ΤΕΙ ΠΑΤΡΑΣ

ΣΧΟΛΗ ΔΙΟΙΚΗΣΗΣ ΚΑΙ ΟΙΚΟΝΟΜΙΑΣ

ΤΜΗΜΑ ΔΙΟΙΚΗΣΗΣ ΕΠΙΧΕΙΡΗΣΕΩΝ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΩΝ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

ΣΠΟΥΔΑΣΤΡΙΑ:

ΜΠΑΡΜΠΟΥΝΗ ΣΤΕΦΑΝΙΑ

ΕΙΣΗΓΗΤΡΙΑ:

ΒΙΣΒΑΡΔΗ ΑΝΑΣΤΑΣΙΑ

ΠΑΤΡΑ ΙΑΝΟΥΑΡΙΟΣ 2009

ΠΕΡΙΕΧΟΜΕΝΑ

ΠΕΡΙΛΗΨΗ

Οι κίνδυνοι που απειλούν την ασφάλεια των πληροφοριών στο διαδίκτυο και τα στοιχεία του, είναι πολλοί και έχουν διάφορες μορφές και αιτίες.

Σε συνδυασμό δε με το ότι το Διαδίκτυο γίνεται όλο και πιο πολύπλοκο, με παράλληλη αύξηση της αλληλεξάρτησης μεταξύ των στοιχείων του, καθιστούν τα θέματα ασφάλειας και προστασίας δύσκολα.

Στην παρούσα εργασία εξετάζονται τα μέσα και οι τρόποι απάτης μέσω του διαδικτύου και οι καταχρήσεις των υπολογιστών, που περιλαμβάνουν την πρόσβαση σε αυτούς χωρίς εξουσιοδότηση, την υπέρβαση της εξουσιοδότησης , όταν έχει δοθεί, καθώς και την διενέργεια επιβλαβών για τους υπολογιστές πράξεων. Χαρακτηριστικές μορφές τέτοιων δραστηριοτήτων αποτελούν η πρόσβαση και η απόκτηση ευαίσθητων πληροφοριών, η πραγματοποίηση εικονικών συναλλαγών, η επέμβαση σε έγγραφα και η καταστροφή προγραμμάτων, αρχείων και εξοπλισμού. Οι ενέργειες αυτές προσφέρουν στο δράστη μεγαλύτερη πρόσβαση σε ευαίσθητες πληροφορίες περιορίζοντας ταυτόχρονα την ακεραιότητα των συστημάτων, που έχουν προσβληθεί καθώς και την ικανότητα τους για την παροχή των υπηρεσιών τους. Ο δράστης μπορεί να είναι ένας εξωτερικός χάκερ ή ένας υπάλληλος που κάνει κακή χρήση των δυνατοτήτων πρόσβασης που έχει στο σύστημα.

Στη συνέχεια θα αναλύσουμε τους τρόπους άμυνας που μπορεί να εφαρμόσει ο καθένας, από τα άτομα και τους διαφόρους οργανισμούς μέχρι τις κυβερνήσεις. Σε ατομική βάση η άμυνα, που ακολουθείται, χρησιμεύει για τη προστασία της ιδιωτικής ζωής, των ατομικών πηγών, της ανταγωνιστικής θέσης και της γενικότερης καλής κατάστασης του συγκεκριμένου ατόμου. Στην περίπτωση των οργανισμών, η άμυνα συμβάλλει στη διατήρηση της ανταγωνιστικότητας τους και στην προφύλαξη των πηγών τους.

Τέλος θα αναφερθούμε στο πως κανείς μπορεί να προστατευθεί νομικά από την επεξεργασία των προσωπικών του πληροφοριών και ταυτόχρονα να διασφαλίζει

την ελεύθερη ροή όσων πληροφοριών δεν επηρεάζουν την προσωπική αρχή και αξιοπρέπεια.

ΕΙΣΑΓΩΓΗ

Τα πληροφοριακά συστήματα είναι πια κοινός τόπος στην καθημερινή ζωή μας. Δεν υπάρχει ανθρώπινη δραστηριότητα που να μην υποστηρίζεται από κάποιο είδος υπολογιστικού συστήματος, ενώ η απίστευτα μεγάλη ροή και συγκέντρωση πληροφοριών, η διεύρυνση των δικτύων επικοινωνίας πληροφοριών και η διαφαινόμενη έξαρση της χρήσης βάσεων πληροφοριών από το σπίτι και από το κινητό τηλέφωνο συνθέτουν την εικόνα "πληροφοριοποιημένης" κοινωνίας. Οι διαστάσεις του φαινομένου είναι μάλιστα τέτοιες που δικαιολογημένα τείνει κανείς να υποθέσει ότι ένα από τα πιο σημαντικά προβλήματα του πλανήτη μας τα επόμενα χρόνια θα είναι η "πληροφοριακή μόλυνση" και η ισχύς που θα αποκτήσουν όσοι "ευφυείς ενδιάμεσοι" θα κάνουν κρίσιμες "επιλογές" για τις πληροφορίες πού θα διανέμονται στους ενδιαφερόμενους χρήστες.

Κάποιοι χαρακτήρισαν το Internet "ηθελημένο χάος", υπονοώντας ότι σκόπιμα αφέθηκε να αποτελεί ένα ανεξέλεγκτο υπόβαθρο ελεύθερης έκφρασης και πληροφόρησης. Η εκτίμηση όμως για τη χρησιμότητα του συνοδεύεται , όλο και πιο συχνά , από τη διατύπωση της ανάγκης κάποιον ρυθμίσεων που θα το "εκλογικεύσουν". Πολλοί επίσης διατείνονται ότι η φαινομενική αυτή ελευθερία διακίνησης πληροφοριών εντείνει το χάσμα ανάμεσα στο στις αναπτυγμένες δυτικές χώρες και τον υπόλοιπο κόσμο, δεδομένου ότι το πληροφοριακό υλικό που διακινείται στο εκτεταμένο αυτό δίκτυο παράγεται, κατά κύριο λόγο, στις ΗΠΑ και τις οικονομικά ισχυρές χώρες της Δυτ. Ευρώπης. Οι μικρές χώρες έχουν την ελευθερία πρόσβασης στο δίκτυο, μόνον που δεν διαθέτουν αξιόλογη "πρώτη ύλη" να προωθηθούν μέσα από αυτό, λειτουργώντας ως καταναλωτές πληροφοριών (συχνά μη ελεγχόμενης αξιοπιστίας), όπως υπήρξαν καταναλωτές προϊόντων πληροφορικής.

Στην καθημερινή ζωή ο σύγχρονος άνθρωπος εξυπηρετείται από εμπειρία συσκευών και συστημάτων αυτόματης επεξεργασίας πληροφοριών. Για

παράδειγμα, συσκευές ιατρικές με ενσωματωμένο υπολογιστή χρησιμοποιούνται για τη διάγνωση ασθενειών και την εκτέλεση θεραπευτικών επεμβάσεων. Αποφάσεις με μεγάλη επαγγελματική και οικονομική σημασία παίρνονται, κυρίως στο Δημόσιο, βασισμένες σε αυτοματοποιημένη επεξεργασία πληροφοριών (σύστημα έκδοσης αποτελεσμάτων πανελληνίων εξετάσεων, προσλήψεις βάσει μορίων, εκκαθάριση δηλώσεων εισοδήματος). Προσωπικές περιουσίες κρίνονται καθημερινά από την πορεία μετοχών στο Χρηματιστήριο, η τιμή των οποίων καθορίζεται από αυτόματη επεξεργασία στοιχείων ζήτησης και προσφοράς κλπ.

Η εξάπλωση δικτύων, όπως το Internet, και η σημασία των αποτελεσμάτων που προκύπτουν από πληροφοριακά συστήματα, όπως αυτά που προαναφέρθηκαν, έχει κάνει ιδιαίτερα αισθητή στις επιχειρήσεις και στα άτομα την ανάγκη διασφάλισης αμεροληψίας και έχει, κατ' επέκταση, αυξήσει σημαντικά το ενδιαφέρον για τα θέματα ασφαλείας των πληροφοριών. Η αξιοπιστία, η ακεραιότητα, η διαθεσιμότητα και η εμπιστευτικότητα των πληροφοριών καθώς και η αποτροπή αθέμιτης ή καταχρηστικής χρήσης πληροφοριακών συστημάτων αποτελούν πλέον κρίσιμα κοινωνικά αιτήματα και προσδοκίες. Για το λόγο αυτό αποτελούν αντικείμενο κοινωνικού προβληματισμού αλλά και συστηματικής επιστημονικής μελέτης και έρευνας. Διεθνείς οργανισμοί ασχολούνται πλέον με τη θέσπιση τυποποιημένων τεχνικών και διαδικασιών ασφάλειας των πληροφοριακών συστημάτων, ενώ πολλά εθνικά κοινοβούλια, διεθνείς οργανισμοί και η Ευρωπαϊκή Ένωση έχουν ρυθμίσει κανονιστικές ρυθμίσεις που διέπουν τη χρήση ευαίσθητων προσωπικών πληροφοριών, που αναφέρονται στο στενό πυρήνα της ιδιωτικής ζωής.

ΚΕΦΑΛΑΙΟ 1 – ΓΕΝΙΚΗ ΕΠΙΣΚΟΠΗΣΗ

1.1 ΓΕΝΙΚΑ

Επιχειρώντας μία αναδρομή σε παλαιότερες εποχές, όταν η πληροφορία και η πληροφόρηση γενικότερα αποτελούσαν προνόμιο των λιγοστών που είχαν τα μέσα να τις αποκτήσουν, μπορούμε ευκολότερα σήμερα να συνειδητοποιήσουμε το αντίκτυπο του Internet στη καθημερινή ζωή μας, όπου όλοι ανεξαιρέτως γινόμαστε πλέον δέκτες εκατοντάδων χιλιάδων μηνυμάτων και πληροφοριών, ειδήσεων και εικόνων που, ηθελημένα ή αθέλητα ,λαμβάνουμε κατά την περιήγηση μας στο κυβερνοχώρο. Η φράση «η πληροφορία προσδίδει δύναμη» έχει χάσει πια την αρχική σημασία της , αφού όλοι όσοι έχουν πρόσβαση στο internet έχουν στη διάθεση τους τη μεγαλύτερη πηγή πληροφοριών που γνώρισε ποτέ η ανθρωπότητα. Το χάσμα ανάμεσα στη πληροφορία και στη γνώση που αυτή συνεπάγεται δείχνει να μεγαλώνει καθημερινά, καθώς ο όγκος των πληροφοριών που άτακτα καθορίζονται καθημερινά στο διαδίκτυο μάλλον δυσχεραίνει παρά διευκολύνει τη πορεία προς την εξερεύνηση ποιοτικών πληροφοριών. Έτσι η πραγματική πρόκληση βρίσκεται ακριβώς στην επιλογή, στην απομόνωση της ποιοτικής πληροφορίας και την ασφάλεια και ακεραιότητα της.

Οι όροι ασφάλεια και ακεραιότητα ακούγονται συχνά μαζί όταν γίνεται αναφορά σε βάσεις δεδομένων, αν και οι δύο έννοιες είναι στην πραγματικότητα εντελώς διαφορετικές. Η ασφάλεια(security) αναφέρεται στη προστασία δεδομένων από τη γνωστοποίηση, την αλλοίωση ή την καταστροφή από μη εξουσιοδοτημένα άτομα. Η ακεραιότητα (integrity) αναφέρεται στην ακρίβεια ή την εγκυρότητα των δεδομένων. Με άλλα λόγια:

- Ø Ασφάλεια σημαίνει να εξασφαλίζεται ότι οι χρήστες επιτρέπεται να κάνουν αυτά που επιχειρούν να κάνουν.
- Ø Ακεραιότητα σημαίνει να εξασφαλίζεται ότι αυτά που επιχειρούν να

κάνουν οι χρήστες είναι σωστά.

1.1.1 ΓΕΝΙΚΑ ΖΗΤΗΜΑΤΑ

Το πρόβλημα της ασφάλειας έχει πολλές πλευρές , μεταξύ των οποίων οι παρακάτω:

- Νομικές ,κοινωνικές και ηθικές πλευρές(για παράδειγμα , το άτομο που υποβάλλει την αίτηση , π.χ. για τη πίστωση ενός πελάτη έχει νομικό δικαίωμα για πρόσβαση στις πληροφορίες που ζητάει;)
- Φυσικοί έλεγχοι (για παράδειγμα ,είναι η αίθουσα του υπολογιστή ή του τερματικού κλειδωμένη ή ασφαλισμένη με κάποιον άλλο τρόπο;)
- Ζητήματα πολιτικής (για παράδειγμα, πως αποφασίζει η επιχείρηση στην οποία ανήκει το σύστημα , σε ποιόν θα επιτρέπεται η πρόσβαση , και σε τι ;)
- Λειτουργικά προβλήματα (για παράδειγμα, αν χρησιμοποιείται ένας μηχανισμός με συνθηματικά ,πως διατηρούνται κρυφά τα ίδια τα συνθηματικά και πόσο συχνά αλλάζουν;)
- Έλεγχοι μέσω του υλικού (για παράδειγμα ,το υποκείμενο λειτουργικό σύστημα σβήνει τα περιεχόμενα της μνήμης και τα αρχεία δεδομένων όταν τελειώσει την εργασία με αυτά;)

  Και τέλος :

- Ζητήματα που αφορούν ειδικά το ίδιο το σύστημα βάσης δεδομένων (για παράδειγμα διαθέτει το σύστημα βάσης δεδομένων κάποια έννοια ιδιοκτησίας δεδομένων;)

1.2 ΠΛΗΡΟΦΟΡΙΑ

Με τον όρο πληροφορία εννοούμε δεδομένα τα οποία έχουν υποστεί μία κάποια επεξεργασία, ώστε να έχουν έννοια για τον αποδέκτη και αξία για τις αποφάσεις που παίρνει ή τις δραστηριότητες που εκτελεί. Όπως μάλιστα αναφέρουν οι Davis και Olson η σχέση που υπάρχει μεταξύ των δεδομένων και των πληροφοριών είναι ίδια με τη σχέση που υπάρχει μεταξύ της πρώτης ύλης και του έτοιμου προϊόντος. Με την επεξεργασία μετατρέπουμε τα δεδομένα από μία μορφή που δεν μπορούν να χρησιμοποιηθούν σε μία άλλη μορφή άμεσης χρησιμοποίησης για τη λήψη αποφάσεων. Η αντιστοιχία των πρώτων υλών προς τα έτοιμα προϊόντα σημαίνει ότι η πληροφορία για ένα πρόσωπο μπορεί να είναι δεδομένα για κάποιο άλλο, όπως τα έτοιμα προϊόντα μιας επιχείρησης μπορεί να είναι η πρώτη ύλη μιας άλλης επιχείρησης , η οποία επιπρόσθετα θα την επεξεργαστεί για να παράγει το τελικό της προϊόν, κ.ο.κ. Για παράδειγμα ,αναφέρουμε της πληροφορίες για τον υπεύθυνο διεκπεραίωσης των παραγγελιών είναι πληροφορία, αλλά ταυτόχρονα αποτελούν δεδομένα για των υπεύθυνο των αποθεμάτων. Λόγω αυτής της σχέσης μεταξύ των δεδομένων και της πληροφορίας είναι σύνηθες να χρησιμοποιούν ορισμένοι τους δύο αυτούς όρους εναλλακτικά.

Από τα προηγούμενα είναι φανερό , ότι τα δεδομένα δεν είναι πληροφορία μέχρι να τεθούν στην κατάλληλη μορφή ώστε να έχουν σημασία για τον συγκεκριμένο αποδέκτη , και ότι η πληροφορία είναι δεδομένα , τα οποία έχουν υποστεί κατάλληλη επεξεργασία για να δώσουν γνώση σε συγκεκριμένο πρόσωπο, ώστε να πάρει τη σωστή απόφαση.

Αξίζει να σημειώσουμε ότι διαφορετικά πρόσωπα μέσα στην ίδια επιχείρηση πιθανόν να χρησιμοποιούν τα ίδια δεδομένα ,για να πάρουν την πληροφόρηση

που θα τους οδηγήσει στη λήψη διαφορετικών αποφάσεων .Πιο συγκεκριμένα στο λειτουργικό επίπεδο διοίκησης τα κατώτερα διευθυντικά στελέχη αποκτούν από τα δεδομένα των συναλλαγών επεξεργασμένες πληροφορίες τις οποίες στη συνέχεια χρησιμοποιούν με βάση συγκεκριμένους κανόνες αποφάσεων, ώστε να πάρουν τις καλύτερες δυνατές αποφάσεις τους. Παραδείγματα τέτοιων αποφάσεων είναι ο προγραμματισμός της εκτέλεσης των παραγγελιών των πελατών για την παραγωγή , η κατανομή των στοιχείων κόστους στα τμήματα και η έκδοση της μισθοδοσίας για το λογιστικό, η επιλογή των διαδρομών για τη διανομή, η διαχείριση των ρευστών διαθέσιμων για το χρηματοοικονομικό, και άλλα πολλά. Όμως συγκεντρωτικά δεδομένα και πληροφορίες του λειτουργικού επιπέδου διοίκησης μπορεί να είναι συγχρόνως δεδομένα για τα διευθυντικά στελέχη της ανώτατης διοίκησης .Τα δεδομένα αυτά μετατρέπονται με την κατάλληλη επεξεργασία σε πληροφορίες για την υποστήριξη των στρατηγικών κυρίως αποφάσεων της ανώτατης διοίκησης.Τέτοιες αποφάσεις είναι,ο σχεδιασμός της παραγωγικής δυναμικότητας για την παραγωγή, οι μακροχρόνιες λογιστικές εκθέσεις για το λογιστικό, η επιλογή των μέσων διακίνησης των προϊόντων για τη διανομή, η πρόβλεψη των μακροχρόνιων χρηματοοικονομικών αναγκών και η επιλογή των πηγών δανεισμού για το χρηματοοικονομικό και άλλες.

1.2.1 ΧΑΡΑΚΤΗΡΙΣΤΚΑ ΠΛΗΡΟΦΟΡΙΩΝ

Από τη μέχρι τώρα ανάλυση είναι φανερό ότι η πληροφορία αυξάνει τη γνώση, περιορίζει την αβεβαιότητα και βοηθάει στη διαδικασία λήψης αποφάσεων. Όμως για να συμβούν αυτά, θα πρέπει οι πληροφορίες , είτε πρόκειται για μεμονωμένες πληροφορίες, είτε για σύνολο πληροφοριών , να έχουν ορισμένα χαρακτηριστικά.

Τα χαρακτηριστικά της μεμονωμένης πληροφορίας είναι:

- Ακρίβεια(Accurancy): Μία πληροφορία μπορεί να είναι αληθινή ή ψευδής, ακριβής ή ανακριβής. Όταν λέμε ότι μια πληροφορία είναι ακριβής, εννοούμε ότι εκφράζει την κατάσταση ενός γεγονότος, όπως αυτό είναι στη πραγματικότητα. Αντίθετα , η αναληθής πληροφορία είναι συνήθως αποτέλεσμα λαθών, που πιθανόν έγιναν κατά τη διάρκεια της συλλογής και της επεξεργασίας των δεδομένων. Ορισμένες φορές τυχαίνει να θεωρούμε ως σωστή μία πληροφορία που είναι ανακριβής. Στην περίπτωση αυτή, και για όσο διάστημα ο χρήστης τη θεωρεί ως ορθή και τη χρησιμοποιεί στη λήψη αποφάσεων ,αυτό αποτελεί πληροφορία για το συγκεκριμένο άτομο. Για παράδειγμα εάν ο διευθυντής πωλήσεων πάρει μια αναφορά, στην οποία ανακριβώς αναγράφεται , ότι οι προβλεπόμενες συνολικές πωλήσεις σε ένα υποκατάστημα κατά το επόμενο τρίμηνο αναμένεται να είναι 300 χιλιάδες ευρώ, αντί του ορθού των 400 χιλιάδων ευρώ , και χρησιμοποιεί αυτό το νούμερο για να πάρει κάποιες αποφάσεις , αυτό αποτελεί πληροφορία για το διευθυντή πωλήσεων , έστω και αν αυτή είναι ανακριβής. Έτσι το βασικό πρόβλημα που υπάρχει με τη πληροφορία είναι ότι μπορεί να είναι ανακριβής, αλλά να μην το έχει αντιληφθεί ο χρήστης και να τη χρησιμοποιεί στη λήψη των αποφάσεων του. Για την αποφύγει τέτοιου είδους καταστάσεων θα πρέπει το άτομο που παρέχει την πληροφορία να επιβεβαιώνει την ακρίβεια της .

  Ο βαθμός ακρίβειας μιας μεμονωμένης πληροφορίας εξαρτάται φυσικά από τη χρησιμοποίηση της .Αυτό σημαίνει πως δεν υπάρχει λόγος για μεγάλο βαθμό ακρίβειας, εφόσον αυτό δεν είναι αναγκαίο. Για παράδειγμα , ο διευθυντής πωλήσεων δεν ενδιαφέρεται ποτέ για τις προβλέψεις των πωλήσεων με ακρίβεια ευρώ αλλά στρογγυλοποιημένες σε εκατοντάδες ,χιλιάδες κ.τ.λ. Αντίθετα ο διευθυντής του λογιστηρίου θέλει πολλές από τις πληροφορίες του να είναι ακριβείς μέχρι και το

τελευταίο ευρώ. Βέβαια ο επιθυμητός βαθμός ακρίβειας εξαρτάται από τη χρησιμοποίηση της πληροφορίας και είναι γνωστός στο χρήστη της.

- Μορφή(Forum): Η μορφή αναφέρεται στη δομή της πληροφορίας. Μια πρώτη διάκριση της είναι σε ποσοτική και ποιοτική πληροφορία .Η ποσοτική πληροφορία εκφράζει το πόσο έχει μετρηθεί από ένα είδος ή γεγονός .Για παράδειγμα , οι πωλήσεις μιας επιχείρησης μπορούν να εκφραστούν ποσοτικά σε σχέση με τις μονάδες του προϊόντος , την καθαρή ή ακαθάριστη αξία τους, το κόστος των πωληθέντων κ.α. .Τέτοιου είδους πληροφορίες ,όπως οι παραπάνω, είναι πολύ συνηθισμένες στο κόσμο των επιχειρήσεων. Η ποσοτική πληροφορία μπορεί να παρουσιάζεται αριθμητικά ή γραφικά με διαγράμματα , ιστογράμματα κ.α. Με τη ποιοτική πληροφορία γίνεται συνήθως περιγραφή μίας κατάστασης ή ενός γεγονότος με βάση ένα ποιοτικό κριτήριο .Για παράδειγμα, τα διευθυντικά στελέχη μίας επιχείρησης είναι δυνατόν να ταξινομηθούν με κριτήριο τη θέση που κατέχουν, σε γενικό διευθυντή, διευθυντή , υποδιευθυντή προϊστάμενο τμήματος, κ.α.

  Μια δεύτερη διάκριση είναι ανάλογα με το μέσο που χρησιμοποιείται για την παρουσίαση τους .Συνήθως εμφανίζονται σε χαρτί (χειρόγραφα, κόλλες γραφομηχανής,φωτοτυπίες ,μηχανογραφικό χαρτί) ή σε οθόνη (διαφάνειες ,μικροφίλμ, οθόνη υπολογιστή, κ.α.).

- Συχνότητα (Frequency): Η συχνότητα αποτελεί το μέτρο για το πόσο συχνά χρειάζεται μια πληροφορία, συλλέγεται ή παράγεται. Μια πληροφορία μπορεί να παράγεται καθημερινά , λιγότερο ή περισσότερο συχνά, ή ακόμη και σπάνια ανάλογα με το κάθε πότε τη χρειάζεται το άτομο που τη χρησιμοποιεί. Έτσι οι πωλήσεις π.χ. σ' ένα super market είναι μια πληροφορία που παράγεται και σε καθημερινή βάση, το ποσό που δίνεται για τους μισθούς των υπαλλήλων παράγεται κάθε μήνα, ενώ ο φόρος εισοδήματος κάθε χρόνο.

- Χρονικός ορίζοντας (Time Horizon):Η πληροφορία μπορεί να αναφέρεται στο παρελθόν, στο παρόν ή στο μέλλον. Η ιστορική πληροφορία μας δείχνει το τι έχει γίνει στο παρελθόν και χρησιμοποιείται συνήθως για να διαπιστωθεί κατά πόσο οι τιμές συγκεκριμένων μεταβλητών όπως π.χ. οι πωλήσεις, τα έξοδα, τα κέρδη,κ.α. έχουν τη τρέχουσα περίοδο μεταβληθεί προς το καλύτερο ή προς το χειρότερο. Η μελλοντική πληροφορία είναι χρήσιμη για το μέλλον. Για παράδειγμα, με βάση τις προβλέψεις που διενεργούνται για σημαντικέ οικονομικές μεταβλητές και άλλες πληροφορίες που αφορούν την μελλοντική εξέλιξη καταστάσεων, οι επιχειρήσεις προγραμματίζουν την ανάπτυξη των νέων τους προϊόντων, την επέκταση της παραγωγικής τους δυναμικότητας, την είσοδο τους σε νέες αγορές , την πρόσληψη νέου προσωπικού κ.τ.λ.
- Έκταση (Breadth): Η έκταση της πληροφορίας είναι το πεδίο δράσεως, στο οποίο αναφέρεται. Μερικές πληροφορίες έχουν ένα ευρύ φάσμα ενδιαφέροντος, ενώ άλλες αφορούν ένα μικρότερο πεδίο δράσεως. Για παράδειγμα ένα ευρύ φάσμα για πληροφορίες σχετικές με τις πωλήσεις μίας επιχείρησης μπορεί να περιλαμβάνει όλες τις περιοχές πώλησης, που καλύπτει η επιχείρηση σε μία χώρα. Αντίθετα ένα μικρότερο πεδίο δράσεως πιθανό να περιλαμβάνει τις πωλήσεις σε μία μόνο πόλη ή σε ένα νομό.

1.2.2 ΤΑ ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΕΝΟΣ ΣΥΝΟΛΟΥ ΠΛΗΡΟΦΟΡΙΩΝ

- Σχετικότητα(Relevance): Σχετικές πληροφορίες θα μπορούσαν να θεωρηθούν εκείνες, τις οποίες χρειάζεται κάποιος για να λύσει ένα πρόβλημα ή να πάρει μια απόφαση. Όμως το κριτήριο με βάση το οποίο κρίνεται αν οι πληροφορίες είναι σχετικές ή όχι είναι ο χρόνος χρησιμοποίηση τους . Ένα σύνολο πληροφοριών θεωρείται σχετικό, εφόσον χρησιμοποιείται σε μία τρέχουσα κατάσταση. Έτσι, πληροφορίες

οι οποίες ήταν στο παρελθόν σχετικές, αλλά σήμερα ο κάτοχος τους δεν τις χρειάζεται και δεν τις χρησιμοποιεί, παύουν να είναι σχετικές .Με την ίδια λογική, αν κάποιος συλλέγει και αποθηκεύει πληροφορίες, επειδή πιστεύει ότι ίσως τις χρησιμοποιήσει στο μέλλον, ούτε αυτές οι πληροφορίες θεωρούνται σχετικές, διότι δεν χρησιμοποιούνται σε μια τρέχουσα κατάσταση.

- Πληρότητα(Completeness): Ένα σύνολο πληροφοριών ενδέχεται να δίνει στο χρήστη σε μικρότερο ή μεγαλύτερο βαθμό την πληροφόρηση που χρειάζεται για να αντιμετωπίσει μια συγκεκριμένη κατάσταση. Όταν ο χρήστης έχει όλες τις αναγκαίες πληροφορίες, τότε θεωρούμε ότι το σύνολο αυτό είναι πλήρες .Αντίθετα όταν το σύνολο δεν δίνει στον χρήστη όλη την πληροφόρηση ή τον αφήνει με αναπάντητες ερωτήσεις, το σύνολο αυτό είναι ελλιπές. Σημειώνουμε , πως ορισμένες φορές είναι δύσκολο ή κόμη και αδύνατο να αποκτήσουμε τον επιθυμητό βαθμό πληρότητας των πληροφοριών. Στις περιπτώσεις αυτές καλό είναι να αναζητάμε διαδικασίες και συστήματα που μπορούν να μας δίνουν όσο το δυνατόν πληρέστερη πληροφόρηση.
- Επικαιρότητα(Timeleness): Οι πληροφορίες θα πρέπει να δίνονται στο χρήστη τη χρονική στιγμή που τις χρειάζεται. Η παραγωγή της πληροφορίας πολύ πριν από τη χρήση της πιθανόν να αυξήσει το κόστος της σημαντικά .Από την άλλη πλευρά , όταν η πληροφορία φτάνει στο χρήστη με καθυστέρηση ή είναι ήδη απαρχαιωμένη κατά την παραλαβή ή τη χρήση της , τότε ενδέχεται να είναι άχρηστη, με αποτέλεσμα τη σπατάλη χρόνου , χρήματος και προσπάθειας, πέρα φυσικά από τις άλλες επιπτώσεις στη λήψη των αποφάσεων.

1.3 ΔΙΑΔΙΚΤΥΟ (INTERNET)

1.3.1 ΙΣΤΟΡΙΚΑ

Το internet είναι (και υπήρξε εδώ και αρκετό καιρό) το μεγαλύτερο δίκτυο υπολογιστών στο κόσμο. Πρόκειται για μία απέραντη συλλογή πληροφοριών και υπολογιστικών πόρων. Η προσπέλαση του είναι εύκολη, οποιοσδήποτε έχει ένα προσωπικό υπολογιστή και ένα μόντεμ ,μπορεί να συνδεθεί στο internet. Η εύκολη πρόσβαση στο internet αλλάζει τον τρόπο ζωής μας , παρέχοντας μας ευκαιρίες για επικοινωνία , μόρφωση , και διασκέδαση που δεν μπορούσαμε ούτε να τις φανταστούμε πριν κάποια χρόνια.

Αυτές οι αλλαγές δεν έγιναν από τη μια στιγμή στη άλλη. Το σημερινό internet είναι απόγονος ενός παλαιότερου δικτύου υπολογιστών (του ARPAnet) που δημιουργήθηκε πριν 35 χρόνια περίπου για να καλύψει τις ανάγκες των ερευνητών που δούλευαν στην αμυντική βιομηχανία των Ηνωμένων Πολιτειών και των συνεργατών τους σε άλλες χώρες. Το ARPAnet μεγάλωσε αργά από τέσσερις υπολογιστές το 1969 σε περισσότερους από 1000 το 1984. Σε αρχική φάση το ARPAnet ήταν ένα δίκτυο μεμονωμένων υπολογιστών συνδεδεμένων μεταξύ τους. Γρήγορα εξελίχθηκε σε δίκτυο αποτελούμενο από δίκτυα υπολογιστών, επιτρέποντας σε όλους τους υπολογιστές ενός τοπικού δικτύου να απολαμβάνουν τα πλεονεκτήματα της μακρινής επικοινωνίας με υπολογιστές και χρήστες σε άλλα δίκτυα .

Δουλεύοντας με το ARPAnet , οι ερευνητές άρχισαν σιγά - σιγά να αναγνωρίζουν ότι ένα υψηλής ταχύτητας , ευρείας περιοχής δίκτυο υπολογιστών είναι απαραίτητο εργαλείο για όλους τους τομείς της ακαδημαϊκής έρευνας .Το 1986, το Εθνικό Ίδρυμα Επιστημών (National Science Foundation) των Η.Π.Α. παρουσίασε το NFSnet για να κάνει τις συνδέσεις δικτύου διαθέσιμες σε περισσότερα ερευνητικά ιδρύματα και για να βελτίωση τη διεθνή συνεργασία των δικτύων. Το 1987 , το Internet εξυπηρετούσε πάνω από 1000 υπολογιστές.

Το 1989, το ARPAnet καταργήθηκε επίσημα, αλλά το Internet συνέχισε να μεγαλώνει, και το 1992 το Internet εξυπηρετούσε πάνω από 6,5 εκατομμύρια υπολογιστές που αντιπροσώπευαν σχεδόν 62000 τοπικά δίκτυα. Το Internet έχει πλέον ξεπεράσει τα όρια του ακαδημαϊκού κόσμου προσφέροντας και πρόσβαση σε πληροφορίες και ένα φτηνό, γρήγορο μέσο επικοινωνίας για το κοινό .Θα είναι το επόμενο αγαθό κοινής ωφέλειας.

1.3.2 ΧΡΗΣΙΜΟΤΗΤΑ ΔΙΑΔΙΚΤΥΟΥ

Οι δραστηριότητες που βασίζονται σε δίκτυο όπως η φυλλομέτρηση του παγκόσμιου ιστού (Word Wide Web) και η ανταλλαγή ηλεκτρονικού ταχυδρομείου είναι πλέον συνηθισμένες σήμερα. Όλα όσα μπορούμε να κάνουμε στο Internet καθορίζονται από τα προγράμματα (ή τις εφαρμογές λογισμικού) που χρησιμοποιούν το Internet .Υπάρχουν έξι εφαρμογές που ευθύνονται για το μεγαλύτερο τμήμα της δραστηριότητας του Internet: τα προγράμματα World Wide Web , Gopher, Usenet, το ηλεκτρονικό ταχυδρομείο (e-mail), το πρόγραμμα μεταφοράς αρχείων FTP,και το Telnet. Για να χρησιμοποιήσουμε τις περισσότερες από τις εφαρμογές του Internet, πρέπει να δουλεύουμε σε κάποιο υπολογιστή που είναι συνδεδεμένος με αυτό. Ο υπολογιστής που χρησιμοποιείται με το Internet δε χρειάζεται να είναι ιδιαίτερα ισχυρός, καθώς ,μπορεί να είναι οτιδήποτε , από ένας προσωπικός υπολογιστής έως ένα μεγάλο σύστημα υπολογιστή (mainframe) .Η σύνδεση με το Internet μπορεί να είναι είτε μόνιμη σε έναν υπολογιστή που ανήκει σε κάποιο τοπικό δίκτυο (για παράδειγμα ένα δίκτυο στο γραφείο η στο πανεπιστήμιο) είτε προσωρινή σύνδεση που εγκαθιδρύεται καλώντας ένα προμηθευτή πρόσβασης στο internet .Ανεξάρτητα από τον υπολογιστή που χρησιμοποιεί κανείς ή τον τρόπο που αυτός είναι συνδεδεμένος στο Internet θα πρέπει να προσδιορίσετε την ταυτότητα σας ως εξουσιοδοτημένος χρήστης του δικτύου για να μπορέσετε να εκτελέσετε διαταγές που προσπελάζουν το Internet.

1.3.3 ΤΡΟΠΟΣ ΛΕΙΤΟΥΡΓΙΑΣ INERNET

Η επικοινωνία, με ένα μέσο, τόσο πολύπλοκο όσο το Internet προκαλεί μερικά προβλήματα που δεν θα προέκυπταν αν για παράδειγμα δύο άνθρωποι προσπαθούσαν να μιλήσουν σε τενεκεδένια κουτιά που είναι συνδεδεμένα με ένα κομμάτι σπάγκο. Φανταστείτε το αποτέλεσμα ενός εκατομμυρίου ομιλητών στο δίκτυο των τενεκεδένιων κουτιών, με ένα απλό κορδόνι που να μεταφέρει την ομιλία καθενός σε όλα τα συνδεδεμένα κουτιά .Ο κυκεώνας του θορύβου που θα διέσχιζε το δίκτυο θα έκανε πρακτικά αδύνατο στον οποιοδήποτε να βρει συνομιλητή.

Ένα μόνιτορ άμεσα συνδεδεμένο σε κάποιο τμήμα του φυσικού δικτύου του Internet θα έδειχνε κάτι ανάλογο με το κυκεώνα της μεταφοράς ομιλίας στο σπάγκο. Θα βλέπατε ένα κυκεώνα μηνυμάτων να πηγαίνουν και να έρχονται από κοντινές περιοχές, και που πιθανόν να συμπορεύονται με μηνύματα που μεταφέρονται από μία μακρινή περιοχή σε κάποια άλλη. Σε αντίθεση με το δίκτυο των τενεκεδένιων κουτιών, οι συνομιλητές του Internet βρίσκουν αυτόματα ο ένας τον άλλον. Μηνύματα και άλλες πληροφορίες ταξιδεύουν σε μακρινές αποστάσεις και φτάνουν στο προορισμό τους άθικτα. Το συστατικό στοιχείο του δικτύου που το κάνει αυτό εφικτό είναι μια συλλογή από πρωτόκολλα, που χειρίζονται διαφορετικές απόψεις παράδοσης μηνυμάτων από μια περιοχή σε κάποια άλλη. Τα πρωτόκολλα δικτύου είναι γλώσσες ειδικού σκοπού τις οποίες χρησιμοποιούν οι υπολογιστές για να επικοινωνούν μεταξύ τους. Διαφορετικά πρωτόκολλα κάνουν διαφορετικά πράγματα. Μερικά πρωτόκολλα συντονίζουν τη κίνηση των μηνυμάτων, άλλα ελέγχουν την ακεραιότητα αυτόν που διαβιβάστηκαν, και άλλα μετατρέπουν τα δεδομένα από μια μορφή σε κάποια άλλη.

Η χρήση των πρωτοκόλλων δεν είναι βέβαια μοναδικό φαινόμενο στα δίκτυα υπολογιστών. Για παράδειγμα, η αναγραφή των στοιχείων του αποστολέα και

του παραλήπτη σε κάποιο φάκελο που πρόκειται να ταχυδρομηθεί είναι ένα είδος πρωτοκόλλου. Η διεύθυνση του παραλήπτη και η διεύθυνση του αποστολέα στο φάκελο είναι μηνύματα προς το ταχυδρομικό γραφείο που περιγράφουν πού θα πάει το γράμμα ,σε διάφορες περιπτώσεις. Τα μηνύματα αυτά πρέπει να εμφανίζονται στις προβλεπόμενες θέσεις του φακέλου, και πρέπει να έχουν μία μορφή που να την καταλαβαίνει η ταχυδρομική υπηρεσία, αν θέλουμε να παραδοθεί σωστά ο φάκελος.

1.3.4 ΤΑ ΠΡΩΤΟΚΟΛΛΑ ΤΟΥ INTERNET

Τα πρωτόκολλα δουλεύουν στο παρασκήνιο. Η εργασία μετάφρασης των μηνυμάτων προς και από τα πρωτόκολλα γίνεται αθόρυβα από τους υπολογιστές υπηρεσίας του δικτύου, και οι χρήστες γλιτώνουν την αγγαρεία να ελέγχουν οι ίδιοι τα μεμονωμένα πακέτα που διατρέχουν το δίκτυο .Κάθε μήνυμα που μεταδίδεται στο Internet περνάει από τουλάχιστον τρία επίπεδα πρωτοκόλλων: το πρωτόκολλο δικτύου (network protocol) που επιτηρεί τη μεταφορά μηνυμάτων από περιοχή σε περιοχή, το πρωτόκολλο μεταφοράς (transport protocol) που διαχειρίζεται την ακεραιότητα των δεδομένων που μεταβιβάζονται και το πρωτόκολλο εφαρμογής (application protocol) που μετατρέπει τη διαβίβαση του δικτύου σε κάτι που μπορούμε να αναγνωρίσουμε ως απάντηση σε κάποια ερωτήματα που απευθύναμε μέσω κάποιας εφαρμογής δικτύου .Το πρωτόκολλο που χρησιμοποιείται από το Internet για την μεταφορά μηνυμάτων από ένα μηχάνημα σε κάποιο άλλο ονομάζεται πρωτόκολλο Internet (Internet Protocol – IP). Το πρωτόκολλο Internet είναι ένα πρωτόκολλο δικτύου, και η δουλειά του είναι να διαχειρίζεται το δύσκολο έργο της μεταφοράς ενός μηνύματος από το μηχάνημα που το στέλνει στο μηχάνημα που θα το παραλάβει.

Τα μηνύματα που διανέμονται από το πρωτόκολλο Internet (IP) ονομάζονται πακέτα (packets) ,και είναι πολύ μικρού μεγέθους ,συνήθως χίλια πεντακόσια

byte ή λιγότερα .Εφόσον λοιπόν είναι πολύ μικρότερα από αρκετά μηνύματα και αρχεία που διαβιβάζονται μέσω του Internet,είναι συνηθισμένο για μία μετάδοση να απαιτούνται πολλά πακέτα .

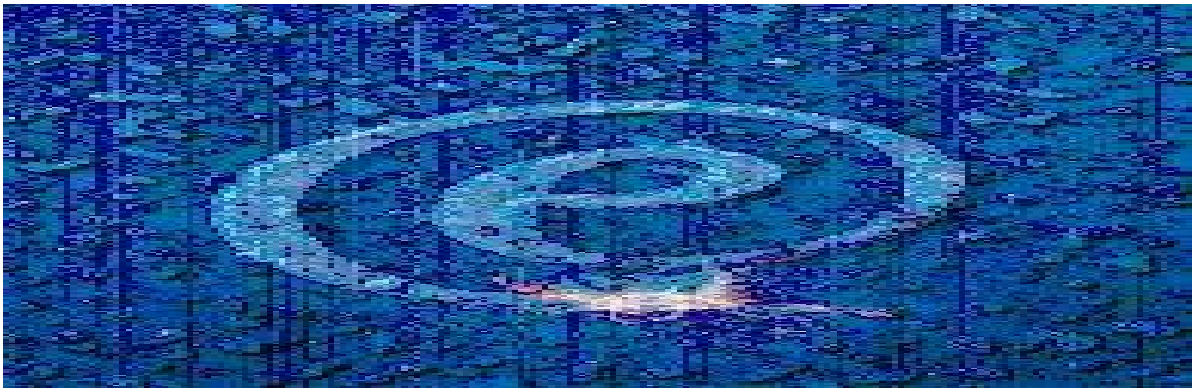
Αφού το Πρωτόκολλο Internet κάνει τη δουλειά του, ένα πρωτόκολλο μεταφοράς (transport protocol) αναλαμβάνει να συλλέξει να σχετικά μεταξύ τους πακέτα, να τα τοποθετήσει σε κατάλληλη σειρά, και να εξακριβώσει ότι κανένα από αυτά δεν έχει αλλοιωθεί . Το Internet έχει δύο πρωτόκολλα μεταφοράς που ασχολούνται με αυτές τις λειτουργίες : το πρωτόκολλο ελέγχου διαβίβασης (Transmission Control Protocol – TCP) και το πρωτόκολλο πακέτου χρήστη (User Datagram Protocol).

Τέλος υπάρχουν πρωτόκολλα εφαρμογών που φροντίζουν την τυποποίηση των αιτήσεων που έχουν διατυπωθεί από χρήστες και των δεδομένων που επιστρέφονται σε απόκριση αυτών των κλήσεων. Υπάρχουν τόσα πρωτόκολλα εφαρμογών όσες είναι και οι εφαρμογές του Internet. Κάθε μία από τις εφαρμογές E-mail,Telnet,FTP, Archie, Usenet, Gopher,και World Wide Web , έχει το δικό του πρωτόκολλο.

Το πρωτόκολλο Internet (IP) και το πρωτόκολλο ελέγχου διαβίβασης (TCP) συνδυάζονται τόσο συχνά, ώστε να είναι συνηθισμένο να μιλάμε για δίκτυα TCP/IP .Εδώ και χρόνια το TCP/IP είναι το πρωτόκολλο που προτιμούν οι κατασκευαστές υπολογιστών πολλών χρηστών και υπάρχουν διάφορες υλοποιήσεις TCP/IP για υπολογιστές Macintosh και PC, όπως και για άλλα συστήματα υπολογιστών πολλών χρηστών. Η χρήση του συνδυασμένου πρωτοκόλλου TCP/IP είναι ευρέως διαδεδομένη και έξω από το Internet, η χρήση του TCP/IP δε σημαίνει απαραίτητα σύνδεση με το Internet.

Από τη σκοπιά του χρήστη κάθε τοπικό δίκτυο που βασίζεται στο συνδυασμό πρωτοκόλλων TCP/IP είναι μια μικρογραφία του Internet. Πολλά από τα εργαλεία που είναι διαθέσιμα στο Internet (mail,telnet,και ftp) συμπεριλαμβάνονται στο βασικό λογισμικό των συστημάτων UNIX. Οι εφαρμογές που έχουν αναπτυχθεί στα μέλη της κοινότητας του Internet μπορούν

επίσης να μεταφερθούν σε κάποιο LAN που βασίζεται στο TCP/IP και δεν υπάρχει κανένας λόγος κάποια εφαρμογή του Internet όπως ο Ιστός να μην χρησιμοποιηθεί για τη διαχείριση των τοπικών πόρων.



ΚΕΦΑΛΑΙΟ 2 – ΕΠΙΘΕΣΗ

2.1 ΒΑΣΙΚΑ ΣΤΟΙΧΕΙΑ

Ένα δίκτυο για να θεωρηθεί ασφαλές πρέπει να διαθέτει τρεις βασικές ιδιότητες:

- Ακεραιότητα (integrity)
- Διαθεσιμότητα (availability)
- Εμπιστευτικότητα (confidentiality)

2.1.1 ΑΚΕΡΑΙΟΤΗΤΑ

Ακεραιότητα ενός δικτύου ονομάζεται η ιδιότητα του να προστατεύει τους χρήστες και τα αντικείμενα , υπό οποιεσδήποτε γενικά συνθήκες. Επίσης να εξασφαλίζει :

- Τη λογική ορθότητα, την αξιοπιστία και την ανοχή σε σφάλματα του υλικού και του λογισμικού του συστήματος.
- Τη λογική πληρότητα των μηχανισμών εξασφάλισης του υλικού και λογισμικού.
- Τη συνοχή των δομών των δεδομένων και την ακρίβεια των αποθηκευμένων δεδομένων.

2.1.2 ΔΙΑΘΕΣΙΜΟΤΗΤΑ

Διαθεσιμότητα ενός δικτύου ονομάζεται η ιδιότητα του να εξασφαλίζει στους εξουσιοδοτημένους χρήστες την πρόσβαση στα αντικείμενα του δικτύου που επιθυμούν, με τον πιο αποδοτικό τρόπο.

Αυτό σημαίνει ότι το δίκτυο πρέπει να λειτουργεί ώστε, όχι μόνο να προστατεύει από τους μη εξουσιοδοτημένους χρήστες αλλά να προστατεύει τα δικαιώματα και των εξουσιοδοτημένων χρηστών .Η διαθεσιμότητα ενός δικτύου είναι συχνά αντιφατική με τις διαδικασίες εξασφάλισης του. Έτσι, αν οι διαδικασίες αυτές εφαρμόζονται συχνά και απαιτούν σημαντικό χρόνο, τότε μειώνεται ο ωφέλιμος χρόνος που διατίθεται στο χρήστη, άρα και η συνολική διαθεσιμότητα του.

Η συνύπαρξη των ιδιοτήτων ασφάλειας και διαθεσιμότητας, είναι θέμα ισορροπίας μεταξύ της επιδιωκόμενης φιλικότητας και αξιοπιστίας ενός δικτύου.

2.1.3 ΕΜΠΙΣΤΕΥΤΙΚΟΤΗΤΑ

Εμπιστευτικότητα ενός δικτύου είναι η ιδιότητα του να επιτρέπει την πρόσβαση σε αντικείμενα του μόνο σε εξουσιοδοτημένους χρήστες , σύμφωνα με τις αρχές λειτουργίας του.

2.2 ΠΛΗΡΟΦΟΡΙΑΚΟΣ ΠΟΛΕΜΟΣ

Στον πρόλογο του βιβλίου του Winn Schwartau που έχει το τίτλο "πληροφοριακός πόλεμος" ο John Alger, κοσμήτορας της σχολής Πληροφοριακού Πολέμου και Στρατηγικής του National Defense University ,έγραψε , "Ο πληροφοριακός πόλεμος αποτελείται από πράξεις με τις οποίες επιδιώκεται η προστασία , η εκμετάλλευση, η φθορά , η διάψευση ή η καταστροφή πληροφοριών ή πηγών πληροφοριών με σκοπό να επιτευχθεί ένα σημαντικό πλεονέκτημα , ένας σκοπός ή μια νίκη σε βάρος ενός αντιπάλου".

Ο πληροφοριακός πόλεμος αποτελείται από επιθετικές και αμυντικές επιχειρήσεις που στρέφονται ενάντια σε πηγές πληροφοριών και οι οποίες είναι του τύπου "νίκης-ήττας" .Ο πόλεμος αυτός διεξάγεται επειδή οι πηγές πληροφοριών έχουν αποκτήσει μεγάλη αξία για τους ανθρώπους .Οι επιθετικές επιχειρήσεις σκοπεύουν να αυξήσουν την αξία αυτή προς όφελος της επίθεσης και ταυτόχρονα να την μειώσουν για την άμυνα. Οι αμυντικές επιχειρήσεις επιζητούν να αντισταθμίσουν τις πιθανές απώλειες της αξίας αυτής .

Υπάρχουν δύο βασικοί παίκτες σε κάθε επιχείρηση πληροφοριακού πολέμου , ένας επιθετικός που επιτίθεται ενάντια σε μια συγκεκριμένη πληροφοριακή πηγή και ένας αμυντικός ο οποίος προσπαθεί να αποκρούσει την προηγούμενη επίθεση.

2.2.1 Η ΕΠΙΘΕΣΗ

Οι παίκτες και των δύο πλευρών μπορεί να είναι άτομα που δουλεύουν μόνα τους ή σε δομημένες ή μη ομάδες. Μπορεί ακόμη να είναι κρατικοί ή μη

υπάλληλοι. Μπορεί επίσης να έχουν ή να μην έχουν και κάποια χρηματοδότηση. Για να συμμετάσχει στον πληροφοριακό πόλεμο ένας παίκτης θα πρέπει να έχει τα κίνητρα, τα μέσα και την ευκαιρία. Τα κίνητρα σχετίζονται με τα ενδιαφέροντα και τις υποχρεώσεις του παίκτη, ενώ τα μέσα προσδιορίζονται από τις ικανότητες του και την δυνατότητα πρόσβασης που έχει στο στόχο του (πόσο προσιτός του είναι). Η ευκαιρία αφορά κι αυτή τη δυνατότητα πρόσβασης αλλά περιλαμβάνει και άλλους παράγοντες, όπως την πεποίθηση ότι η επιχείρηση θα πετύχει κι ότι κανείς δεν θα αποτραπεί από την πραγματοποίηση της ή θα συλληφθεί. Εάν μάλιστα υπάρχει αρχική αδυναμία πρόσβασης στο στόχο τότε θα πρέπει αυτή να διορθωθεί πριν από οτιδήποτε άλλο , ενδεχόμενα με την δολιοφθορά πχ. της συγκεκριμένης πληροφοριακής πηγής.

Παρότι οποιοδήποτε άτομο ή οργανισμός μπορεί να αναμιχθεί σε επιχειρήσεις επιθετικού πληροφοριακού πολέμου, οι περισσότερες από τις επιχειρήσεις αυτές αποδίδονται σε πέντε γενικές κατηγορίες υποκειμένων.Αυτές περιλαμβάνουν τα πρόσωπα, που βρίσκονται εντός του στόχου, τους χάκερς, τους εγκληματίες, τις επιχειρήσεις, τις κυβερνήσεις και τους τρομοκράτες.

Στα πρόσωπα που βρίσκονται εντός του στόχου κατατάσσουμε τούς υπαλλήλους μιας επιχείρησης, τους πρώην υπαλλήλους της, τους προσωρινά απασχολούμενους σε αυτή, τούς συνεργάτες της καθώς και οποιονδήποτε άλλο έχει εσωτερική πρόσβαση στις πηγές των πληροφοριών της. Αυτή η ομάδα θεωρείται γενικά ότι αποτελεί και τη μεγαλύτερη απειλή για κάθε επιχείρηση. Τα άτομα που την αποτελούν λειτουργούν σαν μεσίτες πληροφοριών, πουλώντας ευαίσθητες πληροφορίες, που ανήκουν σ΄αυτή, σε ξένες κυβερνήσεις, σε ανταγωνιστές και σε συμμορίες του οργανωμένου εγκλήματος. Με τις πράξεις τους δημιουργούν προβλήματα σε επιχειρηματικά και σε στρατιωτικά πλάνα, στην αντικατασκοπεία και στον ιδιωτικό χώρο των ατόμων. Τα άτομα αυτά κάνουν σαμποτάζ στα πληροφοριακά συστήματα του εργοδότη τους και στη συνέχεια φεύγουν αποκομίζοντας εμπορικά μυστικά με σκοπό να ξεκινήσουν μία δική τους ανταγωνιστική επιχείρηση. Ακόμη δε κι αν δεν

πραγματοποιήσουν τα ίδια την επίθεση αυτή διευκολύνουν σκόπιμα ή μη άλλους τρίτους για να την κάνουν. Τα κίνητρα τους είναι τα χρήματα, η ιδεολογία, η εκδίκηση και η επιθυμία να βοηθήσουν τους τρίτους που τα εκμεταλλεύονται.

Η επόμενη ομάδα είναι οι χάκερς. Μολονότι η λέξη "χάκερ" μπορεί να υποδηλώνει οποιονδήποτε φανατικό φίλο των υπολογιστών, στα πλαίσια του πληροφοριακού πολέμου αυτή συνήθως σημαίνει κάποιον που αποκτά πρόσβαση ή εισβάλλει σε ηλεκτρονικά συστήματα, κυρίως υπολογιστών και τηλεπικοινωνιών. Στα κίνητρα του περιλαμβάνονται η αίσθηση συγκίνησης η πρόκληση και η επίδειξη δύναμης. Παρότι πολλοί χάκερ, ίσως οι περισσότεροι, δεν επιζητούν οικονομικά οφέλη ή την καταστροφή των μηνυμάτων στα οποία επιτίθενται, ορισμένοι από αυτούς εισβάλλουν τα συστήματα για να κερδίσουν χρήματα ή για να τα καταστρέψουν. Θα πρέπει ωστόσο να παρατηρήσουμε πως έστω και χωρίς κακή πρόθεση η χωρίς εξουσιοδότηση η εισβολή σε ένα σύστημα καταστρέφει την αξιοπιστία και αποτελεί κάτι περισσότερο από απλή ενόχληση για τους ιδιοκτήτες του.

Η τρίτη ομάδα, των εγκληματιών ,έχει σαν στόχο τις πληροφορίες με οικονομικό περιεχόμενο, όπως τραπεζικούς λογαριασμούς, αριθμούς πιστωτικών καρτών και δικαιώματα πνευματικής ιδιοκτησίας, που μπορούν να αποδώσουν χρήματα στο χώρο της παραοικονομίας .Συνήθως λειτουργούν μέσα στα πλαίσια των συμμοριών του οργανωμένου εγκλήματος, χωρίς αυτό να εμποδίζει και μεμονωμένα άτομα να αποκομίσουν λεία εκατομμυρίων δολαρίων .Το βασικό τους κίνητρο είναι βέβαια τα χρήματα. Στην ομάδα αυτή ανήκουν οι μεσίτες των πληροφοριών και εκείνη που πωλούν πειρατικά προγράμματα υπολογιστών, CD και βιντεοταινίες.

Οι επιχειρήσεις είναι η τέταρτη κατηγορία των παικτών. Αυτές εμπλέκονται σε επιθετικό πληροφοριακό πόλεμο, όταν κατασκοπεύουν τους ανταγωνιστές τους ή τους κλέβουν τα εμπορικά τους μυστικά με παράνομους τρόπους, όπως πχ. με τη δωροδοκία των υπαλλήλων τους. Επίσης πωλούν πληροφορίες που αφορούν

τους πελάτες τους, παραβιάζοντας με το τρόπο αυτό τον ιδιωτικό τους χώρο. Κίνητρα τους είναι τα χρήματα αλλά και η ανταγωνιστική τους διάθεση.

Στην πέμπτη κατηγορία ανήκουν οι διάφοροι κυβερνητικοί οργανισμοί, αρκετοί από τους οποίους εμπλέκονται σε επιθετικό πληροφοριακό πόλεμο .Έτσι, στόχος της αστυνομίας είναι οι επικοινωνίες, τα έγγραφα και οι οργάνωση των εγκληματιών με σκοπό τη συλλογή αποδείξεων αλλά και την παρακολούθηση των εγκληματικών τους δραστηριοτήτων. Οι υπηρεσίες κατασκοπείας ,εξάλλου επιδιώκουν να αποκτήσουν τα στρατιωτικά, τα διπλωματικά και τα οικονομικά μυστικά ξενών κυβερνήσεων και και ξένων μικροεπιχειρήσεων στους κατασκόπους τους και στην ηλεκτρονική παρακολούθηση για να πάρουν τις πληροφορίες αυτές. Οι στρατιωτικές μονάδες καταστρέφουν τα συστήματα διοίκησης και ελέγχου των αντιπάλων τους κατά τη διάρκεια του πολέμου. Κυβερνητικοί αξιωματούχοι λογοκρίνουν ομιλίες και περιορίζουν την πρόσβαση σε πληροφορίες εξελιγμένης τεχνολογίας για λόγους εθνικής ασφάλειας και δημόσιας τάξης.

Η έκτη κατηγορία είναι οι τρομοκράτες. Οι τρομοκράτες προκαλούν ιδιαίτερο ενδιαφέρον εξαιτίας των πιθανών ζημιών που μπορεί να προκαλέσουν με τις επιθέσεις τους ενάντια στις βασικές δομές του κράτους, όπως είναι οι υπηρεσίες άμεσης ανάγκης και το οικονομικό σύστημα. Οι τρομοκράτες συγκεντρώνουν πληροφορίες για τους στόχους τους, κάνουν προπαγάνδα και δολιοφθορές σε κτίρια και εγκαταστάσεις. Μέχρι στιγμής μόνο λίγες κυβερνο-επιθέσεις έχουν αναφερθεί ότι έγιναν από τρομοκράτες.

Ο παραπάνω κατάλογος δεν περιλαμβάνει όλους τους παίκτες. Ο καθένας μπορεί να πραγματοποίηση μια επιχείρηση επιθετικού πληροφοριακού πολέμου, κλέβοντας πχ. πληροφορίες, διαδίδοντας ψεύτικες ειδήσεις και εμποδίζοντας τη νόμιμη πρόσβαση σε πληροφορίες. Σε άλλες κατηγορίες επιθετικών παικτών ανήκουν οι πολιτικοί ακτιβιστές, οι εξτρεμιστές, οι καιροσκόποι και οι βάνδαλοι διάφορες κατηγορίες συνδέονται σε κάποιες περιπτώσεις μεταξύ τους. Ένας χάκερ πχ. θα μπορούσε να ήταν πολιτικός ακτιβιστής, τρομοκράτης ,υπάλληλος

επιχείρησης ή βιομηχανικός κατάσκοπος.

Σε κάθε δεδομένη στιγμή, εξάλλου, είναι δυνατόν μια πηγή να αποτελεί στόχο πολλών παικτών. Πχ. Εκατοντάδες χάκερς θα ήταν δυνατόν να προσπαθούσαν να αποκτήσουν πρόσβαση στους υπολογιστές μίας συγκεκριμένης επιχείρησης την ίδια ώρα, ή πολλές κυβερνήσεις θα προσπαθούσαν να μαζέψουν πληροφορίες για τον ίδιο στόχο. Ο αμυνόμενος θα πρέπει να λάβει υπόψη του τις πολλαπλές αυτές απειλές.

2.2.2 ΕΠΙΘΕΤΙΚΟΣ ΠΛΗΡΟΦΟΡΙΑΚΟΣ ΠΟΛΕΜΟΣ

Επιχείρηση επιθετικού πληροφοριακού πολέμου είναι εκείνη που στοχεύει ή εκμεταλλεύεται μια συγκεκριμένη πηγή πληροφοριών με σκοπό της αύξηση της αξίας της για τον παίκτη που επιτίθεται , και την αντίστοιχη μείωση της αξίας της για τον παίκτη που αμύνεται. Το αποτέλεσμα, στην περίπτωση αυτή, συνιστά μια κατάσταση “νίκης-ήττας” για τους δύο παίκτες. Υποτίθεται βέβαια, πως η πλευρά του αμυνόμενου δεν αποδέχεται μια τέτοια κατάσταση. Η σχετική επιχείρηση θεωρείται από αυτόν εχθρική ή τουλάχιστον μη εύκολα αποδεκτή πληροφοριών, δεν θα πρέπει βέβαια, να ανήκει ή να ελέγχεται από τον αμυνόμενο, παρότι αυτό είναι κάτι που συνήθως συμβαίνει.

Το κέρδος για τον επιτιθέμενο μπορεί να πάρει διάφορες μορφές .Έτσι μπορεί να είναι οικονομικό, όπως όταν οι πηγές των πληροφοριών κλαπούν και στη συνέχεια πωληθούν ή όπως όταν στοιχεία τραπεζικών λογαριασμών μεταβληθούν. Μπορεί να προσφέρει διασκέδαση ή συγκίνηση .Μπορεί να αποτελεί τα διαπιστευτήρια για την είσοδο σε μια πασίγνωστη ομάδα χάκερς. Μπορεί να προσφέρει την ευχαρίστηση της εκδίκησης. Μπορεί να αποτελεί ένα στρατιωτικό ή πολιτικό πλεονέκτημα. Το κέρδος αντιπροσωπεύει την αξία , που έχει η επιχείρηση για την πηγή. Εξαρτάται δε από την πηγή ,τούς παίκτες καθώς και από την ίδια την επιχείρηση. Μια πράξη κλοπής παράγει διαφορετικά αποτελέσματα από μια πράξη δολιοφθοράς.

Με τον ίδιο τρόπο, οι ζημιές του αμυνόμενου μπορούν να πάρουν διάφορες μορφές. Μπορεί να είναι η χαμένη εμπιστοσύνη του κοινού ή της ανταγωνιστικής τους θέσης, που θα έχουν σαν συνέπεια την απώλεια πελατών και κεφαλαίων. Μπορεί να είναι η απώλεια της παραγωγικότητας, που θα οφείλεται στις μη προσβάσιμες πλέον πηγές των πληροφοριών. Μπορεί να είναι πρόστιμα και ποινές για διάφορες συναφείς αξιόποινες πράξεις. Μπορεί να είναι η χαμένη δύναμη, πολιτική υποστήριξη ή διαπραγματευτική του θέση .Μπορεί να είναι η απώλεια της ζωής του, του απορρήτου της ιδιωτικής του ζωής, ή η ήττα του στο πεδίο της μάχης. Όπως και το κέρδος, έτσι και η οποιαδήποτε από τις ζημιές αυτές αποτελεί μια λειτουργία, στην οποία εμπλέκονται η πηγή, οι παίκτες καθώς και η φύση της συγκεκριμένης επιχείρησης.

Ο πληροφοριακός πόλεμος δεν αποτελεί αναγκαστικά ένα παιχνίδι με μηδενικό αποτέλεσμα. Αυτό σημαίνει ότι το κέρδος, που αποκομίζεται από την επίθεση, δε χρειάζεται να είναι ίσο με τη ζημιά, που προκαλείται στην άμυνα. Δεν μπορεί ακόμα να έχει ούτε και τις ίδιες απολαβές. Όταν πχ. ένας χάκερ αισθάνεται ικανοποιημένος και κερδίζει κύρος ανάμεσα στους ομοϊδεάτες του επειδή εισέβαλε στα αρχεία μιας επιχείρησης, η επιχείρηση αυτή μπορεί να χάνει την αξιοπιστία της στο κοινό καθώς και να μειώνονται οι επιχειρηματικές δραστηριότητες της.

Η δυσκολία της μέτρησης της αξίας μιας πηγής δεν επιτρέπει και την ακριβή μέτρηση των κερδών και των ζημιών , που προέρχονται από αυτή. Ωστόσο παρότι αυτά δεν μπορούν να μετρηθούν, είναι πολύ πιθανόν να εντοπίσει κανείς το που συμβαίνουν.

2.3 ΑΝΟΙΚΤΕΣ ΠΗΓΕΣ ΚΑΙ ΠΕΙΡΑΤΕΙΑ

Ο όρος “κατασκοπεία των ανοιχτών πηγών” αναφέρεται σε πράξεις κατασκοπείας, που χρησιμοποιούν πληροφορίες ,που απέκτησαν από μη απόρρητες πηγές. Όπως και τα άλλα είδη κατασκοπείας, περιλαμβάνει πολύ περισσότερα πράγματα από μια απλή συλλογή πληροφοριών. Έτσι, αφορά την ανάλυση των ζητούμενων θεμάτων, το φιλτράρισμα των πληροφοριών και την ανάλυση και την ενοποίηση των πληροφοριών μετά τη συλλογή τους. Διενεργείται δε με σκοπό να δώσει απάντηση σε κάποιο ειδικό ζήτημα απαραίτητο για την υποστήριξη μιας αποστολής.

Η “ανταγωνιστική κατασκοπεία” αναφέρεται στη χρήση της κατασκοπείας των ανοιχτών πηγών από εμπορικές εταιρίες εναντίον των εμπορικών ανταγωνιστών τους ,για να μάθουν πχ. όσο γίνεται περισσότερα πράγματα για τα εμπορικά τους σχέδια.

Το ίντερνετ χρησιμοποιείται σταδιακά σαν μία ανοιχτή πηγή στοιχείων. Μέχρι τις αρχές του 1998, ο Παγκόσμιος Ιστός (WWW) διέθετε πάνω από 300 εκατομμύρια έγγραφα, τα περισσότερα από τα οποία συνδέονται μεταξύ τους. Είναι δε δυνατόν να τα εντοπίσει κανείς ακολουθώντας συνδέσμους από άλλα έγγραφα ή χρησιμοποιώντας μία από τις μηχανές αναζήτησης που υπάρχουν. Υπηρεσίες του ίντερνετ ψάχνουν τα ηλεκτρονικά νέα, τις εφημερίδες και τις πρόσφατες εκδόσεις των διαφόρων περιοδικών μετά από απαίτηση χρηστών του και τους στέλνουν ομοειδή άρθρα με τη βοήθεια του ηλεκτρονικού ταχυδρομείου ή μέσω του web.

Σύμφωνα με αναφορά του Κέντρου Ερευνών Πίου, το διαδίκτυο ξεπέρασε τις εφημερίδες ως πηγή ειδήσεων το 2008 στις ΗΠΑ. Συγκεκριμένα, το διαδίκτυο εκτινάχτηκε από το 24% στο 40% μέσα σε ένα χρόνο, ξεπερνώντας το 35% εκείνων που βασίζονται στις εφημερίδες, αναφέρει η εφημερίδα Γκαρντιαν. Σύμφωνα με τους Νιου Γιόρκ Ταιμς, η αλλαγή δεν αντιπροσωπεύει μια πτώση στη δημοτικότητα των εφημερίδων αλλά μάλλον τον σχεδόν διπλασιασμό του

αριθμού των ανθρώπων που ονομάζουν το διαδίκτυο ως την πρωταρχική ειδησεογραφική πηγή τους. Στην πραγματικότητα, οι εφημερίδες κέρδισαν ένα τοις εκατό σε δημοτικότητα το 2008.[Editors weblog]

Ενεργοί πράκτορες οι οποίοι είναι επίσης γνωστοί και σαν “δικτυακά ρομπότ” ή απλά “μποτ”, χτενίζουν το ιντερνέτ για πληροφορίες διαφόρων κατηγοριών, που έχουν ενδιαφέρον για κάποιο χρήστη, εντοπίζουν τις ανανεώσεις δικτυακών τόπων και ενημερώνουν τους χρηστές για την παρουσία συγκεκριμένων προσώπων στο δίκτυο. Ορισμένα “μποτς” μαζεύουν διευθύνσεις που χρησιμοποιούνται για την αποστολή ενοχλητικών μηνυμάτων ηλεκτρονικού ταχυδρομείου. Λίστες συζητήσεων ηλεκτρονικού ταχυδρομείου, ομάδες νέων, τηλεδιασκέψεις και συζητήσεις σε πραγματικό χρόνο αποτελούν χώρους απόκτησης πληροφοριών σε συγκεκριμένα θέματα. Μέσα ζωντανής μουσικής και βίντεο επιτρέπουν στους χρήστες να παρακολουθούν ή να συμμετέχουν στις σχετικές εκδηλώσεις την ώρα που αυτές λαμβάνουν χώρα.

Με τα μέσα αυτά γίνεται δυνατή η απόκτηση πληροφοριών άμεσα με τη θέση της κατάλληλης ερώτησης σε μια ομάδα συζήτησης στο ιντερνέτ ή με το κατάλληλο ερώτημα σε μία μηχανή αναζήτησης. Το μειονέκτημα τους, βέβαια, είναι ότι μπορεί να κατακλυστεί κανείς από πληροφορίες άσχετες με αυτές που ψάχνει. Μια αναζήτηση στο web μπορεί να έχει σαν αποτέλεσμα δεκάδες χιλιάδες sites, τα οποία σταδιακά υποβιβάζουν, αν δεν εξαφανίζουν τελείως την πρακτική χρησιμότητα τους. Η αυτόματη αναζήτηση εξάλλου έχει περιορισμένες ικανότητες για τον εντοπισμό πληροφοριών, με αποτέλεσμα κάποιες από αυτές να μην είναι σημαντικές για τον ερωτώντα. Τα συγκεκριμένα μέσα αναζήτησης βελτιώνονται συνεχώς, όπως πχ με την κατάταξη των διαφόρων πληροφοριών του web σε κατηγορίες, είναι όμως μάλλον βέβαιο πως δεν θα μπορούσαν να αντιμετωπίσουν μία έκρηξη πληροφοριών.

Πολλές εταιρίες ανοίγουν τις πόρτες τους στους εσωτερικούς και στους ξένους ανταγωνιστές τους τοποθετώντας στις σελίδες τους στο web πληροφορίες για την αξία του δυναμικού τους , στις οποίες περιλαμβάνονται πληροφορίες για τα

τρέχοντα και τα σχεδιαζόμενα προϊόντα τους καθώς και τα ονόματα των βασικών τους στελεχών οι οποίοι θα μπορούσαν να στρατολογηθούν από τους ανταγωνιστές τους .Αυτό δεν σημαίνει ,βέβαια, πως δεν θα πρέπει να καταχωρούνται τέτοιες πληροφορίες, δεδομένου ότι αυτές προσπορίζουν επίσης οφέλη στο χώρο του μάρκετινγκ. Παραπέρα οι ανταγωνιστές τους που στηρίζουν τις στρατηγικές τους στο παιχνίδι της "αρπαχτής" δεν είναι πάντοτε πιθανό ότι στο τέλος θα έχουν επιτυχία.

2.3.1 ΔΙΑΡΡΟΗ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

Προσωπικές πληροφορίες που κάποτε υπήρχαν μόνο σε αρχεία δικαστηρίων είναι τώρα διαθέσιμες μέσω ενσύρματων γραμμών καθώς οικονομικά διεφθαρμένες κυβερνήσεις προσπαθούν να κερδίσουν χρήματα από πληροφορίες που έχουν να κάνουν με μητρώα οδηγών ,στοιχεία εκλογέων ,έγγραφα ακίνητης περιουσίας ,διαζύγια και πτωχεύσεις .Η Διεύθυνση Αυτοκινούμενων Οχημάτων της πολιτείας του Meriland στην Αμερική εξοικονόμησε $12,9 εκατ. το 1996 από τη πώληση δεδομένων της βάσης που διατηρούσε και τα οποία αφορούσαν τρία εκατομμύρια οδηγούς, σε δικηγόρους , σε ασφαλιστικές εταιρίες ,σε αυτούς που ταχυδρομούν διαφημιστικά έντυπα και σε μεμονωμένα άτομα. Όταν οι ενδιαφερόμενοι παραπονέθηκαν , ψηφίστηκε ένας πολιτειακός νόμος, που έδινε στους αυτοκινητιστές τη δυνατότητα να μην επιτρέπουν στα αρχεία τους πρόσβαση του κοινού.

Επιχειρήσεις, κυβερνήσεις και εκπαιδευτικά ιδρύματα στις ΗΠΑ ανέφεραν σχεδόν 50% περισσότερες παραβιάσεις δεδομένων το 2008 σε σχέση με το 2007, με αποτέλεσμα να βρεθούν εκτεθειμένα τα προσωπικά δεδομένα τουλάχιστον 35,7 εκ Αμερικάνων. Σύμφωνα με το μη κερδοσκοπικό Κέντρο Κλοπής Προσωπικών Στοιχείων, οι αναφορές παραβιάσεων δεδομένων έφτασαν τις 656 το 2008, από 446 τον προηγούμενο χρόνο. Σχεδόν 37% των παραβιάσεων παρουσιάστηκαν σε επιχειρήσεις, ενώ στα σχολεία εμφανίστηκαν

το 20%των περιπτώσεων. Το Κέντρο βρήκε επίσης ότι το ποσοστό των παραβιάσεων που αφορά σε κλοπή δεδομένων από νυν και πρώην υπαλλήλους υπερδιπλασιάστηκε από το 7% το 2007 σε σχεδόν 16% το 2008.[Benton/Washington post]

2.3.2 ΨΑΧΝΟΝΤΑΣ ΣΤΟ WEB

Οι διαχειριστές Web sites συγκεντρώνουν πληροφορίες για τους επισκέπτες των sites τους σε ορισμένες περιπτώσεις, χωρίς οι τελευταίοι να το ξέρουν ή να έχουν δώσει τη συγκατάθεση τους για κάτι τέτοιο.Στη χειρότερη περίπτωση, οι διαχειριστές αυτοί μπορούν να έχουν τη διεύθυνση του παροχέα ιντερνέτ (IP) του χρήστη, το λειτουργικό σύστημα του υπολογιστή του, το είδος του φυλλομετρητή που χρησιμοποιεί από το πρωτόκολλο του ιντερνέτ, για να κατευθύνει τα μηνύματα σε ένα υπολογιστή. Είναι μια ομάδα από τέσσερις αριθμούς, που χωρίζονται με τελείες, όπως πχ “88.2.65.215”.

Δικτυακοί τόποι οι οποίοι πωλούν αγαθά ή υπηρεσίες ζητούν να τους δοθούν ονόματα, διευθύνσεις και αριθμοί πιστωτικών καρτών σε μία φόρμα παραγγελίας. Sites τα οποία κάνουν διάφορες προσφορές και σε αντάλλαγμα για την εγγραφή σε αυτά ζητούν πληροφορίες , που έχουν να κάνουν με την εκπαίδευση, το επάγγελμα, το εισόδημα ή το τρόπο ζωής. Μία έρευνα που έγινε το1997, σε Web Sites 70 ομοσπονδιακών οργανισμών της Αμερικής από την OMB Watch διαπίστωσε πως 31 από αυτά ζητούσαν από τους επισκέπτες τους προσωπικές πληροφορίες τους, όπως το όνομα τους, τη διεύθυνση τους και το εργασιακό τους παρελθόν. Μόνο δε οι 11 από αυτές δήλωναν το πώς χρησιμοποιούσαν τις πληροφορίες αυτές.

Μια τεχνολογία του Web, με ξεχωριστή σημασία είναι αυτή που αφορά τα λεγόμενα “cookies” (κουλουράκια). Όταν ένας χρήστης επισκέπτεται ένα site, το site αυτό δημιουργεί ένα αρχείο, που ονομάζεται cookie, και το στέλνει στο φυλλομετρητή του χρήστη για αποθήκευση. Την επόμενη φορά που ο χρήστης θα επισκεφτεί το site, ο φυλλομετρητής επιστρέφει το cookie στο site, το οποίο το ενημερώνει και το στέλνει πάλι στο φυλλομετρητή. Με το καιρό το cookie μπορεί να συγκεντρώσει πληροφορίες, που αφορούν τις δραστηριότητες του χρήστη στο site, όπως πχ το ποιες σελίδες επισκέπτεται. Ένα site μπορεί να χρησιμοποιεί τα cookies που δημιουργεί για να διαδώσει τις web σελίδες του

και με το τρόπο αυτό να τραβήξει την προσοχή διαφημιστών και επισκεπτών. Ορισμένα εμπορικά sites χρησιμοποιούν τα cookies για την συμπλήρωση μιας ενσύρματης “κάρτας αγορών”, επιτρέποντας στους χρήστες να επισκεφτούν το site πολλές φορές σε μία περίοδο ημερών ή εβδομάδων, προτού να προχωρήσουν στον ουσιαστικό έλεγχο της. Τα cookies επιτρέπουν επίσης σ'ένα χρήστη την επιστροφή σε sites, που απαιτούν εγγραφή χωρίς να χρειαστεί να επανεγγραφή σε αυτά.

Τα cookies ενός χρήστη σώζονται σε ένα αρχείο του υπολογιστή του. Τα cookies ενός site δεν είναι διαθέσιμα σε άλλα sites και ένα site δεν μπορεί να χρησιμοποιήσει cookies με σκοπό την απόκτηση πρόσβασης σε πληροφορίες που έχουν αποθηκευτεί στον υπολογιστή του χρήστη. Ένα cookie δεν είναι τμήμα εκτελέσιμου κώδικα και έτσι δεν μπορεί να ψάξει στο σκληρό δίσκο ενός χρήστη, για να βρει ευαίσθητες πληροφορίες και να τις επιστρέψει στο δίσκο του web site. Παρόλα αυτά, τα cookies έχουν θεωρηθεί σοβαρές απειλές για την ιδιωτική ζωή ενός ατόμου. Σε μια χρόνια η εφημερίδα της Νέας Υόρκης “New York Times” δημοσίευσε 50 άρθρα για τα cookies και μια άλλη εφημερίδα, η “Wired News” ανέφερε 35 σχετικές ιστορίες. Η U.S. Department of Energy's Computer Incident Advisory Capability (CIAC) έγραψε ότι “Οι λαϊκές αντιλήψεις και οι φήμες για το τι είναι ένα cookie και τι μπορεί να κάνει έχουν πάρει μυθικές διαστάσεις.” Μετά την εκτίμηση των απειλών που προέρχονται από τα cookies,η CIAC κατέληξε στο συμπέρασμα, “Το ευπρόσβλητο των συστημάτων να κάνουν ζημιές ή να παίρνουν αδιάκριτες πληροφορίες χρησιμοποιώντας τα cookies του φυλλομετρητη τους ουσιαστικά δεν υφίστανται.” Παρόλα αυτά όμως, οι χρήστες που ενδιαφέρονται για τα cookies μπορούν να σβήσουν το συγκεκριμένο αρχείο ή να ρυθμίσουν το φυλλομετρητή τους να μην τα αποδέχεται.

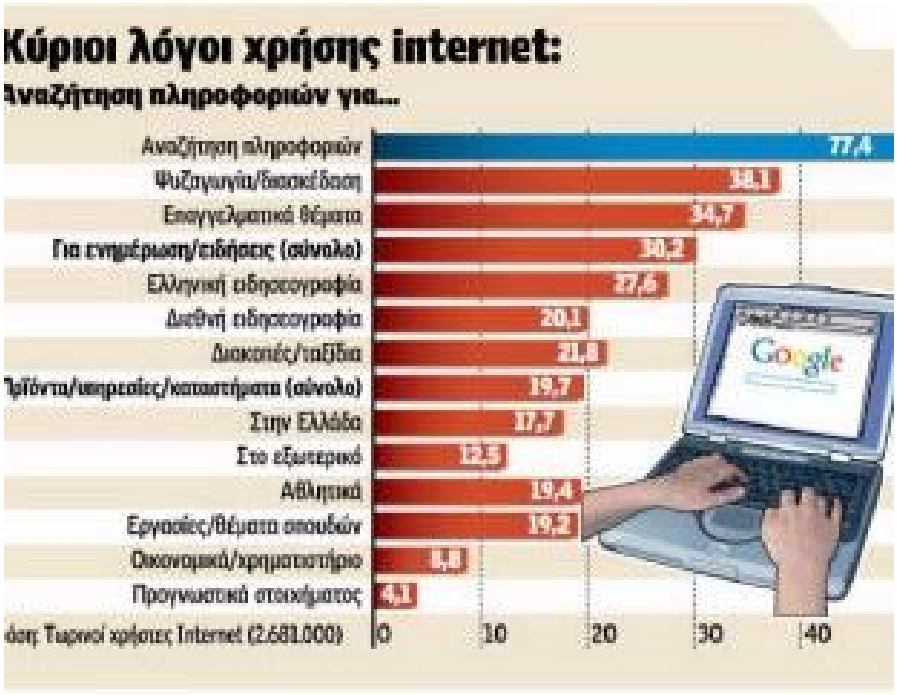
2.3.3 ΠΑΡΑΒΙΑΣΕΙΣ ΑΠΟΚΛΕΙΣΤΙΚΟΤΗΤΑΣ (COPYRIGHT)

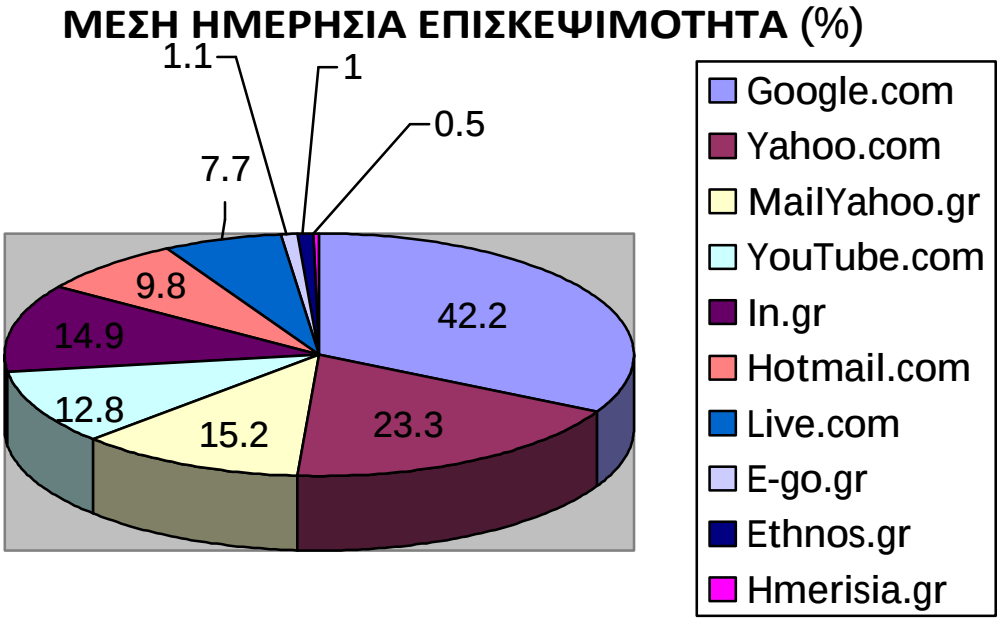
Το γεγονός ότι οι πληροφορίες δημοσιεύονται ελεύθερα, ταχυδρομούνται στο ίντερνετ ή πωλούνται σε καταστήματα λιανικών πωλήσεων δε σημαίνει ότι μπορεί να τις παίρνει ο καθένας και να τις χρησιμοποιεί όπως αυτός νομίζει. Οι πληροφορίες μπορεί να προστατευτούν με τους νόμους για την ευρεσιτεχνία, την αποκλειστικότητα (copyright) και τα εμπορικά σήματα. Η ευρεσιτεχνία δίνει στους κατόχους της το δικαίωμα της αποκλειστικής χρήσης εφευρέσεων τους και της παροχής άδειας για τη χρησιμοποίηση τους από τρίτους, που μπορούν να ενσωματωθούν στο υλικό μέρος ή σε προγράμματα υπολογιστών. Το copyright δίνει στους ιδιοκτήτες το αποκλειστικό δικαίωμα της αναπαραγωγής των έργων τους, της δημιουργίας παραγώγων έργων, και της διανομής, έκθεσης και διεύθυνσης τους. Αυτό ισχύει για πρωτότυπα συγγραφικά έργα , στα οποία περιλαμβάνονται τα γραπτά, οι φωτογραφίες, οι ζωγραφιές, η μουσική, τα βίντεο, τα προγράμματα των υπολογιστών και άλλα απτά έργα. Τα εμπορικά σήματα δίνουν στους ιδιοκτήτες τους το δικαίωμα του περιορισμού της χρήσης διακεκριμένων σημάτων σε συγκεκριμένα πλαίσια. Αυτά ισχύουν για λέξεις, σύμβολα και σχέδια, ήχους και ξεχωριστά χρώματα.

Η παραβίαση της αποκλειστικότητας περιλαμβάνει την απόκτηση προστατευόμενων έργων χωρίς την άδεια του ιδιοκτήτη τούς, και στην περίπτωση που πωλούνται με κάποιο αντίτιμο, χωρίς την κανονική αποζημίωση για αυτά του ιδιοκτήτη τους. Συνήθως ο πειρατής δεν πληρώνει τίποτα για τα έργα που αποκτά. Στη θεωρία, ο ιδιοκτήτης χάνει το εισόδημα, που αυτός ή αυτή θα αποκτούσε από μια νόμιμη πώληση. Ο υπολογισμός των απωλειών του είδους αυτού είναι δύσκολος, δεδομένου ότι δεν μπορεί να διαπιστωθεί εύκολα το εάν ο πειρατής θα είχε πληρώσει τη μεγαλύτερη τιμή που θα του ζητείτο. Ορισμένοι υποστηρίζουν πως ένας περιορισμένος αριθμός περιπτώσεων πειρατείας λογισμικού εξυπηρετεί τους κατόχους, καθώς οι πειρατές είναι πιθανόν να αποτελέσουν μελλοντικούς πελάτες των προϊόντων τους ή να ενθαρρύνουν τρίτους να τα αγοράσουν.

Τα εμπορικά προγράμματα γίνονται τακτικά αντικείμενα πειρατείας και αποστέλλονται σε ιδιώτες BBS και FTP sites, απ'όπου μπορεί κανείς να τα προμηθευτεί (κατεβάσει). Τα πειρατικά προγράμματα περνούν από τρία στάδια: απόκτηση, προετοιμασία και διανομή. Στην αρχή τα προγράμματα αγοράζονται από ένα νόμιμο σημείο διανομής τους ή αποκτώνται από τον οργανισμό, που τα κατασκεύασε ή που έχει τα νόμιμα δικαιώματα για την κυκλοφορία τους.

Στην συνέχεια αφαιρούνται τα χαρακτηριστικά της ασφάλειας τους, που εμποδίζουν την κυκλοφορία τους. Αυτό μπορεί να προϋποθέτει το σπάσιμο κωδικών κρυπτογράφησης ή το σβήσιμο μαρκαρισμάτων. Τα εξωτερικά χαρακτηριστικά διαγράφονται έτσι ώστε τα προγράμματα να είναι αρκετά μικρά, για να μπορούν να μεταβιβασθούν ηλεκτρονικά. Τέλος, τα προγράμματα κυκλοφορούν μέσω ενός πυραμιδικού σχήματος. Οι “ελιτίστικες” ομάδες πειρατικών προγραμμάτων τοποθετούν τα προγράμματα αυτά σε ειδικά sites γνωστά σαν “distro” sites. Η πρόσβαση σε αυτά ελέγχεται αυστηρά για να μην επέμβουν ομάδες προστασίας του copyright και για να προστατευτεί η ανωνυμία εκείνων που τα στέλνουν. Από τα distro sites τα προγράμματα αντιγράφονται στα λεγόμενα “leech” sites τα οποία τα διαθέτουν δωρεάν ή στα “ratio” sites τα οποία λειτουργούν με το σύστημα των ανταλλαγών. Τα sites αυτά λειτουργούν συχνά σαν ιδιωτικά FTP. Από τη στιγμή που θα έρθουν στα δεύτερα sites, τα προγράμματα κυκλοφορούν σε όλη την ηλεκτρονική κοινότητα.





Έρευνα: web ID εταιρία Focus Bari

1995 – 2007 Υπό την αιγίδα παρατηρητηρίου για τη κοινωνία της πληροφορίας

2.3.4 ΠΑΡΑΒΙΑΣΕΙΣ ΕΜΠΟΡΙΚΩΝ ΣΗΜΑΤΩΝ

Τα εμπορικά σήματα έχουν βρεθεί στο επίκεντρο πολλών διενέξεων για θέματα πνευματικής ιδιοκτησίας.

Οι περισσότερες από τις μάχες για τα εμπορικά σήματα στο ιντερνέτ γίνονται για τα ονόματα κυριότητας (domain names),ονόματα δηλαδή όπως “georgetown.edu”, τα οποία προσδιορίζουν συγκεκριμένα sites στο ιντερνέτ, και στην παραπάνω περίπτωση το Πανεπιστήμιο του Georgetown. Επειδή αυτό είναι ένα εκπαιδευτικό ίδρυμα, το Georgetown του έχει δοθεί σαν ένα domain name, που συνοδεύεται από το επικεφαλής domain “edu”. Στο Georgetown λειτουργούν επίσης και τα δικά του τμήματα-domains .Για παράδειγμα το “cs.georgetown.edu” αναφέρεται στο τμήμα της επιστήμης των υπολογιστών που λειτουργεί στο Πανεπιστήμιο αυτό.

Οι διαμάχες για τα domain names ξεσπούν, όταν κάποιος κατοχυρώνει ένα domain name για ένα site και το οποίο περιέχει ένα όνομα εμπορικού σήματος. Ο πειρατής κερδίζει με το τρόπο αυτό το προνόμιο να χρησιμοποιεί αυτός ένα όνομα που μπορεί να έχει ευρύτατα αναγνωριστεί, ενώ ο ιδιοκτήτης του συγκεκριμένου εμπορικού σήματος δεν έχει τη δυνατότητα να χρησιμοποιεί το ίδιο του το όνομα.

Εξετάζοντας το θέμα από πολλές απόψεις, θα πρέπει να πούμε ότι ένας σύνδεσμος στο web είναι σαν μία παραπομπή σε ένα άρθρο ή σένα βιβλίο, για την οποία, βέβαια, δεν χρειάζεται καμία άδεια. Κάνοντας “κλικ” σε αυτόν, το αποτέλεσμα είναι η παρουσίαση του αναφερόμενου εγγράφου στην οθόνη, σε κάποιες περιπτώσεις πλαισιωμένο από υλικό, που αφορά το site αναφοράς. Το αποτέλεσμα της τοποθέτησης των πλαισίων είναι ότι το υλικό αυτό φαίνεται, πως ανήκει στο site που το περιλαμβάνει, και ότι το site αυτό δεν έχει την δυνατότητα να παρουσιάσει το έγγραφο πλαισιωμένο από το δικό του περιεχόμενο, το οποίο τυπικά περιέχει και διαφημίσεις. Παρότι αρκετοί οργανισμοί δεν έχουν αντίρρηση να συνδέεται κάποιος με το site τους – πράγμα που αυξάνει τους επισκέπτες τους- άλλοι δεν επιθυμούν τα θέματα , που τους

αφορούν, να αποτελούν το περιεχόμενο του site κάποιου τρίτου.

2.4 ΕΙΣΒΟΛΕΣ ΣΕ ΥΠΟΛΟΓΙΣΤΕΣ

Σαν πράξεις οι εισβολές σε απομακρυσμένους υπολογιστές συνιστούν μια μορφή υπερκείμενης απάτης, με την έννοια ότι αυτή γίνεται σε βάρος της χρήσης ενός υπολογιστή από τον κανονικό του χρήστη, οι εισβολείς με το τρόπο αυτό κινούνται χωρίς να πληρώνουν, επιβαρύνοντας το λογαριασμό κάποιου άλλου. Ακόμα κι αν οι δραστηριότητες τους δεν δημιουργούν πραγματικά έξοδα, δημιουργούν έξοδα στους ιδιοκτήτες ενός συστήματος, οι οποίοι σπαταλούν χρόνο για να εντοπίσουν τις ενέργειες τους και για να ξεκαθαρίσουν τα ψηφιακά σκουπίδια που αυτοί αφήνουν πίσω τους. Οι σχετικές απώλειες μπορεί να είναι σημαντικές, ιδιαίτερα εάν έχουν διαγραφεί δεδομένα, τα οποία δεν είναι δυνατόν να ανακτηθούν.

Ένα άλλο είδος επιθέσεων είναι αυτές που αχρηστεύουν το σύστημα με επιθέσεις από απόσταση του τύπου της “άρνησης παροχής υπηρεσιών”. Οι επιτιθέμενοι εδώ δε χρειάζεται να εισβάλλουν στους υπολογιστές που αχρηστεύουν.

2.4.1 ΛΟΓΑΡΙΑΣΜΟΙ

Η μέθοδος που ακολουθείται για την εισβολή σε έναν υπολογιστή προϋποθέτει την απόκτηση ενός λογαριασμού πρόσβασης στο σύστημα στο οποίο αυτός ανήκει. Χρησιμοποιώντας το λογαριασμό, ο εισβολέας μπορεί να κάνει κάθε ενέργεια που έχει επιτραπεί στον ιδιοκτήτη του, όπως πρόσβαση σε αρχεία, τρέξιμο προγραμμάτων για την ανάγνωση και τροποποίηση εγγράφων, ανάγνωση μηνυμάτων ηλεκτρονικού ταχυδρομείου, που έχουν σταλεί σε αυτόν, αποστολή μηνυμάτων ηλεκτρονικού ταχυδρομείου από το λογαριασμό σε τρίτους, και καταστροφή αρχείων. Εν συντομία, ο εισβολέας αποκτά πλήρη πρόσβαση στο λογαριασμό και με αυτή πλήρη πρόσβαση σε όλες τις πηγές, που είναι διαθέσιμες στο λογαριασμό αυτό. Το τι μπορεί να επακολουθήσει

εξαρτάται από τις ενέργειες, που έχει τη δυνατότητα να κάνει ο συγκεκριμένος λογαριασμός.

Πολλά συστήματα διαθέτουν ένα προνομιακό λογαριασμό , που ονομάζεται λογαριασμός βάσης στα συστήματα Unix και λογαριασμός του διαχειριστή στα Windows NT. Ο λογαριασμός αυτός χρησιμοποιείται από διαχειριστές συστημάτων για τη διαχείριση του συστήματος τους. Οποιοσδήποτε χρησιμοποιεί το λογαριασμό έχει πρόσβαση σε όλα τα προγράμματα και τα δεδομένα του συστήματος. Από το λογαριασμό αυτό ένας εισβολέας μπορεί να τρέξει οποιοδήποτε πρόγραμμα και να διαβάσει, να αλλάξει ή να διαγράψει οποιοδήποτε αρχείο. Από τη στιγμή που θα αποκτηθεί έλεγχος στο λογαριασμό ενός χρήστη, είναι μάλλον εύκολη η πρόσβαση σ'ενα προνομιακό λογαριασμό.

Για να αποκτήσει πρόσβαση ένας εισβολέας σ' ένα λογαριασμό, χρειάζεται αρχικά να αποκτήσει πρόσβαση στο μηχάνημα πού τον φιλοξενεί, είτε με τηλεφωνική γραμμή, είτε μέσω δικτυακής σύνδεσης. Εάν το σύστημα είναι στο ιντερνέτ και ο εισβολέας γνωρίζει το όνομα του τομέα του (domain) ή τη διεύθυνση του παροχέα του (IP Adress), τότε ένας τρόπος σύνδεσης είναι μέσω του Telnet, μια εφαρμογή του ιντερνέτ για είσοδο στο σύστημα από απόσταση.

Εάν ένα έγκυρο όνομα λογαριασμού και ένας κωδικός πρόσβασης δεν είναι γνωστά, ο χάκερ μπορεί να τα μαντέψει. Πολλοί χρήστες χρησιμοποιούν κωδικούς πρόσβασης που βρίσκονται εύκολα, όπως για παράδειγμα τα επώνυμα ή τα μικρά τους ονόματα.

2.4.2 ΕΡΓΑΛΕΙΑ ΚΑΙ ΤΕΧΝΙΚΕΣ

Οι εισβολείς στηρίζονται σε πληθώρα προγραμμάτων, τα οποία αποτελούν τα εργαλεία, που τους βοηθούν για να κάνουν μία επίθεση. Σε αυτά περιλαμβάνονται οι εντολές, που δίνονται από το πληκτρολόγιο, προγράμματα και κείμενα, που είναι σειρές εντολών, που περιέχονται σε ένα αρχείο και εκτελούνται σαν ομάδα, αυτόνομοι πράκτορες, οι οποίοι εκτελούν και

απλώνονται χωρίς την παρεμβολή του ιδιοκτήτη τους (όπως οι ιοί και τα σκουλήκια), και τα κιβώτια εργαλείων, τα οποία είναι πακέτα λογισμικού με εργαλεία. Με τη πάροδο του χρόνου, οι επιθέσεις έχουν γίνει σταδιακά όλο και πιο αυτοματοποιημένες και απειλητικές , επιτρέποντας με το τρόπο αυτό ακόμα και σε άπειρους εισβολείς να εισβάλλουν σε ένα σύστημα. Τα αυτοματοποιημένα εργαλεία των χάκερς είναι διαθέσιμα για τον καθένα μέσω του ιντερνέτ από πολυάριθμες ιστοσελίδες και από τόπους που χρησιμοποιούν το FTP (πρωτόκολλο μεταφοράς αρχείων).

- ΣΑΡΩΤΕΣ ΔΙΚΤΥΩΝ

Οι ειδικοί στην ασφάλεια των υπολογιστών έχουν αναπτύξει εργαλεία, για να βοηθήσουν τους διαχειριστές συστημάτων στον έλεγχο των δικτύων τους για μια σειρά προβλημάτων ασφαλείας, που παρουσιάζουν. Παραδείγματα τέτοιων εργαλείων αποτελούν ο Σαρωτής Ασφαλείας του ιντερνέτ (ISS), που δημιουργήθηκε από τον Christopher Klaus και το Εργαλείο Ανάλυσης της Ασφάλειας για τον Έλεγχο των Δικτύων (SATAN), το οποίο αναπτύχθηκε από τους Dan Farmer και Weste Venema. Το ISS 1. και το SATAN είναι διαθέσιμα στο internet όπου αυτά και άλλοι σαρωτές ανευρίσκονται από τους χάκερς και χρησιμοποιούνται για να βρεθούν οι τρύπες ασφαλείας ενός δικτύου , οι ανοιχτές πόρτες του και οι γενικές πληροφορίες που το αφορούν, καθώς και το αρχείο με το κωδικό εισόδου σε αυτό. Οι σαρωτές αυτοί είναι ίδιοι με τους κοινούς σαρωτές (scanners), παρέχουν όμως περισσότερες πληροφορίες. Ορισμένοι από αυτούς διαθέτουν δορυφορική διασύνδεση με το χρήστη και, έτσι, για να τους τρέξει κανείς χρειάζονται μόνο μέτριες τεχνικές γνώσεις.

Όταν ο Farmer και ο Venema ανήγγειλαν το 1995 ότι θα διέθεταν ελεύθερα το SATAN μέσω του internet, οι δύο ειδικοί ασφαλείας δέχτηκαν σκληρή κριτική επειδή παρέδιδαν στα χέρια του υποκόσμου των υπολογιστών ένα εργαλείο με τόσο μεγάλη δύναμη. Ορισμένοι μάλιστα προέβλεπαν και την εξαιτίας του γεγονότος αυτού κατάρρευση του διαδικτύου. Στο τέλος, τα περισσότερα από

όσα αναμένονταν δε συνέβησαν. Ωστόσο μία εβδομάδα περίπου μετά την διάθεση του, διαπιστώθηκε σε αυτό ένα πρόβλημα, το οποίο σε σπάνιες περιπτώσεις θα μπορούσε να έχει ανοίξει ένα δίκτυο σε τρίτους. Εάν το SATAN έτρεχε σε ορισμένους φυλλομετρητές στους οποίους περιλαμβανόταν και το Netscape Navigator, το μηχάνημα που το έτρεχε θα μπορούσε να υποστεί εισβολή από μια άλλη ιστοσελίδα. Ο Farmer κατέβασε μια καινούργια έκδοση με οδηγίες για την αποφυγή του προβλήματος. Το πρόβλημα που παρουσιάστηκε δείχνει πως ακόμα και τα εργαλεία ασφαλείας μπορούν να προκαλέσουν ζημιές σε ένα σύστημα.

Το 1996 ο Farmer χρησιμοποίησε το SATAN για να κάνει μία ενδελεχής έρευνα σε 1700 περίπου ιστοσελίδες υψηλού προφίλ. Οι ιστοσελίδες αυτές άνηκαν σε τράπεζες και σε πιστωτικούς οργανισμούς, σε ορισμένες ομοσπονδιακές υπηρεσίες των Η.Π.Α σε εφημερίδες και σε ορισμένες εμπορικές επιχειρήσεις. Χωρίς να μπει πραγματικά στα συστήματα τους, διαπίστωσε πως ένα ποσοστό άνω των 60% από αυτά θα μπορούσαν να υποστούν εισβολή ή να καταστραφούν (όλες οι λειτουργίες του δικτύου να διαγραφούν ή να μεταφερθούν) και ότι ένα επιπλέον ποσοστό από 9% έως 24% θα μπορούσε να αποτελέσει αντικείμενο εισβολής εάν διαπιστωνόταν το παραμικρό ελάττωμα σε αυτό. Συγκρινόμενο με τα παραπάνω, ένα ψευτοτυχαίο δείγμα 500 ιστοσελίδων χαμηλού προφίλ βρέθηκε να μην αντιμετωπίζει ανάλογα προβλήματα κατά το ήμισυ, με το 30% περίπου από αυτές να μην έχουν σοβαρή προστασία.

Οι χάκερς χρησιμοποιούν συχνά σαρωτές για να βρίσκουν τις αδυναμίες των συστημάτων.

- SNIFFERS ΠΑΚΕΤΩΝ

Το μεγαλύτερο τμήμα της κυκλοφορίας δεδομένων σε δίκτυα υπολογιστών είναι δυνατόν να καταστεί αντικείμενο παρακολούθησης μέσω των sniffers (αναρροφητών). Αυτά είναι προγράμματα που εγκαθίστανται σε ορισμένους

υπολογιστές, που συνδέονται με το δίκτυο. Το sniffer συλλαμβάνει μηνύματα, καθώς αυτά ταξιδεύουν μέσα στο δίκτυο, σώζοντας τα πιο ενδιαφέροντα από αυτά σε ένα ημερολογιακό αρχείο για μεταγενέστερη εξέταση. Επειδή τα μηνύματα διασχίζουν το δίκτυο σε ομάδες δεδομένων που ονομάζονται “πακέτα”, τα sniffers αναφέρονται σαν “sniffers πακέτων”. Ένα μήνυμα ηλεκτρονικού ταχυδρομείου ή μια ιστοσελίδα μπορούν να διαχωριστούν σε διάφορα πακέτα προτού να αρχίσουν το ταξίδι τους στο δίκτυο. Στο σημείο λήψης τους, τα πακέτα επανασυγκολλώνται για να συγκροτήσουν και πάλι όλο το μήνυμα.

Σε τελική ανάλυση, ένα sniffer μπορεί να μαζέψει πακέτα, τα οποία ταξιδεύουν προς ένα συγκεκριμένο υπολογιστή. Εάν αυτός ο υπολογιστής είναι ένας δρομολογητής ή ένας κόμβος εισόδου, που συνδέει δύο ή περισσότερα δίκτυα, η κυκλοφορία που γίνεται μέσω αυτού είναι υπολογίσιμη.

Σε ορισμένες δικτυακές τεχνολογίες ένα sniffer που έχει τοποθετηθεί σε οποιονδήποτε υπολογιστή, που συνδέεται με το δίκτυο, μπορεί να διαβάσει όλα τα εισερχόμενα μηνύματα ανεξάρτητα από τον προορισμό τους. Αυτό συμβαίνει, επειδή τα μηνύματα αυτά κυκλοφορούν μέσα στο δίκτυο, επιτρέποντας με το τρόπο αυτό σε κάθε υπολογιστή του δικτύου, τη συλλογή τους. Παρότι ένας υπολογιστής θα μπορούσε να ρυθμιστεί με τέτοιο τρόπο ώστε να αγνοεί τα μηνύματα που δεν απευθύνονται σε αυτόν, μπορεί ωστόσο να παραμείνει “αδιάκριτος” και να βλέπει όλη τη κυκλοφορία του δικτύου, στο οποίο ανήκει. Κανένας υπολογιστής, βέβαια, δεν μπορεί να δει την κυκλοφορία μηνυμάτων άλλων δικτύων. Για παράδειγμα, ένα sniffer που έχει τοποθετηθεί σε ένα τοπικό δίκτυο δεν μπορεί να παρακολουθήσει την κυκλοφορία ενός άλλου τοπικού δικτύου (LAN).

Στην αρχή του φθινοπώρου του 1993, το CERT/CC διαπίστωσε μια έξαρση εισβολών στο internet, οι οποίες ήταν βασικά διαφορετικές από προηγούμενες επιθέσεις. Οι χάκερς εισέβαλαν σε συστήματα, όπου και εγκαθιδρούσαν προγράμματα sniffers, για να πάρουν τα ονόματα χρηστών και κωδικών

εισόδου κατά τη διάρκεια της λειτουργίας. Η συλλογή των σχετικών πληροφοριών δεν ήταν δύσκολη, όπως αναμενόταν από τα προγράμματα που χρησιμοποιούσαν. Σε ορισμένες περιπτώσεις, οι χάκερς εισέβαλαν στα συστήματα περιφερειακών παροχέων ίντερνετ, από όπου συνέλεγαν μεγάλες ποσότητες στοιχείων από τα sniffers που είχαν εγκαταστήσει.

- HACKING ΚΑΙ CRACKING

Εάν θα έπρεπε να διαχωρίσουμε τους όρους hacker και cracker το συμπέρασμα θα ήταν:

- Ένας hacker είναι εκείνος που ενδιαφέρεται έντονα για τις μυστικές και απόκρυφες λειτουργίες οποιουδήποτε λειτουργικού συστήματος υπολογιστή. Οι hackers είναι συχνά προγραμματιστές. Ως προγραμματιστές, οι hackers έχουν προχωρημένη γνώση των λειτουργικών συστημάτων και των γλωσσών προγραμματισμού. Ίσως ανακαλύψουν κενά μέσα στα συστήματα και τους λόγους της ύπαρξης αυτών των κενών. Οι hackers αναζητούν σταθερά πρόσθετη γνώση, μοιράζονται ελεύθερα ότι ανακαλύψουν και ποτέ δεν καταστρέφουν δεδομένα σκοπίμως.
- Ένας cracker είναι εκείνος που διεισδύει ή διαφορετικά παραβιάζει την ακεραιότητα συστήματος απομακρυσμένων μηχανών, με κακή πρόθεση. Έχοντας αποκτήσει μη εντεταλμένη πρόσβαση, οι crackers καταστρέφουν δεδομένα ζωτικής σημασίας, αποτρέπουν την εξυπηρέτηση των νόμιμων χρηστών ή προξενούν προβλήματα στα θύματα τους. Οι crackers μπορούν εύκολα να προσδιοριστούν , επειδή οι ενέργειες τους είναι κακόβουλες.

Στην εργασία αυτή θα χρησιμοποιούμε τον όρο hacker, καθώς είναι ο πιο διαδεδομένος, για να μην υπάρξει σύγχυση.

Τυπικά, οι κωδικοί εισόδου των λογαριασμών των χρηστών είναι αποθηκευμένοι σε ένα αρχείο του συστήματος κρυπτογραφημένοι, από όπου

χρησιμοποιούνται σαν ένα κλειδί αποκρυπτογράφησης μιας γνωστής ομάδας δεδομένων. Εάν οι χάκερς μπορέσουν να αποκτήσουν πρόσβαση στο αρχείο αυτό , θα έχουν τη δυνατότητα να σπάσουν τους κωδικούς χρησιμοποιώντας ένα πρόγραμμα. Τα προγράμματα αυτά κάνουν αυτό που είναι γνωστό σαν “επίθεση λεξικού”. Δηλ. παίρνουν κάθε λέξη ενός λεξικού, τη χρησιμοποιούν σαν κλειδί κρυπτογράφησης της ομάδας των γνωστών δεδομένων και στη συνέχεια συγκρίνουν το αποτέλεσμα με μία εγγραφή του αρχείου. Εάν αυτά ταιριάζουν, τότε η λέξη αυτή είναι ο επιθυμητός κωδικός του συγκεκριμένου λογαριασμού. Εκτός από τις λέξεις του λεξικού , το πρόγραμμα μπορεί να δοκιμάσει συνηθισμένες λέξεις, όπως για παράδειγμα, ονόματα που συλλαβίζονται ανάποδα και σειρές γραμμάτων του πληκτρολογίου όπως “asdf”. Το σπάσιμο των κωδικών συνήθως γίνεται εύκολα, επειδή πολλοί χρήστες χρησιμοποιούν κωδικούς, που μπορεί εύκολα να μαντέψει κανείς.

Οι ειδικοί ασφάλειας χρησιμοποιούν τα ίδια εργαλεία σπασίματος κωδικών, που χρησιμοποιούν και οι χάκερς, προκειμένου να εκτιμήσουν την ασφάλεια των δικών τους αρχείων κωδικών.

- ΥΠΕΡΧΕΙΛΙΣΗ ΠΕΡΙΟΧΗΣ ΜΝΗΜΗΣ ΠΡΟΣΩΡΙΝΗΣ ΑΠΟΘΗΚΕΥΣΗΣ ΠΛΗΡΟΦΟΡΙΩΝ

Μερικές φορές οι χάκερ εισβάλλουν σε συστήματα χωρίς να χρησιμοποιούν ένα λογαριασμό ή ένα κωδικό εισόδου. Πράγματι, στην περίπτωση αυτή επιζητούν τη βοήθεια ενός προγράμματος που τρέχει ήδη στο σύστημα το οποίο το χρησιμοποιούν σαν ένα όχημα για την εισαγωγή επιβλαβούς κώδικα σ'αυτό, ο οποίος στη συνέχεια εκτελείται.

Για να κάνουν το σύστημα να τρέξει το δικό τους κώδικα, οι χάκερς δημιουργούν μια μεγάλη σειρά στοιχείων , που εισάγουν στο πρόγραμμα, που αποτελεί το στόχο τους. Η εισαγόμενη σειρά στοιχείων περιλαμβάνει το κώδικα τους μαζί με άλλα δεδομένα. Φυσιολογικά, το πρόγραμμα που αποτελεί στόχο δεν θα εκτελούσε το κώδικα, που εισάγεται σε αυτό. Εάν, ωστόσο τα εισαγόμενα στοιχεία είναι τόσα πολλά ώστε να υπερφορτωθεί η μνήμη, που

διατίθεται για αυτά (που ονομάζεται “περιοχή προσωρινής αποθήκευσης.”), ο κώδικας κάτω από περιορισμένες προϋποθέσεις, μπορεί να εκτελεστεί. Ο λόγος που μπορεί να το προκαλέσει αυτό είναι ότι τα εισαγόμενα στοιχεία στο πρόγραμμα τοποθετούνται στο πάνω μέρος αυτού , που ονομάστηκε η “διαδικασία της συσσώρευσης”. Αυτή είναι μια προσωρινή περιοχή στην μνήμη του υπολογιστή, όπου το σύστημα καταγράφει τα εισαγόμενα στο πρόγραμμα στοιχεία και τον κώδικα που χρησιμοποιείται για την επεξεργασία τους. Οποτεδήποτε ζητείται η εκτέλεση μιας λειτουργίας του προγράμματος , επιστρέφεται μια διεύθυνση, η οποία υποδεικνύει το κώδικα που θα πρέπει να εκτελεστεί, όταν η συγκεκριμένη λειτουργία συμπληρωθεί και η οποία τοποθετείται στο πάνω μέρος των στοιχείων που μαζεύονται. Τότε η εισαγόμενη περιοχή προσωρινής αποθήκευσης τοποθετείται πάνω από αυτή. Εάν τα εισαγόμενα δεδομένα υπερχειλίσουν το χώρο της περιοχής προσωρινής αποθήκευσης, θα τον κάνουν να ρίξει τα δεδομένα, που έχει στη περιοχή της πυραμίδας που είναι από κάτω του, καταγράφοντας οτιδήποτε υπήρχε εκεί προηγουμένως, περιλαμβανόμενης και της διεύθυνσης που επέστρεψε. Εξετάζοντας προσεχτικά την σειρά των εισηγμένων στοιχείων, ο ενδιαφερόμενος θα μπορέσει να ρυθμίσει την περιοχή των συσσωρευθέντων στοιχείων η οποία περιέχει και την καταστραφείσα διεύθυνση, έτσι ώστε αυτή να στείλει τον επιβλαβή κώδικά προς την περιοχή της προσωρινής αποθήκευσης. Στη περίπτωση αυτή ο κωδικός θα εκτελεστεί στο μηχάνημα του χρήστη. Στη συνέχεια ο κώδικας εκτελείται έχοντας τα προνόμια του προγράμματος που εκμεταλλεύεται, το οποίο συνήθως είναι το βασικό. Η επίθεση αυτή αποφεύγεται εύκολα, εάν το πρόγραμμα μπορεί να ελέγξει το μέγεθος των εισαγόμενων στοιχείων, προτού αυτά να αρχίσουν να συσσωρεύονται. Δυστυχώς αυτό δεν το κάνουν όλα τα προγράμματα.

2.4.3 ΚΛΟΠΗ ΠΛΗΡΟΦΟΡΙΩΝ ΚΑΙ ΠΑΡΕΜΒΑΣΕΙΣ

Από τη στιγμή που θα γίνει εισβολή σε ένα λογαριασμό, ο εισβολέας μπορεί να αποκτήσει πρόσβαση, να διαβάσει και να κατεβάσει πληροφορίες, που επιτρέπεται να πάρει ο λογαριασμός αυτός, στις οποίες περιλαμβάνονται προσωπικό και ηλεκτρονικό ταχυδρομείο, διάφορα ατομικά ή ευαίσθητα έγγραφα, και βάσεις δεδομένων με πληροφορίες. Ακόμη και αν ο ιδιοκτήτης των πληροφοριών εξακολουθεί να έχει πρόσβαση στα πρωτότυπα, μπορεί να προκληθούν σε αυτόν αξιοσημείωτες βλάβες από αυτό που γενικά θεωρείται ως κλοπή πληροφοριών. Ο εισβολέας μπορεί να χρησιμοποιήσει τις πληροφορίες, για να αποκτήσει οικονομικά οφέλη ή για λόγους ανταγωνισμού ή για να επιφέρει στο νόμιμο ιδιοκτήτη τους κάποιες άλλες βλάβες.

Όπως αναφέραμε και νωρίτερα, οι εισβολείς συχνά παρεμβαίνουν στα δεδομένα των υπολογιστών, στους οποίους διεισδύουν. Έτσι δημιουργούν ψεύτικους λογαριασμούς, οι οποίοι τους εξασφαλίζουν μια μεταγενέστερη εισβολή τους, εγκαθιστούν προγράμματα sniffers με σκοπό τη σύλληψη ονομάτων χρηστών και κωδικών, διαγράφουν τα ίχνη τους από αρχεία εισόδου, αντικαθιστούν βοηθητικά προγράμματα με άλλα που κρύβουν τη παρουσία τους και παίρνουν και διάφορα άλλα μέτρα για να ενισχύσουν τις δραστηριότητες τους. Μερικοί πηγαίνουν ακόμη πιο μακριά και αλλάζουν προσωπικά αρχεία του χρήστη και εφαρμογές που χρησιμοποιεί, τις οποίες έχει αποθηκεύσει στο σύστημα, του αποτέλεσμα όλων αυτών των ενεργειών είναι η προβληματική λειτουργία όλου του συστήματος και των δεδομένων, που έχουν προσβληθεί. Το κόστος για τους ιδιοκτήτες του συστήματος περιλαμβάνει το χρόνο που θα διαθέτει για τη αποκατάσταση τόσο του ίδιου όσο και των δεδομένων του. Θα πρέπει να υπολογιστούν επίσης σ'αυτό και οι ζημιές που προκαλούνται από την αρνητική δημοσιότητα που προσλαμβάνει το συγκεκριμένο γεγονός και από την αδυναμία πρόσβασης στα κανονικά δεδομένα για ένα μακρύ χρονικό διάστημα.

2.5 ΜΕΤΑΜΦΙΕΣΕΙΣ

Οι κλέφτες της ταυτότητας κάποιου εισπράττουν χρήματα, συνάπτουν δάνεια και χρεώνουν τα αγαθά που αγοράζουν στο όνομα κάποιου. Οι πλαστογράφοι φτιάχνουν έγγραφα και μηνύματα ηλεκτρονικού ταχυδρομείου. Οι χάκερς κρύβουν επιβλαβείς κωδικούς σε προγράμματα δούρειων ίππων, που απέξω φαίνονται αθώα ή ελκυστικά, δυνάμεις επιβολής του νόμου παράλληλα οργανώνουν μυστικές επιχειρήσεις και στήνουν παγίδες, για να πιάνουν τους απατεώνες.

Στην ενότητα αυτή θα αναφερθούμε στις διάφορες μορφές μεταμφίεσης. Αυτό που όλες διαθέτουν από κοινού είναι το ότι εξαπατούν κάποιον στο να δεχτεί ψευδείς πληροφορίες ή ψεύτικα έγγραφα. Κάνοντας το αυτό ο απατεώνας μπορεί να αποκτήσει μεγαλύτερη πρόσβαση σε μία πληροφοριακή πηγή, είτε αυτή είναι η ταυτότητα ενός προσώπου είτε ένας τρόπος απόκτησης χρημάτων ή οι πληροφορίες που έχει ένας υπολογιστής. Η επιχείρηση αυτή μπορεί να υποβιβάζει την ακεραιότητά των πληροφοριακών πηγών ή να εμποδίζει τη νόμιμη χρήση τους από οποιονδήποτε.

2.5.1 Η ΚΛΟΠΗ ΤΑΥΤΟΤΗΤΑΣ

Ως κλοπή της ταυτότητας νοείται η διαστρέβλωση των στοιχείων της ταυτότητας ενός προσώπου περιλαμβανομένου του ονόματος του, του αριθμού της κοινωνικής του ασφάλισης, της άδειας του για οδήγηση, των αριθμών των πιστωτικών του καρτών και των αριθμών των τραπεζικών του λογαριασμών. Ο σκοπός που επιδιώκεται με αυτή είναι η δυνατότητα τέλεσης πράξεων, που επιτρέπονται στο κάτοχο της συγκεκριμένης ταυτότητας, όπως η ανάληψη μετρητών, η μεταφορά χρημάτων, η χρέωση αγορών, η απόκτηση πρόσβασης σε πληροφορίες ή η αποστολή εγγράφων και επιστολών με το όνομα του θύματος. Οι πληροφοριακές πηγές που προσβάλλονται στην περίπτωση αυτή, είναι τα έγγραφα και οι πληροφορίες που προσδιορίζουν το συγκεκριμένο

πρόσωπο. Σε αυτά περιλαμβάνονται τα έγγραφα από χαρτί, οι ταυτότητες, τα τραπεζικά βιβλιάρια, τα ηλεκτρονικά αρχεία καθώς και οι πληροφορίες, που περιλαμβάνονται σε όλα αυτά .Ο κλέφτης αποκτά με το τρόπο αυτό πρόσβαση στις πηγές και τις χρησιμοποιεί πλέον για λογαριασμό του. Η ακεραιότητα των πληροφοριών που αφορούν το θύμα, όπως αυτές που μιλούν για την οικονομική τους κατάσταση, υποβαθμίζεται επίσης. Το θύμα και εκείνοι που του έχουν προμηθεύσει τα σχετικά στοιχεία καθώς και οι διάφορες άλλες πηγές υφίστανται τις τυχόν απώλειες. Πολλές επιχειρήσεις του είδους αυτού, ιδιαίτερα εκείνες που αφορούν την απάτη με πιστωτικές κάρτες, αποτελούν περιπτώσεις πολύ σοβαρής απάτης, δεδομένης της δυνατότητας που αποκτά εξαιτίας τους ο κλέφτης στο να χρησιμοποιήσει τους τραπεζικούς λογαριασμούς του θύματος του.

Η κλοπή της ταυτότητας αφορά συνήθως την απάτη με πιστωτικές κάρτες. Οι κλέφτες κατασκευάζουν πλαστές κάρτες ή χρησιμοποιούν κλεμμένες κάρτες ή αριθμούς καρτών, για να προμηθευτούν αγαθά και υπηρεσίες. Επωφελούνται επίσης από τους ομοσπονδιακούς κανονισμούς για τις πιστώσεις, οι οποίοι απαιτούν την πίστωση του λογαριασμού ενός κατόχου πιστωτικής κάρτας αμέσως μόλις γίνει η πληρωμή της. Κάνοντας προπληρωμή ενός λογαριασμού ή πληρώνοντας παραπάνω από το υπάρχον υπόλοιπο με μία πλαστή επιταγή, μπορούν να πάρουν μετρητά προκαταβολικά προτού να γίνει η εκκαθάριση της πληρωμής της επιταγής.

Η κλοπή ταυτότητας μπορεί να χρησιμοποιηθεί για λόγους που δεν έχουν να κάνουν με την απόκτηση χρημάτων και οι οποίοι μπορεί να σχετίζονται, πχ. δανειζόμενος την ταυτότητα ενός γιαπωνέζου εθνικιστή που εξαφανίστηκε το 1965, ένας Ρώσος κατάσκοπος απέκτησε κατοικία στο Τόκιο , παντρεύτηκε μία Γιαπωνέζα και δημιούργησε ένα δίκτυο πληροφοριοδοτών που εργαζόταν για τη KGB, μέσα στους κόλπους του Υπουργείου Άμυνας της Ιαπωνίας. Ο Ρώσος κατάσκοπος, του οποίου τα χαρακτηριστικά θύμιζαν Ιαπωνία, εργάστηκε με το τρόπο αυτό για 30 χρόνια προτού μια φιλονικία με τη σύζυγο του κάνει τη

τελευταία να αποκαλύψει τις δραστηριότητες του. Μετά τη φυγή του στη Κίνα, η υπηρεσία αντικατασκοπείας της Ιαπωνίας βρήκε ένα διαβιβαστή μικροκυμάτων και υλικό κωδικοποιήσεων στο διαμέρισμα του στο Τόκιο.

2.5.2 ΠΛΑΣΤΟΓΡΑΦΗΜΕΝΑ ΕΓΓΡΑΦΑ ΚΑΙ ΜΗΝΥΜΑΤΑ

Η πλαστογραφία είναι μια πράξη, η οποία στοχεύει σε ένα σύνολο εγγράφων, που προέρχονται από ένα συγκεκριμένο πρόσωπο ή οντότητα. Η διαθεσιμότητα του συνόλου αυτού αυξάνεται για τον πλαστογράφο με την έννοια ότι αυτός μπορεί να προσθέσει ότι θέλει σε αυτά, πράγμα που αποκλείεται από την πηγή της προέλευσης τους. Η εισαγωγή των απατηλών εγγράφων στο σύνολο έχει επίσης σαν αποτέλεσμα τη μείωση της ακεραιότητας του. Η αξία τους εξάλλου αυξάνεται για τον πλαστογράφο, μειώνεται όμως για εκείνον που το έχει υπογράψει καθώς και για τα άλλα πρόσωπα που μπορεί να ξεγελαστούν πιστεύοντας ότι κάποια πράγματα είναι αληθινά ενώ αυτά είναι ψευδή. Ο πλαστογράφος μπορεί να ωφεληθεί οικονομικά ή να έχει την ικανοποίηση πως κατέστρεψε τη φήμη και το καλό όνομα του θύματος του. Οι κλέφτες ταυτότητας χρησιμοποιούν την πλαστογραφία όταν υπογράφουν επιταγές, χρεωστικά έγγραφα και άλλα έγγραφα με το όνομα των θυμάτων τους. Η Πλαστογραφία αποτελεί πράγματι ένα στοιχείο της κλοπής ταυτότητας. Η πλαστογραφία αποτελεί επίσης ένα είδος διαμόρφωσης απόψεων, της οποίας το αντικείμενο είναι η εξαπάτηση κάποιων, για να πιστέψουν ότι τα ψευδή έγγραφα είναι αληθινά.

Με τους υπολογιστές είναι πολύ απλή η πλαστογράφηση. Φτιάχνει κανείς ένα έγγραφο και βάζει το όνομα κάποιου σε αυτό. Οι προσφορές με το ηλεκτρονικό ταχυδρομείο αποτελούν ένα ιδιαίτερα ελκυστικό εργαλείο για τους δράστες, καθώς μπορούν όχι μόνο να βάλουν το όνομα του θύματος τους σε ένα μήνυμα αλλά και να το κάνουν να φαίνεται πως προέρχεται από το λογαριασμό ηλεκτρονικού ταχυδρομείου του τελευταίου.

2.5.3 ΠΛΑΣΤΟΓΡΑΦΗΣΕΙΣ ΚΑΙ ΣΚΟΥΠΙΔΟΤΑΧΥΔΡΟΜΕΙΟ (SPAM)

Τα spam e-mail είναι ανεπιθύμητη αλληλογραφία που διανέμεται σε τεράστιο αριθμό παραληπτών. Συνήθη παραδείγματα είναι τα spam με περιεχόμενο που σχετίζεται με πορνογραφία, φαρμακευτικά προϊόντα, ή αμφίβολης αξιοπιστίας οικονομικές συναλλαγές. Στις περισσότερες περιπτώσεις τα spam αποστέλλονται με σκοπό την εξαπάτηση των παραληπτών.

Υπάρχουν βέβαια και περιπτώσεις όπου αξιόπιστες εταιρίες ή απλοί χρήστες στέλνουν μαζικά e-mails σε λίστες αποδεκτών τους, καθώς η μαζική αποστολή ηλεκτρονικού ταχυδρομείου αποτελεί έναν πολύ φθηνό και ταυτόχρονα μαζικό τρόπο διαφήμισης των προϊόντων και υπηρεσιών τους. Οι νόμοι έχουν ποικίλους ορισμούς σχετικά με το χαρακτηρισμό ενός e-mail ως spam.

Οι εταιρίες που αποστέλλουν μηνύματα spam χρησιμοποιούν ειδικό λογισμικό που ερευνά τις ιστοσελίδες και συλλέγει λογαριασμούς ηλεκτρονικού ταχυδρομείου που έχουν καταχωρηθεί σε αυτές. Για να καταφέρουν να παραπλανήσουν τον παραλήπτη και να τον κάνουν να ανοίξει το e-mail χρησιμοποιούν ψεύτικα στοιχεία αποστολέα και στο πεδίο «θέμα» τοποθετούν μια φράση που προσελκύει την προσοχή ή δημιουργεί την εντύπωση ότι το μήνυμα προέρχεται από φιλικό πρόσωπο. Για παράδειγμα: «Κερδίσατε στην κλήρωση!» «Χρόνια Πολλά» ή «Έχουμε καιρό να τα πούμε».

ΠΩΣ ΝΑ ΑΝΑΓΝΩΡΙΖΕΤΑΙ ΤΑ ΜΗΝΥΜΑΤΑ SPAM:

- Δεν γνωρίζετε τον αποστολέα.
- Οι εικόνες και τα κείμενα είναι σύνδεσμοι προς ιστοσελίδες.
  Επίσης τα κουμπιά «κλείσιμο», «ναι» και «όχι», δεν έχουν τη συνήθη λειτουργία τους, αλλά αντίθετα παραπέμπουν και αυτά σε ιστοσελίδες.
- Υπάρχει συχνά η ένδειξη «FW» (Forward, δηλαδή προώθηση) χωρίς αυτό βέβαια να σημαίνει απαραίτητα ότι πρόκειται για spam.
- Όταν το μήνυμα είναι σε ελληνική γλώσσα, συχνά έχει πολύ εμφανή

συντακτικά και γραμματικά λάθη.

2.5.4 ΚΑΤΑΚΛΥΣΜΟΣ ΑΠΟ ΜΗΝΥΜΑΤΑ ΗΛΕΚΤΡΟΝΙΚΟΥ ΤΑΧΥΔΡΟΜΕΙΟΥ

Ορισμένοι από εκείνους που επιτίθενται στέλνουν στα θύματα τους όχι μόνο ένα ψεύτικο μήνυμα ή δύο ή τρία. Κατακλύζουν τις ηλεκτρονικές γραμματοθυρίδες τους με χιλιάδες μηνύματα, τα οποία μερικές φορές περιλαμβάνουν και τεράστια συννημένα αρχεία (attachments). Όλα αυτά που ονομάζονται βόμβες ηλεκτρονικού ταχυδρομείου μπορούν να κάνουν μεγάλη ζημιά στην γραμματοθυρίδα ενός λήπτη και να τη καταστήσουν ανίκανη να λαμβάνει το κανονικό ταχυδρομείο. Με το τρόπο αυτό , μπορεί να οδηγήσουν στην άρνηση της παροχής υπηρεσιών καθώς και στην απώλεια της αξιοπιστίας ενός συστήματος. Το κίνητρο για την τέλεση της πράξης αυτής μπορεί να είναι η εκδίκηση ή απλώς η παρενόχληση του θύματος.

Οι δράστες στην προκειμένη περίπτωση προγραμματίζουν τους υπολογιστές τους έτσι ώστε να στέλνουν με συνεχή ροή μηνύματα στους λογαριασμούς του ηλεκτρονικού ταχυδρομείου των θυμάτων τους. Τα μηνύματα αυτά μπορεί να προωθούνται στο προορισμό τους μέσω πολλών συστημάτων με ψεύτικες απαντητικές διευθύνσεις, καθιστώντας, έτσι πιο δύσκολη την εγκατάσταση από το λήπτη τους ενός προγράμματος αντιμετώπισης τους, το οποίο θα φιλτράρει όσα από αυτά θεωρούνται ανεπιθύμητα. Η άμυνα κατά των επιθέσεων αυτών δεν διαφέρει από εκείνη που απαιτείται για την αντιμετώπιση των μηνυμάτων του σκουπιδοταχυδρομείου, εκτός από το γεγονός ότι ο όγκος των μηνυμάτων, που λαμβάνει ένας και μοναδικός λήπτης, είναι στην περίπτωση αυτή σημαντικά μεγαλύτερος.

2.5.5 ΠΛΑΣΤΟΓΡΑΦΙΑ ΤΗΣ ΔΙΕΥΘΥΝΣΗΣ ΤΗΣ ΠΗΓΗΣ ΠΡΟΕΛΕΥΣΗΣ

Κάθε πακέτο που κινείται μέσα στο ιντερνέτ έχει μια πηγή προέλευσης (από)

και έναν προορισμό (προς). Κάθε ένα από αυτά περιέχει τη διεύθυνση Πρωτοκόλλου του ιντερνέτ (IP) ενός υπολογιστή του Διαδικτύου. Μία συνηθισμένη επίθεση που ονομάζεται “IP Spoofing”, είναι εκείνη στην οποία πλαστογραφείται η διεύθυνση της πηγής προέλευσης έτσι ώστε τα μηνύματα να φαίνονται ότι προέρχονται από διαφορετική από τη διεύθυνση της πραγματικής πηγής προέλευσης. Κανονικά, η ψεύτικη διεύθυνση είναι εκείνη ενός υπολογιστή τον οποίο εμπιστεύεται ο υπολογιστής που λαμβάνει το μήνυμα ,έτσι ώστε το πακέτο να γίνεται αποδεκτό και να ενεργοποιείται, και σε ορισμένες περιπτώσεις μάλιστα να δίνει τη δυνατότητα στον εισβολέα να ξεπερνάει και το εμπόδιο ενός τοίχου φωτιάς (firewall=πρόγραμμα ασφαλείας). Το σετ των υπολογιστών που εμπιστεύεται ο υπολογιστής που λαμβάνει το μήνυμα, προσδιορίζεται σε ένα αρχείο ή σε μία βάση δεδομένων (π.χ. “/etc/hosts.equiv” ή “.rhosts” στο λειτουργικό σύστημα Unix) και τυπικά περιλαμβάνει τις διευθύνσεις που έχουν τα συγκεκριμένα μηχανήματα στο ίδιο εσωτερικό δίκτυο. Γνωρίζοντας την IP διεύθυνση του στόχου, ο εισβολέας μπορεί να μαντέψει τις IP διευθύνσεις των υπολοίπων υπολογιστών του ίδιου τοπικού δικτύου δεδομένου ότι όλοι έχουν τους ίδιους περίπου αριθμούς (π.χ. “20.30.40.1” και “20.30.40.2”).

Σε μία μορφή της επίθεσης που περιγράψαμε παραπάνω ο δράστης παρεμβάλλεται στην ανοιχτή σύνδεση μεταξύ ενός κύριου υπολογιστή και του στόχου του, στέλνοντας στο πρώτο μεγάλο αριθμό πακέτων, για να τον αχρηστεύσει και στη συνέχεια να υπεισέρχεται στη θέση του στέλνοντας παραποιημένα πακέτα στο σύστημα που αποτελεί το στόχο του. Όταν αυτό το τελευταίο στέλνει απάντηση στον κύριο υπολογιστή, ο δράστης εμποδίζει τη διέλευση των συγκεκριμένων πακέτων. Ο κύριος υπολογιστής, μη λειτουργώντας ακόμη κανονικά, δε μαθαίνει ποτέ αυτό που πραγματικά συμβαίνει.

2.5.6 ΠΑΡΑΧΑΡΑΞΗ

Η παραχάραξη αποτελεί ένα είδος απάτης στην οποία η παραποιημένη ταυτότητα ανήκει σε έναν οργανισμό ή σε μία κυβερνητική υπηρεσία η οποία εκδίδει κάποιο είδος εγγράφων. Στη σύγχρονη τεχνολογία, στην οποία περιλαμβάνονται οι υπολογιστές, οι ηλεκτρονικές εκδόσεις, οι έγχρωμοι εκτυπωτές και τα υψηλής ποιότητας έγχρωμα φωτοαντιγραφικά μηχανήματα, είναι πολύ συχνή η παραγωγή ψεύτικων εγγράφων και εικόνων υψηλής ποιότητας. Λογότυπα και σχέδια μπορούν να αντιγραφούν από έγκυρα έγγραφα ιστοσελίδων και να προστεθούν σε πλαστά, για να τα κάνουν να φαίνονται περισσότερο αξιόπιστα.

Από πρακτική άποψη κάθε μορφή έντυπου υλικού θέτει υποψηφιότητα για να παραχαραχτεί, και σε αυτό το υλικό συμπεριλαμβάνονται επιστολές, εισιτήρια, ταυτότητες, νομίσματα.

2.5.7 ΔΟΥΡΕΙΟΙ ΙΠΠΟΙ

Σύμφωνα με το μύθο, οι Έλληνες στρατιώτες μπήκαν στη Τροία κρυμμένοι μέσα σε ένα ξύλινο άλογο, που είχαν κάνει δώρο στους Τρώες. Βρισκόμενοι μέσα από τα τείχη, άνοιξαν τις πύλες για να μπει όλος ο στρατός τους και έτσι κατέλαβαν τη Τροία. Σήμερα ο όρος “Δούρειος Ίππος” χρησιμοποιείται για να υποδηλώσει κάθε αντικείμενο, που έχει τοποθετηθεί στην περιοχή του αντιπάλου με τέτοιο τρόπο ώστε να μην είναι φανερή η ανατρεπτική φύση του. Ένα τέτοιο παράδειγμα αποτελεί το μηχάνημα ATM Δούρειος Ίππος, το οποίο ο Alan Scott Pace, 30 ετών τοποθέτησε σε ένα πολυκατάστημα στο Connecticut της Αμερικής. Το μηχάνημα αυτό χρησιμοποιήθηκε για τη συλλογή αριθμών λογαριασμών και PIN ανυποψίαστων πελατών των οποίων οι συναλλαγές στη συνέχεια απορρίπτονταν. Οι απατεώνες βέβαια χρησιμοποιούσαν τις πληροφορίες που έπαιρναν με το τρόπο αυτό , για να φτιάχνουν πλαστές κάρτες ATM, με τις οποίες είχαν αποσύρει περισσότερα από $100.000 σε μετρητά.

Ένας Δούρειος Ίππος είναι ένα εργαλείο το οποίο χρησιμοποιείται για την απόκτηση πρόσβασης σε μια πληροφοριακή πηγή.

Ένα πρόγραμμα Δούρειου ίππου είναι εκείνο το οποίο όταν ενεργοποιηθεί, αναπτύσσει μια ανεπιθύμητη δραστηριότητα η οποία δεν είχε προβλεφθεί από το πρόσωπο που το ενεργοποίησε. Το πρόγραμμα αυτό μπορεί να διαγράψει αρχεία, να ξεφορμάρει το σκληρό δίσκο ή να γνωστοποιήσει ευαίσθητα δεδομένα στο δημιουργό τους, εάν η εκτέλεση του σχετικού κώδικα προκληθεί από κάποιο γεγονός . Ο Δούρειος ίππος ονομάζεται επίσης "λογική βόμβα" ή σε περίπτωση ενεργοποίησης του με ρολόι, "ωρολογιακή βόμβα". Ο επιβλαβής κώδικας είναι συνήθως κρυμμένος σ'ένα πρόγραμμα του συστήματος ή μιας εφαρμογής που φαίνεται αθώα αν όχι υπερβολικά ελκυστική. Στα προγράμματα αυτά μπορεί να περιλαμβάνεται ένας επεξεργαστής κειμένου, ένα λογιστικό φύλλο, ένα παιχνίδι, μια οικονομική εφαρμογή ή ένα βοηθητικό πρόγραμμα. Ο Δούρειος ίππος μπορεί να διανεμηθεί με ηλεκτρονικό ταχυδρομείο ή μέσω του Ιστού. Ανυποψίαστοι χρήστες μπορεί να εισαγάγουν στο σύστημα τους ανοίγοντας τα προσαρτημένα σε ένα μήνυμα ηλεκτρονικού ταχυδρομείου ή κατεβάζοντας προγράμματα από τον Ιστό.

Χάκερς έχουν πάρει κωδικούς αντικαθιστώντας το κανονικό πρόγραμμα εισόδου σ'έναν υπολογιστή με μία έκδοση του που περιέχει Δούρειο ίππο και η οποία φαίνεται κανονική, ενώ στην πραγματικότητα δεν κάνει τίποτα άλλο από το να κλέβει κωδικούς ανυποψίαστων χρηστών. Αφού οι χρήστες γράψουν το όνομα τους και τον κωδικό τους, το πρόγραμμα αυτό στέλνει τα στοιχεία αυτά σε ένα αρχείο, δίνει ένα μήνυμα μη αποδοχής τους και στη συνέχεια παραδίδει τον έλεγχο στο κανονικό πρόγραμμα εισόδου, το οποίο πλέον εκτελείται ως συνήθως. Επειδή οι κωδικοί δεν φαίνονται κατά τη διαδικασία της εισόδου, οι χρήστες οδηγούνται στο να πιστέψουν ότι έχουν κάνει κάποιο λάθος και έτσι, τους ξαναγράφουν απαντώντας στη δεύτερη ζήτηση τους. Στη συνέχεια μπορείτε να δείτε τι θα εμφανιστεί στη οθόνη του υπολογιστή σε περίπτωση που το πρόγραμμα εισόδου σε ένα σύστημα έχει κάποιο Δούρειο Ίππο:

login:denning

Password:

login incorect

login:denning

Password:

Last Login:thu Aug 7 08:43:12 from guvax

Λίγη ώρα αργότερα ο χάκερ μπορεί να πάρει το αρχείο του και να έχει στη διάθεση του τους κωδικούς. Με ένα τέτοιο πρόγραμμα, κάποιος από τους εργαζόμενους σε ένα σύστημα ή ένας εισβολέας, που έχει τη δυνατότητα πρόσβασης σ'ένα μόνο λογαριασμό με περιορισμένα προνόμια, μπορεί να ασκήσει το κύριο κωδικό εισόδου στο σύστημα αυτό.

2.5.8 ΔΙΑΡΚΕΙΣ ΔΙΕΥΘΥΝΣΕΙΣ ΗΛΕΚΤΡΟΝΙΚΟΥ ΤΑΧΥΔΡΟΜΕΙΟΥ

Μία διαρκής διεύθυνση ηλεκτρονικού ταχυδρομείου είναι μία υπηρεσία του internet, που προσφέρει ένα μόνιμο λογαριασμό ηλεκτρονικού ταχυδρομείου σε χρήστες των οποίων η εργασία ή τα αντικείμενα ενασχόλησης αλλάζουν συχνά. Οι συνδρομητές μπορούν στην περίπτωση αυτή να γράφουν τις διευθύνσεις τους αυτές στις επαγγελματικές τούς κάρτες, και να ρυθμίζουν τους λογαριασμούς τους αυτούς έτσι ώστε να στέλνουν όλα τα μηνύματα του ηλεκτρονικού τους ταχυδρομείου στους κανονικούς τους λογαριασμούς , απ'όπου μπορούν να τα διαβάσουν και να τα επεξεργαστούν. Τα πλεονεκτήματα που έχουν οι συγκεκριμένοι χρήστες είναι ότι διαθέτουν μία μόνιμη διεύθυνση ηλεκτρονικού ταχυδρομείου, ακόμη κι αν αλλάζουν εργασία ή παροχείς ιντερνέτ, μειονέκτημα είναι ότι ο παροχέας της διεύθυνσης αυτής έχει τη δυνατότητα να διαβάζει κρυφά όλα τα μηνύματα, που περνούν μέσα από το σύστημα του.

Παρότι στη προκειμένη περίπτωση δεν έχουν αναφερθεί περιστατικά εμφάνισης Δούρειων Ίππων, τον Οκτώβριο του 1997 η Air Force Computer Emergency

Response Team ανέφερε σε ένα έγγραφο της πώς μία εταιρία στην Ολλανδία είχε σαν στόχο της στρατιωτικούς, που χρησιμοποιούσαν τις υπηρεσίες του μόνιμου ηλεκτρονικού ταχυδρομείου. Το στρατιωτικό ηλεκτρονικό ταχυδρομείο προσέφερε στους χρήστες του διευθύνσεις με στρατιωτικά ονόματα περιοχών, όπως “Air Force.net” ή “F16.AirForce.net”. Μηνύματα ηλεκτρονικού ταχυδρομείου, που στάλθηκαν σε στρατιωτικές διευθύνσεις , θα μπορούσαν αυτόματα να επαναπροωθήθούν στους κανονικούς λογαριασμούς των χρηστών, οτιδήποτε κι αν συνέβαινε τη περίοδο αυτή. Ένα τέτοιο σύστημα μόνιμου ηλεκτρονικού ταχυδρομείου θα μπορούσε να έχει στη διάθεση του σημαντικές πληροφορίες για το στρατιωτικό προσωπικό και τη δουλειά του.

2.5.9 ΔΟΥΡΕΙΟΙ ΙΠΠΟΙ ΣΕ ΜΙΚΡΟΤΣΙΠ

Στο βιβλίο του Information Warface, ο Winn Schwartau αναφέρεται στη πιθανότητα κατασκευής μικροτσίπ με Δούρειους Ίππους, μια διαδικασία που την αποκαλεί “chiipping”. Τα τσιπς αυτά δε θα διαφέρουν από τα κανονικά αλλά θα έχουν κατασκευαστεί έτσι ώστε να περιέχουν οδηγίες, που θα προξενούν ζημιές. Οι οδηγίες αυτές θα μπορούν να προκαλέσουν την πρόωρη απενεργοποίηση του τσιπ ή θα μπορούν να βοηθήσουν μυστικές ηλεκτρονικές παρακολουθήσεις, για παράδειγμα. Ο Schwartau υποστηρίζει πως η βιομηχανία των οπλικών συστημάτων θα μπορούσε να αποτελέσει μία ιδανική αγορά για chipping, που θα χρηματοδοτούσε η κυβέρνηση. Δεν έχουν υπάρξει μέχρι σήμερα ουσιαστικές αναφορές για τη χρήση του chipping σε οποιονδήποτε τομέα.

2.6 ΚΥΒΕΡΝΟΜΙΚΡΟΒΙΑ

Τα κυβερνομικρόβια είναι προγράμματα υπολογιστών, τα οποία μιμούνται μορφές ζωής. Αναπαράγονται (κάνουν αντίγραφα του εαυτού τους) και κινούνται στο χώρο, έτσι όπως κάνουν οι συνάδελφοι τους στο βιολογικό κόσμο. Όπως και ένα κανονικό μικρόβιο, είναι πολύ κολλητικά και μπορούν να προκαλέσουν σημαντικές βλάβες. Κάποια από αυτά συμπεριφέρονται σαν ωρολογιακές βόμβες, αποκρύπτοντας το πραγματικό του χαρακτήρα, έως ότου τους δοθεί η ευκαιρία να εκδηλωθούν. Εφόσον έχουν εισβάλλει σε ένα σύστημα, μπορούν να καταστρέψουν ή να διαγράψουν τα δεδομένα του, να υποβαθμίσουν τις υπηρεσίες του ή να στείλουν τα δεδομένα του στους δικούς του δημιουργούς.

Δύο είδη κυβερνομικροβίων υπάρχουν: οι ιοί και τα σκουλήκια. Και τα δύο αυτά είδη μολύνουν τους υπολογιστές, και τα δύο μπορούν να απλωθούν. Η κύρια διαφορά τους συνιστάται στο ότι ένα σκουλήκι είναι ένας αυτόνομος πράκτορας, ο οποίος εξαπλώνεται από μόνος του ενώ ένας ιός κολλάει σε άλλα προγράμματα και εξαπλώνεται μαζί με αυτά, συνήθως σε μία απάντηση σε πράξεις πού έναν χρήστες. Επίσης ενώ ένα σκουλήκι εξαπλώνεται μόνο σε δίκτυα υπολογιστών, ένας ιός μπορεί να εξαπλωθεί και με Η διάκριση ανάμεσα σε ιούς και σε σκουλήκια, ωστόσο μπερδεύει τα πράγματα και είναι ίσως ατυχής, καθώς η συμπεριφορά ορισμένων μικροβίων μοιάζει και με τα δύο αυτά είδη καθώς και τα δύο είδη μολύνουν υπολογιστές.

Σαν ένα εργαλείο πληροφοριακού πολέμου, τα κυβερνομικρόβια καταστρέφουν την ακεραιότητα δικτύων υπολογιστών, οδηγούν επίσης σε άρνηση παροχής υπηρεσιών. Ακόμη όμως κι αν δεν καταστρέφουν σκοπίμως δεδομένα ή δεν ενεργοποιούν συστήματα, οι μολυσμένοι από αυτά υπολογιστές θα πρέπει να τεθούν εκτός λειτουργίας και επομένως να μη γίνονται αυτά που πρέπει να κάνουν όσο χρόνο θα γίνεται προσπάθεια για την απομάκρυνση τους από το σύστημα.

2.6.1 ΙΟΙ ΤΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

Ένας ιός είναι ένα τμήμα κώδικα, το οποίο κολλάει τον εαυτό του σε άλλες εντολές του υπολογιστή στις οποίες περιλαμβάνονται ο κώδικας εφαρμογών προγράμματος, ο κώδικας που χρησιμοποιείται για την εκκίνηση ενός υπολογιστή, καθώς και οι μακροεντολές, που έχουν τοποθετηθεί σε έγγραφα. Σε οποιαδήποτε περίπτωση ο χρήστης (ή το σύστημα) δίνει μία εντολή στον υπολογιστή (για παράδειγμα να ξεκινήσει τη λειτουργία του ή μία εφαρμογή η να ένα προσαρτημένο σ'ένα μήνυμα ηλεκτρονικού ταχυδρομείου), ο ιός ενεργοποιείται παράλληλα και αυτός. Ο κώδικας του ιού προστίθεται στο κώδικα του υπολογιστή με τέτοιο τρόπο έτσι ώστε όταν αυτός φορτώνεται στη μνήμη για να εκτελεστεί , ο ιός είναι εκείνος που ενεργοποιείται πρώτος. Ο ιός ενεργοποιείται αρχικά από μόνος του και στη συνέχει αποκτά τον έλεγχο του υπολογιστή, που τον φιλοξενεί. Ενώ ενεργοποιείται, ο ιός μπορεί να τοποθετήσει ένα αντίγραφο του εαυτού του στη μνήμη του υπολογιστή, όπου αυτό παραμένει “εγκατεστημένο” , μέχρις ότου να κλείσει ο υπολογιστής. Το εγκατεστημένο αυτό αντίγραφο ψάχνει για μη μολυσμένους υπολογιστές. Όταν βρει κάποιον του μεταβιβάζει ένα αντίγραφο του εαυτού του. Στη συνέχεια ο ιός εκτελεί ένα “ωφέλιμο φορτίο”, το οποίο μπορεί να κάνει οτιδήποτε από το να δείξει ένα ψυχαγωγικό ή ένα πολιτικό μήνυμα μέχρι να σβήσει αρχεία από το σκληρό δίσκο. Ο Ιός του Smiley, για παράδειγμα δείχνει χαμογελαστά πρόσωπα τα οποία χοροπηδάνε στην οθόνη. Ο ιός που είναι γνωστός με το όνομα Michelangelo είναι ιδιαίτερα βλαβερός. Ξαναγράφει τους πρώτους κυλίνδρους του σκληρού δίσκου, εφόσον ενεργοποιηθεί την ημέρα της γέννησης του μεγάλου καλλιτέχνη του οποίου φέρει το όνομα, δηλαδή 6 Μαρτίου. Ο ιός Win95/CIH είναι ακόμη πιο καταστροφικός. Εκτός του ότι διαγράφει τα πρώτα αναμπαιχτείς δεδομένων του σκληρού δίσκου, ξαναγράφει μέρος του BIOS (βασικό σύστημα εισόδου-εξόδου) σε ορισμένα τσιπς αναλαμπής της μνήμης ROM. Το BIOS χρειάζεται για την εκκίνηση του υπολογιστή έτσι ώστε η επανεκκίνηση του υπολογιστή με μία εφεδρική δισκέτα να μην απαιτείται. Μια

εταιρία ανέφερε ότι βρήκε τον ιό αυτό στο 80%, ή σε περίπου 500 από τους υπολογιστές της. Ένας “κρυπτούς” φέρει φορτίο, το οποίο κρυπτογραφεί αρχεία με ένα μυστικό κλειδί, εμποδίζοντας με το τρόπο αυτό την πρόσβαση του ιδιοκτήτη τους σ' αυτά. Ένας τέτοιος ιός μπορεί να χρησιμοποιηθεί για εκβιασμό. Περίπου μόνο το 5% των ιών περιέχουν κάποιο φορτίο, οι περισσότεροι από αυτούς δεν κάνουν τίποτα άλλο από το να πολλαπλασιάζονται. Εάν ένας ιός δεν εγκαταστήσει τον εαυτό του, τότε θα πρέπει να μολύνει έναν άλλο υπολογιστή και να του αφήσει το φορτίο του, προτού να αποκτήσει τον έλεγχο του. Οι ιοί διαδίδονται από το ένα μηχάνημα στο άλλο μέσω δισκετών και δικτύων υπολογιστών.

Η ιδέα του αυτό-αναπαραγώμενου κώδικα υπήρχε από το 1970, όταν ο Gregory Benford χρησιμοποίησε τον όρο “ιός” προκειμένου να αναφερθεί σε ανεπιθύμητο κώδικα υπολογιστή που θα μπορούσε να αναπαράγει τον εαυτό του κυκλοφορώντας σε υπολογιστές και να εισβάλει με το τρόπο αυτό στο ARPANET (τον πρόδρομο του ιντερνέτ).Από τις αρχές του 1980 οι ιοί, όπως τους γνωρίζουμε σήμερα άρχισαν να εμφανίζονται και η έννοια τους αποδόθηκε από τον Fred Cohen, τότε μεταπτυχιακό φοιτητή του πανεπιστημίου της Νότιας Καλιφόρνιας.

Ο Cohen όρισε τον ιό των υπολογιστών σαν “ένα πρόγραμμα που μπορεί να “μολύνει” άλλα προγράμματα τροποποιώντας τα έτσι ώστε να μπορούν να δεχτούν ένα αντίγραφο του. Με τη μόλυνση που διαθέτει, ένας ιός μπορεί να απλωθεί σ'ένα ολόκληρο σύστημα υπολογιστών ή σ'ένα δίκτυο χρησιμοποιώντας την ακούσια σύμφωνη γνώμη κάθε χρήστη, που τον χρησιμοποιεί, για να μολύνει τα προγράμματα του. Κάθε πρόγραμμα που έχει μολυνθεί μπορεί επίσης να λειτουργήσει σαν ιός και με τον τρόπο αυτό η μόλυνση απλώνεται.”

Μέχρι τις αρχές του 1998, είχαν βρεθεί περισσότεροι από 13000 ιοί υπολογιστών, παρότι οι περισσότεροι προέρχονται ο ένας από τον άλλο. Ο τεράστιος αυτός αριθμός εξηγείται εν μέρει από την ευκολία, με την οποία οι

πιθανοί δημιουργοί τους μπορούν να βρουν τα εργαλεία κατασκευής τους, καθώς και το πραγματικό ιικό κώδικα για να εργαστούν , είτε μέσω του ίντερνετ ,είτε από άλλα κανάλια. Το Μάιο του 1997 μια ομάδα χάκερς ανήγγειλε τη διάθεση στο κοινό ενός CD-ROM, που περιείχε 10.000 ιούς.

Οι ίδιοι προσέφεραν δωρεάν στους 100 πρώτους πελάτες τους μία συλλογή από 50 εργαλεία κατασκευής ιών.

Ένας χρήστης μπορεί να "αρπάξει" έναν ιό από διάφορες πηγές, στις οποίες περιλαμβάνονται οι δισκέτες, τα CD-ROMs, τα προσαρτώμενα σε μηνύματα ηλεκτρονικού ταχυδρομείου καθώς και ιστοσελίδες με ενσωματωμένο κώδικα, ο οποίος φορτώνεται και τρέχει στο μηχάνημα του χρήστη. Κανονικά, ο χρήστης θα πρέπει να ανοίξει το προσαρτώμενο σε ένα μήνυμα ηλεκτρονικό ταχυδρομείου μπορούν να ανοίγουν τα προσαρτώμενα αυτομάτως.

Υπάρχουν τρία βασικά είδη ιών, του προγράμματος, του συστήματος, του συστήματος εκκίνησης, και των μακροεντολών, πού έχουν πάρει το όνομα τους ανάλογα με τα μέρη του υπολογιστή που μολύνουν. Οι πολυμερείς ιοί συνδυάζουν τα πρώτα δύο από τα είδη αυτά, μολύνοντας και τα αρχεία του προγράμματος και τούς τομείς εκκίνησης του σκληρού δίσκου.

2.6.2 ΙΟΙ ΤΟΥ ΠΡΟΓΡΑΜΜΑΤΟΣ

Ένας ιός προγράμματος μολύνει αρχεία, τα οποία περιέχουν κώδικα υπολογιστή, και προτιμά ειδικότερα τα αρχεία ".EXE" και ".COM" ,χωρίς όμως να εξαιρεί και άλλα αρχεία, όπως τα ".SYS" και ".DLL". Οποτεδήποτε ο χρήστης ξεκινάει μια εφαρμογή αυτή θα τρέξει το μολυσμένο αρχείο και ο ιός θα απελευθερωθεί. Για παράδειγμα, εάν το αρχείο "netscape.exe"μολυνθεί, ο ιός θα ενεργοποιείται κάθε φορά, που ο χρήστης θα ξεκινάει το Netscape.

Οι ιοί προγράμματος μπορούν να διαδίδονται μέσω οποιουδήποτε μέσου χρησιμοποιείται για τη μεταφορά λογισμικού, στα οποία περιλαμβάνονται οι δισκέτες, τα CD-ROM, τα προσαρτώμενα σε μηνύματα ηλεκτρονικού ταχυδρομείου και τα δίκτυα. Το 85% περίπου των 10.000 γνωστών ιών ανήκει

στους ιούς προγράμματος οι ιοί αυτοί, είναι και οι λιγότερο διαδεδομένοι.

2.6.3 ΙΟΙ ΤΟΥ ΣΥΣΤΗΜΑΤΟΣ ΕΚΚΙΝΗΣΗΣ

Ένας ιός του συστήματος εκκίνησης μολύνει τον τομέα εκκίνησης και τις περιοχές , που συνδέονται με αυτόν του σκληρού δίσκου ή της δισκέτας. Κάθε δίσκος διαθέτει έναν τομέα εκκίνησης και γι'αυτό δυνητικά μπορεί να μολυνθεί. Από τη στιγμή που ο σκληρός δίσκος ενός μηχανήματος έχει μολυνθεί, ο ιός θα ενεργοποιείται κάθε φορά που το μηχάνημα αυτό θα ανοίγει. Θα εγκατασταθεί δε στη μνήμη και θα μεταβιβάσει τον έλεγχο στον κανονικό κώδικα εκκίνησης. Ο ιός στη συνέχεια θα μολύνει κάθε δισκέτα που θα μπαίνει στο μηχάνημα.

Μετά από τη μόλυνση μίας δισκέτας, ο ιός μπορεί να μεταβιβαστεί σ'έναν άλλο προσωπικό υπολογιστή σε περίπτωση που η μολυσμένη δισκέτα τοποθετηθεί στον οδηγό “Α” :του υπολογιστή αυτού, μόλις αυτός ανοίξει (η δισκέτα μπορεί να έχει μείνει εκεί από προηγούμενη λειτουργία του υπολογιστή).Αυτό θα συμβεί, επειδή ο υπολογιστής θα προσπαθήσει να βρει το κώδικα εκκίνησης από τη δισκέτα και όχι από το σκληρό δίσκο, εφόσον η δισκέτα βρίσκεται στον οδηγό. Τη στιγμή που ο υπολογιστής θα αντιληφθεί πως η δισκέτα δεν έχει τον κώδικα που χρειάζεται για να ολοκλήρωση την εκκίνηση, είναι ήδη πάρα πολύ αργά. Ο ιός θα έχει τοποθετήσει τον εαυτό του στη μνήμη και θα έχει μολύνει το σκληρό δίσκο ωστόσο, μία μολυσμένη δισκέτα μπορεί να μπει σε έναν υπολογιστή μετά την ολοκλήρωση της διαδικασίας εκκίνησης του, ο ιός δε θα έχει σε καμία περίπτωση την ευκαιρία να ενεργοποιηθεί και να μολύνει το σκληρό δίσκο.

Ένας από τους πρώτους ιούς ευρείας κυκλοφορίας, που αναφέρθηκαν, ήταν ένας σχετικά αβλαβής ιός εκκίνησης που λεγόταν Brain (εγκέφαλος). Έχοντας χρονολογία γέννησης του το 1986, υπήρξε κάποτε ο πλέον διαδεδομένος ιός των προσωπικών υπολογιστών. Κατά τη δεκαετία του 1990, ο ιός Form ήταν ο περισσότερο συνηθισμένος ιός εκκίνησης, σύμφωνα με την ετήσια έρευνα των ιών της Εθνικής Ένωσης για την Ασφάλεια των Υπολογιστών (NSCA). Σε

περίπτωση ενεργοποίησης του στις 18 του μήνα, ο Form έκανε έναν ήχο σαν “κλικ” οποτεδήποτε ο χρήστης του υπολογιστή πατούσε ένα πλήκτρο. Το κείμενο που είναι γραμμένο στο κώδικα του ιού αυτού λέει : “Ο ιός FORM χαιρετίζει αυτόν που διαβάζει το κείμενο αυτό. Ο FORM δεν καταστρέφει δεδομένα! Μην πανικοβάλλεστε !”Στην πραγματικότητα ωστόσο, ο ιός ήταν ιδιαίτερα επιβλαβής για τους νεότερους προσωπικούς υπολογιστές, οι οποίοι είχαν ρυθμιστεί διαφορετικά από τους παλιούς. Η έρευνα που πραγματοποίησε η NCSA το 1997 διαπίστωσε πώς οι 9 στους 10 περισσότερο διαδεδομένους ιούς και οι 17 στους 20 κορυφαίους άνηκαν στην κατηγορία των ιών εκκίνησης. Παρά την υπεροχή τους αυτή, οι ιοί εκκίνησης υπολογίζεται πως αντιστοιχούν μόνο στο 5% του συνόλου των γνωστών ιών.

Ο ιός Michelangelo είναι ένας ιός εκκίνησης, η εξάπλωση του όμως μετά από μία περίοδο έντονης κυκλοφορίας του φαίνεται πώς έχει περιοριστεί. Την άνοιξη του 1992, αναφέρθηκε επανειλημμένα καθώς πωλητές και ειδικοί στην ασφάλεια των υπολογιστών ανέμεναν την εξάπλωση τους με τη μορφή ενδημοεπιδημίας. Η ημερομηνία της 6ης Μαρτίου πλησίαζε γρήγορα και οι χρήστες έβρισκαν αντίγραφα τού καταστροφικού κώδικα στους υπολογιστές τους. Ορισμένοι χαρακτήριζαν την αντίδραση των ΜΜΕ για το θέμα αυτό υπερβολική, η απειλή όμως ήταν πραγματική. Σύμφωνα με τον καθηγητή Robert Slade για τους ιούς των υπολογιστών σε ορισμένα μέρη της Ευρώπης ήταν 25% και περισσότερο .Τουλάχιστον 15 εταιρίες μετέφεραν εμπορικό λογισμικό από μολυσμένους δίσκους. Όταν ήρθε η 6η Μαρτίου, ένας μικρός αριθμός υπολογιστών στην Ιαπωνία αντιμετώπισαν το πρόβλημα, οι περισσότεροι όμως από αυτούς επέζησαν, αναμφίβολα επειδή πολλοί άνθρωποι πήραν τις απαραίτητες προφυλάξεις.

2.6.4 ΜΑΚΡΟ-ΙΟΙ

Ένας μακρό-ιός εμφανίζεται σαν μία αυτόματη μακροεντολή ενσωματωμένη σε αρχεία εγγράφων εφαρμογών με ικανότητα μακροεντολών, όπως είναι για

παράδειγμα, οι επεξεργαστές κειμένου και τα λογιστικά φύλλα. Οι μακροεντολές αυτές εκτελούνται αυτόματα σε απάντηση ενός γεγονότος, όπως για παράδειγμα, το άνοιγμα ή το κλείσιμο ενός αρχείου ή το ξεκίνημα μίας εφαρμογής. Εφόσον δε ενεργοποιηθούν, αντιγράφουν τον κώδικα τους σε άλλα αντίγραφα.

Για τους μακρό-ιούς έγινε γενικά λόγος πριν από την ανακάλυψη τον Ιούλιο του 1995 του Concept, ενός ιού, που προσβάλει τα αρχεία εγγράφων του Word της Microsoft, ο οποίος όμως δεν έχει άλλο ωφέλιμο φορτίο. Μέχρι το φθινόπωρο ο Concept ήταν ο ιός, που αναφερόταν πιο συχνά από όλους τους ιούς των υπολογιστών, ξεπερνώντας και των Form, ο οποίος είχε παλαιότερα την αναμφίβολη αυτή τιμή. Τούς δύο πρώτους μήνες του 1997, ο Concept είχε μολύνει σχεδόν τους μισούς (49%) από τους δικτυακούς τόπους που εξέτασε η NSCA. Είχε μάλιστα επεκτείνει τη δράση του στα δύο τρίτα περίπου του συνολικού αριθμού των μολύνσεων, που είχαν προξενηθεί από τους 10 κορυφαίους ιούς. Συγκρίνοντας των αριθμό των περιστατικών με ιούς των δύο πρώτων μηνών του 1997 , η NSCA έβγαλε το συμπέρασμα ότι ο αριθμός των μολύνσεων με μακρό-ιούς διπλασιαζόταν κάθε 116 μέρες.

Μετά την ανακάλυψη του Concept, βρέθηκαν πάρα πολλοί μακρό-ιοί του Word, ορισμένοι από τους οποίους ήταν ιδιαίτερα καταστροφικοί. Ένας από αυτούς πού ονομαζόταν FormatC, διέγραφε αρχεία από το σκληρό δίσκο. Ο Wazzu, ο οποίος τοποθετήθηκε δεύτερος στον κατάλογο της NCSA του 1997 των πιο συνηθισμένων ιών, σβήνει στην τύχη μέχρι τρεις λέξεις ενός εγγράφου σε τυχαίες σειρές ή παρεμβάλλει τη λέξη wazzu WM/PolyPoster που ανακαλύφθηκε τον Ιούλιο του 1998 από την εταιρία ασφάλειας υπολογιστών Data Fellows, προσπαθεί να στείλει τα αρχεία των χρηστών του Word σε δημόσιες ομάδες νέων, στις οποίες περιλαμβάνονται το “alt.hacker”, το “alt.2600” και το “alt.sex”.Ένα θύμα του ιού αυτού θα μπορούσε να βρει τις προσωπικές του επιστολές ή τα έγγραφα της εταιρίας του δημοσιευμένα στο ιντερνέτ έτσι ώστε, να μπορεί να τα διαβάσει ο καθένας.

Τον Οκτώβριο του 1997, η υπηρεσία Αεροναυτικής και Διαστήματος των Η.Π.Α (NASA) είδε των εαυτό της να τα βάζει με ένα μακρό-ιό, ο οποίος είχε ταξιδέψει από το Διαστημικό Κέντρο Johnson του Χιούστον σε υπολογιστές στη Μόσχα, οι οποίοι χρησιμοποιούνταν για τη καθημερινή επικοινωνία με το πλήρωμα του διαστημικού σταθμού Mir, που βρισκόταν στο διάστημα, ο ιός διέφυγε εξαιτίας του ελέγχου του από παρωχημένο αντιβιοτικό λογισμικό, είχε μολύνει τους υπολογιστές PC και Apple Macintosh, που χρησιμοποιούταν για την επικοινωνία με τον Mir. Δεν είχε διαβιβαστεί στο MCs είχε όμως, σύμφωνα με τη σχετική αναφορά μολύνει μηνύματα ηλεκτρονικού ταχυδρομείου, που είχαν διαβιβαστεί στον Αμερικάνο αστροναύτη David Wolf. Οι επίσημοι θα έπρεπε να έχουν αποφύγει τη χρήση προσαρτημένων στο ηλεκτρονικό ταχυδρομείο τη στιγμή που απάλειφαν των ιό από τα συστήματα τους. Η επίθεση του ιού αυτού έγινε ακριβώς ένα μήνα μετά τη, για τρεις φορές μέσα σε 15 μέρες, διακοπή της λειτουργίας των υπολογιστών Mir.

Οι μακρό-ιοί εισβάλλουν σε οργανισμούς μέσω των προσαρτημάτων του ηλεκτρονικού ταχυδρομείου, των δισκετών, των εγγράφων και της πλοήγησης στον κυβερνοχώρο. Φυσιολογικά ένας ιός δε θα μπορούσε να εξαπλωθεί μέσω του ηλεκτρονικού ταχυδρομείου εκτός κι αν ο αποστολέας, ηθελημένα ή όχι, προσαρτήσει ένα μολυσμένο αρχείο σε ένα μήνυμα. Ο μακρό-ιός του Word , ShareFun, αποτελεί εξαίρεση των παραπάνω Όταν ανοίγεται ένα μολυσμένο έγγραφο, ο ιός αυτός μολύνει αρχικά όλο το περιβάλλον, για να εξασφαλίσει τη μόλυνση όλων των νέων εγγράφων. Στη συνέχεια τρέχει ένα πρόγραμμα, το οποίο του δίνει μία στις τέσσερις πιθανότητες για να κάνει το επόμενο βήμα, το οποίο είναι ο έλεγχος του συστήματος, για να διαπιστώσει εάν το Ταχυδρομείο της Microsoft είναι εγκατεστημένο. Εάν είναι έτσι, επιλέγει τρεις διευθύνσεις στη τύχη από τον ταχυδρομικό κατάλογο του χρήστη και στέλνει σε καθεμία από αυτές ένα μήνυμα με προσαρτημένο ένα μολυσμένο μήνυμα γραμμένο με το Word. Στη γραμμή τού θέματος του μηνύματος διαβάζει κανείς “θα πρέπει να το διαβάσεις αυτό” , ενώ το κύριο τμήμα του μηνύματος είναι λευκό, όταν ο

λήπτης ανοίξει το προσαρτημένο έγγραφο θα μολυνθεί το μηχάνημα του.

Ο ιός ShareFun μοιάζει με ένα παλαιότερο πρόγραμμα, που ονομαζόταν “CHRISTMA EXEC.”Το πρόγραμμα αυτό το οποίο ήταν ένα υβρίδιο ιού/σκουληκιού/Δούρειο ίππου, εντοπίστηκε για πρώτη φορά το Δεκέμβριο του 1987 στους μεγάλους υπολογιστές της IBM στην Ευρώπη, που ήταν συνδεδεμένοι με το σύστημα ηλεκτρονικού ταχυδρομείου EARN. Αυτό διαδιδόταν μέσω του ηλεκτρονικού ταχυδρομείου του PROFS. Όταν ένα μολυσμένο μήνυμα διαβαζόταν, δινόταν συμβουλή στο λήπτη, “Η κυκλοφορία του μηνύματος αυτού δεν είναι καθόλου αστείο. Ξεκίνα το Christmas.”Ακολουθώντας τη συμβουλή αυτή ο χρήστης ξεκινούσε το πρόγραμμα, το οποίο έδειχνε στην οθόνη του υπολογιστή του ένα χριστουγεννιάτικο δέντρο. Το πρόγραμμα αυτό έψαχνε στη συνέχεια για διευθύνσεις ηλεκτρονικού ταχυδρομείου άλλων χρηστών, που είχαν στείλει ή λάβει μηνύματα από το λογαριασμό του λήπτη, και έστελνε ένα αντίγραφο του στους χρήστες αυτούς. Το πρωτότυπο του κώδικα αυτού βρέθηκε σε δύο σπουδαστές ενός Γερμανικού πανεπιστημίου, οι οποίοι προφανώς δεν είχαν επιδιώξει να προξενήσουν τη ζημιά που επακολούθησε, ο ιός αυτός λέγεται πως χτύπησε υπολογιστές σε 130 διαφορετικές χώρες.

Το παραπάνω πρόγραμμα θεωρήθηκε σκουλήκι επειδή, αντίθετα από τους περισσότερους ιούς, δεν προσάρτησε τον εαυτό του σε άλλο κώδικα. Δε χρειάστηκε να το κάνει αυτό, γιατί ήταν ένα αυτοσυντηρούμενο πρόγραμμα. Όσο όμως είναι σκουλήκι είναι και ιός, επειδή, αντίθετα από τα άλλα σκουλήκια, πολλαπλασιάζεται μέσω μηνυμάτων ηλεκτρονικού ταχυδρομείου και χρειάζεται και τη βοήθεια του χρήστη. Ο χρήστης πρέπει να κάνει μία πράξη ενεργοποίησης του. Το πρόγραμμα αυτό έχει επίσης και τα χαρακτηριστικά ενός Δούρειου Ίππου, δεν πολλαπλασιάζεται αναγκαστικά όπως ο Δούρειος Ίππος έτσι το πρόγραμμα αυτό φαίνεται να είναι τόσο ιός/σκουλήκι όσο και Δούρειος Ίππος. Το CHRISTMA.EXEC δείχνει τις δυσκολίες που υπάρχουν στην ορολογία των ιών/σκουληκιών ιοί των υπολογιστών θα μπορούσαν να ορίζονται

καλύτερα εξαιτίας των πολλών τους διαστάσεων σύμφωνα με το εάν πολλαπλασιάζονται ή όχι, με το αν εκείνοι που πολλαπλασιάζονται το κάνουν αυτό από μόνοι τους ή χρειάζονται και τη βοήθεια του χρήστη, και με τα αντικείμενα (εάν υπάρχουν τέτοια) στα οποία προσαρτώνται (εκτελέσιμα αρχεία, έγγραφα, μηνύματα ηλεκτρονικού ταχυδρομείου, τομείς εκκίνησης κ.ο.κ)

2.6.5 ΤΕΧΝΙΚΕΣ ΑΠΟΚΡΥΨΗΣ

Οι ιοί χρησιμοποιούν αρκετές τεχνικές για να κρύψουν τη παρουσία τους .Οι ιοί stealth διακόπτουν κάποιες από τις λειτουργίες ενός συστήματος και δίνουν στη συνέχεια ψευδείς πληροφορίες για αυτές, όπως για παράδειγμα το μέγεθος ή τα περιεχόμενα ενός αρχείου, όπως αυτά ήταν πριν τα μολύνουν, έτσι ένας έλεγχος που γίνεται για να διαπιστωθεί εάν ένα αρχείο έχει μεγαλώσει ή έχει ένα κώδικα ιού ξεγελιέται και νομίζει πώς το αρχείο αυτό δεν έχει αλλάξει. Οι κρυπτογραφημένοι ιοί αποκρύπτουν την παρουσία τους αποθηκεύοντας των όγκο του κώδικα τους σε κρυπτογραφημένοι μορφή. Μία μικρή ρουτίνα κρυπτογράφησης τοποθετείται στην αρχή του κώδικα, για να αποκρυπτογραφήσει το υπόλοιπο τμήμα του ιού, όταν αυτός ενεργοποιηθεί. Οι πολυμορφικοί ιοί μεταλλάσσονται καθώς κοπιάρονται , τρελαίνοντας τους σαρωτές που ψάχνουν για μία συγκεκριμένη μορφή τους .Αυτό γίνεται συνήθως με τη κρυπτογράφηση, με κάθε μετάλλαξη να κρυπτογραφείται με βάση ένα διαφορετικό τυχαίο κλειδί και έτσι, όλα τα κρυπτογραφημένα κομμάτια να είναι διαφορετικά. Μια ποικιλία εργαλείων διευκολύνουν τη κατασκευή ιών με εξειδικευμένες δυνατότητες. Μια πολυμορφική μηχανή, όπως είναι η μηχανή παράλλαξης,(MtE) μπορεί να προστεθεί σε κάθε κώδικα ιού και να τον μετατρέψει σε πολυμορφικό ιό.

2.6.6 ΠΟΙΟΣ ΦΤΙΑΧΝΕΙ ΙΟΥΣ

Οι περισσότεροι ιοί φαίνεται πως έχουν φτιαχτεί από χάκερς. Με δεδομένο το γεγονός ότι οι χάκερς αυτό που κάνουν το κάνουν για να διασκεδάσουν, πολλοί από αυτούς έχουν σα κίνητρο τους περισσότερο την πρόκληση και την περιπέτεια παρά τη πρόθεση να προκαλέσουν καταστροφές. Η θέση αυτή ενισχύεται και από το ότι σχετικά μικρό ποσοστό ιών διαθέτει φορτίο.

Υπάρχουν ορισμένες ενδείξεις ότι κάποιες κυβερνήσεις χρησιμοποιούν τους ιούς σαν όπλα αμυντικού πληροφοριακού πολέμου.

2.6.7 ΣΚΟΥΛΗΚΙΑ

Ένα σκουλήκι (worm) είναι ένα πρόγραμμα, το οποίο μεταδίδεται από τον ένα υπολογιστή σε έναν άλλο, μέσω ενός δικτύου υπολογιστών εισβάλλοντας σε υπολογιστές με των ίδιο τρόπο, που ένας χάκερ εισβάλλει σε αυτούς. Σε αντίθεση με τους ιούς, τα προγράμματα αυτά δεν παίρνουν καμία βοήθεια από αμελείς χρήστες να βρουν ένα υπολογιστή στον οποίο να μπορούν να εισβάλλουν, να του επιτεθούν και να μεταφέρουν ένα αντίγραφο του κώδικα τους σ'αυτόν, το οποίο θα μπορεί εκεί να εκτελεστεί. Στη πραγματικότητα, ένα τέτοιο πρόγραμμα αυτοματοποιεί εντελώς τα βήματα που κάνει ένας εισβολέας υπολογιστών, ο οποίος πηδάει από το ένα σύστημα στο άλλο.

Το σπουδαιότερο περιστατικό στην ιστορία του internet άρχισε στις 2 Νοεμβρίου του 1988, όταν ο Robert Tappan Morris, μεταπτυχιακός φοιτητής πληροφορικής στο πανεπιστήμιό Cornell της Αμερικής, δημιούργησε ένα πρόγραμμα, το οποίο έφτιαξε αντίγραφα του τα οποία κυκλοφόρησε σε ολόκληρο το δίκτυο. Μέσα σε λίγες ώρες, το σκουλήκι αυτό είχε εισβάλλει σε 2.000 με 6.000 υπολογιστές, σε ποσοστό μεταξύ 3% έως 10% του συνόλου των υπολογιστών που βρίσκονταν στο ίντερνετ την ώρα εκείνη. Το πρόγραμμα αυτό υπερφόρτωνε επίσης τα συστήματα που χτυπούσε δημιουργώντας ουσιαστικά πρόβλημα σε κάθε υπολογιστή στον οποίο εισέβαλε, αυτά θα έπρεπε να αποσυνδεθούν από το δίκτυο ή να σταματήσουν να λειτουργούν εντελώς, ορισμένα από αυτά για αρκετές μέρες, ενόσω η διαχειριστές τους τα καθάριζαν. Όταν ο Moris είδε τη ζημιά που είχε προκαλέσει, έβαλε ένα φίλο του να στείλει ένα μήνυμα στο Δίκτυο με οδηγίες για την απενεργοποίηση του worm. Τότε όμως ήταν πολύ αργά για να σταματήσει το πείραμα που έκανε. Ο Moris καταδικάστηκε στις 16 Μαΐου του 1990 για παράβαση του νόμου για την κατάχρηση και την απάτη με υπολογιστές. Για τις πράξεις του, του επιβλήθηκε

πρόστιμο $10.000 και η ποινή της επιτήρησης για τρία χρόνια καθώς και παροχή 400 ωρών εργασίας στην κοινότητα. Οι εκτιμήσεις των ζημιών που προκάλεσε ποικίλουν δραματικά, αποδεικνύοντας ότι υπάρχει μεγάλη δυσκολία αποτίμησης των απωλειών, που προέρχονται από μια τέτοια επίθεση.

2.6.8 ΕΞΕΛΙΓΜΕΝΑ ΣΚΟΥΛΗΚΙΑ ΠΟΥ ΧΡΗΣΙΜΟΠΟΙΟΥΝ ΜΕΘΟΔΟΥΣ ΚΟΙΝΩΝΙΚΗΣ ΜΗΧΑΝΙΚΗΣ (PHISING)

Εδώ και αρκετό καιρό η συμπεριφορά των σκουληκιών είναι να προσπαθούν να μολύνουν άλλα ευπαθή μηχανήματα. Μία από τις μεθόδους που χρησιμοποιούν είναι η αποστολή μηνυμάτων ηλεκτρονικού ταχυδρομείου χρησιμοποιώντας μια ενσωματωμένη μηχανή μαζικής αποστολής μηνυμάτων e-mail για να παρακάμπτουν τους κεντρικούς εξυπηρετητές αλληλογραφίας.

Μια καινούργια τάση που έχει κάνει την εμφάνιση της είναι η αποστολή προσεκτικά γραμμένων μηνυμάτων από σκουλήκια, με σκοπό την εξαπάτηση του τελικού χρήστη ώστε να νομίζει ότι είναι αυθεντικής προέλευσης. Για να φαίνονται έγκυρα και αυθεντικά, πολλές φορές περιέχουν συνδέσμους σε ιστοσελίδες που είναι καθ' όλα νόμιμες (δηλαδή των πραγματικών τραπεζών που ισχυρίζονται ότι εκπροσωπούν). Έτσι, καταφέρνουν να κερδίσουν την εμπιστοσύνη του αποδέκτη του μηνύματος ώστε να εκτελέσει το επισυναπτόμενο αρχείο ή να ακολουθήσει άλλους συνδέσμους που οδηγούν σε ιστοσελίδες που περιέχουν κακόβουλο κώδικα.

Το εκτελέσιμο αρχείο που βρίσκεται συνήθως συνημμένο στο μήνυμα αλληλογραφίας, δεν είναι ιός και δεν ανιχνεύεται από προγράμματα προστασίας από ιούς (antivirus). Μόλις όμως εκτελεστεί, συνδέεται στο δίκτυο, κατεβάζει (κάνει download) και εκτελεί άλλα αρχεία που περιέχουν επικίνδυνο κώδικα με σκοπό να εκμεταλλευτούν ευπάθειες του λειτουργικού συστήματος και μετά να μολύνουν το σύστημα με κάποιο ιό ή σκουλήκι.

Η ανησυχία που υπάρχει είναι ότι οι χρήστες με λιγότερη εμπειρία μπορεί να

πέσουν πιο εύκολα σε τέτοιες παγίδες και έτσι άθελά τους να δώσουν τον έλεγχο του μηχανήματος τους σε κακόβουλους χρήστες.

ΚΕΦΑΛΑΙΟ 3 - Η ΕΡΓΑΛΕΙΟΘΗΚΗ ΤΟΥ ΑΜΥΝΟΜΕΝΟΥ

3.1 FIREWALL

Τα Firewalls υπάρχουν χρόνια και εξυπηρετούν ως υποστήριξη για τις πληροφορίες στρατηγικών ασφαλείας των περισσοτέρων επιχειρήσεων. Αν και τα firewalls είναι πολύ σημαντικά, κάποια επιχείρηση που βασίζεται ολοκληρωτικά σε ένα firewall για να εκπληρώσει τις ανάγκες ασφαλείας , το κάνει χωρίς σύνεση. Τα firewalls δεν είναι αλεξίσφαιρα. Στην πραγματικότητα πολλές από τις πιο γνωστές πλατφόρμες firewall έχουν πέσει θύματα κάποιων προβλημάτων που έχουν βασανίσει επί μακρόν τα λειτουργικά συστήματα και τις εφαρμογές.

3.1.1 ΤΙ ΕΙΝΑΙ ΕΝΑ FIREWALL

Ένα firewall μπορεί να είναι οποιαδήποτε συσκευή που χρησιμοποιείται ως ένας μηχανισμός ελέγχου της πρόσβασης σε επίπεδο δικτύου, για ένα συγκεκριμένο δίκτυο ή ομάδα δικτύων. Στις περισσότερες περιπτώσεις, τα firewalls μπορούν να χρησιμοποιηθούν για να αποτρέψουν την πρόσβαση των παρείσακτων σε ένα εσωτερικό δίκτυο. Ωστόσο τα firewalls μπορούν επίσης να χρησιμοποιηθούν για τη δημιουργία πιο ασφαλών θυλάκων στα εσωτερικά LANs, για πολύ ευαίσθητες λειτουργίες, όπως μισθοδοτικές καταστάσεις, επεξεργασία πληρωμών και συστήματα έρευνας και ανάπτυξης .Δεν περιορίζονται μόνο σε αποκλειστική περιμετρική χρήση, οι συσκευές firewalls είναι συνήθως αυτόνομοι υπολογιστές, routers ή “μέσα” firewall .Τα μέσα firewall είναι συνήθως εξειδικευμένες συσκευές υλικού οι οποίες συχνά εκτελούν ένα προσαρμοσμένο ή ειδικό ΛΣ.Η σειρά Cisco PIX είναι ένα καλό παράδειγμα συσκευών firewall.

Τα firewalls είναι σχεδιασμένα να λειτουργούν ως σημεία ελέγχου προς και από

το δίκτυο συνεκτιμώντας τις αιτήσεις σύνδεσης καθώς αυτές λαμβάνονται, ελέγχουν αν πρέπει ή όχι να επιτραπεί η κίνηση στο δίκτυο βασιζόμενα σε μία προκαθορισμένη ομάδα κανόνων ή “πολιτικών”.Μόνο αιτήσεις σύνδεσης από εξουσιοδοτημένους κόμβους προς εξουσιοδοτημένους προορισμούς υπόκεινται σε επεξεργασία. Οι υπόλοιπες απορρίπτονται.

Τα περισσότερα firewalls το πετυχαίνουν αυτό “φιλτράροντας” τις διευθύνσεις προέλευσης και προορισμού, μαζί με τους αριθμούς θυρών .Για παράδειγμα ,αν δε θέλετε κάποιοι από το www.mcp.com να συνδέονται στην τοποθεσία σας FTP (μέσω FTP) μπορείτε να εμποδίσετε τη πρόσβαση τους μπλοκάροντας τις αιτήσεις σύνδεσης από τη διεύθυνση 206.246.131.227, στην διεύθυνση της τοποθεσίας σας FTP (ftp.τοποθεσία.παράδειγμα) στη θύρα 21. Στη πλευρά τους , οι άνθρωποι του mcp.com βλέπουν ένα μήνυμα που λέει “Connection Refused” (απορρίφθηκε η σύνδεση) ή κάτι παρόμοιο (ή μπορεί να μη λάβουν κανένα μήνυμα .Απλώς θα μπλοκαριστούν οι προσπάθειες τους για σύνδεση).

3.1.2 ΑΛΛΑ ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΤΩΝ ΠΡΟΙΟΝΤΩΝ FIREWALL

Τα firewalls μπορούν να αναλύουν τα εισερχόμενα πακέτα διαφόρων πρωτοκόλλων. Με βάση αυτή την ανάλυση, ένα firewall μπορεί να εκτελέσει διάφορες ενέργειες. Γι'αυτό τα firewalls είναι ικανά να εκτελούν εκτιμήσεις υπό συνθήκες. (“Εάν συναντήσω αυτού του τύπου πακέτα, θα κάνω το εξής”).

Αυτές οι δομές συνθηκών ονομάζονται κανόνες (rule). Γενικά, όταν ορίζεται ένα firewall, το “εξοπλίζετε” με κανόνες που αντιπροσωπεύουν τις πολιτικές πρόσβασης του δικού σας οργανισμού. Για παράδειγμα , υποθέστε ότι έχετε λογιστικό τμήμα και τμήμα πωλήσεων .Η πολιτική της εταιρείας απαιτεί μόνο το τμήμα πωλήσεων να έχει πρόσβαση στη τοποθεσία σας FTP. Για να θέσετε σε ισχύ αυτή τη πολιτική,παρέχεται ένα firewall με ένα κανόνα .Σε αυτή τη περίπτωση, ο κανόνας ορίζει ότι απορρίπτονται οι αιτήσεις σύνδεσης από το λογιστικό τμήμα στην τοποθεσία FTP.

Με αυτή τη λογική, τα firewalls αποτελούν για τα δίκτυα ό,τι αποτελούν τα δικαιώματα χρήστη για τα λειτουργικά συστήματα. Για παράδειγμα , τα Windows NT σας δίνουν τη δυνατότητα να ορίσετε ποιοι χρήστες μπορούν να έχουν πρόσβαση σε ένα δεδομένο κατάλογο ή αρχείο. Αυτός είναι ο διακριτικός έλεγχος πρόσβασης σε επίπεδο λειτουργικού συστήματος. Ομοίως τα firewalls σας δίνουν τη δυνατότητα να εφαρμόσετε τέτοιο έλεγχο πρόσβασης στους σταθμούς εργασίας του δικτύου και στην ιστοσελίδα σας.

Ωστόσο το φιλτράρισμα της πρόσβασης είναι μόνο ένα μέρος όσων μπορεί να κάνει ένα firewall. Στα τελευταία δύο χρόνια, οι κατασκευαστές firewall έχουν αρχίσει να υλοποιούν τη τεχνική του “νεροχύτη” (kitchen sink) στην ανάπτυξη χαρακτηριστικών , δηλαδή, πολλοί κατασκευαστές έχουν βάλει κάθε χαρακτηριστικό ΕΚΤΟΣ του “νεροχύτη” στα firewall τους. Μερικά από τα πρόσθετα χαρακτηριστικά είναι:

- **Φιλτράρισμα περιεχομένων.** Κάποιες επιχειρήσεις θέλουν να σταματήσουν τους χρήστες τους από τη διεξαγωγή αναζητήσεων σε συγκεκριμένες τοποθεσίες στο web. Τοποθεσίες email βασισμένες στο web, “περιθωριακές” ιστοσελίδες, πύλες ημερησίων συναλλαγών, ιστοσελίδες πορνογραφίας κ.τ.λ. Τα χαρακτηριστικά και οι υπηρεσίες φιλτραρίσματος περιεχομένων μπορούν να βοηθήσουν στο μπλοκάρισμα αυτών των ιστοσελίδων, καθώς και στη προστασία κάποιων τύπων “εχθρικών”μικρο εφαρμογών και κώδικα, βασισμένων σε ActiveX και Java.
- **Εικονικά Ιδιωτικά Δίκτυα (Virtual Private Networks – VPN)** .Τα VPNs χρησιμοποιούνται για να κατευθύνουν με ασφάλεια τη κίνηση από το σημείο Α στο σημείο Β, συνήθως μέσω εχθρικών δικτύων (όπως το Internet).Αν και υπάρχει μια ευρεία κλίμακα ειδικών συσκευών VPN στην αγορά, κατασκευαστές όπως η Checkpoint και η Cisco παρέχουν ευχαρίστως και υπηρεσίες VPN,μαζί με τα προϊόντα τους firewall. Πολλά προϊόντα firewall τώρα παρέχουν και VPN λειτουργικότητα client προς

enterprise, καθώς και λειτουργικότητα LAN προς LAN.

- **Μετάφραση Διευθύνσεων Δικτύου (Network Address Translation – NAT)**.Η μετάφραση διευθύνσεων δίκτυο χρησιμοποιείται συχνά για την αντιστοίχιση άκυρων ή δεσμευμένων ομάδων διευθύνσεων σε έγκυρες. Αν και το NAT δεν είναι απαραίτητα ένα χαρακτηριστικό ασφαλείας, οι πρώτες συσκευές NAT που παρουσιάζονται σε επιχειρησιακά περιβάλλοντα, είναι συνήθως προϊόντα firewall.
- **Εξισορρόπηση Φόρτου.** Περισσότερο γενικός όρος από οτιδήποτε άλλο, η εξισορρόπηση φόρτου των firewalls είναι ένα πράγμα, κάποια προϊόντα firewall υποστηρίζουν τώρα και χαρακτηριστικά που σας βοηθούν να κατευθύνεται τη κίνηση Web και FTP με έναν κατανεμημένο τρόπο.
- **Ανοχή Σφαλμάτων.** Τα υψηλού επιπέδου firewalls,όπως το Cisco PIX και ο συνδυασμός Nokia/Checkpoint, υποστηρίζουν μερικά περίπλοκα χαρακτηριστικά “μεταβίβασης αρμοδιοτήτων σε περίπτωση αποτυχίας”. Συχνά αναφέρονται ως λειτουργικότητα Υψηλής Διαθεσιμότητας (High-Availibility – HA), και αυτά τα προχωρημένα χαρακτηριστικά ανοχής σφαλμάτων συχνά επιτρέπουν στα firewalls να λειτουργούν σε ζευγάρια, με τη μία συσκευή να λειτουργεί ως μια “εν θερμώ εφεδρεία” (hot standby) της άλλης, για τη περίπτωση που η δεύτερη θα αποτύχει.
- **Ανίχνευση Εισβολών (Instruction Detection).** Ο όρος “ανίχνευση εισβολών” μπορεί να σημαίνει πολλά πράγματα, όμως σε αυτή τη περίπτωση, κάποιοι κατασκευαστές έχουν αρχίσει να ενσωματώνουν ένα τελείος διαφορετικό τύπο προϊόντος μαζί με τα προϊόντα firewall. Ενώ αυτό από μόνο του δε δημιουργεί προβλήματα, ο κόσμος θα πρέπει να προσέχει για το είδος του φόρτου εργασίας που μπορεί να επιβληθεί έτσι στο firewall τους.

3.1.3 ΠΑΓΙΔΕΣ ΤΟΥ FIREWALL

Μία παγίδα στο κόσμο των firewalls είναι οτι η ασφάλεια μπορεί να διαμορφωθεί τόσο αυστηρά, ώστε να μπορεί να επιδράσει αρνητικά στη διεργασία δικτύωσης. Για παράδειγμα κάποιες μελέτες αναφέρουν τη χρήση ενός firewall ως μη πρακτική για περιβάλλοντα όπου οι χρήστες εξαρτώνται ιδιαίτερα από κατανεμημένες εφαρμογές. Επειδή τα firewalls μπορούν να υλοποιήσουν τέτοιες αυστηρές πολιτικές ασφάλειας, αυτά τα περιβάλλοντα μπορεί να οδηγηθούν σε τέλμα. Αυτό που κερδίζουν σε ασφάλεια, το χάνουν σε λειτουργικότητα. Για κάποιους αυτό μπορεί να μην είναι βολικό. Όμως το πρόβλημα μπορεί να έχει και μακροχρόνιες συνέπειες που ίσως είναι καταστροφικές. Για παράδειγμα, αναπόφευκτα όλοι οι διαχειριστές αντιμετωπίζουν το κλασσικό δίλημμα ανάμεσα στον χρήστη Χ που θέλει να κάνει Υ ενέργειες και στα προβλήματα ασφαλείας που προκύπτουν από την αίτηση του. Αν και το δίλημμα προσεγγίζεται σε ένα πλήθος αρχών ασφαλείας πληροφοριών, με μια από τις σημαντικότερες την εφαρμογή μιας πολιτικής, μπορεί επίσης να ξεπερνά κάποια όρια της επιχείρησης. Αν για παράδειγμα το τεχνικό προσωπικό χάσει την μάχη να μπλοκάρει την υπηρεσία Υ, θα διατρέχει το κίνδυνο της ύπαρξης ενός “προηγούμενου”σε όλη την επιχείρηση. Αυτό μπορεί να οδηγήσει το προσωπικό ασφαλείας σε διενέξεις με τους εργαζομένους και αργά ή γρήγορα κάτι θα ανοίξει στο firewall που δε θα έπρεπε. Από την άλλη πλευρά, οι έξυπνες επιχειρήσεις γνωρίζουν πως να χειρίζονται αυτές τις καταστάσεις ανά περίπτωση και να ενεργούν κατάλληλα .

Τα firewalls μπορούν να βοηθήσουν στην πρόκληση δυσάρεστων καταστάσεων. Η λύση είναι να γνωρίζει κανείς πως να αποφεύγει αυτές τις καταστάσεις και να γνωρίζει τι να κάνει όταν χάνει μια μάχη. Για παράδειγμα αν κάποιος πάρει την έγκριση να επιτρέπει πρόσβαση τρίτων στο σύστημα μισθοδοσίας μέσω του internet πρέπει να σκεφτείτε τρόπους για να ελέγξετε τη κατάσταση. Απομονώστε τα συστήματα μισθοδοσίας σε ξεχωριστό υποδίκτυο, κοιτάξτε να υλοποιήσετε ισχυρότερες διαδικασίες καταγραφών παρακολούθησης σε επίπεδο

συστήματος, εργαστείτε για την υλοποίηση ενός συστήματος ανίχνευσης παρεισφρήσεων (Instruction Detection System – IDS) στον εν λόγω και ούτω καθ'εξής. Πολλές φορές οι απώλειες που γίνονται αντιληπτές μπορεί να μετατραπούν σε νίκες μακροπρόθεσμα, αν παίξετε τα χαρτιά σας σωστά.

Ένα άλλο ακόμα πιο σοβαρό θέμα είναι εκείνο της εσφαλμένης αίσθησης και αντίληψης της ασφάλειας. Οι διαχειριστές που θεωρούν ότι τα firewalls τους θα τους προστατέψουν από όλα τα κακά, θα βρεθούν προ εκπλήξεων. Μέρος της πρόκλησης υλοποίησης ενός firewall είναι να βοηθήσετε να αναπτυχθεί ένα αίσθημα σιγουριάς, χωρίς να υπερβάλλετε. Ο λόγος που αυτή η ισορροπία είναι τόσο σημαντικά είναι ότι , χωρίς δευτερεύοντα επίπεδα άμυνας, “βάζετε όλα τα αυγά σε ένα καλάθι”. Αν το firewall παραβιαστεί, τα εσωτερικά σας δίκτυα μπορεί εύκολα να καταστραφούν. Τα firewalls αποτελούν μέρος ενός μοντέλου ασφαλείας. Δεν πρέπει να είναι το μοντέλο ασφαλείας, αφού έχουν τα δικά τους μειονεκτήματα.

3.1.4 ΣΥΣΚΕΥΕΣ FIREWALL

Η λέξη συσκευή (appliance) έγινε “μόδα” στα τέλη του 1999 καθώς ο όρος έμοιαζε να υιοθετήθηκε παγκοσμίως από τα τμήματα marketing. Η έννοια της συσκευής είναι απλή και αναμφισβήτητα ελκυστική: Μια ολοκληρωμένη λύση ετοιμοπαράδοτου υλικού/λογισμικού που είναι έτοιμο να λειτουργήσει με ασφάλεια άμεσα. Τα παραδοσιακά firewalls ήταν συνήθως προϊόντα λογισμικού που εκτελούνταν σε ένα υποκείμενο (βάσης) λειτουργικό σύστημα (ΛΣ).Πριν την εγκατάσταση του firewall, έπρεπε να δομήσετε και να ρυθμίσετε πρώτα το υποκείμενο ΛΣ καθώς και να φροντίσετε για την ασφάλεια του. Οι συσκευές firewall, από τη μια πλευρά, προσέφεραν το δέλεαρ της τεχνολογίας “σταθερής κατάστασης” (που σημαίνει “όχι κινητά μέρη”) και εξαιρετικά βελτιστοποιημένους πυρήνες που μπορούσαν να υποστηρίξουν υψηλά επίπεδα επεξεργασίας πακέτων.

Κάπως έτσι εξελίχθηκε η ιστορία σύντομα φάνηκε ότι η συσκευή δεν ήταν συνώνυμη με τη σταθερότητα, καθώς οι κατασκευαστές άρχισαν να διανέμουν συσκευές που βασίζονταν σε σκληρούς δίσκους και κρυμμένα λειτουργικά συστήματα. Οι συζητήσεις για την υψηλή βελτιστοποίηση σπιλώνονταν από άτομα που προωθούσαν πυρήνες BSD και βασικό κώδικα προστασίας firewalling είναι μάλλον ακριβέστερο να πούμε ότι ο όρος συσκευή ορίζει πλέον τη διαφορά ανάμεσα σε κάτι που μπορείτε να απορρίψετε (ένα μηχάνημα σε 2U) και σε κάτι που μπορείτε να πετάξετε (ένα εγχειρίδιο και ένα CD-ROM).

3.2 ΕΡΓΑΛΕΙΑ ΑΝΙΧΝΕΥΣΗΣ ΤΡΩΤΩΝ ΣΗΜΕΙΩΝ (ΣΑΡΩΤΕΣ)

Με τις ανακοινώσεις ευάλωτων σημείων να δημοσιεύονται σε καθημερινή βάση, οι περισσότεροι οργανισμοί αντιμετωπίζουν μια επίπονη μάχη, όταν πρέπει να κυνηγήσουν τα κενά ασφαλείας που υπάρχουν στα συστήματα τους. Σε μία προσπάθεια να βοηθηθούν οι επιχειρήσεις σε αυτή τη διαρκή αναζήτηση, έχουν γίνει προσπάθειες από πολλές πηγές, εμπορικές και “ανοιχτές”, να αυτοματοποιηθεί η διαδικασία της ανακάλυψης των τρωτών σημείων. Αυτά τα εργαλεία αξιολόγησης τρωτών σημείων ή σαρωτές (scanners), διατίθενται σε πολλά σχήματα και μεγέθη και με ποικίλους βαθμούς ακρίβειας.

3.2.1 ΠΩΣ ΛΕΙΤΟΥΡΓΟΥΝ ΟΙ ΣΑΡΩΤΕΣ ΤΡΩΤΩΝ ΣΗΜΕΙΩΝ

Τα τρωτά σημεία εκδηλώνονται σε πολλές μορφές υπάρχουν δύο βασικές κατηγορίες για τα τρωτά σημεία του λειτουργικού συστήματος: Εκείνα τα σημεία που εκτίθενται τοπικά (σε επίπεδο κόμβου) και εκείνα που είναι εκτεθειμένα από μακριά (σε απομακρυσμένο επίπεδο).

Όταν δρομολογούμε σημεία απομακρυσμένης έκθεσης, υπάρχει ένας αριθμός μεθόδων που μπορεί να χρησιμοποιήσει κανείς για να προσεγγίσει την εργασία της αυτόματης σάρωσης ευάλωτων σημείων. Για παράδειγμα μια προσέγγιση μπορεί να εμπλέκει τη χρήση ενός εργαλείου σάρωσης θυρών όπως το nmap,

προσδιορίζοντας το λειτουργικό σύστημα και καταγράφοντας εν συνεχεία όλες τις ανοιχτές θύρες ακρόασης, δίνεται δηλαδή στο χρήστη μια λίστα των θυρών (δηλαδή, 21.25.53.80 και άλλες)και ο τύπος ΛΣ (δηλαδή, Linux Kernel 2,2).Αυτή η προσέγγιση έχει μερικά προβλήματα, ωστόσο αφού ο χρήστης απόκτα πληθώρα δεδομένων (δηλαδή, τις πληροφορίες θυρών) και δε γνωρίζει λεπτομέρειες όπως ποιες υπηρεσίες είναι πραγματικά ευάλωτες. Στον χρήστη δίνεται απλώς ένα ίχνος του συστήματος. Ο προσδιορισμός των υπηρεσιών που λειτουργούν σε αυτές τις θύρες, και το αν είναι πρώτες ή όχι, είναι η "άσκηση" που πρέπει να λύσει ο χρήστης. Για παράδειγμα, αν το σύνολο των δεδομένων μου λέει ότι το μηχάνημα X εκτελεί Linux 2.2 Kernel και έχει μία υπηρεσία που ακροάται στην θύρα 21, πάλι δεν γνωρίζω πολλά για το αν είναι ευάλωτο το σύστημα σε κάποια προβλημάτων υπερχείλισης buffer τύπου wu-ftpd. Στην πραγματικότητα δεν γνωρίζω ούτε αν αυτό το συγκεκριμένο σύστημα εκτελεί wu-ftpd (μπορεί να εκτελεί ProFTPd ή glftpd).Επομένως όταν εντοπίσω μια θύρα, θα πρέπει επιπλέον να :

α)Προσδιορίσω τι λειτουργεί στη θύρα αυτή.

β)Προσδιορίσω ποιας έκδοσης είναι αυτή η υπηρεσία

γ)Ψάξω αν υπάρχουν γνωστά ευάλωτα σημεία που σχετίζονται με αυτή την υπηρεσία και τον αριθμό έκδοσης.

Αν και αυτή η προσέγγιση μπορεί να είναι εφικτή για μία δεκάδα μηχανές περίπου, προφανώς δεν μπορεί να εφαρμοστεί σε μεσαίες και μεγάλες επιχειρήσεις όπου υπάρχουν χιλιάδες μηχανές. Η διαδικασία καθίσταται από δύσκολη έως αδύνατη.

Μία πιο πρακτική προσέγγιση είναι η δόμηση με βάση το προηγούμενο μοντέλο της σάρωσης θυρών και του προσδιορισμού του ΛΣ, με τη προσθήκη κάποιον μηχανισμών για το προσδιορισμό των τύπων υπηρεσιών που λειτουργούν και των εκδόσεων τους. Έτσι θα έχετε συμπληρώσει ακόμη ένα κομμάτι του παζλ. Γυρνώντας πίσω στο παράδειγμα της υπερχείλισης buffer wu-ftpd, προσδιορίζοντας την έκδοση της υπηρεσίας, θα πρέπει να γνωρίζετε:

α)Ότι ο server βασίζεται σε Linux Kernel 2,2

β)Ότι η θύρα 21 είναι ανοικτή

γ)Το τύπο και την έκδοση της υπηρεσίας

Ας υποθέσουμε ότι η διαδικασία ερωτήματος για την υπηρεσία σας πληροφορεί ότι χρησιμοποιείτε wu-ftpd 2.4.2. Αυτό σας φέρνει πιο κοντά, αφού πλέον το μόνο που χρειάζεται είναι να ψάξετε αν η έκδοση 2.4.2 του wu-ftpd έχει κάποια γνωστά τρωτά σημεία.

Το τελευταίο στοιχείο αυτής της διαδικασίας είναι η εξακρίβωση-γνώση για το αν οι εκδόσεις αυτών των υπηρεσιών είναι κατά κάποιο τρόπο ύπουλες, αυτό οδηγεί τους επιτιθέμενους σε: σάρωση, αναζήτηση, διερεύνηση και εκμετάλλευση. Σε αυτή την περίπτωση, προκύπτει ότι η έκδοση 2.4.2 του wu-ftpd είναι τρωτή σε ένα γνωστό τύπο επίθεσης.

Με βάση τον αριθμό των γνωστών ευάλωτων σημείων των προϊόντων (που υπολογίζεται ανάμεσα σε 2000-3000, μέχρι σήμερα),η δημιουργία ενός λεπτομερούς συστήματος για τον σωστό προσδιορισμό και την παρακολούθηση όλων αυτών των τρωτών σημείων των προϊόντων, είναι μια αρκετά εκφοβιστική εργασία. Η εξεύρεση και διαχείριση αυτών των δεδομένων αποτελεί τη μεγαλύτερη πρόκληση και το μεγαλύτερο επιχείρημα για την χρήση ενός αυτοματοποιημένου εργαλείου.

Αν και οι λεπτομέρειες της υλοποίησης ποικίλουν, βασισμένοι σε αυτά τα παραδείγματα, μπορείτε να συμπεράνετε ότι υπάρχει ένας αριθμός κοινών στοιχείων στις περισσότερες προσέγγισης σάρωσης:

- **Τα δεδομένα τρωτών .**Οι σαρωτές τρωτών σημείων έχουν εσωτερικές βάσεις δεδομένων με πληροφορίες για ευάλωτα σημεία που τους βοηθούν να προσδιορίζουν με ακρίβεια σημεία του συστήματος εκτιθέμενα από μακριά.
- **Ο μηχανισμός σάρωσης.** Τα τεχνικά στοιχεία του σαρωτή βασίζονται στη δυνατότητα του να προσδιορίζει σωστά τις υπηρεσίες, τα δευτερεύοντα συστήματα και τα τρωτά σημεία. Ανάλογα με το πώς έχει

γραφεί ο σαρωτής , μπορεί να μην είναι επαρκής για τη σάρωση πολλών μηχανημάτων.

- **Ο μηχανισμός δημιουργίας αναφορών.** Η εύρεση ενός προβλήματος είναι ένα πράγμα. Η άρτια αναφορά σε αυτό είναι κάτι το τελείως διαφορετικό. Μερικά προϊόντα είναι ισχυρότερα από άλλα σε ότι αφορά τη δυνατότητα σαφούς διατύπωσης όσων ανακάλυψαν.

3.2.2 ΒΑΣΙΚΑ ΜΕΙΟΝΕΚΤΗΜΑΤΑ

Σχεδόν όλα τα εργαλεία ασφάλειας έχουν μερικά βασικά προβλήματα, και οι σαρωτές τρωτών σημείων δεν διαφέρουν. Η γνώση των ορίων τους είναι το ίδιο σημαντική με τη γνώση των δυνατοτήτων τους.

Τα μεγαλύτερα μειονεκτήματα αυτών των προϊόντων μπορούν να ομαδοποιηθούν σε τρεις κατηγορίες: Πληρότητα, επικαιρότητα και ακρίβεια. Πρώτον, οι αναφορές για τα προϊόντα αυτά έχουν δείξει ότι πολλά από αυτά εντοπίζουν ένα μεγάλο αριθμό τρωτών σημείων, όμως κανένα από αυτά δεν είναι εξοπλισμένο για να τα αναγνωρίζει όλα.

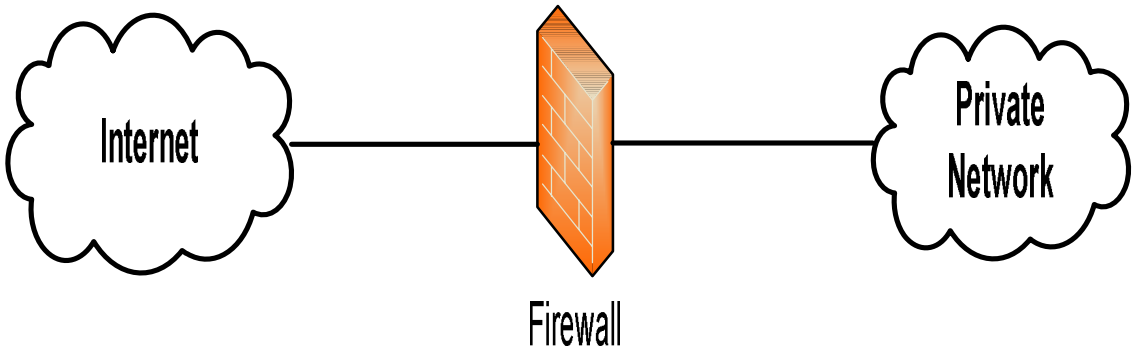
Δεύτερον, τα περισσότερα από αυτά τα προϊόντα ενημερώνονται μια φορά το τρίμηνο, αν όχι πιο συχνά. Αν ένα τρωτό σημείο ανακοινωθεί τον Ιανουάριο, ο σαρωτής σας μπορεί να μην είναι ενημερωμένος για να το ανιχνεύσει μέχρι το Μάρτιο. Δηλαδή αφήνει δύο μήνες στην διάρκεια των οποίων θα πρέπει να προφυλάξετε μόνοι σας τον εαυτό σας .Τώρα, η προσπάθεια προσδιορισμού εσωτερικών απειλών θα πρέπει να είναι σε κάθε περίπτωση πάνω από αυτό το πρόβλημα, αλλά το θέμα είναι ότι αυτοί οι σαρωτές δεν θα πρέπει να είναι η πρωταρχική σας μέθοδος άμυνας, όταν πρόκειται να κυνηγήσετε εκτεθειμένα σημεία από μακριά.

Ένα άλλο πρόβλημα είναι ότι οι περισσότεροι σημερινοί σαρωτές απλώς υλοποιούν τεχνικές “απόσπασης σημαίας” για να προσδιορίσουν τις εκδόσεις των υπηρεσιών. Αυτή η τεχνική είναι αναμφισβήτητα αρκετή για τα περισσότερα περιβάλλοντα. Όμως, μπορεί να δημιουργήσει κάποια ενδιαφέροντα σενάρια. Για παράδειγμα, εκτελώντας άπλα telnet στη θύρα 25 (SMTP mail) και στη θύρα 21 (FTP), μπορεί κανείς να προσδιορίσει τις εκδόσεις αυτών των δύο υπηρεσιών.

Σημειώστε ότι αυτές οι δύο μηχανές εμφανίζονται να εκτελούν το Microsoft Exchange 5,5 και την έκδοση 4,0 του Microsoft FTP server. Όμως πολλές υπηρεσίες όπως το Bind, το sendmail και το wu-ftpd επιτρέπουν πλέον στους

διαχειριστές να αλλάζουν αυτά τα banners στα αρχεία ρυθμίσεων. Αν και αυτό δεν αποτελεί απειλή για την ασφάλεια, η αλλαγή ενός προεπιλεγμένου wu-ftpd banner σε “Fabio's favorite FTP Server version 1,0”,θα μπερδέψει τελείως τα περισσότερα εργαλεία σάρωσης τρωτών σημείων. Το περίεργο και ενοχλητικό δίδαγμα αυτής της ιστορίας είναι ότι αν θέλετε οι σαρωτές σας να είναι αποτελεσματικοί, μην αλλάζετε τα προεπιλεγμένα banners.

Τέλος, αυτά τα προϊόντα ακόμη αντιπαλεύουν τις ψευδείς διαβεβαιώσεις σε μεγάλα και διαφορετικά δίκτυα, οι σαρωτές τρωτών σημείων θα σημάνουν εσφαλμένα συναγερμό και θα αναφέρουν τρωτά σημεία, που απλώς δεν υπάρχουν.



3.3 ΣΥΣΤΗΜΑ ΑΝΙΧΝΕΥΣΗΣ ΠΑΡΕΙΣΦΡΗΣΗΣ (IDSs)

Η ανίχνευση παρείσφρησης είναι μία από τις θερμότερες περιοχές στο πεδίο της ασφάλειας πληροφοριών. Αν και οι επαγγελίες της τεχνολογίας να ανιχνεύει αυτόματα, να προειδοποιεί, και ενδεχομένως να σταματά τους τεχνικούς εισβολείς, είναι εξαιρετικά ελκυστικές, η τεχνολογία αυτή είναι πολύ νέα ακόμη.

3.3.1 ΕΙΣΑΓΩΓΗ ΣΤΗ ΑΝΙΧΝΕΥΣΗ ΠΑΡΕΙΣΦΡΗΣΕΩΝ

Ο όρος ανίχνευση παρεισφρήσεων σημαίνει πολλά πράγματα σε πολλούς ανθρώπους. Ωστόσο, για λόγους σαφήνειας θα τον ορίσουμε ως την ενέργεια του εντοπισμού ενός εχθρικού χρήστη ή εισβολέα που επιχειρεί να αποκτήσει πρόσβαση χωρίς άδεια. Με τη προϋπόθεση αυτού του ορισμού, ένα πλήθος δημοφιλών μεθόδων χρησιμοποιούνται για τον εντοπισμό εισβολέων – για παράδειγμα, η διερεύνηση συστήματος, web, εφαρμογών, firewall, και router καταγράφει πληροφορίες για εχθρικές ή ασυνήθεις δραστηριότητες. Μερικοί διαχειριστές συστημάτων θα υλοποιούν δυαδικούς ελέγχους ακεραιότητας όπως το AIDE ή το Tripwire, με την ελπίδα να εντοπίσουν επιτιθέμενους, όταν τοποθετούν κώδικα Δούρειου Ίππου σε εκτεθειμένους servers. Άλλοι διαχειριστές θα παρακολουθούν απλώς καταγραφές συμβάντων αναζητώντας αποτυχημένες προσπάθειες σύνδεσης των χρηστών.

Αν και όλες αυτές οι μέθοδοι είναι χρήσιμες, είναι δύσκολο, αν όχι αδύνατο , να εκτελούνται σε καθημερινή βάση. Και αν μιλάμε για μερικές εκατοντάδες μηχανές, η εργασία καθίσταται αμέσως εξουθενωτική. Λύση: Το σύστημα ανίχνευσης παρεισφήσεων.

Οι ρίζες των σύγχρονων συστημάτων ανίχνευσης παρεισφήσεων βρίσκονται στα μοντέλα συστημάτων Intrusion Detection Expert System (IDES) και Distributed Insrusion Detection System (DIDS) που αναπτύχθηκαν από το υπουργείο άμυνας (Department of Defense – DOD) των ΗΠΑ στα τέλη της

δεκαετίας του '80 και τις αρχές τις δεκαετίας του '90.Πρόκειται για κάποια από τα πρώτα αυτοματοποιημένα συστήματα που υλοποιήθηκαν. Σήμερα, τα περισσότερα συστήματα IDSs σχεδιάζονται με τον ίδιο στόχο: Να βοηθήσουν στην αυτοματοποίηση της διαδικασίας αναζήτησης εισβολέων. Αυτό μπορεί να είναι απλό όσο η ανάλυση των καταγραφών firewall σε πραγματικό χρόνο, ερευνώντας θύρες, ή πολύπλοκη, όσο η εφαρμογή ρουτινών διερεύνησης στην καθαρή διακίνηση του δικτύου, ερευνώντας για προσπάθειες υπερχείλισης buffer.

Τα παραδοσιακά σχήματα ταξινόμησης IDS τοποθετούν τα περισσότερα συστήματα σε δύο διακριτούς χώρους: Μοντέλα ανίχνευσης κατάχρησης και μοντέλα ανίχνευσης ανωμαλιών. Θα επικεντρωθούμε σε δύο υλοποιήσεις του μοντέλου ανίχνευσης κατάχρησης: Συστήματα ανίχνευσης παρεισφρήσεων βασισμένα σε δίκτυα (NIDS) και σύστημα ανίχνευσης παρεισφρήσεων βασισμένα σε κόμβους (HIDS).Υπάρχουν πολλά άλλα μοντέλα ανίχνευσης παρεισφρήσεων, αλλά είναι λιγότερο δημοφιλή. Ωστόσο, οι περισσότερες σύγχρονες υλοποιήσεις IDS μπορούν να ομαδοποιηθούν στις εξής κατηγορίες:

- **IDSs Βασισμένα στο δίκτυο**. Στην τρέχουσα μορφή τους, οι συσκευές NIDS είναι μηχανές ανάλυσης καθαρών πακέτων – sniffers μεγαλοποιημένα σε στεροειδή .Παρεμβαίνουν στην κίνηση δικτύου και συγκρίνουν τη κίνηση με ένα σύνολο γνωστών προτύπων ή υπογραφών αντεπιθέσεων συσκευές NIDS συγκρίνουν αυτές τις υπογραφές σε κάθε πακέτο που βλέπουν , με την ελπίδα να πιάσουν τους εισβολείς σε δράση. Οι συσκευές NIDS μπορούν να χρησιμοποιηθούν παθητικά, χωρίς να απαιτούνται βασικές τροποποιήσεις στα συστήματα και τα δίκτυα.
- **IDSs Βασισμένα σε κόμβους**. Αυτά τα συστήματα ποικίλλουν από κατασκευαστή σε κατασκευαστή, αλλά είναι συνήθως συστηματοκεντρικά ως προς την ανάλυση τους. Τα περισσότερα βασισμένα σε κόμβους IDSs έχουν συστατικά που αναλύουν τις καταγραφές συστήματος και παρακολουθούν τις συνδέσεις των χρηστών

και τις διεργασίες. Μερικά από τα πλέον προχωρημένα συστήματα θα έχουν ακόμη ενσωματωμένες δυνατότητες σύλληψης υλοποιήσεων κώδικα Δούρειου ίππου. Τα βασισμένα σε κόμβους συστήματα βασίζονται σε agents δηλαδή , απαιτούν την εγκατάσταση ενός προγράμματος στα συστήματα που προστατεύουν. Αυτό τους επιτρέπει να είναι διεξοδικότερα σε ορισμένα επίπεδα, αλλά και πονοκέφαλος στην υλοποίηση και διαχείριση τους.

- **IDSs Βασισμένα σε ανωμαλίες**. Τα βασισμένα σε ανωμαλίες συστήματα είναι κάπως περισσότερο δυσνόητα και συχνά αναφέρονται ως “έννοιες” μάλλον, παρά ως πραγματικά μοντέλα. Η φιλοσοφία πίσω από τις προσεγγίσεις που βασίζονται στις ανωμαλίες είναι να κατανοηθούν τα πρότυπα των χρηστών και της κίνησης στο δικτυοειδής, και να ευρεθούν παρεκκλίσεις σε αυτά τα πρότυπα .Για παράδειγμα, ένας χρήστης που κανονικά συνδέεται από Δευτέρα έως την Παρασκευή αλλά τώρα συνδέεται στις 3 πμ. την Κυριακή , μπορεί να σημειωθεί ως ενδεχόμενο πρόβλημα από ένα IDS ανωμαλιών, ένα IDS βασισμένο στην διερεύνηση ανωμαλιών θα μπορούσε να ανιχνεύσει κάτι που δεν πάει καλά, χωρίς να γνωρίζει συγκεκριμένα την πηγή του προβλήματος.

Οι συνηθέστεροι τύποι IDS, εμπορικοί και ανάπτυξης, είναι τα μοντέλα HIDS και NIDS. Αν και υπάρχουν λειτουργικά μοντέλα IDSs βασισμένων στην ανάλυση ανωμαλιών, υλοποιούνται σπανίως εκτός των κυβερνητικών και ακαδημαϊκών κύκλων.

3.3.2 ΠΟΙΟΣ ΠΡΕΠΕΙ ΝΑ ΧΡΗΣΙΜΟΠΟΙΕΙ ΕΝΑ IDS

Αν και η τεχνολογία IDS είναι σαφώς ελκυστική, πριν αφιερώσετε κάποιο χρόνο στην έρευνα των IDSs, θα πρέπει πρώτα να αναρωτηθείτε αν έχει νόημα ένα IDS για τον οργανισμό σας. Εάν για παράδειγμα, ένας οργανισμός δεν διαθέτει βασικά συστατικά ασφαλείας, όπως firewalls, διαδικασίες προστασίας

συστήματος ΛΣ, ή προστασία από ιούς, δεν θα πρέπει να αποκτήσει προτεραιότητα στην υλοποίηση ενός IDS, έναντι των προαναφερθεισών προσπαθειών. Ένα IDS θα πρέπει να εγκατασταθεί μόνο αφού έχουν ήδη εξεταστεί άλλες όψεις τής στρατηγικής ασφάλειας πληροφοριών , ή για να αντιμετωπιστούν συγκεκριμένες καταστάσεις ή μικροπροβλήματα παράδειγμα, εάν ξεκίνησε μια νέα πρωτοβουλία ηλεκτρονικού εμπορίου που απλώς δε μπορείτε να την ασφαλίσετε επαρκώς, ένα IDS μπορεί να σας βοηθήσει να ρίχνετε μια πιο οξυδερκή ματιά σε αυτό. Επιπλέον, ορισμένοι άνθρωποι χρησιμοποιούν τα IDSs ως εργαλείο επικύρωσης των κανόνων που έχουν θεσπίσει για τα firewalls .Αλλά αν το δίκτυο σας αποτελεί ένα χαοτικό κολάζ ευάλωτων σημείων, ένα IDS θα σας βοηθήσει απλώς να αντιληφθείτε το προφανές. Θυμηθείτε, τα σύγχρονα IDS εξακολουθούν, στο μεγαλύτερο μέρος, να είναι συσκευές που αντιδρούν. Δεν επιλύουν τα προβλήματα σας.

3.3.3 ΣΥΝΗΘΗ ΚΡΙΤΗΤΡΙΑ ΑΞΙΟΛΟΓΗΣΗΣ

Όταν επιλέγετε ένα σύστημα ανίχνευσης παρεισφρήσεων, κατανοήστε ότι επιλέγετε δύο πράγματα: Α) ένα προϊόν, και Β) έναν κατασκευαστή που θα ενημερώνει αυτό το προϊόν. Αν και ο κατασκευαστής (ή η ομάδα, στην περίπτωση των λύσεων open-source) πίσω από το προϊόν είναι πάντοτε ένα θέμα που θα λάβετε υπόψη σας, αυτό γίνεται ακόμη πιο κρίσιμο στην αγορά της ανίχνευσης παρεισφρήσεων. Επειδή τα IDSs είναι τόσο “ευαίσθητα” στο χρόνο, και τόσο εξαρτώμενα από ενημερώσεις του προϊόντος, ένα καλό σύστημα θα γίνεται διαρκώς λιγότερο χρήσιμο, αν δεν επιτηρείται κατάλληλα και τακτικά. Η αξιολόγηση των εγγράφων παρακολούθησης του κατασκευαστή σε ενημερώσεις του προϊόντος είναι μια προσπάθεια που αξίζει το κόπο.

Από την πλευρά του προϊόντος, υπάρχει ένας αριθμός θεμάτων και χαρακτηριστικών που μπορούν να βρεθούν σε ένα IDS αλλά όχι σε ένα άλλο. Ωστόσο πολλά από τα χαρακτηριστικά εντυπωσιασμού αυτών των προϊόντων

είναι απλώς χαριτωμένα χαρακτηριστικά. Βεβαιωθείτε ότι αξιολογείτε πρώτα τα ουσιαστικά χαρακτηριστικά και κατόπιν εξετάστε τα πρόσθετα .Ακολουθεί μία λίστα ουσιωδών χαρακτηριστικών που θα πρέπει να αξιολογήσετε, όταν παίρνετε απόφασης για την επιλογή ενός IDS:

- **Βάθος κάλυψης**. Ένα από τα σημαντικότερα συστατικά ενός συστήματος ανίχνευσης παρεισφρήσεων είναι η δυνατότητα του να ανιχνεύει ένα ευρύ φάσμα επιθέσεων .Αν και μία θαυμάσια μηχανή υψηλών προδιαγραφών, επιλογές διαφορετικών ρυθμίσεων, και ένα "στιλπνό" περιβάλλον διαχείρισης είναι όλα καλά σημεία για πωλήσεις, εάν το προϊόν είναι ανίκανο να ανιχνεύσει περισσότερες από μερικές επιθέσεις, θα κάνει ελάχιστο καλό. Βεβαιωθείτε ότι οποιαδήποτε λύση NIDS εξετάζετε και συνοδεύεται από ένα καλό σύνολο υπογραφών επιθέσεων. Στην πλευρά των HIDS, βεβαιωθείτε ότι το προϊόν κάνει περισσότερα από την απλή διερεύνηση μερικών αρχείων καταγραφών για μερικά συμβάντα, και βεβαιωθείτε ότι το προϊόν υποστηρίζει όλες τις πλατφόρμες που χρειάζεται να παρακολουθείτε. Εάν για παράδειγμα, οι HIDS agents υποστηρίζουν μόνο τα Windows NT, αλλά έχετε μηχανές Solaris και Linux, θα έχετε προβλήματα στη συνολική κάλυψη.
- **Ακρίβεια κάλυψης**. Είναι δύσκολο να καθοριστεί αυτός ο παράγοντας, χωρίς διεξοδικούς ελέγχους, αλλά θα πρέπει να σημειωθεί ότι δεν έχουν δημιουργηθεί με τον ίδιο τρόπο όλες οι υπογραφές. Οι ψευδείς διαβεβαιώσεις είναι ένα μεγάλο πρόβλημα με τις περισσότερες λύσεις NIDS, και σε μεγάλα περιβάλλοντα αυτοί οι ψευδείς συναγερμοί, μπορεί να θέσουν σε κίνδυνο την γενική αποτελεσματικότητα της προσπάθειας ανίχνευσης παρεισφρήσεων. Τα προϊόντα που έχουν σχεδιαστεί με γνώμονα το περιορισμό των ψευδών διαβεβαιώσεων, θα είναι προτιμότερα τα επόμενα χρόνια.
- **Ισχυρή Αρχιτεκτονική**. Υπάρχουν πολλά συστατικά σε μία λύση ανίχνευσης παρεισφρήσεων, και είναι σημαντικό και για τις μηχανές και

για το ίδιο το πλαίσιο IDS να έχουν σχεδιαστεί με γνώμονα την ισχύ. Στη πλευρά της μηχανής/agent, τα προϊόντα θα πρέπει να μπορούν να ανθίστανται σε τεχνικές επιθέσεων και βασικών ελιγμών. Αν και οι ελιγμοί αποτέλεσαν παραδοσιακά ένα πρόβλημα των συσκευών NIDS, και μάλλον θα συνεχίζουν να τις ταλανίζουν για αρκετό χρόνο ακόμη, οι διορατικοί κατασκευαστές συνεχίζουν τις προσπάθειες τους αντιμετώπισης αυτών των θεμάτων. Οι λιγότερο διορατικοί κατασκευαστές έχουν επιλέξει να τα αγνοήσουν, κάτι που όχι μόνο περιορίζει την αποτελεσματικότητα του προϊόντος, αλλά και την σιγουριά μεταξύ των επαγγελματιών ασφαλείας.

- **Δυνατότητα κλιμάκωσης**. Υπάρχουν πολλά συστατικά που επηρεάζουν τα IDSs στο θέμα της "κλιμάκωσης" αλλά τα σημαντικότερα είναι στις περιοχές της παρακολούθησης υψηλού bandwitch και τις διαχείρισης δεδομένων. Τα θέματα bandwitch ισχύουν και στις συσκευές NIDS από την άποψη ότι πολλά προϊόντα έχουν προβλήματα παρακολούθησης περιβαλλόντων υψηλού brandwitch και πολλαπλών συνεδριών. Στην πλευρά της διαχείρισης, μερικά προϊόντα αγωνίζονται με τη παρακολούθηση, την αποθήκευση και τη παρουσίαση μεγάλου όγκου δεδομένων προειδοποίησης. Για παράδειγμα, αν χρησιμοποιείτε μερικές δεκάδες αισθητήρες (βασισμένους σε δίκτυα ή κόμβους) σε ένα δίκτυο υψηλής κίνησης/υψηλών επιπέδων προειδοποιήσεων, θα διοχετεύουν πολλά δεδομένα πίσω στις κεντρικές βάσεις δεδομένων ή στις κονσόλες. Μερικά συστήματα back-end θα καταρρέουν κάτω από τέτοια φορτία, ή το χειρότερο, ο όγκος των δεδομένων θα καθιστά απίστευτα δύσκολο για τους διαχειριστές ασφάλεια να ταξινομήσουν τις προειδοποιήσεις. Ωστόσο, θα πρέπει να σημειωθεί ότι αυτά τα θέματα δεν αφορούν όλα τα περιβάλλοντα. Για παράδειγμα, αν ψάχνετε να τοποθετήσετε μερικές συσκευές ID για να παρακολουθείτε μερικές συνδέσεις T1, είναι απίθανο να αντιμετωπίσετε ζητήματα bandwitch και αποθήκευσης δεδομένων.

- **Πλαίσιο εργασιών διαχείρισης**. Η δυνατότητα ανίχνευσης επιθέσεων είναι κρίσιμη για ένα IDS, αλλά εξίσου σημαντική είναι η δυνατότητα σαφούς και αποτελεσματικής παρουσίασης των δεδομένων που αφορούν αυτές τις επιθέσεις. Εάν οι επιτετραμμένοι της ασφάλειας δεν μπορούν να προσπελάσουν εύκολα τα δεδομένα επιθέσεων και προειδοποιήσεων, η συνολική χρησιμότητα του IDS θα είναι περιορισμένη. Όταν αξιολογείτε συστήματα ανίχνευσης παρεισφρήσεων, βεβαιωθείτε ότι χρησιμοποιείτε τη κονσόλα διαχείρισης ενός συστήματος, και βεβαιωθείτε ότι σας επιτρέπει να προσπελάσετε τις πληροφορίες που θέλετε εύκολα. Εν συντομία, το πλαίσιο εργασία διαχείρισης που χρησιμοποιείται για να ελέγχει και να παρακολουθεί τις συσκευές, είναι σημαντικό σχεδόν όσο το HIDS και οι ίδιες οι συσκευές NIDS.
- **Έγκαιρες ενημερώσεις**. Όπως και στη περιοχή των προϊόντων προσδιορισμού ευάλωτων σημείων (VA), καθώς νέες επιθέσεις θα συνεχίζουν να έρχονται στο προσκήνιο, η ανάγκη για έγκαιρες ενημερώσεις των προϊόντων IDS θα καθίσταται κρίσιμη. Η λειτουργία ενός ξεπερασμένου IDS είναι ανάλογη με τη λειτουργία ενός αεροδρομίου χωρίς ραντάρ. Αν και οι ενημερώσεις είναι το μεγαλύτερο θέμα σε ότι αφορά τα προϊόντα NIDS, το θέμα είναι εξίσου σημαντικό για όλα τα μοντέλα IDS.
- **Προσαρμοστικότητα**. Μερικά προϊόντα ανίχνευσης παρεισφρήσεων επιτρέπουν διαφορετικές περιοχές προσαρμογών, ενώ άλλα είναι μάλλον στατικά και καθόλου ευέλικτα. Για τους περισσότερους οργανισμούς, τα χαρακτηριστικά προσαρμογών δεν θα αποτελούν σημαντικό θέμα, επειδή λειτουργούν τις λύσεις τους IDS με τις έτοιμες ρυθμίσεις. Για άλλους, η προσαρμοστικότητα είναι σημαντική. Ωστόσο, όταν επιλέγετε ένα κατασκευαστή IDS, είναι επιθυμητό να αξιολογήσετε τις ανάγκες σας για τη στιγμή, αλλά και για το μέλλον. Αν και μπορεί να μην χρειάζεστε την ικανότητα εγγραφής μίας προσαρμοσμένης υπογραφής σήμερα, μπορεί να

χρειαστείτε αυτή τη λειτουργικότητα στο μέλλον.

- **Απαιτήσεις ικανοτήτων**. Οι συσκευές ανίχνευσης παρεισφρήσεων θα πρέπει να αντιμετωπίζονται όπως οποιοδήποτε άλλο συστατικό του IT enterprise – κατάλληλα εκπαιδευμένο προσωπικό θα πρέπει να χειρίζεται τη λύση. Δυστυχώς, εκείνο που και οι διαχειριστές και οι διευθυντές μοιάζει να θέτουν στην άκρη είναι τα θέματα που περιβάλλουν την εκπαίδευση τους στο IDS.

3.4 ΕΡΓΑΛΕΙΑ ΚΑΤΑΓΡΑΦΗΣ ΚΑΙ ΠΑΡΑΚΟΛΟΥΘΗΣΗΣ

3.4.1 ΓΙΑΤΙ ΚΑΤΑΓΡΑΦΕΤΕ

Τα αρχεία καταγραφών είναι ένα άλλο σύνολο “δίκοπων μαχαιριών” που βρίσκονται στο παρασκήνιο. Μπορούν να σας σώσουν, η να σας εξουθενώσουν ολοκληρωτικά, ανάλογα με την περίπτωση. Η σημασία τους ωστόσο, υποτιμάται συχνά.

Τα αρχεία καταγραφών είναι χρήσιμα για διάφορα πράγματα. Μπορούν να βοηθήσουν στην ανίχνευση και αντιμετώπιση προβλημάτων. Μπορούν να χρησιμοποιηθούν για την παρακολούθηση ανωμαλιών στο δίκτυο. Μπορούν να βοηθήσουν στην παρακολούθηση των βημάτων ενός εισβολέα, ή να βοηθήσουν να αποδείξετε τη κατάσταση σε ένα νομικό δικαστήριο.

3.4.2 ΔΙΑΜΟΡΦΩΣΗ ΜΙΑΣ ΣΤΡΑΤΗΓΙΚΗΣ ΚΑΤΑΓΡΑΦΩΝ

Για να περιχαρακώσετε το χώρο σας έναντι των παρεμβάσεων των crackers στις εισαγωγές καταγραφών σας, θα πρέπει να δημιουργήσετε μια στρατηγική καταγραφών που θα είναι δύσκολο να καταστρατηγηθεί. Ο ευκολότερος τρόπος για να το πετύχετε αυτό είναι να δημιουργείτε τις καταγραφές σας σε μία συσκευή μια κατεύθυνσης, και μίας εγγραφής, ή να αντιγράφετε τα αρχεία σας καταγραφών σε έναν ασφαλή server καταγραφών συμβάντων. Μερικοί διαχειριστές ορίζουν τα συστήματα τους UNIX να δημιουργούν τις καταγραφές τους σε μία σειριακή θύρα συνδεδεμένη σε μία ανεξάρτητη μηχανή. Αν και αυτό είναι αρκετά ασφαλές, το μοντέλο δεν επεκτείνετε το ίδιο καλά.

Ένα μοντέλο που είναι κάπως περισσότερο κλιμακούμενο περιστρέφεται γύρω από τη χρήση του πρωτοκόλλου syslog. Το syslog είναι μια τυπική υπηρεσία σχεδόν σε κάθε πλατφόρμα UNIX, και πρόσφατα προϊόντα την έχουν καταστήσει διαθέσιμη και για άλλες πλατφόρμες (όπως τα Windows NT).Αν και

υπάρχουν μερικές ασφαλέστερες εναλλακτικές λύσεις στο syslog, το syslog είναι πλέον κοινό στα περισσότερα προϊόντα router και firewall. Αυτή η καθολική παρουσία δίνει στους διαχειριστές έναν κοινό παρανομαστή για να επικεντρώνουν όλη τη διαδικασία καταγραφών συμβάντων. Για παράδειγμα, οι διαχειριστές θα μπορούσαν να ρυθμίσουν όλους τους κόμβους να καταγράφουν σε έναν προστατευμένο, κεντρικό server καταγραφών, βασισμένων στο syslog δίνοντας στις ομάδες ασφαλείας ένα κοινό σημείο συντονισμού των δεδομένων καταγραφών.

Με κατάλληλη ρύθμιση, η μόνη κίνηση που επιτρέπεται στον syslog server είναι η κίνηση που προορίζεται για την UDP θύρα 514 (την θύρα του syslog).Αποστέλλοντας τα αρχεία καταγραφών συστημάτων σε μια ξεχωριστή, ασφαλή μηχανή, δυσκολεύετε αρκετά τους εισβολείς στην απαλοιφή των ιχνών τους.

- Η Adiscon δημιουργεί ένα θαυμάσιο βοήθημα βασισμένο σε Windows NT,με το όνομα Event Reporter, που σας δίνει τη δυνατότητα να στέλνετε καταγραφές συμβάντων των Windows NT σε ένα server βασισμένο στο syslog.
- Τον προηγούμενο χρόνο έκανε την εμφάνιση του σε ένα πρόγραμμα με το όνομα SRS (Secure Remote Streaming).Το SRS έχει γραφεί για να αντικαταστήσει το syslog, με την ασφάλεια στο κέντρο της σχεδίασης. Δεν έχει υιοθετηθεί τόσο πολύ όσο το syslog, αλλά αξίζει να το εξετάσετε ως μία ασφαλέστερη εναλλακτική λύση.

Εκτός της κεντρικής συλλογής των καταγραφών σας, μπορεί να θέλετε να σκεφτείτε την χρήση τουλάχιστον ενός εργαλείου καταγραφών ή ανάλυσης τρίτων. Αυτή η προσέγγιση έχει αρκετά πλεονεκτήματα. Πρώτο, αν και η κοινότητα των crackers είναι εξοικειωμένοι με τις καταγραφές που βασίζονται στο λειτουργικό σύστημα, μερικοί crackers έχουν τη γνώση ή τα μέσα για να καταστρατηγήσουν το λογισμικό καταγραφών τρίτων. Δεύτερον, τα καλά πακέτα λογισμικού καταγραφών τρίτων αποσπούν τις καταγραφές τους

ανεξάρτητα από τις καταγραφές του λειτουργικού συστήματος. Θα γνωρίζετε ότι οι εισβολείς έχουν επιτεθεί στο σύστημα σας όταν συγκριθούν αυτές οι πληροφορίες, και υπάρχει ασυμφωνία ανάμεσα στις καταγραφές των πακέτων τρίτων και στις συνήθεις καταγραφές του συστήματος.

Αυτό είναι ιδιαιτέρως αληθές αν απομονώσετε τις καταγραφές πακέτων τρίτων για παράδειγμα, υποθέστε ότι χρησιμοποιείτε ένα εργαλείο καταγραφών συμβάντων τρίτου για να επαληθεύσετε αργότερα την ακεραιότητα των βασισμένων στο λειτουργικό σύστημα καταγραφών. Αν και ακριβό, η τοποθέτηση αυτών των καταγραφών τρίτων σε μέσα μιας εγγραφής, σας εξασφαλίζει ένα σύνολο αξιόπιστων καταγραφών, και η αξιοπιστία είναι το παν.

Η χρήση προϊόντων τρίτων είναι συνετή ενέργεια στη περίπτωση αποτυχίας των βοηθημάτων καταγραφής συμβάντων. Για παράδειγμα, σε μερικές εκδόσεις του Solaris, το αρχείο tmpx θα περικόπτει τα εισερχόμενα ονόματα κόμβων, εισάγοντας οποιαδήποτε δεδομένα λαμβάνονται από την εντολή last εσφαλμένα και μη ολοκληρωμένα.

Προσεγγίζοντας το θέμα από διαφορετική γωνιά, είναι πλέον μια μάλλον συνήθης διαδικασία για τους crackers να τερματίζουν τις δυνατότητες σας καταγραφής συμβάντων, πριν ξεκινήσουν μια πραγματική επίθεση. Εάν ο στόχος εκτελεί μια έκδοση Solaris 2.5.x χωρίς διορθωτικά patchs, για παράδειγμα, μπορείτε να τερματίσετε το syslog, στέλνοντας του απλώς ένα εξωτερικό μήνυμα από μια ανύπαρκτη διεύθυνση IP .Ομοίως, εάν το syslog δέχεται απομακρυσμένα μηνύματα, καθένας μπορεί να κάνει μία εσφαλμένη εισαγωγή στο αρχείο καταγραφής συμβάντων.

3.5 ΚΡΥΠΤΟΓΡΑΦΗΣΗ

Η κρυπτογράφηση έρχεται να εξασφαλίσει το απόρρητο των προσωπικών πληροφοριών. Πρόκειται για μια επιστήμη που βασίζεται στα μαθηματικά για την κωδικοποίηση και αποκωδικοποίηση των δεδομένων. Οι μέθοδοι κρυπτογράφησης καθιστούν τα ευαίσθητα προσωπικά δεδομένα προσβάσιμα μόνο από όσους είναι κατάλληλα εξουσιοδοτημένοι. Εξασφαλίζουν έτσι το απόρρητο στις ψηφιακές επικοινωνίες αλλά και στην αποθήκευση ευαίσθητων πληροφοριών. Το αρχικό μήνυμα ονομάζεται απλό κείμενο (plaintext), ενώ το ακατάληπτο μήνυμα που προκύπτει από την κρυπτογράφηση του απλού κειμένου ονομάζεται κρυπτογράφημα (ciphertext).

Αποκρυπτογράφηση είναι η ανάκτηση του απλού κειμένου από το κρυπτογράφημα με την εφαρμογή αντίστροφου αλγορίθμου. Η κρυπτογραφημένη επικοινωνία είναι αποτελεσματική, όταν μόνο τα άτομα που συμμετέχουν σε αυτήν μπορούν να ανακτήσουν το περιεχόμενο του αρχικού μηνύματος. Η κρυπτογραφία δεν πρέπει να συγχέεται με την κρυπτανάλυση, που ορίζεται ως η επιστήμη για την ανάλυση και αποκωδικοποίηση κωδικοποιημένων πληροφοριών χωρίς τη χρήση του αντίστροφου αλγορίθμου κρυπτογράφησης.

Ο αλγόριθμος κρυπτογράφησης είναι μια μαθηματική συνάρτηση που χρησιμοποιείται για την κρυπτογράφηση και αποκρυπτογράφηση πληροφοριών. Όσο αυξάνεται ο βαθμός πολυπλοκότητας του αλγορίθμου, τόσο μειώνεται η πιθανότητα να τον προσπελάσει κάποιος. Ο αλγόριθμος κρυπτογράφησης λειτουργεί σε συνδυασμό με ένα κλειδί (key), για την κρυπτογράφηση του απλού κειμένου. Το ίδιο απλό κείμενο κωδικοποιείται σε διαφορετικά κρυπτογραφήματα όταν χρησιμοποιούνται διαφορετικά κλειδιά.

3.5.1 ΠΑΡΕΛΘΟΝ

Η κρυπτογράφηση δεν είναι νέα υπόθεση. Ακόμη και στην αρχαιότητα χρησιμοποιούνταν διάφορες μέθοδοι κρυπτογράφησης, με χαρακτηριστικότερη αυτή του Ιουλίου Καίσαρα, ο οποίος επινόησε έναν απλό αλγόριθμο για να επικοινωνεί με τους επιτελείς του, με μηνύματα που δεν θα ήταν δυνατόν να τα διαβάσουν οι εχθροί του. Ο αλγόριθμος βασιζόταν στην αντικατάσταση κάθε γράμματος του αλφαβήτου με κάποιο άλλο, όχι όμως τυχαία. Ο αλγόριθμος κρυπτογράφησης είναι η ολίσθηση των γραμμάτων του αλφαβήτου προς τα δεξιά. Κάθε γράμμα αντικαθίσταται από κάποιο άλλο με κάποιο κλειδί, πχ. το 3. Η κρυπτογράφηση δηλαδή του μηνύματος γίνεται με αντικατάσταση κάθε γράμματος από το γράμμα που βρίσκεται τρεις θέσεις δεξιότερα του στο αλφάβητο. Διατηρώντας τον ίδιο αλγόριθμο κρυπτογράφησης και επιλέγοντας διαφορετικό κλειδί, παράγονται διαφορετικά κρυπτογραφημένα μηνύματα.

Αν, για παράδειγμα, το απλό κείμενο είναι η λέξη secret, θα προκύψει το κρυπτογράφημα wigvix. Για να το αποκρυπτογραφήσει κάποιος θα πρέπει να αντιστρέψει τη διαδικασία κρυπτογράφησης, με άλλα λόγια να αντικαταστήσει κάθε γράμμα με αυτό που βρίσκεται τρεις θέσεις αριστερά στο αλφάβητο. Δεν αρκεί να γνωρίζει ότι ο κατάλληλος αλγόριθμος αποκρυπτογράφησης είναι η ολίσθηση των γραμμάτων του αλφαβήτου προς τα αριστερά, αλλά και πόσες θέσεις χρειάζεται να τα ολισθήσει. Πρέπει να γνωρίζει λοιπόν το κλειδί, που σε αυτή την περίπτωση είναι

ο αριθμός 3 Κρυπτογράφηση: Το Α και το Ω της δικτυακής ασφάλειας

3.5.2 ΤΟ ΜΕΛΛΟΝ:ΚΒΑΝΤΙΚΗ ΚΡΥΠΤΟΓΡΑΦΗΣΗ

Οι σημερινές τεχνολογίες κρυπτογράφησης, παρότι παρέχουν μεγάλο ποσοστό ασφάλειας, έχει αποδειχθεί ότι δεν είναι άτρωτες. Η απάντηση στο πρόβλημα

είναι η χρήση της κβαντικής Φυσικής, όπως υποστηρίζει ο Νικολά Ζισίν, πρωτοπόρος της συγκεκριμένης τεχνολογίας στο Πανεπιστήμιο της Γενεύης. Εν συντομία, το σκεπτικό έχει ως εξής: οποιαδήποτε προσπάθεια παρατήρησης ενός κβαντικού συστήματος αυτόματα προκαλεί την "αλλοίωσή" του. Κατ' αυτό τον τρόπο, ακόμη και η παραμικρή προσπάθεια υποκλοπής γίνεται αμέσως αντιληπτή. Η κβαντική κρυπτογράφηση βρίσκεται εδώ και μια δεκαετία στο στάδιο των εργαστηριακών δοκιμών, αλλά σύντομα αναμένεται να εφαρμοστεί και εμπορικά.

3.5.3 ΓΙΑΤΙ ΠΡΕΠΕΙ ΝΑ ΧΡΗΣΙΜΟΠΟΙΕΙΤΑΙ

Δεν είναι λίγοι αυτοί που πιστεύουν ότι η χρήση κρυπτογραφικών εργαλείων αφορά μόνο... κατασκόπους ή μανιώδεις χρήστες υπολογιστών. Στην πραγματικότητα, όταν κάποιος αποστέλλει ένα προσωπικό e-mail ή ανταλλάσσει εμπιστευτικές εμπορικές πληροφορίες για ένα έργο μέσω του ηλεκτρονικού ταχυδρομείου, οφείλει να γνωρίζει ότι, εάν δεν έχει κρυπτογραφηθεί, είναι σαν να το στέλνει με καρτ-ποστάλ: μπορεί να το διαβάσει σχεδόν οποιοσδήποτε.

Ένα e-mail, εκτός από τον αποστολέα και τον παραλήπτη, μπορεί να διαβαστεί εύκολα και από τους εργαζόμενους στον ISP (εταιρία παροχής Internet) του αποστολέα, τους εργαζόμενους στον ISP του παραλήπτη, από οποιονδήποτε ελέγχει τους routers από τους οποίους θα περάσουν τα "πακέτα" του μηνύματος και από οποιονδήποτε έχει πρόσβαση στον εξοπλισμό τηλεφωνίας στην τηλεφωνική εταιρία. Αν το μήνυμα αποστέλλεται ή παραλαμβάνεται από κινητό τηλέφωνο με σύνδεση στο Διαδίκτυο, τότε μπορεί να υποκλαπεί από άτομα με ειδικές συσκευές υποκλοπής συνομιλιών και μηνυμάτων κινητής τηλεφωνίας. Επιπλέον, είναι πολύ απλό να πλαστογραφηθεί η διεύθυνση αποστολής, ακόμα και με ένα τυπικό πρόγραμμα e-mail. Με λίγο περισσότερη δουλειά, κάποιος επιτήδειος μπορεί να αποκρύψει και άλλα σημάδια που δείχνουν από πού

πραγματικά προέρχεται ένα μήνυμα.

Λύση στα παραπάνω προβλήματα δίνουν οι τεχνολογίες κρυπτογράφησης. Οι τεχνολογίες αυτές εξασφαλίζουν ότι το μήνυμα θα μπορεί να το διαβάσει μόνο ο παραλήπτης του, καθώς στα ενδιάμεσα στάδια το μήνυμα εμφανίζεται με ακατάληπτους χαρακτήρες, είναι δηλαδή μη αναγνώσιμο. Εκτός από την κρυπτογράφηση, μια άλλη τεχνολογία που παρέχει τέτοιου είδους ασφάλεια είναι η ηλεκτρονική υπογραφή, τομέας με τον οποίο έχουμε ήδη ασχοληθεί. Αξίζει, πάντως, να σημειώσουμε ότι είναι δυνατόν ένα μήνυμα να κρυπτογραφηθεί και ταυτόχρονα να υπογραφεί ηλεκτρονικά. Έτσι εξασφαλίζονται εξίσου η ασφάλεια στην επικοινωνία και η πιστοποίηση περιεχομένου και ταυτότητας αποστολέα.

3.5.4 ΜΕΘΟΔΟΙ ΚΡΥΠΤΟΓΡΑΦΗΣΗΣ

- **Συμμετρική Κρυπτογράφηση**

Στη συμμετρική κρυπτογράφηση χρησιμοποιείται το ίδιο κλειδί για την κρυπτογράφηση και την αποκρυπτογράφηση. Το κλειδί αυτό θα πρέπει να είναι γνωστό μόνο στα εξουσιοδοτημένα μέρη και, κατά συνέπεια, απαιτείται κάποιο ασφαλές μέσο για τη μετάδοσή του, όπως μια προσωπική συνάντηση, κατά την οποία θα συμφωνηθεί το κλειδί που θα χρησιμοποιείται. Αν κάτι τέτοιο δεν είναι εφικτό, η συμμετρική κρυπτογραφία είναι αναποτελεσματική.

Υπάρχουν αρκετοί αλγόριθμοι που ανήκουν στην κατηγορία αυτή, με πιο γνωστό τον Data Encryption Standard (DES), ο οποίος αναπτύχθηκε αρχικά από την IBM και υιοθετήθηκε το 1977 από την κυβέρνηση των Ηνωμένων Πολιτειών ως το επίσημο πρότυπο κρυπτογράφησης απόρρητων πληροφοριών

Τα συστήματα συμμετρικής κρυπτογράφησης προϋποθέτουν την ύπαρξη ενός ασφαλούς καναλιού για την ανταλλαγή των μυστικών κλειδιών. Τέτοια συστήματα έχουν αναπτυχθεί και ήδη χρησιμοποιούνται, με πιο διαδεδομένο το σύστημα Kerberos, του MIT (Massachusetts Institute of Technology).

- **Ασύμμετρη Κρυπτογράφηση**

Στην ασύμμετρη κρυπτογράφηση, χρησιμοποιούνται διαφορετικά κλειδιά για την κρυπτογράφηση και την αποκρυπτογράφηση: το δημόσιο (public) και το ιδιωτικό (private) κλειδί αντίστοιχα. Τα κλειδιά αυτά δημιουργούνται με τρόπο ώστε να έχουν τις εξής ιδιότητες:

Μήνυμα κρυπτογραφημένο με το δημόσιο κλειδί μπορεί να αποκρυπτογραφηθεί μόνο με το ιδιωτικό κλειδί και αντίστροφα

Το ένα κλειδί δεν μπορεί να προκύψει από το άλλο με απλό τρόπο

Η βασική αυτή αρχή της κρυπτογραφίας δημόσιου κλειδιού διατυπώθηκε το 1976 από τους Diffie και Hellman, ενώ το 1977 οι Rivest, Shamir και Adleman, βασιζόμενοι σε αρχές της θεωρίας των πεπερασμένων πεδίων, δημιούργησαν το κρυπτοσύστημα RSA, την πρώτη υλοποίηση συστήματος κρυπτογραφίας δημόσιου κλειδιού.

Προκειμένου να επιτευχθεί η επικοινωνία με χρήση ασύμμετρης κρυπτογραφίας, ο κάθε χρήστης πρέπει να διαθέτει τα δικά του κλειδιά, ένα δημόσιο και ένα ιδιωτικό. Ο αποστολέας ενός μηνύματος πρέπει να γνωρίζει το δημόσιο κλειδί του παραλήπτη και να κρυπτογραφήσει το μήνυμα με αυτό. Ο παραλήπτης αποκρυπτογραφεί το μήνυμα με το ιδιωτικό του κλειδί

Το δημόσιο κλειδί δεν αποτελεί μυστική πληροφορία, συνεπώς μπορεί να μεταδοθεί χωρίς την απαίτηση ύπαρξης ασφαλούς μέσου. Το ιδιωτικό κλειδί χρησιμοποιείται μόνο από τον ιδιοκτήτη του και δεν μεταδίδεται ποτέ. Όταν ένα μήνυμα έχει κρυπτογραφηθεί με το δημόσιο κλειδί κάποιου χρήστη, μπορεί να αποκρυπτογραφηθεί μόνο με το ιδιωτικό του κλειδί. Και επειδή μόνο ο ίδιος ο χρήστης γνωρίζει το ιδιωτικό του κλειδί, μόνο αυτός μπορεί να αποκρυπτογραφήσει τα μηνύματα που απευθύνονται σε αυτόν. Ούτε καν το δημόσιο κλειδί που χρησιμοποιήθηκε για την κρυπτογράφηση δεν μπορεί να αποκωδικοποιήσει το μήνυμα, γι' αυτό και η γνώση του δημόσιου κλειδιού από τρίτους δεν αποτελεί πρόβλημα.

Η ασύμμετρη κρυπτογράφηση παρέχει μεγαλύτερη ασφάλεια από ό,τι η

συμμετρική. Έχει όμως το μειονέκτημα ότι οι αλγόριθμοι που χρησιμοποιεί είναι πολύ βραδύτεροι από τους αντίστοιχους της συμμετρικής.

Η Υποδομή Δημόσιου Κλειδιού (Public Key Infrastructure - PKI) αποτελεί ένα συνδυασμό λογισμικού, τεχνολογιών κρυπτογραφίας και υπηρεσιών, ο οποίος πιστοποιεί την εγκυρότητα του κάθε φυσικού προσώπου που εμπλέκεται σε μια συναλλαγή στο Διαδίκτυο, και παράλληλα προστατεύει την ασφάλεια της συναλλαγής.

Το PKI ενσωματώνει ψηφιακά πιστοποιητικά, κρυπτογραφία δημόσιου κλειδιού και αρχές πιστοποίησης σε ένα ασφαλές αρχιτεκτονικό σχήμα. Μια τυπική υλοποίηση του PKI περιλαμβάνει την παροχή ψηφιακών πιστοποιητικών σε χρήστες, εξυπηρετητές (servers) και λογισμικό χρηστών. Παράλληλα προσφέρει σειρά εργαλείων για τη διαχείριση, ανανέωση και ανάκληση των πιστοποιητικών.

Η υποδομή δημόσιου κλειδιού και η κρυπτογράφηση στην πράξη

Οι βασικές λειτουργίες/υπηρεσίες των Υποδομών Δημόσιου Κλειδιού είναι οι εξής:

Εμπιστευτικότητα (Confidentiality): Πρόκειται για την προστασία των δεδομένων ενάντια σε μη εξουσιοδοτημένη πρόσβαση ή γνωστοποίησή τους. Η υπηρεσία αυτή υλοποιείται μέσω μηχανισμών ελέγχου πρόσβασης στην περίπτωση αποθήκευσης δεδομένων και μέσω κωδικοποίησης κατά την αποστολή τους. Η Υποδομή Δημόσιου Κλειδιού παρέχει κωδικοποίηση, αφού οι μηχανισμοί ελέγχου πρόσβασης υλοποιούνται κατά βάση από το συνδυασμό μεθόδων πιστοποίησης (authentication) και εξουσιοδότησης (authorization).

Ακεραιότητα (Integrity): Είναι η προστασία των δεδομένων ενάντια σε μη εξουσιοδοτημένη τροποποίηση ή αντικατάστασή τους. Παρέχεται από μηχανισμούς κρυπτογραφίας όπως οι ηλεκτρονικές υπογραφές.

Μη Άρνηση Αποδοχής (Non-Repudiation): Η Μη Άρνηση Αποδοχής συνδυάζει τις υπηρεσίες της Πιστοποίησης και της Ακεραιότητας. Ο αποστολέας δεδομένων δεν μπορεί να αρνηθεί ότι δημιούργησε και απέστειλε το μήνυμα. Η

ασύμμετρη κρυπτογραφία παρέχει ηλεκτρονικές υπογραφές, κατά συνέπεια μόνο ο αποστολέας του μηνύματος θα μπορούσε να κατέχει τη συγκεκριμένη υπογραφή. Με αυτόν τον τρόπο, ο οποιοσδήποτε, και φυσικά ο παραλήπτης του μηνύματος, μπορεί να επιβεβαιώσει την ηλεκτρονική υπογραφή του αποστολέα.

Πιστοποίηση (Authentication): Πρόκειται για την επιβεβαίωση της ταυτότητας ενός ατόμου ή της πηγής αποστολής των πληροφοριών. Κάθε χρήστης που επιθυμεί να επιβεβαιώσει την ταυτότητα ενός άλλου προσώπου ή εξυπηρετητή με τον οποίο επικοινωνεί, βασίζεται στην πιστοποίηση. Οι παραδοσιακές μέθοδοι πιστοποίησης είναι οι εξής:

Με κάποιον κωδικό που γνωρίζουμε, όπως το PIN μιας τραπεζικής κάρτας ή το password ενός λογαριασμού

Με κάποιο αντικείμενο που έχουμε στην ιδιοκτησία μας, λόγου χάρη το κλειδί μιας πόρτας ή μια τραπεζική κάρτα

Με δακτυλικά αποτυπώματα, φωνή κλπ. Το πιστοποιητικό (certificate) είναι ο τρόπος με τον οποίο η Υποδομή Δημόσιου Κλειδιού μεταδίδει τις τιμές των δημόσιων κλειδιών ή πληροφορίες που σχετίζονται με αυτά, ή και τα δύο. Η εκδότρια αρχή των πιστοποιητικών ονομάζεται Αρχή Πιστοποίησης (Certificate Authority - CA). Οι Αρχές Πιστοποίησης διασφαλίζουν τη δημοσίευση και τη διανομή των δημόσιων κλειδιών και λαμβάνουν το δημόσιο κλειδί του ενδιαφερόμενου χρήστη. Εάν ο χρήστης ενεργεί στη συγκεκριμένη περίπτωση ως ιδιώτης, θα πρέπει να παραχωρήσει όλα τα απαραίτητα στοιχεία που αποδεικνύουν την ταυτότητά του. Σε αντίθετη περίπτωση, ο χρήστης θεωρείται ότι ενεργεί εκ μέρους κάποιας επιχείρησης, οπότε οφείλει να παραχωρήσει όλες τις νομικές πληροφορίες που απαιτούνται για την αξιοπιστία και τη νόμιμη λειτουργία της.

Ουσιαστικά ένα ψηφιακό πιστοποιητικό αποτελεί μια ψηφιακά υπογεγραμμένη δήλωση από μια αρχή πιστοποίησης, η οποία:

Προσδιορίζει την αρχή πιστοποίησης που το εξέδωσε

Περιέχει το όνομα και κάποιες άλλες πληροφορίες του εγγεγραμμένου

Περιέχει το δημόσιο κλειδί του εγγεγραμμένου, το οποίο είναι ψηφιακά υπογεγραμμένο από την αρχή πιστοποίησης που το εξέδωσε

Η υποδομή δημόσιου κλειδιού και η κρυπτογράφηση στην πράξη

Για την πιστοποίηση της ταυτότητας των συναλλασσομένων χρησιμοποιούνται τα πιστοποιητικά ασφαλείας, που επιπλέον εγγυώνται και την ασφάλεια ενός δικτυακού τόπου. Υπάρχουν δύο είδη πιστοποιητικών:

Τα προσωπικά πιστοποιητικά, τα οποία αποτελούν ένα είδος εγγύησης ότι ο χρήστης είναι αυτός που δηλώνει ότι είναι. Σε αυτά καταχωρούνται προσωπικές πληροφορίες, όπως όνομα χρήστη και κωδικός πρόσβασης. Στη συνέχεια, οι πληροφορίες αυτές αποθηκεύονται σε ένα πιστοποιητικό, το οποίο χρησιμοποιείται όταν στέλνονται προσωπικές πληροφορίες σε ένα διακομιστή ελέγχου ταυτότητας που απαιτεί πιστοποιητικό. Επίσης, ένα προσωπικό πιστοποιητικό επιτρέπει στο χρήστη να λαμβάνει κρυπτογραφημένα μηνύματα από τους υπόλοιπους χρήστες.

Α πιστοποιητικά δικτυακών τόπων, τα οποία περιέχουν πληροφορίες που πιστοποιούν ότι η συγκεκριμένη ιστοσελίδα είναι γνήσια και ασφαλής. Αυτό διασφαλίζει ότι κανένα άλλο site δεν μπορεί να παρουσιαστεί με την ταυτότητα της γνήσιας, ασφαλούς τοποθεσίας. Επίσης, τα πιστοποιητικά δικτυακών τόπων χρονολογούνται κατά την έκδοσή τους. Όταν προσπαθείτε να συνδεθείτε με το website ενός οργανισμού, το πρόγραμμα ανάγνωσης επαληθεύει τη διεύθυνση Internet που είναι αποθηκευμένη στο πιστοποιητικό και ελέγχει την ημερομηνία λήξης του. Εάν οι πληροφορίες αυτές δεν είναι έγκυρες ή εάν έχει παρέλθει η ημερομηνία λήξης, εμφανίζεται προειδοποιητικό μήνυμα (Warning).

Έχουν αναπτυχθεί ή βρίσκονται υπό κατασκευή διάφορα πρωτόκολλα ασφαλείας που κάνουν χρήση των παραπάνω τεχνικών, όπως το SSL (Secure Sockets Layer), της Netscape, και το SET (Secure Electronic Transactions), που αναπτύχθηκε από τη Visa και τη MasterCard. Από αυτά σήμερα χρησιμοποιείται το SSL. Αρκετές ιστοσελίδες είναι εξοπλισμένες με προγράμματα που χρησιμοποιούν το πρωτόκολλο αυτό, αποτρέποντας έτσι τα μη εξουσιοδοτημένα

πρόσωπα από την πρόσβασή τους σε δεδομένα που αποστέλλονται από και προς αυτές τις ιστοσελίδες. Τέτοια sites ονομάζονται "ασφαλή".

Οι πιο γνωστοί φυλλομετρητές ιστοσελίδων (browsers) υποστηρίζουν το πρωτόκολλο SSL και την κρυπτογράφηση που προσφέρει, ενώ ενημερώνουν το χρήστη ότι βρίσκεται σε ασφαλή τοποθεσία και μπορεί να στέλνει πληροφορίες ακίνδυνα. Με το πρωτόκολλο αυτό οι επικοινωνίες πραγματοποιούνται σε κωδικοποιημένη μορφή και επιπλέον γίνεται έλεγχος της αυθεντικότητας της ιστοσελίδας.

Η διαδικασία μιας ασφαλούς επικοινωνίας έχει ως εξής:

- Ο φυλλομετρητής συνδέεται με τον ασφαλή δικτυακό τόπο.
- Ο δικτυακός τόπος δηλώνει την ταυτότητά του, η οποία ελέγχεται με τα πιστοποιητικά που εκδίδονται από υπηρεσίες πιστοποίησης.
- Η ασφαλής ιστοσελίδα και ο browser συμφωνούν στη χρήση συγκεκριμένου κλειδιού/αλγορίθμου που χρησιμοποιείται για την κρυπτογράφηση της υπόλοιπης επικοινωνίας
- Τα δεδομένα που διακινούνται είναι κρυπτογραφημένα με το κλειδί/αλγόριθμο που συμφωνήθηκε στο προηγούμενο βήμα.
- Η κρυπτογράφηση γίνεται με χρήση αλγορίθμου 40bit ή 128bit. Εάν έχει χρησιμοποιηθεί κρυπτογράφηση 40bit, τότε για να αποκρυπτογραφήσει κανείς τα δεδομένα που ανταλλάχθηκαν, θα πρέπει να δοκιμάσει περίπου 240 διαφορετικά κλειδιά, ενώ, εάν έχει χρησιμοποιηθεί κρυπτογράφηση 128bit, τότε θα πρέπει να δοκιμάσει περίπου 2.128 διαφορετικά κλειδιά.

Η υποδομή δημόσιου κλειδιού και η κρυπτογράφηση στην πράξη έχει ως εξής:

Με τη χρήση μεγάλης υπολογιστικής ισχύος, η αποκρυπτογράφηση του κλειδιού των 40bit μπορεί να επιτευχθεί σε μερικές ημέρες, ενώ η αποκρυπτογράφηση του κλειδιού των 128bit, με τα σημερινά δεδομένα, είναι πρακτικά αδύνατη. Θα πρέπει να σημειωθεί ότι απαγορεύεται από τη νομοθεσία των ΗΠΑ η εξαγωγή και χρήση προγραμμάτων που υποστηρίζουν κωδικοποίηση 128bit εκτός των Ηνωμένων Πολιτειών και του Καναδά.

Στο πλαίσιο των προσπαθειών που καταβάλλονται για την ανάπτυξη των ηλεκτρονικών συναλλαγών, έχει επιτραπεί η χρήση της τεχνολογίας SGC (Server Gated Cryptography) ή International Step-Up Encryption, που αποτελεί επέκταση του πρωτοκόλλου SSL, από πιστωτικά ιδρύματα και άλλων χωρών. Η επέκταση αυτή επιτρέπει στα πιστωτικά ιδρύματα, εφόσον διαθέτουν το κατάλληλο πιστοποιητικό, να επικοινωνούν με τους πελάτες τους με κωδικοποίηση 128bit.

3.5.5 PGP (Pretty Good Privacy)

Στην αγορά κυκλοφορούν αρκετά προγράμματα λογισμικού κρυπτογράφησης. Είναι πολύ σημαντικό να γίνεται σωστή επιλογή του προϊόντος που θα χρησιμοποιηθεί. Υπάρχουν προγράμματα που είτε δεν χρησιμοποιούν αρκετά ασφαλείς αλγόριθμους είτε δημιουργούν σφάλματα (bugs) στην υλοποίηση της κρυπτογράφησης. Επίσης, θα πρέπει η τεχνική κρυπτογράφησης να ελέγχεται από ειδικούς, ενώ οι μέθοδοι πρέπει να είναι γνωστές και το λογισμικό που τις υλοποιεί υψηλής ποιότητας.

Για την κρυπτογράφηση ηλεκτρονικού ταχυδρομείου και αρχείων, δημοφιλέστερο πρόγραμμα είναι το PGP (Pretty Good Privacy). Οι αλγόριθμοι του PGP είναι γνωστοί και ασφαλείς. Ο πηγαίος κώδικάς του είναι διαθέσιμος στο κοινό, γεγονός που επέτρεψε σε ειδικούς επιστήμονες των κλάδων της πληροφορικής και της κρυπτογραφίας να το εξετάσουν και να αναζητήσουν σφάλματα ή "κερκόπορτες" (back doors). Χρησιμοποιείται εδώ και αρκετά χρόνια, και οι ειδικοί της κρυπτογραφίας το θεωρούν σε μεγάλο βαθμό αξιόπιστο.

Το PGP αποτελεί ένα κρυπτοσύστημα που δημιουργήθηκε από τον καθηγητή Philip Zimmerman του MIT και χρησιμοποιεί τους αλγόριθμους για την κρυπτογράφηση και υπογραφή μηνυμάτων ηλεκτρονικού ταχυδρομείου. Όταν κυκλοφόρησε για πρώτη φορά, η αμερικανική κυβέρνηση προσπάθησε να

απαγορεύσει τη διανομή του, με τη δικαιολογία ότι η υψηλής ποιότητας κρυπτογράφηση συμπεριλαμβάνεται στα... όπλα, και η κυβέρνηση έχει δικαίωμα να περιορίσει τη χρήση της.

Πρόκειται βέβαια για εμπορικό πρόγραμμα, μπορεί ωστόσο να χρησιμοποιηθεί χωρίς χρέωση για μη επαγγελματική χρήση. Επίσης υπάρχουν και εκδόσεις open source/free software (λογισμικό ανοιχτού/ελεύθερου κώδικα και δωρεάν διανομής), όπως το gnupgp. Το PGP ήταν αρχικά διαθέσιμο από την PGP Inc. Η εταιρία εξαγοράστηκε από τη Network Associates, η οποία ανέλαβε την εξέλιξη και τις αναβαθμίσεις του προγράμματος. Στις αρχές του 2002 η Network Associates ανακοίνωσε ότι θα σταματήσει την πώληση και υποστήριξη του PGP. Αργότερα, όμως, αποφασίσθηκε η επανασύσταση της PGP Corporation, η οποία αναπτύσσει τη νέα έκδοση (8.0) του προγράμματος και θα αναλάβει την υποστήριξή του.

Ο χρήστης προγραμμάτων τύπου PGP πρέπει αρχικά να δημιουργήσει ένα ζευγάρι κλειδιών (key pair), δημόσιο και ιδιωτικό. Παρέχει το δημόσιο κλειδί σε όλους τους παραλήπτες είτε με e-mail είτε δημοσιεύοντας το στο Internet. Το ιδιωτικό κλειδί παραμένει κρυφό, στο σταθμό εργασίας του χρήστη, και δεν θα πρέπει να διαρρεύσει, καθώς εξασφαλίζει την αποτελεσματικότητα της κρυπτογράφησης.

Η υποδομή δημόσιου κλειδιού και η κρυπτογράφηση στην πράξη

Ο αποστολέας κρυπτογραφεί το μήνυμα με το δημόσιο κλειδί. Αυτή είναι μια μονόδρομη διαδικασία: αφού κρυπτογραφηθεί το μήνυμα, δεν μπορεί να αποκρυπτογραφηθεί παρά μόνο με το ιδιωτικό κλειδί. Για το λόγο αυτό, είναι σημαντικό να μη διαρρεύσει. Επειδή και το ιδιωτικό και το δημόσιο κλειδί μπορεί να αποτελούν αρκετά μεγάλα σε όγκο αρχεία, το πρόγραμμα PGP αποθηκεύει το ιδιωτικό κλειδί στο δίσκο κρυπτογραφημένο. Κάθε φορά που ο χρήστης θέλει να το χρησιμοποιήσει, πρέπει να εισάγει την "passphrase", κωδικό που δεν αποθηκεύεται πουθενά αλλά έχει ο ίδιος απομνημονεύσει.

Κάθε χρήστης του PGP διατηρεί λίστα με τα δημόσια κλειδιά των χρηστών με

τους οποίους επικοινωνεί (keyring). Για την προστασία της λίστας, την υπογράφει ο ίδιος με το ιδιωτικό του κλειδί. Κάθε κλειδί που προστίθεται στη λίστα είναι δυνατόν να φέρει έναν από τους παρακάτω χαρακτηρισμούς:

Απολύτως Έμπιστο (Completely Trusted)

Μερικώς Έμπιστο (Marginally Trusted)

Μη Έμπιστο (Untrusted)

Άγνωστο (Unknown)

Πάντως, αν και το PGP είναι σε μεγάλο βαθμό αξιόπιστο για εφαρμογές απλής ταυτοποίησης που εκτελούνται από απλούς χρήστες, δεν θεωρείται κατάλληλο για εφαρμογές ηλεκτρονικού εμπορίου και για όσες απαιτούν ισχυρή ταυτοποίηση. Τα πιστοποιητικά του PGP δεν είναι επεκτάσιμα και περιέχουν μόνο μία διεύθυνση ηλεκτρονικής αλληλογραφίας, την τιμή ενός δημόσιου κλειδιού και ένα χαρακτηρισμό βαθμού εμπιστοσύνης.

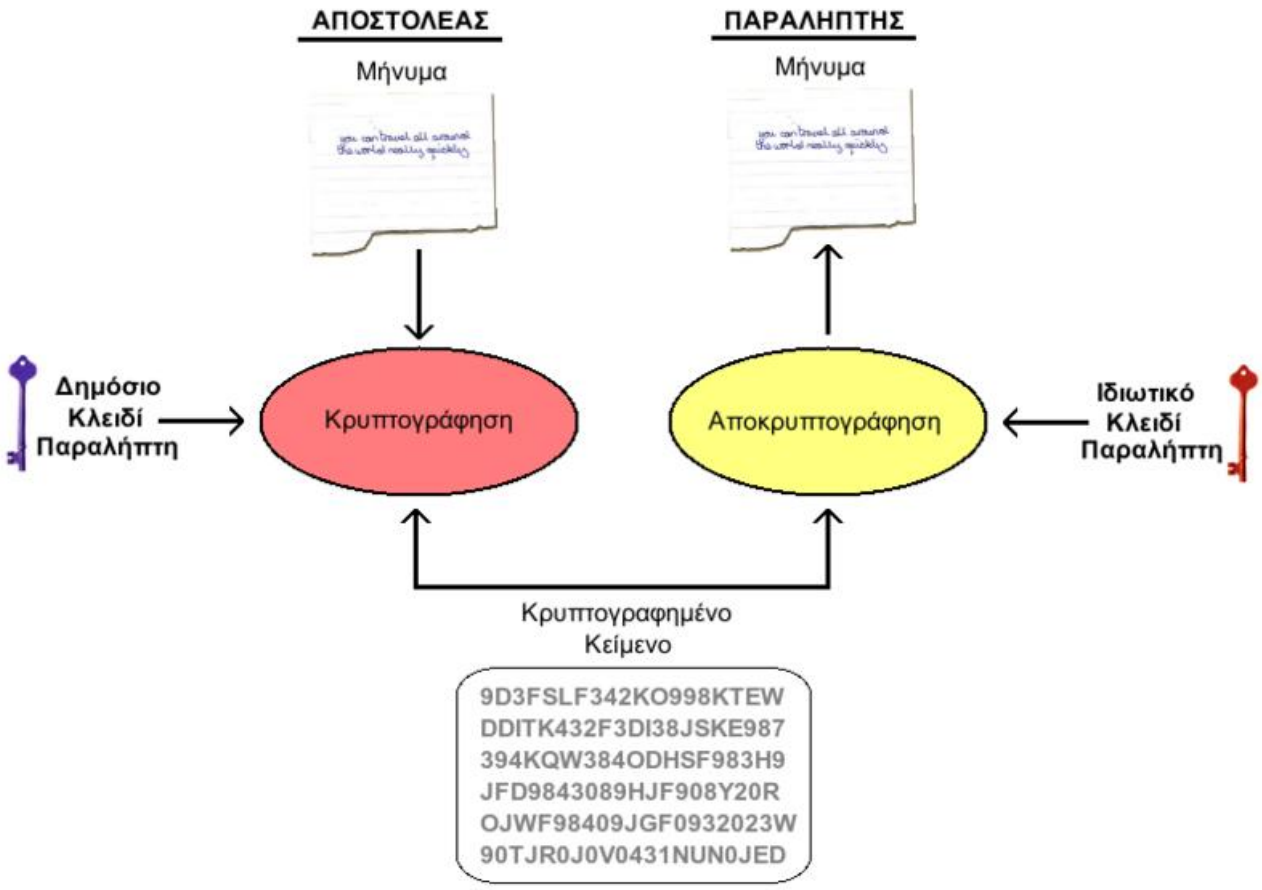
Καθώς η διεύθυνση ηλεκτρονικής αλληλογραφίας δεν μπορεί να αποτελέσει ασφαλές μέσο προσδιορισμού της ταυτότητας ενός χρήστη, το PGP δεν μπορεί να παράσχει ισχυρή ταυτοποίηση (strong authentication). Η έλλειψη επεκτασιμότητας των πιστοποιητικών του PGP τα καθιστά ακατάλληλα για άλλες εφαρμογές εκτός της ηλεκτρονικής αλληλογραφίας. Επίσης, το συγκεκριμένο πρόγραμμα δεν υποστηρίζει μεθόδους επαλήθευσης και ανάκλησης των πιστοποιητικών. Οι διαδικασίες αυτές διεξάγονται αποκλειστικά με άμεση επικοινωνία των χρηστών. Επιπλέον, δεν παρέχει την επιλογή της ανωνυμίας, καθώς η χρήση μιας διεύθυνσης e-mail που δεν περιέχει κάποια ένδειξη για την ταυτότητα του χρήστη καθιστά αδύνατη την επικοινωνία μεταξύ των χρηστών για την επαλήθευση και ανάκληση των πιστοποιητικών.

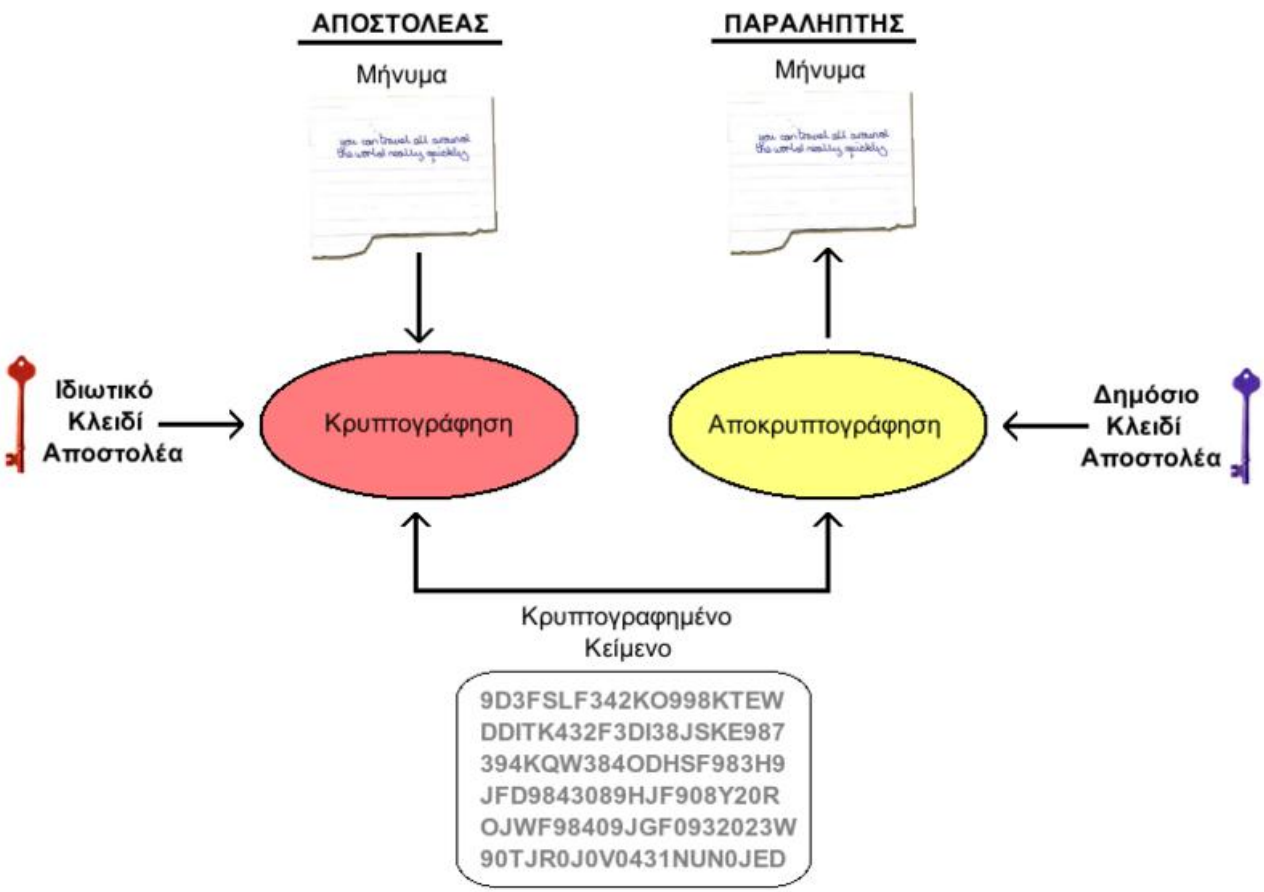
3.5.6 X.509

Το X.509 είναι ένα πρότυπο κρυπτογράφησης το οποίο σχεδιάστηκε για να παρέχει την υποδομή πιστοποίησης στις υπηρεσίες καταλόγου X.500 (LDAP).

Το πρωτόκολλο X.500 αποτελεί μια ιεραρχική μέθοδο οργάνωσης ευρετηρίων (καταλόγων), η οποία σχεδιάστηκε από το Διεθνή Οργανισμό Τυποποίησης (International Standards Organization - ISO) και ενσωματώθηκε στο διαδικτυακό πρωτόκολλο LDAP (Lightweight Directory Access Protocol).

Η πρώτη έκδοση του X.509 δημοσιεύθηκε το 1988, καθιστώντας το την παλαιότερη πρόταση για μια παγκόσμια Υποδομή Δημόσιου Κλειδιού. Το γεγονός αυτό, σε συνδυασμό με την υποστήριξη του προτύπου από τον ISO και τη Διεθνή Ένωση Τηλεπικοινωνιών (International Telecommunications Union - ITU), έχουν οδηγήσει στην υιοθέτηση του X.509 από μεγάλο αριθμό οργανισμών και κατασκευαστών. Αρκετά χρηματοπιστωτικά ιδρύματα χρησιμοποιούν το X.509 για το πρότυπο ασφαλών συναλλαγών SET (Secure Electronic Transactions). Χρησιμοποιείται επίσης σε φυλλομετρητές ιστοσελίδων (browsers), εξυπηρετητές (servers).


ΑΠΟΣΤΟΛΕΑΣ
Μήνυμα
ΠΑΡΑΛΗΠΤΗΣ
Μήνυμα
Δημόσιο Κλειδί Παραλήπτη
Κρυπτογράφηση
Αποκρυπτογράφηση
Ιδιωτικό Κλειδί Παραλήπτη
Κρυπτογραφημένο Κείμενο
9D3FSLF342KO998KTEW
DDITK432F3DI38JSKE987
394KQW384ODHSF983H9
JFD9843089HJF908Y20R
OJWF98409JGF0932023W
90TJR0J0V0431NUN0JED


ΑΠΟΣΤΟΛΕΑΣ
Μήνυμα
ΠΑΡΑΛΗΠΤΗΣ
Μήνυμα
Ιδιωτικό Κλειδί Αποστολέα
Κρυπτογράφηση
Αποκρυπτογράφηση
Δημόσιο Κλειδί Αποστολέα
Κρυπτογραφημένο Κείμενο
9D3FSLF342KO998KTEW
DDITK432F3DI38JSKE987
394KQW384ODHSF983H9
JFD9843089HJF908Y20R
OJWF98409JGF0932023W
90TJR0J0V0431NUN0JED

3.6 ΑΝΑΤΡΟΠΗ ΕΠΙΘΕΣΕΩΝ SNIFFERS

Η ανατροπή τών sniffers δεν είναι εύκολη. Μπορείτε να ακολουθήσετε δύο προσεγγίσεις:

- Ανίχνευση και εξάλειψη sniffers.
- Απομόνωση των δεδομένων σας από τα sniffers.

Ας εξετάσουμε εν συντομία τα υπέρ και τα κατά κάθε μεθόδου.

3.6.1 ΑΝΙΧΝΕΥΣΗ ΚΑΙ ΕΞΑΛΕΙΨΗ ΤΩΝ SNIFFERS

Τα sniffers είναι εξαιρετικά δύσκολο να εντοπιστούν επειδή είναι παθητικά προγράμματα. Δεν δημιουργούν ένα ίχνος εξέτασης, και καταναλώνουν ελάχιστους πόρους δικτύου. Μερικά λειτουργικά συστήματα παρέχουν ένα μηχανισμό για να καθορίζεται αν μια κάρτα δικτύου έχει τεθεί σε κατάσταση αδιακρισίας, και αυτό μπορεί να βοηθήσει σημαντικά να καθορίσετε αν εκτελείται ένα sniffer σε ένα συγκεκριμένο κόμβο.

Σε μία μόνο μηχανή είναι θεωρητικά εφικτό να βρείτε εάν ένα sniffer έχει εγκατασταθεί. Για παράδειγμα θα μπορούσατε να βασιστείτε στον αλγόριθμο MD5, με τη προϋπόθεση ότι έχετε μια ικανοποιητική βάση δεδομένων των αρχικών αρχείων εγκατάστασης. Εάν προτίθεστε να χρησιμοποιήσετε των MD5 και να ψάξετε με βάση το check-sum, θα πρέπει να πάρετε το md5check,ένα script της awk που αυτοματοποιεί τη διαδικασία. Το md5check διανεμήθηκε αρχικά από την CERT και λειτουργεί καλά σε SunOS.

Σαφώς, η αναζήτηση ανά checksum σε ένα μόνο σύστημα είναι αρκετά αποτελεσματική. Ωστόσο, η εύρεση ενός sniffer σε ένα μεγάλο δίκτυο είναι δύσκολη. Το θέμα του εντοπισμού sniffers σε διαφορετικές αρχιτεκτονικές αποτελεί μια έντονη διαμάχη στην κοινότητα των ασχολούμενων με την ασφάλεια. Όμως, υπάρχουν τουλάχιστον τέσσερα εργαλεία που μπορούν να βοηθήσουν αν έχετε την κατάλληλη αρχιτεκτονική:

- **Snifftest**. Γραμμένο από τους “Beavis and Butthead”, το Snifftest θα εντοπίζει ένα sniffer σε SunOS και Solaris. Είναι ιδιαιτέρως χρήσιμο επειδή θα εντοπίζει ένα sniffer ακόμη και αν η κάρτα δικτύου δεν είναι σε κατάσταση αδιακρισίας. Λειτουργεί μόνο για SunOS και απαιτεί έναν μεταγλωττιστή C και όλα τα αρχεία επικεφαλίδων TCP/IP.
- **Nitwit**. Το nitwit εκτελεί ένα NIT (Network Interface Tap) και μπορεί να εντοπίζει sniffers, ακόμη και αν η κάρτα δικτύου δεν είναι σε κατάσταση αδιακρισίας. Είναι όμοιο με το Snifftest από αυτή την άποψη.
- **Promisc**. Το promisc θα εντοπίζει sniffers στο Linux.
- **Cpm.** Το cpm είναι ένα παλιό πρόγραμμα που εντοπίζει την κατάσταση σε SunOS 4.x.

Δυστυχώς αυτά τα εργαλεία λειτουργούν μόνο σε SunOS ή Solaris. Ο εντοπισμός ενός sniffer σε ετερογενή δίκτυα είναι πιο δύσκολος. Για παράδειγμα υποθέστε ότι το δίκτυο σας απαρτίζεται αποκλειστικά από συστήματα AIX. Υποθέστε ακόμη ότι κάποιος πηγαίνει σε ένα άδειο γραφείο αποσυνδέει ένα RS/6000 και συνδέει ένα φορητό υπολογιστή .Το χρησιμοποιεί αυτό ως sniffer. Αυτό είναι δύσκολο να εντοπιστεί, εκτός αν χρησιμοποιείτε χάρτες τοπολογίας δικτύου (εργαλεία που σημειώνουν με κόκκινο οποιαδήποτε αλλαγή στη τοπολογία) και τους ελέγχετε καθημερινά .Διαφορετικά το δίκτυο εμφανίζεται όπως ήταν, χωρίς ενδείξεις του προβλήματος. Τέλος πάντων, το PC έχει την ίδια διεύθυνση IP που είχε το PC, εκτός αν διεξάγετε καθημερινούς ελέγχους.

Ένα πιο πρόσφατο εργαλείο που έχει αναπτυχθεί από την ομάδα L0pht των “grey-hat” hackers, ονομάζεται AntiSniff. Το AntiSniff δίνει στους διαχειριστές δικτύων την δυνατότητα να εντοπίζουν από μακριά τους υπολογιστές που εκτελούν sniffing πακέτων, ανεξάρτητα από το λειτουργικό σύστημα. Σύμφωνα με τους προγραμματιστές, το AntiSniff λειτουργεί εκτελώντας διαφόρους μη παρεισφηκτικούς ελέγχους, σχεδιασμένους να καθορίζουν αν ένας απομακρυσμένος υπολογιστής παρακολουθεί όλες τις επικοινωνίες δικτύου ή

όχι.

Μια πολυπλοκότερη κατάσταση λαμβάνει χώρα όταν εισβολείς επιτίθενται στις φυσικές συσκευές που υποκλέπτουν. Εκτός από το φυσικό έλεγχο κάθε καλωδίου που περνά από το δίκτυο, δεν υπάρχει εύκολος τρόπος προσδιορισμού μιας τέτοιας σύνδεσης.(Και πάλι, τα εργαλεία απεικόνισης της τοπολογίας δικτύου θα μπορούσαν να προειδοποιήσουν ότι έχει προστεθεί μια ακόμη διεύθυνση IP στο υποδίκτυο σας. Δυστυχώς, όμως, οι περισσότερες μικρές επιχειρήσεις δεν χρησιμοποιούν τέτοια εργαλεία.)

Εν πάση περιπτώσει, όμως ,οι προνοητικές λύσεις είναι δύσκολες και ακριβές. Θα μπορούσατε να πάρετε περισσότερο αμυντικά μέτρα. Υπάρχουν δύο βασικές άμυνες εναντίον των sniffers:

- Ασφαλής τοπολογία
- Κρυπτογραφημένες συνεδρίες

Ας καλύψουμε εν συντομία και τους δύο τρόπους άμυνας.

3.6.2 ΑΣΦΑΛΗΣ ΤΟΠΟΛΟΓΙΑ

Τα sniffers μπορούν να συλλέγουν μόνο δεδομένα στο στιγμιαίο τμήμα δικτύου. Αυτό σημαίνει οτι όσο πιο σφικτά χωρίζετε σε τμήματα το δίκτυο σας, τόσο λιγότερες πληροφορίες θα μπορεί να συλλέξει ένα sniffer. Δυστυχώς, αυτή η λύση μπορεί να είναι ακριβή ή έχετε απεριόριστους πόρους. Ο διαχωρισμός σε τμήματα απαιτεί ακριβό εξοπλισμό. Υπάρχουν τρεις τύποι συσκευών δικτύου που δεν μπορεί να παρακάμψει εύκολα ένα sniffer:

- Switches
- Routers
- Bridges

Μπορείτε να δημιουργήσετε πιο αυστηρά τμήματα δικτύου τοποθετώντας στρατηγικά αυτές τις συσκευές στο δίκτυο σας. Θα μπορούσατε πιθανόν να χωρίσετε ένα τμήμα 20 σταθμών εργασίας. Μια φορά το μήνα στη συνέχεια, θα μπορούσατε να ελέγχετε φυσικά κάθε τμήμα (και ,ίσως μια φορά τον μήνα, θα

μπορούσατε να εκτελείτε ελέγχους MD5 σε τυχαία τμήματα).Θα πρέπει να σημειωθεί ότι προγράμματα όπως το macof έχουν αναπτυχθεί για να πλημμυρίζουν τα switches με την ελπίδα ότι θα αποτύχουν μένοντας ανοικτά. Αυτό θα εξαφάνιζε την προστασία που μπορεί να παρέχει διαφορετικά η διαδικασία switching.

Η κατάτμηση του δικτύου είναι πρακτική μόνο σε μικρότερα δίκτυα. Εάν έχετε περισσότερους από 500 σταθμούς εργασίας, διαμοιρασμένους σε περισσότερα από 50 οργανικά τμήματα, η κατάτμηση σε πλήρη κλίμακα ενδεχομένως να έχει απαγορευτικό κόστος. (Ακόμη και αν υπάρχει ένας προϋπολογισμός για την ασφάλεια, μάλλον δε θα πείσετε τους διαχειριστές ότι χρειάζεστε 50 συσκευές, απλώς και μόνο για να ασφαλιστείτε εναντίον ενός sniffer). Σε αυτή την περίπτωση, οι κρυπτογραφημένες συνεδρίες είναι η καλύτερη επιλογή.

3.6.3 ΚΡΥΠΤΟΓΡΑΦΗΜΕΝΕΣ ΣΥΝΕΔΡΙΕΣ

Οι κρυπτογραφημένες συνεδρίες παρέχουν μια διαφορετική λύση. Αντί να ανησυχείτε για τα δεδομένα που θα υποστούν επιθέσεις sniffers, απλώς μπερδεύετε το τμήμα των δεδομένων του πακέτου, πέραν της αναγνώρισης. Τα πλεονεκτήματα αυτής της προσέγγισης είναι προφανή: Ακόμη κι αν ένας επιτιθέμενος υποκλέπτει δεδομένα, θα του είναι άχρηστα. Ωστόσο, τα μειονεκτήματα είναι σημαντικά.

Υπάρχουν δύο κύρια προβλήματα με την κρυπτογράφηση. Το ένα είναι τεχνικό, και το άλλο ανθρώπινο.

Το τεχνικό θέμα είναι αν η κρυπτογράφηση είναι αρκετά ισχυρή και αν υποστηρίζεται. Για παράδειγμα, η κρυπτογράφηση 40-bit μπορεί να είναι ανεπαρκής, και δεν έχουν όλες οι εφαρμογές ενσωματωμένη υποστήριξη κρυπτογράφησης. Επιπλέον, οι λύσεις κρυπτογράφησης πολλαπλών πλατφορμών είναι σπάνιες και τυπικά διαθέσιμες μόνο σε εξειδικευμένες εφαρμογές.

Επιπλέον, οι χρήστες μπορεί να αντισταθούν στην χρήση κρυπτογράφησης.

Μπορεί να βρουν πολύ ενοχλητική διαδικασία. (Για παράδειγμα, μπορείτε να φανταστείτε ότι θα εξαναγκάσετε χρήστες Machintosh να χρησιμοποιούν το S/Key κάθε φορά που συνδέονται στον server. Αυτοί οι χρήστες είναι συνηθισμένοι στην εύκολη χρήση, και όχι στην δημιουργία κωδικών πρόσβασης μιας χρήσης για κάθε νέα συνεδρία). Οι χρήστες μπορεί αρχικά να συμφωνήσουν σε τέτοιες πολιτικές, αλλά σπανίως εμμένουν σε αυτές.

Εν συντομία ,πρέπει να βρείτε ένα χαρούμενο μέσο, εφαρμογές που υποστηρίζουν ισχυρή, αμφίδρομη κρυπτογράφηση και επίσης είναι σε κάποιο επίπεδο φιλικές στο χρήστη.

ΚΕΦΑΛΑΙΟ 4 – ΝΟΜΙΚΑ ΘΕΜΑΤΑ

4.1 ΔΙΑΔΙΚΤΥΟ ΚΑΙ ΔΙΚΑΙΟ

Η προσέγγιση των νομικών θεμάτων που αφορούν τον Κυβερνοχώρο ενέχει την δυσκολία ότι, προϋποθέτει όχι μόνο νομικές, αλλά μέχρι ένα βαθμό τουλάχιστον και τεχνικές γνώσεις σε θέματα ηλεκτρονικών υπολογιστών (computers) και διαδικτύου (internet) . Είναι πολύ δύσκολο να αντιληφθεί κάποιος τα συμβαίνοντα στον πεδίο του εγκλήματος στον κυβερνοχώρο (cyber crime), όπως άλλωστε συμβαίνει και στα εγκλήματα με ηλεκτρονικούς υπολογιστές (computer crimes) χωρίς την κατοχή αυτών των τεχνικών γνώσεων . Οι τεχνικές όμως γνώσεις δεν επαρκούν για την κατανόηση της νομικής διάστασης του θέματος. Αυτό σε πρακτικό επίπεδο σημαίνει ότι, ο νομικός πρέπει να διαθέτει τεχνικές γνώσεις, ο δε τεχνικός πρέπει να κατέχει τουλάχιστον βασικές νομικές γνώσεις. Ο συνδυασμός των δύο βασικών, αλλά και διαφορετικών τρόπων σκέψεως αποτελεί "τον σταυρό του μαρτυρίου" για την κατανόηση του θέματος, δηλαδή του εγκλήματος στο διαδίκτυο και της αντιμετώπισής του.

Ένα εξ ίσου σημαντικό πρόβλημα που αντιμετωπίζει αυτός που ασχολείται με την νομική πλευρά του θέματος από ποινική άποψη, είναι η έλλειψη επαρκούς βιβλιογραφίας και σχετικών άρθρων. Είναι ευνόητο ότι, η έλλειψη αυτή οφείλεται στο γεγονός ότι, το έγκλημα στον κυβερνοχώρο αποτελεί νέα μορφή εγκλήματος. Αποτελεί κοινή διαπίστωση ότι, η ανάπτυξη των σχετικών νομικών θεμάτων από αστική και εμπορική άποψη έχει διερευνηθεί σε μεγαλύτερη έκταση, από ότι η αντίστοιχη ποινική πλευρά. Αυτό οφείλεται στην μεγάλη επιρροή του κυβερνοχώρου, τόσο στο αστικό (σύναψη συμβάσεων εξ αποστάσεως δια του κυβερνοχώρου κλπ), όσο και στον οικονομικό τομέα (ηλεκτρονικό εμπόριο, νέα οικονομία κλπ).

Σε κάθε περίπτωση όμως ο μελετητής των σχετικών με τον κυβερνοχώρο θεμάτων θα πρέπει να καταφεύγει στα διάφορα (πολυπληθή) τεχνικά περιοδικά

για τους ηλεκτρονικούς υπολογιστές, καθώς και σε δημοσιεύματα του ημερήσιου Τύπου. Άλλωστε και το ίδιο το διαδίκτυο αποτελεί πηγή αντλήσεως πληροφοριών (ίσως την σημαντικότερη), ανατρέχοντας στις ειδικές τοποθεσίες - θέσεις (Sites).

4.1.1 ΤΟ ΓΕΝΙΚΟΤΕΡΟ ΠΡΟΒΛΗΜΑ ΤΗΣ ΝΟΜΙΚΗΣ ΟΡΟΛΟΓΙΑΣ

Πρέπει ιδιαιτέρως να τονιστεί ότι, η διαφορετική κατανόηση - αντίληψη των ίδιων εννοιών από τον τεχνικό και νομικό αποτελεί ένα από τα σημαντικότερα προβλήματα του υπό εξέταση θέματος. Έτσι, π.χ. διαφορετικά αντιλαμβάνεται την έννοια του όρου "κυβερνοχώρος", "ασφάλεια", "χάκερ" κλπ ο τεχνικός και διαφορετικά ο νομικός. Για τη νομική επιστήμη οι έννοιες έχουν το περιεχόμενο που ρητώς τους προσδίδει ο νόμος. Σε περίπτωση δε, που δεν υπάρχει σχετικός νόμος, ανατρέχει ο νομικός στη νομολογία, δηλαδή, στις υπάρχουσες δικαστικές αποφάσεις. Για την ύπαρξη όμως σχετικής νομολογίας, είναι απαραίτητο να έχει "φθάσει" η υπόθεση ή άλλη παρόμοια στο δικαστήριο. Σε περίπτωση που, ούτε νομολογία υπάρχει, ο νομικός ανατρέχει στη νομική επιστήμη, προς αναζήτηση θεωρητικής τουλάχιστον λύσης του θέματος. Αυτό βέβαια δεν σημαίνει ότι, η νομική θεωρία, όπως αυτή έχει αναπτυχθεί ή αναπτύσσεται από τη (νομική) επιστήμη, γίνεται υποχρεωτικώς δεκτή στην νομική πρακτική, δηλαδή στην διερεύνηση ή την εκδίκαση των σχετικών εγκλημάτων.

4.1.2 ΤΟ ΠΡΟΒΛΗΜΑ ΤΗΣ ΕΛΛΗΝΙΚΗΣ ΝΟΜΙΚΗΣ ΟΡΟΛΟΓΙΑΣ

Τόσο η τεχνική όσο και η νομική ορολογία στο συγκεκριμένο θέμα είναι διατυπωμένη - κατά κανόνα - στην Αγγλική γλώσσα. Η αντίστοιχη μεταφορά των όρων αυτών στα Ελληνικά, δεν είναι ούτε εύκολη, ούτε δόκιμη. Βέβαια κατά την καθημερινή πρακτική πολλοί όροι χρησιμοποιούνται στην ξενόγλωσση διάστασή των, κατά τρόπο που τείνουν να ενσωματωθούν και στο Ελληνικό νομικό λεξιλόγιο. Έτσι π. χ. αντί του Ελληνικού όρου "διαδικτυακό 'έγκλημα" ή "έγκλημα στο διαδίκτυο" ή ``έγκλημα στον κυβερνοχώρο`` πολλές

φορές χρησιμοποιείται αυτούσιος ο όρος Cyber crime ή Internet crime . Σχετικοί με το θέμα ξενόγλωσσοι όροι είναι: Cyber crime, Internet, crime, Crime in cyberspace, On line crime, On line computer crime, communication crime, digital crime, electronic crime, electronic evidence, Computer crimes (υπολογιστικά εγκλήματα), Computer related crime. Σχετικοί με τον δράστη όροι είναι: hacker, Cracker, Internet freak, Cyber crook, Cyber freak, Internet freak.

4.1.3 Η ΝΟΜΙΚΗ ΕΝΝΟΙΑ ΤΟΥ ΔΙΑΔΙΚΤΥΟΥ ΚΑΙ ΤΟΥ ΚΥΒΕΡΝΟΧΩΡΟΥ

Η Ελληνική νομοθεσία δεν προσδιορίζει την έννοια του διαδικτύου ή του κυβερνοχώρου. Κατά συνέπεια οι έννοιες αυτές λαμβάνονται από την τεχνολογία. Έτσι λοιπόν, ως διαδίκτυο (internet) μπορεί να οριστεί η παγκόσμια συλλογή δικτύων και πυλών, που χρησιμοποιούν την ομάδα πρωτοκόλλων TCP/IP για να επικοινωνούν μεταξύ των , ενώ ως κυβερνοχώρος μπορεί να οριστεί το σύνολο των ηλεκτρονικών κόσμων, όπως το internet, όπου οι άνθρωποι έρχονται σε αλληλεπίδραση μέσω συνδεδεμένων υπολογιστών, όπου δηλαδή η επικοινωνία είναι ανεξάρτητη από την υλική υπόσταση . Στο άρθρο 2 του Ν 2867/19-12-2000 για την οργάνωση και λειτουργία τηλεπικοινωνιών προσδιορίζονται οι έννοιες "δίκτυο καλωδιακής τηλεόρασης", "ιδιωτικό δίκτυο", "παροχή ανοικτού δικτύου" και "τηλεπικοινωνιακό δίκτυο". Δεν προσδιορίζεται όμως η έννοια του διαδικτύου ή του κυβερνοχώρου.

Πρέπει να λεχθεί ότι, στη συνείδηση του μέσου νομικού, δεν γίνεται διάκριση μεταξύ διαδικτύου και κυβερνοχώρου και κατά κανόνα οι έννοιες αυτές θεωρούνται ως ταυτόσημες και χρησιμοποιούνται πάντα με το ίδιο περιεχόμενο.

4.1.4 ΠΡΟΣΔΙΟΡΙΣΜΟΣ ΤΗΣ ΕΝΝΟΙΑΣ ΤΟΥ ΕΓΚΛΗΜΑΤΟΣ ΣΤΟ ΚΥΒΕΡΝΟΧΩΡΟ

Δεν υπάρχει ακόμα γενικά αποδεκτός ορισμός του εγκλήματος στον κυβερνοχώρο, ούτε στην διεθνή νομοθεσία, ούτε στην διεθνή νομολογία ή βιβλιογραφία . Ομοίως ούτε στην Ελληνική βιβλιογραφία υπάρχει ορισμός του εγκλήματος στον κυβερνοχώρο.

Η άποψη ότι το έγκλημα στον κυβερνοχώρο (cyber crime) αποτελεί τον ίδιο τύπο εγκλήματος με το ``κοινό`` ή "συμβατικό έγκλημα" και η μόνη διαφορά που το διακρίνει απ΄ αυτό είναι ότι, διαπράττεται σε διαφορετικό περιβάλλον , (δηλ. σε ηλεκτρονικό περιβάλλον και δη σε περιβάλλον διαδικτύου) δεν ανταποκρίνεται πλήρως στην πραγματικότητα. Υπάρχουν βέβαια εγκλήματα, που διαπράττονται τόσο σε κοινό, όσο και σε ηλεκτρονικό περιβάλλον. Άλλα εγκλήματα διαπράττονται μόνο σε περιβάλλον ηλεκτρονικών υπολογιστών, χωρίς δηλαδή να υπάρχει σύνδεση των υπολογιστών με το διαδίκτυο (ή ακόμα και εάν υπάρχει δεν χρησιμοποιείται). Μια άλλη κατηγορία ηλεκτρονικών εγκλημάτων διαπράττονται αποκλειστικώς σε περιβάλλον του κυβερνοχώρου. Με το παραπάνω λοιπόν κριτήριο τα σχετικά (ηλεκτρονικά) εγκλήματα μπορούν να διακριθούν:

- Σε εγκλήματα που διαπράττονται τόσο σε " κοινό " περιβάλλον, όσο και στο διαδίκτυο (internet) π.χ. η συκοφαντική δυσφήμηση διαπράττεται και με την χρήση του ηλεκτρονικού ταχυδρομείου (αποστολή e-mail). Η αντιγραφή ενός πνευματικού έργου π.χ. μουσικού τραγουδιού (άρθρ. 66 Ν.2121/93) ή ενός προγράμματος ηλεκτρονικού υπολογιστή. Όταν το έγκλημα αυτό τελεστεί σε "περιβάλλον internet" (εννοείται βέβαια ότι απαιτείται και η χρήση computer) τότε πρόκειται για έγκλημα σχετιζόμενο με τον κυβερνοχώρο ή για έγκλημα που διαπράττεται στον κυβερνοχώρο ή για έγκλημα που διαπράττεται με την βοήθεια του κυβερνοχώρου (internet related crime).

- Σε εγκλήματα που διαπράττονται μόνο σε περιβάλλον ηλεκτρονικών υπολογιστών (ενν. χωρίς την χρήση του διαδικτύου). Τέτοια είναι τα εγκλήματα που προβλέπονται από το άρθρο 370 Γ παραγρ. 1 του Π.Κ. π.χ. η χωρίς δικαίωμα αντιγραφή προγράμματος από δισκέτα ή CD-ROM ή σε ηλεκτρονικό υπολογιστή.

Σε "Γνήσια εγκλήματα κυβερνοχώρου" (Cyber crimes) με την έννοια της ποινικοποίησης συμπεριφοράς που αποκλειστικώς έχει σχέση με τον κυβερνοχώρο. Μια τέτοια αξιόποινη συμπεριφορά μπορεί να θεωρηθεί η παράνομη ή χωρίς δικαίωμα πρόσβαση σε ηλεκτρονικό υπολογιστή (hacking) ή η διάδοση παιδικού πορνογραφικού υλικού δια του κυβερνοχώρου. Τέτοια εγκλήματα δεν υπάρχουν ακόμα στην Ελληνική έννομη τάξη, αφού δεν υπάρχει σχετική νομοθεσία. Δηλαδή τα γνήσια εγκλήματα του κυβερνοχώρου διαπράττονται αποκλειστικώς σε περιβάλλον διαδικτύου. Σε περίπτωση που ο υπολογιστής δεν είναι συνδεδεμένος με το διαδίκτυο, αλλά ενεργεί αυτοτελώς, οποιοδήποτε έγκλημα και εάν διαπραχθεί θεωρείται έγκλημα που διαπράττεται με ηλεκτρονικό υπολογιστή (computer crime).

4.1.5 Η ΝΟΜΙΚΗ ΕΝΝΟΙΑ ΤΗΣ ΑΣΦΑΛΕΙΑΣ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

Για τον νομικό, κάθε έννοια έχει το περιεχόμενο εκείνο, που με ακρίβεια καθορίζει ο νόμος για το συγκεκριμένο θέμα. Το ίδιο συμβαίνει βέβαια και με την έννοια της ασφάλειας. Άρα για το νομικό ασφάλεια στο διαδίκτυο σημαίνει αυτό που ο νόμος ορίζει ως ασφάλεια στο διαδίκτυο. Ο νόμος επίσης καθορίζει και το περιεχόμενο όλων εκείνων των επιμέρους εννοιών που αναφέρονται στον βασικό ορισμό της ασφάλειας. Έτσι αν π.χ. ο νομοθέτης ορίσει ως ασφάλεια στο διαδίκτυο "τον κίνδυνο να επέλθει κάποια βλάβη", θα πρέπει να ορίσει ταυτόχρονα και τους όρους "κίνδυνο" και "βλάβη".

Για το συγκεκριμένο θέμα, της ασφάλειας του διαδικτύου, ή της ασφάλειας στο διαδίκτυο η Ελληνική νομοθεσία δεν έχει δώσει ακόμα ορισμό.

Βέβαια, η έννοια της ασφάλειας δεν είναι άγνωστη στο ποινικό δίκαιο. Έτσι, στο 14ο κεφάλαιο του ποινικού Κώδικα και στα άρθρα 290 επόμενα, ο ποινικός νομοθέτης με συγκεκριμένες διατάξεις προσδιορίζει τα εγκλήματα κατά της ασφάλειας των συγκοινωνιών και κατά των κοινωφελών εγκαταστάσεων. Επίσης στο άρθρο 388 Π.Κ. που ρυθμίζει την απάτη την σχετική με τις ασφάλειες, η έννοια της ασφάλειας λαμβάνεται από το ασφαλιστικό δίκαιο, ενώ στα άρθρα 69 επόμ. Π.Κ. που αναφέρονται στα μέτρα ασφαλείας, ως μέρος της επιβολής ή εκτέλεσης των ποινών, η έννοια της ασφάλειας λαμβάνεται από το δημόσιο δίκαιο (δημόσια ασφάλεια).

Συμπερασματικός μπορεί να λεχθεί ότι, η έννοια της ασφάλειας στο διαδίκτυο δεν έχει καθοριστεί ακόμα από το νομοθέτη. Κατά τον καθορισμό της όμως, πρέπει να ληφθούν υπόψη οι βασικές Αρχές του Δικαίου, όπως αυτές προσδιορίζονται στο Ελληνικό Σύνταγμα και στους ισχύοντες Διεθνείς Κανόνες.

4.1.6 ΕΥΡΩΠΑΙΚΗ ΝΟΜΟΘΕΣΙΑ

Για την αντιμετώπιση του κινδύνου αυτού ήταν απαραίτητη η συνεννόηση μεταξύ των κρατών και η εκπόνηση μιας αναλυτικής και αποτελεσματική στρατηγικής. Ο σκοπός αυτός επετέθη με το Συνέδριο για το Ηλεκτρονικό έγκλημα (Convention on Cybercrime), του οποίου όλα τα συμπεράσματα αποκρυσταλλώνονται στην συνθήκη που υπογράφει στην Βουδαπέστη στις 23.11.2001.

Στη συνθήκη της Βουδαπέστη, που υπέγραψε μεταξύ πολλών άλλων χωρών και η Ελλάδα υπάρχουν επεξηγήσεις και ρυθμίσεις για όλα τα ηλεκτρονικά εγκλήματα:

- Για τα αδικήματα κατά της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των δεδομένων και των συστημάτων ηλεκτρονικών υπολογιστών. Τέτοια αδικήματα είναι η παράνομη πρόσβαση, η παράνομη υποκλοπή, η επέμβαση σε δεδομένα, η επέμβαση σε

συστήματα και η κακή χρήση συσκευών.

- Για τα αδικήματα που σχετίζονται με τους υπολογιστές όπως η απάτη με ηλεκτρονικό υπολογιστή και η πλαστογραφία.
- Για τα αδικήματα σχετικά με το περιεχόμενο όπως είναι το αδίκημα της παιδικής πορνογραφίας.
- Για τα αδικήματα που σχετίζονται με καταπάτηση πνευματικής ιδιοκτησίας.

Επίσης η συνθήκη περιέχει ρυθμίσεις για την συνεργεία, την απόπειρα και την υποκίνηση ηλεκτρονικών εγκλημάτων καθώς και την ευθύνη των επιχειρήσεων. Ακόμα τονίζει την αναγκαιότητα της διεθνούς συνεργασίας μεταξύ των κρατών για την καταπολέμηση του ηλεκτρονικού εγκλήματος και θίγει το πολύ σημαντικό θέμα της αρμοδιότητας και της δικαιοδοσίας των δικαστηρίων σχετικά με τα εγκλήματα αυτά. Η συνθήκη αυτή αποτελεί το πιο άρτιο κείμενο σχετικά με το ηλεκτρονικό κείμενο στην Ευρωπαϊκή ένωση. Υπάρχουν φυσικά και άλλα γενικά νομοθετήματα που βοηθούν στην καταπολέμηση του Ηλεκτρονικού εγκλήματος.

Στην Ευρωπαϊκή Ένωση ισχύουν:

- Η Σύσταση του Συμβουλίου με αριθμό 9193/01, με την οποία καλούνται τα κράτη μέλη να συμμετάσχουν στο δίκτυο πληροφόρησης της Ομάδας των Οκτώ, το οποίο λειτουργεί 24 ώρες το εικοσιτετράωρο, για την καταπολέμηση του εγκλήματος υψηλής τεχνολογίας.
- Το Ψήφισμα του Συμβουλίου με αριθμό 2003/ C 48/01, για την ασφάλεια των δικτύων και των πληροφοριών.
- Η Σύσταση του Συμβουλίου με αριθμό 95/144/ΕΚ, όπου αναφέρονται οι προτροπές του Συμβουλίου σχετικά με την ασφάλεια των συστημάτων πληροφορικής.
- Η Κοινή θέση της 27ης Μαΐου 1999 (1999/364/ΔΕΥ), όπου τα κράτη μέλη υποστηρίζουν την κατάρτιση του σχεδίου σύμβασης του Συμβουλίου της Ευρώπης σχετικά με την καταπολέμηση του εγκλήματος

στον κυβερνοχώρο και ότι φροντίζουν ώστε να περιληφθούν στη σύμβαση διατάξεις που θα διευκολύνουν την αποτελεσματική διερεύνηση και δίωξη εγκλημάτων που άπτονται των ηλεκτρονικών συστημάτων και δεδομένων.

- Το Ψήφισμα του Συμβουλίου με αριθμό 2002/C 43/02 για κοινή προσέγγιση και ειδικές δράσεις στον τομέα της ασφάλειας των πληροφοριών και των δικτύων.
- Το έγγραφο με αριθμό 2000/C 124/01 σχετικά με τη στρατηγική της Ευρωπαϊκής Ένωσης για την πρόληψη και τον έλεγχο του οργανωμένου εγκλήματος. Στο έγγραφο αυτό αναλύονται διεξοδικά τα μέτρα που πρέπει να ληφθούν για την πρόληψη και την καταπολέμηση του οργανωμένου εγκλήματος όπου εντάσσονται και πολλές μορφές του ηλεκτρονικού εγκλήματος.
- Το Σχέδιο Δράσης με αριθμό 97/C 251/01 για την καταπολέμηση του οργανωμένου εγκλήματος.

4.1.7 ΕΛΛΗΝΙΚΗ ΝΟΜΟΘΕΣΙΑ

Στην Ελλάδα ισχύουν οι εξής νόμοι:

- 2867/2000 “Οργάνωση και λειτουργία των τηλεπικοινωνιών και άλλες διατάξεις” (ΦΕΚ Α'273/19.12.00)
- 2672/1998 “Διακίνηση εγγράφων με ηλεκτρονικά μέσα (τηλεομοιοτυπία – ηλεκτρονικό ταχυδρομείο)” (ΦΕΚ Α'90/28.12.98)
- 3471/2006 “Προστασία δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στο τομέα των ηλεκτρονικών επικοινωνιών” (ΦΕΚ Α'133/28.6.06)
- 2246/1994 “Οργάνωση και λειτουργία στο τομέα των τηλεπικοινωνιών” (ΦΕΚ Α'172/20.10.94)
- 2472/1997 “Προστασία ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα (ΦΕΚ Α'50/10.4.97)
- 3115/2003 “Κανονισμός εσωτερικής λειτουργίας της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ) (ΦΕΚ Α'25/4.3.03)
- 2121/1993 “Πνευματική ιδιοκτησία , συγγενικά δικαιώματα και πολιτιστικά θέματα” (ΦΕΚ Α'25/4.3.93)
- 3431/2006 “Περί ηλεκτρονικών επικοινωνιών και άλλες διατάξεις (ΦΕΚ Α'19/3.3.06).

5.1 ΣΥΜΠΕΡΑΣΜΑΤΑ

Καταλήγοντας πρέπει να παραδεχτούμε ότι το διαδίκτυο πλέον χαρακτηρίζεται από την τεράστια χωρική και ποιοτική εξάπλωση .Το Ίντερνετ είναι ένα θαυμάσιο μέσο επικοινωνίας, ενημέρωσης, επιμόρφωσης, και ψυχαγωγίας. Οι εμπειρίες που προσφέρει στους χρήστες του είναι μοναδικές και δεν μπορούν να προσεγγιστούν από κανένα άλλο μέσο. Χάρη στην επινοητικότητα των ανθρώπων ο πλούτος των πηγών του αυξάνεται ραγδαία μέρα με την μέρα. Είναι ένα μέσο το οποίο πρέπει να εξερευνήσουν οι νέοι της εποχής μας ώστε να μπορούν να προσαρμοστούν στον κόσμο της τεχνολογίας.
Δυστυχώς η επινοητικότητα των ανθρώπων δεν χρησιμοποιείται πάντα για καλούς σκοπούς με αποτέλεσμα η παράνομη δραστηριότητα στο Ίντερνετ να έχει πάρει επικίνδυνες διαστάσεις. Μέρα με την μέρα νέες μορφές παράνομων δραστηριοτήτων κάνουν την εμφάνιση τους. Μερικές από τις πιο βασικές παράνομες ή επιβλαβείς δραστηριότητες που συναντάμε σήμερα στο Ίντερνετ είναι οι παρακάτω:
Έκθεση υλικού παιδικής πορνογραφίας

- Έκθεση υβριστικού περιεχομένου για συγκεκριμένα άτομα ή κοινωνικές ομάδες
- Βίαια, ρατσιστική και τρομοκρατική θεματολογία
- Παράνομες on-line συναλλαγές (οικονομικό έγκλημα)
- Παράνομος ηλεκτρονικός τζόγος
  Αποστολή μηνυμάτων με ακατάλληλο περιεχόμενο, χωρίς να είναι πάντα γνωστά τα στοιχεία του αποστολέα
- Αποστολή ιών (computer viruses) με σκοπό την πρόκληση ζημιάς στους υπολογιστές των αποδεκτών
- Τηλεσυνομιλίες (chatrooms) με άτομα που εκμεταλλεύονται τις τεχνολογικές τους δεξιότητες για να αντλήσουν προσωπικά δεδομένα και να προβούν σε παράνομες δράσεις

- Προώθηση ναρκωτικών και παράνομων ουσιών ή φαρμάκων για την χρήση των οποίων απαιτείται ειδική άδεια
- Διακίνηση αρχείων με προσωπικά ευαίσθητα δεδομένα και η παραβίαση του ιδιωτικού απορρήτου
- Προώθηση σατανιστικών και παραθρησκευτικών οργανώσεων
- Διάδοση μηνυμάτων με σκοπό τον προσηλυτισμό και γενικά η προώθηση προπαγανδιστικού υλικού
- Παρότρυνση σε αυτοκαταστροφικές ενέργειες

Σημαντική παράμετρος του ηλεκτρονικού εγκλήματος και της παραβατικότητας στις μέρες μας θα αποτελέσει και η χρηματοοικονομική κρίση που πλήττει την παγκόσμια οικονομία.

Όπως επισημαίνουν ειδικοί, η οικονομική κρίση όχι μόνο δεν αναμένεται να πλήξει το οργανωμένο ηλεκτρονικό έγκλημα που έχει οικονομικά κίνητρα, αλλά θα συμβάλλει στην ένταση του προβλήματος, καθώς οι χάκερς θεωρούν ότι μπορούν να επωφεληθούν σημαντικά από τις παρούσες συνθήκες εκμεταλλευόμενοι τις «αδυναμίες» και την έντονη ανασφάλεια που νιώθει αυτή την περίοδο η πλειονότητα του πληθυσμού. «Είθισται να υπάρχει αύξηση της εγκληματικότητας σε περιόδους έντονης ανεργίας», αναφέρουν χαρακτηριστικά αναλυτές της γνωστής εταιρείας ηλεκτρονικής ασφαλείας F-Secure. Στην περίπτωση, μάλιστα, των ηλεκτρονικών επιθέσεων στο Internet επισημαίνουν ότι «το πρόβλημα δεν έχει τεχνολογικές αλλά κοινωνικές ρίζες».

Άρα καταλήγουμε στο γεγονός ότι πρωταρχικός στόχος της πολιτείας πρέπει να είναι η ενημέρωση των πολιτών, η πρόληψη αλλά και η αντιμετώπιση κινδύνων που σχετίζονται με τις νέες τεχνολογίες πληροφορικής και ηλεκτρονικών επικοινωνιών, κάτι που προϋποθέτει την ένωση των δυνάμεων των αρμόδιων φορέων.

ΒΙΒΛΙΟΓΡΑΦΙΑ

ΤΕΧΝΙΚΕΣ ΑΝΑΖΗΤΗΣΗΣ ΕΠΙΧΕΙΡΗΜΑΤΙΚΩΝ ΠΛΗΡΟΦΟΡΙΩΝ ΣΤΟ ΔΙΑΔΙΚΤΥΟΥ
Σπύρος Α. Κωνσταντινίδης
Εκδόσεις ANUBIS

ΕΙΣΑΓΩΓΗ ΣΤΑ ΣΥΣΤΗΜΑΤΑ ΒΑΣΕΩΝ ΔΕΔΟΜΕΝΩΝ
C.S. Date
Εκδόσεις Κλειδάριθμος

ΕΞΕΡΕΥΝΗΣΤΕ ΤΟ INTERNET
Bennet Falk
Εκδόσεις Κλειδάριθμος

ΠΛΗΡΟΦΟΡΙΑΚΑ ΣΥΣΤΗΜΑΤΑ ΓΙΑ ΤΗ ΔΙΟΙΚΗΣΗ ΕΠΙΧΕΙΡΗΣΕΩΝ
Γ. Οικονόμου – Ν. Γεωργοπούλου
Εκδόσεις Ε. Μπένου

MAXIMUM SECURITY
Ανώνυμος
Γκιούρδας Εκδοτική

ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ, ΕΙΣΑΓΩΓΗ – ΒΑΣΙΚΑ ΘΕΜΑΤΑ
Δημήτρη Γκριζάνη
Ελληνική εταιρία επιστημόνων Η/Υ και πληροφορικής

NETWORK SECURITY
Devargas Mario
Εκδόσεις Blackwell

ΧΑΚΕΡ: ΕΠΙΘΕΣΗ ΚΑΙ ΑΜΥΝΑ
Scambray Joel – McClure Stuart - Kurtz George
Εκδόσεις Γκιούρδας

ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ ΚΑΙ ΥΠΟΛΟΓΙΣΤΙΚΩΝ ΣΥΣΤΗΜΑΤΩΝ
ΑΝΑΧΑΙΤΙΣΤΕ ΤΟΥΣ ΕΙΣΒΟΛΕΙΣ
Κομνηνός Θοδωρής – Σπυράκης Παύλος
Εκδόσεις Ελληνικά Γράμματα

ΗΛΕΚΤΡΟΝΙΚΕΣ ΔΙΕΥΘΥΝΣΕΙΣ

www.inatelecom.org

ΠΕΡΙΦΕΡΕΙΑΚΟ ΦΟΡΟΥΜ ΗΛΕΚΤΡΟΝΙΚΗΣ ΑΣΦΑΛΕΙΑΣ

www.igf.gr

ΦΟΡΟΥΜ ΔΙΑΚΥΒΕΡΝΗΣΗΣ ΔΙΑΔΙΚΤΥΟΥ

www.wikipedia.gr

ΗΛΕΚΡΤΟΝΙΚΗ ΒΙΒΛΙΟΘΗΚΗ

www.cert.sch.gr

ΥΠΗΡΕΣΙΑ ΑΝΤΙΜΕΤΩΠΙΣΗΣ ΠΕΡΙΣΤΑΤΙΚΩΝ ΑΣΦΑΛΕΙΑΣ

www.symantec.com

www.dart.gov.gr

ΟΜΑΔΑ ΔΡΑΣΗΣ ΓΙΑ ΤΗΝ ΨΗΦΙΑΚΗ ΑΣΦΑΛΕΙΑ, ΓΡΑΜΜΑΤΕΙΑ ΨΗΦΙΑΚΟΥ ΣΧΕΔΙΑΣΜΟΥ

www.ics.forth.gr

ΙΝΣΤΙΤΟΥΤΟ ΠΛΗΡΟΦΟΡΙΚΗΣ

www.europa.gr

ΔΡΑΣΤΗΡΙΟΤΗΤΕΣ ΤΗΣ ΕΥΡΩΠΑΙΚΗΣ ΕΝΩΣΗΣ

www.imerisia.gr
ΕΦΗΜΕΡΙΔΑ “ΗΜΕΡΗΣΙΑ”

www.haniotika-nea.gr
ΕΦΗΜΕΡΙΔΑ “ΧΑΝΙΩΤΙΚΑ ΝΕΑ”

www.fotoseartch.com
ΦΩΤΟΓΡΑΦΙΕΣ