ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΜΕΛΕΤΗ ΕΞΑΠΛΩΣΗΣ ΤΩΝ WORMS

Γκρόζας Νικόλαος
Α.Μ : ΜΕ/07044

Μεταπτυχιακή Διπλωματική Εργασία

Επιβλέπων: Κωνσταντίνος Λαμπρινουδάκης
Επίκουρος Καθηγητής Πανεπιστημίου Πειραιά

Πειραιάς, Απρίλιος 2012

Περιεχόμενα

Εισαγωγή

Πολλοί είναι εκείνοι στις μέρες μας οι οποίοι έχουν αναρωτηθεί τι είναι ο ηλεκτρονικός υπολογιστής και τι προσφέρει. Η απάντηση που θα μπορούσε να δοθεί εδώ είναι πως ο ηλεκτρονικός υπολογιστής, δεν είναι τίποτα άλλο παρά ένα ακόμα μηχάνημα, το οποίο κατασκεύασε ο άνθρωπος και φυσικά όπως και τόσες άλλες μηχανές, οι οποίες έχουν ως στόχο να κάνουν ευκολότερη ή δυσκολότερη την καθημερινή ζωή των ανθρώπων[1]. Η σχετική ωφέλεια ή η βλάβη βέβαια και η οποία μπορεί να προξενείτε από τη χρήση του, εξαρτάται ουσιαστικά αποκλειστικά από τη χρήση που θα του κάνει κάποιος και όπως άλλωστε συμβαίνει με όλες τις μηχανές.

Θα πρέπει αντίστοιχα να σημειωθεί πως τα παλαιότερα χρόνια η εκπαίδευση και μόνο με τη βοήθεια ηλεκτρονικών υπολογιστών γινόταν μόνον για τους αστροναύτες ή επίσης για τους πιλότους των πολεμικών αεροσκαφών και η χρήση τους στο σπίτι περιοριζόταν μόνον στο να παίζουν μικροί ή μεγάλοι διάφορα σχετικά παιχνίδια. Στην εποχή μας όμως, τα πράγματα έχουν αισθητά αλλάξει και διαφοροποιηθεί. Οι νέας τεχνολογίας ηλεκτρονικοί υπολογιστές μπορούν επίσης να χρησιμοποιηθούν από τον κατάλληλα εκπαιδευμένο εκπαιδευτικό προσωπικό ή από τον κατάλληλα ενημερωμένο γονέα, για να μάθουν σε παιδιά από τριών ως έξι ετών, για παράδειγμα τις πρώτες πράξεις της αριθμητικής ή τις πρώτες τους λέξεις[2].

1. Κεφάλαιο Πρώτο : Λειτουργία Ηλεκτρονικών Υπολογιστών στις Μέρες μας και Συστήματα Ασφαλείας

[1] Miglino, O., Lund, H.H. & Cardaci, M. (1999), Robotics as an Educational Tool, Journal of Interactive Learning Research, 10(1), 25-48

[2] Meinel, C., P., 1998, "*The Happy Hacker"*, American Eagle Publications

1.1 Ιστορία των Ηλεκτρονικών Υπολογιστών

Αποτελεί γεγονός πως ένας ηλεκτρονικός υπολογιστής θεωρείται και είναι μια μηχανή κατασκευασμένη κυρίως από συγκεκριμένα ηλεκτρονικά κυκλώματα αλλά και δευτερευόντως από ηλεκτρικά και μηχανικά συστήματα, και έχει ως σκοπό ουσιαστικά να επεξεργάζεται επίσης συγκεκριμένες πληροφορίες. Ο ηλεκτρονικός υπολογιστής είναι ένα απολύτως αυτοματοποιημένο, ηλεκτρονικό αλλά και ψηφιακό επαναπρογραμματιζόμενο σύστημα μιας γενικής χρήσης και το οποίο μπορεί να επεξεργάζεται δεδομένα βάσει ενός συνόλου προκαθορισμένων οδηγιών, των εντολών που συνολικά ονομάζονται και αναφέρονται στις μέρες μας ως Πρόγραμμα[3].

Θα πρέπει αντίστοιχα να σημειωθεί πως υπάρχουν διάφοροι τύποι ηλεκτρονικών υπολογιστών στις μέρες μας και οι οποίοι διαφέρουν κατά το μέγεθος, τις δυνατότητες οι οποίες καθορίζονται σύμφωνα με την επεξεργαστική τους ισχύς αλλά και την αρχιτεκτονική τους, δηλαδή τον τρόπο βέβαια που τα βασικά τους μέρη συνδέονται αλλά και συνεργάζονται μεταξύ τους. Φυσικά, στην πιο διαδεδομένη κατηγορία υπολογιστών ανήκουν και οι επωνομαζόμενοι μικρο-ϋπολογιστές. Στους μικροϋπολογιστές αντίστοιχα, τα βασικά εξαρτήματα, και τα οποία είναι ο επεξεργαστής, η μνήμη κ.ά., βρίσκονται τοποθετημένα σ' ένα λεγόμενο «τυπωμένο» κύκλωμα το οποίο ονομάζεται μητρική κάρτα[4]. Ωστόσο, εκτός από τον επεξεργαστή και τη μνήμη, θα πρέπει να σημειωθεί πως πάνω στη μητρική βρίσκονται οι θέσεις επέκτασης στις οποίες αντίστοιχα τοποθετούνται και οι διάφορες κάρτες γραφικών αλλά και ήχου σχετικά. Τέλος, στη μητρική επίσης βρίσκονται υποδοχές για τη σύνδεση διαφόρων άλλων συσκευών οι οποίες προσφέρουν στους χρήστες άμεση εξυπηρέτηση στις καθημερινές τους ανάγκες.

1.2 Ποια η Μορφή των Ηλεκτρονικών Υπολογιστών στις Μέρες μας και τα Υλικά τα Οποία Αποτελούνται

[3] Miglino, O., Lund, H.H. & Cardaci, M. (1999), *Robotics as an Educational Tool, Journal of Interactive Learning Research*, 10(1), 25-48

[4] Miglino, O., Lund, H.H. & Cardaci, M. (1999), Robotics as an Educational Tool, Journal of Interactive Learning Research, 10(1), 25-48

Οι μορφές των ηλεκτρονικών υπολογιστών και οι οποίες εντοπίζονται στις μέρες μας με τα διάφορα κριτήρια που παρουσιάζουν, αναφέρονται ως εξής[5].

- *Υπερυπολογιστής – supercomputer*
- *Μικρός Υπολογιστής*
- *Κεντρικός Υπολογιστής – mainframe*
- *Εξυπηρετητής – server*
- *Σταθμός Εργασίας – Workstation*
- *Προσωπικός Υπολογιστής – PC*
- *Επιτραπέζιο Υπολογιστή - desktop PC*
- *Φορητός Υπολογιστής - Laptop*

Θα πρέπει βέβαια να σημειωθεί πως κάθε ηλεκτρονικός υπολογιστής και το αντίστοιχο πρόγραμμα που διαθέτει, όσο βέβαια μεγάλο ή μικρό κι αν είναι, αποτελείται από το υλικό μέρος από το hardware καθώς και το λογισμικό το οποίο είναι γνωστό ως software[6]. Τα βασικά στοιχεία του υλικού μέρους του υπολογιστή είναι η κεντρική μονάδα επεξεργασίας όπως η Κεντρική Μονάδα Επεξεργασίας, το CPU - Central Prossesing Unit, η κεντρική μνήμη RAM και ROM BIOS, οι μονάδες εισόδου – εξόδου, το λεγόμενο «ποντίκι», η οθόνη, το πληκτρολόγιο όπως και οι διάφορες περιφερειακές συσκευές όπως οι σκληροί δίσκοι, η δισκέτα, το μόντεμ, ο σαρωτής καθώς και οι εκτυπωτές αλλά και τα DVD.

Είναι γεγονός επίσης πως το λογισμικό του ηλεκτρονικού υπολογιστή αποτελείται από εκείνα τα απαραίτητα προγράμματα που προσφέρουν τις κατάλληλες εντολές, με σκοπό να λειτουργεί το υλικό μέρος. Συνίσταται δε πως από το λειτουργικό σύστημα ενός ηλεκτρονικού υπολογιστή το βασικό πρόγραμμα για τη λειτουργία του καθώς και για την επικοινωνία του με τον

[5] Meinel, C., P., 1998, "*The Happy Hacker"*, American Eagle Publications

[6] Denning, D., E., 2007, "*Cryptography and Data Security*", Addison – Wesley

άνθρωπο, ιδιαίτερα σημαντικό είναι και το λογισμικό εφαρμογών με πακέτα εφαρμογών, γλώσσες προγραμματισμού, εκπαιδευτικό λογισμικό, προγράμματα – εργαλεία κ.α.

Θα πρέπει τέλος να σημειωθεί πως η ικανότητα ενός ειδικού και με σκοπό να προγραμματιστεί κατάλληλα ένας ηλεκτρονικός υπολογιστής, προμηθεύοντάς τον αντίστοιχα με ένα σύνολο εντολών προς εκτέλεση και χωρίς βέβαια να χρειαστεί να αναδιαμορφωθεί η φυσική διάταξή του και όπως αντίστοιχα γινόταν με τις καλωδιώσεις και τους χιλιάδες διακόπτες των πρώτων υπολογιστών, είναι ουσιαστικά ένα θεμελιώδες σχεδιαστικό στοιχείο των σύγχρονων υπολογιστών στις μέρες μας. Αυτό το χαρακτηριστικό βέβαια επεκτάθηκε όταν οι υπολογιστές μπόρεσαν αντίστοιχα να ελέγξουν δυναμικά την ροή της εκτέλεσης των εντολών ενός προγράμματος βασιζόμενοι σε ενδιάμεσα αποτελέσματα του υπολογιστή στις μέρες μας[7].

1.3 Συστήματα Ασφαλείας που Χρησιμοποιούνται στους Ηλεκτρονικούς Υπολογιστές

Εφαρμογή FIREWALL

Οι τοίχοι προστασίας (firewalls) αποτελούν μία πολύ αποτελεσματική μέθοδο προστασίας δικτύου. Στην ουσία πρόκειται για ένα σύστημα σχεδιασμένο να κάνει το δίκτυο προσβάσιμο με προσεκτικά ελεγχόμενους και παρακολουθούμενους τρόπους. Ένα σύστημα firewall επιτυγχάνει δύο στόχους: Παρέχει στους ανθρώπους της εταιρείας πρόσβαση στον παγκόσμιο ιστό, χωρίς ταυτόχρονα να επιτρέπει σε όλο τον κόσμο να παρακολουθεί παρανόμως και δεύτερον μπορεί να υψωθεί μεταξύ ενός ανέμπιστου τμήματος λογισμικού, του δημόσιου εξυπηρετητή ιστού και των ευαίσθητων πληροφοριών που ανήκουν στο ιδιωτικό δίκτυο της[8].

Στις κατασκευές κτιρίων, ο τοίχος προστασίας είναι σχεδιασμένος ώστε να εμποδίζει την εξάπλωση φωτιάς από το ένα μέρος του κτιρίου στο άλλο. Κάτι αντίστοιχο πραγματοποιείται με την τοποθέτησή του ανάμεσα στο εξωτερικό

[7] Denning, D., E., 2007, "*Cryptography and Data Security*", Addison – Wesley

[8] Denning, D., E., 2007, "*Cryptography and Data Security*", Addison – Wesley

και εσωτερικό δικτυακό περιβάλλον μιας εταιρείας. Η βασική ιδέα ενός firewall είναι γενικά απλή. Σε ένα παραδοσιακό ανοιχτό σύστημα, όλοι οι κεντρικοί υπολογιστές στο δίκτυο τοπικής περιοχής (Local Area Network - LAN) έχουν άμεση πρόσβαση στο Διαδίκτυο και είναι ισοδύναμα ευάλωτοι σε επιθέσεις από έξω[9]

Η ασφάλεια του τοπικού δικτύου εξαρτάται από την ασφάλεια του πιο αδύναμου κεντρικού υπολογιστή. Ένας απλός ανασφαλής κεντρικός υπολογιστής θα επιτρέψει σε ένα εισβολέα να εισέλθει. Όταν εισέλθει είναι εύκολο κλέβοντας τους λογαριασμούς νομίμων χρηστών, αντικαθιστώντας το λογισμικό του συστήματος με αντίγραφα και με άλλα τέτοια τεχνάσματα, να ανατρέψει άλλους κεντρικούς υπολογιστές στο χώρο. Όχι μόνο είναι δύσκολο να προστατευθεί ένα ανοιχτό σύστημα από επίθεση αλλά είναι δύσκολο να ανιχνευθεί η προσβολή του.

Τα firewalls αντιμετωπίζουν αυτό το πρόβλημα παρεμβάλλοντας μία ειδικά διαμορφωμένη μηχανή πύλης (gateway) ανάμεσα στον έξω κόσμο και στο εσωτερικό δίκτυο του χώρου. Η άμεση επαφή μεταξύ των κεντρικών υπολογιστών του εσωτερικού δικτύου και του εξωτερικού κόσμου απαγορεύεται. Αντίθετα όλη η κίνηση πρέπει πρώτα να πάει στην πύλη όπου το λογισμικό αποφασίζει αν η κίνηση μπορεί να επιτραπεί ή να απορριφθεί. Αυτό διαιρεί αποτελεσματικά το δίκτυο σε ένα "εσωτερικό" έμπιστο δίκτυο (δηλαδή το τοπικό) και σε ένα "εξωτερικό" ανέμπιστο δίκτυο (δηλαδή το διαδίκτυο).

Η ζώνη συνόρων μεταξύ των εσωτερικών και εξωτερικών δικτύων είναι γνωστή σαν "περίμετρος ασφάλειας". Τώρα η εργασία προστασίας του τοπικού δικτύου γίνεται πιο απλή καθώς αντί να προστατεύεται ένα ετερογενές σύνολο μεμονωμένων κεντρικών υπολογιστών από προσβολή, οι προσπάθειες επικεντρώνονται στην προστασία της απλής μηχανής πύλης του δικτύου. Αν η πύλη δικτύου είναι ασφαλής, το τοπικό δίκτυο είναι ασφαλές[10].

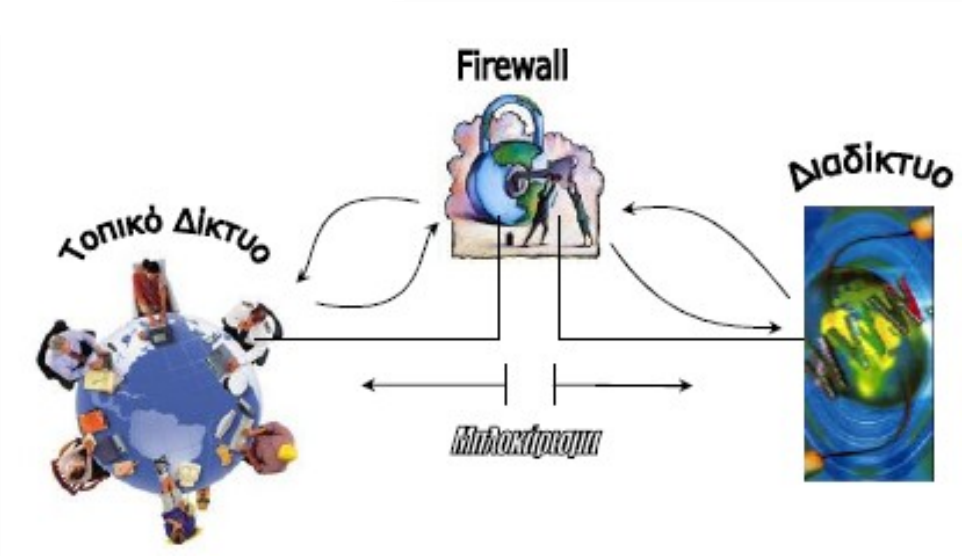
[9] Schneier, B., 1996, "*Applied Cryptography*", Prentice Hall

[10] Schneier, B., 1996, "*Applied Cryptography*", Prentice Hall

Υπάρχουν δύο βασικές υλοποιήσεις για συστήματα firewalls. Στην προσέγγιση "πύλη διπλής στέγης" (Σχήμα No.1), η μηχανή του firewall που ονομάζεται "οχυρή θέση", έχει δύο κάρτες δικτύου, μία που συνδέεται με το εσωτερικό δίκτυο και μία που συνδέεται με το ανέμπιστο δίκτυο. Η μηχανή έχει ρυθμιστεί έτσι ώστε τα πακέτα δικτύου που φθάνουν στη μία κάρτα να μη βασίζονται στην άλλη. Εξ ορισμού τα δύο δίκτυα είναι εντελώς απομονωμένα. Παρόλα αυτά, επειδή υπάρχει πάντα η ανάγκη κάποιας επικοινωνίας μεταξύ των εσωτερικών και των εξωτερικών δικτύων, ειδικά προγράμματα, που ονομάζονται "μεσολαβητές" (proxies), τρέχουν στη μηχανή firewall. Η δουλειά ενός μεσολαβητή είναι να προωθήσει επιλεκτικά πληροφορίες από το ένα δίκτυο στο άλλο.

Οι μεσολαβητές μπορούν να καθορίσουν ποιά πακέτα δικτύου να προωθήσουν κοιτάζοντας τις διευθύνσεις προέλευσης και προορισμού, εξετάζοντας τον τύπο πακέτου, εξετάζοντας τις θύρες προέλευσης και προορισμού ή ακόμη ελέγχοντας τα περιεχόμενα που υπάρχουν μέσα στο πακέτο. Τα πακέτα δικτύου ποτέ δεν μεταφέρονται άμεσα. Τα δεδομένα τους εξάγονται και τοποθετούνται σε νέα πακέτα πριν μεταφέρουν τις πληροφορίες τους μέσω της πύλης δικτύου.

Σχεδιάγραμμα No. 1 - Firewall σύμφωνα με την προσέγγιση "Πύλη διπλής στέγης"

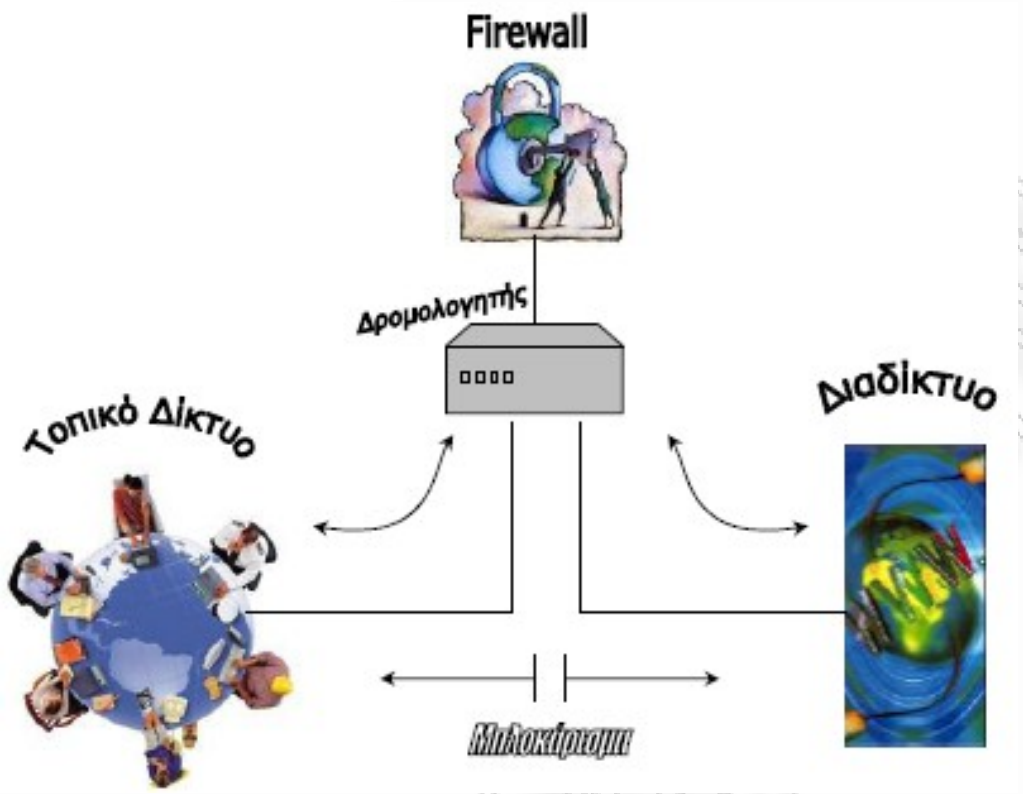


Στην προσέγγιση "διαχωριστικού κεντρικού υπολογιστή πύλης" (Σχήμα No.2) ένας δρομολογητής δικτύου χρησιμοποιείται για να ελέγξει την πρόσβαση στο εσωτερικό δίκτυο. Ο δρομολογητής περιορίζει την επικοινωνία μεταξύ των εξωτερικών και εσωτερικών δικτύων διασφαλίζοντας ότι τα δικτυακά πακέτα που ξεκινούν μέσα από το εξωτερικό δίκτυο μπορούν να φτάσουν μόνο όταν η καλά ασφαλισμένη μηχανή της οχυρής θέσης τα εξετάσει και με την παρουσία των μεσολαβητών, που τα αναμεταδίδουν στο εσωτερικό δίκτυο. Στις περισσότερες περιπτώσεις, οι μηχανές στο εσωτερικό δίκτυο είναι εντελώς αόρατες στο εξωτερικό[11]

Τα εξωτερικά πακέτα από το εσωτερικό δίκτυο είτε περιορίζονται στη μηχανή τοίχου προστασίας, όπου πάλι πρέπει να συνοδευτούν στο διαδίκτυο μέσω ενός προγράμματος μεσολάβησης ή επιτρέπεται να περάσουν άμεσα μέσω του δρομολογητή, αφού ικανοποιήσουν ορισμένους κανόνες φιλτραρίσματος για να προσδιορίσουν ότι είναι ασφαλή.

Σχεδιάγραμμα No. 2 - Firewall σύμφωνα με την προσέγγιση " διαχωριστικού κεντρικού υπολογιστή πύλης"

[11] Pfleeger, C., P., 1997, "*Security in Computing*", Prentice Hall



Σε ένα καλά σχεδιασμένο σύστημα firewall, δεν υπάρχει καμία ουσιαστική διαφορά ανάμεσα στα συστήματα διπλής στέγης και διαχωριστικού κεντρικού υπολογιστή. Σε κάθε περίπτωση το εσωτερικό δίκτυο εμφανίζεται στον έξω κόσμο να περιέχει μία απλή καλά προστατευμένη μηχανή, τον κεντρικό υπολογιστή οχυρής θέσης. Όλη η εξερχόμενη κίνηση από το εσωτερικό δίκτυο στον έξω κόσμο εμφανίζεται να ξεκινά από την οχυρή θέση και όλη η εισερχόμενη κίνηση απευθύνεται σε αυτή τη θέση. Το λογισμικό στο οχυρό θέσης ελέγχει κάθε κομμάτι δεδομένων δικτύου που φτάνει, το καταγράφει και του επιτρέπει να περάσει αν ικανοποιεί το σύνολο κανόνων και ρυθμίσεων που έχουν οριστεί από τους διαχειριστές του firewall[12]

Πολλοί οργανισμοί έχουν εγκαταστήσει συστήματα firewalls που δεν είναι καθόλου firewalls. Είναι δρομολογητές δικτύου που έχουν διαμορφωθεί να σταματούν την επικίνδυνη κυκλοφορία δικτύου ενώ επιτρέπουν να προχωρήσει η ασφαλής κυκλοφορία του δικτύου. Αυτού του είδους το σύστημα μπορεί να είναι δύσκολο να διαχειριστεί αποτελεσματικά λόγω της δυσκολίας του να δημιουργήσει αποτελεσματικούς κανόνες φιλτραρίσματος. Ακόμη και μία φαινομενικά αβλαβής αλλαγή σε ένα πίνακα δρομολόγησης

[12] Taylor, A., 1999, "*The Hackers*", Routledge

μπορεί να έχει αθέλητες επιδράσεις. Επειδή οι δρομολογητές δεν έχουν σχεδιαστεί βασικά για σκοπούς ασφάλειας, συνήθως δεν καταγράφουν τη δραστηριότητα του δικτύου, κάνοντας δύσκολο το να προσδιοριστεί αν το σύστημα δουλεύει κανονικά ή ακόμη και αν έχει προσβληθεί.

Η ουσία μιας πολιτικής ασφάλειας ενός firewall έχει ενσωματωθεί στα φίλτρα που επιτρέπουν ή απαγορεύουν τη δίοδο στην κυκλοφορία δικτύου. Τα προγράμματα μεσολάβησης έρχονται σε δύο εκδόσεις. Υπάρχουν μεσολαβητές "επιπέδου εφαρμογής", που έχουν γραφτεί για συγκεκριμένα πρωτόκολλα επικοινωνίας. Για παράδειγμα ένας μεσολαβητής επιπέδου εφαρμογής θα είναι υπεύθυνος για την προώθηση HTTP αιτήσεων μπρος και πίσω πάντα μέσω του firewall, ένας άλλος υπεύθυνος για FTP αιτήσεις και ένας τρίτος υπεύθυνος για το ηλεκτρονικό ταχυδρομείο. Επειδή οι μεσολαβητές επιπέδου εφαρμογής καταλαβαίνουν το νόημα των πληροφοριών τις μεταδίδουν μπρος πίσω και μπορούν να εφαρμόσουν κανόνες φιλτραρίσματος με βάση τα περιεχόμενα των δικτυακών πακέτων[13]

Για παράδειγμα, αν μια εταιρεία αποφασίσει να προστατεύσει τους υπαλλήλους της από πιθανούς κινδύνους ActiveX ελέγχων, θα μπορούσε να στήσει ένα HTTP μεσολαβητή για να εξετάσει κάθε HTML σελίδας που περνά την οχυρή θέση και να διαγράψει αθόρυβα τις αναφορές σε ActiveX. Οι μεσολαβητές επιπέδου εφαρμογής μπορούν επίσης να φιλτράρουν την κυκλοφορία δικτύου από τις IP διευθύνσεις των πλευρών αποστολής και παραλαβής, τις θύρες δικτύου σε οποιαδήποτε πλευρά της σύνδεσης και άλλα χαρακτηριστικά των επικεφαλίδων των πακέτων δικτύου.

Σε αντίθεση με τους μεσολαβητές επιπέδου εφαρμογής είναι οι μεσολαβητές "επιπέδου κυκλώματος", προγράμματα γενικού σκοπού που φέρονται στα πακέτα δικτύου σαν σε πολλά μαύρα κουτιά που θα προωθηθούν μέσω της οχυρής θέσης ή όχι. Αυτού του είδους ο μεσολαβητής μπορεί να φιλτράρει μόνο τη βάση της πληροφορίας επικεφαλίδας στα πακέτα δικτύου. Οι μεσολαβητές επιπέδου κυκλώματος μπορούν να απαγορέψουν πακέτα δικτύου που προέρχονται από απαγορευμένες πηγές, αλλά δεν μπορούν να κρυφοκοιτάξουν μέσα στο πακέτο να δουν αν ένα πακέτο, που φαίνεται

[13] Denning, D., E., 2007, “*Cryptography and Data Security*”, Addison – Wesley

νόμιμο, κρύβει μια επικίνδυνη δραστηριότητα. Το κύριο πλεονέκτημα των μεσολαβητών επιπέδου κυκλώματος είναι η γενικότητα και η ταχύτητά τους. Ένας μεσολαβητής μπορεί να διαχειριστεί πολλά πρωτόκολλα και είναι πιο γρήγοροι διότι η εργασία τους είναι λιγότερο έντονη υπολογιστικά[14].

Σε όλους τους τύπους των συστημάτων firewalls, η ασφάλεια του εσωτερικού δικτύου εξαρτάται από την ασφάλεια του κεντρικού υπολογιστή οχυρής θέσης. Κάποιος που αποκτά πρόσβαση στον τοίχο προστασίας ή είναι ικανός να αναδιαμορφώσει τα μέτρα ασφαλείας, το πιο πιθανό είναι να μπορεί να εισέλθει και σε άλλες μηχανές στο τοπικό δίκτυο. Σε συστήματα διαχωριστικού κεντρικού υπολογιστή, ο δρομολογητής είναι επίσης ένας πιθανός αδύνατος σύνδεσμος. Για να εμποδιστεί η έκθεση είτε της οχυρής θέσης είτε του κεντρικού υπολογιστή, τα firewalls είναι ειδικά διαμορφωμένα και διαχωρισμένα. Τυπικά, εκτελούν μία "σκληραγωγημένη" έκδοση των UNIX και NT λειτουργικών συστημάτων, από τις οποίες έχουν αφαιρεθεί διάφορα τρωτά σημεία. Τα firewalls δεν εκτελούν αχρείαστες υπηρεσίες, δεν περιέχουν ανέμπιστο λογισμικό και κρατούν μια ασφαλή καταγραφή όλης της δραστηριότητας[15].

Αδυναμίες των Συστημάτων Firewalls

Τα firewalls είναι γεγονός ότι προσφέρουν υψηλού επιπέδου προστασία απέναντι στους κινδύνους που προέρχονται από το διαδίκτυο. Υπάρχουν όμως και κίνδυνοι από τους οποίους τα firewalls αδυνατούν να μας προστατέψουν. Μερικές τέτοιες αδυναμίες τους είναι οι επόμενες[16]:

- ***Το firewall δεν μπορεί να εμποδίσει τους εσωτερικούς κινδύνους***. Μπορεί να έχει την δυνατότητα να ελέγχει τα δεδομένα που εισέρχονται και εξέρχονται του δικτύου δεν μπορεί όμως να εμποδίσει κάποιον από την εταιρεία (ή κάποιον που κατάφερε να μπει μέσα στα γραφεία της εταιρείας) να αντιγράψει δεδομένα σε δισκέττα, Cd, ή ακόμη και σε χαρτί και να τα μεταφέρει τελικά εκτός της εταιρείας. Εάν ο εισβολέας

[14] Pfleeger, C., P., 1997, "*Security in Computing*", Prentice Hall

[15] Pfleeger, C., P., 1997, "*Security in Computing*", Prentice Hall

[16] Denning, D., E., 2007, "*Cryptography and Data Security*", Addison – Wesley

βρεθεί πίσω και από το firewall τότε το firewall δεν μπορεί να τον ελέγξει, ούτε ασφαλώς να τον εμποδίσει.

- ***Δεν μπορεί να ελέγξει οτιδήποτε δεν περνάει από μέσα του***. Το firewall παρακολουθεί και ελέγχει όλη την κίνηση που διέρχεται από μέσα του αλλά αδυνατεί να κάνει τα ίδια για τα δεδομένα εκείνα που δεν περνούν από το ίδιο.

- ***Δεν μπορεί να προστατέψει το σύστημα από νέες απειλές***. Κανένα firewall δεν έχει τη δυνατότητα να ασφαλίσει το δίκτυο και τα δεδομένα, από καινούργιες απειλές. Η τοποθέτηση του δεν σημαίνει ότι το συγκεκριμένο σύστημα ασφαλείας εξασφαλίζει μόνιμη και διαρκή προστασία. Άλλωστε κανείς δεν μπορεί να γνωρίζει τι μορφή και τι δυνατότητες θα έχουν οι μελλοντικοί κίνδυνοι.

- ***Δεν μπορεί να προστατέψει το σύστημα από ιούς***. Τα firewalls δεν είναι πλέον αποκλειστικό προνόμιο των εταιρικών δικτύων. Ο απλός χρήστης έχει αρκετές επιλογές για να εξασφαλίσει σε ένα μεγάλο βαθμό την ακεραιότητα του υπολογιστή του. Με την εγκατάσταση ενός Antivirus στον υπολογιστή σας, μειώνετε δραματικά την πιθανότητα εισβολής κάποιου ιού, σκουληκιού ή δούρειου ίππου. Με κανέναν όμως τρόπο δεν αποτρέπετε κακόβουλους hacker ή καλύτερα cracker από το να δοκιμάσουν να διεισδύσουν στον υπολογιστή σας χωρίς την έγκρισή σας. Για να εξασφαλιστείτε όσο το δυνατόν περισσότερο, θα πρέπει να εγκαταστήσετε στο PC σας κάποιο firewall. Θα πρέπει βέβαια να αναφέρουμε ότι δεν προσφέρουν απόλυτη προστασία.

Εάν, για παράδειγμα, το πανάκριβο firewall της Microsoft "τρύπησε", το ίδιο μπορεί να γίνει, αρκετά πιο εύκολα μάλιστα, και στα PC μας. Βέβαια, η Microsoft και κάθε άλλος εταιρικός δικτυακός τόπος είναι επώνυμοι στόχοι και είναι φυσικό να προσελκύουν το ενδιαφέρον των απανταχού cracker, ενώ ο απλός χρήστης είναι στην κυριολεξία σταγόνα μέσα στον ωκεανό. Παρ' όλα αυτά, υπάρχουν δυστυχώς αρκετοί ερασιτέχνες και ημιεπαγγελματίες οι οποίοι "σκανάρουν" το Internet για να βρουν "ανοιχτές πόρτες" στους υπολογιστές μας.

Εάν κάποιος έχει μόνιμη σύνδεση με το Internet (και κατά συνέπεια σταθερό IP), εάν λειτουργεί κάποιο διακομιστή (π.χ., Web) στον υπολογιστή σας ή εφαρμογή απομακρυσμένης πρόσβασης (PC Anywhere-Wingate κ.λπ.) ή απλώς επιθυμεί να ελέγχει τι εισέρχεται και τι «φεύγει» από το PC του, θα πρέπει να εγκαταστήσει ένα firewall. Μόνο έτσι θα απομονωθεί το σύστημά από το Internet και στην ουσία θα "εξαφανιστεί" από τον έξω κόσμο, ακόμα και αν είναι on-line. Επιπλέον, με βάση κάποιους συγκεκριμένους κανόνες, ελέγχει και κατά συνέπεια επιτρέπει ή εμποδίζει να εισέλθουν στον υπολογιστή ή να εξέλθουν από αυτόν τα πακέτα δεδομένων του Internet.

Μέθοδος Passwords

Τα passwords είναι η πιο συνηθισμένη διαδικασία που χρησιμοποιείται σχεδόν παντού για να διασφαλίζει και να επιβεβαιώνει την ταυτότητα του χρήστη, επιτρέποντάς του εν συνεχεία την είσοδο στο κάθε σύστημα. Η συγκεκριμένη μέθοδος εφαρμόζεται για κάθε είσοδο χρήστη σε ένα πληροφοριακό σύστημα ή στο δίκτυο. Από το χρήστη ζητούνται το user name και το password του, τα οποία εφόσον ταιριάζουν με αυτά που υπάρχουν στο password file, θεωρούνται από το σύστημα ως επιβεβαίωση της ταυτότητάς του και έτσι ο χρήστης εισάγεται εντός του συστήματος ή του δικτύου. Τα passwords θεωρούνται ως αξιόπιστη και ασφαλής διαδικασία ελέγχου ταυτότητας αλλά όπως σε όλα τα θέματα που αφορούν την ασφάλεια έτσι και εδώ ο κίνδυνος κρύβεται στις λεπτομέρειες και οι οποίες αναφέρονται ως εξής[17]

1ος Κίνδυνος

Η επιλογή του password είναι ίσως το κρισιμότερο σημείο και αυτό διότι οι επιλογές που κάνουν οι χρήστες συνήθως είναι προβλέψιμες. Αν από την άλλη τους δοθεί έτοιμο το password τότε επιλέγουν να το σημειώσουν παρά να το αποστηθίσουν. Στη χειρότερη περίπτωση θα ανακαλύψει κάποιος το password σε σημείωμα κολλημένο στο πλάι της οθόνης του υπολογιστή του χρήστη. Η ορθότερη επιλογή είναι το password να αποτελείται από συνδυασμό γραμμάτων και αριθμών.

[17] Pfleeger, C., P., 1997, "*Security in Computing*", Prentice Hall

2ος Κίνδυνος

Προκειμένου τα passwords να εξασφαλίζουν προστασία πρέπει τακτικά να αντικαθίστανται από νέες επιλογές. Οι χρήστες δυστυχώς αποφεύγουν αυτή την αλλαγή ή επιλέγουν να ανακυκλώνουν ένα μικρό αριθμό από passwords. Καλό θα ήταν η τακτική αλλαγή τους να επιβάλλεται από το ίδιο το λογισμικό.

3ος Κίνδυνος

Εάν κάποιος έχει λογαριασμούς σε διαφορετικούς υπολογιστές ή sites στο internet θα πρέπει για λόγους ασφαλείας να χρησιμοποιεί διαφορετικά passwords για την είσοδό του σε κάθε σύστημα ή ιστοσελίδα. Ασφαλώς, κάτι τέτοιο είναι ιδιαίτερα δύσκολο για τον χρήστη και το πιθανότερο είναι κάπου να τα σημειώσει προκειμένου να μην τα ξεχάσει. Από την άλλη μεριά η ύπαρξη ενός μόνο password αυξάνει την πιθανότητα από κάπου να αποκαλυφθεί. Σε κάθε περίπτωση η όσο το δυνατόν συχνότερη αντικατάστασή τους είναι μια καλή και ενδεδειγμένη πρόταση.

4ος Κίνδυνος

Είναι προφανές πως το σημείο που το σύστημα ή το δίκτυο αποθηκεύει τα διάφορα passwords είναι σημείο που απαιτεί αυξημένη ασφάλεια αφού αποτελεί βασικό στόχο για εισβολή. Ο συνηθισμένος τρόπος για να περιορίζεται ο κίνδυνος είναι να μην αποθηκεύονται ως κείμενο, ούτε ακόμη και με κρυπτογράφηση (encrypted), αλλά με τη μορφή που έχει το καθένα ως συνάρτηση hash. Η αντιστροφή της τιμής της συνάρτησης στο αντίστοιχο password είναι εξαιρετικά δύσκολη και έτσι τα passwords, ναι μεν δεν μπορούν να ανακτηθούν, αλλά εύκολα μπορεί να γίνεται ο έλεγχος ανάμεσα στο αποθηκευμένο password και σε αυτό που πληκτρολογείται κατά την είσοδο ενός χρήστη. Στις μεθόδους για επιβεβαίωση της ταυτότητας κάποιου χρήστη εκτός από τα passwords, συμπεριλαμβάνονται ακόμη[18]:

Passwords μιας χρήσης

[18] Meinel, C., P., 1998, "*The Happy Hacker"*, American Eagle Publications

Ένα πρόβλημα που αντιμετωπίζει η τεχνολογία των passwords είναι πως αν μεταδοθεί από μη ασφαλές τηλεπικοινωνιακό κανάλι τότε αυξάνεται αισθητά ο κίνδυνος να έχει υποκλαπεί. Μία λύση στο πρόβλημα είναι ο κάθε χρήστης να έχει ένα σύνολο από passwords που το καθένα θα μπορεί να χρησιμοποιηθεί μόνο μια φορά. Ένα τέτοιο σύστημα είναι το S/Key το οποίο χρησιμοποιεί μία συνάρτηση η οποία παράγει την αλυσίδα των διαδοχικών password. Στην πράξη κάθε έγκυρο password αντικαθίσταται στη συνάρτηση και έτσι σχηματίζεται το επόμενο.

Smart Cards

Πρόκειται για μικρές κάρτες -αντίστοιχες με τις πιστωτικές- οι οποίες περιέχουν έναν επεξεργαστή, κάποια μνήμη και μια διασύνδεση με το εξωτερικό περιβάλλον. Χρησιμοποιούνται σε μία σειρά εφαρμογών συμπεριλαμβάνοντας και την ηλεκτρονική πληρωμή. Εκτελούν τρεις βασικές λειτουργίες: Αποθήκευση και διαχείριση πληροφοριών, επιβεβαίωση της ταυτότητας του χρήστη, καθώς και κρυπτογράφηση-αποκρυπτογράφηση. Το πλεονέκτημά της ως προς την ασφάλεια είναι ότι λειτουργεί σε ένα απομονωμένο περιβάλλον.

Σήμερα υπάρχει μία μεγάλη γκάμα από smart cards, οι οποίες μεταξύ τους διαφέρουν στην απόδοση και την ικανότητα του επεξεργαστή, το μέγεθος της μνήμης καθώς και την ταχύτητα διασύνδεσης με το εξωτερικό περιβάλλον. Για να λειτουργήσει απαιτείται η ύπαρξη της συσκευής που θα "διαβάσει" την smart card. Υπάρχουν διαφόρων ειδών τέτοιες συσκευές ανάλογα με τι είδους τεχνολογία διαθέτουν. Έτσι έχουμε συσκευές που διαβάζουν την smart card όταν αυτή τοποθετηθεί στην ειδική σχισμή και άλλες που είναι χωρίς επαφή και τη "διαβάζουν" με τη βοήθεια υπέρυθρων ακτινών[19]. Είτε με την πρώτη, είτε με τη δεύτερη μέθοδο, επιτυγχάνεται η απαραίτητη ανταλλαγή δεδομένων ανάμεσα σε κάρτα και συσκευή ανάγνωσης και έτσι γίνεται ο έλεγχος της ταυτότητας του χρήστη.

Antivirus

[19] Pfleeger, C., P., 1997, "*Security in Computing*", Prentice Hall

Παρά την ύπαρξη περίπου πενήντα χιλιάδων ιών, σύμφωνα με το Norton Antivirus (προφανώς πρέπει να είναι ιδιαίτερα διασκεδαστικός ο σχεδιασμός τους, ώστε να δικαιολογείται το πλήθος τους), εάν τηρηθούν μερικοί βασικοί κανόνες, ελαχιστοποιούμε τον κίνδυνο μόλυνσης. Εκτός από την αναβάθμιση των εφαρμογών που σχετίζονται με το Internet, είναι πλέον επιβεβλημένη η εγκατάσταση στο πληροφοριακό σύστημα κάποιας εφαρμογής προστασίας από τους ιούς. Μετά την εγκατάσταση θα πρέπει να γίνεται εβδομαδιαία ενημέρωση από τους δημιουργούς του antivirus (μέσω Internet κατά προτίμηση), ώστε να υπάρχει αυξημένο επίπεδο προστασίας απέναντι και στους νεότερους των ιών[20].

Με την τεράστια εξάπλωση των ιών και των σκουληκιών που χρησιμοποιούν κυρίως το e-mail για να εξαπλωθούν, θα πρέπει το antivirus να είναι ικανό να ελέγχει και την εισερχόμενη αλληλογραφία της εταιρείας, προστατεύοντας έτσι το σύστημα από τον βασικότερο τρόπο εγκατάστασης των ιών από το εξωτερικό περιβάλλον. Με αυτό τον τρόπο συλλαμβάνονται τα κακόβουλα προγράμματα, προτού φτάσουν στο ηλεκτρονικό γραμματοκιβώτιο της εταιρείας.

Βέβαια, οι εφαρμογές προστασίας δεν λειτουργούν πάντα καλά, με συνέπεια να παρουσιάζονται περιστασιακά προβλήματα στη λήψη της αλληλογραφίας, αλλά μπροστά στον υπαρκτό κίνδυνο, τα συγκεκριμένα προβλήματα είναι αποδεκτά. Γενικά, δεν πρέπει να εκτελούνται επισυναπτόμενα αρχεία, εάν δεν υπάρχει βεβαιότητα για την καθαρότητά τους. Ακόμα και αν φαίνονται αθώα (μια εικόνα jpg, για παράδειγμα) ή προέρχονται από γνωστό αποστολέα, δεν αποκλείεται το αρχείο να είναι εκτελέσιμο και να έχει τη μορφή picture.jpg.exe (όπως, π.χ., συμβαίνει σε έναν πρόσφατο δούρειο ίππο του ICQ).

Να ξεκαθαρίσουμε ότι ελάχιστες είναι οι πιθανότητες να μολυνθεί το σύστημα ανοίγοντας απλώς ένα e-mail. Θα πρέπει να εκτελεστεί ο επισυναπτόμενος, καμουφλαρισμένος, κακόβουλος κώδικας. Προσοχή χρειάζεται και με τα αρχεία word και excel που λαμβάνονται, τα οποία καλό θα είναι να περνούν από έλεγχο για μακροϊούς. Επίσης, πρέπει να προσεχθούν και οι διάφορες εφαρμογές που εγκαθίστανται, ειδικά εάν προέρχονται από αμφιλεγόμενες

[20] Denning, D., E., 2007, "*Cryptography and Data Security*", Addison – Wesley

πηγές. Η παρουσία του antivirus προστατεύει επίσης το σύστημα και από τους εσωτερικούς κινδύνους για την περίπτωση που κάποιος χρήστης είτε εν αγνοία του, είτε εσκεμμένα προσπαθήσει να εγκαταστήσει έναν τέτοιο ιό. Άλλωστε ο κίνδυνος των δολιοφθορών εκ των έσω πρέπει να βρίσκεται ιδιαίτερα ψηλά στην ιεραρχία των κινδύνων, για το σχεδιαστή του συστήματος ασφαλείας.

Όλα τα παραπάνω είναι πολύ καλά για την πρόληψη. Τι πρέπει να γίνεται όμως στην περίπτωση που το πληροφοριακό σύστημα μολυνθεί από κάποιον ιό; Αυτό είναι κάτι που διαπιστώνεται με την παρατήρηση βασικών χαρακτηριστικών και συμπεριφορών του υπολογιστή. Εάν ξαφνικά αρχεία εμφανίζονται ή εξαφανίζονται, το σύστημα γίνεται πιο αργό, μειώνεται η διαθέσιμη μνήμη, εφαρμογές αρνούνται να τρέξουν ή παράξενα μηνύματα εμφανίζονται στην οθόνη, όλα αυτά είναι ενδείξεις που "φωτογραφίζουν" την παρουσία ιού. Η αμέσως επόμενη κίνηση είναι να ελεγχθεί ο υπολογιστής με κάποιο antivirus.

Αφού εντοπιστεί ο ιός και καθαρίσει το σύστημα, καλό θα ήταν να δημιουργηθούν δισκέτες ασφαλείας, διαδικασία η οποία συνήθως προσφέρεται από το antivirus πρόγραμμα που χρησιμοποιείται από το σύστημα. Οι δισκέτες αυτές δίνουν τη δυνατότητα να εκκινηθεί το σύστημα και να γίνει έλεγχος για ιούς, ενώ μπορεί να περιέχουν και αντίγραφα των τομέων εκκίνησης του σκληρού δίσκου σε περίπτωση μόλυνσης του boot sector[21].

1.4 Κρυπτογραφικά Συστήματα για Ασφάλεια Δεδομένων σε Ηλεκτρονικούς Υπολογιστές και Τρόπος Εφαρμογής τους

Κρυπτογραφία (cryptography) είναι η μελέτη τεχνικών που βασίζονται σε μαθηματικά προβλήματα δύσκολο να λυθούν. Κρυπτανάλυση (cryptanalysis) είναι η επίλυση αυτών των προβλημάτων και κρυπτολογία (cryptology) είναι ο συνδυασμός της κρυπτογραφίας και κρυπτολογίας σε ένα ενιαίο επιστημονικό κλάδο. Εφαρμογή της κρυπτογραφίας είναι η κρυπτογράφηση. Κρυπτογράφηση είναι ο μετασχηματισμός δεδομένων σε μορφή που να είναι αδύνατον να διαβαστεί χωρίς την γνώση της σωστής ακολουθίας bit. Η

[21] Meinel, C., P., 1998, "*The Happy Hacker"*, American Eagle Publications

ακολουθία bit καλείται "κλειδί" και χρησιμοποιείται σε συνδυασμό με κατάλληλο αλγόριθμο / συνάρτηση[22].

Η αντίστροφη διαδικασία είναι η αποκρυπτογράφηση και απαιτεί γνώση του κλειδιού. Σκοπός της κρυπτογράφησης είναι να εξασφαλίσει το απόρρητο των δεδομένων κρατώντας τα κρυφά από όλους όσους έχουν πρόσβαση σε αυτά. Η κρυπτογράφηση και η αποκρυπτογράφηση απαιτούν, όπως είπαμε, την χρήση κάποιας μυστικής πληροφορίας, το κλειδί. Για μερικούς μηχανισμούς χρησιμοποιείται το ίδιο κλειδί και για την κρυπτογράφηση και για την αποκρυπτογράφηση, για άλλους όμως τα κλειδιά που χρησιμοποιούνται διαφέρουν[23].

Η κρυπτογραφία αναφέρεται στην υλοποίηση μεθόδων τροποποίησης των μεταδιδομένων πληροφοριών, έτσι ώστε να γίνονται κατανοητά μόνο από τον προβλεπόμενο παραλήπτη ή παραλήπτες. Είναι μια διαδικασία που μπορεί να εκτελεστεί τόσο σε hardware όσο και σε software. Η ενσωμάτωση των μεθόδων της κρυπτογραφίας σε hardware επιταχύνει σε μεγάλο βαθμό την διεκπεραίωση της. Επίσης, οι χρήστες δεν γνωρίζουν, ούτε καν αντιλαμβάνονται την παρουσία της και πραγματοποιούν ανενόχλητοι τις εργασίες τους. Το γεγονός ότι ο χρήστης δεν ανακατεύεται καθόλου στις διαδικασίες της κρυπτογραφίας, αυξάνει την αποτελεσματικότητα του εργαλείου στην παρεχόμενη ασφάλεια. Παρ' όλα αυτά, δεν έχει καθιερωθεί η κρυπτογραφία σε hardware λόγω του υψηλού κόστους της, που απαγορεύει την αγορά και διατήρηση των ειδικών μηχανημάτων που χρειάζονται για την εφαρμογή της. Τα ειδικά αυτά μηχανήματα βρίσκονται τοποθετημένα σε στρατηγικά σημεία κάθε δικτύου[24].

Η λέξη κρυπτογραφία προέρχεται από τα συνθετικά "κρυπτός" + "γράφω" και είναι ένας επιστημονικός κλάδος που ασχολείται με την μελέτη, την ανάπτυξη και την χρήση τεχνικών κρυπτογράφησης και αποκρυπτογράφησης με σκοπό την απόκρυψη του περιεχομένου των μηνυμάτων. Στις μέρες μας κρυπτογραφία δεν είναι μόνο κρυπτογράφηση και αποκρυπτογράφηση. Εκτός

[22] Denning, D., E., 2007, "*Cryptography and Data Security*", Addison – Wesley

[23] Schneier, B., 1996, "*Applied Cryptography*", Prentice Hall

[24] Denning, D., E., 2007, "*Cryptography and Data Security*", Addison – Wesley

από την διασφάλιση του απόρρητου (privacy), η πιστοποίηση ταυτότητας (authentication) είναι άλλη μία έννοια που έχει γίνει μέρος της ζωής μας. Πιστοποιούμε την ταυτότητα μας καθημερινά και ανεπαίσθητα, για παράδειγμα όταν υπογράφουμε ένα έγγραφο, όταν δείχνουμε την ταυτότητα μας. Καθώς ο κόσμος εξελίσσεται σε ένα περιβάλλον που όλες οι αποφάσεις και οι συναλλαγές θα γίνονται ηλεκτρονικά, χρειαζόμαστε ηλεκτρονικές τεχνικές που θα επιτελούν την πιστοποίηση της ταυτότητας μας[25].

Η κρυπτογραφία παρέχει μηχανισμούς για τέτοιες διαδικασίες. Η ψηφιακή υπογραφή συνδέει ένα έγγραφο με τον κάτοχο ενός κλειδιού έτσι ώστε όλοι όσοι είναι σε θέση να το αναγνώσουν να είναι σίγουρη για το ποιος το έχει γράψει. Επίσης, μία ψηφιακή χρονοσφραγίδα (digital timestamp) συνδέει ένα έγγραφο με την ώρα της δημιουργίας του. Τέτοιο μηχανισμοί μπορούν να χρησιμοποιηθούν για έλεγχο πρόσβασης σε ένα σκληρό δίσκο, για ασφαλής συναλλαγές μέσω του Διαδικτύου ή ακόμα και για σύνδεση με καλωδιακή τηλεόραση[26].

2. Κεφάλαιο Δεύτερο : Είδη Ιών σε Ηλεκτρονικούς Υπολογιστές και ο Ιός των Worms

2.1 Είδη Περιπτώσεων και Ιών που Εισβάλουν σε Ηλεκτρονικούς Υπολογιστές για Κακόβουλες Ενέργειες

Βασικό τμήμα του σχεδιασμού ενός συστήματος ασφαλείας οικονομικών συναλλαγών, αποτελεί να εξακριβώσουμε τι επίπεδο ασφάλειας χρειάζεται και ποιές απειλές θα κληθεί να αντιμετωπίσει. Η επιλογή των μέτρων προστασίας γίνεται λαμβάνοντας υπόψη τι κόστος (οικονομικό, απόδοσης ή ενόχλησης λόγω της παρουσίας τους) έχουν για την εταιρεία. Το πρώτο λοιπόν, βήμα είναι να εντοπίσουμε τον εχθρό. Συνήθως οι άνθρωποι επικεντρώνονται στο είδος της επίθεσης ξεχνώντας ότι οι επιθέσεις είναι τα εργαλεία. Για

[25] Schneier, B., 1996, "*Applied Cryptography*", Prentice Hall

[26] Denning, D., E., 2007, "*Cryptography and Data Security*", Addison – Wesley

παράδειγμα, ένας αποφασισμένος εισβολέας θα επιμείνει πολύ περισσότερο από ένα τυπικό εισβολέα. Έτσι, παρόλο που θα χρησιμοποιηθούν τα ίδια είδη επίθεσης, η επιμονή μπορεί να είναι αυτή που θα αποβεί καταλυτική για την επιτυχία ή μη της επίθεσης. Για το λόγο αυτό είναι σημαντικό να έχουμε προσδιορίσει[27]:

- Ποιοί είναι οι εχθροί μας.
- Ποιές είναι οι προθέσεις τους
- Ποιά είναι τα μέσα τους

Οι εν δυνάμει εχθροί ενός πληροφοριακού συστήματος οικονομικών συναλλαγών κατηγοριοποιούνται στις ακόλουθες ομάδες[28]:

Hackers - Crackers

Είναι οι "αναρχικοί" του κυβερνοχώρου που εισβάλουν στα πληροφοριακά συστήματα είτε για διασκέδαση, είτε για να καταστρέψουν, είτε για επίδειξη. Τους ελκύουν όλοι οι απαγορευμένοι χώροι. Πολλές εταιρείες συνηθίζουν να προσλαμβάνουν άτομα που εισέβαλαν στα συστήματά τους με τη λογική "Καλύτερα να δουλεύουν για μας παρά εναντίον μας". Άλλωστε αυτοί που παραβίασαν ένα σύστημα ασφαλείας ξέρουν καλύτερα από τον καθένα που μειονεκτεί και μπορούν να το βελτιώσουν.

Κλέφτες

Είναι όλοι αυτοί που εισβάλουν σε ένα σύστημα έχοντας ως στόχο την κλοπή δεδομένων που θα τους αποφέρει οικονομικά οφέλη είτε χρησιμοποιώντας τα, είτε πουλώντας τα.

Ανταγωνιστές

[27] Denning, D., E., 2007, "*Cryptography and Data Security*", Addison – Wesley

[28] Schneier, B., 1996, "*Applied Cryptography*", Prentice Hall

Ένας ανταγωνιστής συνήθως, δεν εισβάλει για να κλέψει χρήματα, ούτε για να καταστρέψει αλλά για να αποκτήσει πληροφορίες που είναι σημαντικές προκειμένου να κυριαρχήσει στον "επιχειρηματικό πόλεμο".

Εσωτερικοί εχθροί

Δυσαρεστημένοι, αποξενωμένοι και άπληστοι υπάλληλοι μπορούν να αποτελέσουν ένα ιδιαίτερα σοβαρό εκ των έσω κίνδυνο για τις βάσεις δεδομένων μιας εταιρείας.

Ατυχήματα

Πολλές καταστροφές δεν είναι αποτέλεσμα πρόθεσης ούτε οργανωμένης επίθεσης, αλλά πρόκειται για ατυχήματα ή λάθη από αφέλεια. Δεν είναι καθόλου ασυνήθιστο γεγονός εταιρείες να καταστρέφουν από μόνες τους τις βάσεις δεδομένων τους, ή να τις απελευθερώνουν στο internet κατά λάθος.

Έχοντας γνωρίσει τους πιθανούς εισβολείς ενός συστήματος, εν συνεχεία, περιγράφουμε τους τρόπους που έχουν οι crackers για να αποκτούν παράνομη ή έστω παράτυπη πρόσβαση σε υπολογιστικά συστήματα, τα εργαλεία που χρησιμοποιούν για να κερδίζουν τον έλεγχο σε υπολογιστές, καθώς και τις διαθέσιμες τεχνικές στις οποίες καταφεύγουν για να προκαλούν ζημιές ή να «γονατίζουν» ένα σύστημα, ανεξαρτήτως της ισχύος του. Στο ξεχωριστό κείμενο στο τέλος της ενότητας περιέχεται ένα σύντομο γλωσσάρι με τεχνικούς όρους, η γνώση των οποίων βοηθά στην καλύτερη κατανόηση όσων ακολουθούν. Εξάλλου, αν και επικρατεί η αντίληψη ότι οι crackers είναι άνθρωποι με υψηλό επίπεδο τεχνογνωσίας, καθώς και με άπειρα αποθέματα υπομονής και επιμονής, δυστυχώς διαπιστώνουμε ότι οι αρετές αυτές δεν είναι απαραίτητη προϋπόθεση για να μπορέσει κάποιος να μας προκαλέσει πονοκεφάλους ακόμα και ζημιές.

Τύποι επιθέσεων

Μία από τις πλέον διάσημες και αποτελεσματικές μεθόδους που χρησιμοποιούν οι crackers για να θέτουν εκτός λειτουργίας δικτυωμένους υπολογιστές ενός συστήματος ασφαλείας οικονομικών συναλλαγών είναι οι επιθέσεις DoS (Denial of Service attacks). Το όνομα της τεχνικής (άρνηση εξυπηρέτησης) οφείλεται στο γεγονός ότι ο υπολογιστής-θύμα για ένα χρονικό διάστημα δεν είναι σε θέση να εξυπηρετεί αιτήσεις μηχανημάτων-πελατών (clients), εξαιτίας του τεράστιου πλήθους κίβδηλων αιτήσεων (bogus requests) που δέχεται από τον επιτιθέμενο[29].

Υπάρχουν διάφορα είδη επιθέσεων DoS, πολλά από τα οποία εκμεταλλεύονται εγγενείς αδυναμίες του ζεύγους πρωτοκόλλων TCP/IP. Για τα περισσότερα από αυτά είναι ήδη γνωστά τα αντίστοιχα μέτρα προστασίας. Συγκεκριμένα, οι διαχειριστές συστημάτων μπορούν να εγκαθιστούν patches σε λειτουργικά συστήματα και προγράμματα - διακομιστές, ώστε να αποτρέπουν επιθέσεις DoS ή να ελαχιστοποιούν τις συνέπειές τους. Όπως, όμως, συμβαίνει και με τους ιούς υπολογιστών, κατά καιρούς εφευρίσκονται νέα είδη ή παραλλαγές επιθέσεων DoS. Παραθέτουμε εν συντομία τέσσερις από τις διασημότερες παραλλαγές, σε αλφαβητική σειρά.

Ping of death

Αίτηση PING ή, αλλιώς, αίτηση ICMP, προς τον υπολογιστή-στόχο, με άκυρο μέγεθος πακέτου στην κεφαλή (header) του τελευταίου (πάνω από 64Kb). Τέτοια «παράτυπα» πακέτα μπορούν να «κρεμάσουν» υπολογιστές που τρέχουν λειτουργικά συστήματα ανίκανα να τα μεταχειριστούν[30].

Smurf Attack

Επιτυγχάνεται αποστέλλοντας αιτήσεις ICMP σε μια διεύθυνση εκπομπής (broadcast address) στο υπό επίθεση δίκτυο ή σε κάποιο άλλο, ενδιάμεσο. Η διεύθυνση επιστροφής (return address) των πακέτων ICMP πλαστογραφείται, ώστε να είναι ίδια με αυτήν του υπολογιστή-στόχου. Από τη στιγμή που μια διεύθυνση εκπομπής αντιστοιχεί σε όλα τα μηχανήματα ενός υποδικτύου,

[29] Schneier, B., 1996, "*Applied Cryptography*", Prentice Hall

[30] Schneier, B., 1996, "*Applied Cryptography*", Prentice Hall

λειτουργεί ενισχυτικά, δημιουργώντας από μία μόνο αίτηση ICMP δεκάδες ή και εκατοντάδες απαντήσεις, προκαλώντας με τον τρόπο αυτό πληροφοριακό «μποτιλιάρισμα»[31].

Ας σημειωθεί ότι μια διεύθυνση εκπομπής αντιστοιχεί το πολύ σε 255 μηχανήματα (ανήκουν όλα στο ίδιο υποδίκτυο), επομένως κατά τη διάρκεια μιας επίθεσης Smurf, από κάθε αίτηση PING μπορούν να παραχθούν μέχρι και 255 απαντήσεις. Καταλαβαίνουμε, λοιπόν, τον υπέρογκο αριθμό των άχρηστων πακέτων που δημιουργούνται, όταν ο επιτιθέμενος στέλνει εκατοντάδες ή ακόμη και χιλιάδες πακέτα ICMP[32].

Syn flood attack

Πριν εγκαθιδρυθεί μια συνεδρία μεταξύ ενός πελάτη και ενός διακομιστή, λαμβάνει χώρα μια ακολουθία τριών βημάτων, γνωστή και ως «ακολουθία χειραψίας» (handshaking sequence). Εάν ο πελάτης αγνοήσει την τελευταία απάντηση SYN-ACK (SYNchronize ACKnowledge) του διακομιστή, ο τελευταίος θα επιμένει για ένα προκαθορισμένο χρονικό διάστημα. Ένας cracker μπορεί να εκμεταλλευτεί τη συγκεκριμένη συμπεριφορά για να υπερφορτώσει το διακομιστή-θύμα ή ακόμα και για να τον «κρεμάσει». Κατά τη διάρκεια μιας τέτοιας επίθεσης, ο θύτης παραποιεί τη δικτυακή του διεύθυνση (IP address), κρύβοντας με τον τρόπο αυτό τα ίχνη του.

Tear Drop Attack

Ο επιτιθέμενος εκμεταλλεύεται αδυναμίες στην ανασυγκρότηση των πακέτων IP. Όταν ένα τέτοιο πακέτο αποστέλλεται στο Internet, ενδέχεται να ταξιδεύει σε επιμέρους, μικρότερα τμήματα. Κάθε τμήμα περιλαμβάνει στην κεφαλή του ένα πεδίο, όπου εκεί περιγράφεται η θέση του στο αρχικό πακέτο IP. Ο θύτης χρησιμοποιεί ένα πρόγραμμα, ονόματι «Teardrop», το οποίο τεμαχίζει πακέτα IP σε τμήματα με λανθασμένες πληροφορίες στο υπό συζήτηση πεδίο. Όταν ο υπολογιστής-στόχος προσπαθήσει να συναρμολογήσει τα «παραπλανητικά» αυτά τμήματα, θα κολλήσει ή θα επανεκκινήσει, εκτός και αν ο διαχειριστής

[31] Schneier, B., 1996, "*Applied Cryptography*", Prentice Hall

[32] Pfleeger, C., P., 1997, "*Security in Computing*", Prentice Hall

συστήματος έχει φροντίσει να αναβαθμίσει το λειτουργικό με το κατάλληλο patch που διορθώνει το πρόβλημα[33].

Όταν σε μια επίθεση DoS συμμετέχουν περισσότερα του ενός μηχανήματα, έχουμε τις λεγόμενες κατανεμημένες επιθέσεις DDoS (Distributed Denial of Service ή DDoS attacks). Στις επιθέσεις του είδους είναι δυνατόν να συμμετέχουν και προσωπικοί υπολογιστές ακόμα και το PC στο σπίτι μας χωρίς να το γνωρίζουν οι χρήστες τους. Ο επιτιθέμενος cracker κατορθώνει με κάποιον τρόπο να βάλει ένα μικρό πρόγραμμα σε καθένα από τα μηχανήματα που θα συμμετάσχουν εν αγνοία τους στην επίθεση.

Τη στιγμή που θα την εξαπολύσει, στέλνει μια ειδοποίηση σε ένα από αυτά (διακομιστής DDoS). Τότε, εκείνο ειδοποιεί μια συγκεκριμένη χρονική στιγμή καθέναν από τους υπόλοιπους υπολογιστές (πελάτες DDoS) και όλοι μαζί αρχίζουν να βάλλουν κατά του στόχου με πλαστές αιτήσεις. Το αποτέλεσμα είναι εκείνος να «πλημμυρίσει» και να μην μπορεί να ανταποκριθεί σε αιτήσεις νομότυπων πελατών. Ένας καλός τρόπος για να προστατεύουμε τους υπολογιστές μας, ώστε να μη χρησιμοποιούνται εν αγνοία μας, είναι να χρησιμοποιούμε κάποιο προσωπικό πρόγραμμα firewall.

Αν και ένα μηχάνημα που έχει πέσει θύμα επίθεσης DoS ή DDoS μπορεί να επανέλθει σε ομαλή λειτουργία σχετικά εύκολα, υπάρχουν έμμεσες αρνητικές συνέπειες. Αναφερόμαστε σε οικονομικές ζημιές που οφείλονται στο χρόνο που ένας κεντρικός διακομιστής μένει εξουδετερωμένος, καθώς και στον τραυματισμό του κύρους της εταιρείας στην οποία ανήκει ο διακομιστής-θύμα. Είναι γνωστό, εξάλλου, ότι στην διαδικτυακή εποχή ο ανταγωνισμός βρίσκεται μερικά «κλικ» μακρύτερα[34].

Απρόσκλητοι Ωτακουστές

Από τα παλαιότερα εργαλεία που χρησιμοποιούσαν και συνεχίζουν να χρησιμοποιούν οι διαχειριστές συστημάτων για να αναλύουν τη συμπεριφορά δικτύων και να εντοπίζουν (πιθανά) προβλήματα, είναι τα λεγόμενα «sniffer».

[33] Schneier, B., 1996, "*Applied Cryptography*", Prentice Hall

[34] Pfleeger, C., P., 1997, "*Security in Computing*", Prentice Hall

Έτσι ονομάζεται ένα πρόγραμμα που είναι ικανό να «υποκλέπτει» δεδομένα που ταξιδεύουν σε ένα δίκτυο. Εάν το δίκτυο είναι βασισμένο στο TCP/IP, τότε επειδή το sniffer παρακολουθεί πακέτα IP, ονομάζεται και packet sniffer. Εξάλλου, σε ένα δίκτυο τοπολογίας αστέρα, όπως είναι πολλά τοπικά δίκτυα, τα πακέτα που φεύγουν από έναν κόμβο (μηχάνημα) εκπέμπονται προς όλους τους άλλους κόμβους του δικτύου. Ωστόσο, μόνο ο κόμβος για τον οποίο προορίζονται τα πακέτα θα τα χρησιμοποιήσει· οι άλλοι θα τα αγνοήσουν. Εάν, τώρα, ένα πρόγραμμα sniffer είναι εγκατεστημένο σε έναν υπολογιστή με κάρτα δικτύου σε «επιδιδόμενη» κατάσταση (promiscuous mode), τότε το μηχάνημα αυτό θα μπορεί να «βλέπει» όλα τα πακέτα που διακινούνται στο δίκτυο[35].

Οι διαχειριστές συστημάτων κάνουν χρήση των sniffer για να αναλύουν την κυκλοφορία των πακέτων σε ένα δίκτυο και να εντοπίζουν εστίες προβλημάτων. Επίσης, συχνά χρησιμοποιούν περισσότερα του ενός sniffer, στρατηγικά εγκατεστημένα σε διάφορους κόμβους του δικτύου, ώστε να εντοπίζουν εισβολές παρείσακτων. Με άλλα λόγια, τα sniffer μπορούν να λειτουργήσουν και ως ένα σύστημα ανίχνευσης εισβολών (intrusion detection systems). Βλέπουμε, λοιπόν, ότι τα προγράμματα αυτά αποτελούν πολύτιμο εργαλείο για τους διαχειριστές συστημάτων. Ωστόσο, όπως ήδη θα έχει γίνει προφανές, τις υπηρεσίες τους μπορούν να εκμεταλλευτούν και οι crackers, αυτή τη φορά για όχι και τόσο θεάρεστους σκοπούς. Για παράδειγμα, ο cracker μπορεί να χρησιμοποιεί ένα sniffer για να υποκλέπτει κωδικούς πρόσβασης, αριθμούς πιστωτικών καρτών, διάφορα άλλα προσωπικά στοιχεία χρηστών, για να διαβάζει την ηλεκτρονική τους αλληλογραφία κ.λπ..

Ο προφανής τρόπος για να προστατευτεί ένα δίκτυο από την επιβλαβή χρήση των sniffer είναι να υπάρχει αυστηρή επίβλεψη στα προγράμματα που εγκαθιστούν οι χρήστες στους υπολογιστές. Εάν ένας cracker δεν μπορεί να αποκτήσει φυσική πρόσβαση σε κάποιον υπολογιστή, τότε είναι απλώς ανίκανος να εγκαταστήσει ένα sniffer. Άλλος ένας τρόπος για την παρόπλιση των sniffer είναι η αποστολή δεδομένων σε κρυπτογραφημένη μορφή. Το sniffer θα εξακολουθεί να συλλαμβάνει τα πακέτα, μόνο που τώρα δεν θα

[35] Taylor, A., 1999, "*The Hackers*", Routledge

μπορεί να εξαγάγει κάποιο νόημα από τα περιεχόμενά τους. Βεβαίως, στην περίπτωση αυτή υπάρχει πάντοτε ο κίνδυνος της αποκρυπτογράφησης. Για το λόγο αυτό, προτείνεται η χρήση ισχυρής κρυπτογραφίας, με το ανάλογο κόστος σε υπολογιστική ισχύ. Το ζητούμενο, λοιπόν, είναι η χρυσή τομή ανάμεσα στη δύναμη των μεθόδων κρυπτογράφησης από τη μία, και στην ευκολία των χρηστών, από την άλλη[36].

Τέλος, υπάρχει μια ολόκληρη κατηγορία προγραμμάτων που μπορούν να εντοπίζουν ποιοι υπολογιστές σε ένα δίκτυο έχουν κάρτα δικτύου σε επιδιδόμενη κατάσταση. Έτσι, ο διαχειριστής συστήματος μπορεί να ελέγξει εάν κάποιος υπολογιστής τρέχει ένα sniffer, αν έχει δοθεί επίσημη άδεια για την εγκατάστασή του κ.λπ..

Αδιάκριτοι Διαβάτες

Μια άλλη τεχνική που χρησιμοποιούν διαχειριστές και crackers, καθένας για διαφορετικούς σκοπούς, είναι η σάρωση θυρών (port scanning). Πρόκειται για μια διαδικασία αποστολής ερωτημάτων σε διακομιστές, με σκοπό να ληφθούν πληροφορίες για τις υπηρεσίες που προσφέρουν, καθώς και για το χρησιμοποιούμενο επίπεδο ασφαλείας. Από τη στιγμή που ο επίδοξος εισβολέας μάθει ποιες υπηρεσίες προσφέρει το μηχάνημα-στόχος, μπορεί στη συνέχεια να σχεδιάσει την επίθεσή του βασιζόμενος σε γνωστές αδυναμίες των περί ου ο λόγος υπηρεσιών. Επειδή μια διαδικασία port scanning αφήνει τα ίχνη της στα αρχεία καταγραφής (log files) του λειτουργικού συστήματος, ορισμένοι crackers χρησιμοποιούν ορισμένες «ύπουλες» παραλλαγές.

Μία από αυτές είναι η λεγόμενη «ημι-ανοιχτή σάρωση SYN» (half-open SYN scan). Κατά τη διάρκεια μιας τέτοιας σάρωσης, το πρόγραμμα συνδέεται στα port, αλλά τερματίζει καθεμία ακολουθία σύνδεσης, πριν αυτή ολοκληρωθεί. Από τη στιγμή, λοιπόν, που οι ακολουθίες σύνδεσης δεν ολοκληρώνονται, το λειτουργικό σύστημα στο μηχάνημα-στόχος συνήθως δεν τις καταγράφει, θεωρώντας ότι δεν συνέβησαν ποτέ. Ωστόσο, το πρόγραμμα που κάνει τη σάρωση μπορεί να καταλάβει εάν κάποιο port είναι «ανοιχτό», κρίνοντας από την απάντηση του λειτουργικού συστήματος. Υπάρχουν διάφορα εργαλεία για

[36] Pfleeger, C., P., 1997, "*Security in Computing*", Prentice Hall

το μπλοκάρισμα των port scan. Αυτό που προτείνεται στους απλούς χρήστες είναι η χρήση κάποιου προσωπικού προγράμματος firewall.

Social Engineering

Ακούγεται ειρωνικό αλλά αποτελεί μια πραγματικότητα, το γεγονός ότι μία από τις πιο ύπουλες μεθόδους επίθεσης σε ένα σύστημα ασφαλείας δεν βασίζεται στην τεχνολογία αλλά στην ψυχολογία! Ως "social engineering" ορίζεται η "τέχνη" του να αποκτάς πρόσβαση σε ένα σύστημα, εξαπατώντας τους χρήστες και τους διαχειριστές του και αποσπώντας τους όλες εκείνες τις πληροφορίες που χρειάζονται. Σε ένα πείραμα που έγινε, μια ομάδα από hackers ξεκίνησαν την προσπάθειά τους να διεισδύσουν σε ένα πληροφοριακό σύστημα μεγάλης εταιρείας. Μοναδικό τους όπλο είχαν τον τηλεφωνικό κατάλογο της εταιρείας. Τηλεφώνησαν στην εταιρεία, ζήτησαν να μιλήσουν με την γραμματεία του δικτύου και κατόρθωσαν μέσα σε εικοσιτέσσερις ώρες η ίδια η εταιρεία να τους δημιουργήσει λογαριασμό, να τους δώσει ID και κωδικό μέσω τηλεφώνου και μάλιστα να τους στείλει με courier μέσα στη νύχτα το απαιτούμενο, για την είσοδό τους στο δίκτυο, software.

Δούρειοι Ίπποι

Δεν θα ήταν υπερβολή, εάν λέγαμε ότι ο μεγαλύτερος κίνδυνος μετά τους ιούς, για την πλειονότητα των χρηστών Internet, προέρχεται από τους δούρειους ίππους (Trojan horses). Πρόκειται για προγράμματα που αποτελούνται από δύο μέρη, τον πελάτη και το διακομιστή. Ο διακομιστής «φωλιάζει» με κάποιον τρόπο στον υπολογιστή του θύματος και ο πελάτης τρέχει στο μηχάνημα του θύτη. Από τη στιγμή που ο χρήστης του υπό επίθεση υπολογιστή συνδεθεί με το Internet, το Trojan-διακομιστής, που τρέχει σιωπηρά στο υπόβαθρο (background), στέλνει ένα σήμα το οποίο λαμβάνει το Trojan-πελάτης (στο μηχάνημα του θύτη).

Στη συνέχεια εγκαθιδρύεται μεταξύ τους μια συνεδρία και ο κράκερ αποκτά πρόσβαση στον υπολογιστή-στόχο. Τώρα, ο μακρόθεν έλεγχος του επιτιθέμενου στο άλλο μηχάνημα ποικίλλει, αναλόγως του Trojan. Ο πρώτος

μπορεί απλώς να παίζει με τα νεύρα του ανυποψίαστου χρήστη, π.χ., ανοιγοκλείνοντας το πορτάκι του οδηγού CD-ROM ή εμφανίζοντας γαργαλιστικά μηνύματα στην οθόνη του. Μπορεί όμως και να του διαγράψει αρχεία ή ακόμα και να του προκαλέσει ζημιές στο υλικό του υπολογιστή, όπως, π.χ., να του διαγράψει το BIOS ή να «χτυπήσει» τις κεφαλές του σκληρού δίσκου[37].

Μια άλλη, ύπουλη λειτουργία των δούρειων ίππων είναι η παρακολούθηση και η καταγραφή των πλήκτρων που πιέζει το θύμα. Το Trojan-διακομιστής παρακολουθεί συνεχώς τις κινήσεις του χρήστη. Έτσι, όταν εκείνος πληκτρολογεί κωδικούς πρόσβασης ή αριθμούς πιστωτικών καρτών, το πρόγραμμα τα καταγράφει για να τα στείλει αργότερα στο θύτη. Πώς όμως μπορεί να «μπει» ένα Trojan σε έναν υπολογιστή; Ο συνηθέστερος τρόπος είναι να έρχεται ως επισυναπτόμενο σε κάποιο e-mail ή να βρίσκεται κρυμμένο μέσα σε κάποιο άλλο πρόγραμμα, π.χ., σε ένα παιχνίδι freeware ή shareware, σε κάποιο χρήσιμο, διάσημο εργαλείο κ.λπ. Υπάρχουν δύο τρόποι για να αποφεύγουμε τα Trojan. Ο πρώτος είναι να χρησιμοποιούμε ένα πρόγραμμα «Antivirus» ή «AntiTrojan».

Πολλά προγράμματα του είδους μπορούν να τα ανιχνεύουν όταν τα κατεβάζουμε ακόμα και στην περίπτωση που είναι ήδη εγκατεστημένα στο PC μας και να τα διαγράφουν. Ο άλλος τρόπος είναι να χρησιμοποιούμε ένα προσωπικό firewall. Κάθε φορά που ένα Trojan-διακομιστής θα προσπαθεί να «βγει» στο Internet, το firewall θα μας ειδοποιεί αναλόγως. Είναι προφανές ότι ο συνδυασμός των δύο προηγούμενων μεθόδων παρέχει τη μέγιστη προστασία. Τέλος, καλό είναι να «κατεβάζουμε» στον υπολογιστή μας μόνο «έμπιστα» προγράμματα, από γνωστούς, επίσημους δικτυακούς τόπους.

«Κουνέλια»

Αυτά είναι προγράμματα, που όταν ξεκινήσουν, κάνουν πολλά αντίγραφα του εαυτού τους. Μπορούν να αντιγράψουν τον εαυτό τους στη μνήμη γεμίζοντας τη Ram και πιθανώς να καταρρεύσουν τον υπολογιστή. Σε αντίθεση με τους ιούς, τα κουνέλια δεν προσκολλούν τους εαυτούς τους σε υπάρχοντα αρχεία.

[37] Schneier, B., 1996, "*Applied Cryptography*", Prentice Hall

Παρόλα αυτά, μπορεί να επιχειρήσουν να συγκαλύψουν τους εαυτούς τους υιοθετώντας ένα αθώο όνομα ή ενεργοποιώντας μια ιδιότητα της λίστας κρυφών αρχείων.

Σκουλήκια

Είναι παρόμοια με τα κουνέλια, αλλά είναι ικανά να μεταδοθούν από ένα μηχάνημα στο άλλο επί του δικτύου εκμεταλλευόμενα λογικά κενά σε πρωτόκολλα του διαδικτύου. Τα σκουλήκια (worms) κάνουν χρήση των υπηρεσιών του δικτύου, με ιδιαίτερη προτίμηση στο ηλεκτρονικό ταχυδρομείο, για να πολλαπλασιάζονται και να εξαπλώνονται. Συνήθως δεν μολύνουν αρχεία από τον υπολογιστή που περνούν. Πολύ γνωστές περιπτώσεις, όπως αυτές των Melissa και Love Letter, εξαπλώθηκαν στο δίκτυο με αστραπιαίο ρυθμό. Μάλιστα, το Melissa worm είχε αρχίσει ένα νέο γύρο καλυμμένο αυτήν τη φορά ως έγγραφο του Office για Mac. Η μέθοδος επίθεσης είναι εξαιρετικά ύπουλη, αφού μόλις καταφέρουν να διεισδύσουν σε έναν υπολογιστή, στέλνουν μολυσμένα και καμουφλαρισμένα email σε όλη τη λίστα επαφών του Outlook.

Έτσι, ο ανυποψίαστος χρήστης λαμβάνει ένα e-mail από κάποιον γνωστό του και δείχνοντας εμπιστοσύνη ανοίγει το επισυναπτόμενο αρχείο και μαζί τον ασκό του Αιόλου. Η μαζική αποστολή email, εκτός από την κατασπατάληση του ήδη μικρού εύρους ζώνης του modem σε ατομικό επίπεδο, επιβαρύνει δραματικά τους κεντρικούς διακομιστές αλληλογραφίας του Internet, με αποτέλεσμα να βγαίνουν συχνά εκτός λειτουργίας. Δυστυχώς, όσα μέτρα προστασίας και αν παίρνουμε, πάντοτε τα προγράμματα που χρησιμοποιούμε θα είναι ατελή, υπό την έννοια ότι θα παρουσιάζουν αδυναμίες τις οποίες ενίοτε θα εκμεταλλεύονται οι αποφασισμένοι κράκερ. Πρόκειται για τα λεγόμενα «exploits», προγραμματιστικές αδυναμίες σε γνωστές και ευρέως χρησιμοποιούμενες εφαρμογές, τα οποία μπορούν να αξιοποιούν καταλλήλως οι crackers για να αποκτούν μη εξουσιοδοτημένη πρόσβαση ή έλεγχο σε συστήματα, να προκαλούν ζημιές σε υπολογιστές-στόχους κ. ο. κ. Συχνά, πάντως, οι εταιρείες κυκλοφορούν αναβαθμίσεις ή διορθώσεις (bug fixes, patches) προγραμμάτων με γνωστά προβλήματα[38].

[38] Schneier, B., 1996, "*Applied Cryptography*", Prentice Hall

2.2 Τι Είναι ο Ιός - Συνοπτική Περιγραφή του

Αναμφίβολα το Internet έδωσε μεγάλη ώθηση στην εξάπλωση των πάσης φύσεως ιών και «μικροβίων». Στις μέρες της Amiga και των PC XT ο μόνος τρόπος για να «κολλήσει» κάποιος ένα ειδεχθές πρόγραμμα ήταν να χρησιμοποιήσει μολυσμένες δισκέτες, κυρίως με παιχνίδια. Τότε η μόλυνση με έναν ιό ήταν κάτι το συνηθισμένο μέχρι και γοητευτικό (το γνωστό μπαλάκι που έκανε βόλτες στην οθόνη). Βέβαια, το αστείο τελείωνε με την οδυνηρή ανακάλυψη ότι οι δισκέτες ή ο σκληρός δίσκος ήταν άχρηστα. Η κατάσταση άλλαξε δραματικά με την είσοδο του Internet στη ζωή μας, και συγκεκριμένα με το e-mail. Το ηλεκτρονικό ταχυδρομείο εκμηδένισε τις αποστάσεις και έκανε την επικοινωνία ανάμεσα στους εταιρικούς και τους οικιακούς χρήστες πολύ εύκολη και ευχάριστη υπόθεση. Το email όμως είναι προς το παρόν το κυριότερο μέσο για τη μετάδοση κάθε είδους ιών και σκουληκιών, μετατρέποντάς τα σε πραγματική επιδημία λόγω της μεγάλης ταχύτητας με την οποία εξαπλώνονται.

Στη συντριπτική τους πλειονότητα οι ιοί, τα σκουλήκια και οι δούρειοι ίπποι δεν μπορούν να προκαλέσουν καμία ζημιά, εάν δεν τρέξετε τα εκτελέσιμα αρχεία/script που τα μεταφέρουν. Η κακόβουλη αυτή εφαρμογή μπορεί να έχει καλυφθεί κάτω από το μανδύα μιας εικόνας ή ενός κειμένου word, παραπλανώντας σας ή κάνοντας πολύ δύσκολο τον εντοπισμό της από το χρήστη. Ας πάρουμε όμως τα πράγματα από την αρχή.

Όταν αναφερόμαστε σε ιούς, εννοούμε προγράμματα τα οποία έχουν δημιουργηθεί για να εισέλθουν στον υπολογιστή χωρίς την έγκρισή μας και να μολύνουν άλλα αρχεία. Είναι μικρά κομμάτια ηλεκτρονικού κώδικα, που έχουν τη δυνατότητα να αντιγράφουν και να εισάγουν τον εαυτό τους σε ένα εκτελέσιμο πρόγραμμα, αρχείο, δισκέτα ή μέρος σκληρού δίσκου. Ανάλογα με τη φύση του ιού, οι συνέπειες από τη μόλυνση μπορεί να είναι μηδαμινές έως και καταστροφικές. Ο ιός θα προσπαθήσει να αναπαραχθεί και να εξαπλωθεί, μολύνοντας όσο το δυνατόν περισσότερα αρχεία ή άλλους υπολογιστές σε τοπικό επίπεδο ή στο Internet. Υπάρχουν αρκετά ήδη ιών[39]:

[39] Pfleeger, C., P., 1997, "*Security in Computing*", Prentice Hall

- αυτοί που προσβάλλουν τον τομέα εκκίνησης μιας δισκέτας ή ενός σκληρού δίσκου (boot sector viruses) και είναι σχετικά σπάνιοι σήμερα,
- αυτοί που περιέχονται σε εκτελέσιμα αρχεία (Program/File viruses),
- αυτοί που εκμεταλλεύονται τις γλώσσες μακροεντολών, όπως, π.χ., του Word και του Excel (Macro viruses), και
- οι πολυμορφικοί, οι οποίοι μπορεί να ανήκουν σε μερικές ή όλες τις προαναφερθείσες κατηγορίες. Υπάρχει και μία ειδική κατηγορία ιών, η οποία εκμεταλλεύεται αδυναμίες γνωστών εφαρμογών, όπως, για παράδειγμα, το Outlook Express, με αποτέλεσμα ένα απλό e-mail κειμένου να μπορεί να κάνει τη ζημιά.

Βέβαια, οι ιοί αυτοί είναι σπάνιοι και παροπλίζονται με την εγκατάσταση νεότερων εκδόσεων των προβληματικών εφαρμογών. Σε αυτό το σημείο οι ειδικοί μας προτρέπουν να αναβαθμίζουμε στη νεότερη έκδοση όλες τις εφαρμογές μας, ειδικά αυτές που σχετίζονται με το Internet. Με αυτό τον τρόπο μειώνονται αρκετά οι πιθανότητες μόλυνσης.

2.2.1 Είδη Ιομορφικών Λογισμικών

Αν και θα μπορούσε κανείς να κατηγοριοποιήσει τους ιούς σε πολλά σκέλη, οι σημαντικότερες κατηγορίες σύμφωνα με επιστημονικά έγγραφα που θα μπορούσε να αναφέρει κανείς ότι είναι οι εξής[40] :

- Τομέας εκκίνησης
- Παρασιτικοί
- Πολυμερείς
- Διανέμοντες στην κύρια μνήμη
- Κρυφοί
- Κρυπτογραφημένοι

[40] Meinel, C., P., 1998, "*The Happy Hacker"*, American Eagle Publications

- Πολυμορφικοί
- Ρετρο-ιοί
- Ιοί που διαγράφουν το τμήμα του ξενιστή
- Μακρο-ιοί

Σχετικές σημαντικές λεπτομέρειες για τις παραπάνω κατηγορίες, είναι οι ακόλουθες :

Τομέας εκκίνησης

Οι συγκεκριμένοι ιοί εγκαθίστανται στον τομέα εκκίνησης ενός «δίσκου» αντικαθιστώντας τις υπάρχουσες ρουτίνες, τις οποίες τοποθετούν σε άλλο μέρος του δίσκου. Αυτό έχει σαν σκοπό να εκτελεστεί τουλάχιστον μια ρουτίνα λόγω μικρής χωρητικότητας του τομέα εκκίνησης. Σε αρκετές περιπτώσεις μετά την εκτέλεσή τους παραμένουν ενεργοί στη μνήμη για να μην ανιχνεύονται. Ο πρώτος ιός τομέα εκκίνησης δημιουργήθηκε στο Πακιστάν το 1986, επηρεάζοντας συγκεκριμένο τύπο δισκετών.

Παρασιτικοί

Είναι μια από τις πρώτες κατηγορίες ιών στον κόσμο των υπολογιστών και μια από τις κατηγορίες με την μεγαλύτερη γκάμα ιών. Ο σκοπός των συγκεκριμένων ιών είναι να λειτουργήσουν σαν παράσιτο σε ένα πρόγραμμα ξενιστή, ενσωματώνοντας τον κώδικα τους στην αρχή στη μέση και στο τέλος του κώδικα του εκτελέσιμου αρχείου. Όταν λοιπόν τεθεί σε λειτουργία το εκτελέσιμο αρχείο παράλληλα θα εκτελεστεί και ο συγκεκριμένος ιός.

Πολυμερείς

Η συγκεκριμένη κατηγορία ιών μολύνει είτε εκτελέσιμα αρχεία είτε στον τομέα εκκίνησης. Όταν μολύνουν εκτελέσιμα αρχεία τότε λειτουργούν σαν παρασιτικοί ιοί και όταν επηρεάζουν τον τομέα εκκίνησης τότε δρουν σαν boot sector viruses.

Διανέμοντες στη Κύρια Μνήμη

Οι συγκεκριμένοι ιοί παραμένουν ενεργοί στην κύρια μνήμη ακόμα και μετά το πέρας της εκτέλεσης του ξενιστή τους. Ο ξενιστής τους μπορεί να είναι ένα εκτελέσιμο αρχείο ή ένας τομέας εκκίνησης δίσκου. Μετά την εκτέλεση του ξενιστή αποκολλώνται από το συγκεκριμένο εκτελέσιμο αρχείο και αυτό-τοποθετούνται στην κύρια μνήμη του συστήματος. Αυτό έχει σαν αποτέλεσμα να μπορούν να αποκτούν τον έλεγχο του συστήματος σε χαμηλό επίπεδο έτσι ώστε να προσθέτουν τμήματα κώδικα σε άλλα εκτελέσιμα αρχεία και να αποφεύγουν την ανίχνευση από τα αντιβιοτικά. Ένας άλλος λόγος που παραμένουν στην μνήμη οι ιοί αυτοί, είναι γατί έχουν την δυνατότητα να μολύνουν άλλους ξενιστές σε συγκεκριμένες χρονικές στιγμές που τα αντιβιοτικά λογισμικά υπολειτουργούν.

Κρυφοί ιοί

Κρυφοί ιοί είναι αυτοί που με συγκεκριμένες μεθόδους αποκρύπτουν την μόλυνση αρχείων που έχουν επηρεάσει ώστε μα μη γίνονται αντιληπτά από τα αντιβιοτικά λογισμικά. Κάθε ιομορφικό λογισμικό αλλά και κάθε αλλαγή ενός αρχείου αλλάζει το *checksum* του με αποτέλεσμα να γίνεται εύκολα αντιληπτό από ένα απλό πρόγραμμα αντί – ιομορφικού λογισμικού. Η συγκεκριμένη μέθοδος αναζήτησης ιών γίνεται ελέγχοντας το *chechsum* του αρχείου με το τωρινό. Αυτό λοιπόν που κάνει η συγκεκριμένη κατηγορία ιών είναι να παραποιεί τα στοιχεία που ζητά ένα πρόγραμμα κατά των ιών. Σε περίπτωση που του ζητηθεί μέγεθος θα στείλει το παλιό μέγεθος, σε περίπτωση που του ζητηθεί να στείλει τις ιδιότητες του αρχείου θα στείλει τις ιδιότητες προτού μολυνθεί. Σε περίπτωση που του ζητηθεί να εκτελέσει το συγκεκριμένο αρχείο, τότε θα εκτελεστεί και ο κρυφός ιός[41].

Κρυπτογραφημένοι ιοί

Η πιο συνηθισμένη ρουτίνα ελέγχου ενός αρχείου για κάποια μόλυνση γίνεται με την μέθοδο σύγκρισης-ταυτοποίησης. Ανιχνεύεται η ύπαρξη ιού συγκρίνοντας τον κώδικα σε αρχεία που ελέγχουν με ακολουθίες κώδικα που

[41] Denning, D., E., 2007, "*Cryptography and Data Security*", Addison – Wesley

ανήκουν σε ήδη ταχτοποιημένους ιούς. Αυτό γίνεται κρυπτογραφώντας το μεγαλύτερο μέρος κώδικα κάποιου ιού και αφήνοντας εκτεθειμένη μια συνηθισμένη ρουτίνα αποκρυπτογράφησης και ένα τυχαίο κλειδί κρυπτογράφησης.

Πολυμορφικοί ιοί

Οι ιοί αυτοί αποτελούν ίσως τους πιο ισχυρούς και δύσκολα ανιχνεύσιμους ιούς από τα αντιβιοτικά λογισμικά που κυκλοφορούν στο εμπόριο. Είναι η μετεξέλιξη των κρυπτογραφημένων ιών με τη διαφορά ότι όταν μολύνουν κάποιο αρχείο μεταβάλλουν τη μορφή τους σε αυτό. Έτσι λοιπόν ο κώδικας του ιού αλλάζει από αρχείο σε αρχείο δυσκολεύοντας τον εντοπισμό τους.

Ρετρο-ιοί

Οι συγκεκριμένοι ιοί έχουν σαν σκοπό την αναποτελεσματικότητα των αντιβιοτικών. Αυτό το επιτυγχάνουν σε περιπτώσεις που τα αντιβιοτικά λογισμικά είναι ευάλωτα, όπως σε περίπτωση ενημέρωσης της επόμενης έκδοσής τους.

Ιοί που διαγράφουν τμήμα του ξενιστή

Αν και οι ιοί μπορούν να διατηρούν την λειτουργικότητα των εκτελέσιμων ξενιστών που προσβάλλουν ώστε να αποφύγουν τον εντοπισμό τους από τα αντιβιοτικά υπάρχουν όμως και ιομορφικά λογισμικά που διαγράφουν ολοκληρωτικά ή και κάποια επιμέρους τμήματα του ξενιστή, αυτό βέβαια τους καθιστά και ιδιαίτερα ανιχνεύσιμους.

Μακρο-ιοί

Η συγκεκριμένη κατηγορία ιών είναι ίσως από τις πιο διαδεδομένες και οι ιοί αυτοί διαδίδονται σχετικά εύκολα μέσω δικτύων ηλεκτρονικού ταχυδρομείου και από αρχείο σε ίδιας επέκτασης αρχείο. Αυτοί μπορεί να αποτελούνται από μια ακολουθία εντολών η οποία διερμηνεύεται αντί να εκτελείται. Συνήθως βρίσκονται σε αρχεία έτοιμων λογισμικών όπως της Microsoft Office οι οποίοι

διερμηνεύονται κατά την εκκίνηση του αρχείου που έχει αιτηθεί ο χρήστης να ανοίξει.

2.3 Τρόποι Αντιμετώπισης Ιών Μέσω Συγκεκριμένων AntiVirus της Αγοράς

Οι ιοί αποτελούν ένα από τα πιο διαδεδομένα λογισμικά. Η ανίχνευσή τους από τον απλό χρήστη του υπολογιστή είναι από δύσκολη έως και αδύνατη . Για την προστασία λοιπόν του υπολογιστή έχει δημιουργηθεί μία ειδική κατηγορ**ία λογισμικού, το λεγόμενο αντιϊκό (antivirus).** Προκειμένου να εξασφαλίσουν την απρόσκοπτη και χωρίς μολύνσεις λειτουργία ενός συστήματος, τα αντιϊκά εκκινούν ταυτόχρονα με το λειτουργικό σύστημα του υπολογιστή, χωρίς εντολές από το χρήστη, και παραμένουν ως διαδικασίες στη μνήμη (memory resident), ώστε να είναι σε θέση να ανιχνεύουν τυχόν μολύνσεις σε πραγματικό **χρόνο. Τα προγράμματα αυτά πρέπει να αναβαθμίζονται σε τακτική βάση, ώστε να είναι σε θέση να αντιμετωπίζουν με επιτυχία τους νέο δημιουργούμενους ιούς. Τα πλέον σύγχρονα αντιϊκά και τα οποία εντοπίζονται στην Ελληνική και παγκόσμια αγορά στις μέρες μας, προσφέροντας σχετική προστασία από ιούς worms, αναφέρονται ως εξής.**

Avira AntiVir Personal

Είναι από τα κορυφαία δωρεάν προγράμματα προστασίας του pc γιατί είναι ικανό να εντοπίζει με επιτυχία όλους τους ιούς και όλες τις κακόβουλες απειλές. Γρήγορο, ικανό, αξιόπιστο είναι μερικά από τα χαρακτηριστικά του. Εκτελείται αθόρυβα στο παρασκήνιο, καταναλώνει ελάχιστους πόρους και ενημερώνεται αυτόματα.

Avast! Free Antivirus

Είναι ένα από τα πιο ισχυρά δωρεάν προγράμματα antivirus της αγοράς. Θα κρατήσει τον υπολογιστή σε τέλεια κατάσταση καθώς είναι ικανό να εντοπίζει τους περισσότερους ιούς, worms και trojans που υπάρχουν στο internet. Έχει ένα μόνιμο σύστημα ενημέρωσης το οποίο σας επιτρέπει να είστε πάντα ενημερωμένοι.

AVG Antivirus Free

Είναι ένα ισχυρό δωρεάν πρόγραμμα που προστατεύει το pc καθώς εντοπίζει και διαγράφει όλων των ειδών τις ηλεκτρονικές απειλές, τους ιούς και τα spyware. Διαθέτει εξελιγμένες και δυνατές μηχανές σκαναρίσματος και ενημερώνεται συνεχώς έτσι ώστε να έχει κανείς πάντα τα πιο καινοτόμα και αξιόπιστα εργαλεία προστασίας.

Pc Tools AntiVirus Free

Προσφέρει δωρεάν βασική προστασία για τον υπολογιστή από κακόβουλο λογισμικό. Διαρκή προστασία σε πραγματικό χρόνο. Κάνει αυτόματα ενημέρωση για νέους ιούς και κακόβουλες απειλές. Η εγκατάσταση, η λειτουργία και η παραμετροποίηση του είναι πολύ εύκολη και δεν θα προβληματίσουν καθόλου.

BitDefender Antivirus Free

Το BitDefender Antivirus Free είναι καλό λογισμικό με όλες τις κλασικές δυνατότητες όπως άμεσο scan αρχείων, προγραμματισμένο scan, quarantine και άλλες πολλές. Επιπλέον μπορείτε να αλλάξετε την εμφάνιση του αφού υπάρχουν πολλά διαφορετικά skin για αυτό το δωρεάν πρόγραμμα.

Panda Cloud Antivirus

Το Panda Cloud Antivirus είναι ένα καλό δωρεάν λογισμικό προστασίας από ιούς και κακόβουλο λογισμικό. Ενσωματώνει πολλές σύγχρονες τεχνολογίες προστασίας από διαδικτυακές απειλές και όχι μόνο. Είναι εύκολο στη χρήση και διαθέτει ένα καλοσχεδιασμένο γραφικό περιβάλλον.

Comodo Antivirus

Είναι ένας ευέλικτος κυνηγός κακόβουλου λογισμικού με πάρα πολλές δυνατότητες. Παραμετροποιήσιμο σε κάθε πτυχή του και με πολλά ενδιαφέροντα χαρακτηριστικά.

McAfee Labs Stinger

Το McAfee Labs Stinger μπορεί να απομακρύνει worms και ιούς από το σύστημα σας μετά από μια μόλυνση, καθώς εμπεριέχει μια μεγάλη βάση δεδομένων για τους πιο σύγχρονους και δημοφιλείς ιούς όπως και τις παραλλαγές τους. Αναγνωρίζει χιλιάδες ιούς, trojans και άλλα συναφή κακόβουλα προγράμματα.

ClamWin Free Antivirus

Το ClamWin είναι ένα antivirus πρόγραμμα ανοιχτού λογισμικού κατάλληλο για όλους, που εδώ και αρκετό καιρό επιδεικνύει πολύ καλά αποτελέσματα στην αντιμετώπιση ιών, spyware και διάφορων άλλων απειλών. Κύριο χαρακτηριστικό του είναι οι μικρές απαιτήσεις σε πόρους συστήματος.

Rising Antivirus Free

Εκτός από την όμορφο περιβάλλον εργασίας του, που θα αρέσει στους περισσότερους χρήστες, το δωρεάν αυτό πρόγραμμα είναι εξοπλισμένο με σωρεία αξιόλογων εργαλείων και δυνατοτήτων που προσφέρουν πραγματικά αληθινή ασφάλεια στον υπολογιστή σας σε πραγματικό χρόνο.

Returnil System Safe Free

Δημιουργεί έναν κλώνο του λειτουργικού σας συστήματος, επιτρέποντας σας να δουλέψετε σε ένα εικονικό περιβάλλον. Στην περίπτωση που μολυνθείτε από κακόβουλο λογισμικό, το αληθινό λειτουργικό δεν θα έχει μολυνθεί ποτέ και το μόνο που χρειάζεται για να εξοντώσει κανείς το πρόβλημα είναι να επανεκκινήσει τον pc του.

Microsoft Security Essentials

Παρέχει προστασία στον οικιακό υπολογιστή σε πραγματικό χρόνο, αποτρέποντας την εισβολή ιών και την εκτέλεση λογισμικού κατασκοπίας και άλλου κακόβουλου λογισμικού. Εγκαθίσταται εύκολα και διατηρείται πάντα ενημερωμένο. Εκτελείται αθόρυβα και αποτελεσματικά στο παρασκήνιο.

ZenOK

Με το δωρεάν antivirus ZenOK μπορεί κανείς να μπλοκάρει ιούς, spyware, επικίνδυνα trojans, worms, bots και rootkits. Προστατεύει τα προσωπικά δεδομένα από phishing ιστοσελίδες και διαφυλάξτε το σύστημα. Μια αξιόπιστη λύση για τον υπολογιστή.

Kingsoft PC Doctor

Είναι ένα δωρεάν antivirus που προσφέρει αποτελεσματική και αποδοτική λύση προστασίας με ταχύτερη λειτουργία και μειωμένη χρήση της cpu. Εντοπίζει τις αναδυόμενες απειλές και καταργεί τις κρυφές απειλές από τον pc σας. Παρέχει επίσης εργαλεία όπως η προστασία συσκευών usb, disk cleaner, καθαρισμό ιστορικού.

NANO AntiVirus

Είναι μια ισχυρή και προηγμένη εφαρμογή σχεδιασμένη να παρέχει προστασία σε πραγματικό χρόνο, δίνοντάς έτσι εγγύηση για την ασφάλεια των πληροφοριών κατά τη διάρκεια του χρόνου εργασίας. Διαθέτει ένα εύχρηστο περιβάλλον και καταναλώνει λίγους πόρους.

Digital Defender Antivirus Free

Ένα πολύ ελαφρύ πρόγραμμα προστασίας από ιούς. Είναι πολύ γρήγορο, δεν δεσμεύει πολλούς πόρους συστήματος και είναι πολύ απλό στην χρήση. Στην δωρεάν έκδοση του προσφέρει ένα βασικό επίπεδο ασφάλειας του pc, από παντός είδος κακόβουλης απειλής.

DriveSentry Desktop

Μια εύχρηστη και αρκετά αποτελεσματική λύση προστασίας του υπολογιστή σας από ανεπιθύμητα στοιχεία. Προσφέρει μηχανή ανίχνευσης και καταπολέμησης ιών και άλλων ανεπιθύμητων προγραμμάτων αλλά και παρακολούθηση των ενεργειών του υπολογιστή σε πραγματικό χρόνο.

eScan Antivirus Toolkit

Είναι ένα δωρεάν εργαλείο που δίνει τη δυνατότητα να ελέγχει και να καθαρίσει τον υπολογιστή από ιούς, spyware, adware και κάθε είδους κακόβουλου λογισμικού, που μπορεί να τον έχουν μολύνει. Δεν χρειάζεται εγκατάσταση και μπορεί να τρέξει απευθείας από μονάδες όπως flash drives ή απο cd.

2.4 Ο Ιός των Worms - Περιγραφή του Συγκεκριμένου Ιού και Χαρακτηριστικά του

Όπως αναφέρθηκε και σε προηγούμενες ενότητες, ο ιός είναι ένα αυτό-παραγόμενο πρόγραμμα υπολογιστή, το οποίο διαδίδεται αντιγράφοντας τον εαυτό του σε κάποιο άλλο κώδικα ή έγγραφο. Ένα ιομορφικό λογισμικό συμπεριφέρεται σαν ένα βιολογικό ιό το οποίο διαδίδεται με την είσοδό του σε ζωντανούς οργανισμούς χωρίς τη βούληση τους[42]. Έτσι λοιπόν είναι μια ακολουθία συμβόλων που όταν εκτελούν κάτω από ορισμένες συνθήκες ή σε ένα ορισμένο περιβάλλον δημιουργούν ένα ακριβές ή παρόμοιο αντίγραφο της ακολουθίας το οποίο και τοποθετούν μέσα στον υπο-μόλυνση υπολογιστή προκαλώντας τις ανάλογες επιπτώσεις.

[42] Meinel, C., P., 1998, "*The Happy Hacker"*, American Eagle Publications

Σχετικά με τον ιό των Worms και στο τρόπο που εκείνος δρα εντός ενός υπολογιστή προκαλώντας σχετικές βλάβες και προβλήματα, θα πρέπει να αναφέρουμε συγκεκριμένους ιούς worms οι οποίοι είναι γνωστοί ως οι χειρότεροι ιοί worms της ιστορίας με συγκεκριμένα χαρακτηριστικά δράσης τους, ως εξής[43].

Ιός Melissa

Την άνοιξη του 1999, ο David Smith δημιούργησε έναν ιό υπολογιστή ο οποίος βασιζόταν σε μια μακρο-εντολή του Microsoft Word. Τον προγραμμάτισε έτσι ώστε να μπορεί να εξαπλώνεται μέσω ηλεκτρονικών μηνυμάτων ηλεκτρονικού ταχυδρομείου. Ο άνδρας αυτός ονόμασε τον ιό Melissa. Χρησιμοποίησε το όνομα μια εξωτικής χορεύτριας στη Φλώριδα. Ο ιός αυτός προκαλούσε τους παραλήπτες στο να ανοίξουν έγγραφο με ένα μήνυμα ηλεκτρονικού ταχυδρομείου όπως «εδώ είναι το έγγραφο που ζητήσατε» Μόλις ενεργοποιηθεί, ο ιός στέλνει σε 50 άτομα της ηλεκτρονικής ατζέντας διευθύνσεων του παραλήπτη. Ο ιός εξαπλώθηκε γρήγορα μετά την του αποστολή στον κόσμο. Η ομοσπονδιακή κυβέρνηση των ΗΠΑ άρχισε να ενδιαφέρεται για το συγκεκριμένο ιό και σύμφωνα με δηλώσεις των αξιωματούχων του FBI στο Κογκρέσο, αφού ο ιός αυτός είχε προκαλέσει χάος σε κρατικά και ιδιωτικά δίκτυα[44].

Η αύξηση της κίνησης του ηλεκτρονικού ταχυδρομείου σε ορισμένες εταιρείες τις ανάγκασε να διακόψουν τα προγράμματα ηλεκτρονικού ταχυδρομείου μέχρι να ελαττωθεί η παρουσία του ιού. Μετά από δίκη, ο Σμιθ έχασε την υπόθεση και έλαβε 20 μήνες φυλάκιση. Το δικαστήριο του επέβαλε πρόστιμο 5.000$ και του απαγόρευσε τη πρόσβαση σε δίκτυα ηλεκτρονικών υπολογιστών. Σε τελική ανάλυση, ο συγκεκριμένος ιός δεν προκάλεσε αβάσταχτη ζημιά στο διαδίκτυο αλλά ήταν ένας από τους πρώτους ιούς υπολογιστών που τράβηξαν την προσοχή του κοινού.

Ιός ILOVEYOU

[43] Denning, D., E., 2007, "*Cryptography and Data Security*", Addison – Wesley

[44] Denning, D., E., 2007, "*Cryptography and Data Security*", Addison – Wesley

Ένα χρόνο μετά τον ιό Melissa, «χτυπά» το διαδίκτυο μια ψηφιακή απειλή που προερχόταν από τις Φιλιππίνες. Σε αντίθεση με τον πρώτο ιό, προήλθε σε μορφή worm. Ήταν ένα αυτοτελές πρόγραμμα με την ιδιότητα να αναπαράγει το εαυτό του. Ο ιός αυτός ταξίδευε ανά τον κόσμο μέσα από το ηλεκτρονικό ταχυδρομείο. Ο τίτλος του μηνύματος των email προκαλούσε τον χρήστη να το ανοίξει λέγοντας του ότι είναι από κάποιο κρυφό του θαυμαστή. Ένα επιπρόσθετο αρχείο στο συγκεκριμένο email ήταν αυτό που προκαλούσε το πρόβλημα.

Η αρχική μορφή του σκουληκιού περιείχε ένα μήνυμα με το όνομα *LOVE LETTER FOR YOU TXT vbs*. Ο προγραμματιστής χρησιμοποίησε μια τεχνική απόκρυψης της επέκτασης του αρχείου στηρίζοντας τις ελπίδες του στην απόπειρα των χρηστών και στην απόκρυψη των επεκτάσεών. Έτσι ο χρήστης μπορούσε να δει μόνο το κομμάτι *LOVE LETTER FOR YOY TXT*. Σύμφωνα με τον ιδιοκτήτη του αντι—ιομορφικού λογισμικού McAfee, ο συγκεκριμένος ιός είχε μεγάλη γκάμα επιθέσεων στο διαδίκτυο :

- Αντέγραφε τον εαυτό του αρκετές φορές και έκρυβε τα αρχεία του σε διαφόρους φακέλους του σκληρού δίσκου του θύματος
- Αντικαθιστούσε διαφορετικά είδη αρχείων με αντίγραφα του ίδιου του ιού
- Έστελνε τον ιό μέσω διαφόρων καναλιών συνομιλίας σαν να είναι κάποιο μήνυμα
- Επίσης κατέβασε ένα αρχείο με το όνομα WIN-BUGSFIX.EXE από το διαδίκτυο και το εκτελούσε στον υπολογιστή του θύματος. Το συγκεκριμένο πρόγραμμα ναι μεν διόρθωνε πολλά λάθη του υπολογιστή αλλά έκλεβε όλους τους κωδικούς του θύματος και τους έστελνε στο ηλεκτρονικό ταχυδρομείο του δημιουργού.

Ποιος δημιούργησε όμως τον ιό αυτό; Κάποιοι πιστεύουν ότι ήταν ο Onel de Guzman από τις Φιλιππίνες. Οι τοπικές αρμόδιες αρχές ερεύνησαν τον υποτιθέμενο προγραμματιστή με τη κατηγορία κλοπής τη στιγμή όμως που δεν είχε αναπτύξει συγκεκριμένο τμήμα ηλεκτρονικού εγκλήματος όπως

επίσης και ανάλογους νόμους. Ο ίδιος επικαλούμενος την έλλειψη ηλεκτρονικών στοιχείων, αφέθηκε ελεύθερος χωρίς να αρνηθεί την ευθύνη εξάπλωσης του ιού. Ο συγκεκριμένος ιός προκάλεσε 10 δις. δολάρια ζημιά.

Ιός KLEZ

Υπήρξε καινοτόμος στην ιστορία των ιών θέτοντας ψηλά τον πήχη για εκείνους που θα τον διαδέχονταν. Έκανε την εμφάνισή του στα τέλη του 2001. Διάφορες παραλλαγές του ιού κατέλυσαν το διαδίκτυο για πολλούς μήνες. Ο βασικός ιός μόλυνε τον υπολογιστή μέσω ενός μηνύματος email, έπειτα πολλαπλασιαζόταν και μεταδιδόταν μέσω της ηλεκτρονικής αλληλογραφίας στις υπόλοιπες επαφές του χρήστη του μολυσμένου υπολογιστή. Κάποιες παραλλαγές του ιού αυτού συνοδεύονταν από άλλα επιβλαβή προγράμματα που καθιστούσαν το μολυσμένο μηχάνημα αδύνατο να λειτουργήσει[45].

Ανάλογα με την έκδοση, ο ιός αυτός μπορούσε να ενεργεί σαν ένας συνήθης ηλεκτρονικός ιός ένα σκουλήκι ή ένας Trojan. Άλλες φορές μπορούσε να εμφανισθεί σαν αντίγραφο αντι-ιομορφικού λογισμικού καθιστώντας άχρηστο και απενεργοποιώντας το ήδη υπάρχον λογισμικό. Μετά την εμφάνισή στο διαδίκτυο κάποιοι τροποποίησαν τον ιό σε πολύ πιο αποτελεσματικό και καταστρεπτικό. Όπως όλοι οι ιοί μπορούσε να σαρώσει ολόκληρη ατζέντα ηλεκτρονικής αλληλογραφίας του χρήστη και να αποσταλεί σε άλλες επαφές.

Είχε τη δυνατότητα να αντικαταστήσει τον αποστολέα στο αντίστοιχο πεδίο με το όνομα κάποιας επαφής. Η διαδικασία αυτή κατά την οποία το email φαινομενικά αποστέλλεται από άλλη πηγή ενώ στην πραγματικότητα προέρχεται από διαφορετικό αποστολέα ονομάζεται spoofing. Αυτό επιτυγχάνεται ως εξής[46]: Αρχικά δε θα ωφελούσε σε τίποτα τον παραλήπτη του φέροντος ηλεκτρονικού μηνύματος να μπλοκάρει τον φαινομενικά αποστολέα πρόβλημα που φαντάζει χαοτικό σε περίπτωση που το «σκουλήκι» έχει προγραμματισθεί να αποστέλλεται σε ρυθμούς spam οπότε και θα ήταν αδύνατο να εντοπισθεί από το χρήστη η αιτία του προβλήματος. Έπειτα ο παραλήπτης του μηνύματος που φέρει τον ιό ενδεχομένως να

[45] Meinel, C., P., 1998, "*The Happy Hacker"*, American Eagle Publications

[46] Denning, D., E., 2007, "*Cryptography and Data Security*", Addison – Wesley

γνώριζε τον εμφανιζόμενο αποστολέα κάτι που θα κέντριζε ακόμα και το ενδιαφέρον του παραλήπτη – θύματος για το περιεχόμενο του μηνύματος[47].

Ιός Code red and Code red II

Τα συγκεκριμένα σκουλήκια εμφανίσθηκαν το καλοκαίρι του 2001. Και τα δυο εκμεταλλεύονταν μια ευπάθεια των λειτουργικών συστημάτων Windows 2000 και Windows NT. Το ευπαθές και αδύναμο σημείο ήταν ένα πρόβλημα υπερχείλισης της προσωρινής μνήμης του υπολογιστή που σήμαινε ότι αν ένα μηχάνημα με τα προαναφερθέντα λειτουργικά συστήματα λάμβανε περισσότερα δεδομένα από όσα μπορούσε να καλύψει τότε ξεκινούσε η διαγραφή της ήδη υπάρχουσας ευπρόσιτης μνήμης. Το αυθεντικό «σκουλήκι» με το όνομα *Code red* έθεσε σε εφαρμογή μια επίθεση Διαμοιρασμένης Άρνησης Παροχής Ενέργειας στο Λευκό Οίκο. Αυτό σημαίνει ότι όλοι οι μολυσμένοι ιοί με των εν λόγω ιό υπολογιστές προσπαθούσαν να έλθουν σε επικοινωνία με τους Web servers εντός του Λευκού Οίκου με άμεσο αποτέλεσμα την υπερφόρτωση των μηχανημάτων.

Ένα μηχάνημα με λειτουργικό σύστημα Windows 2000 μολυσμένο από αυτό το σκουλήκι Code red II, δεν υπακούει στις εντολές του χρήστη. Αυτό συμβαίνει γιατί το σκουλήκι δημιουργεί μια πίσω πόρτα στο λειτουργικό σύστημα του υπολογιστή επιτρέποντας σε ένα απομακρυσμένο χρήστη να αποκτήσει πρόσβαση και έλεγχο του μηχανήματος. Σε τεχνολογικούς όρους, αυτό σημαίνει *system-level compromise*. Το τρίτο αυτό πρόσωπο που δεν είναι άλλο από τον απομακρυσμένο χρήστη μπορεί να έχει πρόσβαση σε πληροφορίες του υπολογιστή ή και να χρησιμοποιήσει το μολυσμένο σύστημα για να διαπράξει ηλεκτρονικά εγκλήματα[48].

Αυτό σημαίνει ότι το θύμα έχει να αντιμετωπίσει όχι μόνο τη μόλυνση αλλά και κάποιες ενδεχόμενες υποψίες για εγκλήματα που πρακτικά διέπραξε. Παρά την ευπάθεια των λειτουργικών συστημάτων Windows NT στο σκουλήκι αυτό, οι επιπτώσεις μια ενδεχόμενης μόλυνσης από τον ιό δεν είχαν ακραία αποτελέσματα. Οι web servers με λειτουργικό windows NT ενδεχομένως να

[47] Denning, D., E., 2007, "*Cryptography and Data Security*", Addison – Wesley

[48] Denning, D., E., 2007, "*Cryptography and Data Security*", Addison – Wesley

αντιμετώπιζαν περισσότερα <<κρεμάσματα>> από το σύνηθες αλλά πρακτικά αυτός ήταν και ο μοναδικός κίνδυνος που ελλόχευε. Η Microsoft ανακοίνωσε τη διανομή λογισμικού που απευθυνόταν σε προστασία του εν λόγω λειτουργικού συστήματος από την εκμετάλλευση της ευπάθειας αυτής και καθιστούσε τα συγκεκριμένα σκουλήκια αβλαβή[49].

Ιός Nimda

Ένας ακόμα ιός που χτύπησε το διαδίκτυο το 2001, ήταν ένα «σκουλήκι» Nimda. Το συγκεκριμένο σκουλήκι διασκορπίστηκε μέσω του διαδικτύου με πολύ γρήγορο ρυθμό ώστε να αποτελεί τον πιο επικίνδυνο ιό εκείνη την εποχή. Στην πραγματικότητα σύμφωνα με τον TruSecure CTO Peter Tippet χρειάστηκαν μόλις 22 λεπτά από τη στιγμή που ο ιός εμφανίσθηκε στο διαδίκτυο για να αγγίξει την κορυφή της λίστας με τις αναφερθείσες επιθέσεις. Οι βασικοί στόχοι αυτού του ιού ήταν οι εξυπηρετητές του διαδικτύου. Αν και είχε τη δυνατότητα να μολύνει έναν οικιακό ιδιωτικό υπολογιστή ο πραγματικός του σκοπός ήταν να προκαλέσει διαδικτυακή συμφόρεση.

Μεταφερόταν από το διαδίκτυο χρησιμοποιώντας διάφορες μεθόδους συμπεριλαμβανομένης και της ηλεκτρονικής αλληλογραφίας κάτι που υπήρξε καθοριστικός παράγοντας για την μόλυνση πολλών servers σε χρόνο ρεκόρ. Ο ιός αυτός δημιούργησε μια πίσω πόρτα στο λειτουργικό σύστημα του θύματος. Επέτρεπε στον απομακρυσμένο χρήστη που επωφελούταν την παράνομη είσοδο στο σύστημα, την πρόσβαση σε οποιεσδήποτε λειτουργίες είχαν πρόσβαση και οι νόμιμοι χρήστες τη στιγμή της μόλυνσης. Με άλλα λόγια αν ένας χρήστης με περιορισμένα δικαιώματα ενεργοποιούσε τον ιό θα είχε ακριβώς απεριόριστα δικαιώματα στο συγκεκριμένο σύστημα και ο υποτιθέμενος χρήστης θα είχε τον έλεγχο. Η εξάπλωση αυτού του ιού είχε σαν αποτέλεσμα ορισμένα δικτυακά συστήματα να «κρασάρουν» καθώς όλο και περισσότεροι πόροι του συστήματος παραδίδονταν στο σκουλήκι. Στο τέλος, ο ιός κατέληξε σαν επίθεση διανεμημένης άρνησης παροχής υπηρεσίας[50].

Ιός SQL Slammer / Sapphire

[49] Denning, D., E., 2007, "*Cryptography and Data Security*", Addison – Wesley

[50] Denning, D., E., 2007, "*Cryptography and Data Security*", Addison – Wesley

Στα τέλη του 2003, ένας ιός βασισμένος σε web server απλώθηκε στο διαδίκτυο. Πολλά δίκτυα υπολογιστών ήταν απροετοίμαστα για αυτή την ηλεκτρονική επίθεση με αποτέλεσμα ο ιός αυτός να αχρηστεύσει πολλά σημαντικά συστήματα. Οι υπηρεσίες των ATM των τραπεζών της Αμερικής αντιμετώπιζαν on line προβλήματα και η πόλη Σηάτλ εντόπισε πρόβλημα σε κλήσεις αμέσου δράσεως. Κάποιες παγκόσμιες αεροπορικές χρειάσθηκαν να ακυρώσουν πολλές πτήσεις λόγω της online υπηρεσίας δέσμευσης εισιτηρίων. Ο ιός slammer υπολογίζεται ότι προκάλεσε ζημιές χρηματικής αξίας ενός δις. δολαρίων πριν αρχίσουν οι εταιρείας να τον αντιμετωπίζουν. Ο ιός μεταδιδόταν με ρυθμούς γεωμετρικής προόδου μετά από 15 λεπτά από την πρώτη επίθεση. Ο ιός αυτός δίδαξε ένα σημαντικό μάθημα στην ιστορία. Ότι ακόμα και υπολογιστικά συστήματα με τρομερή ασφάλεια μπορούν να χτυπηθούν από κάποιο hacker – προγραμματιστή[51].

Ιός My Doom

Ο ιός αυτός είναι ένα ακόμα σκουλήκι που μπορεί να δημιουργήσει μια πίσω πόρτα στο λειτουργικό σύστημα του θύματος. Ο αυθεντικός ιός έχει δυο διακόπτες ενεργοποίησης. Ο πρώτος διακόπτης περιελάμβανε την προγραμματισμένη για την 1 Φεβρουαρίου 2004 έναρξη μιας Dos επίθεσης η αλλιώς μιας επίθεσης άρνησης παροχής υπηρεσιών. Ο δεύτερος περιελάμβανε τη διακοπή αναδιανομής και επέκτασης του ιού. Ακόμα και μετά την διακοπή του ιού, οι πίσω πόρτες που δημιουργήθηκαν κατά την πρωταρχική μόλυνση του συστήματος παρέμεναν ενεργές. Αργότερα την ίδιας χρονιά ένα δεύτερο ξέσπασμα του ιού αυτού είχε σαν αποτέλεσμα πολλές εταιρείες μηχανών αναζήτησης να λυγίσουν. Όπως αρκετοί άλλοι ιοί και αυτός αναζητούσε τα προσβεβλημένα υπολογιστικά συστήματα για ηλεκτρονικές διευθύνσεις σαν μέρος της διαδικασίας αναπαραγωγής και επέκτασής του[52].

Έστελνε αίτηση αναζήτησης σε μηχανές αναζήτησης με σκοπό την χρήση ηλεκτρονικών διευθύνσεων που βρίσκονταν σε αποτελέσματα αναζήτησης. Σύντομα οι μηχανές αναζήτησης άρχισαν να λαμβάνουν εκατομμύρια αιτήσεις

[51] Denning, D., E., 2007, "*Cryptography and Data Security*", Addison – Wesley

[52] Denning, D., E., 2007, "*Cryptography and Data Security*", Addison – Wesley

αναζήτησης από μολυσμένους υπολογιστές. Οι επιθέσεις αυτές καθυστέρησαν πολύ τις μηχανές αναζήτησης με αποτέλεσμα κάποιες από αυτές να παρουσιάσουν και σημαντικές βλάβες. Ο ιός αυτός μεταδιδόταν μέσω ηλεκτρονικής αλληλογραφίας και peer-to-peer συνδέσεις. Σύμφωνα με την εταιρεία ηλεκτρονικής προστασίας και ασφάλειας MessageLabs ένα στα δώδεκα email ήταν φορείς του ιού.

Ιοί Sasser και Netsky

Ορισμένες φορές προγραμματιστές ηλεκτρονικών καταφέρνουν και αποφεύγουν τον εντοπισμό τους. Άλλες πάλι βρίσκουν τρόπο να εντοπίσουν την πραγματική πηγή του ιού. Αυτό συνέβη στην υπόθεση των παραπάνω ιών. Ένας 17χρονος γερμανός εν ονόματι, Sven Jaschan, δημιούργησε δυο προγράμματα και τα απελευθέρωσε στο διαδίκτυο. Παρ' ότι τα δυο σκουλήκια συμπεριφέρονταν με διαφορετικό τρόπο ορισμένες ομοιότητες στον κώδικα οδήγησαν τους ειδικούς ασφαλείας στο συμπέρασμα ότι και τα δυο ήταν δουλειά του ίδιου ανθρώπου[53].

Ο ιός Sasser προσέβαλε τους υπολογιστές μέσω μιας αστάθειας των Microsoft Windows. Αντίθετα από άλλα σκουλήκια δεν εξαπλωνόταν μέσω ηλεκτρονικής αλληλογραφίας. Στη πραγματικότητα αυτός ο ιός αναζητούσε άλλα επιρρεπή συστήματα. Επικοινωνούσε με αυτά τα συστήματα και τους έδινε την εντολή μεταφόρτωσης του ιού. Σάρωνε τυχαίες διευθύνσεις IP για πιθανά θύματα. Επίσης αλλοίωνε το λειτουργικό σύστημα του υπολογιστή με τέτοιο τρόπο ώστε καθιστούσε δύσκολο τον τερματισμό λειτουργίας του συστήματος χωρίς τη διακοπή παροχής ρεύματος. Ο ιός Netsky μεταδιδόταν μέσω email και δικτύων βασισμένων σε λειτουργικά Windows . Ανακάτευε τα εμφανιζόμενα ονόματα σαν αποστολείς και διαδιδόταν μέσω ενός επισυναπτόμενου αρχείου μεγέθους 22,016 bytes[54].

Μπορούσε να προκαλέσει επίθεση Dos καθώς τα συστήματα κατέρρεαν σε μια προσπάθεια να χειριστούν την όλη διαδικτυακή κυκλοφορία. Πολλές φορές θεωρούταν ότι οι ιοί αυτοί αποτελούσαν το 25% όλων των ενεργειών

[53] Denning, D., E., 2007, "*Cryptography and Data Security*", Addison – Wesley

[54] Denning, D., E., 2007, "*Cryptography and Data Security*", Addison – Wesley

στο διαδίκτυο. Ο ίδιος ο 17χρονος καταδικάστηκε σε 21νος μηνών ποινή φυλάκισης με αναστολή.

Ιός Leap-A/Oompa-A

Πολλοί έχουν παρατηρήσει την διαφήμιση της Apple σύμφωνα με την οποία υπάρχουν πάνω από 100.000 ιοί που μπορούν να επιτεθούν σε ένα λειτουργικό σύστημα. Σύμφωνα με την ίδια διαφήμιση, οι ιοί αυτοί στοχεύουν σε προσωπικούς υπολογιστές αλλά όχι σε Macintosh. Κατά κύριο λόγο αυτό είναι σωστό. Οι υπολογιστές Mac, προστατεύονται λόγω της βασικής αρχής *security through obscurity*. Σύμφωνα με αυτό το δόγμα οι προγραμματιστές μέσα στο σκοτάδι ή αλλιώς στην άγνοια των λεπτομερειών του προγραμματιστικού κώδικα του λειτουργικού συστήματος επιτυγχάνουν τη μέγιστη ασφάλεια απέναντι σε κινδύνους. Έτσι η Apple είναι γνωστό ότι κρατά τα μυστικά του λειτουργικού συστήματος αλλά και του υλικού της. Οι υπολογιστές αυτοί απέχουν πολύ από τους αριθμούς αγοράς οικιακών υπολογιστών. Κάποιος που δημιουργεί ιό για αυτούς τους υπολογιστές δεν θα έχει την ίδια αναμενόμενη επιτυχία.

Αυτό όμως δεν αποτελεί και εμπόδιο για κάποιον. Το 2006, ο ιός Leap–A έκανε την εμφάνισή του. Χρησιμοποιεί το πρόγραμμα άμεσης αποστολής και λήψης μηνυμάτων για τη διάδοσή του σε υπολογιστές Mac. Μετά την προσβολή ενός τέτοιου συστήματος ο ιός αναζητά μια τις επαφές του θύματος και αποστέλλει μηνύματα σε κάθε χρήστη της λίστας. Ο ιός αυτός δεν προκάλεσε καμία συγκεκριμένη βλάβη σε υπολογιστές απλά ήθελε να αποδείξει ότι και τα συστήματα αυτά μπορούν να προσβληθούν[55].

Ιός Storm Worm

Είναι ο πιο πρόσφατος ιός της κατηγορίας Worms. Οι ειδικοί στον τομέα ηλεκτρονικής ασφάλειας αναγνώρισαν τον ιό αυτό στα τέλη του 2006. Το κοινό άρχισε να τον αποκαλεί Worm Storm από τα μηνύματα τα οποία έφεραν το εξής θέμα : 230 νεκροί από καταιγίδα στη Ευρώπη[56]. Οι εταιρείες

[55] Denning, D., E., 2007, "*Cryptography and Data Security*", Addison – Wesley

[56] Denning, D., E., 2007, "*Cryptography and Data Security*", Addison – Wesley

ανάπτυξης ιομορφικού υλικού του έδωσαν διάφορα ονόματα. Για παράδειγμα η Symantec το απεκάλεσε Peacomm, η Mac Afee τον έλεγε Nuwar. Πάντως ο ιός του 2002 και το σκουλήκι του 2006, είναι εντελώς διαφορετικά μεταξύ τους. Το πρόγραμμα Δούρειος ίππος είναι ένα επιβλαβές πρόγραμμα αλλά όχι πάντα το ίδιο. Μεριές εκδοχές του μετατρέπουν τους υπολογιστές σε *zombies*. Καθώς οι υπολογιστές προσβάλλονται γίνονται επιρρεπείς σε ενδεχόμενο απομακρυσμένο έλεγχό από το πρόσωπο που κρύβεται πίσω από την επίθεση. Κάποιοι χρησιμοποιούν αυτόν τον ιό σε αποστολή μηνυμάτων spam σε όλο το διαδίκτυο.

Πολλές εκδοχές του ιού αυτού εξαπατούν το θύμα τους παροτρύνοντάς το να μεταφορτώσει την εφαρμογή ψεύτικων συνδέσμων για ιστορίες και βίντεο για διάφορα νέα της ημέρας. Συχνά το θέμα των email αλλάζει για να κεντρίσουν το ενδιαφέρον. Το email έφερε συνδέσμους σε βίντεο και ειδησεογραφικά άρθρα γύρω από το θέμα της αλληλογραφίας. Στην πραγματικότητα όμως, κάνοντας κλικ με το σύνδεσμο το θύμα ενεργοποιούσε τη μεταφόρτωση του ιού στον υπολογιστή του. Χαρακτηρίσθηκε σαν ο χειρότερος ιός. Μέχρι το Ιούλιο του 2007, η εταιρεία Postini ανακοίνωσε ότι είχε εντοπίσει πάνω από 200 εκατομμύρια emails φορέων συνδέσμων σε πηγές μεταφόρτωσης αυτού του ιού. Πλέον δεν είναι επικίνδυνος και δύσκολος.

Αναφερόμενοι λοιπόν στον ιό worms, αρχικά θα μπορούσε να πει κανείς ότι το συγκεκριμένο ιομορφικό λογισμικό δρα γενικά σαν κακόβουλο λογισμικό και ειδικά σαν επικίνδυνος ιός. Αρχική ιδέα ήταν να δημιουργηθεί ένα ιομορφικό λογισμικό που θα προκαλεί μόνο μια καταστροφή σε ένα ελεγχόμενο περιβάλλον για μεγαλύτερη ευκολία στην πραγματοποίηση του και την αποφυγή αντι-ιομορφικών λογισμικών. Χρησιμοποιήθηκε η γλώσσα C# της Microsoft με αποτέλεσμα να δρα σε λειτουργικά Windows XP, Vista, Widows 7. Το ιομορφικό λογισμικό με όνομα *kl4* είχε σαν σκοπό να μηδενίζει τα αρχεία εγγράφων με επεκτάσεις doc, txt. Xls, rtf, docx και τα συναφή. Αυτά που έκανε ήταν τα εξής[57] :

- Αντιγραφή του εκτελέσιμου αρχείου και του αρχείου rar που περιέχει τον ιό σε διάφορα λειτουργικά σημεία

[57] Denning, D., E., 2007, "*Cryptography and Data Security*", Addison – Wesley

- Κρυφή εκκίνηση του ιού σε processes από την registry.

- Διαγραφή όλων των αρχείων εγγράφων του χρήστη από ένα συγκεκριμένο φάκελο

- Καταγραφή όλων των πλήκτρων που θα πατήσει ο χρήστης μέχρι το κλείσιμο του υπολογιστή σε αρχείο txt

- Αποστολή αρχείου σε email μαζί με την διεύθυνση IP του θύματος

- Αποστολή του ιού σε 5 τυχαίους παραλήπτες .

2.5 Βλάβες που Προκαλεί ο Συγκεκριμένος Ιός

Όπως ο ιός, έτσι και το worm είναι ένα πρόγραμμα που εξαπλώνεται από υπολογιστή σε υπολογιστή χωρίς να το γνωρίζει ο χρήστης. Επίσης, όπως και οι ιοί, τα worms μπορεί μερικές φορές να έχουν σκόπιμα επιβλαβή αποτελέσματα, παρόλο που σε πολλές περιπτώσεις και μόνο το γεγονός της αντιγραφής τους μπορεί να είναι αρκετό για να βλάψει υπολογιστές και δίκτυα. Οι βλάβες που προκαλεί ο συγκεκριμένος ιός, είναι οι εξής[58]

- Ο ιός προσκολλάται σε αρχεία (προγράμματα ή έγγραφα) στο δίσκο του χρήστη και εξαπλώνεται όταν αυτά τα αρχεία αντιγραφούν ή εκτελεστούν.
- Ένα worm παραμένει στο active memory του υπολογιστή και εξαπλώνεται από τον ένα υπολογιστή στον άλλο, ενώ παράλληλα μολύνει και άλλους υπολογιστές μέσω της σύνδεσης στο Διαδίκτυο.

- Λόγω του ότι τα worms χρησιμοποιούν τις δικτυακές συνδέσεις για να εξαπλωθούν, μπορούν να έχουν υπερβολικά γρήγορη εξάπλωση και να δημιουργήσουν μεγάλη δικτυακή κίνηση (μειώνοντας την ταχύτητα ή μη επιτρέποντας τη νόμιμη πρόσβαση στο δίκτυο).

- Ένα πρόσφατο και γνωστό worm ήταν το «CodeRed worm», το οποίο επηρεάζει τους Windows NT και Windows 2000 web servers. Αυτό το

[58] Denning, D., E., 2007, "*Cryptography and Data Security*", Addison – Wesley

worm έχει υπό τον έλεγχό του τους μολυσμένους servers και τους χρησιμοποιεί για να επιτεθεί με «Denial of Service» σε άλλα Internet sites.

3. Κεφάλαιο Τρίτο : Τρόποι Αντιμετώπισης των Worms

3.1 Ασφάλεια Ηλεκτρονικών Υπολογιστών Έναντι των Worms

Η ασφάλεια των ηλεκτρονικών υπολογιστών έναντι των ιών Worms, μπορεί ως επί των πλείστων να εφαρμοστεί και να επιτευχθεί μέσω της μεθόδου της κρυπτογραφίας και των δύο μορφών που εκείνη διαθέτει, δηλαδή της ασύμμετρης και της συμμετρικής. Οι δύο αυτές μορφές καθώς και ο τρόπος με τον οποίο εφαρμόζονται για να προστατέψουν τους ηλεκτρονικούς υπολογιστές έναντι των worms, αναλύονται ως εξής.

3.1.1 Ασύμμετρη Κρυπτογραφία (Public-Key Cryptography)

Η ασύμμετρη κρυπτογραφία χρησιμοποιεί δύο διαφορετικά κλειδιά για την κρυπτογράφηση και αποκρυπτογράφηση. Κάθε χρήστης έχει στην κατοχή του ένα ζεύγος κλειδιών, το ένα καλείται δημόσια κλείδα και το άλλο καλείται ιδιωτική κλείδα. Η δημόσια κλείδα δημοσιοποιείται, ενώ η ιδιωτική κλείδα κρατείται μυστική. Η ιδιωτική κλείδα δεν μεταδίδεται ποτέ στο δίκτυο και όλες οι επικοινωνίες βασίζονται στην δημόσια κλείδα. Η ανάγκη ο αποστολέας και ο παραλήπτης να μοιράζονται το ίδιο κλειδί εξαφανίζεται και μαζί και πολλά προβλήματα που θα δούμε παρακάτω. Η μόνη απαίτηση της ασύμμετρης κρυπτογραφίας είναι η εμπιστεύσιμη και επιβεβαιωμένη συσχέτιση των δημόσιων κλείδων με τους κατόχους τους ώστε να μην είναι δυνατή η σκόπιμη ή μη πλαστοπροσωπία. Η ασύμμετρη κρυπτογράφηση μπορεί να χρησιμοποιηθεί όχι μόνο για κρυπτογράφηση, αλλά και για παραγωγή ψηφιακών υπογραφών[59].

[59] Denning, D., E., 2007, "*Cryptography and Data Security*", Addison – Wesley

Η ιδιωτική κλείδα είναι μαθηματικά συνδεδεμένη με την δημόσια κλείδα. Τυπικά, λοιπόν, είναι δυνατόν να νικηθεί ένα τέτοιο κρυπτοσύστημα ανακτώντας την ιδιωτική κλείδα από την δημόσια. Η επίλυση αυτού του προβλήματος είναι πολύ δύσκολη και συνήθως απαιτεί την παραγοντοποίηση ενός μεγάλου αριθμού. Η κρυπτογράφηση με χρήση της ασύμμετρης κρυπτογραφίας γίνεται ως εξής: όταν ο χρήστης Α θέλει να στείλει ένα μυστικό μήνυμα στον χρήστη Β, χρησιμοποιεί την δημόσια κλείδα του Β για να κρυπτογραφήσει το μήνυμα και έπειτα το στέλνει στον Β. Ο χρήστης Β, αφού παραλάβει το μήνυμα, κάνει χρήση της ιδιωτικής του κλείδας για να το αποκρυπτογραφήσει. Κανένας που "ακούει" την σύνδεση δεν μπορεί να αποκρυπτογραφήσει το μήνυμα[60].

Οποιοσδήποτε έχει την δημόσια κλείδα του Β μπορεί να του στείλει μήνυμα και μόνο αυτός μπορεί να το διαβάσει γιατί είναι ο μόνο που γνωρίζει την ιδιωτική κλείδα. Όταν ο Α θέλει να χρησιμοποιήσει την ασύμμετρη κρυπτογραφία για να υπογράψει ένα μήνυμα, τότε πραγματοποιεί ένα υπολογισμό που απαιτεί την ιδιωτική του κλείδα και το ίδιο το μήνυμα. Το αποτέλεσμα του υπολογισμού καλείται ψηφιακή υπογραφή και μεταδίδεται μαζί με το μήνυμα. Για να επαληθεύσει την υπογραφή ο Β πραγματοποιεί ανάλογο υπολογισμό χρησιμοποιώντας την δημόσια κλείδα του Α, το μήνυμα και την υπογραφή. Εάν το αποτέλεσμα είναι θετικό, τότε η υπογραφή είναι αυθεντική. Διαφορετικά η υπογραφή είναι πλαστή ή το μήνυμα έχει τροποποιηθεί[61].

3.1.2 Συμμετρική Κρυπτογραφία (Symmetric Cryptography ή Secret-Key Cryptography)

Στην συνηθισμένη κρυπτογραφία, ο αποστολέας και ο παραλήπτης ενός μηνύματος γνωρίζουν και χρησιμοποιούν το ίδιο μυστικό κλειδί. Ο αποστολέας χρησιμοποιεί το μυστικό κλειδί για να κρυπτογραφήσει το μήνυμα και ο παραλήπτης χρησιμοποιεί το ίδιο κλειδί για να αποκρυπτογραφήσει το μήνυμα. Αυτή η μέθοδος καλείται συμμετρική κρυπτογραφία ή κρυπτογραφία μυστικού κλειδιού. Η συμμετρική κρυπτογραφία χρησιμοποιείται όχι μόνο για

[60] Schneier, B., 1996, "*Applied Cryptography*", Prentice Hall

[61] Pfleeger, C., P., 1997, "*Security in Computing*", Prentice Hall

κρυπτογράφηση, άλλα και για πιστοποίηση ταυτότητας. Μία τέτοια τεχνική είναι η Message Authentication Code (MAC). Το κύριο πρόβλημα της συμμετρικής κρυπτογραφίας είναι η συνεννόηση του αποστολέα και του παραλήπτη στο κοινό μυστικό κλειδί που θα κρυπτογραφεί και αποκρυπτογραφεί όλη την διακινούμενη πληροφορία, χωρίς κάποιον άλλο να λάβει γνώση αυτού. Πλεονέκτημα της είναι ότι είναι ταχύτερη από την ασύμμετρη κρυπτογραφία[62].

3.1.3 Πλεονεκτήματα Ασύμμετρης Κρυπτογραφίας για την Αντιμετώπιση Ιών Worms

Σε σχέση με τη συμμετρική κρυπτογραφία, η ασύμμετρη παρουσιάζει μια σειρά πλεονεκτημάτων ως προς την αντιμετώπιση των Ιών Worms, ως εξής[63]:

- Δεν απαιτείται η ύπαρξη ασφαλούς διαύλου για την αρχική μετάδοση του δημόσιου κλειδιού. Αν κάποιος (π.χ. το πρόσωπο Β παραπάνω) βρει ή υποκλέψει το δημόσιο κλειδί ενός προσώπου Α, μπορεί μεν να το χρησιμοποιήσει για να στείλει στον Α ένα ιδιωτικό μήνυμα, όχι όμως για να προσποιηθεί προς τρίτους ότι είναι ο Α ούτε για να αποκρυπτογραφήσει μηνύματα τρίτων που έχουν σταλεί στον Α κρυπτογραφημένα με το δημόσιου κλειδί του Α. Και τούτο διότι αυτά μπορούν να αποκρυπτογραφηθούν μόνο με τη χρήση του ιδιωτικού κλειδιού του Α, του οποίου μοναδικός κάτοχος και χρήστης είναι ο ίδιος ο Α. Από τα παραπάνω προκύπτει ότι ο Α μπορεί να στείλει στον Β το δημόσιο κλειδί του (Apu) είτε μέσω e-mail ή ακόμη και να το «δημοσιεύσει» σε ειδικές για το σκοπό αυτό ηλεκτρονικές υπηρεσίες καταλόγου (public key directories).
- Ο Α δεν χρειάζεται να ανησυχεί για το αν ο Β, με τον οποίο επικοινωνεί (και κατά συνέπεια ο Β έχει λάβει γνώση του δημοσίου κλειδιού του Α) είναι «διπλός πράκτορας». Ο Β δεν είναι δυνατόν να επωφεληθεί από

[62] Taylor, A., 1999, "*The Hackers*", Routledge

[63] Pfleeger, C., P., 1997, "*Security in Computing*", Prentice Hall

την υποκλοπή μηνυμάτων τρίτων προσώπων προς τον Α (αφού για την αποκρυπτογράφηση τους απαιτείται η γνώση του ιδιωτικού κλειδιού του Α), ούτε και να προσποιηθεί ότι είναι ο Α. Εξάλλου η εκχώρηση, από τον Β προς τρίτους του δημόσιου κλειδιού του Α δεν έχει κανένα νόημα, αφού (από τον σχεδιασμό του συστήματος) προορισμός του είναι ακριβώς να είναι γνωστό και διαθέσιμο σε κάθε ενδιαφερόμενο.

- Η χρήση των ασύμμετρων κλειδιών μπορεί να επεκταθεί με επιτυχία για να εξυπηρετήσει μεγάλους πληθυσμούς χρηστών. Αυτό οφείλεται στο γεγονός ότι κάθε χρήστης χρειάζεται να μοιραστεί με τους άλλους μόνο ένα κλειδί, το δικό του δημόσιου κλειδί. Το ίδιο ισχύει και για τους υπόλοιπους. Έτσι, για να επικοινωνήσουν τέσσερα πρόσωπα (έστω τα Α, Β, Γ, Δ) μεταξύ τους, χρειάζεται να κοινοποιηθούν μόνο τέσσερα κλειδιά, ενώ για την επικοινωνία μεταξύ 100 προσώπων χρειάζεται να κοινοποιηθούν αντίστοιχα 100 κλειδιά, σε αντίθεση με τα 9.900 κλειδιά που απαιτούνται κατά την χρήση συμμετρικών κλειδιών. Δηλαδή ο αριθμός των χρησιμοποιούμενων κλειδιών είναι ανάλογος του πλήθους των συμμετεχόντων στην επικοινωνία, ενώ στα συστήματα συμμετρικής κρυπτογραφίας ο αριθμός των κλειδιών είναι ανάλογος του τετραγώνου των συμμετεχόντων. Κατά συνέπεια, οργανισμοί με μεγάλο πλήθος χρηστών δεν έχουν προβλήματα διαχείρισης υπερβολικού πλήθους κλειδιών. Όλοι όσοι χρειάζονται να στείλουν κρυπτογραφημένα μηνύματα σε ένα πρόσωπο Α, χρησιμοποιούν το ίδιο κλειδί: το δημόσιο κλειδί του Α.
- Μια ακόμη μη προφανής ωφέλεια που προκύπτει από τη χρήση συστημάτων δημόσιου / ιδιωτικού κλειδιού είναι ότι δεν απαιτείται να έχει κανείς εκ των προτέρων κάποια σχέση με κάποιον στον οποίο θέλει να απευθύνει ένα μήνυμα. Αυτό ήταν απαραίτητο στα συστήματα συμμετρικού κλειδιού, προκειμένου να καταστεί δυνατή η ανταλλαγή του συμμετρικού κλειδιού, στο οποίο θα βασιστεί στη συνέχεια η κρυπτογράφηση και η αποκρυπτογράφηση. Με το σύστημα δημόσιου / ιδιωτικού κλειδιού, ο αποστολέας απλώς εντοπίζει το δημόσιο κλειδί του παραλήπτη, κρυπτογραφεί το μήνυμα και το αποστέλλει. Ο

παραλήπτης διαθέτει ήδη το ιδιωτικό του κλειδί με βάση το οποίο και αποκρυπτογραφεί το μήνυμα.

- Τέλος, λόγω της ασύμμετρης φύσης του συστήματος δημόσιου / ιδιωτικού κλειδιού, κάθε κάτοχος ενός τέτοιου ζεύγους κλειδιών είναι σε θέση να πραγματοποιεί μαθηματικές διεργασίες με το ιδιωτικό του κλειδί, τις οποίες κανείς άλλος παγκοσμίως δεν έχει τη δυνατότητα να εκτελέσει. Η παρατήρηση αυτή αποτελεί τη βάση για τις ψηφιακές υπογραφές (digital signatures) και τη διασφάλιση της δυνατότητας της μη-αποκήρυξης (non-repudiation). Βεβαίως, εκτός από πλεονεκτήματα, η ασύμμετρη κρυπτογραφία παρουσιάζει και ορισμένα μειονεκτήματα.
- Κατ' αρχήν επειδή οι ασύμμετροι αλγόριθμοι έχουν πολύ μεγαλύτερες απαιτήσεις σε μαθηματικούς υπολογισμούς από ότι οι συμμετρικοί, με αποτέλεσμα να είναι συγκριτικά πιο αργοί και μάλιστα 10 έως 100 φορές πιο αργοί σε σχέση με αντίστοιχης κρυπτογραφικής ισχύος συμμετρικούς. Παρά το γεγονός ότι οι όποιες απαιτούμενες διαδικασίες υπολογισμών διεκπεραιώνονται σήμερα με τη βοήθεια ηλεκτρονικών υπολογιστών και τη χρήση κατάλληλων προγραμμάτων λογισμικού, η παραπάνω διαφορά αποκτά ιδιαίτερη σημασία, ιδίως αν τα προς κρυπτογράφηση (και αποκρυπτογράφηση) δεδομένα δεν είναι τα περιεχόμενα ενός μηνύματος λίγων γραμμών, αλλά πληροφορίες για ένα πολύ μεγάλο έργο, όπως π.χ. κάποιο έργο γενετικής μηχανής. Οι συμμετρικοί όμως αλγόριθμοι έχουν ένα σοβαρό μειονέκτημα, εάν υποκλαπεί το κλειδί τους, μπορεί να χρησιμοποιηθεί για την αποκρυπτογράφηση μηνυμάτων από μη εξουσιοδοτημένα άτομα. Από την άλλη, οι ασύμμετροι αλγόριθμοι είναι αρκετά ασφαλείς, εντούτοις πολύ περισσότερο αργοί.
- Επιπλέον, με τη χρήση ασύμμετρων αλγόριθμων το μέγεθος του κρυπτογραφημένου μηνύματος είναι μεγαλύτερο από το αντίστοιχο αρχικό. Αυτό μπορεί να αποτελέσει ένα σοβαρό ζήτημα όταν χρησιμοποιούνται πολλαπλά επίπεδα κρυπτογράφησης. Π.χ. μια εφαρμογή λογισμικού κρυπτογραφεί δεδομένα (και επομένως διογκώνει το μέγεθός τους), τα οποία στη συνέχεια αποστέλλονται

μέσω μιας ασφαλούς σύνδεσης Web (secure Web session), οπότε και πάλι θα διογκωθεί το μέγεθός τους. Εξάλλου είναι πιθανόν η αποστολή να γίνει μέσα από ένα κρυπτογραφημένο δίαυλο (IPSec tunnel), με αποτέλεσμα την παραπέρα διόγκωση του μεγέθους των δεδομένων.

Είναι εμφανές από τα παραπάνω ότι κάθε ένα από τα δύο συστήματα κρυπτογραφίας παρουσιάζει πλεονεκτήματα και μειονεκτήματα. Μάλιστα είναι χαρακτηριστικό ότι υπάρχει μια συμπληρωματικότητα, με την έννοια ότι όπου υπερτερεί το ένα υστερεί το άλλο. Επομένως θα ήταν δυνατό να γίνει ένας συνδυασμός των δύο που να εκμεταλλεύεται τα πλεονεκτήματα του καθενός, χωρίς να κληρονομεί τα αντίστοιχα μειονεκτήματα. Ένας τέτοιος συνδυασμός θα πρέπει να συγκεντρώνει τις εξής ιδιότητες[64]:

- ✓ Η προσφερόμενη λύση να είναι ασφαλής
- ✓ Η κρυπτογράφηση να είναι ταχεία
- ✓ Το κρυπτογραφημένο κείμενο να είναι συμπαγές
- ✓ Η λύση να μπορεί να επεκταθεί για την εξυπηρέτηση μεγάλων πληθυσμών
- ✓ Η λύση να μην είναι ευάλωτη ως προς την υποκλοπή του κλειδιού
- ✓ Η λύση να μην απαιτεί προϋπάρχουσα σχέση μεταξύ των δύο μερών
- ✓ Η λύση να μπορεί να υποστηρίξει ψηφιακές υπογραφές και μη-αποκήρυξη

Η συνδυασμένη αυτή χρήση συμμετρικής και ασύμμετρης κρυπτογραφίας περιγράφεται στο ακόλουθο παράδειγμα. Ο αποστολέας (έστω Α) δημιουργεί ένα τυχαίο συμμετρικό κλειδί, το οποίο και χρησιμοποιείται για την κρυπτογράφηση του μηνύματος. Το ζήτημα είναι πως θα μεταφερθεί το κλειδί αυτό στον παραλήπτη (έστω Β). Αυτό επιτυγχάνεται με αξιοποίηση της ασύμμετρης κρυπτογραφίας και με εντοπισμό του δημόσιου κλειδιού του παραλήπτη με τη βοήθεια κάποιου καταλόγου δημοσίων κλειδιών.

[64] Denning, D., E., 2007, "*Cryptography and Data Security*", Addison – Wesley

Το δημόσιο κλειδί του παραλήπτη χρησιμοποιείται για την κρυπτογράφηση του συμμετρικού κλειδιού. Βεβαίως η ασύμμετρη κρυπτογραφία είναι αργή, αλλά δεδομένου ότι το συμμετρικό κλειδί είναι πολύ μικρού μεγέθους (128bits), αυτό δεν αποτελεί πρόβλημα. Το αποτέλεσμα είναι ένα τυχαίο συμμετρικό κλειδί κρυπτογραφημένο (προστατευμένο) με τη βοήθεια ενός ασύμμετρου κλειδιού. Το τελευταίο βήμα είναι η επισύναψη του προστατευμένου συμμετρικού κλειδιού στο κρυπτογραφημένο μήνυμα, έτσι ώστε τα δύο μαζί να αποτελούν ένα αντικείμενο προς αποστολή και το οποίο είναι γνωστό ως ψηφιακός φάκελος (digital envelope).

Στη συνέχει ο ψηφιακός φάκελος αποστέλλεται στον παραλήπτη μέσω του Internet. Το πρώτο βήμα μετά την παραλαβή είναι ο διαχωρισμός που περιεχομένου του ψηφιακού φακέλου και η ανάκτηση αφ' ενός του κρυπτογραφημένου μηνύματος και αφ' ετέρου του προστατευμένου συμμετρικού κλειδιού. Ο παραλήπτης χρησιμοποιεί το δικό του ιδιωτικό κλειδί για την ανάκτηση/ αποκρυπτογράφηση του συμμετρικού κλειδιού. Τέλος, με τη χρήση του συμμετρικού κλειδιού αποκρυπτογραφεί το κείμενο του μηνύματος. Το συμμετρικό κλειδί δεν είναι πλέον χρήσιμο και μπορεί να αχρηστευτεί.

Κίνδυνος υποκλοπής του μηνύματος δεν υφίσταται, ακόμη και αν κάποιος τρίτος αποκτήσει πρόσβαση στον ψηφιακό φάκελο, ενώ αυτός βρίσκεται καθ' οδόν προς τον παραλήπτη. Ο πιθανός υποκλοπέας δεν μπορεί σε καμία περίπτωση να επωφεληθεί, δεδομένου ότι θα πρέπει να λάβει γνώση του συμμετρικού κλειδιού, το οποίο όμως είναι κρυπτογραφημένο και είναι δυνατόν να αποκωδικοποιηθεί μόνο με το ιδιωτικό κλειδί του παραλήπτη, το οποίο είναι ούτως ή άλλως απόρρητο.

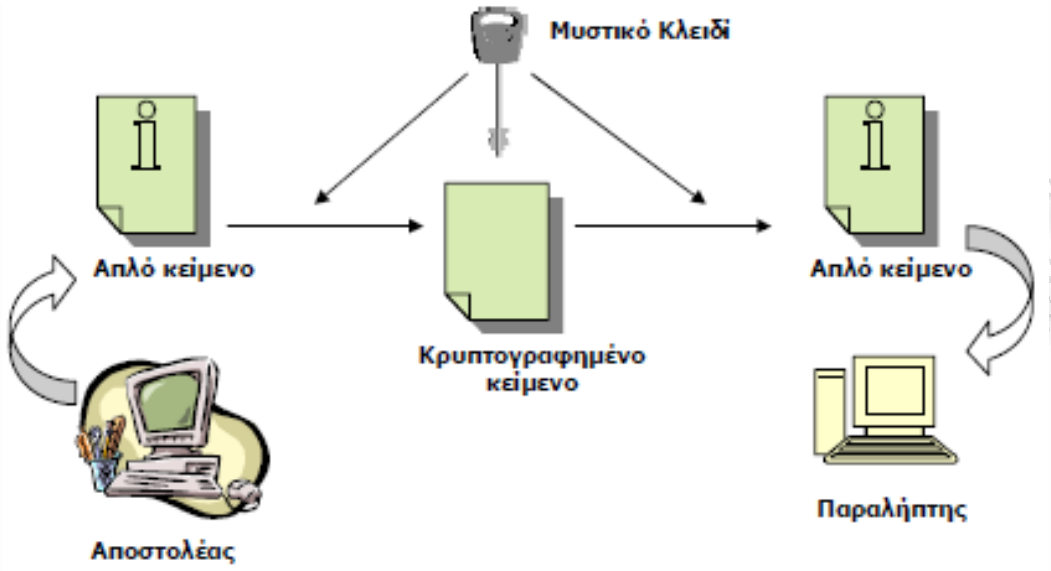
Παρ' όλα αυτά η μέθοδος αυτή παρουσιάζει το εξής πρόβλημα: Ένας τρίτος μπορεί να εντοπίσει το δημόσιο κλειδί του παραλήπτη Β (μέσω καταλόγου) και στη συνέχεια να δημιουργήσει ένα συμμετρικό κλειδί, με το οποίο να κρυπτογραφήσει ένα τελείως διαφορετικό μήνυμα, το οποίο και να αποστείλει στον Β με τη μορφή ψηφιακού φακέλου όπως παραπάνω. Ο Β θα παραλάβει τον ψηφιακό φάκελο, θα αποκωδικοποιήσει το συμμετρικό κλειδί με χρήση του δικού του ιδιωτικού κλειδιού και τέλος θα αποκρυπτογραφήσει το μήνυμα

με το συμμετρικό κλειδί. Το μήνυμα όμως αυτό δεν έχει καμία σχέση με το πραγματικών αναμενόμενο και βεβαίως δεν έχει προέλθει από τον Α. Προκύπτει επομένως πρόβλημα πιστοποίησης της ταυτότητας του αποστολέα. Η απάντηση στο πρόβλημα αυτό μπορεί να δοθεί με τη βοήθεια των ψηφιακών υπογραφών, οι οποίες προϋποθέτουν τη χρήση των λεγομένων αλγορίθμων κατατεμαχισμού (hash algorithms). Τα θέματα αυτά εξετάζονται στη συνέχεια.

3.1.4 Σχέση Λειτουργίας Συμμετρικής Κρυπτογραφίας με Αλγορίθμους και με Σκοπό τη Προστασία από τους Ιούς Worms

Το κρυπτογραφικό αυτό σύστημα είναι το πλέον γνωστό και χαρακτηρίζεται από την ύπαρξη ενός και μόνο κώδικα ή κλειδιού, το οποίο χρησιμοποιείται τόσο για την κρυπτογράφηση του μηνύματος από τον αποστολέα - πριν την αποστολή - όσο και για την αποκρυπτογράφηση του από τον παραλήπτη - μετά την μεταφορά. Για τον λόγο αυτό άλλωστε ονομάζεται και συμμετρικό. Επίσης είναι γνωστό και με τα ονόματα κρυπτογραφία μυστικού κλειδιού (secret key) ή διαμοιραζομένου μυστικού (shared secret), δεδομένου ότι το κλειδί θα πρέπει να παραμείνει μυστικό, αλλά και ταυτόχρονα να είναι γνωστό μόνο στα δύο μέρη που ανταλλάσσουν μηνύματα. Για να λειτουργήσει λοιπόν το σύστημα με αποτελεσματικό τρόπο, ο αποστολέας και ο παραλήπτης πρέπει, εκ των προτέρων, να συμφωνήσουν σε ένα μυστικό κλειδί και του οποίου η λειτουργία εμφανίζεται στο ακόλουθο σχεδιάγραμμα No.3

Σχεδιάγραμμα No.3 - Λειτουργία Συμμετρικής Κρυπτογραφίας



Τα κρυπτογραφικά κλειδιά παρουσιάζουν πολλές ομοιότητες με τα φυσικά κλειδιά της καθημερινής ζωής, που χρησιμοποιούνται π.χ. για να κλειδώσουν ή να ξεκλειδώσουν μια πόρτα. Για κάθε τύπο «κλειδαριάς», υπάρχει ένα κλειδί ειδικού σχήματος που ταιριάζει σ' αυτήν και το οποίο πρέπει να έχει το σωστό μήκος και τη σωστή μορφολογία. Ένα κλειδί για κλειδαριές συγκεκριμένου κατασκευαστή είναι πολύ πιθανόν να ταιριάζει σε οποιαδήποτε κλειδαριά αντίστοιχου τύπου, αλλά μόνο το σωστό κλειδί, αυτό με το κατάλληλο μήκος και μορφολογία μπορεί να περιστραφεί και να ανοίξει την «κλειδαριά».

Κατ' αναλογία, και στα σύγχρονα συστήματα κρυπτογραφίας που λειτουργούν με χρήση υπολογιστών, κάθε κρυπτογραφικός αλγόριθμος χρειάζεται ένα κλειδί με το σωστό μήκος, δηλαδή με το σωστό αριθμό bits. Ένας κρυπτογραφικός αλγόριθμος μπορεί να λειτουργήσει με οποιοδήποτε κλειδί έχει το κατάλληλο μήκος, αλλά η εφαρμογή του αλγόριθμου θα έχει ως αποτέλεσμα την αποκρυπτογράφηση ενός κρυπτογραφημένου μηνύματος μόνο με το κλειδί που διαθέτει τη σωστή ακολουθία bits[65].

Οι συμμετρικοί αλγόριθμοι κρυπτογράφησης δέχονται σαν είσοδο κανονικό αναγνώσιμο κείμενο (clear text- plain text) και με τη χρήση του συμμετρικού κλειδιού παράγουν σαν αποτέλεσμα (εξαγόμενο) μια κρυπτογραφημένη μορφή του αρχικού κειμένου. Το συμμετρικό κλειδί δεν είναι παρά ένα τυχαίος

[65] Schneier, B., 1996, "*Applied Cryptography*", Prentice Hall

αριθμός με το σωστό μέγεθος. Έτσι, αν ο αλγόριθμος είναι συμμετρική κρυπτογράφηση των 40bits, το συμμετρικό κλειδί θα είναι μήκους 40bits, ενώ αν πρόκειται για αλγόριθμο συμμετρικής κρυπτογράφησης των 128 bits, τότε το συμμετρικό κλειδί θα είναι μήκους 128 bits[66].

Ένας κρυπτογραφικός αλγόριθμος χαρακτηρίζεται ως ασφαλής εφ' όσον έχει προηγηθεί ο εξαντλητικός έλεγχός του από τους κρυπταναλυτές, χωρίς να εντοπισθούν αδυναμίες. Υπ' αυτές τις προϋποθέσεις ο μόνος τρόπος να παραβιαστεί ένα κρυπτογραφημένο μήνυμα, είναι να δοκιμαστούν όλες οι πιθανές τιμές κλειδιών που αντιστοιχούν στο συγκεκριμένο μέγεθος. Αυτό αποκαλείται επίθεση ωμής βίας (brute force attack). Στατιστικά θα χρειαστεί να δοκιμαστούν μόνο οι μισές από τις πιθανές τιμές του κλειδιού, προκειμένου να εντοπισθεί το σωστό κλειδί[67].

Αυτό μπορεί να ακούγεται μη πρακτικό αλλά μη ξεχνάμε πως ένας υπολογιστής υψηλής ταχύτητας μπορεί να προσπαθήσει εκατομμύρια πιθανότητες σε ένα δευτερόλεπτο. Αυτός είναι και ο λόγος που καθιστά το μήκος του κλειδιού σημαντικό. Για παράδειγμα, ένα κλειδί μήκους 16 δυαδικών ψηφίων (bits) διαθέτει 216=65536 διαφορετικούς συνδυασμούς και θα υποστεί επίθεση ωμής βίας αμέσως. Ένα κλειδί μήκους 40 bits διαθέτει περισσότερους από 1012 συνδυασμούς.

Παρ' όλο που φαίνονται πολλοί, ένα κλειδί 40 bits θεωρείται αδύναμο ώστε να του εμπιστευθούν πολύτιμες πληροφορίες. Τα κλειδιά που χρησιμοποιούνται για να κρυπτογραφηθούν ευαίσθητες πληροφορίες είναι συνήθως 128 bits ή και μεγαλύτερα. 128 bits σημαίνει 1038 συνδυασμοί περισσότεροι από των αριθμό σταγόνων νερού που υπάρχει σε όλους τους ωκεανούς της γης. Τα μεγέθη των κλειδιών επιλέγονται έτσι ώστε να είναι πρακτικά αδύνατο να δοκιμαστούν έστω και οι μισές πιθανές τιμές του κλειδιού, ακόμη και με χρήση τεράστιου αριθμού υπολογιστών, μέσα στο χρονικό διάστημα κατά το οποίο τα υπό προστασία δεδομένα πρέπει να παραμείνουν ασφαλή. Είναι φυσικά αδύνατο να προβλεφθεί με ακρίβεια η εξέλιξη της τεχνολογίας των υπολογιστών οπότε είναι απαραίτητο να γίνουν κάποιες υποθέσεις σχετικά με

[66] Denning, D., E., 2007, "*Cryptography and Data Security*", Addison – Wesley

[67] Schneier, B., 1996, "*Applied Cryptography*", Prentice Hall

την πιθανή αύξηση της επεξεργαστικής τους ισχύος[68]. Θα πρέπει αντίστοιχα να σημειωθεί πως υπάρχουν οι εξής κατηγορίες συμμετρικών αλγορίθμων κρυπτογράφησης[69]:

- ***DES*** Οι αλγόριθμοι, οι οποίοι χωρίζουν τα προς κρυπτογράφηση δεδομένα σε πακέτα των 64bits και είναι γνωστοί ως "block ciphers". Ο πιο γνωστός από αυτούς είναι ο DES (Data Encryption Standard), ο οποίος έχει σταθερό μήκος κλειδιού 56bits και αναπτύχθηκε αρχικά από την IBM στην δεκαετία του 1970, ενώ στη συνέχεια υιοθετήθηκε και από την κυβέρνηση των ΗΠΑ ως το επίσημο πρότυπο κρυπτογράφησης απορρήτων πληροφοριών. Ο DES υπήρξε εν χρήσει για μεγάλο διάστημα και χρησιμοποιήθηκε σε πολλά κρυπτογραφικά συστήματα, όπως το σύστημα Kerberos, το οποίο αναπτύχθηκε στο MIT. Λόγω όμως της αυξανόμενης ισχύος των υπολογιστών το μήκος 56bits κλειδί του αρχίζει να γίνεται ευάλωτο σε επιθέσεις τύπου ωμής βίας. Ο "κλασσικός" αλγόριθμος DES είναι πλέον ξεπερασμένος, αφού με τη χρήση ενός σύγχρονου υπολογιστή μπορεί να παραβιαστεί σχετικά εύκολα. Το πρότυπο που αναμένεται να δώσει νέα ζωή στο DES είναι το AES (Advanced Encryption Standard, Εξελιγμένο Πρότυπο Κωδικοποίησης). Στο μεταξύ, εφαρμόζοντας διάφορες τεχνικές επάνω στο DES, μπορούμε να αυξήσουμε σημαντικά την ασφάλειά του. Με τη μέθοδο Triple-DES, για παράδειγμα, το μήνυμα κωδικοποιείται τρεις φορές, με τρία διαφορετικά κλειδιά. Άλλες παραλλαγές του DES είναι: DESX, GDES, RDES όπου χρησιμοποιούνται μεγαλύτερα κλειδιά
- ***RC4***. Στην κατηγορία αυτή ανήκουν οι αλγόριθμοι που δεν εφαρμόζονται σε πακέτα δεδομένων συγκεκριμένου μεγέθους (64 ή 128bits), αλλά σε ακολουθίες bits (stream ciphers).Ο πιο γνωστός από αυτούς είναι ο RC4, με κυριότερα χαρακτηριστικά του την ταχύτητα (είναι ταχύτερος από όλους της προηγούμενος κατηγορίας) και την υποστήριξη κλειδιών μεταβλητού μήκους.

[68] Denning, D., E., 2007, "*Cryptography and Data Security*", Addison – Wesley

[69] Pfleeger, C., P., 1997, "*Security in Computing*", Prentice Hall

- ***IDEA***. Ο Διεθνής Αλγόριθμος Κρυπτογράφησης Δεδομένων (International Data Encryption Algorithm), είναι δημοφιλής στην Ευρώπη αλλά όχι τόσο στην Αμερική. Με ένα μυστικό κλειδί 128 bits, θεωρείται ότι είναι πιο ασφαλής από τον DES. Ο IDEA είναι από τους βασικότερους αλγορίθμους στο λογισμικό κρυπτογράφησης του ηλεκτρονικού ταχυδρομείου, του PGP (Pretty Good Privacy). Ο άλλος είναι ο RSA που αναλύεται παρακάτω.

Τέλος, κοινές σε όλους τους συμμετρικούς αλγόριθμους είναι οι εξής ιδιότητες:

- Είναι γενικά γρήγοροι στην εκτέλεσή τους.
- Είναι συμπαγείς, με την έννοια ότι το παραγόμενο κρυπτογραφημένο μήνυμα έχει γενικά το ίδιο μέγεθος με το αρχικό μήνυμα.

- Με βάση τα παραπάνω, εάν δύο πρόσωπα Α και Β θέλουν να επικοινωνήσουν και έστω ότι ο Α επιθυμεί να στείλει ένα μυστικό μήνυμα στον Β, θα πρέπει να κινηθούν Ος εξής (Κολοκοτρώνης Δ.,2005):

- Επιλέγεται ένας συμμετρικός αλγόριθμος

- Επιλέγεται το συμμετρικό κλειδί

- Το κλειδί πρέπει να γίνει γνωστό και στους δύο: εάν το έχει επιλέξει ο Α, θα πρέπει να το αποστείλει εκ των προτέρων στον Β

- Ο Α κρυπτογραφεί το μήνυμα με τη χρήση του κλειδιού

- Ο Α αποστέλλει το κρυπτογραφημένο μήνυμα στον Β

- Ο Β αποκρυπτογραφεί το μήνυμα

Η συμμετρική κρυπτογραφία χαρακτηρίζεται από την απλότητά της, δεδομένου ότι απαιτεί την ύπαρξη ενός μόνο κλειδιού. Παρουσιάζει όμως ορισμένα σημαντικά προβλήματα. Πρέπει να υπάρχει ένας ασφαλής δίαυλος

για την αρχική μεταφορά του μυστικού κλειδιού. Αν το μυστικό κλειδί υποκλαπεί, τότε όλες οι επόμενες επικοινωνίες θα είναι επισφαλείς. Βασική προϋπόθεση επιτυχούς λειτουργίας είναι η ύπαρξη αμοιβαίας εμπιστοσύνης μεταξύ των δύο μερών. Όταν ένα συμμετρικό κλειδί αποκαλυφθεί, αυτό και κάθε μήνυμα που το χρησιμοποίησε για να κρυπτογραφηθεί έχει χάσει τα προνόμιά του. Ένα νέο κλειδί πρέπει να επιλεγεί και να διανεμηθεί[70].

Τα πράγματα δυστυχώς όμως δυσκολεύουν, αν ληφθεί υπ' όψη η αρχή της μη χρησιμοποίησης του ίδιου κλειδιού για παραπάνω από μια επικοινωνίες, έστω και αν αυτές γίνονται με το ίδιο πρόσωπο, δεδομένου ότι τότε αυξάνουν οι κίνδυνοι υποκλοπής του. Τέλος, σε σχέση με τις βασικές αρχές ασφάλειας που προαναφέρθηκαν στην εισαγωγή, η συμμετρική κρυπτογραφία δεν διασφαλίζει την επιβεβαίωση, αλλά ούτε και την μη αποκήρυξη. Κάθε ένα από τα δύο μέρη έχει τη δυνατότητα να τροποποιήσει κακόβουλος τα δεδομένα (ενός μηνύματος ή μιας συναλλαγής), έχοντας συγχρόνως τη βεβαιότητα ότι ένας τρίτος δεν θα είναι σε θέση να προσδιορίσει τον ένοχο[71].

Σήμερα χρησιμοποιεί κλειδιά μήκους τουλάχιστον 1024bits και είναι πιθανόν ο πιο πολύπλοκος και απαιτητικός σε υπολογιστική ισχύ από όλους τους εν χρήσει κρυπτογραφικούς αλγορίθμους. Επίσης πολύ γνωστός είναι ο αλγόριθμος ελλειπτικών καμπυλών (Elliptic curve cryptography- ECC), ο οποίος είναι σχετικά πιο πρόσφατος. Είναι λιγότερο πολύπλοκος και απαιτητικός σε σχέση με τον RSA και μπορεί να χρησιμοποιήσει μικρότερου μήκους κλειδιά, επιτυγχάνοντας το ίδιο επίπεδο ασφάλειας με τον RSA. Για να γίνει πιο κατανοητή η σημασία του μήκους των κρυπτογραφικών κλειδιών σε σχέση με το επιδιωκόμενο επίπεδο ασφάλειας, παρατίθεται ο πιο κάτω πίνακας, στον οποίο απεικονίζονται συγκριτικά τα μήκη κλειδιών (σε bits) των διαφόρων αλγορίθμων, σε συνδυασμό με τον χρόνο που απαιτείται προκειμένου να επιτευχθεί η παραβίαση ("σπάσιμο") του κλειδιού.

Η υπόθεση που έχει γίνει είναι ότι υπάρχει διαθέσιμο ποσό 10 εκατ. δολαρίων για αγορά εξοπλισμού (υπολογιστών) και ότι η μνήμη κοστίζει περίπου 0.5 δολάρια ανά MB.

[70] Schneier, B., 1996, "*Applied Cryptography*", Prentice Hall

[71] Denning, D., E., 2007, "*Cryptography and Data Security*", Addison – Wesley

Πίνακας Νο. 1 – Χαρακτηριστικά Στοιχεία Συμμετρικών και Ασύμμετρων Κλειδιών

Συμμετρικό κλειδί DES	Ασύμμετρο κλειδί ECC	Ασύμμετρο κλειδί RSA	Απαιτούμενος χρόνος Ι	Πλήθος Μηχανών	Ι Μνήμη
56	112	420	5 λεπτά	10.000	Ελάχιστη
80	160	760	600 μήνες	4.300	4 GB
96	192	1020	3 εκατ. έτη	114	170 GB
128	256	1620	1016 έτη	0,16	120 TB

Από τον πίνακα αυτό μπορεί να γίνει αντιληπτό γιατί αρχίζει να εγκαταλείπεται ο αλγόριθμος DES με υποχρεωτικό σταθερό μήκος κλειδιού 56 bits, καθώς και γιατί τα προτιμητέα μήκη κλειδιών στον αλγόριθμο RSA είναι πλέον 1024 και άνω. Εδώ θα άξιζε να αναφερθεί ότι όλοι οι κατασκευαστές λογισμικού ασύμμετρης κρυπτογράφησης υποστηρίζουν πολλαπλούς αλγόριθμους. Έτσι αν κάποια στιγμή βρεθεί ένα αδύνατο σημείο σε κάποιο αλγόριθμο, το οποίο επιτρέπει την παραβίασή του, υπάρχει πάντα η επιλογή της ενεργοποίησής ενός άλλου εναλλακτικού αλγορίθμου, ο οποίος να είναι ασφαλής[72].

3.1.5 Αλγόριθμοι Ασύμμετρης Κρυπτογραφίας με Σκοπό τη Προστασία των Ηλεκτρονικών Υπολογιστών από τους Ιούς Worms

RSA

Το σύστημα RSA είναι ένα σύστημα ασύμμετρης κρυπτογραφίας που προσφέρει Τεχνικές κρυπτογράφηση και ψηφιακές υπογραφές. Αναπτύχθηκε το 1977 από τους Ron Rivest, Adi Shamir και Leonard Adleman. Από τα αρχικά των επιθέτων τους προέρχεται το ακρωνύμιο RSA[73].

Περιγραφή του RSA

[72] Denning, D., E., 2007, "*Cryptography and Data Security*", Addison – Wesley

[73] Denning, D., E., 2007, "*Cryptography and Data Security*", Addison – Wesley

Απ' όλους τους αλγόριθμους δημοσίου κλειδιού που έχουν προταθεί, ο RSA είναι ο πιο κατανοητός και εύκολος να υλοποιηθεί. Γι' αυτό ίσως είναι και ο δημοφιλέστερος. Έχει αντέξει σε χρόνια κρυπτανάλυσης. Ο RSA στηρίζει την ασφάλειά του στη δυσκολία παραγοντοποίησης μεγάλων αριθμών. Για να δημιουργήσουμε τα δύο κλειδιά, διαλέγουμε δύο μεγάλους πρώτους αριθμούς, p και q. Για μέγιστη ασφάλεια, διαλέγουμε τα p και q να είναι ίδιου μήκους. Υπολογίζουμε το γινόμενο[74]:

n = pq

Έπειτα διαλέγουμε στην τύχη το κλειδί κρυπτογράφησης, e, να είναι τέτοιο ώστε το e και το (p-1)(q-1) να είναι πρώτοι μεταξύ τους αριθμοί. Τελικά, χρησιμοποιούμε τον επεκταμένο αλγόριθμο του Ευκλείδη για να υπολογίσουμε το κλειδί αποκρυπτογράφησης, που δίνεται από τη σχέση[75] :

ed ≡ 1 mod (p-1)(q-1)

1.4.5 Αλγόριθμοι Συμμετρικής Κρυπτογραφίας

A. DES (Data Encryption Standard)

DES είναι το ακρωνύμιο των λέξεων Data Encryption Standard. Αντιπροσωπεύει την τυποποίηση Federal Information Processing Standard (FIPS) 46-1 που επίσης περιγράφει τον Data Encryption Algorithm (DEA). Αρχικά αναπτύχθηκε από την IBM, ενώ σημαντικό ρόλο στην ανάπτυξη του έπαιξε η NSA και το National Institute of Standards and Technology (NIST). Είναι ο πιο γνωστός και παγκόσμια χρησιμοποιούμενος συμμετρικός αλγόριθμος. Ο DES είναι συμμετρικός αλγόριθμος· ο ίδιος αλγόριθμος και το ίδιο κλειδί χρησιμοποιούνται τόσο για την κρυπτογράφηση όσο και για την αποκρυπτογράφηση[76].

Το κλειδί έχει μήκος 56 bit. Στην πραγματικότητα είναι 64 bit, αλλά κάθε όγδοο bit χρησιμοποιείται για έλεγχο ισοτιμίας (parity check) και αγνοείται. Το bit

[74] Pfleeger, C., P., 1997, "*Security in Computing*", Prentice Hall

[75] Schneier, B., 1996, "*Applied Cryptography*", Prentice Hall

[76] Pfleeger, C., P., 1997, "*Security in Computing*", Prentice Hall

ισοτιμίας είναι το χαμηλής τάξης bit κάθε byte. Στη βάση του ο DES εφαρμόζει έναν συνδυασμό των δύο βασικότερων τεχνικών στην κρυπτογραφία, την σύγχυση και την διάχυση (confusion και diffusion). Τη σύγχυση την πετυχαίνει με αντικατάσταση και τη διάχυση με μετάθεση (substitution και permutation). Και οι δύο τεχνικές εφαρμόζονται στο κείμενο, με τρόπο εξαρτώμενο από το κλειδί. Αυτό είναι γνωστό σαν γύρος (round). Ο DES αποτελείται από 16 γύρους Ο αλγόριθμος χρησιμοποιεί βασικές αριθμητικές και λογικές πράξεις.

B. Triple-DES

Είναι μια παραλλαγή του DES όπου το μήνυμα κρυπτογραφείται και αποκρυπτογραφείται διαδοχικά με διαφορετικά κλειδιά για την ενίσχυση του βασικού αλγόριθμου. Υπάρχουν τέσσερις διαφορετικοί τρόποι για να επιτευχθεί αυτό[77]:

• DES-EEE3 (Encrypt-Encrypt-Encrypt): πραγματοποιούνται τρεις συνεχόμενες

κρυπτογραφήσεις με το τρία διαφορετικά κλειδιά.

• DES-EDE3 (Encrypt-Decrypt-Encrypt): το μήνυμα διαδοχικά κρυπτογραφείται, αποκρυπτογραφείται και τέλος κρυπτογραφείται με χρήση τριών διαφορετικών κλειδιών.

• DES-EEE2: είναι η ίδια με την πρώτη διαδικασία εκτός του ότι απαιτούνται δύο διαφορετικά κλειδιά.

• DES-EDE2: είναι η ίδια με την δεύτερη διαδικασία εκτός του ότι απαιτούνται δύο κλειδιά.

Τα επιπλέον κλειδιά δημιουργούνται από το κοινό μυστικό κλειδί με κατάλληλο αλγόριθμο. Από αυτούς τους τρόπους, ο πιο ασφαλής είναι ο DES-EEE3, με την τριπλή κρυπτογράφηση και τα τρία διαφορετικά κλειδιά.

[77] Taylor, A., 1999, "*The Hackers*", Routledge

Γ. DESX

Ο DESX είναι μια άλλη παραλλαγή του DES. Η διαφορά του DES και του DESX είναι ότι η είσοδος στο DESX περνάει από μια X-OR πράξη με ένα επιπλέον κλειδί 64 bits και ομοίως η έξοδος της κρυπτογράφησης. Η αιτία ανάπτυξης του DESX είναι η δραματική αύξηση της αντοχής του DES σε γνωστές επιθέσεις.

Δ. AES (Advanced Encryption Standard)

Το ακρωνύμιο AES προέρχεται από την φράση Advanced Encryption Standard. Είναι ένας block cipher που προορίζεται να γίνει τυποποίηση του FIPS και να αντικαταστήσει τον DES. Ο DES βρίσκεται ήδη πολλά χρόνια σε χρήση και από το 1998 το NIST δεν τον ανανεώνει.

E. DSS (Digital Signature Algorithm)

Το National Institute of Standards and Technology (NIST) δημοσιοποίησε το Digital Signature Algorithm (DSS), που είναι μέρος του Capstone Project της κυβέρνησης των Ηνωμένων Πολιτειών, τον Μάιο του 1994. Έχει καθιερωθεί σαν το επίσημο αλγόριθμο παραγωγής ψηφιακών υπογραφών της κυβέρνησης των Η.Π.Α. Βασίζεται στο πρόβλημα του διακριτού λογαρίθμου και χρησιμοποιείται μόνο για παραγωγή ψηφιακών υπογραφών. Η διαφορά από τις υπογραφές του RSA είναι ότι ενώ στο DSS η παραγωγή των υπογραφών είναι πιο γρήγορη από την επιβεβαίωση τους, στο RSA συμβαίνει το αντίθετο: η επιβεβαίωση είναι ταχύτερη από την υπογραφή. Παρ' όλο που μπορεί να υποστηριχθεί ότι η γρήγορη παραγωγή υπογραφών αποτελεί πλεονέκτημα, επειδή ένα μήνυμα υπογράφεται μία φορά αλλά η υπογραφή του μπορεί να επαληθευτεί πολλές φορές, κάτι τέτοιο δεν ανταποκρίνεται στην πραγματικότητα.

Το DSS έχει ολοκληρωθεί σε πολλά συστήματα ασφαλείας, αν και έχει λάβει πολλές άσχημες κριτικές. Τα κυριότερα θέματα κριτικής είναι η έλλειψη ευελιξίας, η αργή επαλήθευση των υπογραφών, η αδυναμία συνεργασίας με

άλλο πρωτόκολλο πιστοποίησης ταυτότητας και τέλος ότι ο αλγόριθμος δεν είχε αποκαλυφθεί.

3.2 Χαρακτηριστικά της Νεότερης Φύσης Ιών Worms και Σημεία Επιρροής των Ηλεκτρονικών Υπολογιστών

Αποτελεί γεγονός πως όποιος συνδέεται σήμερα στο Διαδίκτυο από τον υπολογιστή του, θα πρέπει προηγουμένως να έχει οπωσδήποτε εγκαταστήσει ένα ενημερωμένο πρόγραμμα προστασίας από ιούς, ώστε να προστατεύεται από κακόβουλα λογισμικά, όπως ιοί, δούρειοι ίπποι και ιοί τύπου worm. Οι ιοί τύπου worm διαδίδονται κυρίως μέσω του Διαδικτύου πολύ γρήγορα και απλά. Αυτή η μορφή κακόβουλου λογισμικού δεν χρειάζεται κάποιο αρχείο-φορέα, αλλά διαδίδεται αυτόνομα ως κρυφή δέσμη ενεργειών μέσω e-mail και ειδοποιήσεων κοινωνικών δικτύων, όπως το Facebook. Εκτός από τα αφαιρούμενα μέσα USB, κινδυνεύουν εν τω μεταξύ και τα έξυπνα τηλέφωνα από ιούς τύπου worm[78].

Εφόσον ενεργοποιηθεί μία φορά στον υπολογιστή, η δέσμη ενεργειών αρχίζει να υποκλέπτει κωδικούς πρόσβασης, δεδομένα λογαριασμών και άλλες παρόμοιες ευαίσθητες πληροφορίες και να τις στέλνει μέσω e-mail και ειδοποιήσεων. Ο ιός τύπου worm προσκολλάται σαν ιός στον τομέα εκκίνησης ενός υπολογιστή ή ενεργοποιείται κάθε φορά που εκτελείται κάποιο αρχείο. Δρα αυτόνομα στο παρασκήνιο. Πολλές φορές ένας ιός τύπου worm δεν χρειάζεται κάποιο βοηθητικό πρόγραμμα για να ενεργοποιηθεί, ενώ αρκεί η ενεργή επιφάνεια εργασίας των Windows ή η αυτόματη ρύθμιση παραμέτρων ενός USB stick.

Ακόμη και στην περίπτωση των ιών τύπου worm που δεν ενεργοποιούνται αυτόνομα, χάρη στο καλό καμουφλάρισμα το θύμα στέλνει οικειοθελώς τον ιό τύπου worm. Πολλές φορές οι ιοί τύπου worm καμουφλάρονται π.χ. σε κοινωνικά δίκτυα όπως το Facebook ως αναβαθμίσεις παιχνιδιού, κοινωνική βοηθητική δράση ή πρόσθετη λειτουργία, ώστε το ίδιο το θύμα να διαδίδει ανυποψίαστα τον ιό τύπου worm.

[78] Denning, D., E., 2007, "*Cryptography and Data Security*", Addison – Wesley

Οι ιοί τύπου worm μπορούν εύκολα να εισχωρήσουν κρυφά μέσω e-mail. Πολλές φορές το θύμα ακολουθεί κάποιον διαδικτυακό σύνδεσμο που φαίνεται να παρουσιάζει ενδιαφέρον και περιέχεται σε κάποιο e-mail με παραλήπτη το θύμα, και έτσι ξεκινά ο ιός τύπου worm. Η δέσμη ενεργειών του ιού τύπου worm ψάχνει κατά κανόνα τις πραγματικές διευθύνσεις e-mail από τα βιβλία διευθύνσεων των προγραμμάτων ηλεκτρονικού ταχυδρομείου στο σκληρό δίσκο του υπολογιστή, όπως π.χ. το Microsoft Outlook[79].

Το Μάιο του 2000 έγινε παγκοσμίως γνωστός ο ιός τύπου worm «I love you». Τα θύματα λάμβαναν έναν e-mail, φαινομενικά από κάποιον γνωστό αποστολέα του βιβλίου διευθύνσεών τους, με θέμα «I love you». Επισυναπτόταν μια δέσμη ενεργειών σε θεωρητικά ακίνδυνη μορφή txt. Η αποστολή της πραγματικής εφαρμογής «vbs» δεν φαινόταν στην τυπική εγκατάσταση του λειτουργικού συστήματος Windows. Μετά την ενεργοποίηση το μήνυμα «I love you» στελνόταν χιλιάδες φορές αυτόματα μέσω οποιουδήποτε προγράμματος ηλεκτρονικού ταχυδρομείου και προκαλώντας ζημιά δισεκατομμυρίων. Ο ιός τύπου worm διέγραφε από τους μολυσμένους υπολογιστές όλα τα αρχεία με κατάληξη .jpg, .jpeg, .vbs, .vbe, .js, .jse, .css, .wsh, .sct και .hta και τα αντικαθιστούσε με ομώνυμα αντίγραφα του ιού με κατάληξη .vbs. Επίσης, ο ιός «I love you» επισήμαινε όλα τα αρχεία με κατάληξη .mp2 και .mp3 ως κρυφά και τα αντικαθιστούσε επίσης με ένα ομώνυμο αντίγραφο του ιού με κατάληξη .vbs.[80]

Τέλος, ο διάσημος ιός τύπου worm «I love you» διαδόθηκε και μέσω του εξυπηρετητή IRC mIRC και αντικατέστησε τα αρχεία script.ini. Έτσι, ο ιός τύπου worm στάλθηκε σε όλους του χρήστες ενός καναλιού IRC. Όπως και στην περίπτωση των e-mail, οι ιοί τύπου worm μεταδίδονται και μέσω των προγραμμάτων άμεσης ανταλλαγής μηνυμάτων, όπως το ICQ ή το MSN Messenger. Ο χρήστης λαμβάνει ένα μήνυμα συνομιλίας από κάποιον γνωστό συνομιλητή, το οποίο περιλαμβάνει κάποιον ενδιαφέροντα σύνδεσμο. Ακολουθώντας το σύνδεσμο, ενεργοποιείται ο ιός τύπου worm. Και σε αυτήν την περίπτωση, δημιουργούνται αντίγραφα του ιού τύπου worm στις

[79] Meinel, C., P., 1998, "*The Happy Hacker"*, American Eagle Publications

[80] Denning, D., E., 2007, "*Cryptography and Data Security*", Addison – Wesley

προσωπικές επαφές του εκάστοτε βιβλίου διευθύνσεων, τα οποία αποστέλλονται αντιστοίχως σε όλες τις διευθύνσεις[81].

Οι διαδικτυακές πλατφόρμες ανταλλαγής, όπως το Kazaa ή το BitTorrent ευνοούν τη διάδοση των ιών τύπου worm. Σε αυτά τα ομότιμα δίκτυα [Peer-to-Peer (P2P)] βρίσκονται αρκετοί ιοί τύπου worm, οι οποίοι καμουφλάρονται με ελκυστικούς τίτλους, λαμβάνονται από το Διαδίκτυο, ενεργοποιούνται και προωθούνται εκατοντάδες φορές μέσω του μεγάλου αριθμού συμμετεχόντων. Το 2004 εμφανίστηκε για πρώτη φορά ο ιός τύπου worm σε κινητά τηλέφωνα και στάλθηκε αυτόνομα μέσω Bluetooth σε όλους τους διαθέσιμους παραλήπτες. Καθώς τα σύγχρονα κινητά τηλέφωνα, και ειδικά τα έξυπνα τηλέφωνα, μοιάζουν όλο και περισσότερο με τους υπολογιστές, η διάδοση των ιών τύπου worm είναι και σε αυτήν την περίπτωση αρκετά εύκολη – μέσω UMTS, WLAN, e-mail ή MMS[82].

3.3 Νεότερες Τεχνολογίες Προστασίας Έναντι των Worms

Οι νεότερες τεχνολογίες με σκοπό τη προστασία των ηλεκτρονικών υπολογιστών έναντι των ιών worms, επιτυγχάνεται στις μέρες μας μέσω των ακόλουθων εφαρμογών.

Εφαρμογή Firewall F-Secure Client Security 9

Υποστηρίζονται τα παρακάτω λειτουργικά:

- Microsoft Windows 7 (32 και 64 bit)
- Microsoft Windows Vista (32 και 64 bit)
- Microsoft Windows XP (με SP2 ή νεότερο)
- Microsoft Windows 2000 Professional (με SP4 Rollup 1 ή νεότερο)

[81] Denning, D., E., 2007, "*Cryptography and Data Security*", Addison – Wesley

[82] Denning, D., E., 2007, "*Cryptography and Data Security*", Addison – Wesley

Υπάρχει επίσης και έκδοση που περιλαμβάνει Firewall το οποίο έχει περισσότερες δυνατότητες από τα Firewall των Windows XP και Vista, F-Secure Client Security 9 με Firewall

Το λογισμικό που παρέχεται είναι το Firewall F-Secure Client Security και περιλαμβάνει:

- Antivirus για την πρόληψη και καταστολή των ιών σε αρχεία και email.
- Firewall για προστασία του Η/Υ από δικτυακές επιθέσεις κακόβουλων χρηστών και σκουληκιών (WORMS) του διαδικτύου.

Το συγκεκριμένο Firewall εκτελεί δύο κύριες λειτουργίες:

- Φιλτράρισμα των πακέτων βάση προρυθμισμένων ή καθορισμένων από το χρήστη κανόνων απόρριψης/αποδοχής πακέτων από και προς συγκεκριμένες υπηρεσίες.
- Έλεγχο των εφαρμογών (πχ Internet Explorer, Outlook, Firefox) που αποκτούν πρόσβαση στο διαδίκτυο ύστερα από έγκριση του χρήστη.

Αποτελεί λοιπόν γεγονός πως μια από τις μεγαλύτερες απειλές για τα συστήματα, είναι οι ιοί. Υπάρχει λογισμικό που μπορεί να αγοράσει κανείς και λέγεται λογισμικό anti-virus το οποίο εγκαθίσταται στο σύστημά και ελέγχει όλα τα εισερχόμενα και εξερχόμενα αρχεία για ιούς, συμπεριλαμβανομένων των αρχείων και e-mail που λαμβάνει κανείς στο Internet, προγραμμάτων που «κατεβάζει» και αρχείων που εισάγει μέσω CD-ROM ή δισκετών.

Οι περισσότεροι πάροχοι λογισμικών anti-virus έχουν δείγματα που μπορείτε να κατεβάσετε μέσω Internet και να χρησιμοποιήσουν για ένα περιορισμένο χρονικό διάστημα, αλλά και πολλοί νέοι υπολογιστές έχουν ήδη εγκατεστημένη μια δοκιμαστική έκδοση του λογισμικού αυτού. Όποιο λογισμικό και να επιλέξει κανείς, πρέπει να το ανανεώνει συχνά. Πολλοί πάροχοι των λογισμικών anti-virus προσφέρουν την δυνατότητα για συχνές αναβαθμίσεις (ή σε κάποιες περιπτώσεις ελέγχουν ακόμα και καθημερινά για αναβαθμίσεις) για ένα σταθερό κόστος κάθε χρόνο. Τα λογισμικά κατά των

ανεπιθύμητων e-mail και με σκοπό τη προστασία από ιούς worms, έχουν ως εξής.

Υπάρχει λογισμικό κατά των ανεπιθύμητων e-mail (λογισμικό anti-spam) που είναι σχεδιασμένο για να φιλτράρει τα ανεπιθύμητα μηνύματα. Μπορεί κανείς να δημιουργήσει ένα βασικό φίλτρο στα περισσότερα λογισμικά e-mail. Για παράδειγμα, μπορεί να ορίσει προϋποθέσεις ώστε να διαγράφονται τα e-mail ανάλογα με τις λέξεις στους τίτλους, τον παραλήπτη ή ανάλογα με λέξεις κλειδιά στο κυρίως κείμενο του e-mail.

Όπως προαναφέραμε, δεν υπάρχει 100% εγγύηση ότι δεν θα προσβληθεί ποτέ ο Η/Υ από κάποιον ιό όσο είστε στο Internet, ότι ποτέ δεν θα λάβει ανεπιθύμητα μηνύματα ή ότι δεν θα βρεθεί ποτέ σε ρίσκο. Μπορεί να χρησιμοποιήσει τα διαθέσιμα εργαλεία, συνδυάζοντάς τα όμως με κοινή λογική και ασκώντας ασφαλείς τακτικές για το Internet. Μερικοί τρόποι που μπορούν να βοηθήσουν να αποφύγει κάποιος την μόλυνση του συστήματός από ιούς είναι οι ακόλουθοι:

- Πάντα να έχει κανείς εγκατεστημένο λογισμικό anti-virus και να το κρατά ενημερωμένο.
- Να ορίσει το λογισμικό να ψάχνει το σύστημα αυτόματα για ανανεώσεις σε ώρες χαμηλής χρήσης όπως αργά το βράδυ ή τα Σαββατοκύριακα.
- Μην ανοίγει επισυναπτόμενα αρχεία σε e-mail εκτός και αν είναι κάτι που έχετε ζητήσει.
- Να λαμβάνει λογισμικό μόνο από εταιρίες που εμπιστεύεται. Να κάνει έρευνα αγοράς πριν αγοράσει και εγκαταστήσει κάποιο λογισμικό.
- Να απενεργοποιεί την επιλογή «προεπισκόπηση» (preview) στο λογισμικό του e-mail του.
- Να κρατά το σύστημά του ανανεωμένο με μέτρα ασφαλείας.

3.4 Σχεδιασμός Συστήματος Ασφαλείας για Ασφάλεια από Ιούς Worms

Ο σχεδιασμός του συστήματος βάσεως δεδομένων ασφαλείας για προστασία από ιούς worms οφείλει να αποτελεί τμήμα του αρχικού σχεδιασμού του συστήματος και όχι μια διαδικασία που θα εκτελείται μετά την εγκατάσταση του συστήματος. Οι λόγοι είναι απλοί. Αφενός είναι οικονομικότερο να σχεδιάζονται και να υλοποιούνται ταυτόχρονα το σύστημα και η ασφάλεια του και αφετέρου είναι λειτουργικότερο. Ο σχεδιασμός στηρίζεται σε πέντε βασικά βήματα[83]:

- *Βήμα 1*: Δημιουργία πολιτικής ασφαλείας
- *Βήμα 2*: Προσθήκη των κατάλληλων μεθόδων προστασίας ανάλογα με το πληροφοριακό σύστημα που θα χρησιμοποιήσουμε

- *Βήμα 3*: Σχεδίαση του συστήματος προστασίας που θα καλύπτει το φυσικό, το δικτυακό περιβάλλον και το περιβάλλον του υπολογιστικού συστήματος.

- *Βήμα 4*: Ανάπτυξη διαδικασιών για την παρακολούθηση, τον έλεγχο, την συντήρηση και την αναβάθμιση του συστήματος ασφαλείας.

- *Βήμα 5*: Χρήση των συμπερασμάτων από την παρακολούθηση και τον έλεγχο του συστήματος με στόχο την βελτίωση τόσο του σχεδιασμού, όσο και της υλοποίησης και λειτουργίας του συστήματος.

Στο πρώτο στάδιο πρέπει αρχικά να καθοριστεί η πολιτική ασφαλείας που θα ακολουθηθεί για το σύνολο του συστήματος για προστασία από ιούς worms. Αυτό περιλαμβάνει (υπολογιστές και δίκτυα), τα δεδομένα και τους ανθρώπους (διαχειριστές, προσωπικό συντήρησης, χρήστες, πελάτες). Η πολιτική ασφαλείας δημιουργείται μετά από ανάλυση και αξιολόγηση των αναγκών κάθε οργανισμού για τη διαθεσιμότητα, τους κινδύνους και τις δυνατότητες που πρέπει να διαθέτει το πληροφορικό του σύστημα. Απαρτίζεται από πλάνο που περιέχει τις διαδικασίες λειτουργίας και ελέγχου, τον απαραίτητο εξοπλισμό, αλλά και σενάρια, σχέδια και διαδικασίες

[83] Pfleeger, C., P., 1997, "*Security in Computing*", Prentice Hall

αντιμετώπισης κρίσεων. Σε αυτό το έγγραφο υπάρχουν λίγες τεχνικές λεπτομέρειες. Απλά λέει τι πρέπει να γίνει, όχι πως να γίνεται.

Το δεύτερο στάδιο περιλαμβάνει το σχεδιασμό του περιβάλλοντος που θα εγκατασταθεί η βάση δεδομένων για προστασία από ιούς worms. Με την έννοια περιβάλλον ορίζουμε όλα όσα υπάρχουν έξω από την εφαρμογή. Δηλαδή: οι υπολογιστές, τα λειτουργικά συστήματα, τα δίκτυα, καθώς και η φυσική τοποθεσία της εφαρμογής.

Το τρίτο στάδιο στο σχεδιασμό του συστήματος ασφαλείας για προστασία από ιούς worms αποτελεί η επιλογή των κατάλληλων μεθόδων προστασίας που θα χρησιμοποιηθούν. Γνωρίζοντας το γενικό σχεδιασμό της βάσης δεδομένων, την πολιτική ασφαλείας της εταιρείας, θα πρέπει ήδη να έχουμε καταλάβει ποιές είναι οι ανάγκες μας, τι προστασία θα χρειαστούμε και ποια τεχνολογία είναι η κατάλληλη.

Για να είναι επιτυχής ο σχεδιασμός του συστήματος ασφαλείας είναι ιδιαίτερα σημαντικό να έχει ληφθεί υπόψη και να έχουν καθοριστεί οι διαδικασίες μέσα από τις οποίες θα παρακολουθείται καθημερινά η λειτουργία του και θα ελέγχεται σε τακτικά χρονικά διαστήματα η απόδοσή του. Έτσι θα γίνονται οι απαραίτητες βελτιώσεις, προσθήκες και αναβαθμίσεις.

Για την χάραξη της πολιτικής που ακολουθεί μια εταιρεία ή ένας οργανισμός για την υλοποίηση της ασφάλειας της βάσης δεδομένων απαιτείται η ανάλυση επικινδυνότητας, όπου θα μελετηθούν οι εκθέσεις σε κίνδυνο (exposures) του συστήματος, προσδιορίζοντας τις ευπάθειες (vulnerabilities) και τις απειλές (threats) του με βάση τον υφιστάμενο έλεγχο (control). Τα αποτελέσματα μιας ανάλυσης επικινδυνότητας (risk analysis review) της υπολογιστικής και επικοινωνιακής υποδομής της εταιρείας θα προσδιορίσουν τις απαιτήσεις ασφαλείας της βάσης δεδομένων, καλύπτοντας τις παρακάτω συνιστώσες[84]:

- *Φυσική ασφάλεια του συστήματος (physical security)*: Προστασία ολόκληρου του σχετικού εξοπλισμού από φυσικές καταστροφές.

[84] Taylor, A., 1999, "*The Hackers*", Routledge

- *Ασφάλεια υπολογιστικού συστήματος (computer security)*: Προστασία των πληροφοριών της βάσης που διαχειρίζεται το λειτουργικό σύστημα (εφαρμογές, αρχεία δεδομένων, κ.ά.).

- *Ασφάλεια βάσεων δεδομένων (database security)*: Προστασία των περιεχομένων μιας βάσης δεδομένων.

- *Ασφάλεια δικτύων επικοινωνιών (network security)*: Προστασία των πληροφοριών κατά τη μετάδοσή τους μέσω τοπικών, τηλεφωνικών ή άλλων δικτύων (π.χ. Internet).

Επίλογος – Συμπεράσματα

Πολλοί είναι εκείνοι στις μέρες μας οι οποίοι έχουν αναρωτηθεί τι είναι ο ηλεκτρονικός υπολογιστής και τι προσφέρει. Η απάντηση που θα μπορούσε να δοθεί εδώ είναι πως ο ηλεκτρονικός υπολογιστής, δεν είναι τίποτα άλλο παρά ένα ακόμα μηχάνημα, το οποίο κατασκεύασε ο άνθρωπος και φυσικά όπως και τόσες άλλες μηχανές, οι οποίες έχουν ως στόχο να κάνουν ευκολότερη ή δυσκολότερη την καθημερινή ζωή των ανθρώπων[85]. Η σχετική ωφέλεια ή η βλάβη βέβαια και η οποία μπορεί να προξενείτε από τη χρήση του, εξαρτάται ουσιαστικά αποκλειστικά από τη χρήση που θα του κάνει κάποιος και όπως άλλωστε συμβαίνει με όλες τις μηχανές.

Βασικό τμήμα του σχεδιασμού ενός συστήματος ασφαλείας οικονομικών συναλλαγών, αποτελεί να εξακριβώσουμε τι επίπεδο ασφάλειας χρειάζεται και ποιές απειλές θα κληθεί να αντιμετωπίσει. Η επιλογή των μέτρων προστασίας γίνεται λαμβάνοντας υπόψη τι κόστος (οικονομικό, απόδοσης ή ενόχλησης λόγω της παρουσίας τους) έχουν για την εταιρεία. Το πρώτο λοιπόν, βήμα είναι να εντοπίσουμε τον εχθρό. Συνήθως οι άνθρωποι επικεντρώνονται στο

[85] Miglino, O., Lund, H.H. & Cardaci, M. (1999), Robotics as an Educational Tool, Journal of Interactive Learning Research, 10(1), 25-48

είδος της επίθεσης ξεχνώντας ότι οι επιθέσεις είναι τα εργαλεία. Για παράδειγμα, ένας αποφασισμένος εισβολέας θα επιμείνει πολύ περισσότερο από ένα τυπικό εισβολέα.

Όταν αναφερόμαστε σε ιούς, εννοούμε προγράμματα τα οποία έχουν δημιουργηθεί για να εισέλθουν στον υπολογιστή χωρίς την έγκρισή μας και να μολύνουν άλλα αρχεία. Είναι μικρά κομμάτια ηλεκτρονικού κώδικα, που έχουν τη δυνατότητα να αντιγράφουν και να εισάγουν τον εαυτό τους σε ένα εκτελέσιμο πρόγραμμα, αρχείο, δισκέτα ή μέρος σκληρού δίσκου. Ανάλογα με τη φύση του ιού, οι συνέπειες από τη μόλυνση μπορεί να είναι μηδαμινές έως και καταστροφικές. Ο ιός θα προσπαθήσει να αναπαραχθεί και να εξαπλωθεί, μολύνοντας όσο το δυνατόν περισσότερα αρχεία ή άλλους υπολογιστές σε τοπικό επίπεδο ή στο Internet.

Όπως ο ιός, έτσι και το worm είναι ένα πρόγραμμα που εξαπλώνεται από υπολογιστή σε υπολογιστή χωρίς να το γνωρίζει ο χρήστης. Επίσης, όπως και οι ιοί, τα worms μπορεί μερικές φορές να έχουν σκόπιμα επιβλαβή αποτελέσματα, παρόλο που σε πολλές περιπτώσεις και μόνο το γεγονός της αντιγραφής τους μπορεί να είναι αρκετό για να βλάψει υπολογιστές και δίκτυα. Οι βλάβες που προκαλεί ο συγκεκριμένος ιός, είναι οι εξής[86]

- Ο ιός προσκολλάται σε αρχεία (προγράμματα ή έγγραφα) στο δίσκο του χρήστη και εξαπλώνεται όταν αυτά τα αρχεία αντιγραφούν ή εκτελεστούν.
- Ένα worm παραμένει στο active memory του υπολογιστή και εξαπλώνεται από τον ένα υπολογιστή στον άλλο, ενώ παράλληλα μολύνει και άλλους υπολογιστές μέσω της σύνδεσης στο Διαδίκτυο.
- Λόγω του ότι τα worms χρησιμοποιούν τις δικτυακές συνδέσεις για να εξαπλωθούν, μπορούν να έχουν υπερβολικά γρήγορη εξάπλωση και να δημιουργήσουν μεγάλη δικτυακή κίνηση (μειώνοντας την ταχύτητα ή μη επιτρέποντας τη νόμιμη πρόσβαση στο δίκτυο).

[86] Denning, D., E., 2007, "*Cryptography and Data Security*", Addison – Wesley

- Ένα πρόσφατο και γνωστό worm ήταν το «CodeRed worm», το οποίο επηρεάζει τους Windows NT και Windows 2000 web servers. Αυτό το worm έχει υπό τον έλεγχό του τους μολυσμένους servers και τους χρησιμοποιεί για να επιτεθεί με «Denial of Service» σε άλλα Internet sites.

Βιβλιογραφία

- Adams, J., 1998, "*The next world war*", Simon and Schuster
- BloomBecker, B., 1990, "*Spectacular Computer Crimes*", Dow Jones – Irwin
- Ransom, A. W., 1994, "*Who Owns Information*", Basic Books
- Cavoukian, A., Tapscott, D., 1997, "*Who Knows",* McGraw-Hill
- Denning, D., E., 2007, "*Cryptography and Data Security*", Addison – Wesley
- Diffie, W., Landau, S., 1998, "*Beyond Calculation*", The MIT Press
- Hager, N., 1996, "*Secret Power*", Craig Cotton Publishing, New Zealand, 1996
- Kesler, R., 1988, "*Spy vs. Spy*", Pocket Books
- Libicki, G., M., 1995, "*What information is warfare?",* National Defense University of USA
- Ludlow, P., 1996, "*High Noon on the Electric Frontier*", The MIT Press
- McCarthy, L., 1997, "*Intranet Security*", Prentice Hall
- Meinel, C., P., 1998, "*The Happy Hacker"*, American Eagle Publications
- Pfleeger, C., P., 1997, "*Security in Computing*", Prentice Hall
- Rosenoer, J., 1997, "*CyberLaw"*, Springer – Verlag
- Timpton, H., F., Ruthberg, Z., G., 1993, "*Handbook of Information Security Management*", Acerbic
- Schneier, B., 1996, "*Applied Cryptography*", Prentice Hall
- Slade, P., 1994, "*Guide to Computer Viruses*", Springer – Verlag
- Schweizer, P., 1993, "*Friendly Spies*", The Atlantic Monthly Press
- Sterling, B., 1992, "*The Hacker Crackdown*", Bantam
- Taylor, A., 1999, "*The Hackers*", Routledge