ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΑΤΡΩΝ

ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΗΛΕΚΤΡΟΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ & ΠΛΗΡΟΦΟΡΙΚΗΣ

ΕΡΓΑΣΙΑ ΕΞΑΜΗΝΟΥ

ΓΙΑ ΤΟ ΜΑΘΗΜΑ

<ΔΙΚΤΥΑ ΔΗΜΟΣΙΑΣ ΧΡΗΣΗΣ>

<ΑΣΦΑΛΕΙΑ ΣΤΟ ΙΝΤΕΡΝΕΤ>

<ΓΑΤΟΥ ΜΑΡΙΑ>

Α.Μ <4967>

ΔΙΔΑΣΚΩΝ: ΧΡΗΣΤΟΣ ΜΠΟΥΡΑΣ

ΠΑΤΡΑ 2015

Πίνακας περιεχομένων

Ακρωνυμια

Εισαγωγή

Σήμερα θα μπορούσε να πει κανείς ότι ανήκουμε στην κοινωνία του διαδικτύου. Το διαδίκτυο αποτελεί σήμερα την καθημερινή αναφορά εκατομυρίων ανθρώπων και μια πραγματικότητα, η οποία μας μας περιβάλλει από παντού, γεμίζοντάς μας πληροφορίες. Ο εικονικός κόσμος του διαδικτύο ουσιαστικά καταργεί το χώρο και το χρόνο, είναι πάντα διαθέσιμο δημιουργώντας ένα σύμπαν διαφορετικό Έτσι το Διαδίκτυο πλέον ανοίγει μια ουσιαστική συζήτηση με ολόκληρη την κοινωνία αφού οι συνέπειες της εφαρμογής του γίνονται αισθητές σε όλα τα πεδία της ζωής όπως στην επαγγελματική ενασχόληση του καθενός, στην αναψυχή, στις οικογενειακές σχέσεις, στην ψυχολογική συμπεριφορά των ανθρώπων, στην πολιτική, στο τρόπο διάθρωσης του εμπορίου, στην εκπαίδευση κ.α. Η παροχή τόσο άφθονων πληροφοριών, καταργεί τα γεωγραφικά σύνορα, ενώνει τις εμπειρίες των ανθρώπων και οδηγεί σε μια αναπόφεκτη παγκοσμιοποίηση

Έτσι το Διαδίκτυο είναι σήμερα το καθημερινό εργαλείο στη ζωή μας: για την αναζήτηση πληροφοριών, επικοινωνία, αγορές, για ψυχαγωγία. Μάλιστα σήμερα από μικρή ηλικία τα παιδιά έχουν πρόσβαση σε αυτό και το θεωρούν μια από τις πιο αγαπημένες τους δραστηριότητες. Μάλιστα έρευνα έδειξε ότι τα παιδιά στην πλειοψηφία τους χρησιμοποιούν το Διαδίκτυο αρκετές φορές την ημέρα, ενώ η χρήση του Διαδικτύου και των κινητών έξυπνων συσκευών θεωρείτε αυτονόητη σε όλους τους νέους του κόσμου. Γενικά έχει αποδειχθεί ότι οι νέοι γνωρίζουν τις προκλήσεις κατά την χρηση τους στο Διαδίκτυο, παρόλα αυτά όταν αντιμετωπίσουν πρόβλημα, οι ανήλικοι απευθύνονται στους μεγαλύτερους μόνο ως τελευταία λύση.

Ο λόγος που εκατομύρια άνθρωποι καθημερινά κάνουν χρήση του διαδικτύου είναι ότι προσφέρει τεράστιες δυνατότητες και δίνει την δυνατότητα σε άπειρες εφαρμογές. Η αποτελεσματική όμως αξιοποίησή του, όμως, προϋποθέτει την ορθή χρήση του. Έτσι σε παγκόσμια κλίμακα έχουν αναπτυχθεί δράσεις και προγράμματα που στοχεύουν στη δημιουργία ασφαλέστερων συνθηκών αξιοποίησης των δυνατοτήτων του Διαδικτύου.

Το θέμα της ασφαλούς χρήσης του Διαδικτύου απασχολεί πλέον έντονα την παγκόσμια κοινότητα εξετάζοντας και προτείνοντας εκπαίδευση στη διαχείριση των

κινδύνων που αντιμετωπίζουν οι χρήστες, είτε αυτοί οι κίνδυνοι αφορούν στην καθημερινή φυσική τους ζωή είτε στη χρήση του Διαδικτύου προς αναζήτηση πληροφοριών, κοινωνικής δραστηριότητας ή απλώς ανταλλαγής υλικού. Αποτελεί μάλιστα βασική προτεραιότητα τόσο των επιστημονικών όσο και κοινωνικών δομών κάθε χώρας.

Έτσι η ασφάλεια των δικτύων επικοινωνίας χρηστών έχει πλέον αναδειχθεί σε ένα σημαντικό και άκρως ενδιαφέρων κομμάτι της σύγχρονης τεχνολογίας των επικοινωνιών. Η καθολικότητα του παγκοσμίου ιστού και η χρήση του σε κάθε δραστηριότητα της καθημερινότητας, επιχειρήσεις και ιδιώτες ορίζει πλέον την αναγκαιότητα της ασφαλούς περιήγησης. Έτσι ορίζονται κανόνες ασφάλειας όπου αν δεν τηρούνται οι χρήστες εκτίθονται σε γνωστούς και επιβλαβείς κινδύνους όπως Spam, ιούς και κλοπή προσωπικών δεδομένων. Η ασφάλεια των δικτύων και των διακινούμενων πληροφοριών αποτελεί παρόλα αυτά ένα αρκετά πολύπλοκο θέμα. Ο λόγος είναι ότι η ασφάλεια αφορά διαφορετικές δράσεις σε διαφορετικές κατηγορίες χρηστών, αφού μπορεί να αποτελεί απλά τη δυνατότητα μιας ανώνυμης περιήγησης στον παγκόσμιο ιστό, την ασφάλεια εκτέλεσης χρηματοοικονομικών συναλλαγών, την εύρυθμης λειτουργίας μιας ιστοσελίδας, την προστασία ενός εταιρικού δικτύου, την προστασία ιδιωτικών αρχείων.

Δυστυχώς υπάρχουν αρκετά προβλήματα ασφαλείας επηρεάσουν τους εξυπηρετητές δικτύου (web servers) και τα τοπικά δίκτυα που αυτοί φιλοξενούνται. Επίσης υπάρχουν σοβαρά προβλήματα ακόμα και στους απλούς περιηγητές δικτύου (web browsers) των απλών χρηστών. Μάλιστα στις εταιρίες η εγκατάστασή ενός web server για την προβολή μιας ιστοσελίδα ουσιαστικά ορίζει και ένα παράθυρο πρόσβασης από τους χρήστες του ίντερνετ στο τοπικό δίκτυο της εταιρίας, κάτι το οποίο μπορεί να οδηγήσει σε μία πληθώρα προβλημάτων. Τα προβλήματα αυτά διευρύνονται από την απλή τροποποίηση της ιστοσελίδας ως και την κλοπή προσωπικών δεδομένων των χρηστών της εταιρίας, ή για την απόκτηση πρόσβασης σε θέσεις για τοποθέτηση νέων ξένων αρχείων στο τοπικό δικτύου.

Όμως πέρα των εξειδικευμένων δομών και χρηστών και ο απλός χρήστης ,όμως, καλείται να αντιμετωπίσει πολλά θέματα ασφαλείας. Η περιήγηση στο διαδίκτυο για ένα απλό χρήστη ενώ φαίνεται αρχικά ασφαλής και ανώνυμη, κάτι δεν ισχύει. Αυτό γιατί περιεχόμενα που είναι ενσωματωμένα στις ιστοσελίδες όπως Active X , Java applets, άλλα scripts εισάγουν πιθανότητα διείσδυσης ιών και άλλων

επιβλαβών προγραμμάτων σε τελικές συσκευές όπως ο υπολογιστής, το tablet, ή το κινητό του χρήστη. Επίσης η πράξη της περιήγησης αφήνει ηλεκτρονικές καταγραφές περιήγησης του χρήστη, κάτι το οποίο μπορεί να οδηγήσει στην κατασκευή και κατασκευή ενός προφίλ του χρήστη που πιθανά να χρησιμοποιηθεί από τρίτους γνωρίζοντας πλέον τα ενδιαφέροντα και τις συνήθειες του χρήστη.

Σήμερα δε με την χρήση και των κοινωνικών δικτύων εισαγόμαστε σ' ένα είδος παγκοσμίου και πολύμοφού διαλόγου, που δεν διακρίνεται από όρια ή περιορισμούς, παρά μόνο σε αυτούς που οι ίδιοι οι χρήστες επιβάλλουν στους εαυτούς τους. Σήμερα ο χρήστης δαπανά ένα μεγάλο μέρος του χρόνου του σε ομαδικές συσκέψεις, συζητήσεις και φόρουμ γύρω από κάθε είδους θέματα. Η δράση αυτή γίνεται σήμερα επώνυμα, ανώνυμα ή με χρήση ψευδονύμων ή πλαστών λογαριασμών και αυτή η πιθανή ανωνυμία κάνει πολλούς από τους χρήστες του να συμπεριφέρονται όπως οι ραδιοπειρατές και να κυκλοφορούν στον κυβερνοχώρο σε αναζήτηση μακρινών και άγνωστων συνομιλητών, που τους προτείνουν από ερωτικά ραντεβού ως δοκιμές κρασιών, περνώντας από την πρόσβαση σε κυβερνητικές βιβλιοθήκες, σε τραγούδια ή σε αρχεία Πανεπιστημίων. Έτσι δημιουργείται η ανατριχιαστική δυνατότητα καταστροφής της προσωπικής ζωής κατά τρόπο ανεπίστρεπτο, με αρκετές κοινωνικές και ψυχολογικές επιπλοκές.

ΚΕΦΑΛΑΙΟ 1: ΕΙΣΒΟΛΕΙΣ ΚΑΙ ΕΠΙΘΕΣΕΙΣ

1.1 Εισβολείς

Οι επιθέσεις που γίνονται στα διάφορα υπολογιστικά συστήματα δεν είναι τυχαίες αφού συνήθως το άτομο που τις διαπράττει πιστεύει και στόχο έχει να κερδίσει κάτι από το δίκτυο που επιτίθεται, υποκλέπτοντας τα δεδομένα. Έτσι το πρώτο βήμα που μπορεί να κάνει κάποιος για να προστατευθεί είναι να προσδιορίσει ποιος θα μπορούσε να έχει όφελος από την υποκλοπή ή την παρενόχληση των πόρων του συστήματος του.

Οι εισβολείς συνήθως αναφέρονται σαν "εισβολέας" (attacker), χάκερ (HACKER) ή κράκερ (cracker) και μάλιστα οι παραπάνω έννοιες χρησιμοποιούνται συνήθως με ταυτόσημη σημασία. Παρόλα αυτά οι όροι αυτοί έχουν διαφορετική σημασία.

Σαν Εισβολέας ορίζεται κάποιος ο οποίος αναζητά τρόπους για να κλέψει ή να καταστρέψει τα υπολογιστικά συστήματα που επιτίθεται . Ο εισβολέας μπορεί να έχει υψηλό επίπεδο τεχνικών ή προγραμματιστικών γνώσεων, ή να είναι απλώς ερασιτέχνης που με χρήση εργαλειών που κυκλοφορούν στο διαδίκτυο επιτήθεται στα υπολογιστικά συστήματα. Ο εισβολέας μπορεί να παρομοιάστει με έναν κατάσκοπο, ένα κλέφτη, ή έναν κοινό ληστή.

Σαν χάκερ (hacker) είναι αυτός που πρακτικά ανακαλύπτει τις αδυναμίες ενός συστήματος και μπορεί να τις χρησιμοποιήσει για θετικό ή αρνητικό λόγο. Μάλιστα η αρχική σημασία της λέξης hacker ήταν θετική. Σαν χάκερ χαρακτηρίζοταν κάποιος ο οποίος είχε αρκετές γνώσεις πάνω σε υπολογιστές και δίκτυα. Το χαρακτηριστικό των hacker είναι ότι δεν αρκούνται στην απλή εκτέλεση ενός προγράμματος·με στόχο μια πιθανή πρόσβαση σε ένα σύστημα αλλά στοχεύουν στο γνωρίσουν τα πάντα για τον τρόπο λειτουργίας του ακόμη και την παραμικρή λεπτομέρεια ώστε πλέον να

μπορούν πιθανά να το ελέγξουν πλήρως. Η τέχνη των χάκερ μπορεί να είναι είτε θετική, είτε αρνητική, ανάλογα με το ποια είναι τα κίνητρα των hackers. Για να καταλάβουμε την δράση ενός hacker ας υποθέσουμε ότι ένας κατασκευαστής ισχυρίζεται ότι το προϊόν του είναι 100% ασφαλές. Ένας hacker μπορεί να εκλάβει την δήλωση αυτή σαν πρόκληση την οποία πρέπει οπωσδήποτε να αντιμετωπίσει και να βρει τελικά πρόσβαση ή να αποδείξει ότι η δήλωση του κατασκευαστή είναι ψευδής. Το τι ακριβώς θα κάνει ο hacker με πληροφορίες που θα αποκαλύψει είναι αυτό που καθορίζει σε ποια πλευρά θα καταταχθεί στους "καλούς" ή στους "κακούς" hackers.

Ουσιαστικά αρχικά ο hacker βρίσκει έναν τρόπο για να εκμεταλλευτεί μία "ρωγμή" στην ασφάλεια ενός προγράμματος και την δημοσιοποιεί, αντί να προσπαθήσει να την εκμεταλλευτεί με στόχο ιδίου όφελους, θεωρείται αυτό που λέμε «λευκός» hacker. Αν όμως ένας hacker εντοπίσει μία ρωγμή στην ασφάλεια ενός προγράμματος και τελικά θα χρησιμοποιήσει έναντι ανυποψίαστων θυμάτων για προσωπικό όφελος, τότε λέμε ότι είναι «μαύρος» hacker. Το «γκρι» hacker δίνεται στους χάκερ οι «λευκοί» hacker που εξελίσονται σε «μαύρους», δηλαδή οι hacker οι οποίοι απασχολούνται νόμιμα σαν σύμβουλοι ασφάλειας αλλά ταυτόχρονα αναπτύσσουν παράνομη δραστηριότητα στον ελεύθερο χρόνο τους.

Πολλοί από τους «λευκούς» hacker δημοσιεύουν τις αδυναμίες των συστημάτων σε blogs ή άλλες σελίδες με τεχνικό περιεχόμενο. Μάλιστα πολλοί παρεξηγούν τα κίνητρα αυτών που δημοσιεύουν τις λεπτομέρειες σφαλμάτων (bugs) λογισμικού. Συνήθως ο στόχος αυτών των δημοσιεύσεων δεν είναι για την εκπαίδευση άλλων εισβολέων αλλά η κοινοποίηση των αδυναμιών ενός υπολογιστικού συστήματος ή λογισμικού με στόχο την βελτιστοποίηση του από τους κατασκευαστές και τους επόπτες συστημάτων. Πολλές φορές, η δημόσια κοινοποίηση ενός τρωτού σημείου γίνεται από απλή ενόχληση ή από αναγκαιότητα.

Μάλιστα πολλές φορές πιστεύεται ότι όταν κάποιος βρίσκει ένα πρόβλημα σχετιζόμενο με την ασφάλεια ενός συστήματος και το αναφέρει στο ευρύ κοινό, θεωρείται ότι αυτός που το αναφέρει είναι ένας εισβολέας ο οποίος εκμεταλλεύεται το πρόβλημα για προσωπικό όφελος. Ωστόσο, αυτή η τακτική αποτελεί ορθή τακτική. Δηλαδή το να κοινοποιούνται και να συζητιούνται ανοικτά τα σχετιζόμενα με την ασφάλεια προβλήματα οδηγεί στην ανάπτυξη πιο εύρωστου λογισμικού, με υψηλότερο βαθμό ακεραιότητας.

Ο cracker είναι αυτός που ουσιαστικά «σπάει» το λογισμικό δηλαδή βρίσκει τρόπους να χρησιμοποιεί παράνομα ένα λογισμικό παραβιάζοντας τους κανόνες δικαιωμάτων χρήσης. Επίσης ο cracker στο διαδίκτυο είναι αυτός που παραβιάζει με την εξεύρεση username – passwords την πρόσβαση στα συστήματα με πολύ επικίνδυνες συνέπειες.

1.2 Κίνητρα Επίθεσης

Όπως αναφέραμε για να μπορέσουμε να προστατεύσουμε τα υπολογιστηκά μας συστήματα είναι σημαντικό να ξέρουμε τα κίνητρα των επιθέσεων. Έτσι έχουμε το παρακάτω ερώτημα: Ποιο λοιπόν είναι το κίνητρο να εξαπολύσει κάποιος μία επίθεση εναντίον ενός δικτύου; Παρακάτω παραθέτουμε τις ποιο πιθανές περιπτώσεις επιθέσεων

Επιθέσεις εκ των Εσω

Η συντριπτική πλειοψηφία των περιπτώσεων επιθέσεων είναι οι επιθέσεις που δέχονται οργανισμοί και προέρχονται εκ των έσω. Δηλαδή από άτομα του ίδου οργανισμού. Στην πραγματικότητα, ορισμένες μελέτες ισχυρίζονται ότι έως και το 70% όλων των επιθέσεων που δέχονται τα υπολογιστικά συστήματα οργανισμών προέρχονται από κάποιον εντός του οργανισμού, ή από κάποιον ο οποίος μπορεί να έχει πληροφόρηση εκ των έσω (δηλαδή πρώην υπάλληλους ή διαχειριστών των οργανισμών).

Κάθε οργανισμός αναπτύσει εργαλεία για την προστασία των δικτύων από εξωτερικές επιθέσεις και μάλιστα συνήθως γίνεται ιδιαίτερη προσπάθεια πάνω σε αυτό με χρήση firewall ή antivirus, ακόμη και σήμερα οι ίδιοι οι υπάλληλοι των εταιριών είναι υπεύθυνοι για τις μεγαλύτερες καταστροφές που μπορούν να υποστούν τα δεδομένα ενός οργανισμού. Τέτοιου είδους καταστροφές μπορεί να είναι τυχαίες από απλά τυχαία λάθη κακής χρήσης ή σε πολλές περιπτώσεις, σκόπιμες.

Η πιο συνηθέστερη αιτία επίθεσης συνήθως είναι ένας δυσαρεστημένος υπάλληλος ή πρώην υπάλληλος που διατηρεί πρόσβαση στο δίκτυο. Παρόλο που οι περισσότεροι επόπτες-διαχειριστές συστημάτων καταβάλλουν προσπάθειες για να προστατέψουν το δίκτυο του οργανισμού από τις εξωτερικές επιθέσεις, συχνά παραβλέπουν την πολύ μεγαλύτερη απειλή των εσωτερικών επιθέσεων. Έτσι ένα άτομο δεν χρειάζεται να είναι χαρακτηρισμένος εισβολέας για να μπορεί να κάνει ζημιά στους πόρους μιας εταιρείας.

Συνήθως η μεγαλύτερη απειλή που συμβαίνει με επιθέσεις εκ των έσω με ανησυχητική συχνότητα είναι η καταστροφή των δεδομένων και η κλοπή τους. Αυτό αναφέρεται συνήθως με τον όρο «βιομηχανική κατασκοπεία» και αν και δεν θεωρείται τόσο κοινό όσο η καταστροφή των δεδομένων, αποτελεί μία υπαρκτή απειλή για οποιονδήποτε οργανισμό. Αυτό γιατί ενώ διατηρεί «εμπιστευτικά» δεδομένα η υποκλοπή αυτών των δεδομένων θα μπορούσε να αφήσει τον οργανισμό νομικά υπεύθυνο ή να του προξενήσει πρόβλημα ανταγωνιστικότητας. Τα δεδομένα αυτά συνήθως κλέπτονται από χρήστες του ίδιου του οργανισμού.

Εξωτερικές Επιθέσεις

Οι εξωτερικές επιθέσεις προέρχονται από πολλές και διαφορετικές πηγές. Αν και μπορούν επίσης να προέρχονται από δυσαρεστημένους υπαλλήλους, η γκάμα των πιθανών εισβολέων που μπορούν να εκκινήσουν μία εξωτερική επίθεση είναι πολύ μεγαλύτερη. Το μόνο κοινό στοιχείο είναι ότι συνήθως κάποιος έχει να κερδίσει κάτι κάνοντας μία τέτοια επίθεση.

Ανταγωνιστές

Στον τομέα των επιχειρήσεων που υπάρχει μεγάλος ανταγωνισμός, ένας φιλόδοξος ανταγωνιστής σας μπορεί να διαβλέψει πιθανό όφελος κάνοντας μία επίθεση στο δίκτυο μιας επιχείρησης. Στόχος μίας τέτοιας επίθεσης είναι η κλοπής των πρωτότυπων κατασκευαστικών σχεδίων ενός νέου προϊόντος, οικονομικών στοιχείων της εταιρείας.η ακόμα και να καταστήσει άχρηστους τους πόρους του δικτύου του ανταγωνισμού, ώστε να σας προκαλέσει οικονομική ζημιά (διαφυγόντα κέρδη) στον ανταγωνισμό.

Έτσι το όφελος από την κλοπή σχεδίων ενός νέου προϊόντος είναι προφανές αφού τέτοιες πληροφορίες, ο "κλέφτης" μπορεί να χρησιμοποιήσει τις πληροφορίες αυτές για να μειώσει τον χρόνο ανάπτυξης του δικού του ανταγωνιστικού προϊόντος, ή για να βελτιωθεί με περισσότερες και καλύτερες λειτουργίες. Επίσης εάν ο ανταγωνισμός γνωρίζει ποια προϊόντα σκοπεύει να κυκλοφορήσει στο εγγύς μέλλον, ένας άλλος ανταγωνιστής μπορεί να προλάβει και να παρουσιάσει πρώτος στην αγορά ένα νέο αντίστοιχο ελκυστικό προϊόν.

Η κλοπή οικονομικών στοιχείων είναι εξίσου ζημειογώνα αφού τέτοια δεδομένα π.χ. του προηγούμενου οικονομικού έτους μιας εταιρείας, ένας ανταγωνιστής σας θα μπορούσε να αποκτήσει σαφές "πλεονέκτημα" στην αγοράς. Το

πλεονέκτημα που απορρέει από την γνώση τέτοιων στοιχείων είναι η γνώση οικονομικής ευρωστίας της εταιρείας του ανταγωνισμού (ή της έλλειψης της) και κυρίων των πηγών από τις οποίες προέρχονται τα έσοδα της εταιρείας.

Διαφορετικές Απόψεις

Η άλλη κατηγορία επιθέσεων είναι αυτή που οδηγεί έναν hacker να επιτεθεί στα συστήματα ενός οργανισμού ή δικτύου με στόχο να πλήξει ή να δημιουργήσει πρόβλημα λόγω διαφορετικών απόψεων που πιθανά υπάρχουν. Στην περίπτωση αυτή έχουμε τους λεγόμενους "hacktivists" δηλαδή hacker και activist όπως προκύπτει η λέξη, δηλαδή άτομα τα οποία επιτίθενται σε συστήματα με στόχο την διακοπή της παροχής υπηρεσιών, την δυσφήμιση των συγκεκριμένων Web sites και γενικότερα την προσέλκυση της προσοχής του κοινού στα δικά τους πιστεύω. Στόχος των επιθέσεων αυτών είναι καθαρά οι πολιτικοί – θρησκευτικοί ή στρατιωτικοί στόχοι, μεταφέροντας τις συγκρούσεις ιδεών από τον πραγματικό κόσμο στον κυβερνοχώρο.

Υψηλό Προφίλ

Οι επιθέσεις αυτές έχουν στόχο οργανισμούς οι οποίοι είναι ευρέως γνωστοί ή έρχονται πολύ συχνά στην δημοσιότητα. Οι επιθέσεις συμβαίνουν απλά και μόνο λόγω της δημοσιότητας που απολαμβάνουν οι φορείς αυτοί (π.χ. η εταιρία Micorosoft αποτελεί ένα τέτοιο στόχο). Ένας εισβολέας επιχειρεί να επιτεθεί σε ένα γνωστό site, ελπίζοντας ότι μια τυχόν επιτυχημένη επίθεση του θα του αποφέρει τα χρήματα αλλά κυρίων δημοσιότητα.

Ηλεκτρονικό Ταχυδρομείο

Μία πολύ συχνή μορφή επίθεσης είναι η χρήση του συστήματος ηλεκτρονικού ταχυδρομείου του οργανισμού σας σαν αναμεταδότη spam. Μάλιστα αποτελεί πολύ συχνό φενόμενο και αποτελεί έναν από τους πιο επικίνδυνους τρόπους επίθεσης σε ένα δίκτυο. Ο όρος “spam” χαρακτηρίζει την αποστολή ανεπιθύμητων μηνυμάτων e-mail (διαφημίσεις, σχήματα πυραμίδας, κ.α.) με μαζικό τρόπο σε άλλους. Οι spammers δηλαδή αυτοί που ασχολούνται με την δημιουργία span ελπίζουν ότι ο τεράστιος όγκος των διαφημίσεων που στέλνουν θα παράγει κάποιο ενδιαφέρον για το προϊόν ή την υπηρεσία που διαφημίζουν. Συνήθως, όταν ένας spammer στέλνει μια

διαφήμιση, αυτή φτάνει σε δεκάδες χιλιάδες διευθύνσεις ηλεκτρονικού ταχυδρομείου και ταχυδρομικές λίστες.

Τα μηνύματα spam συνήθως χρησιμοποιούν της επαφές από το δικό μας e-mail και ταυτόχρονα το σύστημα email που υπάρχει στο δίκτυο του χρήστη και έτσι το σύστημα email γίνεται ο κόμβος από τον οποίο αποστέλλονται όλα αυτά τα μηνύματα σε νέους παραλήπτες οι οποίοι κι αυτοί στην συνέχεια εξελίσουν το σύστημα τους σε spam μεταδότη. Το αποτέλεσμα είναι μία κατάσταση άρνησης εξυπηρέτησης από το δίκτυο αφού τα μαζικά μηνύματα εξαντλούν τους πόρους του δικτύου.

Αυτό γιατί κατά την διάρκεια που ο server ηλεκτρονικού ταχυδρομείου ξοδεύει τον χρόνο του για την διεκπεραίωση του spam, δεν μπορεί να χειριστεί την εισερχόμενη και εξερχόμενη ηλεκτρονική αλληλογραφία των πραγματικών email. Τα περισσότερα σύγχρονα συοτήματα ηλεκτρονικού ταχυδρομείου περιλαμβάνουν πλέον ειδικές ρυθμίσεις για την καταπολέμηση του spam που περιορίζουν την εξάπλωσή τους

Τέτοιες ρυθμίσεις ουσιαστικά εμποδίσουν τα μηνύματα spam να φτάσουν μέχρι την θυρίδα του χρήστη και εμποδίζουν την χρήση του συστήματος email να γίνει αναμεταδότης spam. Μία τέτοια ρύθμιση είναι π.χ. ένας κανόνας που να κάνει δεκτά μόνο τα μηνύματα που προορίζονται για, ή προέρχονται από, συγκεκριμένα domain. Για το λόγο αυτό μία άμυνα των spammers είναι να προτιμούν να χρησιμοποιούν και το δικό τους σύστημα email. Παρόλα αυτά ένας τυπικός spammer προσπαθεί να κρύψει την πραγματική διεύθυνση αποστολέα·έτσι ώστε οποιοσδήποτε προσπαθήσει να τον εντοπίσει να υποθέσει ότι το ανεπιθύμητο μήνυμα προήλθε από άλλο χρήστη δίκτυο.

1.3. Ποιότητα και Ποσότητα Ασφάλειας

Για να παρθούν κατάλληλες αποφάσεις για το ποιος είναι ο καλύτερος τρόπος για να ασφαλίστεί το δίκτυο, θα πρέπει να προσδιοριστεί το επίπεδο της προστασίας που θέλουμε να επιτύχουμε. Συγκεκριμένα, θα πρέπει να γινει ανάλυση του δίκτυο ώστε να εξακριβωθεί το επίπεδο "οχύρωσης" που χρειάζεται.

Η ανάλυστη αυτή οδηγεί στο να χρησιμοποιηθούν οι εξαγόμενες πληροφορίες ώστε να αναπτυχθεί μια πολιτική ασφάλειας για το δίκτυο. Έτσι με την σωστή ανάλυση και την γνώση που προκύπτει είμαστε σε θέση για ν' αρχίσουμε να λαμβάνουμε τις σωστές και εφικτές αποφάσεις σχετικά με την δομή της ασφάλειας που πρέπει να χρησιμοποιηθεί στο δικτύου.

Ανάλυση κινδύνων

Η Ανάλυση κινδύνων (risk analysis) αποτελεί την διαδικασία προσδιορισμού των πόρων που χρειάζονται ώστε να προστατευθεί το δίκτυο από πιθανές απειλές από τις οποίες μπορεί να κινδυνεύουν οι λειτουργία ή τα δεδομένα του δικτύου. Η διεξαγωγή μίας τέτοιας ανάλυσης κινδύνων με ακρίβεια και σαφήνεια είναι ένα βήμα ζωτικής σημασίας για την εξασφάληση της ασφάλειας του περιβάλλοντος του δικτύου σας.

Ποιοί όμως πόροι πρεπει να προστατευθούν στο δίκτυο ;

Η αποτελεσματική ανάλυση κινδύνων πάντα ξεκινά με το παραπάνω ερώτημα που τελικά οδηγεί στον προσδιορισμό των πόρων του συστήματος του οργανισμού σας ουσιαστικά θέλουμε να προστατέψουμε.

Οι πόροι αυτοί συνήθως είναι κάποιοι από τις ακόλουθες τέσσερις κατηγορίες:

- Φυσικοί πόροι
- Πνευματικοί πόροι
- Σχετιζόμενοι με τον χρόνο πόροι
- Πόροι που σχετίζονται με την αντίληψη των άλλων για τον οργανισμό

Φυσικοί πόροι

Οι φυσικοί πόροι είναι όλοι οι πόροι που έχουν οτιδήποτε φυσική μορφή. Σ' αυτή την κατηγορία περιλαμβάνονται οι σταθμοί εργασίας του δικτύου, οι servers, τα τερματικά, τα switch και hub του δικτύου καθώς και οι υπόλοιπες περιφερειακές συσκευές. Φυσικά οποιοσδήποτε υπολογιστικός πόρος έχει φυσική μορφή και ουσιαστικά μπορεί να θεωρηθεί φυσικός πόρος..

Στη περίπτωση αυτή τελικός στόχος της ανάλυσης κινδύνων είναι η κατάστρωση αποτελεσματικών τρόπος που σε σχέση με το κόστος του πλάνου τελικά θα καταλήγει στη διαφύλαξη των φυσικών πόρων του συστήματαος. Κατά την πορεία της ανάλυσης θα πρέπει να λαμβάνονται υπόψη οι προφανείς τομείς προβλημάτων που πιθανά προκύπτουν από την επίθεση και βλάβη ενός φυσικού πόρου καθώς και τις αντίστοιχες άμεσες λύσεις σε μία τέτοια περίπτωση.

Πνευματικοί πόροι

Οι πνευματικοί πόροι είναι σαφώς πιο δύσκολο να προσδιοριστούν από τους φυσικούς πόρους. Ο λόγος είναι γιατί συνήθως υπάρχουν μόνο σε ηλεκτρονική μορφή και πολλές φορές συγχέονται με τους πόρους που δεν ανήκουν πνευματικά σε χρήστες του ιδίου δικτύου αλλά είναι πληροφορίες συλλογής. Στην κατηγορία των πνευματικών πόρων συγκαταλέγεται οποιαδήποτε μορφή πληροφορίας που τελικά είναι σημαντική για την λειτουργία του οργανισμού.

Έτσι στη κατηγορία αυτή μπορεί να περιλαμβάνεται λογισμικό, κείμενα, οικονομικά στοιχεία, βάσεις δεδομένων, σχέδια προϊόντων κ.α..

Σχετιζόμενοι με τον χρόνο πόροι

Σημαντικοί πόροι είναι και οι πόροι του χρόνου. Ο χρόνος αποτελεί ένα πολύ σημαντικό τμήμα για οποιονδήποτε οργανισμό ή επιχείρηση, και συνήθως αγνοείται κατά την διεξαγωγή της ανάλυσης κινδύνων. Όταν λοιπόν γίνεται αποτίμηση για το κόστος της απώλειας χρόνου για τον οργανισμό σας, πρέπει να περιλαμβάνετε στην αξιολόγηση των συνεπειών και όλες τις συνέπειες που θα είχε αυτή η απώλεια. Δηλαδή μια επίθεση που τελικά θα καθυστερούσε την ορθή λειτουργία των συστημάτων μας.

Πόροι που σχετίζονται με την αντίληψη των άλλων για τον οργανισμό

Πολλές φορές η αντίληψη των άλλων για την λειτουργία την επιχείρησης καθορίζει τελικά και την επιτυχία της. Π.χ. επιθέσεις που είχανε μεγάλες εταιρίες όπως οι παρακάτω Yahoo, AMAZON, eBay αντιμετώπισαν πτώση της τιμής των μετοχών τους.

Η επιθέσεις που δέχτηκαν παρά το γεγονός ότι οι απώλειες ήταν σχετικά μικρές αλλά και όχι μακροπρόθεσμες, επέφεραν μία υπαρκτή, μετρήσιμη αρνητική επίδραση στην εμπιστοσύνη των καταναλωτών και των μετόχων των εν λόγω εταιριών. Έτσι λόγω της δημοσιότητας που έλαβε η διείσδυση κάποιων χάκερ π.χ. στα συστήματα της Microsoft το 2010, πάρα πολλοί καταναλωτές αναρωτήθηκαν μήπως οι εισβολείς κατάφεραν να κάνουν αλλαγές σε πολύτιμο πηγαίο κώδικα, οι οποίες θα έχουν περάσει απαρατήρητες και τελικά δημιουργήσουν προβλήματα και στα δικά τους συστήματα.

Η Microsoft φυσικά αρνήθηκε οποιαδήποτε ζημιά, απλά και μόνο το γεγονός της παραβίασης των συστημάτων της ήταν αρκετό να πλήξει την αξιοπιστία της και την εμπιστοσύνη των καταναλωτών όχι μόνο στην εταιρεία, αλλά και στα προϊόντα της. Ο κίνδυνος καταστροφής της φήμης ενός οργανισμού ουσιαστικά αποτελεί αιτία σημαντικών δυσχεριών και μη εμπιστοσύνης ειδικά για όλους όσους εργάζονται στον τομέα της ασφάλειας (συμπεριλαμβανομένων των υπηρεσιών επιβολής του νόμου), οι οποίοι βασίζονται στις πληροφορίες και την απειρία των συναδέλφων τους για να σχεδιάσουν καλύτερα συστήματα προστασίας, ή για να κάνουν νομικές ενέργειες.

Μάλιστα το FBI σε μία προσπάθεια να ενθαρρύνει την ελεύθερη ανταλλαγή τεχνικών λεπτομερειών που θα μπορούσαν να χρησιμοποιηθούν για την προστασία από επιθέσεις που δέχονται οι εταιρείες από χάκερ, χωρίς ωστόσο να ζημιώνεται η φήμη τους, δημιούργησε κατάλληλη ομάδα προστασίας των υποδομών και των υπολογιστικών συστημάτων από πιθανές επιθέσεις την Infrastructure Protection and Computer Intrusion Squad, IPCIS, η οποία λειτουργεί σαν ένα ανώνυμο ίδρυμα "συγκέντρωσης τεχνογνωσίας" και συλλέγει πληροφορίες για τις περιπτώσεις αυτές.

Οντότητες που πρέπει να προστατευτούν

Οι πιθανές επιθέσεις σε δίκτυα μπορούν να προέρχονται από οποιαδήποτε πηγή η οποία έχει πρόσβαση σε ένα δίκτυο. Οι πηγές αυτές μπορούν να ποικίλουν σε μεγάλο βαθμό, ανάλογα με το μέγεθος του οργανισμού που αναφερόμαστε και τις υπάρχουσες μορφές πρόσβασης στο δίκτυο.

Έτσι τέτοιες πηγές μπορεί να είναι:

- Εσωτερικά συστήματα
- Πρόσβαση από υποκαταστήματα, θυγατρικές εταιρείες, ή απομακρυσμένα γραφεία

- Πρόσβαση ενός επαγγελματικού συνεργάτη μέσω μιας σύνδεσης WAN
- Πρόσβαση μέσω του Ιnternet
- Πρόσβαση μέσω δεξαμενών μόντεμ (modem pools)

Στη ανάλυση αυτή στόχος δεν είναι ο προσδιορισμός ποιος μπορεί και θέλει να επιτεθεί στο δίκτυο αλλά ποια είναι τα διαθέσιμα μέσα με τα οποία θα μπορούσε κανείς να αποκτήσει πρόσβαση στους πόρους του συστήματος μας. Έτσι όπως έχουμε αναφέρει οι πιθανοί επιτηθέμενοι είναι οι παρακάτω:

• Οι μόνιμοι υπάλληλοι του οργανισμού

• Προσωρινοί υπάλληλοι ή συνεργάτες

• Ανταγωνιστές

• Άτομα με απόψεις ή στόχους ριζικά διαφορετικούς από αυτούς του οργανισμού

• Άτομα τα οποία έχουν εκδικητική διάθεση έναντι του οργανισμού σας ή συγκεκριμένων υπαλλήλων του

• Άτομα τα οποία επιθυμούν να αποκτήσουν φήμη μέσω της δημόσιας αναγνώρισης του οργανισμού σας

Φυσικά ανάλογα με τον οργανισμό που θέλει να προστατευθεί, μπορεί να υπάρχουν και άλλες πιθανές απειλές οι οποίες θα πρέπει να προστεθούν στην λίστα των πιθανών εισβολέων.

Τα σημαντικά στοιχεία στην περίπτωση μας είναι να προσδιοριστεί τι έχει να κερδίσει κάποιος εξαπολύοντας μία επιτυχημένη επίθεση στο δίκτυο του οργανισμού σας, και τι μπορεί να αξίζει αυτή η επίθεση για έναν πιθανό εισβολέα. Επίσης να προσδιοριστεί πόσες πιθανότητες έχω υπάρχουν για να δεχθούμε επίθεση.

Μετά τον προσδιορισμό των πόρων του οργανισμού και τις πηγές από τις οποίες μπορούν να προέλθουν επιθέσεις, πρέπει να γίνει εκτιμήση του επίπεδου κινδύνου του οργανισμού σας έναντι τέτοιων επιθέσεων.

Έτσι παίζει ρόλο η διάταξη που έχει το δίκτυο.

Έτσι μπαίνουν ερωτήματα αν είναι εντελώς απομονωμένο, ή έχει πολλά σημεία εισόδου - όπως για παράδειγμα σύνδεση μέσω WAN, δεξαμενή μόντεμ, ή ένα

δίκτυο VPN για την διακίνηση πληροφοριών μέσω Internet και πόσο ανοικτό στο internet;

Χρησιμοποιείται στα ανοικτά σημεία σύνδεσης ένα ισχυρό σχήμα πιστοποίησης και κάποιο σύστημα προστασίας (firewall);

Μπορεί το δίκτυο να αποτελέσει στόχο για ένα πιθανό εξωτερικό εισβολέα;

Π.χ αν ο οργανισμός διατειρεί οικονομικά στοιχεία ένας τέτοιος εισβολέας θα προτιμούσε να εξαπολύσει την επίθεση του. Π.χ σε μία τράπεζα έχουμε μεγαλύτερες πιθανότητες επίθεσης από ένα μικρό γραφείο. Η εκτίμηση της πιθανότητας να δεχθεί επίθεση το δίκτυο είναι σημαντικό να εξεταστεί

Παρόλα αυτά κάτι τέτοιο είναι υποκειμενικό. Π.χ διαφορετικοί εργαζόμενοι στον ίδιο οργανισμό θα μπορούσαν να έχουν εντελώς διαφορετική άποψη όσον αφορά στην πιθανότητα επιθέσεων που μπορεί να δεχτεί το δίκτυο. Έτσι είναι σημαντικό η εκτίμηση να γίνει παίρνοντας πολλές διαφορετικές γνώμες από διαφορετικά τμήματα του οργανισμού. Πολλές φορές σε αυτό το σημείο απαιτείται και η συνεργασία με εξειδικευμένους σύμβουλους οι οποίοι έχουν πρακτική εμπειρία στην ανάλυση και αξιολόγηση κινδύνων.

Σημαντική είναι και η ανάλυση του κόστους

Έτσι για κάθε πόρο που αναφέραμε θα πρέπει να καταγραφεί η άμεση επίδραση που θα είχε μια τέτοια παραβίαση ή καταστροφή σε κόστος.

Π.χ. τι γίνεται εάν η παραβίαση του δικτύου επιτρέψει σε έναν ανταγωνιστή να αποκτήσει πρόσβαση σε όλα τα πρωτότυπα σχέδια της νέας σειράς προϊόντων της εταιρείας; Η πιθανότητα αυτή ίσως να έδινε στον ανταγωνιστή σας την δυνατότητα να αναπτύξει ένα καλύτερο προϊόν και να προλάβει την είσοδο του στην αγορά νωρίτερα. Παρόλα αυτά είναι δύσκολο να εκτιμηθεί το ακριβές κόστος,

Επίσης η απώλεια της εμπιστοσύνης των καταναλωτών, ή η δυσφήμιση, μπορούν μπορούν να επηρεάσουν πολύ αρνητικά την πορεία ενός οργανισμού.

Ωστόσο, σε ορισμένες περιπτώσεις ο κύριος συντελεστής για τον προσδιορισμό των απωλειών δεν είναι άμεσο οικονομικό κόστος. Έτσι αν ο οργανισμός είναι ένα νοσοκομείο μπορεί να αντιμετωπίσει απώλειες εάν ένας εισβολέας παραβιάσει ιατρικές του εγγραφές, η καταστροφή εγγραφών που θα

μπορούσαν να συνεπάγονται ακόμη και απώλεια ζωής δηλαδή κάτι ανεκτίμητο και πολύ πιο καταστροφικό.

Έτσι κατά τον προσδιορισμό του άμεσου κόστους από απώλεια ή από τις συνέπειες μιας επίθεσης θα πρέπει να εξετάστει οποιαδήποτε μορφή απώλειας - όχι μόνο οικονομική. Επίσης δεν πρέπει να εξετάζεται μονο το άμεσο αλλά και το μακροπρόθεσμο κόστος. Θα πρέπει επίσης να γίνεται εκτιμήση για το κόστος που συνεπάγεται η πλήρης ανάκαμψη του συστήματος από μία βλάβη ή επίθεση.

Προσδιορίζοντας τις επιπτώσεις που συνεπάγονται διάφορες μορφές απωλειών πλέον πρέπει να προσδιορίστει η πιθανή οικονομική επένδυση που θα πρέπει να γίνει για την διασφάλιση των πόρων του δικτύου.

Έτσι θα πρέπει να μελετήσουμε πόσο θα κοστίσει η ασφάλεια, όταν καθορίστεί το επίπεδο της προστασίας που είναι κατάλληλο για το δικό αντίστοιχο περιβάλλον δικτύου. Για την ασφάλιση του περιβάλλοντος δικτύου μπορεί επίσης να υπάρχουν κόστη τα οποία δεν είναι άμεσα εμφανή αλλά πρέπει να συνυπολογιστούν, όπως π.χ. η απασχόληση των στελέχων για την προστασία, ανάλογα με το μέγεθος του δικτύου σας.

Αυξάνοντας το επίπεδο της λεπτομέρειας που καταγράφεται για τις δραστηριότητες του δικτύου σας ίσως δημιουργήθει η ανάγκη πρόσληψης ενός επιπλέον τελικά ανθρώπινου δυναμικού ειδικά για την ασφάλειά του. Η αυξημένη ασφάλεια συνεπάγεται σε πολλές περιπτώσεις την μείωση της ευκολίας χρήσης ή πρόσβασης στους πόρους του δικτύου, γεγονός που μπορεί να καταστήσει πιο κουραστική ή χρονοβόρες την εκτέλεση εργασιών από τους χρήστες του δικτύου μας.

Φυσικά το παραπάνω δεν οδηγεί στο ότι θα πρέπει να αποφευχθεί με κάθε κόστος αυτή η μείωση ευχρηστίας·αλλά μπορεί να είναι αναγκαίο τελικά συμφωνα με την πολιτική ασφαλείας που θα ακολουθηθεί για την ασφάλιση ενός ασφαλούς περιβάλλοντος, και πρέπει να καταγραφεί σαν πιθανό κόστος λόγω μειωμένης παραγωγικότας.

1.4 Κατάρτιση του προϋπολογισμού για τα μέτρα ασφάλειας

Αφού γίνουν όλα τα παραπάνω ουσιαστικά θα πρέπει να έχουν καταγραφεί τα στοιχεία και να έχει σχηματίσει μία πολύ καλή άποψη σχετικά με το επίπεδο

ασφάλειας του οποίου το κόστος θα πρέπει να καλυφθεί. Το κόστος αυτό σε μία εταιρία συμπεριλάβετε στις αποσβέσεις των παγίων (ο εξοπλισμός του server, τα συστήματα firewall και η κατασκευή ασφαλών περιοχών μέσα στις εγκαταστάσεις της εταιρείας). Παρόλα αυτά θα πρέπει να καταγραφεί και οποιοδήποτε περιοδικό κόστος (μισθοδοσία του προσωπικού ασφάλειας, τακτικοί έλεγχοι και συντήρηση του συστήματος).

Έτσι θα πρέπει όσο είναι δυνατόν να έχουμε ένα πλήρη προϋπολογισμό, για τα μέτρα ασφάλειας που πρέπει και μπορούμε να λάβουμε. Η ασφάλεια είναι ένα προληπτικό έξοδο - δηλαδή ο οργανισμού θα πρέπει να επενδύσει χρήματα σε μέτρα και διαδικασίες οι οποίες, εάν όλα πάνε κατ' ευχήν, θα αποδώσουν μόνο και μόνο επειδή δεν θα χρειαστεί να δαπανηθούν περισσότερα χρήματα στο μέλλον από μία καταστροφή, Όσα περισσότερα μέτρα προφύλαξης λαμβάνονται τόσο περισσότερο μειώνονται οι πιθανότητες καταστροφής.

ΚΕΦΑΛΑΙΟ 2: ΑΠΟΔΟΣΗ ΔΙΚΤΥΟΥ

2.1 Διαχείριση απόδοσης Δικτύου

Σαν απόδοση του δικτύου αναφερόμαστε στην ακριβή και γρήγορη μεταφορά των δεδομένων από μια συσκευή του δικτύου σε μία άλλη. Δηλαδή στην ασφαλή και ορθή μετάδωση πληροφοριών μέσα στο πιο σύντομο χρονικό διάστημα. Η απόδοση του δικτύου αποτελεί πολύ σημαντικό κομμάτι της ασφάλειας των δικτύων αφού είναι η βάση της ορθής λειτουργίας του δικτύου.

Για την διασφάλιση και διαχείριση της απόδοση ενός δικτύου, πρέπει αρχικά να ορίσουμε ποια θα είναι τα μεγέθη πρέπει να μεταράμε ώστε τελικά να έχουμε την καλύτερη απόδοση. Στην συνέχεια θα πρέπει να βρούμε τρόπους με τους οποίους θα γίνονται οι μετρήσεις μας και τέλος να στο πως αυτές θα λαμβάνονται όσο το δυνατόν αυτόματα. Τυπικά, σε ένα δίκτυο μετράμε ανά τακτά διαστήματα χαρακτηριστικά όπως τα παρακάτω:

- Το ποσοστό χρησιμοποίησης των γραμμών WAN ή τμημάτων του τοπικού δικτύου.
- Ανάλυση του ποσοστού κίνησης ανά πρωτόκολλο π.χ. TCP/IP, IPX, Netbios κλπ.
- Το ποσοστό λαθών σε σχέση με όλη την κίνηση.
- Το χρόνο καθυστέρησης σε διάφορα σημεία του δικτύου.
- Το χρόνο απόκρισης κάποιων συσκευών.
- Καθορισμένα κατώφλια (κρίσιμες μέγιστες ή ελάχιστες τιμές).

Στα αυτόματα συστήματα μέτρησης όταν οι τιμές των μετρούμενων παραμέτρων ξεφεύγουν από κάποια όρια, τότε εμφανίζονται συναγερμοί και δημιουργούνται ειδοποιήσεις. Οι μετρήσεις επίδοσης μπορεί να αποθηκεύονται για μελλοντική επεξεργασία και σύγκριση με επόμενες μετρήσεις. Ο υπεύθυνος για αυτή την επεξεργασία είναι ο λεγόμενος διαχειριστής του δικτύου ο οποίος με την κατάλληλη ανάλυση των μετρήσεων μπορεί να καταδείξει τα σημεία που δημιουργούν προβληματική λειτουργία ή συμφόρηση του δικτύου.

Με βάση τα συμπεράσματα των μετρήσεων μπορεί να γίνει ανασχεδίαση σημείων του δικτύου, αλλαγή υλικού ή ρυθμίσεων κλπ. Μετά τις αλλαγές, η σύγκριση με νέες μετρήσεις θα δείξει κατά πόσο ήταν επιτυχής η επίλυση του προβλήματος.

Τυπικά οι μετρούμενες τιμές καταγράφονται κατάλληλους πίνακες και μπορούν επίσης να αναπαρίστανται με μορφή γραφημάτων.

Διαχείριση Σφαλμάτων (Fault Management)

Με τη διαχείριση σφαλμάτων μπορούμε να εντοπίσουμε προβλήματα στη λειτουργία του δικτύου. Μπορούμε επίσης να βρούμε το σημείο στο δίκτυο που τα δημιουργεί και ενδεχομένως να το διορθώσουμε, αν πρόκειται απλώς για κάποια ρύθμιση. Σε περίπτωση που το πρόβλημα αφορά υλικό ή βρίσκεται εκτός της δικαιοδοσίας μας, μπορούμε να προωθήσουμε την περιγραφή του προβλήματος (να δημιουργήσουμε δηλ. κατάλληλη τεκμηρίωση) σε μια άλλη ομάδα που θα το αναλάβει. Σε κάθε περίπτωση, γίνεται καταγραφή του προβλήματος καθώς και των βημάτων που ακολουθήθηκαν για την επίλυση του, ώστε να υπάρχει έτοιμη λύση σε περίπτωση που το πρόβλημα εμφανιστεί ξανά στο μέλλον. Για κάποιες από τις συσκευές του δικτύου, ίσως να είναι χρήσιμο να τηρούνται στατιστικά σχετικά με το ποσοστό λαθών που εμφανίζουν.

Μερικά προβλήματα μπορεί να είναι εύκολο να εντοπιστούν (χαλασμένη ή απενεργοποιημένη συσκευή). Ο σκοπός όμως της διαχείρισης είναι να μπορεί να προβλέψει προβλήματα πριν αυτά παρουσιαστούν και επηρεάσουν τους χρήστες του δικτύου. Η πρόβλεψη πιθανών προβλημάτων σχετίζεται άμεσα με τη διαχείριση επίδοσης του δικτύου. Τα προβλήματα εμφανίζονται στο πρόγραμμα διαχείρισης με τη μορφή συναγερμών (alarms) και καταγράφονται συνήθως σε αρχεία καταγραφής (log files). Σε περίπτωση γραφικών απεικονίσεων, ενδεχομένως να απεικονίζονται οι προβληματικές συσκευές με διαφορετικό χρώμα. Ανάλογα με το πρόβλημα, μπορεί να χρειάζεται αποσύνδεση ή αντικατάσταση προβληματικών συσκευών από το δίκτυο ή αλλαγή των ρυθμίσεων στο λογισμικό των συσκευών.

Διαχείριση Κόστους (Accounting Management)

Το έργο της διαχείρισης κόστους του δικτύου περιλαμβάνει την παρακολούθηση της χρήσης των πόρων του δικτύου και την ανάλυση των διαθέσιμων ορίων χρήσης του δικτύου για συγκεκριμένες ομάδες χρηστών. Γίνεται ακόμα

καταγραφή της χρήσης των πόρων του δικτύου ανά ομάδες χρηστών. Τέλος εξασφαλίζεται ότι οι χρήστες δεν χρησιμοποιούν υπηρεσίες που δεν είναι συμφωνημένες.

Διαχείριση Ασφάλειας (Security Management)

Σημαντικό είναι στο δικτυο μας να γίνεται η λεγόμενη διαχείριση ασφάλειας. Η διαχείριση ασφάλειας περιλαμβάνει τον έλεγχο πρόσβασης σε συσκευές, δεδομένα και προγράμματα απέναντι σε κάθε μη-εξουσιοδοτημένη χρήση (ηθελημένη ή μη).

Ο οργανισμός ή εταιρία που χρησιμοποιεί ένα πληροφοριακό σύστημα, ουσιαστικά δεσμεύεται να οργανώσει και να τηρεί κανόνες ασφαλείας. Τα μέτρα ασφαλείας αφορούν:

- Τη φυσική προστασία των πόρων του συστήματος από μη-εξουσιοδοτημένη πρόσβαση. Αυτό τυπικά σημαίνει ότι τα κρίσιμα μηχανήματα του δικτύου βρίσκονται σε καλά φυλασσόμενο χώρο.
- Την ασφάλεια των συστημάτων που συνδέονται στο δίκτυο. Και αυτό το κομμάτι ανήκει στη διαχείριση ασφαλείας των συστημάτων (για παράδειγμα, μπορεί να υλοποιείται με τη βοήθεια των μηχανισμών ασφαλείας που παρέχει το λειτουργικό σύστημα που χρησιμοποιείται).
- Την ασφάλεια του δικτύου και την προστασία των δεδομένων που μεταφέρονται μέσα από αυτό.

2.2 Ασφάλεια Πληροφοριών

Η ασφάλεια πληροφοριών ενός οποιουδήποτε συστήματος ασχολείται με την προστασία αντικειμένων που έχουν κάποια αξία τα οποία είναι γνωστά ως αγαθά. Η αξία των πληροφοριακών αγαθών μειώνεται αν υποστούν ζημιά. Έτσι πιθανές επιθέσεις μπορούν να μειώσουν την αξία των αγαθών και θα πρέπει να παρθούν τα αντίστοιχα μέτρα προστασίας τους. Τα μέτρα αυτά προφανώς θα έχουν κάποιο κόστος, οικονομικό και εργασιακό. Έτσι θα πρέπει να υπολογιστεί και σταθμιστεί το κόστος προστασίας των αγαθών με το αντίστοιχο ρίσκο αλλά και με το κόστος των ίδιων των αγαθών.

Αν λάβουμε μειωμένα (πλημμελή) μέτρα προστασίας, η ασφάλεια των αγαθών δεν θα είναι εξασφαλισμένη. Ο ιδιοκτήτης των αγαθών είναι υπεύθυνος να

σταθμίσει το κόστος προστασίας ανάλογα με το κίνδυνο και την αξία των αγαθών, και να αποφασίσει ποιο είναι το σημείο ισορροπίας.

Για παράδειγμα, ο χρήστης μιας ιστοσελίδας έχει δυνατότητα να διαβάσει το περιεχόμενο ή να "κατεβάσει" αρχεία, αλλά δεν μπορεί να αλλάξει το περιεχόμενο τους. Αυτό γιατί σε ένα δίκτυο ο ιδιοκτήτης και χρήστης ενός πληροφοριακού αγαθού, δεν είναι απαραίτητα το ίδιο άτομο.

Η έννοια του χρήστη δεν αναφέρεται αναγκαστικά σε κάποιο φυσικό πρόσωπο αλλά και σε διεργασίες που εκτελούνται μέσα στο ίδιο το σύστημα και έχουν πρόσβαση στα δεδομένα.

Έτσι όταν κάποια δεδομένα χαρακτηρίζονται ως ιδιωτικά δηλάδη έχουν πάνω τους την έννοια της ιδιοκτησίας, θα πρέπει να εισάγουμε και την έννοια της εξουσιοδότησης. Σαν εξουσιοδότηση θεωρείται η άδεια που παρέχει ο ιδιοκτήτης σε κάποιον τρίτο (χρήστη) για τη χρήση των δεδομένων ή/και των υπολογιστικών πόρων του δικτύου.

Έτσι είναι σημαντικό θέμα ασφάλειας η εξασφάλιση ότι μόνο εξουσιοδοτημένοι χρήστες έχουν πρόσβαση στα δεδομένα. Επίσης οι εξουσιοδοτημένοι χρήστες μπορεί να θελήσουν να χρησιμοποιήσουν την πρόσβαση τους για να αποκτήσουν περισσότερα δικαιώματα σε σημεία του συστήματος που δεν έχουν πρόσβαση. Για την εξασφάλιση της χρήσης των αγαθών από εξουσιοδοτημένους χρήστες, υπάρχουν τέσσερα ζητούμενα στα πλαίσια της πολιτικής ασφαλείας:

- Αυθεντικότητα (authentication): Η απόδειξη της ταυτότητας του χρήστη προκειμένου να του επιτραπεί η πρόσβαση στα αγαθά που παρέχει το σύστημα. Ένας γνωστός τρόπος είναι η χρήση του συνδυασμού ονόματος χρή- στη/κωδικού πρόσβασης (username/password).
- Ακεραιότητα (integrity): Η διασφάλιση ότι τα δεδομένα δεν έχουν αλλοιωθεί ή ότι η όποια μεταβολή τους έχει επέλθει μόνο από εξουσιοδοτημένα άτομα.
- Εμπιστευτικότητα (confidentiality): Ο περιορισμός της πρόσβασης στα δεδομένα μόνο σε άτομα που επιτρέπεται να έχουν πρόσβαση σε αυτά.
- Μη άρνηση ταυτότητας (non-repudiation): Η δυνατότητα απόδοσης πράξεων (ευθυνών) σε κάποιο συγκεκριμένο χρήστη. Πολύ απλά, η δυνατότητα να δούμε ποιος έκανε οποιαδήποτε αλλαγή στο σύστημα.

Από τα τέσσερα παραπάνω μπορούμε ακόμα να ορίσουμε:

- Εγκυρότητα (validity): Την απόλυτη ακρίβεια και πληρότητα μιας πληροφορίας. Η εγκυρότητα είναι συνδυασμός της Ακεραιότητας και της Αυθεντικότητας.
- Διαθεσιμότητα Πληροφοριών (Information Availability): Την αποφυγή προσωρινής ή μόνιμης απώλειας πρόσβασης στις πληροφορίες από εξουσιο- δοτημένους χρήστες. Σε κάποιες περιπτώσεις, οι χρήστες μπορεί να πληρώ- νουν κάποιο αντίτιμο για να έχουν πρόσβαση στις πληροφορίες που παρέχει το σύστημα μας. Είναι απαραίτητο να εξασφαλίσουμε ότι η πρόσβαση σε αυ- τές τις πληροφορίες θα είναι αδιάλειπτη. Μπορούμε τώρα να δώσουμε και τους παρακάτω ορισμούς:
- Ασφάλεια (security): Η προστασία της Διαθεσιμότητας, Ακεραιότητας και Εμπιστευτικότητας των πληροφοριών. • Ασφάλεια Πληροφοριών (information security): Ο συνδυασμός της Εμπι- στευτικότητας, Εγκυρότητας και Διαθεσιμότητας Πληροφοριών.
- Παραβίαση Ασφαλείας (security violation): Η παραβίαση ενός ή περισσό- τερων από τις παραπάνω ιδιότητες, όπως διαθεσιμότητα, εμπιστευτικότητα και εγκυρότητα. Γενικά ένα πληροφοριακό σύστημα είναι εκτεθειμένο σε κινδύνους. Οι κίνδυνοι μπορούν να διαχωριστούν σε απειλές και αδυναμίες.

Με τον όρο "απειλές" (threats) αναφερόμαστε σε ενέργειες ή γεγονότα που μπορούν οδηγήσουν στην κατάρρευση κάποιου από τα χαρακτηριστικά ασφαλείας που ορίσαμε προηγουμένως. Οι απειλές μπορεί να οφείλονται σε τυχαία ή φυσικά γεγονότα (πυρκαγιά, πλημμύρα κλπ) ή σε ανθρώπινες ενέργειες (σκόπιμες ή μη).

Με τον όρο "αδυναμίες" (vulnerabilities) αναφερόμαστε σε σημεία του πληροφοριακού συστήματος τα οποία (ενδεχομένως λόγω κακού σχεδιασμού ή υλοποίησης) αφήνουν περιθώρια για παραβιάσεις. Σε πολλές περιπτώσεις οι αδυναμίες οφείλονται σε λάθη του λογισμικού ή σε ανεπαρκή παραμετροποίηση του από το προσωπικό που το εγκατέστησε και το συντηρεί.

Πριν προχωρήσουμε στη λήψη μέτρων ασφαλείας, θα πρέπει να εκτιμήσουμε και να υπολογίσουμε διάφορους παράγοντες. Θα πρέπει αρχικά να αξιολογήσουμε ποια είναι τα αγαθά που χρήζουν προστασίας και να εντοπίσουμε τους πιθανούς κινδύνους από τους οποίους θα πρέπει να προστατευθούν.

Έπειτα θα πρέπει να προχωρήσουμε σε ένα αρχικό σχεδιασμό της αρχιτεκτονικής ασφαλείας που θα ακολουθήσουμε και να εκτιμήσουμε το κόστος

του. Το συνολικό κόστος πρέπει να περιλαμβάνει το κόστος αγοράς εξοπλισμού και λογισμικού που θα χρησιμοποιήσουμε, το κόστος εγκατάστασης του από κατάλληλο προσωπικό, αλλά και το μόνιμο λειτουργικό κόστος που θα έχει η συντήρηση και αναβάθμιση του.

Αν το κόστος που υπολογίσουμε υπερβαίνει τα προβλεπόμενα όρια, θα πρέπει να κάνουμε κάποιες νέες παραδοχές ή συμβιβασμούς σχετικά με το τι προβλήματα ασφαλείας και σε τι βαθμό θα καλύπτει η πολιτική ασφαλείας.

Με τον τρόπο αυτό αποδεχόμαστε τους εναπομείναντες κινδύνους που δεν καλύπτονται από την τελική πολιτική ασφαλείας. Στις επόμενες ενότητες θα εξετάσουμε τις τεχνικές μεθόδους που χρησιμοποιούνται για την επίτευξη των παραβιάσεων, αλλά και τα αντίμετρα που μπορούμε να υλοποιήσουμε για να προστατέψουμε ένα πληροφοριακό σύστημα.

2.3 Ορολογία στην Ασφάλεια Δικτύων

Οι πιο βασικοί όροι σε θέματα ασφάλειας πληροφοριακών συστημάτων είναι οι παρακάτω:

• Κρυπτογράφηση (Encryption): Η κρυπτογράφηση είναι η διαδικασία με την οποία μετατρέπονται τα αρχικά δεδομένα (γνωστά και ως plaintext) σε μορφή (κρυπτόγραμμα) η οποία δεν μπορεί πλέον να γίνει κατανοητή χωρίς να αποκρυπτογραφηθεί. Η κρυπτογράφηση γίνεται με τη βοήθεια αλγορίθμου, το αποτέλεσμα του οποίου μπορεί να αντιστραφεί ώστε να παράγει ξανά τα αρχικά δεδομένα εισόδου. Για την κρυπτογράφηση και την αποκρυπτογράφηση χρησιμοποιείται το κλειδί.

• Αποκρυπτογράφηση (Decryption): Προφανώς η αντίστροφη διαδικασία της κρυπτογράφησης. Ο αλγόριθμος δέχεται ως είσοδο τα κρυπτογραφημένα δε- δομένα (κρυπτόγραμμα) και με τη βοήθεια του κλειδιού (το οποίο προφανώς είναι διαθέσιμο μόνο σε εξουσιοδοτημένα άτομα) τα μετατρέπει ξανά στα κανονικά δεδομένα. Τα δεδομένα πλέον δεν είναι κωδικοποιημένα και μπορούν να χρησιμοποιηθούν κανονικά.

• Κλειδί (Key): Στο πεδίο της κρυπτογράφησης, το κλειδί είναι ένας ψηφιακός κωδικός (ένας αριθμός από bits) ο οποίος χρησιμοποιείται για την κρυπτογράφηση και αποκρυπτογράφηση της πληροφορίας. Προφανώς το κλειδί φυλάσσεται σε

ασφαλές μέρος και είναι διαθέσιμο μόνο στα μέρη που επιτρέπεται να έχουν πρόσβαση στα δεδομένα.

• Δημόσιο Κλειδί (Public Key): Στην ασυμμετρική κρυπτογράφηση, χρησιμοποιούνται για κάθε χρήστη δύο κλειδιά, το δημόσιο και το ιδιωτικό. Η βασική ιδέα είναι ότι το δημόσιο το γνωρίζει καθένας, ενώ το ιδιωτικό μόνο ο χρήστης. Το δημόσιο κλειδί χρησιμοποιείται για να "κλειδώνει" (κρυπτογραφεί) ενώ το ιδιωτικό ξεκλειδώνει. Όποιος θέλει να μας στείλει κρυπτογραφημένα δεδομένα, χρησιμοποιεί το δημόσιο μας κλειδί για να τα κλειδώσει.

Μετά από αυτό η αποκρυπτογράφηση γίνεται μόνο με το δικό μας ιδιωτικό κλειδί. Γενικά η ασυμμετρική κρυπτογράφηση θεωρείται πιο ασφαλής από τη συμμετρική, καθώς δεν γνωρίζει κανείς άλλο το ιδιωτικό μας κλειδί. (Στη συμμετρική κρυπτογράφηση χρησιμοποιείται το ίδιο κλειδί και για τις δύο λειτουργίες, άρα πρέπει να το έχουν και τα δύο μέρη της επικοινωνίας)

• Ιδιωτικό Κλειδί (Private Key): Το ιδιωτικό κλειδί χρησιμοποιείται στην ασυμμετρική κρυπτογράφηση για να αποκρυπτογραφεί και να υπογράφει δεδομένα. Το ιδιωτικό κλειδί συνδυάζεται πάντα (σαν ζεύγος) με ένα αντίστοιχο δημόσιο.

• Μυστικό Κλειδί (Secret Key): Ψηφιακός κωδικός που είναι γνωστός και στα δύο μέρη προκειμένου να τον χρησιμοποιήσουν σε ανταλλαγή δεδομένων με χρήση κρυπτογράφησης / αποκρυπτογράφησης.

• Λειτουργία (Συνάρτηση) Κατατεμαχισμού (Hash Function): Μαθηματική συνάρτηση της οποίας η έξοδος δεν μπορεί με αντιστροφή (με κανένα τρόπο) να μας παράγει την αρχική είσοδο. Προφανώς δεν μπορεί να χρησιμοποιηθεί για κρυπτογράφηση, καθώς δεν μπορούμε μετά να αποκρυπτογραφήσουμε το κείμενο, αλλά χρησιμοποιείται για την παραγωγή συνόψεων (digests).

• Σύνοψη Μηνύματος (Message Digest): Η σύνοψη ενός μηνύματος είναι το αποτέλεσμα (έξοδος) της συνάρτησης κατατεμαχισμού. Η σύνοψη δεν έχει το ίδιο μέγεθος (είναι συνήθως μικρότερη) με το αρχικό μήνυμα – κάτι το οποίο έχει νόημα, γιατί όπως εξηγήσαμε δεν μπορούμε έτσι και αλλιώς να ξαναγυρίσουμε στο αρχικό μήνυμα. Οι αλγόριθμοι κατατεμαχισμού είναι φτιαγμένοι με τέτοιο τρόπο ώστε μια μικρή μεταβολή στα δεδομένα εισόδου (π.χ. ένα μόνο γράμμα ή ακόμα και ένα μόνο bit) να προκαλεί ολοκληρωτική αλλαγή στην έξοδο (πλήρης αλλαγή της σύνοψης). Για το λόγο αυτό η σύνοψη χρη- σιμοποιείται πολύ συχνά για να ελέγξουμε την

ακεραιότητα κάποιου αρχείου που κατεβάσαμε π.χ. από το Internet. Σε μεγάλα downloads, μπορούμε συ- νήθως να κατεβάσουμε και ένα αρχείο CHECKSUM (αθροίσματος ελέγχου) που περιέχει μέσα την σύνοψη του μεγάλου αρχείου. Εκτελώντας τη συνάρ- τηση κατατεμαχισμού στο δικό μας μηχάνημα, μπορούμε να συγκρίνουμε τις συνόψεις: αν είναι ίδιες το αρχείο έχει κατέβει σωστά.

• Ψηφιακή Υπογραφή (Digital Signature): Η ψηφιακή υπογραφή είναι τυπικά ένας αριθμός από bit που προστίθεται στο τέλος κάποιου αρχείου και εξασφαλίζει την αυθεντικότητα (“το έστειλε πράγματι ο χρήστης Α”) και την ακεραιότητα (“το έχουμε λάβει σωστά”) ενός μηνύματος.

ΚΕΦΑΛΑΙΟ 3: ΑΣΦΑΛΕΙΑ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

3.1 Ασφαλής πλοήγηση στον παγκόσμιο ιστό

Ο Παγκόσμιος Ιστός (World Wide Web) είναι μια από τις σημαντικότερες υπηρεσίες του Internet και προσφέρει στους χρήστες του τη δυνατότητα πρόσβασης στη μεγαλύτερη δεξαμενή πληροφοριών στον κόσμο.

Ουσιαστικά το ευρύτερο δίκτυο στον κόσμο λέγεται παγκόσμιος ιστός το οποίο είναι μοναδικό (δηλαδή δεν υπάρχουν παραπάνω από ένα δίκτυα υπολογιστών παγκόσμιας κλίμακας), και συμπεριλαμβάνεται τόσο τα γήινα δίκτυα, όσο και τα δίκτυα των δορυφόρων της και άλλων διαστημικών συσκευών που είναι συνδεδεμένα σε αυτό.

Η τεχνολογία του ιστού καθιστά δυνατή την δημιουργία "υπερκειμένων", μία διασύνδεση δηλαδή πάρα πολλών μη ιεραρχημένων στοιχείων που παλαιότερα ήταν απομονωμένα. Τα στοιχεία αυτά μπορούν να πάρουν και άλλες μορφές πέραν της μορφής του γραπτού κειμένου, όπως εικόνας και ήχου.

Ο παγκόσμιος ιστός ουσιαστικά, είναι μια τεράστια συλλογή εγγράφων, τα οποία είναι αποθηκευμένα σε εκατομμύρια υπολογιστές στον κόσμο, η οποία εμπλουτίζεται συνεχώς από όλους τους χρήστες οι οποίοι αποφασίζουν να ανεβάσουν στο χώρο του τις σελίδες τους.

Η πλοήγησης στις σελίδες του παγκοσμίου ιστού πραγματοποιείται μέσω ειδικών προγραμμάτων πλοήγησης του λεγόμενους browsers. Γνωστοί φυλλομετρητές είναι ο Internet Explorer, ο Mozilla , το Chroome κ.α. και απαιτεί ιδιαίτερη προσοχή από τον χρήστη, διότι εγκυμονεί πολλαπλούς κινδύνους, τόσο για την ασφάλεια του υπολογιστή του, όσο και για την ασφάλεια των προσωπικών του δεδομένων.

Κατά την πλοήγησης τα μέτρα τα οποία πρέπει να ληφθούν για να εξασφαλίσουν κατά το δυνατόν ασφαλέστερη πλοήγηση εξαρτώνται

α) από τις υπηρεσίες που μπορεί να προσφέρει ο παροχέας σύνδεσης

β) από τις ενέργειες που κάνει ο ίδιος ο χρήστης.

Έτσι κατά την πλοήγηση στους χώρους του Διαδικτύου είναι καλό να προσέχουμε τα παρακάτω:

Να είμαστε υποψιασμένοι και να γνωρίζουμε ότι οι πληροφορίες που παρουσιάζονται στο Διαδίκτυο δεν είναι πάντα έγκυρες.

Η δημιουργία ενός συνόλου από κανόνες χρήσης των υπολογιστών τόσο στην εργασία όσο και στο εργασιακό περιβάλλον από όλους και η ανάρτηση τους σε εμφανές σημείο δίπλα στον υπολογιστή συντελεί στην προστασία όλων των χρηστών.

Η κοινοποίηση των προσωπικών στοιχείων του χρήστη σε σελίδες άγνωστες στο χρήστη π.χ το ονοματεπώνυμο, διεύθυνση, τηλέφωνο, φωτογραφία, κωδικούς πρόσβασης, e-mail κλπ είναι καλό να αποφεύγεται.

Ειδικά για τα παιδιά η τοποθέτηση του υπολογιστή 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.

Επίσης όσο αφορά τα παιδιά η καλή επικοινωνία είναι απαραίτητη ώστε να ενθαρρύνονται να μιλάνε για αυτούς με τους οποίους επικοινωνούν, ανταλλάσσουν μηνύματα και να ενημερώνουν εάν γίνονται θύματα απειλών, εκφοβισμού ή παρενόχλησης οποιασδήποτε μορφής.

3.2 Υπηρεσίες παροχέα σύνδεσης

Σαν παροχέας σύνδεσης είναι ο παροχέας που μας δίνει την δυνατότητα χρήσης και εισόδου στο παγκόσμιο δίκτυο, το διαδίκτυο. Τα μέτρα για την ασφαλή πλοήγηση έχουν αφετηρία υπηρεσίες του παροχέαπρόσβασης στο διαδίκτυο.

Συνήθως ένας παροχέας μπορεί να προσφέρει τα παρακάτω:

- φιλτράρισμα των ιστοσελίδων που επισκέπτεται ο χρήστης
- φιλτράρισμα των επισυναπτόμενων αρχείων στα emails που δέχεται ο χρήστης-πελάτης.

Για παράδειγμα, το Πανελλήνιο Σχολικό Δίκτυο που χρησιμοποιείται από καθηγητές και μαθητές εποπτεύεται από πρόγραμμα φιλτραρίσματος το οποίο δρα με δύο τρόπους:

- ψάχνει στις ιστοσελίδες που ζητά να δει ο χρήστης και αναζητά συγκεκριμένες λέξεις που είναι ύποπτες για ακατάλληλο υλικό π.χ. sex, crime κ.α.
- ψάχνει να δει αν η ιστοσελίδα έχει καταχωρηθεί στην μαύρη λίστα που διατηρεί στη βάση δεδομένων του.

Έτσι απαγορεύει την πρόσβαση σε αυτές τις ιστοσελίδες, εμφανίζοντας προειδοποιητικά μήνυματα.

Ειδικά στην περίπτωση των εισερχόμενων μηνυμάτων ηλεκτρονικής αλληλογραφίας, γίνεται προταρχική ερευνά για την ύπαρξη ιών στα επισυναπτόμενα αρχεία πριν ακόμα σταλεί στο inbox του παραλήπτη.

Παρόλα αυτά είναι σημαντικό να γνωρίζει ο χρήστης ότι είναι συχνό το φαινόμενο κατά τις οποίες σελίδες που περιέχουν ακατάλληλο υλικό δεν περιέχουν τις λέξεις που φιλτράρουν τα προγράμματα αυτά ή δεν έχουν καταχωρηθεί στην μαύρη λίστα. Αντιθέτως, ιστοσελίδες που δεν περιέχουν ακατάλληλο υλικό μπορεί να απαγορεύονται επειδή περιέχουν λέξεις που φιλτράρει το πρόγραμμα.

Στις περιπτώσεις αυτές είναι καλό ο χρήστης να ενημερώνει τον διαχειριστή του προγράμματος (Cachemaster).

3.3 Ενέργειες του ίδιου του χρήστη

Παρόλα αυτά όπως είδαμε όσο και καλές υπηρεσίες ενός παροχέα σύνδεσης δοθούν δεν εξασφαλίζουν τον χρήστη από τους κινδύνους που πιθανά θα συναντήσει κατά την πλοήγηση αν ο ίδιος δεν λάβει τα κατάλληλα μέτρα προστασίας και δεν υιοθετήσει μια πολύ προσεκτική συμπεριφορά.

Ένας βασικός κανόνας είναι η προσεκτική ανάγνωση όλων των μηνυμάτων που εμφανίζονται στην οθόνη του υπολογιστή. Δυστυχώς ο χρήστης έχει παρατηρηθεί ότι απαντά ενστικτωδώς σε πολλά μηνύματα που εμφανίζονται στην οθόνη του. Ο χρήστης δε θα πρέπει σε καμία περίπτωση να κάνει κλικ στο «Ναι» ή το «Όχι» των παραθύρων χωρίς να διαβάζει το περιεχόμενό τους, και επίσης θα πρέπει να κλείνει το παράθυρο χωρίς να κάνει κλικ, όταν δεν το καταλαβαίνει, αντί να απαντά άβουλα.

Pop up windows

Τα Pop up είναι παράθυρα που ανοίγουν κατά την πλοήγηση μας χωρίς να το προκαλεί ο χρήστης. Μάλιστα πολλές το περιεχόμενο τους ποικίλει και μπορεί να είναι:

Διαφημίσεις: Π.χ. μηνύματα που καλούν τον χρήστη να προβεί σε ενέργειες αν θέλει να αποδεχθεί συγκεκριμένες προσφορές με άγνωστες ή επικίνδυνες για αυτόν συνέπειες.

Καλέσματα: Κάλεσμα για παιγνίδια διαγωνισμούς κ.α.

Δωρεές: Συνήθως είναι σύνδεσμοι σε σελίδες πορνογραφικού περιεχομένου αλλά και δελεαστικών προτάσεων που οδηγούν τον χρήστη στο να αποδεχθεί την είσοδο σε αυτές.

Γενικα η ενδεδειγμένη ενέργεια είναι να κλείνουν άμεσα αυτά τα παράθυρα. Πολλές φορές μάλιστα μπορεί να μην δίνεται αυτή η επιλογή. Τότε ο χρήστης πρεπει να προσπαθήσει με το X που υπάρχει στο πάνω δεξιό τμήμα της οθόνης ή να κάνει τερματισμό μέσω του task manager κλείνοντας οριστικά το browser ή με δεξί κλικ στην γραμμή κατάστασης, στο αντίστοιχο εικονίδιο και επιλογή «κλείσιμο»,

Επισης μπορεί να κάνει Alt + F4 που αποτελεί μια απλή συνήθεια για να κλείνουμε παράθυρα.

Υπάρχουν προγραάμματα που αποκλείουν την εμφάνιση τέτοιων παραθύρων. (pop up blockers/ killers). Τα προγράμματα αυτά προσφέρονται στο διαδίκτυο. Επισημαίνεται ότι η χρήση τέτοιων προγραμμάτων μπορεί να εμποδίσει την πρόσβαση σε κάποιες, χρήσιμες περιπτώσεις π.χ. την είσοδο σε ένα ebanking. Σε αυτή την περίπτωση μπορούμε προσωρινά να απενεργοποιήσουμε τον blocker.

Τοπική αποθήκευση (download)

Η αποθήκευση αρχείων στον υπολογιστή μας, και ειδικά εκτελέσιμων προγραμμάτων στα οποία διατίθενται στο Διαδίκτυο (download) πρέπει να γίνεται με πολύ προσοχή, διότι ενδέχεται τα προγράμματα αυτά να είναι μολυσμένα με ιούς, ή

να αποτελούν τα ίδια ιούς που μπορεί να καταστρέψουν τα αρχεία του υπολογιστή. Έτσι πρέπει να είμαστε σίγουροι για την εγκυρότητα της ιστοσελίδας η οποία μας προτείνει το συγκεκριμένο πρόγραμμα. Τέτοιες ιστοσελίδες συνήθως εμφανίζουν μήνυμα στο οποίο ενημερώνουν ότι η λήψη δεδομένων από αυτές πληροί τις προϋποθέσεις ασφαλείας.

Ρύθμιση ασφαλείας φυλλομετρητών

Οι σύγχρονες εκδόσεις των φυλλομετρητών προσφέρουν δυνατότητα ρύθμισης των επιπέδων ασφαλείας κατά την πλοήγηση στο διαδίκτυο. Οι ρυθμίσεις αυτές είναι καλύτερο να γίνουν με τη βοήθεια ενός τεχνικού, αν ο χρήστης δεν έχει την κατάλληλη εμπειρία ή γνώσεις.

Εγκατάσταση προγραμμάτων ασφαλείας

Συνήθως στους υπολογιστές μας χρησιμοποιούμε ειδικά προγράμματα προγράμματα φιλτραρίσματος (filtering software) ή τειχών προστασίας του υπολογιστή (firewalls) από εξωτερικούς εισβολείς (φυσικά πρόσωπα ή ιοί). Στα προγράμματα αυτά πρέπει φυσικά να γίνονται και οι απαραίτητες ρυθμίσεις. Στα Windows από τα XP και μετά προσφέρεται ενσωματωμένο πρόγραμμα firewall.

3.4 Ασφαλής αναζήτηση στο Διαδίκτυο

Η αναζήτηση στο διαδίκτυο αποτελεί την πιο συχνή χρήση του. Ο λόγος είναι ότι το διαδίκτυο παρέχει μια τεράστια δεξαμενή πληροφοριών και εργαλείων διάσπαρτη σε δισεκατομμύρια ιστοσελίδες που πρακτικά είναι αδύνατον να ερευνηθούν από τον χρήστη χωρίς τη βοήθεια εξειδικευμένων προγραμμάτων. Τα προγράμματα αυτά λέγονται «μηχανές αναζήτησης».

Οι μηχανές αναζήτησης ουσιαστικά είναι ειδικά προγράμματα που χρησιμοποιούν τεχνικές αναζήτητης και κατάλληλο λογισμικό, τις λεγόμενες αράχνες (spiders), τα οποία «χτενίζουν» τις ιστοσελίδες αναζητώντας κείμενα και διευθύνσεις που σχετίζονται με λέξεις κλειδιά. Τα κείμενα και οι διευθύνσεις τους συγκεντρώνονται και καταγράφονται. Με άλλα προγράμματα συγκεντρώνονται

πληροφορίες από τα κείμενα, το είδος των οποίων ποικίλει από μηχανή σε μηχανή, και αποθηκεύονται σε βάσεις δεδομένων, ώστε να είναι εύκολο να ανακτηθούν.

Έτσι όταν ο χρήστης κάνει μια μια αναζήτηση, με την χρήση ενός συνόλου από λέξεις-κλειδιά, αρχικά ερευνάται η βάση δεδομένων της αντίστοιχης μηχανής και ακολούθως συγκεντρώνονται όλες οι διευθύνσεις που περιέχουν αυτές τις λέξεις. Τα αποτελέσματα αναζήτησης, εμφανίζονται στον χρήστη και με κατάλληλα link συνδέουν τον χρήστη με την διεύθυνση της ιστοσελίδας. Φυσικά προβάλεται και ένα δείγμα του κειμένου μέσα στο οποίο υπάρχουν οι λέξεις που αναζητήθηκαν, μια σύντομη περιγραφή και την κατηγορία στην οποία έχει καταγραφεί η ιστοσελίδα στην δεδομένη μηχανή αναζήτησης.

Ο τρόπος αναζήτησης μπρορεί να είναι απλός αλλά και σύνθετος. Μάλιστα ο τρόπος αναζήτησης θεωρείται πλέον ότι μια από τις βασικές δεξιότητες που πρέπει να διαθέτει ο χρήστης για να μη χαθεί στις λεωφόρους των πληροφοριών και, κατά συνέπεια, για να χρησιμοποιεί αποτελεσματικά τα δεδομένα του Διαδικτύου. Είναι επομένως βασικός στόχος της εκπαίδευσης των νέων ανθρώπων, πολιτών της κοινωνίας της πληροφορίας. Μάλιστα λέγεται ότι σήμερα ένας δωδεκάχρονος μαθητής μπορεί να συγκεντρώσει σήμερα σε πολύ μικρό χρόνο τόσες πληροφορίες, όσες θα συγκέντρωνε ένας ερευνητής του μεσαίωνα σε όλη του την ζωή.

3.5 Βασικοί κανόνες σωστής αναζήτησης

Υπάρχουν τρεις βασικοί κανόνες οι οποίοι καθορίζουν έναν συγκεκριμένο τρόπο συμπεριφοράς του χρήστη και συμβάλλουν στη σωστή αναζήτηση, έτσι ώστε να αποφεύγεται η προσπέλαση σε ακατάλληλο υλικό ή να ελαχιστοποιούνται οι συνέπειες όταν αυτό έχει συμβεί. Κάθε κανόνας αναφέρεται σε γνώση και δεξιότητες:

α. Διάβασε, σκέψου και μετά κάνε κλικ.

Οι χρήστες πρέπει να γνωρίζουν ότι όταν ερευνούν στο Διαδίκτυο μια αποδεκτή λέξη, τα αποτελέσματα μπορεί να τους οδηγήσουν σε εντελώς ακατάλληλες ιστοσελίδες. Ακόμη και μια απλή αναζήτηση μπορεί να δώσει τέτοια αποτελέσματα που να είναι ολοφάνερο κάτι τέτοιο.

Το πρόβλημα είναι ότι οι χρήστες συχνά κάνουν κλικ στα αποτελέσματα της αναζήτησης χωρίς να διαβάσουν την περιγραφή. Η συμπεριφορά ενέχει κινδύνους. Έτσι είναι σημαντικό να ξέρει κάποιος ότι, πριν κάνει κλικ σε ένα από τα

αποτελέσματα της αναζήτησης, πρέπει να διαβάσει προσεκτικά την περιγραφή των αποτελεσμάτων. Αν η περιγραφή αυτή δεν ανταποκρίνεται σε αυτό που αναζητούν ή αν δεν είναι σίγουροι που θα τους οδηγήσει ο δεσμός, τότε δεν πρέπει να κάνουν το επιλέξουν.

β. Πληκτρολόγησε, έλεγξε και μετά κάνε κλικ.

Πολλοί από τους πιθανούς εισβολείς σε υπολογιστικά συστήματα χρησιμοποιούν διευθύνσεις του Διαδικτύου οι οποίες είναι σχεδόν όμοιες με τις νόμιμες και χρήσιμες, ελπίζοντας να ξεγελάσουν ανθρώπους και να επισκεφτούν πορνογραφικές ιστοσελίδες.

Έτσι οι χρήστες συχνά πληκτρολογούν μια διεύθυνση και μετά κάνουν κλικ για να την επισκεφτούν, χωρίς να ελέγξουν αν πληκτρολογήθηκε σωστά. Πρέπει λοιπόν να αποκτήσουν την συνήθεια να πληκτρολογούν τη διεύθυνση, στην συνέχεια να ελέγχουν το τι έχουν γράψει και να σιγουρευτούν αν την έγραψαν σωστά, και μετά να κάνουν κλικ.

Επίσης είναι πολύ σημαντικό οι χρήστες να να γνωρίζουν ότι δεν είναι σωστό να προσπαθούν να μαντέψουν μια διεύθυνση γιατί υπάρχει πιθανότητα να βρεθούν σε δικτυκό τόπο που δεν είναι ασφαλής. Αν δεν γνωρίζουν την διεύθυνση με ακρίβεια, σωστό είναι η χρήση μηχανής αναζήτησης.

γ. Κλείσε και συζήτησε.

Συνήθως οι χρήστες είναι πολύ πιθανόν παρά τις προσπάθειές τους για το αντίθετο να βρεθούν σε λάθος ιστοσελίδα. Έτσι θα πρέπει να γνωρίζουν ότι μερικές φορές αυτοί οι δικτυακοί τόποι χρησιμοποιούν αυτό που λέμε «ποντικοπαγίδα».

Στις περιπτώσεις αυτές απενεργοποιούν το κουμπί «πίσω», ανοίγουν πολλαπλά παράθυρα ή χρησιμοποιούν άλλες τεχνικές για να «παγιδεύσουν» τους χρήστες στον χώρο τους. Αν ένας χρήστης βρεθεί σε έναν τέτοιο χώρο, η πρώτη του αντίδραση είναι ο εκνευρισμός, γιατί δε θα μπορεί να φύγει από εκεί με συνέπεια τον φόβο ή ακόμα και τη περιέργεια και αυτή η αντίδραση είναι και η πιο επικίνδυνη.

Για να μην συμβούν τα χειρότερα, οι χρήστες πρέπει να ξέρουν ότι θα πρέπει να κλείσουν αμέσως τον φυλλομετρητή. Και αν δεν μπορούν να το κάνουν, να κλείσουν τον υπολογιστή. Επίσης είναι σημαντικό να ελεγχούν τα αρχεία με τα

cookies του φυλλομετρητή, που έχει προσπελάσει ακατάλληλη ιστοσελίδα. Δηλαδή θα πρέπει να ελεγχθεί για να βεβαιωθεί ότι δεν έχουν τοποθετηθεί ανεπιθύμητα cookies στον υπολογιστή.

3.6 Ασφάλεια στην ηλεκτρονική αλληλογραφία

Το ηλεκτρονικό ταχυδρομείο αποτελεί μια από τις πιο δημοφιλείς υπηρεσίες του Διαδικτύου προσφέροντας οικονομική, ταχύτατη και αξιόπιστη επικοινωνία με εκατομμύρια ανθρώπους σε ολόκληρο τον κόσμο. Διατίθεται συνήθως από τις εταιρείες παροχής σύνδεσης με το Internet ως πρόσθετη υπηρεσία και συνοδεύεται από ιδιαίτερο κωδικό. Οι χρήστες μπορούν να ανταλλάσσουν μεταξύ τους μηνύματα, στα οποία είναι δυνατόν να επισυνάπτονται αρχεία κάθε τύπου. Τα μηνύματα αυτά ξεκινούν από τον υπολογιστή του αποστολέα και, μέσω των δαιδαλωδών διαδρομών του Διαδικτύου, φτάνουν στον παραλήπτη σε διάστημα λίγων λεπτών.

Ωστόσο ο χρήστης του ηλεκτρονικού ταχυδρομείου πρέπει να είναι ιδιαίτερα προσεκτικός και να λαμβάνει αυξημένα μέτρα προστασίας, καθώς η ευρύτατη διάδοσή του και χρήση του το καθιστούν μια από τις πιο ευάλωτες υπηρεσίες του Διαδικτύου απέναντι σε κακόβουλους χρήστες. Είναι σημαντικό να διαχειριζόμαστε τη διεύθυνση της ηλεκτρονικής μας αλληλογραφίας με την ίδια προσοχή που διαχειριζόμαστε τον αριθμό του τηλεφώνου μας.

Μερικά από τα σημαντικότερα προβλήματα που μπορεί να αντιμετωπίσει ένας χρήστης ηλεκτρονικού ταχυδρομείου είναι τα παρακάτω:

3.7 Ιοί στο Ηλεκτρονικό Ταχυδρομείο

Η μετάδοση ιών μέσω ηλεκτρονικού ταχυδρομείου είναι και ο συνηθέστερος τρόπος διάδοσής τους. Οι ιοί επικολλώνται συνήθως στα συνημμένα αρχεία των μηνυμάτων και μολύνουν τον υπολογιστή του χρήστη, μόλις αυτός ανοίξει το συνημμένο αρχείο.

Δε θα πρέπει λοιπόν οι χρήστες να ανοίγουν ποτέ μηνύματα τα οποία προέρχονται από άγνωστο αποστολέα, ιδιαίτερα αν αυτά περιέχουν συνημμένα αρχεία (συνήθως με κατάληξη .exe, .com, .vbs, .dll, .sh, .bat κ.ά), ενώ πιθανόν να περιέχουν καταστροφικό κώδικα (μήνυμα μορφής .html) που ενεργοποιείται αυτόματα με την ανάγνωση του email.

Θα πρέπει να είναι ιδιαίτερα επιφυλακτικοί ακόμα και απέναντι σε μηνύματα που προέρχονται από γνωστό αποστολέα, αλλά με ύποπτο θέμα. Για αυτό το λόγο είναι καλό να απενεργοποιείται η προεπισκόπηση στα εισερχόμενα μηνύματα, ώστε αυτά να μην ανοίγουν αυτόματα (στο outlook express επιλέξτε Προβολή->Διάταξη->απενεργοποίηση του «εμφάνιση παραθύρου προεπισκόπησης»).

Σε κάθε περίπτωση επιβάλλεται ο έλεγχος της αλληλογραφίας (εισερχόμενης και εξερχόμενης) από ένα καλό αντιβιοτικό πρόγραμμα, το οποίο θα ενημερώνεται συνεχώς.

3.8 Ενοχλητική αλληλογραφία (spam mail)

Όπως αναφέραμε τολ spam ή junk mail είναι μηνύματα με ενοχλητικό ή και δυσάρεστο για τον παραλήπτη περιεχόμενο. Στα spam mail συγκαταλέγονται ανεπιθύμητες διαφημίσεις για προϊόντα, υπηρεσίες και ιστοχώρους, καθώς επίσης και διάφοροι άλλοι τύποι e-mail (π.χ.ανεπιθύμητα newsletters). Τα μηνύματα αυτά αποτελούν μία πρακτική που απαγορεύεται από την Δεοντολογία του Internet και από τις νομοθεσίες των περισσότερων ευρωπαϊκών κρατών. Αυτό συμβαίνει γιατί τίθεται σε κίνδυνο η ασφάλεια των προσωπικών δεδομένων των χρηστών του Internet και κινδυνεύει η ασφάλεια των δικτύων.

Ο χρήστης θα πρέπει να προσέχει ιδιαίτερα να μην απαντάει σε μηνύματα τέτοιου είδους, ούτε και σε αυτά με την ένδειξη "remove me from the mailing list", τα οποία αντί να αποσύρουν την ηλεκτρονική του διεύθυνση, όπως υπόσχονται, επιβεβαιώνουν ότι είναι ενεργή και συνεχίζουν να βομβαρδίζουν τα εισερχόμενα του χρήστη με μεγαλύτερη συχνότητα.

Μία αντιμετώπηση είναι η χρήση φίλτρων που προσφέρουν τα περισσότερα web mail για να διαγράφει τα μηνύματα αυτά, ή να ρυθμίσει κατάλληλα το πρόγραμμα διαχείρισης αλληλογραφίας του υπολογιστή του (συνηθέστερα το outlook express), μέσω των επιλογών που δίνονται από τις καρτέλες στο μενού του προγράμματος.

Στο Διαδίκτυο υπάρχουν σειρά από προγράμματα καταπολέμησης των spam mails, τα οποία μπορούν να εγκατασταθούν τοπικά και να ελέγχουν την εισερχόμενη αλληλογραφία του χρήστη.

3.9 Μηνύματα απατηλού περιεχομένου (hoaxes)

Τα μηνύματα αυτά ουσιαστικά είναι μηνύματα ενοχλητικού τύπου και συνήθως είναι:

«Προειδοποιητικά»: είτε ειδοποιούν στο χρήστη για την ύπαρξη ιού ή άλλου τύπου απειλής στο λειτουργικό του σύστημα και τον συμβουλεύουν να προβεί σε ορισμένες ενέργειες, είτε προειδοποιούν για πιθανές επιθέσεις από ιούς, που στην πραγματικότητα δεν αποτελούν απειλή για το σύστημα

«Συμπαράστασης»: παρουσιάζουν υποθετικά προβλήματα κάποιου ανθρώπου (συχνότατα αναφορές σε παιδιά που πάσχουν από σοβαρές ασθένειες) και ζητούν την κινητοποίηση όσο περισσότερων χρηστών γίνεται

«Εκφοβισμού» : οποιουδήποτε τύπου αλυσιδωτές επιστολές που εκφοβίζουν το χρήστη ότι θα του συμβεί κάτι αν δεν προωθήσει το μήνυμα και σε άλλους χρήστες.

Ο κίνδυνος από αυτά τα μηνύματα είναι κυρίως η τεράστια διάδοσή τους και, κατά συνέπεια, η επιβάρυνση των λογαριασμών των χρηστών με άχρηστα μηνύματα. Εκτός αυτού, δημοσιοποιούνται ευρέως και πολλές διευθύνσεις ηλεκτρονικού ταχυδρομείου, καθιστώντας τους ιδιοκτήτες τους ευκολότερα θύματα για περισσότερες παρενοχλήσεις.

Συνήθως τα μηνύματα αυτού του τύπου συνοδεύονται συχνά από φράσεις «στείλτε αυτό το μήνυμα σε όσο περισσότερους χρήστες γνωρίζετε». Στην περίπτωση των «προειδοποιητικών» μηνυμάτων εμφανίζονται ως αποστολείς μεγάλες και γνωστές εταιρείες, με σκοπό να ξεγελάσουν το χρήστη και να τον κάνουν να εμπιστευτεί το περιεχόμενο του μηνύματος.

Είναι σημαντικό ο χρήστης να αγνοήσει όλα τα μηνύματα τέτοιου τύπου, να τα διαγράψει χωρίς φόβο και, κυρίως, να μην τα προωθήσει σε γνωστούς του. Τα γνωστά αντιβιοτικά προγράμματα συνήθως φιλτράρουν τα καταγεγραμμένα μηνύματα αυτού του είδους, ενώ είναι αρκετές οι εταιρείες ζητούν από τους χρήστες των προγραμμάτων τους να τις ενημερώνουν όταν δέχονται τέτοιου είδους μηνύματα, για να προβούν στις κατάλληλες ενέργειες ενημέρωσης των αντιβιοτικών τους προγραμμάτων.

3.10 Προστασία προσωπικών δεδομένων

Είναι σημαντικό να γνωρίζουμε ότι ο χρήστης των προγραμμάτων αλληλογραφίας πρέπει να είναι ιδιαίτερα προσεκτικός και να μην αναφέρει ποτέ σε μηνύματα προσωπικά του στοιχεία, καθώς και αριθμούς πιστωτικών καρτών ή οποιαδήποτε άλλα δεδομένα. Τα emails αποτελούν έναν από τους συνηθέστερους στόχους των κάθε είδους hackers, οι οποίοι μπορούν να υποκλέψουν όλα τα στοιχεία. Γενικά είναι καλό να αλλάζει τακτικά ο κωδικός πρόσβασης του λογαριασμού email.

Μάλιστα ιδιαίτερη προσοχή χρειάζεται η διαχείριση λογαριασμών web mail, οι οποίοι είναι πολύ πρακτικοί και διαθέσιμοι από παντού, αλλά ταυτόχρονα έχουν χαμηλό δείκτη προστασίας προσωπικών δεδομένων. Για την είσοδο σε αυτούς τους λογαριασμούς συχνά παρέχεται επιλογή για απομνημόνευση του ονόματος χρήστη και του κωδικού στον υπολογιστή, ώστε ο χρήστης να μην πληκτρολογεί κανένα από τα στοιχεία του κάθε φορά που συνδέεται από τον ίδιο υπολογιστή ("Απομνημόνευση του ID μου σε αυτό τον υπολογιστή"). Εδώ φυσικά δεν ενεργοποιείται η παραπάνω επιλογή.

3.11 Ασφάλεια κατά την άμεση συνομιλία (chat)

Το chat στο Διαδίκτυο είναι ένας τρόπος άμεσης επικοινωνίας ενός συνόλου ανθρώπων, οι οποίοι βρίσκονται συγκεντρωμένοι σε έναν συγκεκριμένο δικτυακό χώρο που ονομάζεται «δωμάτιο επικοινωνίας» (chat room) και πληκτρολογούν ο ένας στον άλλο μηνύματα κειμένου ή χρησιμοποιούν μικρόφωνο και κάμερα για ζωντανή συνομιλία. Το chat αποτελεί μια κοινωνική δραστηριότητα ιδιαίτερα δημοφιλή ανάμεσα στους νέους, διότι τους προσφέρει έναν εύκολο και ανέξοδο τρόπο γνωριμίας με ανθρώπους απ όλον τον κόσμο.

Η συζήτηση αυτή μπορεί να πραγματοποιηθεί είτε σε ιστοχώρους του Διαδικτύου χωρίς να χρειαστεί η εγκατάσταση κάποιου προγράμματος, είτε εγκαθιστώντας το κατάλληλο λογισμικό(όπως στην περίπτωση του δημοφιλούς IRC). Στα περισσότερα δωμάτια επικοινωνίας η πρόσβαση είναι ελεύθερη και μπορεί ο καθένας, χρησιμοποιώντας απλά ένα ψευδώνυμο, να παρακολουθεί ή να συμμετέχει σε συζητήσεις. Υπάρχει ωστόσο και η δυνατότητα «ιδιωτικής συνομιλίας», όταν κάποιοι από τα μέλη της ομάδας αποφασίζουν να απομονωθούν από τους άλλους σε ένα ιδιαίτερο «δωμάτιο» και να επικοινωνούν μόνο μεταξύ τους.

Η χρήση των ψευδωνύμων επιτρέπει στους χρήστες να διατηρούν την ανωνυμία τους. Αυτή ακριβώς η δυνατότητα, μαζί με την ψευδαίσθηση του παιδιού-χρήστη ότι είναι ασφαλές, επειδή βρίσκεται στο φυσικό χώρο του σπιτιού του, του σχολείου του ή ενός ιντερνετ-καφέ, μπορεί να μετατρέψει τον τρόπο αυτό της επικοινωνίας σε μια από τις μεγαλύτερες και πιο επικίνδυνες παγίδες του Διαδικτύου. Υπάρχουν συχνά καταγγελίες παιδιών ότι, κατά τη διάρκεια τέτοιου είδους συνομιλιών, έχουν υποστεί λεκτική ή σεξουαλική παρενόχληση, ενώ έχουν δεχτεί από αγνώστους προτροπές για συνάντηση σε πραγματικό χώρο. Σε χώρες του εξωτερικού έχουν παρουσιασθεί έως τώρα δεκάδες περιπτώσεις παιδιών που εξαφανίσθηκαν, έπεσαν θύματα παιδοφίλων ή κυκλωμάτων παιδικής πορνογραφίας, ή παρασύρθηκαν από αγνώστους τους οποίους «συνάντησαν» σε δωμάτια επικοινωνίας. Ένα από τα σημαντικότερα προβλήματα είναι και η έλλειψη γνώσεων σχετικά με αυτόν τον τρόπο επικοινωνίας, τόσο από τους γονείς, όσο και από τους εκπαιδευτικούς.

Και μόνο η συμμετοχή σε τέτοιου είδους χώρους αποτελεί από μόνη της μια επικίνδυνη πρακτική. Σε περίπτωση όμως που δε μπορούν οι γονείς να αποτρέψουν ή να ελέγξουν τα παιδιά τους, οφείλουν τουλάχιστον να τους επιστήσουν την προσοχή, γιατί αυτά συχνά ξεγελιούνται και αποκαλύπτουν πολλά προσωπικά τους στοιχεία σε αγνώστους, οι οποίοι καταφέρνουν να κερδίσουν την εμπιστοσύνη τους.

Οι συμμετέχοντες σε τέτοιου είδους συνομιλίες δε θα πρέπει με κανέναν τρόπο να αποκαλύπτουν την ταυτότητά τους, ούτε τα προσωπικά τους στοιχεία (διεύθυνση, αριθμό τηλεφώνου, e-mail, όνομα σχολείου, πόλη), να μη δέχονται ποτέ να στείλουν τη φωτογραφία τους σε αγνώστους, ούτε να τους συναντούν σε πραγματικό χώρο. Επίσης, οφείλουν να γνωρίζουν πως σε καμιά περίπτωση δεν είναι ασφαλείς λόγω της ανωνυμίας τους. Ένας καλός χρήστης του Διαδικτύου είναι σε θέση να εντοπίσει την IP διεύθυνση του υπολογιστή τους, να αποκτήσει πρόσβαση σε προσωπικά τους αρχεία, να μολύνει τον υπολογιστή τους με ιούς ή σκουλήκια, τα οποία συχνότατα κυκλοφορούν σε τέτοιου είδους χώρους.

Τα παιδιά θα πρέπει να ενθαρρύνονται να συζητούν με τους γονείς τους για τις συνομιλίες τις οποίες παρακολουθούν μέσα σε chat-rooms, να μιλάνε για τους νέους φίλους τους, όπως θα έκαναν και για τους φίλους που γνωρίζουν στην πραγματική τους ζωή, να αναφέρουν κάθε περίπτωση κατά την οποία έχουν υποστεί παρενόχληση, οποιουδήποτε είδους. Οι γονείς, με τη σειρά τους, θα πρέπει να

προτρέπουν τα παιδιά τους να χρησιμοποιούν αυτή τη δυνατότητα του Διαδικτύου για να επικοινωνήσουν με φίλους τους που βρίσκονται μακριά και τους οποίους τα παιδιά ήδη γνωρίζουν, και όχι ως μέσο νέων γνωριμιών.

3.12 Ο διαμοιρασμός αρχείων στο Διαδίκτυο

Ο διαμοιρασμός αρχείων στο Διαδίκτυο αποτελεί μια δυνατότητα, του Διαδίκτυου να διαμοιράζονται αρχεία κάθε είδους. Πραγματοποιείται με προγράμματα (ελεύθερα ή με πληρωμή) όπως τα παρακάτω:

Προγράμματα για Windows: Aimster, Audio Galaxy, Bearshare, Gnotella, Gnucleus, Grokster, iMesh, KaZaa, Limewire, Morpheus, SwapNut, WinMX, Torrents

Ουσιαστικα τα παραπάων προγράμματα λειτουργούν έτσι ώστε να κάνουν κοινόχρηστο ένα μέρος του σκληρού δίσκου του τοπικού υπολογιστή, σε όλους χρήστες, οι οποίοι τελικά είναι συνδεδεμένοι στο Διαδίκτυο και χρησιμοποιούν το ίδιο πρόγραμμα.

Έτσι κάθε μέλος της ιδιότυπης αυτής κοινότητας μπορεί να αναζητεί αρχεία στους υπολογιστές των μελών της και να δημιουργεί ένα αντίγραφο οποιουδήποτε από αυτά τα αρχεία, στον δικό του υπολογιστή.

Κατά την αντιγραφή των αρχείων υπάρχει απευθείας, σύγχρονη επικοινωνία μεταξύ υπολογιστών. Τα προγράμματα αυτά ονομάζονται προγράμματα ομότιμης σύνδεσης (peer-to-peer) προγράμματα.

Η ευρύτατη χρήση της δυνατότητας αυτής του Διαδικτύου οφείλεται στην μεγάλη ευκολία εύρεσης και τοπικής αποθήκευσης κάθε είδους αρχείου (μουσικής, εικόνων, προγραμμάτων) με μηδαμινό κόστος για τον χρήστη. Η συγκέντρωση των ταυτόχρονα διασυνδεδεμένων χρηστών σε κάθε τέτοιο πρόγραμμα διαμοιρασμού αρχείων ανέρχεται σε μερικά εκατομμύρια. Δημιουργούνται έτσι μερικές από τις μεγαλύτερες διαδικτυακά πληθυσμιακές κοινότητες, μέσα στις οποίες διακινείται σχεδόν ανεξέλεγκτα κάθε είδους υλικό.

Οι κίνδυνοι, από την χρήση προγραμμάτων διαμοιρασμού αρχείων στο Διαδίκτυο, αφορούν κυρίως στα εξής:

Ασφάλεια

Είναι σημαντικό να γνωρίζουμε ότι η χρήση των προγραμμάτων διαμοιρασμού αρχείων παραβιάζει τους κανόνες «υγιεινής» του υπολογιστή μας. Δηλαδή το να μοιραζόμαστε «πράγματα» με χρήστες που δεν τους γνωρίζουμε και δεν τους εμπιστευόμαστε αποτελεί πολύ μεγάλο κίνδυνο. Έτσι ο υπολογιστή μας κινδυνεύει από ιούς και άλλα καταστροφικά προγράμματα που διαχέονται στον υπολογιστή μας και τον μολύνουν.

Πρόσβαση των παιδιών σε πορνογραφικό υλικό

Προσοχή για τα παιδιά έχει και η ποιότητα των αρχείων που χρησιμοποιούμε . Τα περισσότερα από τα προγράμματα διαμοιρασμού αρχείων στο Διαδίκτυο επιτρέπουν την πρόσβαση ανήλικων σε ακατάλληλα βίντεο ή εικόνες. Αυτό μπορεί να γίνει και με απλό τρόπο καθώς τα παιδιά αναζητούν την αγαπημένη τους μουσική ή παιχνίδια μπορεί αθέλητα να γίνουν παραλήπτες πορνογραφικού υλικού, απλά επειδή αυτό περιέχει τις ίδιες λέξεις-κλειδιά με τις οποίες γίνεται η αναζήτηση. Υπάρχουν προγράμματα ελέγχου της πλοήγησης, συμπεριλαμβανομένου και αυτού του σχολικού δικτύου. Παρόλα αυτά δεν πάντα αποτελεσματικά όταν η διακίνηση του ακατάλληλου υλικού γίνεται μέσα από προγράμματα διαμοιρασμού.

Νομικά προβλήματα

Προσοχή θέλει και η νομική πλευρά των αρχείων που διαθέτουμε. Τα περισσότερα αρχεία, που είναι διαθέσιμα μέσα από τα προγράμματα διαμοιρασμού (βίντεο, μουσική, τραγούδια, βιντεοπαιχνίδια), έχουν προστατευμένα δικαιώματα. Ο νόμος προστατεύει το δικαίωμα του ιδιοκτήτη και επιβάλλει περιορισμούς στην αντιγραφή και την διακίνηση του προϊόντος.

Έτσι πρέπει ο χρήστης να γνωρίζει ότι η απόκτηση (download) και η διάθεση (upload) προϊόντων χωρίς την άδεια του ιδιοκτήτη μπορεί να προκαλέσει νομικά προβλήματα. Η ανωνυμία δεν είναι ποτέ απόλυτα δεδομένη στο Διαδίκτυο. Σε αρκετές περιπτώσεις υπήρξαν διώξεις «πειρατών», που διακινούσαν παράνομα αρχεία μουσικής, video ή βιβλία.

Προσωπικά δεδομένα

Θέλει προσοχή στις ρυθμίσεις των προγράμματων διαμοιρασμού αρχείων. Αυτό γιατί αν γίνει κοινόχρηστος ολόκληρος ο σκληρός δίσκος του τοπικού υπολογιστή, τότε προσωπικά δεδομένα, που πιθανόν έχετε στον υπολογιστή σας όπως αριθμοί πιστωτικών καρτών ή φορολογικά δεδομένα, θα εκτεθούν σε όλους τους χρήστες που χρησιμοποιούν το πρόγραμμα αυτό.

ΚΕΦΑΛΑΙΟ 4: ΠΡΟΓΡΑΜΜΑΤΑ ΠΡΟΣΒΟΛΗΣ ΕΝΟΣ ΥΠΟΛΟΓΙΣΤΗ

4.1. Ιός

Η ύπαρξη ιών είναι ένα από τα σημαντικότερα προβλήματα του Διαδικτύου. Υπάρχουν σήμερα χιλιάδες διαφορετικοί ιοί, οι οποίοι προσβάλλουν εκατομμύρια υπολογιστών σε όλον τον κόσμο.

Ο ιός του υπολογιστή είναι ένα κομμάτι προγράμματος, το οποίο αντιγράφει τον εαυτό του και επισυνάπτεται σε ένα νομότυπο πρόγραμμα με σκοπό να «μολύνει» άλλα προγράμματα.

Όταν το μολυσμένο πρόγραμμα εκτελεστεί (το λεγόμενο «άνοιγμα μολυσμένου αρχείου»), κάτω από ορισμένες συνθήκες, προσπαθεί να μολύνει και άλλα προγράμματα, να διαγράψει, να αλλάξει ή να κρυπτογραφήσει αρχεία. Πολλοί έχουν τη δυνατότητα να μεταλλάσσονται και να διαφέρουν σε μεγάλο βαθμό από τον αρχικό ιό.

Σε περίπτωση που μιλάμε για υπολογιστές δικτύων, η καταστροφή έχει ακόμα μεγαλύτερες διαστάσεις, καθώς μολύνονται και καταρρέουν αρχεία εταιρειών, πανεπιστημίων, υπουργείων, ακόμα και κυβερνήσεων.

4.2. Δούρειος Ίππος (Trojan horse)

Ο δούρειος Ίππος αποτελεί ένα πρόγραμμαμα το οποίο δεν αναπαράγεται και αλλά δρα «υπογείως», χωρίς ο χρήστης του υπολογιστή να αντιλαμβάνεται αρχικά την ύπαρξή του. Το πρόγραμμα αυτό ενεργεί ως μέσο μεταφοράς άλλων μορφών επιβλαβούς λογισμικού (malware), και ενεργοποιείται σε συγκεκριμένο χρόνο και δημιουργεί ένα αντίγραφο του αυθεντικού προγράμματος που χρησιμοποιείται από το χρήστη, το οποίο θα δουλεύει κανονικά, σα να ήταν το αυθεντικό.

Έτσι όταν ο χρήστης εκτελεί το συγκεκριμένο πρόγραμμα τότε χρησιμοποιείται η έκδοση του Δούρειου Ίππου, ο οποίος δρα καταστροφικά ή κατασκπευτικά

4.3. Σκουλήκια (worms)

Τα σκουλήκια αποτετελούν προγράμματα τα οποία αντιγράφουν τον εαυτό τους σε δίκτυα Η/Υ. Έτσι χρησιμοποιούν το Internet ως μέσο διάδοσής τους (emails, irc chat κ.ά.) και αναπαράγονται από υπολογιστή σε υπολογιστή, εκμεταλλευόμενα τα σφάλματα των λειτουργικών προγραμμάτων των υπολογιστών. Έτσι οι μολυσμένοι υπολογιστές μετά από κάποιο χρονικό διάστημα γεμίζουν από μολισμένα αντίγραφα και δε μπορούν να λειτουργήσουν.

4.4 Τρόποι μετάδοσης

Οι τρόποι μετάδοσης μολισμένου λογισμικού γίνονται με ένα από τα παρακάτω μέσα:

- Από μολυσμένο εξωτερικό μέσω αποθήκευσης όπως CD, DVD, Flash Driver κ.α.
- Από εκτέλεση ή άνοιγμα μολυσμένων αρχείων του υπολογιστή
- Από εκτέλεση ή άνοιγμα μολυσμένων αρχείων που επισυνάπτονται σε μηνύματα ηλεκτρονικής αλληλογραφίας
- Από άνοιγμα ή ανάγνωση αγνώστων μηνυμάτων ηλεκτρονικής αλληλογραφίας που περιέχουν καταστροφικό κώδικα (malicious code)
- Από άνοιγμα ή ανάγνωση μολυσμένων ιστοσελίδων .htm και .html

4.5 Τρόποι προστασίας

Οι συνήθεις τρόποι προστασίας από μολυσμένο λογισμικό είναι οι παρακάτω:

- Επιλογή ενός καλού αντιβιοτικού προγράμματος
- Τακτική ανίχνευση όλου του δίσκου με το αντιβιοτικό σας πρόγραμμα
- Συνεχής ανανέωση (update) του αντιβιοτικού προγράμματος
- Έλεγχος κάθε δισκέτας/cd με το αντιβιοτικό σας πρόγραμμα πριν την ανοίξετε.

- Τήρηση αντιγράφων ασφαλείας όλων των αρχείων σας σε cd ή δισκέτα.
- Συχνές επισκέψεις στην τοποθεσία των κρίσιμων ενημερώσεων των Windows (το πιο ευάλωτο λειτουργικό) όπου προσφέρονται δωρεάν προγράμματα (patches) διόρθωσης/κάλυψης των πιθανών ελλείψεων του λειτουργικού σας.
- Ανίχνευση μέσω του αντιβιοτικού κάθε νέου αρχείου που «κατεβάζετε» από το Internet.
- Αν χρησιμοποιείτε irc chat, απενεργοποιείστε την επιλογή αυτόματης αποδοχής αρχείων και αυτόματης εκτέλεσης των αρχείων που σας στέλνουν.
- Επιλέξτε την πλήρη εμφάνιση των τύπων αρχείων στον Η/Υ σας. Ίσως κάποιος να σας στείλει μια «φωτογραφία» ως photo.jpg.vbs. Αν δεν έχετε την παραπάνω επιλογή ενεργοποιημένη, θα εκτελέσετε το αρχείο το οποίο θα περιέχει κάθε άλλο παρά φωτογραφία.
- Διατηρείτε και ανανεώνετε συχνά μια δισκέτα για αποκατάσταση ζημιών από ιούς, την οποία προσφέρουν συνήθως τα ίδια τα αντιβιοτικά προγράμματα.
- Εδώ πρέπει να επισημανθεί πως όσο πιο αυστηρές ρυθμίσεις ασφαλείας ενεργοποιείτε στον υπολογιστή σας, τόσο πιο δύσκολα έχετε πρόσβαση σε σελίδες του Διαδικτύου. Η συνήθης ρύθμιση ασφαλείας στους φυλλομετρητές είναι η «μεσαία».

4.6 Αντιμετώπιση μόλυνσης

Ανάλογα την περίπτωση μόλυνσης μπορούμε να κάνουμε τα παρακάτω προκειμένου να αποκαταστήσουμε την βλάβη.

- Αν υπάρχει μόλυνση από από ιό και υπάρχει εγκατεστημένο αντιβιοτικό πρόγραμμα, κάνουμε πάλι πλήρη έλεγχο όλου των δίσκων και δικτυακών πόρων (full system scan). Αν βρεθεί ιός, τότε φυσιολογικά το αντιβιοτικό θα προβεί αυτόματα στις κατάλληλες ενέργειες, είτε διαγράφοντάς τον, είτε απομονώνοντάς τον από το υπόλοιπο σύστημα.
- Αν το αντιβιοτικό αδυνατεί να αποκαταστήσει τη ζημιά, δεν διαγράφουμε κανένα μολυσμένο αρχείο αλλά ελέγχουμε τα μολυσμένα αρχεία με κάποιο άλλο πρόγραμμα αποκατάστασης που πιθανά υπάρχει.

  Αυτό συνήθως γίνεται με μια αρχική προσπάθεια να βρεθεί (συνήθως από το Διαδίκτυο) το πρόγραμμα απομάκρυνσης του συγκεκριμένου ιού (removal tool) κάνοντας κατάλληλη αναζήτηση και, αφού το κατεβάσουμε σε ένα ξεχωριστό

εξωτερικό μέσω αποθήκευσης το εκτελούμε στον υπολογιστή μας πάνω από μία φορά.

- Σε περίπτωση που ούτε το ειδικό πρόγραμμα απομάκρυνσης δεν μπορεί να «καθαρίσει» τον υπολογιστή τότε πρέπει ο υπολογιστής να βγει εκτός δικτύου για προστασία και τον πιθανών άλλων συσκευών που υπάρχουν σε αυτό και πιθανά να χρειαστεί format. Σε αυτήν την περίπτωση πρέπει να κρατηθούν κατάλληλα αντίγραφα όλων των προγραμμάτων που υπάρχουν στον υπολογιστή ώστε να μην υπαρχει απώλεια πληροφορίας.

Γνωστές εταιρείες προσφέρουν τη δυνατότητα ελέγχου και απομάκρυνσης των ιών του υπολογιστή σας on-line. Τέτοιες διευθύνσεις είναι:

- Trend micro
- Ravantivirus
- Symantec

Γνωστά αντιβιοτικά προγράμματα (στις σελίδες των προγραμμάτων αυτών προσφέρονται συνήθως και τα removal tools της κάθε εταιρείας) :

AVG

- AVK
- Kaspersky
- McAfee
- Norton
- Panda
- Trendmicro pc cillin

ΒΙΒΛΙΟΓΡΑΦΙΑ

1. Safeline, www.safeline.gr
2. Ευρωπαϊκή Επιτροπή, Safer Internet Programme: Empowering and Protecting Children Online, http://ec.europa.eu/information_society/activities/sip/index_en.htm
3. Κέκκερης Γ., Δέλλας Σ. (2005), Υπεύθυνη και Ασφαλής Χρήση του Διαδικτύου: μια Διδακτική Πρόταση, Πρακτικά 3ου Συνεδρίου των εκπαιδευτικών για την Αξιοποίηση των ΤΠΕ στη διδακτική πράξη, Σύρος
4. Calashain, T., Google Hacks, 100 Industrial-Strength tips and tools, O'Reilly publications, California, 2002.
5. Lawrence, S. – Giles C.L., Searching the World Wide Web, Science, Vol. 280, 3/4/1998. • Γουλτίδης, Χρ., ECDL 4: Εύκολα, Τόμος ΄β, Εκδόσεις Κλειδάριθμος, Αθήνα, 2004.
6. Μπένου, Μ., Σκουλαρίδου, Β., Σπινέλλης, Δ., Οδηγός ασφαλούς πλοήγησης στο Διαδίκτυο, Eltrun White Paper Series, Οικονομικό Πανεπιστήμιο Αθηνών, Αθήνα 2003.
7. Παπαθανασίου, Α. Ε., Στοιχεία Υπολογιστικών Συστημάτων, Εκδόσεις Ευγ. Μπένου, Αθήνα 1998.