανομή πορνογραφικού υλικού για τη δική τους ικανοποίηση. Τέτοιες ενέργειες αποτελούν έγκλημα και υπόκεινται στο νόμο.

Πού μπορεί να συμβεί:

- Σε ιστοσελίδες τις οποίες χειρίζονται κυκλώματα παιδοφιλία
- Σε ηλεκτρονικά μηνύματα με φωτογραφίες παιδικής πορνογραφίας

Αντιμετώπιση:

1. Αν γνωρίζουμε κάποιον που ασχολείται με την παιδική πορνογραφία, τον καταγγέλλουμε στην ιστοσελίδα www.cyberethics.info,ή στο τηλέφωνο 22674747 *(Γραμμή Καταγγελιών HotLine)* ή/και στην αστυνομία.
2. Αποφεύγουμε διαδικτυακές συζητήσεις με αγνώστους και κυρίως δεν συμφωνούμε ποτέ να συναντήσουμε κάποιο «φίλο» που, μόλις γνωρίσαμε διαδικτυακά.
3. Αν κάποια διαδικτυακή συζήτηση μάς κάνει να νιώσουμε άβολα την σταματάμε αμέσως και αναφέρουμε το γεγονός σε κάποιο ενήλικα.

4. Δεν στέλνουμε φωτογραφίες που είναι δυνατό να μας εκθέσουν μέσω του ηλεκτρονικού ταχυδρομείου.
5. Δεν ανεβάζουμε σε ιστοσελίδες κοινωνικού δικτύου π.χ. στο Facebook ή Hi5 φωτογραφίες μας, οι οποίες είναι προκλητικές.
6. Ως γονείς συμβουλεύουμε τα παιδιά μας να μην στέλνουν φωτογραφίες και προσωπικά στοιχεία του εαυτού τους ή φίλων τους σε οποιονδήποτε συναντούν σε δωμάτια συνομιλίας.
7. Εγκαθιστούμε λογισμικό φιλτραρίσματος πληροφοριών σε υπολογιστές που χρησιμοποιούνται από παιδιά *(π.χ. Safe Internet της Αρχής Τηλεπικοινωνιών Κύπρου*

11. Παραβίαση Ιδιωτικής Ζωής

Σε κάθε βήμα της περιδιάβασής μας στο Διαδίκτυο "προσφέρουμε" προσωπικές πληροφορίες. πολλές από τις ιστοσελίδες που επισκεπτόμαστε, φυλάνε στον υπολογιστή μας δεδομένα για την επίσκεψη μας, τα λεγόμενα "Cookies".

Τα Cookies είναι μικρά κομμάτια από πληροφορίες όπως το όνομα χρήστη, πληροφορίες της εγγραφής μας σε μια σελίδα, προτιμήσεις, διαδικτυακά «καλάθια με ψώνια» και λοιπά. Οι νόμιμες εταιρείες χρησιμοποιούν τα Cookies για να κάνουν προσφορές σε χρήστες που τους επισκέπτονται ξανά. Παράνομες εταιρείες χρησιμοποιούν Cookies για να πάρουν πληροφορίες για τους χρήστες και να τις πουλήσουν σε εταιρείες Marketing.

Πού μπορεί να συμβεί:

- Μέσω ηλεκτρονικού ταχυδρομείου
- Σε ομάδες συζητήσεων *(groups ή list-serves)* του Διαδικτύου
- Κατά την πλοήγηση μας στο Διαδίκτυο με οποιοδήποτε φυλλομετρητή
- Όταν στέλνουμε μηνύματα της στιγμής *(Instant Messages)*
- Σε κοινωνικά δίκτυα, όπως το Facebook και MySpace
- Σε ιστολόγια του Διαδικτύου *(blogs)*

Αντιμετώπιση:

1. Διαβάζουμε τους κανονισμούς του παροχέα Διαδικτύου για ιδιωτικότητα και τους εμπεδώνουμε. Αν δεν συμφωνούμε, δεν προχωράμε στη δημιουργία λογαριασμού για την υπηρεσία που προσφέρει.
2. Ανανεώνουμε τους φυλλομετρητές μας με αναβαθμίσεις ασφαλείας *(security updates)*, ώστε οι τρόποι προστασίας μας να γίνονται συστηματικά καλύτεροι.
3. Αλλάζουμε τις ρυθμίσεις του φυλλομετρητή μας ώστε να έχει υψηλή ιδιωτικότητα και να απαγορεύει τα cookies. Πρέπει να γνωρίζουμε όμως ότι, εάν επιλέξουμε ψηλή ιδιωτικότητα, τότε μπορεί να μην μπορέσουμε να

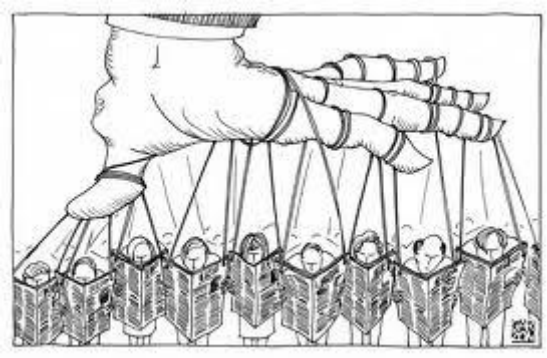
δουλέψουμε πάνω στους τραπεζικούς μας λογαριασμούς ή να ψωνίσουμε χρησιμοποιώντας το Διαδίκτυο, χωρίς αλλαγή αυτών των ρυθμίσεων.

4. Διαγράφουμε cookies που αποθηκεύονται στον υπολογιστή μας.
5. Προσπαθούμε να χρησιμοποιούμε διάφορες μηχανές αναζήτησης κάθε φορά. Με αυτόν τον τρόπο μειώνουμε το μέγεθος της πληροφορίας που κατακρατείται από μια ιστοσελίδα. Για παράδειγμα μπορούμε να χρησιμοποιούμε Yahoo για το ηλεκτρονικό ταχυδρομείο και Google για αναζητήσεις.
6. Θυμόμαστε ότι μπορεί είτε ο αποστολέας είτε ο παραλήπτης, να αποδεχθεί να αποκαλυφθεί η ηλεκτρονική μας διεύθυνση *(e-mail)* όταν συμμετέχουμε σε διαδικτυακές συζητήσεις, που κάποτε ονομάζονται list-servers. Επίσης, θυμόμαστε ότι με τη συμμετοχή μας σε τέτοιες συζητήσεις διαθέτουμε την ηλεκτρονική μας διεύθυνση σε ένα, μεγάλο πολλές φορές, αριθμό ατόμων.
7. Εγκαθιστούμε αντικατασκοπικό πρόγραμμα *(anti-spyware)* για αποτροπή της παράνομης παρακολούθησης της διαδικτυακής μας δραστηριότητας.
8. Προστατεύουμε την ιδιωτική μας ζωή, αποφεύγοντας τη δημοσιοποίηση προσωπικών δεδομένων ή δεδομένων που αφορούν φίλους και οικογένεια. Το ίδιο ισχύει και για προσωπικές φωτογραφίες και βίντεό μας.
9. Οι υπηρεσίες ιστολογιών συνήθως μας επιτρέπουν κάποιο έλεγχο ως προς το τι μπορούμε να μοιραζόμαστε δημόσια, π.χ. τη διεύθυνση ηλεκτρονικού ταχυδρομείου ή ακόμα και τα σχόλιά μας. Διαβάζουμε τις σχετικές συμφωνίες και δηλώσεις απορρήτου προσεκτικά και γνωρίζουμε τι απαιτείται και τι αποκαλύπτεται.
10. Τα πιο πολλά ιστολόγια επιτρέπουν σχόλια στους αναγνώστες. Πολλά από αυτά επιτρέπουν ανώνυμα σχόλια αλλά κάποια απαιτούν εγγραφή και τουλάχιστον μια ηλεκτρονική διεύθυνση. Σκεφτόμαστε προσεκτικά πόσες πληροφορίες θέλουμε να δώσουμε και εάν θέλουμε προσωπικά δεδομένα να συνδεθούν με τα σχόλιά μας.
11. Αποφασίζουμε ποιο θέλουμε να είναι το ακροατήριο ενός ιστολόγου. Εάν γράφουμε μόνο για φίλους και την οικογένεια μπορούμε να κάνουμε το ιστολόγιο προσβάσιμο, επιβάλλοντας χρήση κωδικού
12. Χρησιμοποιώντας ψευδώνυμα σε ιστολόγια μπορούμε να προστατέψουμε την ταυτότητά μας.
13. Θυμόμαστε ότι έχουμε την επιλογή να ρυθμίσουμε τις μηχανές αναζήτησης έτσι ώστε να μην παρουσιάζουν το ιστολόγιο μας στα αποτελέσματά τους.
14. Χρησιμοποιούμε κωδικούς ασφαλείας από συνδυασμό γραμμάτων και αριθμών που είναι δύσκολο να μαντέψει ή να ανακαλύψει κάποιος

διασταυρώνοντας πληροφορίες. Αποφεύγουμε, επίσης, κωδικούς ασφαλείας που είναι αποφθέγματα ή λέξεις από λεξικά

15. Δεν μοιραζόμαστε τους κωδικούς πρόσβασης που έχουμε με άλλα άτομα.
16. Επικοινωνούμε με τα άτομα που δημοσιεύουν προσωπικά μας στοιχεία σε ιστολόγιο και ζητούμε να τα αφαιρέσουν - σε ιστολόγια συνήθως βρίσκονται τα στοιχεία επικοινωνίας όπως η ηλεκτρονική μας διεύθυνση *(e-mail)* όσων συμμετέχουν - ή επικοινωνούμε με τους υπευθύνους του ιστολόγου.
17. Αντιλαμβανόμαστε ότι κατά την πλοήγησή μας στο Διαδίκτυο αφήνουμε ίχνη, επομένως πρέπει να είμαστε προσεκτικοί
18. Σεβόμαστε και δεν δημοσιοποιούμε προσωπικά δεδομένα άλλων ατόμων χωρίς τη συγκατάθεσή τους.

12. Παραπληροφόρηση



Παραπληροφόρηση στο Διαδίκτυο είναι δυνατό να συμβεί με την παρουσίαση διάφορων ψευδών ή αναληθών ή τροποποιημένων πληροφοριών σε ιστοσελίδες, με πιθανό σκοπό την παραπλάνησή μας.

Παραπληροφόρηση συμβαίνει και όταν οι πληροφορίες είναι ελλιπείς με αποτέλεσμα να οδηγήσουν σε λανθασμένα συμπεράσματα.

Πού μπορεί να συμβεί

- Σε οποιαδήποτε σελίδα του Διαδικτύου που προσφέρει πληροφορίες.

Αντιμετώπιση:

1. Αξιολογούμε τις πληροφορίες που βρίσκουμε στο Διαδίκτυο και ελέγχουμε το συγγραφέα, την προέλευση της σελίδας, τη βιβλιογραφία της πληροφορίας.
2. Χρησιμοποιούμε πολλαπλές πηγές πληροφοριών και διασταυρώνουμε τις πληροφορίες που βρίσκουμε στο Διαδίκτυο.
3. Επισκεπτόμαστε βιβλιοθήκες, όχι απλώς το Διαδίκτυο, και χρησιμοποιούμε ποικιλία πηγών, όπως εφημερίδες, περιοδικά και βιβλία.
4. Χρησιμοποιούμε διάφορες μηχανές αναζήτησης και όχι μόνο μία για να βελτιωθεί σημαντικά η ικανότητά μας να βρίσκουμε ποιοτικές πληροφορίες.

5. Μαθαίνουμε πώς λειτουργεί το Διαδίκτυο και γνωρίζουμε πως ο καθένας μπορεί να δημιουργήσει μια διαδικτυακή τοποθεσία, χωρίς να τον ελέγχει κανείς. Γι' αυτό το λόγο απαιτείται να χρησιμοποιούμε πηγές που γενικά θεωρούνται έγκυρες.
6. Μαθαίνουμε πώς να διακρίνουμε ένα γεγονός από μια άποψη και να αναγνωρίζουμε την προκατάληψη, την προπαγάνδα και τις τοποθεσίες που χρησιμοποιούν ιδεολογικά στερεότυπα.
7. Εγκαθιστούμε φίλτρα λογισμικού που μπορούν να αποκλείσουν πηγές που περιέχουν μίσος, ρατσισμό και άλλου είδους προπαγάνδα.

13. Παραποίηση Γλώσσας

Η ανάγκη για γρήγορη και εύκολη επικοινωνία, μια συνήθεια που την αποκτήσαμε με την είσοδο της κινητής τηλεφωνίας και του Διαδικτύου στη ζωή μας, άρχισε να οδηγεί στην Παραποίηση της Γλώσσας μας. Αντί ελληνικά, δηλαδή, χρησιμοποιούνται τα "greeklish", ελληνικά γραμμένα με λατινικούς χαρακτήρες, στα οποία ο τονισμός και η ορθογραφία δεν είναι σημαντικά.

Για παράδειγμα η φράση «θα σε δω σε λίγο» αποδίδεται εσφαλμένα «tha se do se ligo»

Όλα αυτά μπορούν να οδηγήσουν όχι μόνο στη παραποίηση της γλώσσας μας αλλά, όπως κάποιοι υποστηρίζουν και στην αλλοίωση της ταυτότητας των Ελλήνων.

Πού μπορεί να συμβεί:

- Όταν στέλνουμε μηνύματα μέσω κινητού τηλεφώνου (sms).
- Όταν γράφουμε ηλεκτρονικά μηνύματα στο ηλεκτρονικό ταχυδρομείο (e-mail).
- Σε κάθε δραστηριότητα του Διαδικτύου που χρησιμοποιεί το γραπτό λόγο ως μέσο επικοινωνίας.

Αντιμετώπιση:

1. Χρησιμοποιούμε την ελληνική γλώσσα, όπου αυτό είναι δυνατό

14. Υπολοπή Προσωπικών Δεδομένων (Phishing)

Υποκλοπή Προσωπικών Δεδομένων στο Διαδίκτυο είναι η πράξη της εξαπάτησης ενός χρήστη κάνοντας τον να δώσει προσωπικές πληροφορίες σε μια «πλαστή ιστοσελίδα» στο Διαδίκτυο (*π.χ διεύθυνση, αριθμό ταυτότητας, αριθμό διαβατηρίου, αριθμούς τραπεζικών λογαριασμών,ης κ.λπ)*.

Μια τέτοιου είδους δραστηριότητα επιτρέπει σε έναν απατεώνα *(cracker)* να κλέψει ή να πλαστογραφήσει τα στοιχεία του θύματος ή/και να κερδίσει

παράνομη πρόσβαση στα δεδομένα του/της, όπως προσωπικούς λογαριασμούς, συνδρομές, e-mail, κωδικούς,

Πού μπορεί να συμβεί:

- Μέσω ηλεκτρονικών μηνυμάτων (e-mail) που ξεγελούν το χρήστη ώστε να οδηγηθεί σε πλαστές ιστοσελίδες
- .Κατά το φυλλομέτρημα οποιασδήποτε σοβαρής ιστοσελίδας, η οποία έχει μολυνθεί από ιό.
- Κατά τη περιήγηση σε ιστοσελίδες με αναληθή προϊόντα και πληροφορίες.
- Κατά τη χρήση οποιουδήποτε φυλλομετρητή Διαδικτύου, ο οποίος έχει μολυνθεί με πρόγραμμα που καταγράφει προσωπικές και οικονομικές πληροφορίες, τις οποίες χρησιμοποίησε ο χρήστης σε επισκέψεις του σε σελίδες που του τις ζητούν.

Αντιμετώπιση:

1. Ελέγχουμε πάντοτε τον αποστολέα ενός μηνύματος και διερευνούμε την υπόστασή του.
2. Γνωρίζουμε ότι νόμιμοι φιλανθρωπικοί οργανισμοί συνήθως στέλνουν ηλεκτρονικές εκκλήσεις για βοήθεια μόνο σε ανθρώπους που το έχουν ζητήσει. Άλλες παρόμοιες εκκλήσεις, που σχεδόν πάντα ακολουθούν ένα μεγάλο καταστροφικό γεγονός, είναι συνήθως ψευδείς. Επισκεπτόμαστε την επίσημη ιστοσελίδα του οργανισμού για να επιβεβαιώσουμε την αξιοπιστία της έκκλησης.
3. Ελέγχουμε πάντα τη νομιμότητα φιλανθρωπικών ιδρυμάτων, αναζητώντας σχετικές επίσημες ιστοσελίδες *(π.χ. http://www.charitynavigator.org)*
4. Τηλεφωνούμε ή πηγαίνουμε απευθείας στην ιστοσελίδα ενός φιλανθρωπικού οργανισμού και βρίσκουμε τρόπους να προσφέρουμε μέσω αυτής, αντί να απαντούμε και να κατευθυνόμαστε από εκκλήσεις-μηνύματα που παραλαμβάνουμε.
5. Δεν ενεργοποιούμε απερίσκεπτα συνδέσμους από μηνύματα αμφιβόλου προελεύσεως και περιεχομένου γιατί αυτά μπορούν να μας οδηγήσουν σε παράνομες ή επιβλαβείς ιστοσελίδες που μπορεί να μοιάζουν νόμιμες.
6. Αποφεύγουμε να δίνουμε προσωπικές πληροφορίες μέσω του Διαδικτύου. Είναι απίθανο μια τράπεζα ή ένας φιλανθρωπικός οργανισμός να ζητά τέτοιες πληροφορίες με αυτόν τον τρόπο.
7. Γνωρίζουμε ότι σοβαρές τράπεζες και επενδυτικοί οργανισμοί χρησιμοποιούν το πρωτόκολλο επικοινωνίας https αντί για http για ασφάλεια των προσωπικών δεδομένων των πελατών τους. Το “S” σημαίνει ασφαλές πρωτόκολλο.

8. Όταν μας ζητηθεί να πληκτρολογήσουμε ένα ψευδώνυμο συνομιλίας, διαλέγουμε ένα όνομα που δεν προδίδει τα προσωπικά μας στοιχεία όπως το όνομα, το επίθετο, την ημερομηνία γέννησής μας, τον χώρο διαμονής κ.λ.π.

15. Φυσικές Παθήσεις

Με την εισαγωγή του Διαδικτύου στη ζωή μας, οι ώρες χρήσης του υπολογιστή έχουν αυξηθεί κατακόρυφα.

Η πολύωρη χρήση του Διαδικτύου είτε είναι για έρευνα είτε για παιχνίδι είτε για κοινωνικοποίηση εγκυμονεί κινδύνους για την υγεία μας.

Πέρα από τις διαταραχές στην όραση και τις υποψίες για ενδεχόμενα προβλήματα εξαιτίας της έκθεσης σε ακτινοβολία, κυρίως από τις οθόνες, εκείνοι που ασχολούνται για ώρες μπροστά στον υπολογιστή χωρίς διάλειμμα ή εναλλαγή δραστηριοτήτων κάνοντας μεγάλο αριθμό επαναλαμβανόμενων κινήσεων μπορεί να προσβληθούν από: α) διάφορες μυοσκελετικές παθήσεις. Β) Κακώσεις όπως ο ευθειασμός του αυχένα, ο πόνος του αγκώνα, τενοντίτιδα, πηχαιοκαρπική άρθρωση γ) και άλλες παθήσεις έχουν συνδέσει το όνομά τους με την υπερβολική χρήση του υπολογιστή.

Πού μπορεί να συμβεί:

Μια φυσική πάθηση μπορεί να συμβεί ανεξάρτητα με το είδος της δραστηριότητας στο Διαδίκτυο όταν:

- Η χρήση του υπολογιστή είναι πολύωρη και χωρίς διαλείμματα.
- Η απόσταση των ματιών μας από τον υπολογιστή είναι λανθασμένη και η οθόνη βρίσκεται σε λανθασμένο ύψος από το επίπεδο των ματιών μας.
- Δεν καθόμαστε σε ορθή θέση μπροστά από τον υπολογιστή.
- Το δωμάτιο στο οποίο βρίσκεται ο υπολογιστής δεν φωτίζεται ομοιόμορφα.
- Οι προδιαγραφές του εξοπλισμού του υπολογιστή δεν είναι τουλάχιστον εργονομικές.

Αντιμετώπιση:

1. Βεβαιωνόμαστε ότι ο εξοπλισμός του υπολογιστή ακολουθεί τις διεθνείς προδιαγραφές εργονομίας για την ασφάλεια του χρήστη από φυσικές παθήσεις.
2. Βεβαιωνόμαστε ότι η απόσταση της οθόνης από τα μάτια μας είναι μεταξύ 50 και 70 εκατοστών.
3. Βεβαιωνόμαστε ότι το κέντρο της οθόνης βρίσκεται περίπου 15° από το επίπεδο των ματιών μας.
4. Κλείνουμε σε τακτά διαστήματα τα μάτια μας για λίγα λεπτά.
5. Εστιάζουμε κάθε 10 λεπτά περίπου σε κάποιο μακρινό σημείο, εκτός οθόνης.
6. Βεβαιωνόμαστε ότι το δωμάτιο του υπολογιστή φωτίζεται ομοιόμορφα και δεν υπάρχει πηγή φωτός στο πλάι της οθόνης.
7. Βεβαιωνόμαστε ότι κατά την πληκτρολόγηση η παλάμη και ο καρπός είναι σε ευθεία παράλληλη με το επίπεδο του δαπέδου.
8. Βεβαιωνόμαστε ότι πιάνουμε το ποντίκι χρησιμοποιώντας όλη την παλάμη μας και το μετακινούμε κινώντας όλο το βραχίονά μας.
9. Γενικά, βεβαιωνόμαστε ότι το σώμα μας έχει άνετη στάση όταν δουλεύουμε με τον υπολογιστή.
10. Σηκωνόμαστε και περπατάμε μετά από μία ώρα εντατικής ενασχόλησης με τον υπολογιστή.
11. Εναλλάσσουμε εργασίες που γίνονται με υπολογιστή με εργασίες στις οποίες δεν απαιτείται η χρήση υπολογιστή.

Πέρα από τους κινδύνους όμως υπάρχουν και τρόποι αποφυγής των επιθέσεων:

- Έλεγχος γνησιότητας της ταυτότητας *(identification and authentication)*των χρηστών, των προγραμμάτων ή των μηχανημάτων καθώς και των εξουσιοδοτήσεων που αυτά διαθέτουν για την προσπέλαση των προστατευμένων πόρων του συστήματος με συνδυασμένη χρήση συνθηματικών και ψηφιακών πιστοποιητικών
- Προστασία της εμπιστευτικότητας των δεδομένων*(data confidentiality)*,δηλαδή προστασία ενάντια σε μη εξουσιοδοτημένες αποκαλύψεις πληροφοριών
- Αποφυγή συστημάτων με "single points of failure"
- Firewall,το οποίο είναι ένα πρόγραμμα ή ένα μηχάνημα που μπορεί να χρησιμοποιηθεί σαν διαχωριστικό μεταξύ των δύο αυτών δικτύων
- Κωδικοποίηση / Κρυπτογράφηση

- Πρωτόκολλα Ασφαλείας, που αναφέρονται στα επίπεδα Πρόσβασης Δικτύου,Internet,Μεταφοράς και Εφαρμογής
- Ενημέρωση σχετικά με τα "operating systems" και κάποια "patches"
- Αποφυγή τοποθέτησης δεδομένων σε σημεία οπού δεν είναι κατανοητά

ΚΕΦΑΛΑΙΟ4:
ΙΣΤΟΡΙΚΕΣ ΕΠΙΘΕΣΕΙΣ

Σε αυτό την ενότητα θα αναφερθούμε στις ποιο ιστορικές επιθέσεις στο Διαδίκτυο.

Το 2001 μόλις το 8% του παγκόσμιου πληθυσμού χρησιμοποιούσε το Διαδίκτυο δηλαδή περίπου 513 εκατομμύρια χρήστες. Αλλά ο κόσμος σήμερα έχει πάνω από 2,7 δισεκατομμύρια χρήστες του Διαδικτύου ή σχεδόν το 39% του παγκόσμιου πληθυσμού.

Πρέπει να αναφέρουμε ότι μια επίθεση στον κυβερνοχώρο το 2001 θα ήτανε ένα εμπόδιο, αλλά το 90% του κόσμου δεν ανησυχούσε για κάτι

Αυτό όμως δεν ισχύει ποια γιατί οι πρωτοποριακοί τρομοκράτες του σήμερα βρίσκουν ότι ο κυβερνοχώρος είναι μια πλούσια φλέβα για να την εκμεταλλευτούν.

1. Ο ιός «**Morris worm**»

Ο εικονιζόμενος είναι ο δημιουργός του ιού ο Robert Tappan Morris που μόλις 23 χρονών και μεταπτυχιακός φοιτητής στο Cornell University. Έγινε και ο πρώτος άνθρωπος στην ιστορία, που καταδικάστηκε για απάτη σχετιζόμενη με ηλεκτρονικούς υπολογιστές.

Σήμερα ο Μόρις είναι καθηγητής στο MIT.

Ο ιός «**Morris worm**» εμφανίστηκε στις 2 Νοεμβρίου 1988 και ο στόχος του ιού ήτανε να επιβραδύνει τόσο τους υπολογιστές στο σημείο που τους καθιστούσε σχεδόν άχρηστους.

Ήτανε ένας από τους πρώτους ιούς σκουλήκια υπολογιστή που διανέμονται μέσω του Διαδικτύου και η επίθεση του κέρδισε την προσοχή των μέσων ενημέρωσης. Ο ίδιος ο Morris είχε πει ότι απλώς προσπαθούσε να δει πόσο μεγάλο ήταν το διαδίκτυο.

Ωστόσο καταδικάστηκε σε τρία χρόνια δικαστικής επιτήρησης, 400 ώρες κοινωνικής εργασίας και πρόστιμο 10.050 δολαρίων, αλλά δεν ήταν ο μόνος που πλήρωσε ακριβά, υπολογίζεται ότι το κόστος των πιθανών απωλειών παραγωγικότητας και των δαπανών απομάκρυνσης του ηλεκτρονικού "σκουληκιού" του Μόρις στοίχισαν από 200 δολάρια μέχρι 53.000 δολάρια ανά μολυσμένο σύστημα.

Θα πρέπει να αναφέρουμε ότι βρίσκεται στην 7η θέση των 10 χειρότερων ιών Η/Υ όλων των εποχών.

2. Ο ιός « **Melissa** »

Ο εικονιζόμενος είναι ο δημιουργός του ιού ο Αμερικανό David L. Smith. Εμφανίστηκε τον Μάρτιο του 1999. Ο ιός ήτανε απλά εντυπωσιακός

και θα το εξακριβώσουμε καθώς θα αναλύουμε την λειτουργικότητα του.

Όπως είπαμε και νωρίτερα εμφανίστηκε στις 26 Μαρτίου 1999 σε μορφή e-mail. Ο ιός ήταν σε ένα αρχείο με όνομα *"List.doc",* που περιείχε κωδικούς για πρόσβαση σε 80 πορνογραφικές ιστοσελίδες.

Η αρχική έκδοση του ιού εστάλη σε πολλά άτομα με μορφή e-mail. Εξαπλώθηκε με έγγραφα του Microsoft Word *(Microsoft Word 97 και Word 2000, καθώς και με το Microsoft Excel 97, 2000 και 2003)*που στάλθηκαν μέσω e-mail και δούλευε ως εξής: Κάποιος δημιούργησε τον ιό ως ένα έγγραφο του Word που φορτώθηκε σε μια ομάδα ειδήσεων του Internet. Όποιος κατέβαζε το έγγραφο και το άνοιγε θα ενεργοποιούσε τον ιό, ο οποίος θα έστελνε το έγγραφο και συνεπώς και τον εαυτό του μ' ένα μήνυμα e-mail στους πρώτους 50 χρήστες που υπήρχαν στο βιβλίο διευθύνσεων του μολυσμένου υπολογιστή. Το μήνυμα αυτό του e-mail περιείχε ένα φιλικό σημείωμα που εμφάνιζε το όνομα του ατόμου από το οποίο έφευγε και έτσι ο αποδέκτης θα άνοιγε το μήνυμα νομίζοντας ότι είναι αβλαβές. Ο ιός θα δημιουργούσε μετά 50 καινούργια μηνύματα από το μηχάνημα του παραλήπτη.

Ο ιός Melissa ήταν ο πιο γρήγορα διαδεδομένος ιός που εμφανίσθηκε ποτέ και ανάγκασε μάλιστα πολλές μεγάλες εταιρείες να διακόψουν την ηλεκτρονική τους αλληλογραφία. Επίσης ο ιός Melissa εκμεταλλεύτηκε τη γλώσσα προγραμματισμού που είναι ενσωματωμένη στο Microsoft Word και αποκαλείται VBA *(Visual Basic for Applications).* Είναι μια ολοκληρωμένη γλώσσα προγραμματισμού και μπορεί να προγραμματιστεί για να κάνει εργασίες όπως τροποποίηση αρχείων και αποστολή μηνυμάτων e-mail.

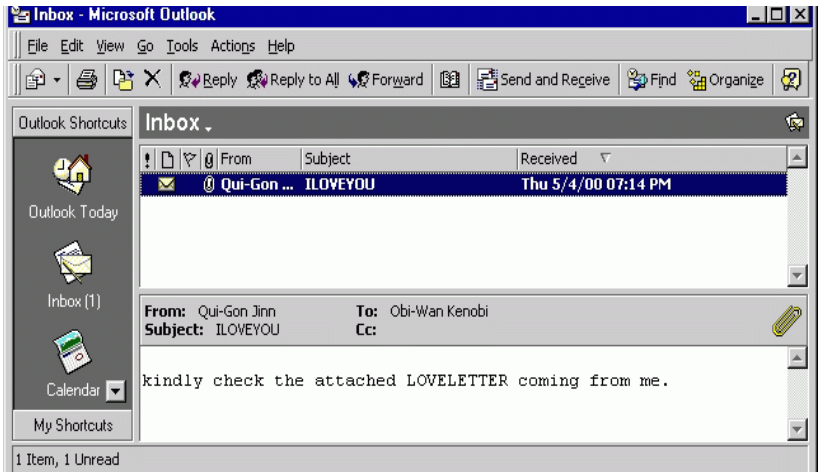
Ένας προγραμματιστής μπορεί να εισάγει ένα πρόγραμμα μέσα σ' ένα έγγραφο, το οποίο θα εκτελεσθεί αμέσως μόλις ανοιχθεί το έγγραφο. Με τον τρόπο αυτό δημιουργήθηκε -προγραμματίσθηκε ο ιός Melissa. Όποιος άνοιγε ένα έγγραφο που ήταν μολυσμένο με τον ιό Melissa θα ενεργοποιούσε αυτόματα τον ιό, θα έστελνε τα 50 e-mails και μετά θα μόλυνε ένα κεντρικό αρχείο με όνομα *NORMAL.DOT* έτσι ώστε όποιο αρχείο δημιουργείτο από δω και πέρα θα περιείχε επίσης τον ιό.

Ο Smith καταδικάστηκε σε 10 χρόνια φυλάκιση, ενώ εξέτισε ποινή 20 μηνών και πρόστιμο 5,000$.

Θα πρέπει να αναφέρουμε ότι ο ιός αυτός βρίσκεται στην 7η θέση από τους 10 χειρότερους ιούς Η/Υ όλων των εποχών.

3. Ο ιός « **I.Love.You** »

Η εικονιζόμενη εικόνα μας δείχνει τον τρόπο που έστελναν τον ιό μέσω email.



Ο ιός I LOVE YOU, μερικές φορές αναφέρεται ως Love Letter, ήταν ένα σκουλήκι υπολογιστή που επιτέθηκε σε δεκάδες εκατομμύρια υπολογιστές

Εμφανίστηκε στις 5 Μαΐου 2000 στης Φιλιππίνες , άρχισε να εξαπλώνεται ως ένα μήνυμα ηλεκτρονικού ταχυδρομείου με γραμμή θέματος "ILOVEYOU", στο σώμα του μηνύματος γράφει "Kindly check the attached LOVELETTER coming from me και το μήνυμα συνοδεύεται από ένα αρχείο με το όνομα LOVE-LETTER-FOR-YOU.txt.vbs όπου εκεί βρίσκεται και ο ιός.

Η τελευταία επέκταση αρχείου ήταν συχνά κρυμμένη από προεπιλογή σε υπολογιστές με Windows , οδηγώντας εν αγνοία τους χρήστες να πιστεύουν ότι ήταν ένα κανονικό αρχείο κειμένου. Όταν άνοιγαν το συνημμένο ενεργοποιούσαν το Visual Basic σενάριο. Το σκουλήκι έκανε ζημιά στο τοπικό μηχάνημα, κάνοντας αντικατάσταση των αρχείων εικόνας, και έστελνε ένα αντίγραφο του εαυτού του σε όλες τις διευθύνσεις στο Βιβλίο διευθύνσεων των Windows που χρησιμοποιείται από το Microsoft Outlook. Σε αντίθεση με τον ιό Melissa που είχε εμφανιστεί πριν από 1 χρόνο που αποστέλλονται μόνο αντίγραφα στις πρώτες 50 επαφές.

Έπειτα από έρευνες που έγιναν εντοπίστηκαν δύο προγραμματιστές από της Φιλιππίνες , ο πρώτος ονομάζεται Reonel Ramones και ο δεύτερος Onel de Guzman.

Οι επιπτώσεις που είχε η δημιουργία του ιού ήτανε πολύ μεγάλη, προκάλεσε 5,5 έως 8.700.000.000 δολάρια σε αποζημιώσεις σε όλο τον κόσμο και υπολογίζεται ότι κοστίζουν 15 δισεκατομμυρίων δολαρίων για να αφαιρέσουν το σκουλήκι. Εντός δέκα ημερών, πάνω από πενήντα εκατομμύρια κρούσματα είχαν αναφερθεί και εκτιμάται ότι το 10% των συνδεδεμένων στο Διαδίκτυο υπολογιστών στον κόσμο, είχε πληγεί. Ζημιές που επικαλέστηκαν ήταν ως επί το πλείστον ο χρόνος και προσπάθεια για να απαλλαγούμε από τη μόλυνση και την ανάκτηση των αρχείων από αντίγραφα ασφαλείας. Για να προστατεύσουν τον εαυτό τους, το Πεντάγωνο, τη CIA, το Βρετανικό Κοινοβούλιο και οι περισσότερες μεγάλες εταιρείες αποφάσισαν να κλείσουν εντελώς το σύστημα του ηλεκτρονικού ταχυδρομείου τους. Αυτός ο ιός

έπληξε πάνω από 45 εκατομμύρια υπολογιστές και ήταν ένα από τα πιο επικίνδυνα συναφείς με την πληροφορική καταστροφές στον κόσμο.

Θα πρέπει να αναφέρουμε ότι ο ιός αυτός βρίσκεται στην 1η θέση από τους 10 χειρότερους ιούς Η/Υ όλων των εποχών.

4. Ο ιός **«Code Red»**

Ο ιός «Code Red» (ή σκουλήκι υπολογιστή) εμφανίστηκε στο Διαδίκτυο στις 15 Ιουλίου 2001.

Το «Code Red» ανακαλύφθηκε για πρώτη φορά και ερευνήθηκε από τους υπαλλήλους της eEye Ψηφιακής Ασφάλειας : Marc Maiffret και Ryan Permeh. Ονόμασαν τον ιό "Code Red", επειδή Code Red Mountain Dew ήταν ό, τι έπιναν κατά το χρόνο που δημιούργησαν τον ιό.

Γενικά τα σκουλήκια εκμεταλλεύονται τον χρόνο των υπολογιστών και το εύρος ζώνης των δικτύων όταν αναπαράγονται και έχουν συχνά κακές προθέσεις. Το συγκεκριμένο σκουλήκι αυτό επιβράδυνε όντως την κυκλοφορία στο Διαδίκτυο *(Internet traffic)* όταν άρχισε να αναπαράγει τον εαυτό του, αλλά όχι τόσο άσχημα όσο περίμεναν. Το κάθε αντίγραφο του σκουληκιού έψαχνε στο Internet για να βρει servers με *Windows NT ή Windows 2000* που να μην έχουν εγκατεστημένο το security patch της Microsoft.Κάθε φορά που έβρισκε έναν μη ασφαλή server, το σκουλήκι αναπαρήγαγε στον εαυτό του σ’ εκείνον τον server και το καινούργιο αντίγραφο έψαχνε μετά να βρει άλλους servers για να μολύνει.

Το σκουλήκι Code Red ήταν σχεδιασμένο για να κάνει τα εξής τρία πράγματα :

1. Να αναπαράγει τον εαυτό του κατά τις 20 πρώτες ημέρες του μήνα.
2. Να αντικαθιστά τις αρχικές ιστοσελίδες στους μολυσμένους servers με μια σελίδα που εμφάνιζε το μήνυμα "Hacked by Chinese".
3. Να ξεκινά μια συντονισμένη επίθεση στον Web server του Λευκού Οίκου σε μια προσπάθεια να τον κάνει να καταρρεύσει.

Θα πρέπει να αναφέρουμε ότι ο ιός αυτός βρίσκεται στην 10η θέση από τους 10 χειρότερους ιούς Η/Υ όλων των εποχών.

5. Ο ιός «Nimda»

Ο ιός εμφανίστηκε στις18 Σεπτεμβρίου 2001. Προκάλεσε μεγάλη καταστροφή στον παγκόσμιο ιστό γιατί ήταν ιδιαίτερα επιθετικός και διαδίδονταν ταχύτατα μέσω του Internet *(e-mails, ιστοσελίδες, κοινόχρηστα αρχεία).*

Ο «Nimda» εμφανίζεται καμουφλαρισμένος στο ηλεκτρονικό ταχυδρομείο ως συνημμένο αρχείο με το όνομα *"readme.exe"* και κατορθώνει εντός ολίγου να μεταλλαχθεί, αλλάζοντας όνομα και υπέρ-πολλαπλασιάζοντας την παρουσία του σε δεκάδες αρχεία. Τόσο στον προσωπικό υπολογιστή σας, όσο και σε κοινό Δίκτυο και διακομιστές που στηρίζονται στο software IIS της Microsoft. Εμφανίσθηκε για πρώτη φορά στις ΗΠΑ και σε λίγες ώρες ακολούθησαν η Ιαπωνία και οι υπόλοιπες ασιατικές χώρες, ενώ τώρα έχει πλήξει όλον τον κόσμο συμπεριλαμβανομένης και της Ελλάδας.

Θα πρέπει να αναφέρουμε ότι ο ιός αυτός βρίσκεται στην 5η θέση από τους 10 χειρότερους ιούς Η/Υ όλων των εποχών.

6. Ο ιός «SirCam»

Πληροφορίες για αυτόν τον ιό δεν έχουμε πολλές δλδ δεν γνωρίζουμε πότε εμφανίστηκε, ούτε ποιοί τον δημιούργησαν ωστόσο μπορούμε να αναφερθούμε στο τρόπο που λειτουργούσε σαν ιός.

Ο ιός φτάνει στον υπολογιστή μέσα σε μήνυμα e-mail και φυσικά έχει ένα attached αρχείο. Ο τίτλος του μηνύματος είναι διαφορετικός κάθε φορά, ίδιος με το όνομα του τυχαίου μολυσμένου αρχείου που συνοδεύει το μήνυμα.

→Στην πρώτη γραμμή μπορούμε να δούμε τη φράση ανάλογα με τη γλώσσα:

Hi! How are you? ή Hola como estas ?

→Μετά θα βρούμε κάποια πρόταση από τις παρακάτω:

I send you this file in order to have your advice ή I hope you can help me with this file that I send ήThis is the file with the information that you ask for, ή Te mando este archivo para que me des tu punto de vista ή Espero me puedas ayudar con el archivo que te mando ή

→Στην τελευταία γραμμή θα λέει:

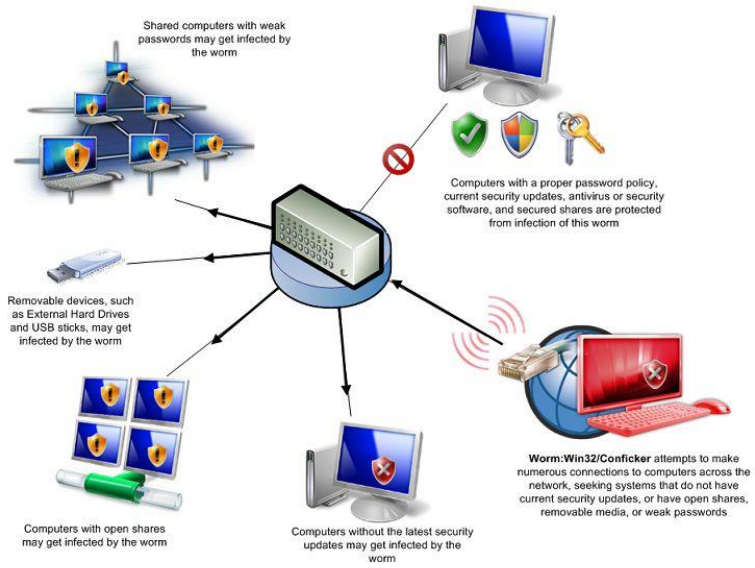
See you later. Thanks ή Nos vemos pronto, gracias.

Αφού μολύνει τον «ξενιστή» υπολογιστή, ψάχνει συγκεκριμένους φακέλους του σκληρού δίσκου του για οποιαδήποτε e-mail διεύθυνση περιέχεται στα αρχεία: *sho*., get*., hot*. και *.htm,* τις οποίες και καταγράφει στα δικά του αρχεία με όνομα scy1.dll, sch1.dll, sci1.dll και sct1.dll

Ακόμη και με κλειστό το πρόγραμμα αποστολής μηνυμάτων, εκείνο έχει δικό του SMTP server, δηλαδή δεν είναι απόλυτα εξαρτημένο από το PC, και θα καταφέρει να στείλει τον εαυτό του 8000 φορές σε όσες διευθύνσεις μαζέψει. Εξαπλώνεται και μέσω ανοικτών μετοχές σε ένα δίκτυο

7. Ο ιός **«Conflicker»**

Ο ιός «Conflicker», επίσης γνωστή ως: Downup, Downadup και Kido**.**



Είναι ένας ιός τύπου worm υπολογιστή με στόχο την Microsoft Windows που εντοπίστηκε για πρώτη φορά το Νοέμβριο του 2008.

Ο ιός τύπου «worm Conflicker» μολυνθεί εκατομμύρια υπολογιστές, συμπεριλαμβανομένων της κυβέρνησης, των επιχειρήσεων και οικιακούς υπολογιστές σε πάνω από 200 χώρες, καθιστώντας την τη μεγαλύτερη γνωστή ιό τύπου worm υπολογιστή από το 2003

Η πρώτη παραλλαγή του ιού «Conflicker», ανακαλύφθηκε στις αρχές Νοεμβρίου του 2008, διαδίδεται μέσω του Διαδικτύου, αξιοποιώντας μια ευπάθεια σε μια υπηρεσία δικτύου *(MS08-067)* για Windows 2000 , Windows XP ,Windows Vista ,Windows Server 2003,Windows Server 2008 και Windows Server 2008 R2 Beta.Αν και τα Windows 7 ενδέχεται να έχουν επηρεαστεί από αυτό το θέμα ευπάθειας, το Windows 7 Beta δεν ήταν διαθέσιμες στο κοινό μέχρι τον Ιανουάριο του 2009.

Μια δεύτερη παραλλαγή του ιού, που ανακαλύφθηκε τον Δεκέμβριο του 2008, προστέθηκε η δυνατότητα να διαδοθεί πάνω στα τοπικά δίκτυα μέσω των αφαιρούμενων μέσων και μετοχών του δικτύου. Οι ερευνητές πιστεύουν ότι αυτές ήταν καθοριστικοί παράγοντες για επιτρέποντας στον ιό να διαδοθεί γρήγορα.

Επίσης μολύνει οποιαδήποτε συσκευή αποθήκευσης δεδομένων *(υπηρεσία autorun)* και μπορεί ακόμα να ανακαλύψει τον κωδικό πρόσβασης του χρήστη του Η/Υ. Μέχρι τα τέλη του 2009 είχε μολύνει περίπου 10 εκατομμύρια Η/Υ.

Θα πρέπει να αναφέρουμε ότι ο ιός αυτός βρίσκεται στην 2η θέση από τους 10 χειρότερους ιούς Η/Υ όλων των εποχών.

8. Ο ιός **«Slammer»**

Ο ιός «Slammer» ήτανε ένα σκουλήκι που εμφανίστηκε στις 25 Ιανουαρίου 2003 και πυροδότησε μια παγκόσμια Διαδικτύου επιβράδυνση και προκάλεσε σημαντικές βλάβες μέσω δικτύου, διακοπές και άλλες απρόβλεπτες συνέπειες. Κυρίως μολύνει συστήματα Microsoft Windows. Ε. Ο ιός αυτός ήτανε γνωστός και ως «Sapphire

Ο ιός «Slammer» είχε μολύνει πάνω από το 90% των ευάλωτων υπολογιστών σε όλο τον κόσμο μέσα σε 10 λεπτά από την απελευθέρωσή του στο Διαδίκτυο, καθιστώντας την ταχύτερη εξάπλωση σκουλήκι υπολογιστών στην ιστορία. Διπλασιάζει σε μέγεθος κάθε 8,5 δευτερόλεπτα και την επίτευξη πλήρους ρυθμού σάρωσης του *(55 εκατομμύρια σαρώσεις ανά δευτερόλεπτο)* μετά από περίπου 3 λεπτά. Θα προκαλέσει σημαντική ζημία μέσω του δικτύου διακοπές και απρόβλεπτα συμβάντα, όπως το κλείσιμο του ενός τηλεφωνικού κέντρου έκτακτης ανάγκης 911, προκαλώντας ακυρώσεις πτήσεων αεροπορικών εταιρειών και στα μηχάνημα αυτόματης ανάληψης *(ATM)* αποτυχίες.

Ο ιός ανακάλυπτε "ευάλωτους" Η/Υ μέσω Internet και μετέδιδε τον εαυτό του σε αυτούς, μολύνοντας τους. Η συνεχής μετάδοση του ιού τελικά οδήγησε σε αδυναμία τους Η/Υ να μπορούν να χρησιμοποιηθούν και να έχουν πρόσβαση στο Internet.

Εξαπλώθηκε τόσο γρήγορα που λέγεται ότι είχε μολύνει 75.000 Η/Υ σε μόλις 10 λεπτά. Αναφορικά εκτιμήσεις κόστους του Slammer κυμαίνονται μεταξύ $ 1,05 και $ 1,250,000,000.

Θα πρέπει να αναφέρουμε ότι ο ιός αυτός βρίσκεται στην 3η θέση από τους 10 χειρότερους ιούς Η/Υ όλων των εποχών

Υπάρχουν και πολύ ακόμα ιοί όπως:

1. Ιός **«Storm Worm»** κατηγορίας "Δούρειος Ίππος"

Εμφανίστηκε στις 17 Ιανουαρίου 2007 και μολύνει συστήματα Microsoft Windows. Μεταδίδεται μέσω e-mail με θέμα το οποίο προειδοποιεί για φονική καταιγίδα *(deadly storm)*. Ο μολυσμένος Η/Υ μπορεί να χρησιμοποιηθεί από χάκερς για να μεταδώσει τον ιό και σε άλλους Η/Υ.

Θα πρέπει να αναφέρουμε ότι ο ιός αυτός βρίσκεται στην 4η θέση από τους 10 χειρότερους ιούς Η/Υ όλων των εποχών

2. Ιός «**CIH**» ή αλλιώς ιός «Chernobyl».

Μολύνει συστήματα Microsoft Windows, προκαλώντας καταστροφή αρχείων. Ονομάστηκε έτσι γιατί μπορεί να παραμείνει "κρυμμένος" στον Η/Υ του χρήστη και να ενεργοποιηθεί αυτόματα στις 26 Απριλίου, επέτειος του τραγικού πυρηνικού ατυχήματος του Τσερνομπίλ στις 26 Απριλίου 1986.

Θα πρέπει να αναφέρουμε ότι ο ιός αυτός βρίσκεται στην 6η θέση από τους 10 χειρότερους ιούς Η/Υ όλων των εποχών

3. Ιός «**Blaster** » ανήκει στην κατηγορίας "σκουλήκι".

Εμφανίστηκε τον Αύγουστο του 2003 και μολύνει συστήματα Microsoft Windows 2000 και XP. Στέλνει τον εαυτό του με e-mail και μολύνει και άλλους Η/Υ. Πέρα από τη δυνατότητα χρήσης του μολυσμένου Η/Υ για την επίθεση του, ο ιός καμία φορά ανάγκαζε τον μολυσμένο Η/Υ να κάνει συνέχεια επανεκκινήσεις.

Θα πρέπει να αναφέρουμε ότι ο ιός αυτός βρίσκεται στην 8η θέση από τους 10 χειρότερους ιούς Η/Υ όλων των εποχών

ΚΕΦΑΛΑΙΟ 5 : ΚΡΥΠΤΟΓΡΑΦΙΑ

5.1. Ιστορική αναδρομή κρυπτογραφίας

Οι προσπάθειες για να διατηρήσουν την μυστικότητα ξεκινάνε από την γέννηση την ανθρωπότητας . Η κρυπτογραφία προέκυψε ως ιδεολογική προσέγγιση και έννοια σχεδόν με την επινόηση της γραφής. Η τέχνη για την διατήρηση της μυστικότητας οδήγησε στην κρυπτογραφία.

Ιστορικά, η κρυπτογραφία χρησιμοποιήθηκε για τη μετατροπή της πληροφορίας μηνυμάτων από μια κανονική, (κατανοητή μορφή) σε έναν «γρίφο», που χωρίς τη γνώση του κρυφού μετασχηματισμού θα παρέμενε ακατανόητος. Κύριο χαρακτηριστικό των παλαιότερων μορφών κρυπτογράφησης ήταν ότι η επεξεργασία γινόταν πάνω στη γλωσσική δομή του μηνύματος.

Στις νεότερες μορφές, η κρυπτογραφία κάνει χρήση του αριθμητικού ισοδύναμου, ενώ η έμφαση έχει μεταφερθεί σε διάφορα πεδία των μαθηματικών, όπως:

1. Διακριτά μαθηματικά
2. Θεωρία αριθμών
3. Θεωρία πληροφορίας
4. Υπολογιστική Πολυπλοκότητα
5. Στατιστική
6. Συνδυαστική ανάλυση

Η ιστορία της κρυπτογραφίας προσεγγιστικά διαιρείται σε τρία στάδια :

$1^{ο}$ στάδιο ή $1^{η}$ περίοδος → 1900 π.Χ – 1900 μ.Χ

Στο πρώτο στάδιο οι διαδικασίες κρυπτογράφησης αφορούσαν τον τρόπο της έντυπης απεικόνισης (μελάνι και χαρτί). Έλαβαν την μορφή αντικατάστασης και αναδιάταξη των γραμμάτων της αλφαβήτου. Ενδεικτικά ο κρυπτογραφικός αλγόριθμος του Καίσαρα)

$2^{ο}$ στάδιο ή $2^{η}$ περίοδος → 1900 μ.Χ – 1950 μ.Χ

Στο δεύτερο στάδιο έχουμε της κρυπτογραφικές μηχανές ιδίως στην περίοδο του Β παγκοσμίου πολέμου . Που είναι η γερμανική μηχανή Enigma

Στην φωτογραφία βλέπουμε πως ήτανε η συσκευή Enigma

Είναι μια οποιαδήποτε συσκευή από μια οικογένεια συσχετιζόμενων ηλεκτρο-μηχανικών rotor συσκευών που χρησιμοποιήθηκαν για την κρυπτογράφηση και αποκρυπτογράφηση μυστικών μηνυμάτων. Η πρώτη συσκευή Enigma εφευρέθηκε από τον Γερμανό μηχανικό Άρθουρ Σέρμπιους στο τέλος του Πρώτου Παγκοσμίου Πολέμου.

3^{ο} στάδιο ή 3^{η} περίοδος →1950 μ.Χ- Σήμερα

Στο τελευταίο στάδιο έχουμε το σύγχρονο κρυπτογραφικό σύστημα όπου μαθηματικά και υπολογιστές αλληλεπιδρούν μεταξύ τους. Οι υπολογιστές επέτρεψαν την χρήση περιπλοκότερων αλγορίθμων κρυπτογράφησης και τα μαθηματικά από την άλλη πρόσφεραν τον σχεδιασμός τους.

Θα πρέπει επίσης να αναφέρουμε κάποιες ακόμα ημερομηνίες που είναι εξίσου σημαντικές σε αυτή την περίοδο:

- **Το 1997:** Η πιο εντυπωσιακή ανάπτυξη στην ιστορία της κρυπτογραφίας ήρθε όταν ο Diffie και ο Hellman δημοσίευσαν το «New directions in cryptography»

Αυτή η επιστημονική δημοσίευση εισήγαγε την επαναστατική έννοια της κρυπτογραφίας δημοσίου κλειδιού. Παρόλο που οι συγγραφείς δεν έκαναν πρακτική εφαρμογή του σχήματος που πρότειναν, η αρχή είχε γίνει και το θέμα έτυχε μεγάλου ενδιαφέροντος από την κρυπτογραφική κοινότητα.

- **Το 1978:** Οι Rivest, Shamir και Adleman ανακάλυψαν την πρώτη πρακτική εφαρμογή του προταθέντος σχήματος.

Ήταν το λεγόμενο σχήμα RSA και βασιζόταν σε ένα άλλο δύσκολο μαθηματικό πρόβλημα, αυτό της δυσκολίας παραγοντοποίησης μεγάλων ακεραίων. Όπως ήταν φυσικό οι κρυπταναλυτές σήκωσαν τα μανίκια και άρχισαν να ψάχνουν πιο αποτελεσματικούς τρόπους παραγοντοποίησης. Παρά τις μεγάλες προόδους τους κυρίως την δεκαετία του 80 το RSA παρέμεινε ακόμα ασφαλές.

Μια από τις σημαντικότερες προσφορές της κρυπτογραφίας δημοσίου κλειδιού ήταν και η ψηφιακή υπογραφή.

Η κρυπτογραφία μπορούμε να πούμε ότι ξεκίνησε σαν τέχνη ή ακόμα και σαν ένα παιχνίδι που εξελίχθηκε σε επιστήμη με στόχο την ασφάλεια των υπολογιστικών πληροφοριών και επικοινωνιακών συστημάτων.

5.2. Βασική ορολογία κρυπτογραφίας

Η λέξη κρυπτογραφία *(cryptography)* προέρχεται από τα συνθετικά «κρυπτός» + «γράφω» και είναι ένα διεπιστημονικό γνωστικό πεδίο που ασχολείται με τη μελέτη, την ανάπτυξη και τη χρήση: τεχνικών κρυπτογράφησης και αποκρυπτογράφησης με σκοπό την απόκρυψη του περιεχομένου των μηνυμάτων.

Με τον όρο «Κρυπτογραφία» εννοούμε τη μελέτη μαθηματικών τεχνικών που στοχεύουν στην εξασφάλιση θεμάτων που άπτονται της ασφάλειας μετάδοσης της πληροφορίας όπως

a. Εμπιστευτικότητα
b. Πιστοποίηση ταυτότητας του αποστολέα
c. Διασφάλιση του αδιάβλητου της πληροφορίας

Ο κύριος στόχος της Κρυπτογραφίας είναι να παρέχει μηχανισμούς ώστε 2 ή περισσότερα άκρα επικοινωνίας π.χ. άνθρωποι, προγράμματα υπολογιστών κλπ. να ανταλλάξουν μηνύματα, χωρίς κανένας τρίτος να είναι ικανός να διαβάζει την περιεχόμενη πληροφορία εκτός από τα δύο κύρια άκρα.

Χρησιμοποιούνται κυρίως δυο μορφές κρυπτογραφίας σε δίκτυα υπολογιστών:

- η κρυπτογραφία συμμετρικού κλειδιού
- και η κρυπτογραφία δημοσίου κλειδιού

5.3. Κρυπτογραφία σε συμμετρικά κλειδιά

Η κρυπτογράφηση συμμετρικού κλειδιού *(Symmetric Cryptography)* βασίζεται στην ύπαρξη ενός και μόνο κλειδιού, το οποίο χρησιμοποιείται τόσο στην κρυπτογράφηση όσο και στην αποκρυπτογράφηση του μηνύματος.

Το κλειδί αυτό θα πρέπει να είναι γνωστό μόνο στα συναλλασσόμενα μέρη.

Ο αριθμό βημάτων είναι:

- Ο αποστολέας ενός μηνύματος κρυπτογραφεί το μήνυμα χρησιμοποιώντας έναν αλγόριθμο που βασίζεται σε κλειδί.
- Το κρυπτογραφημένο μήνυμα στέλνεται μέσω του (ανασφαλούς) δικτύου, π.χ. μέσω του Internet.
- Το κλειδί μεταφέρεται με κάποιο ασφαλή τρόπο στον παραλήπτη.

- Ο παραλήπτης λαμβάνει το κλειδί και το χρησιμοποιεί για να αποκρυπτογραφήσει το μήνυμα που έλαβε.

Η κρυπτογράφηση συμμετρικού κλειδιού είναι πολύ αποδοτική όσον αφορά τους πόρους που απαιτούνται, ωστόσο έχει ένα βασικό πρόβλημα: ότι πρέπει το κλειδί να μεταφερθεί μέσω ενός ασφαλούς μέσου και πιθανόν θα μπορούσε η μετάδοση του να θέσει σε κίνδυνο την ασφάλεια του κρυπτογραφημένου μηνύματος. Περαιτέρω, δεν κάνει διάκριση μεταξύ αποστολέα και παραλήπτη.

5.4. Επιθέσεις σε συμμετρικά κλειδιά

Υπάρχουν διάφοροι τρόποι με τους οποίους ένας αλγόριθμος συμμετρικού κλειδιού μπορεί να δεχθεί επίθεση.

1ος τρόπος: Ο πιο απλός είναι η δοκιμή όλως των δυνατών κλειδιών μέχρι να προκύψει κάποιο κείμενο που φαίνεται να έχει λογικό περιεχόμενο. Αυτό μπορεί να φαίνεται μια όχι και τόσο εύκολη δυνατότητα αλλά αν το μέγεθος του κλειδιού είναι σχετικά μικρό, τότε είναι εφικτό.

2ος τρόπος: είναι να κλέψετε το κλειδί.

3ος τρόπος: γνωστή ως επίθεση γνωστού κειμένου.

Αυτή η τεχνική βασίζεται στο γεγονός ότι ο υποκλοπέας έχει ένα παράδειγμα απλού κειμένου μαζί με το αντίστοιχο του κωδικοποιημένο μήνυμα. Από αυτά ο υποκλοπέας μπορεί να υπολογίσει το κλειδί που χρησιμοποιήθηκε για την κρυπτογράφηση και στη συνέχεια μπορεί να το χρησιμοποιήσει για να αποκωδικοποιήσει εύκολα και άλλα μηνύματα.

Η απόκτηση ενός δείγματος κρυπτογραφημένου κειμένου και του αντίστοιχου αρχικού κειμένου είναι αρκετές φορές αρκετά εύκολο αφού αρκετές φορές μέρος των μηνυμάτων που ανταλλάσσονται είναι αρκετά απλό να βρεθεί, για παράδειγμα τα έχουν κάποια σταθερή μορφή επικεφαλίδας

4ος τρόπος είναι η επίθεση επιλεγμένου κειμένου.

Σε αυτό το είδος επίθεσης ζητά από τον υπολογιστή που εκτελεί την αποκρυπτογράφηση να κωδικοποιήσει ένα ειδικό κομμάτι κειμένου, το οποίο έχει επιλεγεί ώστε η γνώση του αντίστοιχου κρυπτογραφημένου κειμένου να παρέχει αρκετά στοιχεία για το κλειδί.

5ος τρόπος είναι γνωστή ως διαφορική επίθεση κρυπτοανάλυση.

Εδώ ο υποκλοπέας δημιουργεί μια σειρά μηνυμάτων που διαφέρουν ελάχιστα μεταξύ τους και εξετάζει πάλι την αντίστοιχη κρυπτογραφημένη έκδοση τους. Με τον τρόπο αυτό ο υποκλοπέας μπορεί να αποκτήσει σημαντικές πληροφορίες για το κλειδί.

6ος τρόπος: είναι γνωστή ως διαφορική επίθεση λαθών.

Αυτή είναι μια επίθεση με hardware όπου η συσκευή κωδικοποίησης δέχεται πίεση συγκεκριμένης μορφής ώστε να κάνει λάθη. Με προσεκτική εξέταση των λαθών αυτών μπορεί να ανιχνευθεί το κλειδί.

5.5. Κρυπτογραφία Δημόσιου κλειδιού

Η κρυπτογράφηση δημοσίου κλειδιού *(Public Key Cryptography)* ή ασύμμετρου κλειδιού *(Asymmetric Cryptography)* επινοήθηκε στο τέλος της δεκαετίας του 1970 και παρέχει ένα εντελώς διαφορετικό μοντέλο διαχείρισης των κλειδιών κρυπτογράφησης από την προγενέστερη κρυπτογράφηση συμμετρικού κλειδιού .

Η βασική ιδέα είναι ότι ο αποστολέας και ο παραλήπτης δεν μοιράζονται ένα κοινό μυστικό κλειδί όπως στην περίπτωση της κρυπτογράφηση συμμετρικού κλειδιού, αλλά διαθέτουν διαφορετικά κλειδιά για διαφορετικές λειτουργίες

5.6. Επιθέσεις σε συστήματα δημοσίου κλειδιου

Υπάρχουν δυο είδη επιθέσεων σε συστήματα δημοσίου κλειδιού.

1. επίθεση με δεδομένα (*factoring attack).*

Νωρίτερα αναφερθήκαμε ότι οι γνωστές μέθοδοι κρυπτογραφίας δημοσίου κλειδιού βασίζονται στην τεράστια δυσκολία επίλυσης αντεστραμμένων προβλημάτων. Όποιος μπορεί να αναλύσει μεγάλους αριθμούς μπορεί να σπάσει και ένα σύστημα δημοσίου κλειδιού βασιζόμενος σε ανάλυση.

Αυτό δεν είναι απίθανο: μαθηματικοί που δουλεύουν στην περιοχή την θεωρίας αριθμών έχουν μελετήσει προβλήματα ανάλυσης για καιρό και είναι πετυχημένοι με αριθμούς που έχουν συγκεκριμένα χαρακτηριστικά. Η άλλη τεχνική που εφαρμόζεται για το σπάσιμο μιας κρυπτογραφίας δημοσίου κλειδιού είναι να βρεθεί κάποιο μειονέκτημα στον αλγόριθμο που χρησιμοποιείται.

Για παράδειγμα,

Ένα από τα πρώτα προβλήματα που παρουσιάστηκαν είναι το knapsack. Βρέθηκε ότι είναι εύκολο να εξακριβωθεί το ιδιωτικό κλειδί από το δημόσιο κλειδί σε ένα σύστημα με αυτό το πρόβλημα.

2. Κρυπτογραφία ελλειπτικής καμπύλης

Μια πολλά υποσχόμενη μορφή κρυπτογραφίας που απειλεί να ξεπεράσει τη χρήση ανάλυσης στα συστήματα δημοσίου κλειδιού είναι η κρυπτογραφία ελλειπτικής καμπύλης. που περιλαμβάνει την επίλυση δύσκολων υπολογιστικά προβλημάτων χρησιμοποιώντας μια οικογένεια καμπυλών, γνωστές σαν ελλειπτικές καμπύλες.

Πολλά συστήματα δημοσίου κλειδιού χρησιμοποιούν τον RSA. Παρόλα αυτά, η αυξανόμενη ισχύς των υπολογιστών έφερε και την αύξηση του μήκους των bit, που οδήγησε σε ακόμη μεγαλύτερες υπολογιστικές απαιτήσεις.

Η κρυπτογραφία ελλειπτικής καμπύλης είναι το ίδιο ασφαλή με τον RSA. Όμως, απαιτεί μικρότερα μήκη bit και συνεπώς λιγότερους υπολογισμούς

5.7. Συμμετρικό κλειδί vs. Κρυπτογραφία δημόσιου κλειδιού

Συγκεκριμένα κάθε χρήστης διαθέτει δύο κλειδιά κρυπτογράφησης: το ένα ονομάζεται ιδιωτικό κλειδί *(private key)* και το άλλο δημόσιο κλειδί *(public key*).

Το ιδιωτικό κλειδί θα πρέπει ο κάθε χρήστης να το προφυλάσσει και να το κρατάει κρυφό, ενώ αντιθέτως το δημόσιο κλειδί μπορεί να το ανακοινώνει σε όλη τη διαδικτυακή κοινότητα ή σε συγκεκριμένους παραλήπτες. Υπάρχουν δε και ειδικοί εξυπηρετητές δημοσίων κλειδιών *(public key servers)* στους οποίους μπορεί κανείς να απευθυνθεί για να βρει το δημόσιο κλειδί του χρήστη που τον ενδιαφέρει ή να ανεβάσει το δικό του δημόσιο κλειδί για να είναι διαθέσιμο στο κοινό.

Τα δύο αυτά κλειδιά *(ιδιωτικό και δημόσιο)* έχουν μαθηματική σχέση μεταξύ τους. Εάν το ένα χρησιμοποιηθεί για την κρυπτογράφηση κάποιου μηνύματος, τότε το άλλο χρησιμοποιείται για την αποκρυπτογράφηση αυτού.

Η επιτυχία αυτού του είδους κρυπτογραφικών αλγορίθμων βασίζεται στο γεγονός ότι η γνώση του δημόσιου κλειδιού κρυπτογράφησης δεν επιτρέπει με κανέναν τρόπο τον υπολογισμό του ιδιωτικού κλειδιού κρυπτογράφησης. Η κρυπτογράφηση δημοσίου κλειδιού λύνει ένα σημαντικότατο πρόβλημα που υπήρχε στους κρυπτογραφικούς αλγόριθμους συμμετρικού κλειδιού.

Συγκεκριμένα, οι κρυπτογραφικοί αλγόριθμοι συμμετρικού κλειδιού χρησιμοποιούν ένα κοινό μυστικό κλειδί, το οποίο το γνωρίζουν τόσο ο αποστολέας του κρυπτογραφημένου μηνύματος όσο και ο παραλήπτης. Αυτό το κοινό μυστικό κλειδί χρησιμοποιείται κατά τη διαδικασία κρυπτογράφησης και αποκρυπτογράφησης του μηνύματος. Προκύπτει όμως το εξής πρόβλημα: Εάν υποθέσουμε ότι το κανάλι επικοινωνίας δεν είναι ασφαλές, τότε πως γίνεται ο αποστολέας να στείλει το κλειδί κρυπτογράφησης στον παραλήπτη για να μπορέσει αυτός με τη σειρά του να αποκρυπτογραφήσει το μήνυμα;

Αυτό το πρόβλημα είναι ιδιαίτερα έντονο στις σύγχρονες ψηφιακές επικοινωνίες όπου σε πολλές περιπτώσεις ο αποστολέας δεν γνωρίζει καν τον παραλήπτη και απέχει από αυτόν αρκετές χιλιάδες χιλιόμετρα. Οι κρυπτογραφικοί αλγόριθμοι

δημοσίου κλειδιού λύνουν αυτό το πρόβλημα και ανοίγουν νέους δρόμους για εφαρμογές της κρυπτογράφησης *(ηλεκτρονικά μηνύματα, διαδικτυακές αγορές κοκ)*

Γενικα

Η εξέλιξη της χρησιμοποίησης της κρυπτογραφίας ολοένα αυξάνεται καθιστώντας πλέον αξιόπιστη τη μεταφορά της πληροφορίας για διάφορους λειτουργικούς σκοπούς:

1. Ασφάλεια συναλλαγών σε τράπεζες δίκτυα – ATM
2. Κινητή τηλεφωνία *(ΤΕΤΡΑ-ΤΕΤΡΑΠΟΛ-GSM)*
3. Σταθερή τηλεφωνία *(crypto phones)*
4. Διασφάλιση Εταιρικών πληροφοριών
5. Στρατιωτικά δίκτυα *(Τακτικά συστήματα επικοινωνιών μάχης)*
6. Διπλωματικά δίκτυα *(Τηλεγραφήματα)*
7. Ηλεκτρονικές επιχειρήσεις *(πιστωτικές κάρτες, πληρωμές)*
8. Ηλεκτρονική ψηφοφορία
9. Ηλεκτρονική δημοπρασία
10. Ηλεκτρονικό γραμματοκιβώτιο
11. Συστήματα συναγερμών
12. Συστήματα βιομετρικής αναγνώρισης
13. Έξυπνες κάρτες
14. Ιδιωτικά δίκτυα *(VPN)*
15. Word Wide Web
16. Δορυφορικές εφαρμογές *(δορυφορική τηλεόραση)*
17. Ασύρματα δίκτυα *(Hipperlan, Bluetooth, 802.11x)*
18. Συστήματα ιατρικών δεδομένων και άλλων βάσεων δεδομένων
19. Τηλεσυνδιάσκεψη - Τηλεφωνία μέσω διαδικτύου *(VOIP)*

ΚΕΦΑΛΑΙΟ 6: ΑΣΦΑΛΕΙΑ ΣΤΟ ΔΙΑΔΥΚΤΙΟ

6.1 SSL

Το πρωτόκολλο SSL *(Secure Socket Layer)* ή Ασφαλές Επίπεδο Υποδοχών. είναι ένα από τα γνωστότερα πρωτόκολλα ασφαλείας που χρησιμοποιούνται για την διεκπεραίωση συναλλαγών στο Διαδίκτυο.

Ιστορική Αναδρομή

Το 1995 η εταιρεία Netscape Communications, που ήταν ένας από τους δύο κορυφαίους δημιουργούς λογισμικού πλοήγησης, του Netscape Communicator, στην προσπάθεια να ανταποκριθεί στην παραπάνω ανάγκη, παρουσίασε το πακέτο ασφάλειας SSL. Το πρωτόκολλο SSL σχεδιάστηκε και αναπτύχθηκε, αρχικά, για την χρήση του με την εφαρμογή Netscape Communicator. Όμως αργότερα χρησιμοποιήθηκε ευρέως, ακόμη και από τον φυλλομετρητή της Microsoft γνωστό ως Internet Explorer.

Όσων αφορά την ανάπτυξή του πρωτοκόλλου, έχουμε

- Με την έκδοση ν.1.0 χρησιμοποιήθηκε μόνο για εσωτερικές ανάγκες της Netscape.
- Με την έκδοση ν.2.0 ενσωματώθηκε στις εκδόσεις 1. και 2. του Netscape Navigator. Σε αυτή την μορφή ήταν που το SSL καθιερώθηκε ως αναπόσπαστο πρότυπο για την παροχή κρυπτογραφικής προστασίας στην κυκλοφορία δεδομένων μέσω HTTP.
- Ωστόσο, επειδή υπήρχαν αρκετοί περιορισμοί σε αυτή την έκδοσή του, τόσο ως προς την κρυπτογραφική ασφάλεια όσο και ως προς τη λειτουργικότητα του, προέκυψε η αναβάθμιση του στην έκδοση 3.0.

Αξίζει να αναφερθεί πως στην υλοποίηση αυτή της έκδοσης υπήρξε σημαντική συνεισφορά από τη βιομηχανία και η αναθεώρηση έγινε δημόσια. Η έκδοση αυτή τέθηκε επισήμως σε κυκλοφορία στα τέλη του 1995. Η τελική του σύνθεση, με τις τελικές προδιαγραφές, κυκλοφόρησε τέλη του επόμενου έτους

Σε γενικές γραμμές, αυτό που ουσιαστικά κάνει, είναι σε κάθε μήνυμα να δημιουργείται ένα αποτύπωμα το οποίο, αν μεταβληθεί *(παραδείγματος χάριν, αν κάποιος τρίτος προσπαθήσει να ανακτήσει απόρρητες πληροφορίες*), τότε η συναλλαγή ματαιώνεται και ζητείται από το χρήστη να επανεισαγάγει τα στοιχεία του.

Το SSL χρησιμοποιεί κρυπτογράφηση με κοινό κλειδί, μια από τις ισχυρότερες μεθόδους κρυπτογράφησης

Σε απλά βήματα λειτουργεί ως εξής:

1. Οι πληροφορίες κρυπτογραφούνται έτσι ώστε να μην είναι εφικτή η ανάγνωσή τους από τρίτους.
2. Οι πληροφορίες ελέγχονται για την αυθεντικότητα τους με στόχο να μην είναι δυνατή η αποστολή και λήψη τους από και προς υπολογιστές που δεν είναι κατάλληλα εξουσιοδοτημένοι.
3. Εξασφαλίζεται, με κατάλληλο τρόπο, η ακεραιότητα του μεταφερόμενου μηνύματος, έτσι ώστε κάποιος τρίτος να μη μπορεί να το αλλοιώσει

Το SSL προσφέρει συνοπτικά τις ακόλουθες υπηρεσίες:

- Πιστοποίηση του server από τον client.
- Πιστοποίηση του client από τον server.
- Εγκαθίδρυση ασφαλούς κρυπτογραφημένου διαύλου επικοινωνίας μεταξύ των δύο μερών.

6.2 Αδυναμία - μειονεκτήματα του πρωτοκόλλου SSL

Η μεγαλύτερη αδυναμία του πρωτοκόλλου είναι η ευαισθησία των αλγόριθμων που χρησιμοποιούν μικρά κλειδιά.

Ένα άλλο μειονέκτημα της χρήσης του SSL πρωτοκόλλου αποτελεί το γεγονός ότι επιβραδύνεται η επικοινωνία του προγράμματος πλοήγησης του εξυπηρετούμενου με τον HTTPS εξυπηρέτη, η καθυστέρηση οφείλεται στις λειτουργίες κρυπτογράφησης και αποκρυπτογράφησης με ασύμμετρο κρυπτοσύστημα κατά την αρχικοποίηση της SSL συνόδου. (*Πρακτικά, οι χρήστες αντιλαμβάνονται μικρή καθυστέρηση λίγων δευτερολέπτων μεταξύ της έναρξης συνόδου με τον HTTPS εξυπηρέτη και της ανάκτησης της πρώτης HTML σελίδας από αυτόν).*

Επειδή κατά τη σχεδίαση του SSL αποθηκεύεται το κύριο μυστικό κλειδί, η καθυστέρηση επηρεάζει μόνον την πρώτη SSL επικοινωνία μεταξύ προγράμματος πλοήγησης και HTTPS εξυπηρέτη.

Επίσης, μόνο στην έκδοση 2.0, υπάρχει αδυναμία που αφορά την επαναδιαπραγμάτευση κλειδιών συνόδου. Από τη στιγμή που μία σύνοδος δημιουργηθεί, το ίδιο κλειδί *(master key)* χρησιμοποιείται καθ' όλη τη διάρκεια της. Όταν το SSL χρησιμοποιείται πάνω από μια μακρόχρονη σύνοδο *(π.χ. μιας εφαρμογής TELNET)*, η αδυναμία αλλαγής του κλειδιού γίνεται επικίνδυνη. Η καλύτερη μέθοδος επίλυσης αυτού του προβλήματος είναι η επαναδιαπραγμάτευση του κλειδιού σε τακτά χρονικά διαστήματα, μειώνοντας έτσι την πιθανότητα μιας επιτυχούς «Ευθείας Επίθεσης» *(Brute Force Attack)*

6.3 Επιθέσεις- Ανθεκτικότητα του Πρωτοκόλλου SSL

Όπως συμβαίνει σε όλα τα πρωτόκολλα και υπηρεσίες δικτύων, έτσι και εδώ υπάρχουν συγκεκριμένες επιθέσεις που μπορούν να χρησιμοποιηθούν ενάντια στο πρωτόκολλο SSL ή σε εφαρμογές του

Θα πρέπει να σημειωθεί ότι η εύρεση μιας αδυναμίας σε μια συγκεκριμένη εφαρμογή του πρωτοκόλλου SSL δεν σημαίνει απαραίτητα ότι υπάρχει κάποιο ελάττωμα στο πρωτόκολλο SSL. Αυτό που τελικά προκύπτει είναι ότι η εφαρμογή μπορεί να είναι ευάλωτη σε μια συγκεκριμένη επίθεση ή λόγο κάποιας αδυναμίας, που όμως δεν εξυπακούεται πως όλες οι εφαρμογές υλοποιημένες με το πρωτόκολλο αυτό είναι τρωτές.

Ακολουθεί ένας κατάλογος από μεθόδους επίθεσης που θα μπορούσαν να χρησιμοποιηθούν για να παρακάμψουν το SSL πρωτόκολλο:

6.3.1. Επιθέσεις κρυπτογραφίας *(Cipher Attacks ή Cracking Ciphers)*

Επειδή το πρωτόκολλο SSL χρησιμοποιεί πολλαπλές διαφορετικές τεχνολογίες για την εν δυνάμει κρυπτογράφηση, οι επιθέσεις στην μηχανή κρυπτογράφησης ή στα κλειδιά είναι πιθανές. Εάν μια επίθεση, ενάντια σε οποιαδήποτε από τις διαθέσιμες μηχανές κρυπτογράφησης, βρεθεί να είναι επιτυχής, τότε το πρωτόκολλο SSL παύει να είναι ασφαλές.

Άρα οποιαδήποτε από τις διαθέσιμες μεθόδους κρυπτογραφικής ανάλυσης μπορούν να χρησιμοποιηθούν και αυτό περιλαμβάνει την καταγραφή μιας συγκεκριμένης συνόδου επικοινωνίας και τη χρησιμοποίηση πολλών κύκλων επεξεργασίας από την ΚΜΕ (CPU) για να «σπάσει » είτε την σύνοδο αυτή είτε το δημόσιο κλειδί που χρησιμοποιήθηκε.

Επειδή πολλές SSL σύνοδοι χρησιμοποιούν κλειδιά των 128 bit, το κόστος μιας επίθεσης ενάντια ενός τέτοιου κλειδιού είναι ακόμα αρκετά υψηλό. Καθώς νέα πρωτόκολλα και κλειδιά μεγαλύτερου μήκους υποστηρίζονται από το SSL πρωτόκολλο, ο απαιτούμενος φόρτος εργασίας για την αποκρυπτογράφηση του κρυπτογραφημένου μηνύματος αυξάνεται.

6.3.2. Επίθεση Λεξικού *(Dictionary Attack)*

Σε κρυπτοανάλυση και την ασφάλεια του υπολογιστή , ένα λεξικό επίθεση είναι μια τεχνική για να νικήσει ένα κρυπτογραφημένο ή ταυτότητας μηχανισμού προσπαθώντας να καθορίσετε το κλειδί αποκρυπτογράφησης του ή τη φράση πρόσβασης, προσπαθώντας εκατοντάδες ή ακόμη και χιλιάδες πιθανές δυνατότητες, όπως οι λέξεις σε ένα λεξικό.

Ένα λεξικό επίθεση χρησιμοποιεί μια στοχευόμενη τεχνική δλδ προσπαθεί διαδοχικά όλες τις λέξεις σε έναν εξαντλητικό κατάλογο που ονομάζεται λεξικό. Σε αντίθεση με μια ωμή επίθεση, όπου ένα μεγάλο ποσοστό αναζητάται συστηματικά, ένα λεξικό επίθεση προσπαθεί μόνο με αυτές τις δυνατότητες που έχουν τις περισσότερες πιθανότητες να πετύχει, συνήθως προέρχεται από μια λίστα λέξεων για παράδειγμα ένα λεξικό

Σε γενικές γραμμές, η επιθέσεις πετυχαίνει, επειδή πολλοί άνθρωποι έχουν την τάση να επιλέγουν κωδικού πρόσβασης που είναι σύντομες (*7 χαρακτήρες ή λιγότερους)*. Ωστόσο, αυτά είναι εύκολο να το νικήσουμε. προσθέτοντας ένα μόνο τυχαίο χαρακτήρα στη μέση μπορεί να κάνει επιθέσεις λεξικού αστήρικτη.

Σε αντίθεση με τις επιθέσεις Brute-force, οι επιθέσεις λεξικού δεν είναι εγγυημένη για να πετύχει.

6.3.3. Ευθείας Επίθεσης» *(Brute Force Attack)*

Εν συντομία, η επίθεση αυτή θα δοκιμάσει όλους τους πιθανούς συνδυασμούς κάθε κλειδιού προκειμένου να «σπάσει» τον κωδικό πρόσβασης – password. Η μόνη προφύλαξη είναι είτε το μήκος του κλειδιού να είναι πολύ μεγάλο για να «σπασθεί» είτε να γίνεται συχνή αλλαγή αυτού.

Πραγματοποιείται με τη χρήση όλων των πιθανών κλειδιών για την αποκρυπτογράφηση των μηνυμάτων. Όσο πιο μεγάλα σε μήκος είναι τα χρησιμοποιούμενα κλειδιά, τόσο πιο πολλά είναι τα πιθανά κλειδιά.

Τέτοια επίθεση σε αλγορίθμους που χρησιμοποιούν κλειδιά των 128 bits είναι μάταιη.

6.3.4. Επίθεση Επανάληψης *(Replay Attack)*

Μια επίθεση replay *(ή επίθεση αναπαραγωγής)* είναι μια μορφή του διαδικτύου επίθεσης κατά την οποία μια έγκυρη μετάδοση δεδομένων κακόβουλα ή με δόλο ή επανειλημμένη καθυστέρηση.

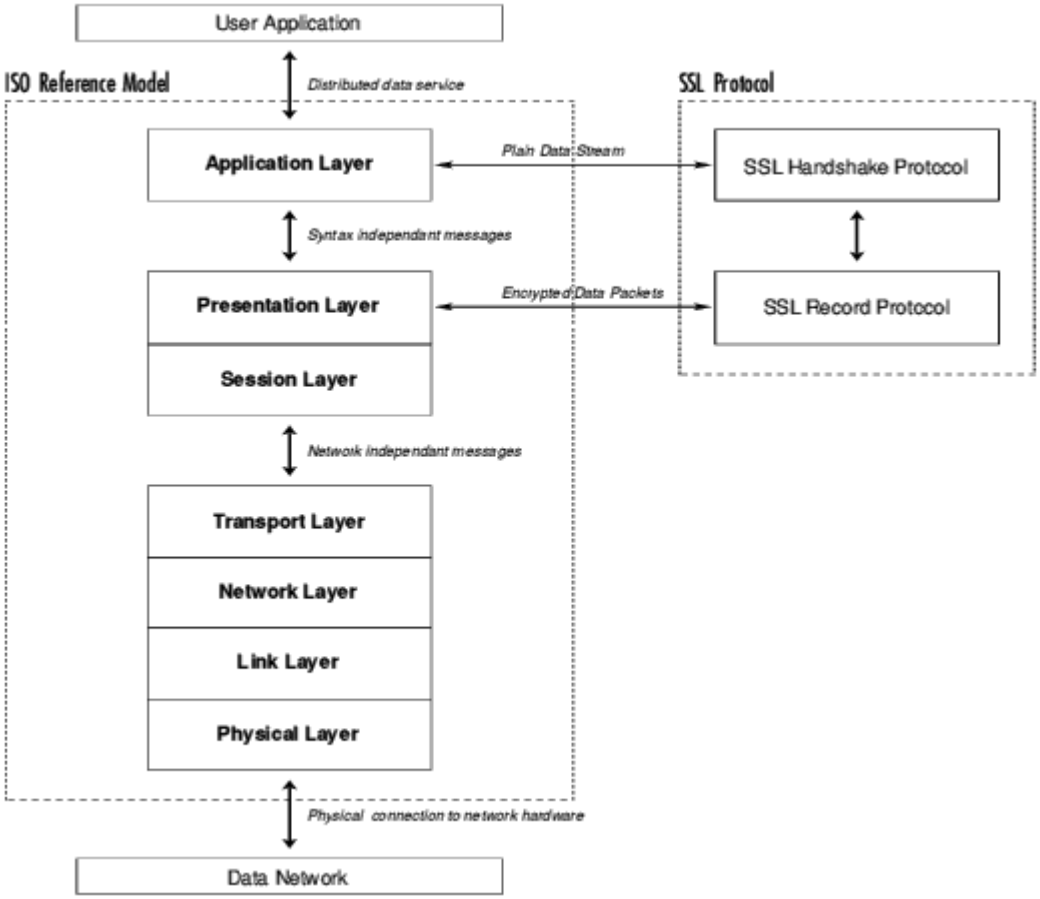
Αυτό πραγματοποιείται είτε από τον εντολέα ή από έναν αντίπαλο ο οποίος αναχαιτίζει τα δεδομένα και αναμεταδίδει, πιθανόν ως μέρος μιας επίθεσης μεταμφίεσης του IP πακέτου υποκατάστασης.

6.3.5. Επίθεση Παρεμβολής *(Man-In-The-Middle Attack)*

Η επίθεση man-in-the-middle είναι μια κοινή παραβίαση ασφαλείας. Ο επιτιθέμενος παρεμποδίζει τη νόμιμη επικοινωνία μεταξύ δύο μερών, τα οποία είναι φιλικά μεταξύ τους. Στη συνέχεια, ο κακόβουλος host ελέγχει τη ροή επικοινωνίας και μπορεί να αποσπάσει ή να αλλάξει πληροφορίες που στέλνονται από έναν από τους αρχικούς συμμετέχοντες.

Οι επιθέσεις man-in-the-middle εφαρμόζονται ιδιαίτερα στο πρωτόκολλο Diffie-Helman όταν η συμφωνία ανταλλαγής κλειδιών γίνεται χωρίς επικύρωση.

6.4. Σχέση του Πρωτοκόλλου SSL και του μοντέλου OSI



Στην παραπάνω εικόνα παρουσιάζεται η σχέση του πρωτοκόλλου SSL και του μοντέλου διασύνδεσης ανοικτών συστημάτων OSI.

Είναι σημαντικό κάθε νέο πρωτόκολλο επικοινωνίας να συμμορφώνεται με το OSI μοντέλο, έτσι ώστε να μπορεί εύκολα να αντικαταστήσει κάποιο υπάρχον πρωτόκολλο ή να ενσωματωθεί στην υπάρχουσα δομή πρωτοκόλλων.

Το SSL χωρίζεται σε δύο μέρη:

- το SSL Handshake Protocol *(SSLHP)*

Το SSLHP διαπραγματεύεται τους αλγόριθμους κρυπτογράφησης που θα χρησιμοποιηθούν και πραγματοποιεί την πιστοποίηση της ταυτότητας του server και εάν ζητηθεί και του client.

- και το SSL Record Protocol *(SSLRP).*

Το SSLRP συλλέγει τα δεδομένα σε πακέτα και αφού τα κρυπτογραφήσει τα μεταδίδει και αποκρυπτογραφεί τα παραλαμβανόμενα πακέτα.

Βλέπουμε πως το SSL λειτουργεί επιπρόσθετα της υπάρχουσας δομής του OSI και όχι σαν πρωτόκολλο αντικατάστασης. Επίσης η χρήση του SSL δεν αποκλείει την χρήσης άλλου μηχανισμού ασφαλείας που λειτουργεί σε υψηλότερο επίπεδο, για παράδειγμα το S/HTTP που εφαρμόζεται στο επίπεδο Εφαρμογών, πάνω από το SSL.

ΚΕΦΑΛΑΙΟ 7: ΑΝΤΙΜΕΤΩΠΙΣΗ

Οι ιοί αποτέλεσαν και αποτελούν έναν από τους πλέον διαδεδομένους τύπους κακόβουλου λογισμικού. Η ανίχνευση τους από τον απλό χρήστη είναι από δύσκολη έως αδύνατη - ορισμένοι, μάλιστα, ιοί, είναι τόσο προσεκτικά δημιουργημένοι που ακόμη και ο πλέον ειδικευμένος χρήστης αδυνατεί να τους εντοπίσει χωρίς να διαθέτει ειδικά προγραμματιστικά εργαλεία.

Για την προστασία ενός συστήματος έχει δημιουργηθεί μια ειδική κατηγορία λογισμικού, γνωστή ως αντιϊκό *(antivirus)* Τα προγράμματα αυτά πρέπει να αναβαθμίζονται σε τακτική βάση, ώστε να είναι σε θέση να αντιμετωπίζουν με επιτυχία τους νέους ιούς.

Σήμερα, αρκετοί οίκοι δημιουργίας λογισμικού ασχολούνται με τη δημιουργία τέτοιων προγραμμάτων. Τα αντιϊκά είναι σε θέση τόσο να εντοπίσουν μμόλυνση τη στιγμή που αποπειράται, όσο και να "καθαρίσουν" τυχόν μολυσμένα αρχεία που εντοπίζουν.

7.1. Συστήματα ανίχνευσης επιθέσεων

Το Σύστημα Ανίχνευσης Εισβολής «ΣΑΕ» ή Intrusion Detection System,« IDS» αποτελεί σύστημα παρακολούθησης και ανάλυσης των συμβάντων, τα οποία λαμβάνουν χώρα τόσο στους ίδιους τους ηλεκτρονικούς υπολογιστές όσο και στα δίκτυα υπολογιστών

Στόχος είναι ο εντοπισμός ενδείξεων για πιθανές προσπάθειες εισβολής, κατά τις οποίες συχνά εντοπίζονται ίχνη παραβίασης

- της ακεραιότητας,
- της εμπιστευτικότητας
- και της διαθεσιμότητας των πληροφοριακών πόρων.

Οι προσπάθειες παράκαμψης των μηχανισμών ασφαλείας μπορεί να προέρχονται από εξωτερικούς χρήστες, προς το εσωτερικό εταιρικό δίκτυο, στους οποίους δεν επιτρέπεται η πρόσβαση στο υπάρχον πληροφοριακό σύστημα. Επίσης, οι προσπάθειες παράκαμψης πιθανόν να προέρχονται από εσωτερικούς χρήστες, με περιορισμένα δικαιώματα πρόσβασης.

Οι λόγοι για να εγκατάστασης ένα σύστημα ανίχνευσης εισβολής ποικίλουν. Οι πιο σημαντικοί από αυτούς τους λόγους είναι:

1. η πρόληψη προβλημάτων,

2. η ανίχνευση παραβιάσεων,
3. η τεκμηρίωση υπαρκτών απειλών,
4. ο έλεγχος ποιότητας για το σχεδιασμό ασφαλείας,
5. καθώς και η θωράκιση παλαιών συστημάτων σε περίπτωση που κρίνεται αναγκαία η διατήρησή τους

7.1. Κρυπτογράφηση

Η ανάγκη για εμπιστευτικότητα στην ηλεκτρονική συναλλαγή ικανοποιείται με την κρυπτογραφία. Ο αποστολέας χρησιμοποιώντας κάποια μαθηματική συνάρτηση μετατρέπει το αρχικό κείμενο σε μορφή μη κατανοητή για οποιονδήποτε τρίτο. Ο παραλήπτης έχοντας γνώση του τρόπου κρυπτογράφησης, αποκρυπτογραφεί το κείμενο στην αρχική του μορφή. Το μήνυμα παραμένει εμπιστευτικό, μέχρι να αποκρυπτογραφηθεί.

Τα σύγχρονα κρυπτοσυστήματα χρησιμοποιούν αλγόριθμους και κλειδιά *(σειρά από bits συγκεκριμένου μήκους)* για να διατηρήσουν την πληροφορία ασφαλή.

Μία ‘παραδοσιακή’ μέθοδος κρυπτογράφησης είναι:

- Η συμμετρική κρυπτογραφία η οποία χρησιμοποιεί το ίδιο κλειδί για την κρυπτογράφηση και την αποκρυπτογράφηση. Δλδ ο αποστολέας κρυπτογραφεί και ο παραλήπτης αποκρυπτογραφεί με το ίδιο κλειδί. Το κλειδί θα πρέπει να παραμένει μυστικό και να είναι γνωστό μόνο στους συναλλασσόμενους.

Η μέθοδος αυτή παρουσιάζει μειονεκτήματα όσον αφορά την εφαρμογή της σε ανοιχτά δίκτυα με πολλούς χρήστες και τις αυξημένες απαιτήσεις της για την ασφάλεια *(π.χ. αποθήκευση των κλειδιών κ.λπ)*.

- Η ασύμμετρη κρυπτογραφία (*ή κρυπτογραφία δημοσίου κλειδιού- public key cryptography)* χρησιμοποιεί δύο διαφορετικά κλειδιά για την κρυπτογράφηση και την αποκρυπτογράφηση.

Κάθε χρήστης έχει στη διάθεσή του δύο κλειδιά. Το δημόσιο κλειδί είναι αυτό που ο χρήστης μπορεί να το γνωστοποιήσει σε τρίτους ενώ το ιδιωτικό είναι εκείνο που το φυλάσσει με ασφάλεια και μόνο αυτός θα πρέπει να το γνωρίζει και κατέχει.

Για να επιτευχθεί η εμπιστευτικότητα, ο αποστολέας κρυπτογραφεί το μήνυμα με το δημόσιο κλειδί του παραλήπτη. Έτσι, το μήνυμα μπορεί να αποκρυπτογραφηθεί μονάχα από τον παραλήπτη *(που είναι ο κάτοχος του αντίστοιχου ιδιωτικού κλειδιού εκτός και αν η μυστικότητα του ιδιωτικού κλειδιού έχει παραβιαστεί)*.

Θα πρέπει να αναφέρουμε ότι με τη συμμετρική κρυπτογραφία, η ασύμμετρη παρουσιάζει μια σειρά από πλεονεκτήματα ως προς την αντιμετώπιση των Ιών

7.2. Εργαλεία παρακολούθησης συστήματος *(logging)*

Αυτά είναι εργαλεία τα οποία παρακολουθούν τη χρήση ενός υπολογιστή ή κάποιας υπηρεσίας ή τμήματος ενός υπολογιστή και κρατούν σε ειδικά ασφαλή αρχεία τη δραστηριότητα που παρακολουθούν.

Συνηθισμένα γεγονότα ή δραστηριότητες που παρακολουθούν τα συστήματα αυτά είναι η είσοδος χρηστών στο σύστημα, η μεταφορά μιας ιστοσελίδας ή η ανάγνωση κάποιων αρχείων.

Ένας καλός διαχειριστής συστημάτων θα εγκαταστήσει ένα εργαλείο παρακολούθησης το οποίο θα δίνει τακτικές αναφορές για την παρατηρούμενη δραστηριότητα και το οποίο επίσης θα ενημερώνει άμεσα τον διαχειριστή αν ένα ιδιαίτερα σημαντικό γεγονός συμβαίνει, όπως για παράδειγμα η ύπαρξη κάποιας σύνδεση η οποία καταναλώνει ένα πολύ μεγάλο μέρος των πόρων του συστήματος.

7.3. Ανιχνευτές ιών

Τα αντιβιοτικά είναι εφαρμογές που προστατεύουν τον υπολογιστή από τους ιούς. Βέβαια πρέπει το αντιβιοτικό να ενημερώνεται τακτικά με τις τελευταίες αναβαθμίσεις. Σε αντίθετη περίπτωση ο υπολογιστής θα μπορεί να προσβληθεί από τους καινούργιους ιούς.

Τα αντιβιοτικά προγράμματα αποτελούνται από δύο τμήματα:

1. η προστασία από τους ιούς και
2. το τμήμα ανίχνευσης

Το πρόγραμμα προστασίας λειτουργεί σαν ασπίδα και ανιχνεύει τους ιούς τη στιγμή που προσπαθούν να εισχωρήσουν στον υπολογιστή και να εγκατασταθούν στη μνήμη του.

Το πρόγραμμα αυτό ελέγχει τη μνήμη του υπολογιστή και τους βασικούς φακέλους με τα αρχεία του λειτουργικού συστήματος. Σε περίπτωση που ένας ιός ενεργοποιηθεί εξαιτίας της εκτέλεσης από το χρήστη μίας μολυσμένης εφαρμογής ή το άνοιγμα ενός μολυσμένου αρχείου, εμφανίζεται το μήνυμα αναφορά ύπαρξης του ιού.

Οι περισσότερες εφαρμογές προστασίας από τους ιούς δίνουν την δυνατότητα στο χρήστη να διαγράψει ή να καθαρίσει *(εάν αυτό είναι εφικτό)* το μολυσμένο αρχείο.

Επίσης τα αντιβιοτικά προγράμματα εκτός από τη μνήμη ελέγχουν και την εισερχόμενη και εξερχόμενη αλληλογραφία.

7.4. Λογισμικό ελέγχου ασφαλείας*(Malware)*

Πρόκειται για προγράμματα *(κώδικας)* που αποσκοπούν σε επιθέσεις κατά της Εμπιστευτικότητας, της Ακεραιότητας ή/και της Διαθεσιμότητας των συστημάτων.

Για την εγκατάσταση ενός κακόβουλου λογισμικού σε έναν Η/Υ, συνήθως απαιτείται (άμμεση ή έμμεση)

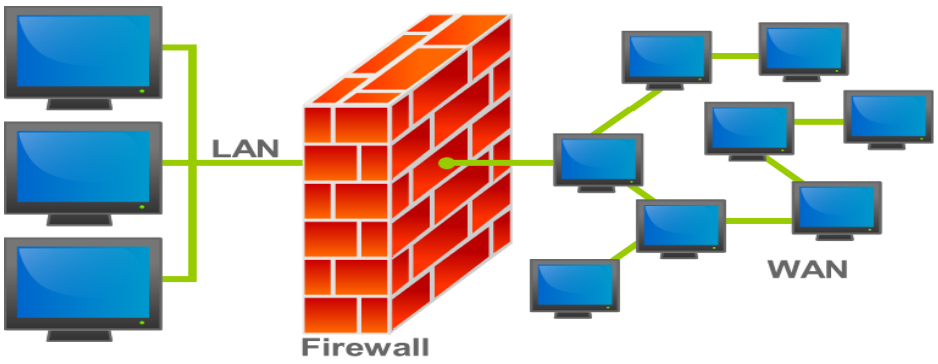
Η ανθρώπινη συμμετοχή είναι η άμεση (*π.χ. ανταλλαγή αρχείων, άνοιγα συνημμένων ή προεπισκόπηση μηνυμάτων αλληλογραφίας αμφιβόλου προέλευσης)* η έμμεση είναι η ανεπαρκής προστασία του υπολογιστή, μη λήψη ενημερωμένων εκδόσεων updates του λογισμικού ασφαλείας και των προγραμμάτων.

Το τμήμα του κώδικα που είναι υπεύθυνο για τις παρενέργειες του λογισμικού ονομάζεται φορτίο *(payload).*

Εκτός από τις παρενέργειες, το κακόβουλο λογισμικό περιλαμβάνει επιπλέον κώδικα με σκοπό την

- Αναπαραγωγή του: Εξάπλωση του στο σύστημα που προσβάλλει («μόλυνση» από πρόγραμμα σε πρόγραμμα).
- Μετάδοση του: Εξάπλωση του από το σύστημα που μολύνθηκε σε άλλο/άλλα συστήματα *(π.χ. από Η/Υ σε Η/Υ)*

7.5. Τεχνικές τοπολογίας δικτύου



Ένας σημαντικός τρόπος να προστατευθείτε από πολλά είδη επιθέσεων είναι να σχεδιάσετε την τοπολογία του δικτύου σας ώστε να είναι δύσκολο να γίνει εισβολή.

Για παράδειγμα,

Μπορεί να είναι σχεδόν αδύνατο να τοποθετηθεί ένας sniffer στο δίκτυο αν το δίκτυο είναι χωρισμένο σε αρκετά τμήματα με τον κατάλληλο τρόπο. Ένας από τους καλύτερους τρόπους να χρησιμοποιηθεί η τοπολογία του δικτύου για να προστατευτεί το δίκτυο είναι χρησιμοποιώντας ένα ***firewall*** *(τείχος προστασίας****).***

Ένα firewall είναι ένα επιπλέον επίπεδο προστασίας τοποθετημένο γύρω από ένα δίκτυο ή από μια συγκεκριμένη εφαρμογή. Ένα firewall που προστατεύει ένα δίκτυο θα περιλαμβάνει συνήθως ένα δρομολογητή (router) που μπορεί να προγραμματιστεί ώστε να μην επιτρέπει επιλεκτικά την πρόσβαση σε ένα δίκτυο, για παράδειγμα θα απορρίπτει πακέτα που δεν στέλνονται σε συγκεκριμένες επιτρεπόμενες θύρες (όπως φαίνεται και στο σχήμα) .

10 τρόποι προστασίας του Η/Υσας είναι:

Πέρα λοιπόν από την εγκατάσταση κάποιου προγράμματος για την προστασία από ιούς θα πρέπει να κάνετε τακτικά και μια σειρά από ενέργειες για να είστε σίγουροι ότι όλα δουλεύουν όπως πρέπει.

1. Αν χρησιμοποιείτε Windows XP, να έχετε πάντα ενεργοποιημένο το Firewall.
2. Να ενημερώνετε πάντα το λειτουργικό σας σύστημα με τις τελευταίες ενημερώσεις και τα Service Packs συμπεριλαμβανομένων και όλων των προγραμμάτων που έχετε. Προσπαθείτε όσο το δυνατόν να ενημερώνετε τις εφαρμογές σας με νέες εκδόσεις και τα updates τους.
3. Να τρέχετε το πρόγραμμα για την προστασία από ιούς τουλάχιστον μια φορά την εβδομάδα. Αν ο υπολογιστής σας είναι συνέχεια ανοικτός μμπορείτε να το κάνετε και κάθε μέρα στον κενό χρόνο που δεν εργάζεστε στον υπολογιστή σας
4. Καλό θα είναι να προμηθευτείτε εκτός από κάποιο πρόγραμμα για ιούς και προγράμματα για τον εντοπισμό spyware/adware.
5. Ενεργοποιήστε στον browser που χρησιμοποιείται το μμπλοκάρισα των παραθύρων popup
6. .Ποτέ μην ανοίγετε e-mails που σας φαίνονται ύποπτα ή σας είναι άγνωστα.
7. Όταν χρησιμοποιείτε προγράμματα Instant Messaging *(MSN Messenger, ICQ κλπ.)* να είστε ιδιαίτερα προσεκτικοί όταν σας στέλνουν αρχεία απευθείας μέσα από το πρόγραμμα. Καλό θα ήταν να απενεργοποιήσετε αυτή την δυνατότητα. Αν κάποιος θέλει να σας στείλει αρχείο μπορεί να το κάνει μέσω e-mail. Σχεδόν όλες οι δημοφιλείς υπηρεσίες παροχής e-mail όπως το Gmail, ελέγχουν τα ηλεκτρονικά μηνύματα για ιούς.

8. Να είστε πολύ προσεκτικοί όταν κατεβάζετε προγράμματα από το Internet και να βλέπετε πάντα τις οδηγίες πριν κατεβάσετε κάτι.
9. Να προσέχετε ιδιαίτερα τα αρχεία που αντιγράφετε στον υπολογιστή σας από δισκέτες, USB keys, DVD, CD-ROM ή άλλα αποσπώμενα μέσα
10. Τρέχετε το πρόγραμμα σε τακτική βάση καθώς και τα εργαλεία καθαριότητας που σας παρέχουν τα Windows.

ΒΙΒΛΙΟΓΡΑΦΙΑ

Κεφάλαιο 2

http://gr.norton.com/7-tips-to-protect-against-phishing/article

http://el.wikipedia.org/wiki/%CE%99%CF%8C%CF%82_%CF%85%CF%80%CE%BF%CE%BB%CE%BF%CE%B3%CE%B9%CF%83%CF%84%CE%AE

http://dide.flo.sch.gr/Plinet/Tutorials/Tutorials-Viruses.html

http://computer.howstuffworks.com/virus4.htm

http://el.wikipedia.org/wiki/%CE%94%CE%BF%CF%8D%CF%81%CE%B5%CE%B9%CE%BF%CF%82_%CE%8A%CF%80%CF%80%CE%BF%CF%82_(%CF%85%CF%80%CE%BF%CE%BB%CE%BF%CE%B3%CE%B9%CF%83%CF%84%CE%AD%CF%82)

http://el.wikipedia.org/wiki/Spoofing

http://el.wikipedia.org/wiki/Phishing

Κεφάλαιο 3

https://sites.google.com/site/ilektronikoegklima/home/eide-epitheseon

http://www.isee.gr/issues/04/insert/index.html

https://sites.google.com/site/ilektronikoegklima/home/eide-epitheseon#_ftn2

http://el.wikipedia.org/wiki/%CE%91%CF%83%CF%86%CE%AC%CE%BB%CE%B5%CE%B9%CE%B1_%CE%B4%CE%B9%CE%BA%CF%84%CF%8D%CF%89%CE%BD_%CF%85%CF%80%CE%BF%CE%BB%CE%BF%CE%B3%CE%B9%CF%83%CF%84%CF%8E%CE%BD

http://www.pi.ac.cy/InternetSafety/kindinoi_akatalperiex.html

Κεφάλαιο 4

http://www.onalert.gr/stories/h-istoria-twn-epithesewn-ston-kybernoxwro-me-xronologio/29368

http://el.wikipedia.org/wiki/Melissa_virus

http://12dim-petroup.att.sch.gr/autosch/joomla15/index.php?option=com_content&view=article&id=113:viruses&catid=96:2012-03-08-15-26-00&Itemid=76

http://en.wikipedia.org/wiki/ILOVEYOU

http://translate.google.gr/translate?hl=el&sl=en&u=http://en.wikipedia.org/wiki/Sircam&prev=search

http://translate.google.gr/translate?hl=el&sl=en&u=http://encyclopedia2.thefreedictionary.com/Nimda%2B%28computer%2Bworm%29&prev=search

http://translate.google.gr/translate?hl=el&sl=en&u=http://en.wikipedia.org/wiki/Code_Red_%28computer_worm%29&prev=search

http://translate.google.gr/translate?hl=el&sl=en&u=http://itlaw.wikia.com/wiki/Slammer_worm&prev=search

κεφάλαιο 5

http://users.teilam.gr/~klimn/cryptography/Lab/Lec1.pdf

http://el.wikipedia.org/wiki/%CE%9A%CF%81%CF%85%CF%80%CF%84%CE%BF%CE%B3%CF%81%CE%B1%CF%86%CE%AF%CE%B1

http://el.wikipedia.org/wiki/%CE%9A%CF%81%CF%85%CF%80%CF%84%CE%BF%CE%B3%CF%81%CE%AC%CF%86%CE%B7%CF%83%CE%B7_%CE%A3%CF%85%CE%BC%CE%BC%CE%B5%CF%84%CF%81%CE%B9%CE%BA%CE%BF%CF%8D_%CE%9A%CE%BB%CE%B5%CE%B9%CE%B4%CE%B9%CE%BF%CF%8D

http://el.wikipedia.org/wiki/%CE%9A%CF%81%CF%85%CF%80%CF%84%CE%BF%CE%B3%CF%81%CE%AC%CF%86%CE%B7%CF%83%CE%B7_%CE%94%CE%B7%CE%BC%CF%8C%CF%83%CE%B9%CE%BF%CF%85_%CE%9A%CE%BB%CE%B5%CE%B9%CE%B4%CE%B9%CE%BF%CF%8D

κεφάλαιο 6

http://el.wikipedia.org/wiki/SSL

http://en.wikipedia.org/wiki/Dictionary_attack

http://en.wikipedia.org/wiki/Replay_attack

http://el.wikipedia.org/wiki/%CE%95%CF%80%CE%AF%CE%B8%CE%B5%CF%83%CE%B7_man-in-the-middle

http://www.islab.demokritos.gr/gr/html/ptixiakes/kostas-aris_ptyxiakh/Phtml/kefalaio5.htm

κεφάλαιο 7

http://el.wikipedia.org/wiki/%CE%A3%CF%8D%CF%83%CF%84%CE%B7%CE%BC%CE%B1_%CE%91%CE%BD%CE%AF%CF%87%CE%BD%CE%B5%CF%85%CF%83%CE%B7%CF%82_%CE%95%CE%B9%CF%83%CE%B2%CE%BF%CE%BB%CE%AE%CF%82

http://pacific.jour.auth.gr/virus/page_9.htm

http://di.ionio.gr/~emagos/security/Simeioseis-Asfaleia%20Part%20B.pdf

http://lyk-vatheos.eyv.sch.gr/ProjectFiles/Pro2011-2012/AsfaleiaDiadiktyo.pdf