Α.Τ.Ε.Ι ΠΑΤΡΩΝ
ΣΧΟΛΗ ΔΙΟΙΚΗΣΗΣ ΚΑΙ ΟΙΚΟΝΟΜΙΑΣ
ΤΜΗΜΑ ΔΙΟΙΚΗΣΗΣ ΕΠΙΧΕΙΡΗΣΕΩΝ

Πτυχιακή Εργασία με Θέμα:

« Ασφάλεια Δεδομένων και Επικοινωνιών των Επιχειρήσεων στο Διαδίκτυο (Internet) »

Σπουδάστρια:
Φίλιππα Βασιλική
(Α.Μ 4890)

Εισηγητής:
Αναγνώστου Παναγιώτης

ΠΑΤΡΑ 2004

Αφιερωμένο στους γονείς μου.

Περιεχόμενα

Γ' Μέρος

Δ' Μέρος

Α΄ Μέρος

Θεωρία Ασφάλειας

Εισαγωγή

Σε ένα συνεχώς διευρυνόμενο μέσο όπως το Διαδίκτυο, επενδύονται σημαντικά κεφάλαια σε υπηρεσίες, η αξία των οποίων αυξάνεται συνεχώς. Μια ιδιαίτερα ελκυστική εφαρμογή αποτελεί το "ηλεκτρονικό επιχειρείν". Μέσα σε αυτό το κλίμα, αυξάνονται δυστυχώς και οι ευκαιρίες για "ηλεκτρονικές απάτες". Μία από τις απαραίτητες προϋποθέσεις για την άνθηση του ηλεκτρονικού εμπορίου είναι η ασφάλεια των συναλλαγών. Για παράδειγμα, ο χρήστης που κάνει μια αγορά "σε πραγματικό χρόνο" (on line) πρέπει να είναι σίγουρος ότι ο αριθμός της πιστωτικής του κάρτας δε θα υποκλαπεί. Κάθε φορά που συνδιαλέγεται δικτυακά με την τράπεζά του (e-banking) θέλει να γνωρίζει ότι όντως έρχεται σε επαφή με την ίδια την τράπεζα και όχι με κάποιον που επιχειρεί να τον εξαπατήσει. Όταν αποστέλλει μέσω του Διαδικτύου ευαίσθητα δεδομένα, θέλει να ξέρει ότι δε θα έχει πρόσβαση σε αυτά κανείς άλλος εκτός από τον πραγματικό τους παραλήπτη. Από τη μεριά της, η κάθε επιχείρηση θα πρέπει να εγγυάται την ισχύ όλων των παραπάνω, εξασφαλίζοντας και διατηρώντας έτσι ένα κλίμα ασφάλειας και εχεμύθειας με τους πελάτες της.

Τα παραπάνω ίσως ακούγονται γενικά, υπερβολικά ή και περιορισμένης εμβέλειας. Ωστόσο, είναι σημαντικό να λαμβάνει κάποιος τα μέτρα του πριν καταλάβει με οδυνηρό τρόπο ότι οι κίνδυνοι είναι υπαρκτοί. Πράγματι, δεν έχει κανείς παρά να παρακολουθήσει για μικρό χρονικό διάστημα την επικαιρότητα γύρω από τα τεκταινόμενα στο Διαδίκτυο. Θύματα επιθέσεων, ενοχλητικών έως και επικίνδυνων "crackers" (κυβερνοναύτες που χρησιμοποιούν τις γνώσεις και τις τεχνικές δεξιότητές τους για παράνομους σκοπούς), πέφτουν συχνά μεγάλοι δικτυακοί τόποι, όπως το Yahoo, το Amazon, το δίκτυο της Microsoft, καθώς επίσης και μεγάλοι χρηματοπιστωτικοί οργανισμοί ή θωρακισμένοι τραπεζικοί λογαριασμοί, οι οποίοι "λυγίζουν" στις επιθέσεις τους.

Αποτελεί ειρωνεία το γεγονός ότι το ταπεινό PC στο σπίτι μας μπορεί στην πράξη να είναι περισσότερο ασφαλές όσον αφορά τους εξωτερικούς κινδύνους σε σύγκριση π.χ με τους διακομιστές της Microsoft. Οι λόγοι είναι σχετικά απλοί. Πρώτα απ' όλα μεγάλοι δικτυακοί τόποι γνωστών εταιρειών αποτελούν συχνά ελκυστικό στόχο για τους hackers, το κύρος των οποίων αυξάνει θεαματικά όταν εξαπολύουν μια επιτυχημένη επίθεση σε κάποιο μεγάλο διακομιστή. Βεβαίως, πέρα από τις "αγνές", ενθουσιώδεις επιθέσεις, υπάρχουν και αυτές που γίνονται από μισθοφόρους hackers με σκοπό την επίτευξη καίριων πληγμάτων σε εταιρείες και τη διάπραξη ηλεκτρονικών οικονομικών εγκλημάτων.

Οι διαχειριστές των συστημάτων των εταιρειών, από τη μεριά τους, είναι υποχρεωμένοι να αναζητούν διαρκώς τη χρυσή τομή ανάμεσα στην ευκολία και την ασφάλεια. Κάποιοι διακομιστές υπάρχουν για να εξυπηρετούν τους χρήστες του Διαδικτύου. Η πλήρης

θωράκισή τους δεν είναι ιδιαίτερα δύσκολη εάν υποθέσουμε ότι η απόλυτη ασφάλεια είναι εφικτή. Εντούτοις, όσο περισσότερο ασφαλείς γίνονται τόσο πιο δύσχρηστοι καθίστανται για τους χρήστες του Διαδικτύου, οι οποίοι μπορεί να είναι είτε πελάτες είτε απλοί επισκέπτες χωρίς ιδιαίτερες γνώσεις πληροφορικής.

Θα λέγαμε, μάλιστα, ότι τελευταία το ερασιτεχνικό "hacking" έχει εξελιχθεί σε κάποιας μορφής κακώς εννοούμενου χόμπι. Έτσι, η απροσεξία, η αμέλεια στη λήψη στοιχειωδών μέτρων ασφαλείας και η έλλειψη ενημέρωσης μπορεί να αποβούν καταστροφικές για την κάθε επιχείρηση. Από τη στιγμή που ο επίδοξος εισβολέας κατορθώσει να παρεισφρήσει στο δίκτυό της, θα έχει πλέον τη δυνατότητα να υποκλέψει τους κωδικούς των εργαζομένων της (password) στο διαδικτυακό φορέα της, να καταστρέψει ή να αλλοιώσει τα δεδομένα της, ή ίσως το χειρότερο απ' όλα, να κρυφτεί πίσω από τις ηλεκτρονικές της διευθύνσεις για να εξαπολύσει επίθεση κάπου αλλού. Ακόμα και εάν είναι απόλυτα προσεκτική και χρησιμοποιεί τα "καλύτερα" προγράμματα προστασίας, ο αποφασισμένος hacker θα προσπαθήσει να εντοπίσει αδυναμίες (π.χ του λογισμικού) και να τις εκμεταλλευθεί.

Στην παρούσα εργασία, θα αναλυθούν μερικές από τις τεχνικές που χρησιμοποιούν οι hackers, καθώς και οι αδυναμίες των υφιστάμενων τεχνολογιών τις οποίες εκμεταλλεύονται στην προσπάθεια για την επίτευξη των στόχων τους. Παράλληλα, θα παρουσιαστούν εργαλεία και προγράμματα που χρησιμοποιούνται για την προστασία ενός δικτύου υπολογιστών μιας επιχείρησης, όπου κατά πάσα πιθανότητα υπάρχει μόνιμη σύνδεση με το Διαδίκτυο. Προγράμματα αντιμετώπισης ιών και δούρειων ίππων, διαχειριστές των cookies, εργαλεία για κρυπτογράφηση και αποκρυπτογράφηση δεδομένων και προσωπικά φράγματα ασφαλείας (firewalls), θα είναι επίσης μερικά από τα θέματα που θα μας απασχολήσουν.

Τι είναι η Ασφάλεια των Πληροφοριακών Συστημάτων;

Η έννοια της ασφάλειας ενός πληροφοριακού συστήματος σχετίζεται με την ικανότητα ενός οργανισμού να προστατεύει τις πληροφορίες του από τυχόν αλλοιώσεις και καταστροφές, καθώς και από μη εξουσιοδοτημένη χρήση των πόρων του. Σχετίζεται επίσης, με την ικανότητά του να παρέχει ορθές και αξιόπιστες πληροφορίες, οι οποίες είναι διαθέσιμες στους εξουσιοδοτημένους χρήστες κάθε φορά που τις αναζητούν. Η ικανότητα αυτή στηρίζεται στη λήψη μέτρων, τα οποία διασφαλίζουν την ακεραιότητα και την εμπιστευτικότητα των δεδομένων, καθώς και την αδιάλειπτη λειτουργία του υπολογιστικού συστήματος.

Σύμφωνα με τα όσα αναφέρθηκαν περί ασφάλειας, η *ασφάλεια πληροφοριακών συστημάτων* έχει να κάνει με την πρόληψη και ανίχνευση μη εξουσιοδοτημένων ενεργειών των χρηστών ενός υπολογιστικού συστήματος καθώς και την λήψη μέτρων. Πιο συγκεκριμένα, η ασφάλεια των πληροφοριακών συστημάτων σχετίζεται με:

- *Πρόληψη (prevention)*: τη λήψη δηλαδή μέτρων για να αποφευχθούν «φθορές» των συστατικών ενός πληροφοριακού συστήματος.
- *Ανίχνευση (detection)*: τη λήψη μέτρων για την ανίχνευση του πότε, πώς και από ποιον προκλήθηκε φθορά σε ένα συστατικό ενός πληροφοριακού συστήματος.
- *Αντίδραση (reaction)*: τη λήψη δηλαδή μέτρων για την αποκατάσταση ή ανάκτηση των συστατικών ενός πληροφοριακού συστήματος.

Απλά παραδείγματα για κάθε ένα από τα παραπάνω σημεία είναι τα εξής:

Α. Από την καθημερινή μας ζωή

- η τοποθέτηση κλειδαριών στις πόρτες ή κάγκελων στα παράθυρα (πρόληψη)
- το σύστημα συναγερμού ή το κλειστό κύκλωμα τηλεόρασης (ανίχνευση)
- η κλήση της αστυνομίας και η αντικατάσταση κλεμμένων αντικειμένων ή η ασφαλιστική κάλυψη

Β. Από το χώρο του ηλεκτρονικού ταχυδρομείου

- η κρυπτογραφημένη διακίνηση δεδομένων παραγγελιών και πληρωμών (πρόληψη)
- η καταγραφή μιας ξένης συναλλαγής στη λίστα της πιστωτικής κάρτας (ανίχνευση)
- και τα πιθανά παράπονα, η ακύρωση συναλλαγής, η αλλαγή κάρτας κλπ (αντίδραση)

Η ασφάλεια μπορεί ακόμη να θεωρηθεί ότι αποτελείται από δύο κύριες συνιστώσες, την προστασία και τον έλεγχο, από τις οποίες η προστασία αναλύεται στην πρόληψη και την θεραπεία. Αξίζει να σημειώσουμε σε αυτό το σημείο, ότι δεν είναι εύκολο να δοθεί ένας μονοσήμαντος γενικός όρος της ασφάλειας των πληροφοριακών συστημάτων. Κατά την μελέτη της ασφάλειας κάθε επιμέρους συστήματος τεχνολογιών πληροφορικής και επικοινωνιών (όπως για παράδειγμα οι κινητές επικοινωνίες) πρέπει συχνά να δίνεται εξαρχής ο κατάλληλος ορισμός. Επομένως, πρέπει να δίνεται ιδιαίτερη προσοχή, όταν για παράδειγμα διαβάζουμε κάποιο σχετικό βιβλίο ή άρθρο, διαφορετικά υπάρχει κίνδυνος να δημιουργηθεί σύγχυση ανάμεσα σε αυτό που εμείς θεωρούμε ως ορισμό της ασφάλειας και τον ορισμό που εννοεί ο συγγραφέας.

Το μοντέλο ΕΑΔ και η Εξουσιοδότηση

Η ασφάλεια των πληροφοριών αποτελείται συνήθως από τρία στοιχεία: την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα. Γι΄ αυτό και συχνά αποκαλούνται από τα αρχικά τους «ΕΑΔ» της ασφάλειας των πληροφοριών. Αναλυτικά:

Εμπιστευτικότητα: σε πολλές περιπτώσεις της καθημερινής ζωής οι έννοιες της ασφάλειας και της εμπιστευτικότητας σχεδόν ταυτίζονται, όπως για παράδειγμα στα στρατιωτικά περιβάλλοντα όπου η ασφάλεια έχει τη σημασία του να κρατούνται μυστικές οι πληροφορίες.
Η εμπιστευτικότητα σημαίνει πρόληψη μη εξουσιοδοτημένης (unauthorized) αποκάλυψης πληροφοριών, δηλαδή πρόληψη από μη εξουσιοδοτημένη ανάγνωση. Επομένως, σημαίνει ότι τα δεδομένα ενός υπολογιστικού συστήματος, καθώς και τα διακινούμενα μεταξύ των υπολογιστών δεδομένα, αποκαλύπτονται μόνο σε εξουσιοδοτημένα άτομα, για συγκεκριμένο μόνο χρονικό διάστημα και με τον εγκεκριμένο μόνο τρόπο. Αυτό αφορά όχι μόνο την προστασία από μη εξουσιοδοτημένη αποκάλυψη των δεδομένων αυτών καθαυτών, αλλά ακόμη και από το γεγονός ότι τα δεδομένα απλώς υπάρχουν. Έτσι, για παράδειγμα, το γεγονός ότι κάποιος έχει φάκελο εγκληματία είναι συχνά το ίδιο σημαντικό όπως και οι λεπτομέρειες για το έγκλημα που διαπράχθηκε.
Άλλες εκφάνσεις της εμπιστευτικότητας είναι:

- Η ιδιωτικότητα (privacy), που σημαίνει προστασία των δεδομένων προσωπικού χαρακτήρα, δηλαδή αυτών που αφορούν συγκεκριμένα πρόσωπα και
- Η μυστικότητα (secrecy), που σημαίνει προστασία των δεδομένων που ανήκουν σε έναν οργανισμό.

Ακεραιότητα: η ακεραιότητα μπορεί να οριστεί γενικότερα ως η απαίτηση να είναι τα πράγματα όπως πρέπει να είναι. Στην πληροφορική, ακεραιότητα σημαίνει πρόληψη μη εξουσιοδοτημένης μεταβολής πληροφοριών, δηλαδή, πρόληψη από μη εξουσιοδοτημένη εγγραφή ή διαγραφή, συμπεριλαμβανομένης και της μη εξουσιοδοτημένης δημιουργίας δεδομένων. Επομένως, σημαίνει ότι η μετατροπή, διαγραφή και δημιουργία των δεδομένων ενός υπολογιστικού συστήματος, γίνεται μόνο από εξουσιοδοτημένα μέρη.

Διαθεσιμότητα ονομάζεται η ιδιότητα του να είναι προσπελάσιμες και χωρίς αδικαιολόγητη καθυστέρηση οι υπηρεσίες ενός πληροφοριακού συστήματος όταν τις χρειάζεται μια εξουσιοδοτημένη οντότητα. Αυτό σημαίνει ότι οι εξουσιοδοτημένοι χρήστες των υπολογιστικών συστημάτων και των επικοινωνιακών μέσων δεν αντιμετωπίζουν προβλήματα άρνησης εξυπηρέτησης (denial of service) όταν επιθυμούν να προσπελάσουν τους πόρους του συστήματος.

Η διαθεσιμότητα καλύπτει περιοχές πέρα από το φυσικό σκοπό της ασφάλειας. Για παράδειγμα, ένα μεγάλο μέρος της τεχνολογίας που απαιτείται για τη διασφάλιση της διαθεσιμότητας προέρχεται από άλλες περιοχές. Για τους σκοπούς της ασφάλειας, μας απασχολεί βασικά η παρεμπόδιση κακόβουλων επιθέσεων που αποσκοπούν στο να παρακωλύσουν την πρόσβαση των νόμιμων χρηστών σε ένα πληροφοριακό σύστημα. Αυτές οι επιθέσεις ονομάζονται *επιθέσεις άρνησης παροχής υπηρεσιών* (denial of service attacks). Η άρνηση παροχής υπηρεσιών σημαίνει παρεμπόδιση της εξουσιοδοτημένης προσπέλασης πληροφοριών και πόρων ή πρόκληση καθυστέρησης των λειτουργιών που είναι κρίσιμες στο χρόνο. Η αντιμετώπισή τους αποσκοπεί στο να υπερνικήσει την σκόπιμη (που προκαλείται από κακόβουλα μέρη) παρά τυχαία απώλεια της διαθεσιμότητας. Ένα παράδειγμα επίθεσης άρνησης παροχής υπηρεσιών είναι οι επιθέσεις «πλημμύρας» στο διαδίκτυο, όπου ο επιτιθέμενος κατακλύζει έναν εξυπηρέτη στέλνοντάς του έναν τεράστιο αριθμό αιτήσεων σύνδεσης.

Παρ' όλο που η διαθεσιμότητα συχνά αναδεικνύεται στο πλέον σημαντικό χαρακτηριστικό της ασφάλειας, εντούτοις λίγοι μηχανισμοί υπάρχουν για να βοηθήσουν την υποστήριξής της.

Το μοντέλο ΕΑΔ στηρίζεται στην αρχή της *εξουσιοδότησης*, δηλαδή στο ποιος επιτρέπεται να έχει πρόσβαση, σε τι και με ποιον τρόπο. Το «ποιος» στην περίπτωση αυτή μπορεί να είναι οποιαδήποτε οντότητα ικανή να δράσει. Περιλαμβάνει πρόσωπα καθώς και προγράμματα υπολογιστών. Το «τι» μπορεί να είναι οποιαδήποτε πηγή πληροφοριών που βρίσκεται σε οποιοδήποτε μέσο, στο οποίο περιλαμβάνονται συνήθως έγγραφα, δισκέτες,

μαγνητοταινίες, τηλεπικοινωνιακά μέσα, ραδιοτηλεοπτικές εκπομπές, υπολογιστές και δίκτυα υπολογιστών. Η πρόσβαση «με ποιο τρόπο» αναφέρεται σε αυτό, που επιτρέπεται να κάνει κάποιος με μία πηγή πληροφοριών. Η ασφάλεια των πληροφοριών ασχολείται με την προστασία των πηγών από πράξεις που δεν επιτρέπονται να γίνουν σε αυτές, ενώ δεν απαγορεύει τις αντίθετές τους. με απλά λόγια, φροντίζει να απομακρύνει τα κακά παιδιά, ενώ επιτρέπει στα καλά παιδιά να έχουν πρόσβαση στις πληροφορίες.

Οι πολιτικές που ακολουθούνται στο θέμα της εξουσιοδότησης ρυθμίζονται με συμβόλαια, με κανονισμούς ή με νόμους ή μπορεί να έχουν καθιερωθεί επίσημα ή ανεπίσημα από εκείνους που κατέχουν ή διευθύνουν διάφορες πηγές.

Πολλοί οργανισμοί χρησιμοποιούν διάφορες κατηγοριοποιήσεις, προκειμένου να χαρακτηρίσουν τις ευαίσθητες πληροφορίες που διαχειρίζονται. Μία εμπορική εταιρεία μπορεί, για παράδειγμα, να χαρακτηρίσει τις πληροφορίες της σαν «δημόσιες», «εμπιστευτικές» ή «για εσωτερική χρήση». Οι χαρακτηρισμοί αυτοί επιβάλλουν δυνατότητες πρόσβασης και χειρισμού των συγκεκριμένων πληροφοριών μέσα στα όριά της. Οι πληροφορίες μπορεί να έχουν και άλλες παραπέρα διακρίσεις και κάθε είδος τους να είναι προσιτό ή μη σε συγκεκριμένη ομάδα ενδιαφερομένων.

Δίκτυα και Διαδίκτυο

Δίκτυο (network) στον τομέα των επικοινωνιών είναι ένα σύστημα που συνδέει κυρίως τερματικές συσκευές κάθε είδους, είτε αυτές είναι απλές είτε πρόκειται για κανονικούς υπολογιστές, ενώ διαθέτει δομή τέτοια ώστε να επιτυγχάνεται η όποια μεταξύ τους επικοινωνία. Ένα δίκτυο αποτελείται επίσης από κόμβους, συσκευές τηλεπικοινωνιών και μέσα σύνδεσης /διέλευσης πληροφοριών. Κύριος σκοπός του είναι να αποκτήσουν οι χρήστες του κοινή χρήση στους υπάρχοντες πόρους, δηλαδή πρόσβαση σε συσκευές υλικού, λογισμικού και δεδομένα.

Ως *διαδίκτυο* (Internet) εννοείται κάθε συνένωση δύο ή περισσοτέρων δικτύων, όχι κατ' ανάγκη ίδιας τεχνολογίας, έτσι ώστε να επιτυγχάνεται η επικοινωνία μεταξύ τους και να λειτουργούν σε λογικό επίπεδο σαν ένα δίκτυο. Για την επίτευξη της διαδικτύωσης των επιμέρους δικτύων χρησιμοποιούνται συσκευές τηλεπικοινωνιών, όπως γέφυρες (bridges), πύλες (gateways), αναδιαμορφωτές (repeaters), δρομολογητές (routers) κλπ. Σήμερα, με τον όρο Διαδίκτυο εννοούμε το μεγαλύτερο σύμπλεγμα διαφορετικών δικτύων (net of nets) που χρησιμοποιούν ως πρωτόκολλο επικοινωνίας το TCP/IP, ενώ μπορεί να βρίσκονται εγκατεστημένα σε κάθε γωνιά του πλανήτη.

Με το Διαδίκτυο επιτυγχάνεται η διασύνδεση ετερογενών δικτύων Η/Υ. Ο ιδιαίτερος χαρακτήρας του προκύπτει από την ανοχή που διαθέτει σε αναξιόπιστες συνδέσεις, καθώς σχεδιάστηκε έτσι ώστε να υποστηρίζει πολλαπλές εναλλακτικές συνδέσεις μεταξύ των υπολογιστών, με αποτέλεσμα να διατηρεί τη λειτουργικότητά του ακόμα και με κατεστραμμένους κλάδους (π.χ σε περίπτωση εκτεταμένων φυσικών καταστροφών ή πυρηνικών εκρήξεων).

Το πρωτόκολλο TCP/IP (Transmission Control Protocol/ Internet Protocol) είναι αυτό που κατά κανόνα χρησιμοποιείται ως η προσυμφωνημένη μέθοδος επικοινωνίας και διαμεταγωγής δεδομένων στο Internet. Βασίζεται στη λογική του «πακέτου»: στον κόμβο του αποστολέα το μήνυμα της μετάδοσης τεμαχίζεται σε μικρά τμήματα σταθερού μεγέθους, τα οποία μεταδίδονται ανεξάρτητα μέσω του δικτύου. Κάθε πακέτο μεταφέρει ζωτικά στοιχεία για τη δρομολόγησή του (όπως π.χ η διεύθυνση προορισμού του) και ακολουθεί τη δική του διαδρομή μέσα στο δίκτυο. Στον κόμβο του παραλήπτη τα πακέτα συναρμολογούνται για να σχηματιστεί το αρχικό μήνυμα. Φυσικά, η όλη διαδικασία προϋποθέτει ότι κάθε υπολογιστής στο Διαδίκτυο έχει τη δική του διεύθυνση επικοινωνίας (IP address). Με τον τρόπο αυτό, επιτεύχθηκε η δημιουργία κατανεμημένων δικτύων, τα οποία δεν εξαρτώνται από ένα κέντρο οργάνωσης/ελέγχου και άρα δε χρειάζεται να στηρίζουν τη λειτουργία τους σε κάποιο κεντρικό υπολογιστή.

Ασφάλεια και Διαδίκτυο

Το Διαδίκτυο σχεδιάστηκε από επιστημονικές και ακαδημαϊκές κοινότητες προκειμένου να επιτευχθεί η ανταλλαγή πληροφοριών μεταξύ έμπιστων οντοτήτων. Το θέμα της ασφάλειας των ευαίσθητων πληροφοριών δεν απασχόλησε αρχικά τους σχεδιαστές του. Ο λόγος είναι ότι κανένας δε μπορούσε να προβλέψει τότε ότι θα επεκταθεί και θα συνδέσει την πλειοψηφία των δημόσιων και ιδιωτικών δικτύων που υπάρχουν στον κόσμο σήμερα.

Ένα δικτυωμένο σύστημα είναι επιρρεπές σε ένα αριθμό απειλών που προέρχονται και από νόμιμους χρήστες του συστήματος, αλλά και κυρίως από επίδοξους εισβολείς. Κάθε κόμβος του δικτύου είναι ένα υπολογιστικό σύστημα με όλα τα γνωστά προβλήματα ασφαλείας. Σε αυτά, έρχεται το δίκτυο να προσθέσει το πρόβλημα της επικοινωνίας (μέσω ενός πολύ εκτεθειμένου μέσου) και της προσπέλασης από μακρινές τοποθεσίες μέσω πιθανώς μη-έμπιστων υπολογιστικών συστημάτων. Μερικοί λόγοι για τους οποίους αποκτούν ιδιαίτερη σημασία τα θέματα ασφαλείας υπολογιστικών συστημάτων λόγω της ύπαρξης των δικτύων, είναι τα εξής:

- Η αυξημένη πολυπλοκότητα, που περιορίζει το αίσθημα εμπιστοσύνης για την ασφάλεια των δικτύων.
- Υπάρχει αύξηση στον αριθμό των διαύλων επικοινωνίας και άρα των πιθανών σημείων επίθεσης, τα οποία πρέπει να «οχυρωθούν» κατάλληλα.
- Έχουν γίνει ασαφή τα όρια των δικτύων και οι διακρίσεις μεταξύ των τμημάτων ενός οργανισμού. Κάθε κόμβος οφείλει να είναι ικανός να αντιδράσει σωστά στην παρουσία ενός νέου και μη-έμπιστου κόμβου. Από την άλλη, κάθε κόμβος μπορεί να ανήκει ταυτόχρονα σε περισσότερα από ένα δίκτυα, με αποτέλεσμα να μην είναι ξεκάθαρη η εικόνα των νομίμων χρηστών του κάθε δικτύου.
- Η δυνατότητα ανωνυμίας ενός χρήστη απαιτεί ισχυρούς μηχανισμούς πιστοποίησης μεταξύ των υπολογιστών, που συνήθως είναι διαφορετικοί από αυτούς που πιστοποιούν τους ανθρώπους (χρήστες) στα υπολογιστικά συστήματα.
- Υπάρχει αδυναμία ελέγχου της δρομολόγησης των δεδομένων που διακινούνται μέσω των δικτύων.

Κίνδυνοι ασφάλειας

Το Διαδίκτυο ως μέσο ψηφιακής επικοινωνίας κρύβει έναν αριθμό από σοβαρούς κινδύνους, όπως:

- Έλλειψη εμπιστευτικότητας, αφού τα δεδομένα που διακινούνται είναι χωρισμένα σε πακέτα και μπορούν εύκολα να κλαπούν και να αποκαλυφθεί το περιεχόμενό τους.
- Έλλειψη μηχανισμών για την ταυτοποίηση των οντοτήτων (χρηστών) των συστημάτων. Όλα τα συστήματα που είναι συνδεδεμένα στο Διαδίκτυο αναγνωρίζονται από την IP διεύθυνσή τους. το πρωτόκολλο IP δεν παρέχει κάποιο μηχανισμό για την αυθεντικοποίηση των χρηστών του συστήματος.
- Έλλειψη αξιόπιστων μέσων για σύνδεση των IP διευθύνσεων με συγκεκριμένους υπολογιστές.
- Εκτεθειμένοι κωδικοί πρόσβασης. Τα περισσότερα συστήματα χρησιμοποιούν κωδικούς για την ταυτοποίηση των χρηστών, οι οποίοι τις περισσότερες φορές μεταφέρονται στο δίκτυο χωρίς να κρυπτογραφηθούν.

Η υπηρεσία του Παγκόσμιου Ιστού (WWW) εισάγει ακόμα περισσότερους κινδύνους. Ένας παρουσιαστής ιστοσελίδων (browser) αποτελεί το ιδανικό μέσο για την αυτόματη εκτέλεση προγραμμάτων χωρίς τη γνώση του χρήστη, γνωστών ως Δούρειοι Ίπποι (των οποίων παρουσίαση θα γίνει στην συνέχεια της παρούσας εργασίας).

Ευπάθειες

Ευπάθεια ονομάζεται μια αδυναμία ή ένα ευάλωτο σημείο στο σύστημα ασφαλείας που μπορεί, αν αξιοποιηθεί κατάλληλα, να προκαλέσει απώλειες ή ζημιές. Όταν ένα άτομο εκμεταλλεύεται μια ευπάθεια, τότε διαπράττει μια *επίθεση* στο σύστημα.

Κάθε πληροφοριακό σύστημα είναι ευπαθές σε πιθανές επιθέσεις. Οι πολιτικές και τα προϊόντα ασφαλείας μπορούν να μειώσουν την πιθανότητα του να καταστεί δυνατόν μια επίθεση να διαπεράσει τις άμυνες του συστήματος (ή τουλάχιστον απαιτούν από έναν επίδοξο εισβολέα να επενδύσει τόσο χρόνο και πόρους ώστε να μην αξίζει πλέον να συνεχίσει). Θα πρέπει όμως να έχουμε σχετικά υπόψη μας, ότι στην πράξη για καμία σχεδόν δραστηριότητα δεν υπάρχει αυτό που αποκαλούμε «πλήρης ασφάλεια» ή «τελείως ασφαλές σύστημα», κάτι που θα επαναληφθεί πολλές ακόμη φορές στην παρούσα εργασία.

Μια κατηγοριοποίηση των τυπικών σημείων ευπάθειας σε ένα υπολογιστικό σύστημα θα μπορούσε να περιλαμβάνει τα εξής:

- *φυσικές ευπάθειες* (physical), που αφορούν το «φυσικό περιβάλλον», π.χ τα κτίρια και τους χώρους των μηχανογραφικών κέντρων. Μια πρώτη άμυνα ενάντια σε πιθανές εισβολές παρέχουν τα κλασσικά μέσα προστασίας, όπως ο έλεγχος της φυσικής προσπέλασης, οι φύλακες, οι βιομετρικές συσκευές, οι αντικλεπτικοί συναγερμοί κλπ.
- *εκ φύσεως ευπάθειες* (natural). Οι υπολογιστές είναι ιδιαίτερα ευπαθείς σε φυσικές καταστροφές και περιβαλλοντικές απειλές, όπως οι πυρκαγιές, οι πλημμύρες, οι σεισμοί, οι κεραυνοί και οι διακοπές ρεύματος. Ακόμη, επηρεάζονται αρνητικά από τη σκόνη, την υγρασία και τις ακραίες θερμοκρασιακές συνθήκες.
- *ευπάθειες υλικού και λογισμικού* (hardware and software), όπου πιθανές δυσλειτουργίες του υλικού και του λογισμικού μπορούν να προκαλέσουν την διακοπή παροχής των υπηρεσιών ενός πληροφοριακού συστήματος είτε λόγω ενδογενών σφαλμάτων είτε λόγω εσφαλμένης εγκατάστασης των συστατικών μερών του.
- *ευπάθειες μέσων* (media), όπου η κλοπή ή καταστροφή μαγνητικών μέσων και εκτυπωτικών καταστάσεων μπορεί να προκαλέσει την απώλεια ή διαρροή ευαίσθητων δεδομένων.
- *ευπάθειες εκπομπών* (emanation). Όλες οι ηλεκτρονικές συσκευές εκπέμπουν ηλεκτρομαγνητική ακτινοβολία. Με κατάλληλο εξοπλισμό είναι πιθανή η υποκλοπή των εκπεμπόμενων σημάτων από συστήματα και δίκτυα υπολογιστών και η αποκωδικοποίησή τους με σκοπό την υφαρπαγή κρίσιμων πληροφοριών, ή την παρεμπόδιση της ομαλής λειτουργίας ενός πληροφοριακού συστήματος.

- *ευπάθειες επικοινωνιών* (communications). Η σύνδεση ενός υπολογιστή σε ένα ανοικτό δίκτυο (όπως το Internet) αυξάνει τον κίνδυνο διείσδυσης από τρίτα μη εξουσιοδοτημένα μέρη. Με αυτό τον τρόπο, μηνύματα μπορούν να υποκλαπούν, να αλλάξουν διαδρομή και να χαλκευτούν. Οι γραμμές σύνδεσης των υπολογιστών είναι τα συνηθέστερα σημεία που μπορούν να χρησιμοποιηθούν για υποκλοπή ή ακόμα και για καταστροφή.
- *ανθρώπινες ευπάθειες* (human). Οι άνθρωποι που διαχειρίζονται και χρησιμοποιούν έναν υπολογιστικό σύστημα αποτελούν συνήθως τη μεγαλύτερη πηγή ευπαθειών γι' αυτό. Συνήθως, η ασφάλεια ενός πληροφοριακού συστήματος εξαρτάται κατά πρώτο λόγο από τους ανθρώπους που το χρησιμοποιούν νόμιμα. Η έλλειψη εκπαίδευσης, ο δόλος, η απροσεξία και η επιπολαιότητα στο χειρισμό ευαίσθητων στοιχείων, όπως για παράδειγμα τα συνθηματικά καθώς και οι κακοπροαίρετοι ή παραπονούμενοι υπάλληλοι αποτελούν τις μεγαλύτερες απειλές (insiders) για την ασφάλεια ενός πληροφοριακού συστήματος.

Απειλές

Απειλή για ένα υπολογιστικό σύστημα αποτελούν καταστάσεις όπου υπάρχει το ενδεχόμενο πρόκλησης απωλειών ή ζημιών (π.χ ανθρώπινες επιθέσεις, φυσικές καταστροφές, ακούσια ανθρώπινα λάθη, εσωτερικές ατέλειες τους εξοπλισμού ή του λογισμικού κλπ). Σε σχέση με τους κύριους πόρους ενός πληροφοριακού συστήματος, (δηλαδή το υλικό, το λογισμικό και τα δεδομένα) διακρίνουμε τα ακόλουθα είδη απειλών του:

- *υποκλοπή*, όπου κάποιο μη εξουσιοδοτημένο μέρος έχει καταφέρει να αποκτήσει προσπέλαση σε ένα τμήμα του συστήματος. Ενδεικτικά παραδείγματα είναι η κλοπή εξαρτημάτων, η αθέμιτη αντιγραφή προγραμμάτων ή αρχείων δεδομένων, η καλωδιωμένη παρακολούθηση ή υποκλοπή γραμμής με σκοπό την απόκτηση δεδομένων καθώς κυκλοφορούν σε ένα δίκτυο κλπ. Πρόκειται για απειλή κυρίως κατά της εμπιστευτικότητας του συστήματος.
- *μεταβολή*, όπου κάποιο μη εξουσιοδοτημένο μέρος δεν έχει απλά καταφέρει να αποκτήσει πρόσβαση, αλλά επιπλέον παραποιεί λογισμικό ή δεδομένα. Ενδεικτικά παραδείγματα είναι η τροποποίηση ενός προγράμματος από έναν ιό, η αλλαγή των τιμών σε μια βάση δεδομένων κλπ. Πρόκειται για απειλή κυρίως κατά της ακεραιότητας του συστήματος.
- *πλαστογραφία*, όπου νοείται η απειλή αποκλειστικά ενάντια στα δεδομένα ενός συστήματος και συμβαίνει όταν κάποιο μη εξουσιοδοτημένο μέρος εισάγει επιπρόσθετα-παραποιημένα δεδομένα σε ένα πληροφοριακό σύστημα. Ενδεικτικά παραδείγματα είναι η εισαγωγή πλαστών συναλλαγών σε ένα τραπεζικό περιβάλλον, η προσπάθεια αναπαραγωγής

παλιών μηνυμάτων κλπ. Πρόκειται για απειλή κατά της ακεραιότητας και της διαθεσιμότητας του συστήματος.

- *διακοπή*, όπου ένα μέρος του συστήματος γίνεται μη διαθέσιμο ή άχρηστο ή χάνεται εντελώς. Ενδεικτικά παραδείγματα είναι το σβήσιμο προγραμμάτων ή αρχείων, η κακοήθης καταστροφή μιας συσκευής κλπ. Πρόκειται κυρίως για απειλή κατά της διαθεσιμότητας του συστήματος. Ο όρος άρνηση εξυπηρέτησης –αντίθετος του όρου διαθεσιμότητα- περιγράφει συνήθως μια επιτυχημένη επίθεση διακοπής.

Πέρα από τα είδη των απειλών που αναφέρθηκαν παραπάνω, έχουμε και την ένταξή τους στις τρεις ακόλουθες κατηγορίες, η οποία γίνεται βάσει της προελεύσεώς τους:

- *φυσικές απειλές*: τέτοιου είδους καταστροφές (φωτιά, πλημμύρα κλπ) δεν είναι πάντα δυνατό να αποτραπούν. Όμως, είναι σημαντικό η εκδήλωση παρόμοιων γεγονότων να διαπιστώνονται έγκαιρα, ώστε να ελαχιστοποιούνται οι πιθανότητες δραματικών ζημιών. Όπως επίσης σημαντικό είναι να αποφεύγονται ενέργειες που αυξάνουν την πιθανότητα εξάπλωσής τους (όπως για παράδειγμα το κάπνισμα). Τέλος, η ετοιμότητα χρήσης εφεδρικού συστήματος, σε συνδυασμό με τη λήψη τακτικών εφεδρικών αρχείων (back ups) για τα κρίσιμα δεδομένα, περιορίζει τις πιθανές δυσάρεστες συνέπειες.
- *ακούσιες απειλές*: προκαλούνται είτε από αστοχίες υλικού ή λογισμικού, είτε από άγνοια ή αδιαφορία του ανθρώπινου παράγοντα. Σημαντικός παράγοντας πρόκλησης τέτοιων απειλών είναι η έλλειψη σωστής εκπαίδευσης, είτε πρόκειται για απλούς χρήστες είτε για διαχειριστές των συστημάτων. Να σημειωθεί, ότι το ποσοστό των προβλημάτων που δημιουργούνται από άγνοια στα πληροφοριακά συστήματα είναι πολύ μεγαλύτερο από εκείνο που οφείλεται σε κακή πρόθεση.
- *εκούσιες απειλές*: είναι αυτές που απασχολούν περισσότερο τη δημοσιότητα. Στην κατηγορία αυτή, οι κακόβουλοι χρήστες μπορεί να ανήκουν στο εσωτερικό του συστήματος (insiders), για παράδειγμα κάποιοι δυσαρεστημένοι υπάλληλοι. Είναι όμως πιθανό, οι απειλές να προέρχονται από κάποιους επίδοξους εισβολείς που είναι εξωτερικοί χρήστες (outsiders). Στην περίπτωση αυτή, η επιτυχία των επιθέσεων εξαρτάται κυρίως από τα μέσα που διαθέτουν, δηλαδή το χρόνο, την υπολογιστική ισχύ, τις γνώσεις, τα άτομα, τα χρήματα, τις συσκευές και τα εξαρτήματα. Οι κακοήθεις χρήστες μπορεί να επιδιώκουν εκδίκηση, οικονομικό κέρδος, αναγνώριση ή λόγω ιδιοσυγκρασίας απλά τη δημιουργία προβληματικών καταστάσεων και τη διάπραξη βανδαλισμών.

Πληροφοριακός πόλεμος

Εν συνεχεία, θα ήταν ιδιαίτερα χρήσιμο και ενδιαφέρον να αναφερθούμε στο περιεχόμενο αυτής της έννοιας, η οποία θα καταστήσει πιο παραστατική την διεξοδική ανάλυση της ασφάλειας των πληροφοριακών συστημάτων. Άρα:

«ο πληροφοριακός πόλεμος αποτελείται από πράξεις με τις οποίες επιδιώκεται η προστασία, η εκμετάλλευση, η φθορά, η διάψευση ή η καταστροφή πληροφοριών ή πηγών πληροφοριών με σκοπό να επιτευχθεί ένα σημαντικό πλεονέκτημα, ένας σκοπός ή μία νίκη σε βάρος ενός αντιπάλου».

Μορφές του πληροφοριακού πολέμου αποτελούν οι εισβολές σε Η/Υ, οι κατασκοπευτικοί δορυφόροι, οι παράνομες ακροάσεις, οι κάμερες επιτήρησης, ο ηλεκτρονικός πόλεμος, οι καταστροφές εγκαταστάσεων επικοινωνιών, η παραποίηση εγγράφων, ο επηρεασμός απόψεων, οι ψυχολογικές πιέσεις και η δημιουργία ιών των Η/Υ. Ακόμη, η κλοπή εμπορικών μυστικών, η παραβίαση του ιδιωτικού απορρήτου, οι απάτες που γίνονται μέσω ηλεκτρονικού ταχυδρομείου κλπ. Με βάση τις περιστάσεις διάπραξής τους, κάποιες από τις πράξεις αυτές θεωρούνται και είναι εγκλήματα. Άλλες είναι νόμιμες παρότι ανήθικες. Κάποιες άλλες θεωρούνται αποδεκτές κυβερνητικές πρακτικές. Κοινό τους χαρακτηριστικό πάντως είναι ότι όλες στοχεύουν ή εκμεταλλεύονται πληροφοριακές πηγές προς όφελος εκείνου που τις κάνει και σε βάρος κάποιου άλλου.

Η θεωρία του πληροφοριακού πολέμου στηρίζεται στην αξία των πηγών των πληροφοριών σε σχέση με μια επιθετική και αμυντική ενέργεια.

➢ Ο *επιθετικός πληροφοριακός πόλεμος* αποτελεί μια δραστηριότητα νίκης-ήττας. Διεξάγεται συνήθως χωρίς τη συγκατάθεση του οποιουδήποτε αμυντικού μηχανισμού και χωρίς τη γνώση των δυνατοτήτων αυτού του τελευταίου. Ακόμα και όταν αυτός ο αμυντικός μηχανισμός συμφωνεί να συμμετάσχει, δε γνωρίζει πλήρως τα κίνητρα της επίθεσης που δέχεται καθώς και τις συνέπειες που θα έχει γι' αυτόν. Με πιο απλά λόγια, αυτό που στέφει με απόλυτη επιτυχία κάθε προσπάθεια για επιθετικό πόλεμο, είναι η εκμετάλλευση των αδυναμιών των πληροφοριακών πηγών. Οι αδυναμίες αυτές αφορούν τόσο το υλικό μέρος όσο και τα προγράμματα των υπολογιστών αλλά και τους χρήστες τους. Ο υπάλληλος, για παράδειγμα, μιας επιχείρησης που αποκαλύπτει το συνθηματικό εισόδου στο σύστημά της σ' ένα hacker, που βρίσκεται στην άλλη άκρη του τηλεφώνου και ο οποίος του λέει ότι το χρειάζεται για να λύσει κάποιο πρόβλημά του, δε γνωρίζει τις αληθινές του προθέσεις. Το μόνο σίγουρο πάντως είναι ότι η λήψη απολύτως ασφαλών αμυντικών μέτρων είναι πάρα πολύ

δύσκολη, και τα προβλήματα ασφάλειας εμφανίζονται σε περιοχές όπου κάτι τέτοιο θεωρείται αδιανόητο. Παρότι πολλές πηγές πληροφοριών μπορούν να ασφαλιστούν ακόμη και ενάντια στην πιο πολύπλοκη επίθεση, 100% ασφάλεια δεν είναι ούτε δυνατή ούτε αξίζει τα λεφτά, που θα μπορούσε να δώσει κανείς προκειμένου να την επιτύχει. Τα συστήματα των υπολογιστών είναι ιδιαίτερα πολύπλοκα και περιέχουν χιλιάδες γραμμές κωδικών. Κανένα άτομο δεν μπορεί να κατανοήσει τόσο καλά τους κώδικες αυτούς έτσι, ώστε να εγγυηθεί την πλήρη ασφάλεια του οποιουδήποτε συστήματος. Επιπλέον, τα συστήματα και τα περιβάλλοντα αλλάζουν συχνά και ακόμα και οι περισσότερο προστατευμένες πηγές είναι σε γενικές πηγές πρώτες στην απειλή, που προέρχεται από χρήστες από το εσωτερικό της επιχείρησης, που εξυπηρετούν και οι οποίοι έχουν νόμιμη πρόσβαση σε αυτά. Το θέμα που προκύπτει στην συγκεκριμένη περίπτωση είναι η διαχείριση του κινδύνου και όχι η ολοκληρωτική αποφυγή του με οποιοδήποτε κόστος.

- Ο *αμυντικός πληροφοριακός πόλεμος* από την άλλη, επιδιώκει την προστασία των πηγών πληροφοριών από κάθε επίθεση. Ο στόχος του είναι η διατήρηση της αξίας των πηγών ή σε περίπτωση που η επίθεση που θα δεχθούν αποδειχθεί επιτυχής, η ανάκτηση της αξίας τους που χάθηκε. Οι αμυντικές τακτικές εμπίπτουν σε έξι γενικές κατηγορίες: την πρόληψη, την αποτροπή, τις οδηγίες και προειδοποιήσεις, την ετοιμότητα για την αντιμετώπιση εκτάκτων περιστατικών και την απάντηση στην επίθεση. Τα μέτρα και η τεχνολογία που χρησιμοποιούνται για αμυντικούς σκοπούς, δεν αποκλείεται να ανήκουν σε περισσότερες από μία από τις κατηγορίες αυτές. Αυτό το είδος του πληροφοριακού πολέμου συνδέεται στενά με την ασφάλεια των πληροφοριών. Δεν ταυτίζονται ωστόσο απόλυτα. Η ασφάλεια των πληροφοριών ασχολείται κυρίως με πηγές, που κατέχει κάποιος ιδιώτης και με την προστασία τους από λάθη, ατυχήματα, φυσικές καταστροφές και από πράξεις που γίνονται σκόπιμα εναντίον τους. Ο αμυντικός πληροφοριακός πόλεμος αντιθέτως, αφορά πηγές που δεν κατέχει κάποιος ιδιώτης και στις οποίες περιλαμβάνονται τα δημόσιας χρήσης γραπτά και ηλεκτρονικά ΜΜΕ αλλά δεν ασχολείται με ακούσιες πράξεις. Ο όρος «διασφάλιση πληροφοριών», που χρησιμοποιείται συχνά, περιλαμβάνει τόσο την ασφάλεια πληροφοριών όσο και τον πληροφοριακό πόλεμο.

Σύντομη ιστορική αναδρομή

Ο πληροφοριακός πόλεμος δεν είναι κάτι το καινούριο. Οι άνθρωποι ενδιαφέρονταν ανέκαθεν για την προστασία των πληροφοριών τους από τους αντιπάλους τους. Πριν από 5000 χρόνια, για παράδειγμα, οι Κινέζοι αυτοκράτορες φύλασσαν το μυστικό της παραγωγής του μεταξιού με την απειλή θανατικής ποινής με βασανιστήρια.

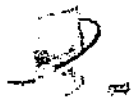
Παρ' όλ' αυτά όμως, έχει αναπόφευκτα υποστεί μεταβολές που οφείλονται στα νέα πληροφοριακά μέσα και στη σύγχρονη τεχνολογία. Προς τα μέσα του 20ου αιώνα, ένας πληροφοριακός πολεμιστής δε θα ήταν δυνατό να σκεφθεί να εισβάλλει σε ένα σύστημα Η/Υ για να κλέψει μυστικά, να τοποθετήσει έναν ιό σε ένα δίκτυο υπολογιστών, να παρακολουθήσει τηλεφωνικές συνομιλίες κλπ. Αυτό θα ήταν αδύνατο, γιατί απλούστατα δεν υπήρχε η συγκεκριμένη τεχνολογία. Γύρω στο 1950 οι υπολογιστές βέβαια υπήρχαν (όπως το ραδιόφωνο και η τηλεόραση), λίγοι όμως τους είχαν και κανείς από αυτούς δεν είχε την παραμικρή σύνδεση με τους άλλους, ούτε υπήρχε δυνατότητα πρόσβασης σε αυτόν. Δεν υπήρχαν τόποι του Παγκόσμιου ιστού για να εισβάλλει κανείς παράνομα, ούτε παροχείς Internet για να τους κάνει κανείς ζημιά, ούτε συναλλαγές μέσω του Internet για να εμποδιστούν και ούτε ηλεκτρονικό ταχυδρομείο για τη διανομή επικίνδυνων κωδικών. Δεν υπήρχε φτηνός οικονομικός τρόπος με τον οποίο ο οποιοσδήποτε θα μπορούσε να στείλει σε χιλιάδες άτομα καταστροφικούς ιούς, υβριστικά και απατηλά μηνύματα κλπ.

Μόλις το 1960 άρχισε η διασύνδεση των υπολογιστών, σε πρώτη φάση στο τοπικό δίκτυο ενός οργανισμού. Το 1969 τέθηκε σε λειτουργία το πρώτο ευρύτερο δίκτυο υπολογιστών στις ΗΠΑ. Παίρνοντας το όνομα του χορηγού του, που ήταν το Advanced Research Project Agency, που λειτουργούσε στο Υπουργείο Άμυνας, το APRANET συνέδεσε διάφορα Πανεπιστημιακά Ιδρύματα μεταξύ τους. Έτσι ξεκίνησε το Internet -το δίκτυο των δικτύων- που απλώνεται πλέον σε όλη την υφήλιο. Όταν τελικά το APRANET παροπλίστηκε το 1990, υπήρχαν περισσότεροι από 300.000 χρήστες του Internet. Ο αριθμός αυτός τινάχθηκε στο 1.000.000 το 1992, στα 10.000.000 το 1996 και στα 30.000.000 το 1998. Κατά το Σεπτέμβριο του 1998 η Ιρλανδικά εταιρεία NUA ανέβαζε τους χρήστες του Internet παγκοσμίως στα 147.000.000.

Δυστυχώς, όμως, καθώς ο δικτυωμένος πληθυσμός αυξάνει παγκόσμια, ο αριθμός των πιθανών πολεμιστών του επιθετικού πληροφοριακού πολέμου και οι πιθανοί στόχοι τους θα αυξάνουν μαζί του. Βρισκόμαστε στις αρχές ενός νέου αιώνα και οι υπολογιστές βρίσκονται παντού. Είναι φθηνοί, συχνά μικροσκοπικοί και συνδεδεμένοι μεταξύ τους και ενσωματωμένοι στα πάντα, από φούρνους μικροκυμάτων μέχρι τηλεκατευθυνόμενα βλήματα. Χρησιμοποιούνται παντού, στις εμπορικές συναλλαγές, στις τράπεζες και στην οικονομία, στις

μεταφορές και τη ναυτιλία, στην ενέργεια και την ύδρευση, στην εκπαίδευση, στη διασκέδαση, στην κυβέρνηση, στην υγεία, σε επείγοντα περιστατικά και σε στρατιωτικές επιχειρήσεις. Με τη βοήθειά τους, έχει αναπτυχθεί το ηλεκτρονικό εμπόριο, η τηλεϊατρική, η τηλεσυνδιάσκεψη και οι τηλεσυναλλαγές. Μία συνέπεια του γεγονότος αυτού είναι ότι οι ευαίσθητες πληροφορίες, που κάποτε περιορίζονταν σε συνομιλίες και σε έγγραφα στο χώρο των γραφείων, μεταφέρονται σήμερα μέσω των δημόσιων δικτύων των υπολογιστών, καθιστώντας έτσι τους εαυτούς τους πιθανά αντικείμενα κλοπής, εκμετάλλευσης, και δολιοφθοράς από τρίτα άτομα που βρίσκονται μακριά.

Β΄ Μέρος



Επιθετικός Πληροφοριακός Πόλεμος

Το έγκλημα

Η εγκληματική δραστηριότητα χωρίζεται σε δύο είδη: στα εγκλήματα της πνευματικής ιδιοκτησίας και στην απάτη. Πολλές από τις υπόλοιπες εγκληματικές πράξεις, που αναφέρονται παρακάτω, εμπίπτουν στον τομέα της δολιοφθοράς των πηγών των πληροφοριών.

Εγκλήματα κατά της πνευματικής ιδιοκτησίας: τα εγκλήματα κατά της πνευματικής ιδιοκτησίας περιλαμβάνουν την πειρατεία και την κλοπή εμπορικών μυστικών. Η πειρατεία πληροφοριών περιλαμβάνει την παράνομη απόκτηση και διανομή υλικών, που καλύπτονται με κοπιράιτ και στα οποία ανήκουν εικόνες σε ηλεκτρονική μορφή, ήχοι και βίντεο, που έχουν αποθηκευθεί σε μαγνητικές ταινίες, σε ψηφιακούς δίσκους και σε σκληρούς δίσκους υπολογιστών, καθώς και προγράμματα υπολογιστών αποθηκευμένα με τη μορφή ηλεκτρονικών αρχείων και τα οποία κυκλοφορούν σε δισκέτες. Παρότι ορισμένοι πειρατές είναι έφηβοι hackers και συνηθισμένοι πολίτες, υπάρχει ένα άλλο σημαντικό εγκληματικό στοιχείο, που προσπαθεί να επωφεληθεί από τη μαζική παραγωγή και την πώληση των κλεμμένων αγαθών. Το 1996 οι μεγαλύτερες βιομηχανίες έχασαν από 18 έως 20 εκατομμύρια δολάρια από την πειρατική κυκλοφορία των προϊόντων τους έξω από τη χώρα., σύμφωνα με την International Intellectual Property Alliance. Μέσα στις ΗΠΑ οι ίδιες απώλειες υπολογίστηκαν σε 2.8 δισεκατομμύρια δολάρια. Η πειρατεία πληροφοριών περιλαμβάνει επίσης την ιδιοποίηση των εμπορικών σημάτων. Η κλοπή των εμπορικών μυστικών περιλαμβάνει τη χωρίς άδεια απόκτηση των μυστικών μιας εμπορικής επιχείρησης.

Θα πρέπει να σημειωθεί, πάντως, πως δεν έχουν όλες οι απόπειρες που στρέφονται ενάντια στην πνευματική ιδιοκτησία, εγκληματική υφή. Οι εμπορικές επιχειρήσεις συγκεντρώνουν συχνά πληροφορίες για τους ανταγωνιστές τους από τις ανοιχτές πηγές, στις οποίες περιλαμβάνονται τα δημόσια αρχεία, έγγραφα από το Internet, εμπορικές εκθέσεις και θέματα, που μπορεί να ζητηθούν με βάση το νόμο για την ελεύθερη διακίνηση των πληροφοριών. Παρότι οι ευαίσθητες πληροφορίες δεν περιλαμβάνονται στις ανοιχτές πηγές, η συλλογή στοιχείων από αυτές είναι απολύτως νόμιμη.

Η απάτη: τα εγκλήματα της κατηγορίας αυτής περιλαμβάνουν τις απατηλές αγορές από μακριά, την κλοπή ταυτότητας και την τραπεζική απάτη, την απάτη στις τηλεπικοινωνίες και την απάτη με τη χρήση και την κατάχρηση του υπολογιστή.

Στην απάτη των αγορών από απόσταση, ο δράστης έχοντας πρόσβαση σε κάποιο μέσο επικοινωνίας με το κοινό, συνήθως το συμβατικό τηλέφωνο, το ηλεκτρονικό ταχυδρομείο ή κάποια ιστοσελίδα, στέλνει μηνύματα με ελκυστικές προσφορές. Τα θύματα ανταποκρίνονται

και πληρώνουν με τις πιστωτικές τους κάρτες ή με τραπεζικές επιταγές για να πάρουν αντάλλαγμα κάποιο μεγάλο χρηματικό βραβείο ή οτιδήποτε θα τα έκανε «γρήγορα πλούσια», όπως τους υποσχόταν ο δράστης.

Η κλοπή της ταυτότητας αφορά την απόκτηση πρόσβασης στα αναγνωριστικά στοιχεία ενός προσώπου, όπως στο όνομά του, στον αριθμό της κοινωνικής του ασφάλισης, στην άδεια οδήγησης και στους αριθμούς των τραπεζικών του λογαριασμών. Ο κλέφτης στη συνέχεια κάνει διάφορες πράξεις στο όνομα του θύματός του, όπως ανάληψη χρημάτων, αγορές και χρηματικά δάνεια. Με τον τρόπο αυτό δημιουργείται σοβαρό πρόβλημα στους τραπεζικούς και πιστωτικούς λογαριασμούς του θύματος, το οποίο δε σχετίζεται με τη συμπεριφορά του ίδιου. Ο εγκληματίας κερδίζει από αυτή την πλαστοπροσωπία, ενώ το θύμα ζημιώνεται οικονομικά και όχι μόνο. Η ζωή ορισμένων θυμάτων γίνεται εφιαλτική, καθώς προσπαθούν να αποκαταστήσουν τις ζημιές που υπέστησαν.

Οι περισσότερες κλοπές ταυτότητας αποτελούν ένα είδος τραπεζικής απάτης. Σε ορισμένες περιπτώσεις, η απάτη στρέφεται κατά ενός εταιρικού λογαριασμού και αφορά τη δημιουργία μεγάλων χρηματικών ποσών, που επιβαρύνουν το λογαριασμό αυτό. Παρότι τέτοιες ενέργειες γίνονται συνήθως από υπαλλήλους της επιχείρησης-θύμα, έχουν αναφερθεί και λίγες περιπτώσεις τρίτων, που απέκτησαν χωρίς να έχουν σχετικό δικαίωμα πρόσβαση στα συστήματα οικονομικών οργανισμών.

Στο χώρο των τηλεπικοινωνιακών απατών, οι εγκληματίες αποκτούν πρόσβαση σε πληροφορίες των θυμάτων τους, που σχετίζονται με τις τηλεφωνικές κυρίως επικοινωνίες τους και στη συνέχεια τις πωλούν. Έτσι, κρυφακούν τηλεφωνικές συνομιλίες, παίρνουν τους αριθμούς των τηλεφώνων και κάνουν τηλεφωνήματα που επιβαρύνουν τους λογαριασμούς των θυμάτων τους.

Οι απάτες με πιστωτικές κάρτες και οι απάτες στις τηλεπικοινωνίες αποτελούν περιπτώσεις της βασικής/κύριας απάτης, η οποία προϋποθέτει την από κάποιο τρίτο χωρίς εξουσιοδότηση χρήση ενός λογαριασμού, αντί για το νόμιμο κάτοχό του. Οι σχετικές επιβαρύνσεις επιβάλλονται στον κλεμμένο λογαριασμό. Η απάτη με υπολογιστές αποτελεί μια ακόμη μορφή της βασικής/κύριας απάτης.

Απάτη με υπολογιστές και καταχρήσεις: η απάτη με υπολογιστές και οι καταχρήσεις των υπολογιστών περιλαμβάνουν την πρόσβαση σε αυτούς χωρίς εξουσιοδότηση, την υπέρβαση της εξουσιοδότησης, όταν έχει δοθεί, καθώς και την διενέργεια επιβλαβών για τους υπολογιστές πράξεων. Χαρακτηριστικές μορφές τέτοιων δραστηριοτήτων αποτελούν η πρόσβαση και η απόκτηση ευαίσθητων πληροφοριών, η πραγματοποίηση εικονικών

συναλλαγών, η επέμβαση σε έγγραφα και η καταστροφή προγραμμάτων, αρχείων και εξοπλισμού. Οι ενέργειες αυτές προσφέρουν στο δράστη μεγαλύτερη πρόσβαση σε ευαίσθητες πληροφορίες περιορίζοντας ταυτόχρονα την ακεραιότητα των συστημάτων, που έχουν προσβληθεί καθώς και την ικανότητά τους για την παροχή των υπηρεσιών τους. Ο δράστης μπορεί να είναι ένας εξωτερικός hacker ή ένας υπάλληλος που κάνει κακή χρήση των δυνατοτήτων πρόσβασης, που έχει στο σύστημα. Οι ζημιές που προκύπτουν από τις επεμβάσεις αυτές και από τις χαμένες υπηρεσίες φτάνουν σε ορισμένες περιπτώσεις πολύ μεγάλα χρηματικά ποσά.

Τα εγκλήματα και οι καταχρήσεις με υπολογιστές βρίσκονται σε ανώτερα επίπεδα, πράγμα το οποίο αναμφίβολα οφείλεται στη διάδοση των συγκεκριμένων τεχνολογιών και στην εξάπλωση του Internet.

Απάτη στις τηλεπικοινωνίες

Η απάτη στις τηλεπικοινωνίες μπορεί να πάρει διάφορες μορφές. Ξεχωριστό ενδιαφέρον παρουσιάζουν στη συγκεκριμένη περίπτωση οι μορφές απάτης στις οποίες ο δράστης προσθέτει την παράνομη χρήση που κάνει ο ίδιος στη νόμιμη χρήση του ιδιοκτήτη ενός λογαριασμού, με αποτέλεσμα η επιπλέον χρέωση να επιβαρύνει αυτόν τον τελευταίο. Σε αυτές τις απάτες τηλεπικοινωνιών το κόστος συνήθως είναι πολύ μεγάλο.

Κρυφή παρακολούθηση συνομιλιών: τα περισσότερα επικοινωνιακά σήματα είναι δυνατό να αποτελέσουν με λίγη προσπάθεια αντικείμενο παρακολούθησης, ενώ για άλλα απαιτούνται περισσότερο εξειδικευμένα όργανα και αξιόλογες πηγές. Επειδή οι ενέργειες αυτές δεν μπορούν να διαπιστωθούν από τα άτομα που επικοινωνούν μεταξύ τους, οι επιθέσεις αυτές ονομάζονται «παθητικές» σε αντίθεση με τις «ενεργητικές» επιθέσεις, οι οποίες απενεργοποιούν ή εξουδετερώνουν τα σήματα. Στα όργανα παρακολούθησης ανήκουν μικρόφωνα («κοριοί»), τα μαγνητόφωνα, οι συσκευές παγίδευσης τηλεφώνων, οι ψηφιακοί σαρωτές, τα ραδιόφωνα, οι δέκτες μικροκυμάτων και δορυφορικών σημάτων, οι δορυφόροι κατάσκοποι, τα δίκτυα υπολογιστών και τα φίλτρα που ξεχωρίζουν τις ενδιαφέρουσες πληροφορίες. Τα παραβολικά μικρόφωνα μπορούν να πιάσουν συνομιλίες από ένα χιλιόμετρο μακριά και οι εκδόσεις τους σε λέιζερ μπορούν να πιάσουν συνομιλίες από την οπτική ευθεία ενός κλειστού παραθύρου.

Για να παρακολουθήσει κανείς ένα κανονικό ενσύρματο τηλέφωνο, θα πρέπει είτε να βρει ένα φυσικό σημείο σύνδεσης, όπως μια τηλεφωνική καμπίνα ή ένα εξωτερικό κουτί ή να αποκτήσει πρόσβαση στο διακόπτη ενός υπολογιστή προς τον οποίο κατευθύνονται οι κλήσεις.

Με την αυξανόμενη όμως χρήση των οπτικών ινών για την πραγματοποίηση τόσο τοπικών όσο και υπεραστικών κλήσεων, η απόκτηση φυσικής πρόσβασης στα ίδια τα σύρματα καθίσταται πραγματικά αδύνατη.

Οι hackers των υπολογιστών, από την μεριά τους, διεισδύουν στους υπολογιστές τηλεφωνικών εταιρειών για να παρακολουθήσουν ή να παρέμβουν στις επικοινωνίες. Τέλος, οι συμμορίες του οργανωμένου εγκλήματος παρακολουθούν συχνά τις επικοινωνίες της αστυνομίας για να ενημερώνονται για τις εναντίον τους δραστηριότητές της.

Πρόσβαση στο τηλεφωνικό κέντρο και άλλες παρόμοιες απάτες: οι σημερινοί phreakers έχουν ανακαλύψει άλλους τρόπους για να κλέβουν τηλεφωνικές υπηρεσίες. Ένας συνηθισμένος τρόπος αφορά την πρόσβαση στο τηλεφωνικό κέντρο (ΤΚ) μιας εταιρείας και τη στη συνέχεια χρησιμοποίησή του για την πραγματοποίηση τηλεφωνικών συνδιαλέξεων, που χρεώνονται στη συγκεκριμένη εταιρεία.

Η απάτη στις τηλεπικοινωνίες προσελκύει τους δράστες για αρκετούς λόγους. Ο πρώτος είναι, ότι ο κίνδυνος της σύλληψής τους είναι μικρός επειδή τα εγκλήματα, που τυπικά γίνονται από απόσταση, είναι πιθανό να ανακαλυφθούν και να εντοπιστούν. Ένας phreaker μπορεί να περάσει μια κλήση από διεθνή κυκλώματα, ιδιωτικά δίκτυα ή αλληλοσυνδεδεμένες γραμμές. Ο δεύτερος λόγος είναι ότι δεν απαιτείται ειδικός εξοπλισμός για ορισμένες κατηγορίες επιθέσεων, όπως πχ εκείνες που γίνονται κατά τηλεφωνικών κέντρων. Ο τρίτος λόγος είναι ότι υπάρχουν χρήματα στις τηλεφωνικές κλήσεις. Οι απατεώνες πωλούν συχνά υπεραστικές κλήσεις σε τρίτους, σε τιμές χαμηλότερες από αυτές που ισχύουν επίσημα.

Οι phreakers μπορούν να μπαίνουν σε τηλεπικοινωνιακά συστήματα σπάζοντας απλούς κωδικούς. Σύμφωνα με την Central & East European CrimiScope, Αραβόφωνοι εγκληματίες έσπασαν τον κωδικό καρτοτηλεφώνων, που ήταν σε χρήση στη Μακεδονία, πράγμα που τους επέτρεψε να κάνουν υπεραστικά τηλεφωνήματα. Στην αρχή τηλεφώνησαν σ' ένα τηλεφωνικό πίνακα. Στη συνέχεια, όταν το ηχογραφημένο μήνυμα άρχισε να παίζεται, κάλεσαν το 9 και ακολούθησε ένας τετραψήφιος μυστικός κωδικός αριθμός. Σε πολλές περιπτώσεις, ο κωδικός ενός συστήματος «1111» δεν έχει αλλάξει. Οι hackers χρησιμοποίησαν τη μέθοδο αυτή για να αποκτήσουν πρόσβαση στα τηλέφωνα του Υπουργείου Εξωτερικών της Μακεδονίας.

Hackers

Στην παρούσα εργασία η χρήση της λέξης «hacker» γίνεται για να αναφερθούμε σε πρόσωπα που αποκτούν πρόσβαση ή που εισβάλλουν σε ηλεκτρονικά συστήματα και ιδιαίτερα σε εκείνα των υπολογιστών και των τηλεπικοινωνιών. Στον όρο αυτό περιλαμβάνονται και οι όροι «crackers» (αναφέρεται σε αυτούς που σπάνε κωδικούς πρόσβασης για να εισβάλλουν σε έναν υπολογιστή) και «phreakers» (αναφέρεται σε αυτούς που εισβάλλουν σε τηλεφωνικά συστήματα). Η λέξη hacker έχει ωστόσο μια πολύ ευρύτερη -και όχι υποτιμητική- έννοια, η οποία περιλαμβάνει κάθε φανατικό οπαδό των υπολογιστών, που το αρέσει να ασχολείται με αυτούς και τα προγράμματά τους. Οι περισσότεροι από αυτούς τους ανθρώπους δεν ασχολούνται με εγκληματικές δραστηριότητες. Είναι έμπειροι προγραμματιστές και τεχνικοί δικτύων και ασχολούνται με την κατασκευή και, όταν χρειαστεί και με την επισκευή τους.

Κάποιοι είναι αντίθετοι με τη χρήση του όρου «hacker» για την αναφορά σε εκείνους που εισβάλλουν παράνομα σε συστήματα υπολογιστών και ειδικότερα σε εκείνους που χρησιμοποιούν τα διάφορα μέσα έχοντας λίγες γνώσεις ή μόνο επιφανειακό ενδιαφέρον για το πώς δουλεύουν. Κατά τη γνώμη τους, τα άτομα αυτά ανήκουν στους crackers και όχι στους hackers.

Κίνητρα και πολιτισμός: τα κίνητρα των νεαρών hackers είναι διάφορα και σε αυτά περιλαμβάνονται η συγκίνηση, η πρόκληση, η ευχαρίστηση, η γνώση, η αναγνώριση, η δύναμη και η φιλία. Σύμφωνα με τα λόγια ενός πρώην hacker η δραστηριότητα αυτή έχει ως εξής:

> «Το hacking ήταν κάτι το εντελώς συναρπαστικό για εμένα. Ερχόμουν από μία ακόμα βαρετή μέρα στο σχολείο, άνοιγα τον υπολογιστή μου και γινόμουν μέλος της ελίτ των hackers. Ήταν ένας εντελώς διαφορετικός κόσμος, στον οποίο δεν υπήρχαν ενήλικοι που δε σε αποδέχονταν και όπου κρινόσουν μόνο από το ταλέντο σου. Με το hacking τρέχω με χίλια μίλια την ώρα και ξεχνώ τα πάντα για' μένα καθώς πετιέμαι από τον υπολογιστή στον άλλο προσπαθώντας να προσεγγίσω το στόχο μου. Είναι σα να προσπαθώ να λύσω ένα σταυρόλεξο βιαστικά και με πολύ μεγάλη ένταση στη σκέψη μου. Η αδρεναλίνη μου φθάνει στα ύψη και η σκέψη πως κάνω κάτι παράνομο την ενισχύει περισσότερο. Κάθε βήμα που κάνω θα μπορούσε να οδηγήσει τις αρχές πάνω μου. Είμαι στην κορυφή της τεχνολογίας και την εξερευνώ, βαδίζοντας σαν σπηλαιολόγος σε ηλεκτρονικά σπήλαια, στα οποία κανονικά δεν πρέπει να βρίσκομαι».

Το hacking είναι μια δραστηριότητα εν μέρει κοινωνική και εν μέρει εκπαιδευτική. Οι hackers εργάζονται και κατοικούν σε ιστοσελίδες του Internet, σε καταλόγους διανομής ηλεκτρονικού ταχυδρομείου, σε χώρους συνομιλιών (ανταλλαγής μηνυμάτων σε πραγματικό χρόνο), σε ιστοσελίδες, σε ομάδες νέων κλπ. Κυκλοφορούν δε και περιοδικά, τα περισσότερα από τα οποία είναι σε ηλεκτρονική μορφή. Οι εκδόσεις αυτές χρησιμοποιούνται για την πώληση τεχνικών και προγραμμάτων για hacking και για την κυκλοφορία σχετικών ειδήσεων. Παρουσιάζουν οδηγούς για το πώς θα εισβάλλει κανείς σε συστήματα υπολογιστών, πώς θα αποφύγει την ανακάλυψή του, πώς θα κλέψει τηλεφωνικές υπηρεσίες, πώς θα κρυφακούσει τηλεφωνικές συνομιλίες, πώς θα διαστρεβλώσει τηλεοπτικά σήματα και γενικά πώς θα αποφύγει κάθε μέτρο ασφάλειας. Προσφέρονται προγράμματα και εντολές για το σπάσιμο των κωδικών, εντοπισμού συνδυασμών ασφάλειας στο Internet και δημιουργίας ιών. Οι hackers μπορούν να κατεβάσουν και να τρέξουν τα συγκεκριμένα προγράμματα χωρίς καν να γνωρίζουν τη λειτουργία τους. παρότι οι περισσότερες από τις πηγές των προγραμμάτων αυτών απευθύνονται σε αυτούς, διαβάζονται και από τους ειδικούς της ασφάλειας των υπολογιστών καθώς και από ερευνητές που επιθυμούν να γνωρίζουν τις τελευταίες πληροφορίες που κυκλοφορούν στον υπόκοσμο των υπολογιστών.

Κάτι περισσότερο από παιδικό παιχνίδι: πολλοί hackers, ίσως οι περισσότεροι, μεγαλώνοντας σταματούν στην ηλικία των 18 ετών τις δραστηριότητές τους, όταν μπορούν να διωχθούν σαν ενήλικοι. Κάποιοι άλλοι, όμως, συνεχίζουν και ορισμένοι από αυτούς δεν είναι ευχαριστημένοι με την παραβίαση των μέτρων ασφαλείας, την απόκτηση γνώσεων και την περιπλάνηση στο χώρο των πληροφοριών. Έτσι, κάνουν απάτες και δολιοφθορές, πράξεις που επιδοκιμάζονται από το σύνολο της υποπολιτισμικής τους κοινότητας. Δεν είναι ασυνήθιστο το να γίνεται λόγος για hackers που κυκλοφορούν με κλεμμένους αριθμούς πιστωτικών καρτών, με πειρατικά προγράμματα, που τοποθετούν graffiti σε ιστοσελίδες και που αποσυντονίζουν παροχείς Internet. Hackers που κατεβάζουν ευαίσθητα έγγραφα, που δεν τους ανήκουν και που παραφυλάνε για να διαβάσουν ηλεκτρονικά μηνύματα. Μια ομάδα hackers έσβησε δεδομένα από το Learning Link, ένα δημόσιο τηλεοπτικό σταθμό, οι υπολογιστές του οποίου εξυπηρετούσαν εκατοντάδες σχολεία. Ακόμα και οι hackers που δεν προκαλούν σκόπιμα ζημιά, μεταβάλλουν τα αρχεία συστημάτων και διαγράφουν τους τρόπους εισόδου τους σε αυτά για να καλύψουν την εισβολή τους και για να μπορούν να επαναλάβουν το εγχείρημά τους οποτεδήποτε στο μέλλον. Εννοείται ότι απαιτείται σημαντικός χρόνος και προσπάθεια για την αποκατάσταση των ζημιών, που προκλήθηκαν στο σύστημα και για την επαναλειτουργία

του. Σε αρκετές περιπτώσεις, τα θύματα υπολογίζουν ότι το κόστος αποκατάστασης των ζημιών τους ανέρχεται σε μερικές εκατοντάδες χιλιάδες δολάρια.

Οι hackers έχουν εισβάλλει σε συστήματα υπολογιστών τόσο του δημοσίου όσο και του ιδιωτικού τομέα, στα οποία περιλαμβάνονται κυβερνητικοί οργανισμοί, εμπορικές επιχειρήσεις, νοσοκομεία, πιστωτικά και οικονομικά ιδρύματα καθώς και πανεπιστήμια. Έχουν εισβάλλει στα δημόσια τηλεφωνικά δίκτυα προξενώντας κάθε είδους ζημιά σ' αυτά σχετιζόμενη με τη λειτουργία τους, τη συντήρησή τους και την τροφοδοσία τους. Έχουν καταστρέψει σταθμούς αναμετάδοσης σημάτων, διακόπτες κυκλοφορίας και άλλα παρόμοια δικτυακά συστήματα. Έχουν βάλει προγράμματα με «βόμβες χρόνου» προγραμματισμένα να κλείσουν κεντρικούς διακόπτες, έχουν καταστρέψει υπηρεσίες παροχής βοήθειας σε επείγοντα περιστατικά και έχουν καυχηθεί ότι μπορούν να κατεβάσουν όλους τους διακόπτες στο Μανχάταν. Έχουν επίσης, πραγματοποιήσει επιθέσεις σε ιδιωτικά ανταλλακτήρια συναλλάγματος και σε εταιρικά δίκτυα. Έχουν κάνει τηλεφωνικές υποκλοπές, έχουν εκτρέψει από την πορεία τους τηλεφωνικές κλήσεις , έχουν αλλάξει τους χαιρετισμούς σε συστήματα φωνητικού ταχυδρομείου, έχουν διαρρήξει ηλεκτρονικά γραμματοκιβώτια και έχουν κάνει υπεραστικά τηλεφωνήματα με έξοδα των θυμάτων τους –επιβαρύνοντας μερικά από αυτά με τηλεφωνικά τέλη υπέρογκων ποσών. Όταν μάλιστα δεν μπορούν να δαμάσουν την τεχνολογία, χρησιμοποιούν την τεχνική της «κοινωνικής χειραγώγησης» για να ξεγελάσουν τους υπαλλήλους για να τους επιτρέψουν την πρόσβαση στα συστήματά τους.

Απ' όλα τα παραπάνω προκύπτει και ο ορισμός του επαγγελματία hacker:

«Σαν επαγγελματίας hacker προσδιορίζεται εκείνος που έχει την ικανότητα να δημιουργήσει πρωτότυπες μεθόδους παράνομης εισόδου σε υπολογιστές. Έχει επίσης ανώτερες ικανότητες προγραμματισμού σε πολλές γλώσσες μηχανής και ταυτόχρονα έχει και αυθεντικές γνώσεις στα τηλεπικοινωνιακά δίκτυα. Όσον αφορά δε τους σκοπούς του, αυτοί είναι συνήθως οικονομικοί».

Κίνδυνος εκ των έσω

Οι υπάλληλοι έχουν κάνει δολιοφθορές σε πηγές πληροφοριών, χρησιμοποιώντας τόσο συμβατικά όπλα όσο και προγράμματα υπολογιστών. Συγκεκριμένα:

- Στις *συμβατικές επιθέσεις* στόχος μπορεί να είναι κάθε στοιχείο ενός συστήματος πληροφοριών-υπολογιστές, εκτυπωτές, συσκευές αποθήκευσης, συστήματα επικοινωνιών, γραπτό υλικό και προσωπικό. Οι δολιοφθορές μπορεί να χρησιμοποιούν όπλα που ξεκινούν από μαχαίρια και σπίρτα και καταλήγουν σε εκρηκτικά μεγάλης ισχύος.
- Στις *επιθέσεις σε προγράμματα υπολογιστών* περιλαμβάνεται κάθε πράξη, που ανακατεύει ή καταστρέφει στοιχεία, που έχουν αποθηκευθεί σε υπολογιστές. Οι συνέπειές τους μπορεί να αφορούν τη σοβαρή καταστροφή των συνηθισμένων δραστηριοτήτων μιας οποιασδήποτε επιχείρησης και τις συνεπακόλουθες οικονομικές της απώλειες.

Ένας τρόπος καταστροφής των δεδομένων ενός υπολογιστή είναι με τη χρήση της λεγόμενης «λογικής βόμβας». Αυτό είναι ένα πρόγραμμα με επιβλαβή κωδικό, το οποίο μένει ανενεργό, μέχρις ότου συμβεί κάποιο γεγονός, οπότε και ενεργοποιείται. Εάν η ενεργοποίηση του προγράμματος συνδέεται με κάποια ημερομηνία ή ώρα, όπως συνήθως συμβαίνει, το πρόγραμμα αυτό ονομάζεται επίσης «ωρολογιακή βόμβα».

Έχουν παρατηρηθεί πολλές περιπτώσεις δυσαρεστημένων μάλιστα υπαλλήλων, οι οποίοι εγκατέστησαν λογικές βόμβες στα συστήματα των εταιρειών τους μόλις τους γνωστοποιήθηκε η απόλυσή τους. Ο επιβλαβής κώδικας προγραμματίζεται να ενεργοποιηθεί μετά από ορισμένες ημέρες , μόνο εφόσον ο υπάλληλος δεν έχει επαναπροσληφθεί

Οι ενέργειες αυτές εκθέτουν την ακεραιότητα αυτών των επιχειρήσεων, που αποτελούν πηγή πληροφοριών, ενώ παράλληλα τις καθιστούν μη προσιτές στους χρήστες τους. Σε ορισμένες περιπτώσεις, οι πηγές αυτές υφίστανται ολοκληρωτική καταστροφή. Η ανάκαμψή τους είναι δυνατή μόνο με την επαναλειτουργία τους. Ακόμα και όταν οι πηγές μπορούν να σωθούν, μια πράξη δολιοφθοράς μπορεί να βλάψει τη δημόσια εικόνα της εταιρείας, με πιθανό αποτέλεσμα την απώλεια πελατών και πωλήσεων. Επίσης, τέτοιες επεμβάσεις σε δεδομένα μπορεί να έχουν επιπτώσεις που θα μπορούσαν να αποβούν μοιραίες, στην περίπτωση που το συγκεκριμένο σύστημα υποστηρίζει θέματα που έχουν να κάνουν με τη ζωή, όπως αυτά που αφορούν την υγειονομική περίθαλψη των ατόμων.

Παρακολούθηση των δικτύων υπολογιστών

Η παρακολούθηση των δικτύων των υπολογιστών, χρησιμοποιείται και όταν πρόκειται να γίνει μια επιθετική επιχείρηση εναντίον κάποιου δικτύου (κατά τη διάρκεια της οποίας, αυτοί που εισβάλλουν σε υπολογιστές παρακολουθούν παράνομα τις δικτυακές επικοινωνίες), αλλά και όταν λαμβάνονται αμυντικά μέτρα εναντίον τέτοιου είδους επιθέσεων (κατά τη διάρκεια των οποίων οι διαχειριστές συστημάτων εντοπίζουν τις δραστηριότητες των εξωτερικών εισβολέων και των εσωτερικών εχθρών τους, οι οποίοι προξενούν βλάβες στα δίκτυά τους).

Sniffers πακέτων: το μεγαλύτερο τμήμα της κυκλοφορίας δεδομένων σε δίκτυα υπολογιστών είναι δυνατό να καταστεί αντικείμενο παρακολούθησης μέσω των sniffers (αναρροφητών). Αυτά είναι προγράμματα που εγκαθίστανται σε ορισμένους υπολογιστές, που συνδέονται με το Δίκτυο. Το sniffer συλλαμβάνει μηνύματα, καθώς αυτά ταξιδεύουν μέσα στο δίκτυο, σώζοντας τα πιο ενδιαφέροντα από αυτά σε ένα ημερολογιακό αρχείο για μεταγενέστερη εξέταση. Επειδή τα μηνύματα διασχίζουν το δίκτυο σε ομάδες δεδομένων που ονομάζονται «πακέτα», τα sniffers αναφέρονται σαν «sniffers πακέτων». Ένα μήνυμα ηλεκτρονικού ταχυδρομείου ή μια ιστοσελίδα μπορούν να διαχωριστούν σε διάφορα πακέτα προτού αρχίσουν το ταξίδι τους στο δίκτυο. Στο σημείο λήψης τους, τα πακέτα επανασυγκολλώνται για να συγκροτήσουν και πάλι όλο το μήνυμα.

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

Τα sniffers πακέτων χρησιμοποιούνται από hackers για να μαζεύουν τα ονόματα και τους κωδικούς εισόδου διαφόρων χρηστών. Χρησιμοποιούνται επίσης από διαχειριστές συστημάτων για να κρατούν μακριά τους hackers και από ανακριτές για να εντοπίζουν την δραστηριότητά τους.

Αποδιοργάνωση: ορισμένες επιθέσεις έχουν σαν αποτέλεσμα την καταστροφή δεδομένων ή την αποτυχία επιχειρήσεων. Αυτές ονομάζονται επιθέσεις «άρνησης υπηρεσίας», επειδή οι νόμιμοι χρήστες δεν μπορούν εξαιτίας τους ούτε να εξυπηρετηθούν ούτε να έχουν πρόσβαση στις πηγές των πληροφοριών. Σε ορισμένες περιπτώσεις οι ζημιές που αναφέρθηκαν υπήρξαν τεράστιες

Οι πράξεις δολιοφθοράς είναι συχνά έργο απολυμένων υπαλλήλων, οι οποίοι επιτίθενται στους υπολογιστές των πρώην εργοδοτών τους, για να τους εκδικηθούν επειδή έχασαν τη δουλειά τους.

Επίσης και πολλοί hackers, παρότι οι περισσότεροι από αυτούς δεν προξενούν σοβαρές ζημιές στα συστήματα στα οποία εισβάλλουν, δεν ακολουθούν τον κανόνα αυτό.

Όπως και με τις εισβολές στις ιστοσελίδες, πιο γενικευμένες πράξεις σαμποτάζ μπορεί να γίνονται, για να διαμαρτυρηθεί κανείς ενάντια σε πολιτικές ή πρακτικές των οργανισμών που υφίστανται την επίθεση αυτή. Όταν η America Online δεν μπορούσε να ανταποκριθεί στις ανάγκες εξυπηρέτησης των πελατών της στις αρχές του 1997, hackers χρησιμοποίησαν το λόγο αυτό για να δικαιολογήσουν την εισβολή τους σε λογαριασμούς της. Ακριβώς πριν από την ημέρα του Αγίου Βαλεντίνου, ένα μήνυμα κυκλοφόρησε στην America Online, το οποίο ανήγγειλε πως εκείνη τη μέρα θα γινόταν μια «εξέγερση των hackers». Οι hackers επρόκειτο να συγκεντρωθούν στις 06:00 μ.μ. σε ιδιωτικούς χώρους συζητήσεων, για να σχεδιάσουν την πορεία τους, η οποία θα άρχιζε στις 09:00 μ.μ. Σύμφωνα με την αναγγελία, οι hackers θα πετούσαν χρήστες έξω από χώρους συζητήσεων, θα ακύρωναν λογαριασμούς και θα μετέδιδαν ιούς των υπολογιστών. Τη συγκεκριμένη ώρα πάνω από 300 hackers εμφανίστηκαν και μοίρασαν προγράμματα για να «κάνουν κόλαση την AOL». Χρησιμοποιώντας πρόχειρα ονόματα, οι εξεγερθέντες έστελναν μηνύματα που έτρεχαν πολύ γρήγορα στην οθόνη με τρόπο που καθιστούσε δύσκολη την ανάγνωσή τους («κυλιόμενα») ενώ χρησιμοποιούσαν μακροεντολές για την αναγραφή κειμένων όπως «ΕΞΕΓΕΡΣΗ!!!ΕΞΕΓΕΡΣΗ!!!ΕΞΕΓΕΡΣΗ!!!».

Μεταμφιέσεις

Την ασφάλεια των δικτύων των υπολογιστών απειλούν συχνά απατεώνες ή άτομα, που κρύβονται πίσω από κάποιο άλλο πρόσωπο. Οι κλέφτες της ταυτότητας κάποιου, εισπράττουν χρήματα, συνάπτουν δάνεια και χρεώνουν τα αγαθά που αγοράζουν στο όνομα κάποιου άλλου. Οι πλαστογράφοι φτιάχνουν έγγραφα, μηνύματα ηλεκτρονικού ταχυδρομείου και παραχαράζουν νομίσματα, που φαίνονται να προέρχονται από άλλα μέρη. Οι hackers κρύβουν επιβλαβείς κώδικες σε προγράμματα Δούρειων Ίππων, παρουσίαση των οποίων θα γίνει στη συνέχεια, που από έξω φαίνονται αθώα ή ελκυστικά. Οι δυνάμεις επιβολής του νόμου παράλληλα οργανώνουν μυστικές επιχειρήσεις και στήνουν παγίδες, για να πιάνουν τους απατεώνες.

Η κλοπή της ταυτότητας: ως κλοπή της ταυτότητας νοείται η διαστρέβλωση των στοιχείων της ταυτότητας ενός προσώπου όπως του ονόματός του, του αριθμού της κοινωνικής του ασφάλισης, της άδειας οδήγησης, των αριθμών των πιστωτικών του καρτών και των αριθμών των τραπεζικών του λογαριασμών. Ο σκοπός που επιδιώκεται μ' αυτή είναι η δυνατότητα τέλεσης πράξεων, που επιτρέπονται στον κάτοχο της συγκεκριμένης ταυτότητας, όπως η ανάληψη μετρητών, η μεταφορά χρημάτων, η χρέωση αγορών, η απόκτηση πρόσβασης σε πληροφορίες ή η αποστολή εγγράφων και επιστολών με το όνομα του θύματος. Οι πληροφοριακές πηγές, που προσβάλλονται στην περίπτωση αυτή, είναι τα έγγραφα και οι πληροφορίες που προσδιορίζουν το συγκεκριμένο πρόσωπο. Σ' αυτά περιλαμβάνονται τα έγγραφα από χαρτί, οι ταυτότητες, τα τραπεζικά βιβλιάρια, τα ηλεκτρονικά αρχεία καθώς και οι πληροφορίες που περιλαμβάνονται σε όλα αυτά. Ο κλέφτης αποκτά με τον τρόπο αυτό πρόσβαση στις πηγές και τις χρησιμοποιεί πλέον για λογαριασμό του. Η ακεραιότητα των πληροφοριών που αφορούν το θύμα, όπως αυτές που μιλούν για την οικονομική του κατάσταση, υποβαθμίζεται επίσης. Το θύμα και εκείνοι που του έχουν προμηθεύσει τα σχετικά στοιχεία, καθώς και οι διάφορες άλλες πηγές υφίστανται τις τυχόν απώλειες. Πολλές επιχειρήσεις του είδους αυτού, ιδιαίτερα εκείνες που αφορούν την απάτη με πιστωτικές κάρτες, αποτελούν περιπτώσεις πολύ σοβαρής απάτης, δεδομένης της δυνατότητας που αποκτά εξαιτίας τους ο κλέφτης στο να χρησιμοποιήσει τους τραπεζικούς λογαριασμούς του θύματός του.

Η κλοπή της ταυτότητας αφορά συνήθως την απάτη με πιστωτικές κάρτες. Οι κλέφτες κατασκευάζουν πλαστές κάρτες ή χρησιμοποιούν κλεμμένες κάρτες ή αριθμούς καρτών, για να προμηθευθούν αγαθά και υπηρεσίες. Παρότι στις περισσότερες περιπτώσεις τα θύματα κλοπής ταυτότητας είναι άτομα, δεν είναι λίγες οι περιπτώσεις που ο κατάλογός τους συμπληρώνεται

και με επιχειρήσεις. Στις 24 Ιουλίου του 1997 ο Salah Areh Sougah οδηγήθηκε σε Αμερικανικό δικαστήριο με κατηγορίες για ξέπλυμα βρώμικου χρήματος, για τραπεζική απάτη και για χρήση αριθμού κοινωνικής ασφάλισης σε μια προσπάθειά του να εξαπατήσει μια εταιρεία και να εισπράξει από αυτή περισσότερα από $641.000. Ο 29χρονος Καλιφορνέζος εξέδωσε 66 ακάλυπτες επιταγές στο όνομα αυτής της εταιρείας και τις κατέθεσε σε ένα τραπεζικό λογαριασμό που είχε δημιουργήσει από πριν, με μοναδικό σκοπό την είσπραξη ακάλυπτων επιταγών. Τα ποσά που εισέπραξε τα χρησιμοποίησε για να αγοράσει αυτοκίνητο, για να πληρώσει την υποθήκη του σπιτιού του και για να εξοφλήσει άλλα χρέη του.

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

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

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

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

Άλλοι τρόποι επίθεσης που απειλούν την ασφάλεια των υπολογιστικών δικτύων

Εκτός από τους τρόπους επίθεσης κατά της ασφάλειας των δικτύων των υπολογιστών που αναφέραμε παραπάνω, υπάρχουν και άλλοι όπως: τα κυβερνομικρόβια, οι δούρειοι ίπποι και τα Cookies (ο ρόλος των οποίων, όπως θα αναλύσουμε στη συνέχεια είναι αμφιλεγόμενος).

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

Στην κατηγορία αυτή, περιλαμβάνονται οι ιοί και τα σκουλήκια. Και τα δύο αυτά είδη μολύνουν τους υπολογιστές, και τα δύο μπορούν να απλωθούν και σε δίκτυα. Η κύρια διαφορά

τους συνίσταται στο ότι ένα σκουλήκι είναι ένας αυτόνομος πράκτορας, ο οποίος εξαπλώνεται από μόνος του, ενώ ο ιός κολλάει σε άλλα προγράμματα και εξαπλώνεται μαζί με αυτά, συνήθως σε μια απάντηση σε πράξεις που έκαναν οι χρήστες. Επίσης, ενώ ένα σκουλήκι εξαπλώνεται μόνο σε δίκτυα υπολογιστών, ένας ιός μπορεί να εξαπλωθεί και με δισκέτες. Η διάκριση ανάμεσα σε ιούς και σκουλήκια, ωστόσο, μπερδεύει τα πράγματα και ίσως είναι ατυχής, καθώς η συμπεριφορά ορισμένων μικροβίων μοιάζει και με τα δύο αυτά είδη, καθώς και τα δύο είδη μολύνουν υπολογιστές.

Σαν όργανα τα οποία απειλούν την ασφάλεια των υπολογιστικών δικτύων, τα κυβερνομικρόβια καταστρέφουν την ακεραιότητα των δικτύων. Οδηγούν επίσης σε άρνηση παροχής υπηρεσιών. Ακόμα, όμως, και αν δεν καταστρέφουν σκοπίμως δεδομένα ή δεν απενεργοποιούν συστήματα, οι μολυσμένοι από αυτά υπολογιστές θα πρέπει να τεθούν εκτός λειτουργίας και επομένως να μη γίνονται αυτά που πρέπει να κάνουν ενόσω χρόνο θα γίνεται προσπάθεια για την απομάκρυνσή τους από το σύστημα. Συγκεκριμένα:

➢ Ιοί υπολογιστών: τον περασμένο Νοέμβριο συμπληρώθηκαν είκοσι χρόνια από τότε που δημιουργήθηκε ο πρώτος ιός για υπολογιστές και κατά συνέπεια από τότε που κάθε χρήστης έπαψε να αισθάνεται ασφαλής. Μπορεί εκείνος ο πρώτος ιός να μη ζει πια για να γιορτάσει τα γενέθλιά του, αλλά το καταστροφικό έργο που ανέλαβαν έκτοτε πάνω από 60000 απόγονοί του, φροντίζοντας να μας ταλαιπωρεί μια ίωση την οποία πολεμάμε καθημερινά με κάθε είδους αντιβιοτικά. Ας γυρίσουμε όμως λίγο πίσω στο χρόνο για να δούμε πώς ξεκίνησαν όλα. Εν αρχή, ήταν ένας Αμερικανός φοιτητής ονόματι Φρεντ Κοέν, ο οποίος μελετούσε την ασφάλεια των υπολογιστών για να ολοκληρώσει τη διατριβή του. Κάνοντας ένα βήμα παραπάνω από το να παρουσιάσει μια θεωρητική εργασία, δημιούργησε ένα ζωντανό παράδειγμα του πώς ένα μικρό πρόγραμμα θα μπορούσε να προσλάβει άλλα προγράμματα τροποποιώντας τα. Η παρουσίαση αυτής της εργασίας στις 10 Νοεμβρίου του 1983 κίνησε το ενδιαφέρον αρκετών, οι οποίοι πραγματοποίησαν τα δικά τους πειράματα. Η διακίνηση αυτών των προγραμμάτων γινόταν μέσω δισκετών που πήγαιναν από χρήστη σε χρήστη. Καθώς η τεχνολογία εξελισσόταν μεταλλάσσονταν και οι ιοί, οι οποίοι άρχισαν να εκμεταλλεύονται τις αδυναμίες των Windows, για να μεταδίδονται πιο γρήγορα και σε περισσότερους ανθρώπους. Έκτοτε, οι ιοί κάνουν το γύρω του κόσμου σε μερικές μόνο ώρες παίρνοντας κάθε φορά νέα μορφή για να αποφύγουν τον εντοπισμό τους από τα προγράμματα anti-virus. Δε μπορεί να πει κανείς με σιγουριά τι μας επιφυλάσσει το μέλλον, αλά οι ιοί έχουν γίνει μια μόνιμη απειλή και το ηθικό δίδαγμα είναι ότι πρέπει να χρησιμοποιούμε μια ασπίδα προστασίας. Αυτά όσον αφορά την ιστορία τους. Θεωρητικά αναφέρονται τα εξής:

Ένας ιός είναι ένα τμήμα κώδικα, το οποίο κολλά τον εαυτό του σε άλλες εντολές του υπολογιστή. Σε οποιαδήποτε περίπτωση ο χρήστης (ή το σύστημα) δίνει μια εντολή στον υπολογιστή (για παράδειγμα, να ξεκινήσει τη λειτουργία του ή μια εφαρμογή ΄η να ανοίξει ένα προσαρτημένο σ' ένα μήνυμα ηλεκτρονικού ταχυδρομείου), ο ιός ενεργοποιείται παράλληλα και αυτός. Ο κώδικας του ιού προστίθεται στον κώδικα του υπολογιστή με τέτοιο τρόπο, έτσι, ώστε όταν αυτός ο τελευταίος φορτώνεται στη μνήμη για να εκτελεστεί, ο ιός είναι εκείνος που ενεργοποιείται πρώτος. Ο ιός ενεργοποιείται αρχικά από μόνος του και στη συνέχεια αποκτά τον έλεγχο του υπολογιστή, που τον φιλοξενεί. Ενώ ενεργοποιείται, ο ιός μπορεί να τοποθετήσει ένα αντίγραφο του εαυτού του στη μνήμη του υπολογιστή, όπου αυτό παραμένει «εγκατεστημένο», μέχρις ότου να κλείσει ο υπολογιστής. Το εγκατεστημένο αυτό αντίγραφο ψάχνει για μη μολυσμένους υπολογιστές. Όταν βρει κάποιον, του μεταβιβάζει ένα αντίγραφο του εαυτού του. Στη συνέχεια, ο ιός εκτελεί ένα «ωφέλιμο φορτίο», το οποίο μπορεί να κάνει οτιδήποτε: από το να δείξει ένα ψυχαγωγικό ή πολιτικό μήνυμα, μέχρι να σβήσει αρχεία από το σκληρό δίσκο.

Εάν ένας ιός δεν εγκαταστήσει τον εαυτό του, τότε θα πρέπει να μολύνει έναν άλλο υπολογιστή και να του αφήσει το φορτίο του, προτού αποκτήσει τον έλεγχό του. Οι ιοί διαδίδονται από το ένα μηχάνημα στο άλλο μέσω δισκετών και δικτύων υπολογιστών.

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

Ποιος φτιάχνει ιούς;

Οι περισσότεροι ιοί φαίνεται πως έχουν φτιαχτεί από hackers. Με δεδομένο το γεγονός ότι οι hackers αυτό που κάνουν το κάνουν για να διασκεδάσουν, πολλοί από αυτούς έχουν σαν κίνητρό τους περισσότερο την πρόκληση και την περιπέτεια παρά την πρόθεση να προκαλέσουν καταστροφές. Η θέση αυτή ενισχύεται και από το ότι σχετικά μικρό ποσοστό ιών διαθέτει φορτίο. Ο Spanska, ένας 29χρονος δημιουργός ιών, που συνδεόταν με την ομάδα Virus Xchange, της οποίας τα μέλη είχαν αυτή την απασχόληση, είπε πως τον διασκέδαζε η «διανοητική προσπάθεια, η εμπειρία της μυστικότητας και η πρόκληση της δημιουργίας ενός προγράμματος» στα προγράμματα των ιών. Παραδέχτηκε επίσης πως διασκέδαζε φτιάχνοντας κάτι που ήταν κατά κάποιο τρόπο «ανατρεπτικό». «Το να δημιουργείς ιούς σε κάνει να

ανατριχιάζεις επειδή βρίσκεσαι στην σκοτεινή πλευρά, κάνοντας πράγματα που απαγορεύονται, τρομοκρατώντας το μέσο χρήστη», είπε.

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

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 εξαπλώθηκαν μα ταχύτατο ρυθμό. Η μέθοδος επίθεσης είναι πολύ ύπουλη, αφού μόλις καταφέρουν να διεισδύσουν σε έναν υπολογιστή στέλνουν μολυσμένα και καλυμμένα/ παραλλαγμένα μηνύματα ηλεκτρονικού ταχυδρομείου σε όλη τη λίστα επαφών του Outlook. Έτσι, ο ανυποψίαστος χρήστης λαμβάνει μήνυμα ηλεκτρονικού ταχυδρομείου από κάποιο γνωστό του και δείχνοντας εμπιστοσύνη ανοίγει το επισυναπτόμενο αρχείο με «οδυνηρές» συνέπειες για τον υπολογιστή του. Η μαζική αποστολή μηνυμάτων ηλεκτρονικού ταχυδρομείου, εκτός από την κατασπατάληση του εύρους ζώνης, ιδίως των συνδέσεων με modem ανεξαρτήτων χρηστών, επιβαρύνει δραματικά τους κεντρικούς εξυπηρέτες αλληλογραφίας του Διαδικτύου, με αποτέλεσμα να τίθενται συχνά εκτός λειτουργίας.

Δούρειοι ίπποι: δε θα ήταν υπερβολή εάν λέγαμε ότι ο μεγαλύτερος κίνδυνος μετά τους ιούς, για την πλειονότητα των χρηστών του Διαδικτύου, προέρχεται από τους «Δούρειους Ίππους» (Trojan horses). Πρόκειται για προγράμματα που χρησιμοποιούνται για την απόκτηση πρόσβασης σε μία πληροφοριακή πηγή. Τα προγράμματα αυτά ονομάσθηκαν έτσι γιατί λειτουργούν όπως το μυθικό άλογο του Τρωικού Πολέμου. Δηλαδή, ενώ επικαλούνται ότι επιτελούν κάποια εργασία, στην πραγματικότητα εκτελούν και/ή μια διαφορετική λειτουργία. Αυτή η λανθάνουσα δραστηριότητα είναι που συνήθως εκτελεί καλυμμένες ενέργειες, όπως η κλοπή των συνθηματικών των χρηστών.

Υπάρχουν Δούρειοι Ίπποι που η εργασία που υποτίθεται ότι προσφέρουν δεν υπάρχει καν. Έτσι, όταν εκτελούνται απλά προχωρούν στην απροκάλυπτη καταστροφή αρχείων και

πόρων του συστήματος. Από την άλλη, υπάρχουν Δούρειοι Ίπποι που λειτουργούν με συγκαλυμμένο τρόπο, έτσι ώστε να επιτελούν την εργασία που επικαλούνται χωρίς να προκαλούν υποψίες. Σε κάποιες ανώδυνες περιπτώσεις μπορεί απλώς να παίζει με τα νεύρα του ανυποψίαστου χρήστη, πχ 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, πχ να χτυπήσει τις κεφαλές του σκληρού του δίσκου. Μια άλλη ύπουλη λειτουργία των Δούρειων Ίππων είναι η παρακολούθηση και καταγραφή των κινήσεων του χρήστη. Έτσι, όταν εκείνος πληκτρολογεί κωδικούς πρόσβασης ή αριθμούς πιστωτικών καρτών, το πρόγραμμα το καταγράφει για να τα στείλει αργότερα στο θύτη/ εισβολέα.

Πώς όμως μπορεί να «εισαχθεί» ένας Δούρειος Ίππος στον υπολογιστή μας; Ο συνηθέστερος τρόπος είναι να έρχεται ως επισυναπτόμενο σε κάποιο μήνυμα ηλεκτρονικού ταχυδρομείου ή να βρίσκεται κρυμμένο μέσα σε κάποιο άλλο πρόγραμμα, πχ σε ένα παιχνίδι με ευρεία διάδοση, σε κάποιο διάσημο, χρήσιμο εργαλείο κλπ.

Η καλύτερη μέθοδος πρόληψης κατά των Δούρειων Ίππων είναι η ενημέρωση των χρηστών. Σε κάθε περίπτωση, όμως, είναι δύσκολη αλλά όχι αδύνατη η ανίχνευση των Δούρειων Ίππων πριν να εισχωρήσουν σε ένα υπολογιστικό σύστημα. Γι' αυτό επιβάλλεται η καθιέρωση και η συνεπής εφαρμογή από τους διάφορους οργανισμούς συγκεκριμένων πολιτικών εγκατάστασης επίσημα αγορασμένου λογισμικού, καθώς και εκπαίδευσης των χρηστών, έτσι ώστε να αποκτήσουν τα απαραίτητα κίνητρα για να συμμερίζονται τους κινδύνους που αναλαμβάνουν όταν δοκιμάζουν προγράμματα άγνωστης προέλευσης.

COOKIES: Το Internet (WWW) είναι χτισμένο σε μία πολύ απλή, αλλά πανίσχυρη προϋπόθεση. Όλα τα υλικά στο Διαδίκτυο είναι σχεδιασμένα βάσει ενός γενικού, ομοιόμορφου σχήματος που ονομάζεται HTML (HyperText Markup Language) , και όλες οι πληροφοριακές αιτήσεις και απαντήσεις εξομοιώνονται σε ένα παρόμοιο υπόδειγμα πρωτοκόλλου. Όταν κάποιος αποκτά πρόσβαση σε έναν server στο Διαδίκτυο, όπως για παράδειγμα η Βιβλιοθήκη του Κογκρέσου, η Web browser (παρουσιαστής Ιστοσελίδων) του χρήστη θα αποστείλει μια αίτηση πληροφοριών στον υπολογιστή της Βιβλιοθήκης του Κογκρέσου. Αυτός ο υπολογιστής ονομάζεται "Web Server". Ο Web Server θα απαντήσει στην αίτηση εκπέμποντας τις επιθυμητές πληροφορίες στον υπολογιστή του χρήστη. Εκεί, η Web browser του χρήστη θα εκθέσει την ληφθείσα πληροφορία στην οθόνη του χρήστη.

Τα COOKIES είναι κομμάτια πληροφοριών που έχουν παραχθεί και αποθηκευθεί από έναν Web Server στον υπολογιστή του χρήστη, και είναι σε αναμονή για κάθε μελλοντική

χρήση. Τα COOKIES είναι χαραγμένα στην HTML μνήμη πληροφοριών και κινούνται συνέχεια από τον υπολογιστή του χρήστη προς τους servers και το αντίστροφο. Τα COOKIES παρασκευάστηκαν για να επιτρέπουν την -από πλευράς του χρήστη- επιτήρηση των πληροφοριών που προέρχονται από το Διαδίκτυο.

Βασικά, τα COOKIES κάνουν χρήση συγκεκριμένων πληροφοριών που εκπέμπονται από τον Web Server στον υπολογιστή του χρήστη έτσι ώστε η πληροφορία να είναι διαθέσιμη για κάποια μελλοντική πρόσβαση του ίδιου ή άλλων Servers. Στις περισσότερες περιπτώσεις δεν μένει απαρατήρητη μόνο η αποθήκευση προσωπικών πληροφοριών σε cookies, αλλά και η ανά πάσα στιγμή πρόσβαση σε αυτά. Οι Web Servers αυτόματα αποκτούν πρόσβαση σε σχετικά COOKIES οποτεδήποτε ο χρήστης εγκαθιδρύει μια σύνδεση με αυτά, συνήθως με τη μορφή Web αιτήσεων.

Τα COOKIES βασίζονται σε μια διαδικασία δύο σταδίων. Πρώτα, το Cookie αποθηκεύεται στον υπολογιστή του χρήστη χωρίς τη συγκατάθεση ή τη γνώση του. Για παράδειγμα, με πελατειακές μηχανές εξερεύνησης (όπως το Yahoo!) ένας χρήστης επιλέγει κατηγορίες ενδιαφέροντος από την Ιστοσελίδα.. Ο Web Server δημιουργεί τότε ένα συγκεκριμένο νέο COOKIE, που βασικά είναι μια κωδικοποιημένη σειρά κειμένου που περιέχει τις προτιμήσεις του χρήστη, και μεταβιβάζει αυτό το COOKIE στον υπολογιστή του χρήστη . Η Web browser του χρήστη, εάν "πιάσει" το COOKIE, το εισπράττει και το αποθηκεύει σε ένα συγκεκριμένο αρχείο που ονομάζεται "Λίστα COOKIES". Αυτό συμβαίνει χωρίς καμία γνωστοποίηση ή συγκατάβαση του χρήστη. Σαν αποτέλεσμα αυτού, οι προσωπικές πληροφορίες (σε αυτή την περίπτωση οι κατηγοριοποιημένες προτιμήσεις του χρήστη) σχηματοποιούνται και εκπέμπονται από τον Web Server, ενώ φυλάσσονται από τον υπολογιστή του χρήστη.

Κατά τη διάρκεια του δεύτερου σταδίου, το COOKIE μεταφέρεται μυστικά και αυτόματα από το μηχάνημα του χρήστη σε κάποιον Web Server. Οποτεδήποτε ένας χρήστης κατευθύνει την Web browser του για να εκθέσει μια ορισμένη Ιστοσελίδα από τον Server , η browser, χωρίς την γνώση του χρήστη, θα εκπέμψει το COOKIE που θα περιέχει προσωπικές πληροφορίες στον Web Server.

Η νέα τεχνολογία, ή η ήδη υπάρχουσα, δέχεται επίθεση.

Το πρωτόκολλο των COOKIES σχεδιάστηκε αρχικά για καταναλωτική άνεση και όχι για να είναι κακό. Το COOKIE είναι απλά ένα ακόμα εργαλείο στο Διαδίκτυο, αλλά είναι ο τρόπος

με τον οποίο μερικά sites παρέχουν αυτό το εργαλείο το οποίο μπορεί να προκαλέσει προβλήματα, κυρίως προβλήματα μυστικότητας.

Αλλά, ένας συνασπισμός υποστηρικτών μυστικότητας αρχίζει να αλλάζει αυτό το πρωτόκολλο. Μια νέα πρόταση προτείνεται στην IETF (Internet Engineering Task Force), όπως επίσης και στις κεφαλές της Microsoft και της Netscape. Εάν τεθεί σε ισχύ, θα μπορούσε να περιορίσει την διάρκεια των Cookies και να δώσει στον χρήστη μια ευρύτερη δυνατότητα επιλογών. Εάν η νέα προδιαγραφή δοθεί σαν στάνταρ, θα ενσωματωθεί σε όλες τις κύριες σελίδες εγκαίρως. Αυτό μπορεί να δώσει στον κόσμο ευρύτερες επιλογές στην δεδομένη browser τους, παρά να πρέπει να αγοράσουν επιπλέον προγράμματα.

Η IETF είναι ένας μη κερδοσκοπικός οργανισμός με χιλιάδες μέλη, και τελευταία ασκεί μεγάλη επιρροή σε αποφάσεις που καθορίζουν το μέλλον στο Διαδίκτυο. Συνεστάθη τον Οκτώβριο του 1996.

Ένα άλλο κομμάτι της πρότασης, θα ζητά browsers τουλάχιστον για να προειδοποιούν προτού αποδεχθούν τα Cookies από προεπιλογή, έτσι ώστε τα Cookies να είναι λιγότερο φανερά στους νέους χρήστες, και οι χρήστες μη γνώστες των Cookies. «Θέλουμε οι προεπιλογές να είναι ρυθμισμένες κατά τέτοιο τρόπο ώστε κανείς να μη μπορεί να στέλνει ένα Cookie χωρίς να το γνωρίζει ο παραλήπτης», είπε ο Marc Rotenberg, διευθυντής της EPIC που είναι ένας από τους οργανισμούς που υποστηρίζουν τη νέα πρόταση.

Το πιο αμφιλεγόμενο θέμα της πρότασης είναι η ικανότητα να περιοριστούν ή να εκλείψουν εντελώς οι αιτήσεις Cookies από τρίτους Servers. Αυτό είναι το ένα χαρακτηριστικό που επιπροσθέτως δεν μπορούν να σταματήσουν τα προγράμματα των πελατών. Αυτό θα μπορούσε να θέσει σε κίνδυνο το μέλλον των στοχευόμενων ποιοτικών εταιρειών. Πολλά sites τώρα χρησιμοποιούν αυτές τις εταιρείες ή χρησιμοποιούν σύμβολα από τρίτους servers για τη διαφήμισή τους. Σε ένα site το οποίο αποκτά τις διαφημίσεις του από έναν τρίτο server, θα υπήρχε μια αίτηση στην σελίδα του άλλου server. Επειδή το Cookie μπορεί να τοποθετηθεί σε οποιοδήποτε αντικείμενο, όταν το site ζητά το σύμβολο από το άλλο site, τότε θα διαβάσει ή θα θέσει σε λειτουργία ένα Cookie.

Η αίτηση για το σύμβολο θέτει τότε σε λειτουργία ένα Cookie, και μετά επιστρέφει μια διαφημιστική εικόνα. Το Cookie με την αίτηση εικόνας μπορεί τότε να καταγράψει τι διαφημίσεις έχουν προβληθεί στο χρήστη και σε ποια σύμβολα έχουν δείξει προτίμηση κλικάροντάς τα. Εάν ο πελάτης πήγε σε ένα άλλο site το οποίο απέκτησε τις διαφημίσεις του από τον ίδιο server, όταν αυτή η σελίδα ζήτησε το σύμβολο από τον τρίτο server θα διάβαζε το ίδιο Cookie μετά θα ήταν ικανό να προβάλλει τις διαφημίσεις οι οποίες έχουν γίνει κατά παραγγελία από τα δεδομένα στο Cookie, έτσι ώστε να μην ξαναδεί τις ίδιες διαφημίσεις πάλι

(εκτός και αν η εταιρεία πλήρωσε για να ξαναπαιχτεί πάλι), μία άλλη μεταβλητή θα ρυθμιζόταν στο Cookie καθορίζοντας ότι έχουν επισκεφθεί αυτό το site, όλες αυτές οι πληροφορίες μπορούν συγκεντρωμένες να χρησιμοποιηθούν για να χτιστεί ένα λεπτομερές προφίλ των προτιμήσεων, μη προτιμήσεων και που πάνε του χρήστη, έτσι ώστε να στοχεύουν με τη διαφήμιση ακόμη ακριβέστερα τον χρήστη. Με την πάροδο μιας μακράς χρονικής περιόδου αυτό θα μπορούσε να γίνει πολύ ακριβές. Για μερικούς ανθρώπους, το να έχουν διαφημίσεις οι οποίες είναι του ενδιαφέροντός τους, δεν είναι τόσο κακό. Θα ήταν προτιμότερο να κατεβάσει κάποιος ένα banner που μπορεί να τον ενδιαφέρει, παρά μια διαφήμιση που δεν έχει απολύτως καμμία σχέση με τον ίδιο.

Το να σκεφθεί κάποιος ότι όλες αυτές οι πληροφορίες σχετικά με αυτόν συγκεντρώνονται σε ένα κεντρικό μέρος, μπορεί να είναι μια τρομακτική σκέψη. Παρ' όλο που αυτές οι ποιοτικές σημαδεμένες εταιρείες δεν μπορούν να χρησιμοποιήσουν ένα Cookie για να αποκτήσουν προσωπικές πληροφορίες από τον υπολογιστή μας όπως το όνομά μας ή τη διεύθυνση e-mail, θα μπορούσαν παρ' όλ' αυτά να προσθέσουν πληροφορίες που αποκαλύψαμε σε ανόμοια sites. Για παράδειγμα, εάν μπήκαμε σε ένα site με χαλαρά στάνταρ και αποφασίσαμε να υποβάλλουμε το όνομά μας και το e-mail μας, αυτές οι πληροφορίες μπορεί να περαστούν και να ταιριαχτούν με μια βάση δεδομένων των προτιμήσεών μας, μη προτιμήσεών μας και των διαφημιστικών μας στατιστικών. Μερικοί ισχυρίζονται πως αυτό δεν αποτελεί εισβολή στην ιδιωτική ζωή κάποιου, παρ' όλ' αυτά η εξάπλωση και η αυτοματοποιημένη φύση αυτής της τεχνολογίας επιτρέπει τη συλλογή δεδομένων χωρίς να το γνωρίζει κάποιος, και αυτό ασφαλώς διαλύει την αντίληψη περί ανωνυμίας στο Διαδίκτυο.

Μερικοί μπορεί να πιστεύουν ότι αυτό αποτελεί εισβολή στην προσωπική τους ζωή, και άλλοι να μην το πιστεύουν, αλλά αυτή πρόταση ελπίζεται πως σαν αποτέλεσμα θα δώσει στον κόσμο μια επιλογή.

Παραδείγματα τέτοιου είδους εταιρειών (targeted marketing companies) είναι : η Doubleclick, Focalink, Globaltrack, ADSmart. Όλες αυτές οι εταιρείες χρησιμοποιούν Cookies για να σημαδεύουν με τις διαφημίσεις τους εμάς, στα επιτρεπόμενα sites τους. Εάν η πρόταση περάσει, και το πρωτόκολλο των Cookies βελτιωθεί για να αποτρέψει τα Cookies από τρίτους servers, το μέλλον αυτών των εταιρειών φαίνεται πραγματικά πολύ σκοτεινό. Μέχρι τώρα, τα Cookies που χρησιμοποιούνται σε αυτές τις εταιρείες εγκαθίστανται αυτόματα και μπορούν να ακολουθήσουν μόνο συγκεκριμένο αριθμό μεταβλητών. Οι χρήστες εμφανίζονται ανώνυμα σε αυτές τις εταιρείες εκτός και αν εθελοντικά παραδώσουν προσωπικές τους πληροφορίες.

Αποτελεί ελπίδα το γεγονός πως αυτή η πρόταση θα φέρει σαν αποτέλεσμα το να μας δώσει περισσότερες επιλογές και έλεγχο επάνω στην ιδιωτική μας ζωή. Επειδή αυτές οι τεχνολογίες μας επηρεάζουν θα πρέπει και εμείς να έχουμε την επιλογή ελέγχου τους.

Το Persistent Cookie πρωτόκολλο εξελίχθηκε αρχικά από την Netscape για να διατηρήσει την τάξη στο άτακτο περιβάλλον του HTTP. Απεδείχθη πως έχει πολλές χρήσεις, καλές και κακές, και πολύ μακριά από την αρχική του πρόθεση. Το θέμα των Cookies και άλλων εισβολέων τεχνολογιών έχουν θίξει το πολύ αμφιλεγόμενο ζήτημα της ιδιωτικής ζωής, την οποία προσωρινά έχουμε χάσει στο Διαδίκτυο. Από τότε που παρουσιάστηκαν για πρώτη φορά μερικά χρόνια πριν, το πρωτόκολλο έχει αλλάξει και πιο πριν, και στο παρελθόν οποιοδήποτε site μπορούσε να δει όλα τα Cookies στο δοχείο, αλλά αυτό συνδυάστηκε με πιο σοβαρά και άλλα προβλήματα στο Java. Η νέα πρόταση θα πάρει πολύ καιρό για να παρέχει διευκολύνσεις, πολλές δύσκολες αποφάσεις θα πρέπει να τακτοποιηθούν προτού το τελικό αποτέλεσμα συσταθεί.

Ποιες είναι οι πιθανότητες να κολλήσεις ιό από ένα Cookie

Ένα συνηθισμένο Cookie βασισμένο σε κείμενο, δεν αποτελεί κίνδυνο για τους υπολογιστές μας και δεν εξαπλώνει ιούς. Ασχέτως με το αν άλλα Cookies μπορεί να είναι επικίνδυνα και να εξαπλώνουν ιούς έχει να κάνει με το εάν ένα αρχείο είναι ή δεν είναι "προς εκτέλεση", εννοώντας εάν είναι ένα πρόγραμμα παρά δεδομένα.

Τα περισσότερα Cookies δεν είναι προς εκτέλεση, και γενικά είναι πολύ σπάνια. Γενικά, τα Cookies αποθηκεύονται σαν φάκελοι κειμένου και δεν μπορούν να αποτελούν κίνδυνο ή να μεταδώσουν ιούς. Ακόμα και εάν ένα Cookie είναι εκτελέσιμο δεν μπορεί αυτομάτως να εξαπλώσει έναν ιό εκτός και αν το εκτελέσουμε. Αλλά φυσικά με τα πρόσφατα bugs στον Internet Explorer 3.0, θα αφήσει ένα site να πραγματοποιήσει την εγκατάσταση. Θεωρητικά, εάν ένα εκτελέσιμο Cookie ρυθμίστηκε με κακοπροαίρετο περιεχόμενο, τότε είναι πιθανό πως ο Internet Explorer 3.0 θα μπορούσε να το εκτελέσει, και τότε θα μπορούσε να επηρεάσει τον υπολογιστή μας με έναν ιό.

Το μεγαλύτερο περιεχόμενο ενός Cookie είναι 4kb και η γραμμή για να διαγράψουμε αυτά τα περιεχόμενα ενός σκληρού δίσκου είναι μόνο 18bytes, οπότε είναι φανερό πως ο ιός μπορεί να κάνει κάποια ζημιά ακόμα και εάν δεν μπορεί να είναι απολύτως ο "Δούρειος Ίππος". Να σημειωθεί πως αυτό είναι απλά μια θεωρία και πως δεν έχει ακόμη εμφανιστεί ένα Cookie το οποίο είναι ικανό να εξαπλώνει κάποιο ιό. Αυτό θα ήταν εικονικά αδύνατο και θα χρειαζόταν μεγάλη ποσότητα εργασίας. Αυτή η θεωρία είναι μηδαμινή συγκριτικά με κάποιες

άλλες πολύ αληθινές διεξόδους στο Διαδίκτυο. Μια διέξοδος στο Active παρουσιάσθηκε, και ήταν ικανή να έχει πρόσβαση στα βασικά αρχεία του συστήματος.

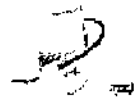
Βασικά τα Cookies δεν μπορούν να βλάψουν τον υπολογιστή μας. Η γενική αμφισβήτηση δεν είναι σχετικά με το τι μπορούν τα Cookies να κάνουν στον υπολογιστή μας, αλλά τι πληροφορίες μπορούν να αποθηκεύσουν, και τι μπορούν να μεταδώσουν στους servers. Τελευταία υπάρχει μια νέα πρόταση για περιορισμό των χαρακτηριστικών του πρωτοκόλλου των Cookies, η οποία θα μπορούσε να δώσει στον κόσμο ένα μεγαλύτερο έλεγχο σχετικά με το τι μπορούν να δεχθούν και από πού.

Οπότε εάν τα Cookies είναι τόσο ενοχλητικά, τότε γιατί αναπτύχθηκαν;

Η πρώτη φουρνιά Cookies μαγειρεύτηκε αρχικά σαν απλός μηχανισμός για να κάνει πιο εύκολη την πρόσβαση των χρηστών στα αγαπημένα τους sites χωρίς να χρειάζεται να υποστούν μία χρονοβόρα διαδικασία αυτοαναγνώρισης κάθε φορά που χρειάζεται να τα επισκεφθούν. Για παράδειγμα, στην πρώτη μας επίσκεψη σε ένα δοσμένο site, πιθανότατα θα μας ζητηθεί να αποκαλύψουμε το όνομά μας και ίσως και μερικές προσωπικές ή οικονομικές πληροφορίες απαραίτητες για να αποκτηθεί πρόσβαση σε αυτό το site στο μέλλον. Το site τότε, θα τοποθετήσει στο σύστημά μας ένα Cookie που περιέχει αυτές τις πληροφορίες και όταν επιστρέφουμε θα μας ζητά πληροφορίες βασισμένες στο Cookie για να καθορίσει ποιοι είμαστε και αν εάν έχουμε την αρμοδιότητα για να εισέλθουμε στο site.

Δυστυχώς, η αρχική πρόθεση των Cookies έχει υπονομευθεί από μερικές ασυνείδητες οντότητες οι οποίες έχουν βρει μάλιστα τρόπο να χρησιμοποιούν αυτή τη διαδικασία για να εντοπίζουν τις κινήσεις μας στο Διαδίκτυο. Αυτό το κάνουν φυτεύοντας ύπουλα τα Cookies τους και έπειτα βρίσκοντάς τα με τέτοιο τρόπο που τους επιτρέπει να χτίζουν λεπτομερή προφίλ σχετικά με τα ενδιαφέροντά μας, τις συνήθειες με τις οποίες περνάμε την ώρα μας και του τρόπου ζωής μας. Επιφανειακά, αυτή η πρακτική μπορεί να φαίνεται ακίνδυνη και καθόλου άξια ταραχής, αφού το χειρότερο πράγμα που μπορούμε να φανταστούμε είναι ότι οι ενσωματωμένες ανησυχίες θα χρησιμοποιήσουν αυτές τις πληροφορίες σε ενοχλητικές συσκευές, σε σχετικά ασήμαντες διαφημιστικές καμπάνιες, που στοχεύουν κατευθείαν σε συγκεκριμένες ομάδες ή άτομα. Παρ΄ όλ' αυτά, είναι μάλλον τρομακτικό το να σκεφθεί κανείς πώς μία τέτοια μυστική γνώση των προσωπικών μας προτιμήσεων και ιδιωτικών μας δραστηριοτήτων μπορεί τελικά να χρησιμοποιηθεί για να κατατάξει καθένα μας ως μέλη συγκεκριμένων ομάδων.

Γ΄ Μέρος



Αμυντικός Πληροφοριακός Πόλεμος

Μέτρα Προστασίας

Τα μέτρα προστασίας ή αντίμετρα είναι όλες εκείνες οι διαδικασίες, τεχνικές, ενέργειες και συσκευές που περιορίζουν τις ευπάθειες ενός πληροφοριακού συστήματος. Οι διαφορετικοί τύποι αντίμετρων έχουν σαν αποτέλεσμα την ανάλυση του προβλήματος της ασφάλειας των πληροφοριών στις ακόλουθες συνιστώσες:

o *Φυσική ασφάλεια συστήματος.* Αναφέρεται στην προστασία ολόκληρου του σχετικού εξοπλισμού του υπολογιστή από φυσικές καταστροφές, όπως κλοπή, βανδαλισμοί, πλημμύρες, φωτιά κλπ.

o *Ασφάλεια υπολογιστικού συστήματος.* Αναφέρεται στην προστασία εκείνων των πληροφοριών του υπολογιστή που διαχειρίζεται άμεσα το λειτουργικό σύστημα (προγράμματα εφαρμογών, αρχεία δεδομένων κλπ). Επικεντρώνεται κυρίως στις συγκεκριμένες υπηρεσίες των λειτουργικών συστημάτων που καθορίζουν το ποιος και πώς θα δικαιούται να προσπελάσει τα δεδομένα και τις εφαρμογές που φιλοξενεί το υπολογιστικό σύστημα.

o *Ασφάλεια βάσεων δεδομένων.* Αναφέρεται στην ικανότητα του συστήματος να εφαρμόσει μια προκαθορισμένη πολιτική προστασίας των περιεχομένων μιας βάσης δεδομένων, στην οποία διευκρινίζεται ποιοι εξουσιοδοτούνται να δουν ή/και να τροποποιήσουν τα προστατευμένα δεδομένα.

o *Ασφάλεια δικτύων επικοινωνιών.* Αναφέρεται στην προστασία των πληροφοριών κατά τη μετάδοσή τους μέσω τηλεφωνικών, δορυφορικών ή άλλων δικτύων, όπως είναι τοπικά δίκτυα και το Internet.

Κατηγορίες Μέτρων Προστασίας

Γενικά, υπάρχουν τέσσερις βασικοί τρόποι άμυνας οι οποίοι μπορεί να βοηθήσουν ώστε να υπάρξει επαρκής ασφάλεια σε ένα πληροφοριακό σύστημα.:

o *Μέτρα προσπέλασης συστήματος.* Εξασφαλίζουν ότι οι μη εξουσιοδοτημένοι χρήστες δεν εισάγονται στο σύστημα.

o *Μέτρα προσπέλασης δεδομένων.* Ελέγχουν ποιος μπορεί να έχει πρόσβαση σε ποια δεδομένα και με ποιο σκοπό. Οι εφαρμογές βάσεων δεδομένων τυπικά απαιτούν έναν υψηλό βαθμό λεπτομέρειας του ελέγχου προσπέλασης.

o *Διαχείριση συστήματος και ασφάλειας.* Εκτέλεση των off-line διαδικασιών που διαμορφώνουν ή επιβάλλουν ένα ασφαλές σύστημα, ορίζοντας ξεκάθαρα τις υπευθυνότητες του διαχειριστή συστήματος, εκπαιδεύοντας τους χρήστες κατάλληλα και ελέγχοντας ότι οι διαδικασίες ασφάλειας τηρούνται από τους χρήστες.

ο *Σχεδιασμός συστήματος.* Αξιοποίηση βασικών χαρακτηριστικών και δυνατοτήτων ασφάλειας του υλικού και του λογισμικού.

Τύποι Μέτρων Προστασίας

Οι κύριοι τύποι μέτρων για την πρόληψη της εκμετάλλευσης των ευπαθειών ενός πληροφοριακού συστήματος είναι:

❖ *Κρυπτογράφηση.* Μετασχηματίζοντας τα δεδομένα ώστε να είναι ακατάληπτα από τον εξωτερικό παρατηρητή, η αξία των υποκλοπών και η πιθανότητα για τροποποιήσεις σχεδόν εκμηδενίζεται.

❖ *Μέτρα λογισμικού.* Τα προγράμματα πρέπει να είναι αρκετά ασφαλή και αξιόπιστα ώστε να αποτρέπουν εξωτερικές επιθέσεις. Τα μέτρα προγραμμάτων περιλαμβάνουν:

- Τα μέτρα ανάπτυξης, όπου πρόκειται για τα πρότυπα σύμφωνα με τα οποία σχεδιάζονται, κωδικοποιούνται, ελέγχονται και συντηρούνται τα προγράμματα.
- Τα μέτρα λειτουργικού συστήματος, όπου πρόκειται για περιορισμούς που επιβάλλονται από το λειτουργικό σύστημα με σκοπό την προστασία κάθε χρήστη από τους υπόλοιπους χρήστες.
- Τα μέτρα μέσα στα προγράμματα, όπου πρόκειται για μέτρα που επιβάλλουν περιορισμούς ασφάλειας, όπως για παράδειγμα οι περιορισμοί προσπέλασης σε ένα σύστημα διαχείρισης βάσης δεδομένων.

❖ *Μέτρα υλικού.* Έχουν εφευρεθεί αρκετές συσκευές για να βοηθούν στην ασφάλεια των υπολογιστών. Αυτές ποικίλλουν από την υλοποίηση της κρυπτογράφησης με υλικό μέχρι τις συσκευές για επιβεβαίωση της ταυτότητας των χρηστών.

❖ *Φυσικά μέτρα υλικού.* Τα φυσικά μέτρα είναι από τα πιο εύκολα, πιο αποτελεσματικά και λιγότερο δαπανηρά μέτρα για την ασφάλεια των πληροφοριακών συστημάτων και των συστημάτων βάσεων δεδομένων (για παράδειγμα, κλειδαριές στις πόρτες, φύλακες, αντίγραφα ασφάλειας κλπ).

❖ *Πολιτικές ασφάλειας.* Μερικά άλλα μέτρα αποτελούν αντικείμενο πολιτικής, όπως για παράδειγμα ο έλεγχος προσπέλασης. Παρά τα προβλήματα διαχείρισης σε μεγάλους και εξελισσόμενους οργανισμούς, οι πολιτικές ελέγχου προσπέλασης πρέπει να προσαρμόζονται στις επί μέρους συνθήκες και απαιτήσεις ασφάλειας του κάθε πληροφοριακού συστήματος.

Αποτελεσματικότητα των Μέτρων Προστασίας

Η αποτελεσματικότητα των μέτρων προστασίας ή αντίμετρων εξαρτάται από το πόσο σωστά χρησιμοποιούνται. Ορισμένοι βασικοί παράγοντες που επηρεάζουν την αποτελεσματικότητα των αντίμετρων είναι:

- *Η επίγνωση του μεγέθους του προβλήματος.* Τα άτομα που εφαρμόζουν τα μέτρα ή ακόμη περισσότερο αυτά που είναι υπεύθυνα για τη διαμόρφωσή τους, πρέπει να έχουν πειστεί για την ανάγκη για ασφάλεια και για το επίπεδο της ασφάλειας που προβλέπεται σε κάθε περίπτωση.
- *Οι περιοδικές αναθεωρήσεις.* Η αμφισβήτηση της αποτελεσματικότητας ενός μέτρου, πρέπει να είναι συνεχής. Το περιβάλλον λειτουργίας ενός πληροφοριακού συστήματος είναι δυναμικό αφού συνεχώς οι συνθήκες, οι απειλές και οι ανάγκες εξελίσσονται. Είναι πολύ λογικό λοιπόν τα περισσότερα μέτρα προστασίας να παύουν να είναι αποδοτικά αν δε γίνουν οι κατάλληλες προσαρμογές και αντικαταστάσεις.
- *Η αλληλοεπικάλυψη μέτρων.* Στις περισσότερες περιπτώσεις η ορθή αντιμετώπιση μιας ευπάθειας απαιτεί την εφαρμογή διαφορετικών μεταξύ τους αντιμέτρων. Ένας συνδυασμός φυσικών, δικτυακών-επικοινωνιακών και υπολογιστικών μέτρων προστασίας ελαχιστοποιεί τις υπαρκτές απειλές, ενώ συχνά η συνολική αξιοπιστία του συστήματος προστασίας στηρίζεται στις δυνατότητες αλληλοσυμπλήρωσης και αλληλοεπικάλυψης των μέτρων αυτών. Αυτό φυσικά δε σημαίνει ότι το κάθε μέτρο μεμονωμένα δεν είναι ανθεκτικό και ισχυρό.

Άλλωστε, σύμφωνα με την «αρχή του ασθενέστερου σημείου», οι ειδικοί στην ασφάλεια πληροφοριακών συστημάτων πρέπει να συνυπολογίζουν όλα τα υπάρχοντα ρήγματα ασφάλειας, διότι οχυρώνοντας μόνο κάποια από αυτά απλώς κάνουν τις υπόλοιπες ευπάθειες πιο ελκυστικές για όσους κακοήθεις σκοπεύουν να εκδηλώσουν επιθέσεις. Συχνά, λέγεται σχετικά ότι η ασφάλεια έχει παρόμοια συμπεριφορά με μια αλυσίδα: η ισχύς της είναι τόση όση και η ισχύς του ασθενέστερου κρίκου της.

- *Οι πιθανότητες χρησιμοποίησης.* Σύμφωνα με την «αρχή της αποτελεσματικότητας», για να είναι αποτελεσματικά τα μέτρα πρέπει να χρησιμοποιούνται και να είναι επαρκή, κατάλληλα και εύκολα στη χρήση τους. Δηλαδή, υπονοείται εδώ ότι πρωταρχική προϋπόθεση για την απόδοση ενός μέτρου είναι το να βρίσκεται σε εφαρμογή την κρίσιμη στιγμή. Αυτό σημαίνει ότι η χρήση των αντιμέτρων δεν πρέπει να επηρεάζει αρνητικά τις εργασίες που αυτά προστατεύουν και να είναι «οικονομική» ως προς την κατανάλωση των πόρων του συστήματος (χρόνο, χώρο μνήμης, ανθρώπινη δραστηριότητα κλπ).

Απαιτήσεις Ασφάλειας Πληροφοριακού Συστήματος

Ο βασικός σκοπός της ασφάλειας Πληροφοριακών Συστημάτων πρέπει να είναι η προστασία του υπολογιστικού συστήματος και οποιουδήποτε άλλου στοιχείου που σχετίζεται με αυτό (όπως για παράδειγμα ο Η/Υ αυτός καθαυτός), με πρώτη προτεραιότητα για τις πληροφορίες που είναι αποθηκευμένες στο πληροφοριακό σύστημα.

Αξίζει να σημειωθεί, ότι η μη εξουσιοδοτημένη ενέργεια δεν περιορίζεται μόνο σε μη-εξουσιοδοτημένα πρόσωπα, όπως οι επισκέπτες ενός νοσοκομείου. Ακόμη και εξουσιοδοτημένοι χρήστες, ή ακόμα χειρότερα, διαχειριστές συστήματος, πιθανόν να προσπαθήσουν να εκτελέσουν μη-εξουσιοδοτημένες ενέργειες. Αυτό αυξάνει την ανάγκη για μια τεχνολογία πληροφορικής που να είναι ικανή να παρέχει σε ένα άτομο αναμφισβήτητες αποδείξεις για το αν έκανε μια κάποια ενέργεια ή όχι (*απόδοση ευθυνών*).

Ασφάλεια των Πληροφοριών που Διακινούνται στο Διαδίκτυο

Η διακίνηση των δεδομένων μέσω του Διαδικτύου προσφέρει σημαντικά πλεονεκτήματα σε σχέση με τις κλασικές μεθόδους διακίνησής τους. τα δεδομένα γίνονται διαθέσιμα σε ελάχιστο χρόνο για χρήση και αξιοποίηση, ανεξάρτητα από τον όγκο τους, ενώ το κόστος αποστολής σε οποιαδήποτε απόσταση είναι εξαιρετικά μικρό. Η χρήση του Διαδικτύου προσθέτει όμως επιπλέον απειλές κατά της ασφάλειας των πληροφοριών. Ακόμη, οι συνδεδεμένοι στο Διαδίκτυο υπολογιστές είναι δυνατόν να αποτελέσουν στόχο διάφορων επιθέσεων.

Κατά την πραγματοποίηση οποιασδήποτε επικοινωνίας ή συναλλαγής μέσω του Διαδικτύου θα πρέπει λοιπόν να εξασφαλίζεται για τα δεδομένα που διακινούνται ότι:

- Δεν είναι αναγνώσιμα και αναγνωρίσιμα παρά μόνο από τον νόμιμο αποστολέα και τον αποδέκτη τους.
- Δεν έχουν αλλοιωθεί κατά τη μεταφορά τους μέσω του Διαδικτύου. Δηλαδή, το μήνυμα που παραλήφθηκε είναι το ίδιο με αυτό που αποστάλθηκε.
- Ο αποστολέας και ο παραλήπτης είναι πράγματι αυτοί που ισχυρίζονται ότι είναι.
- Ο αποστολέας δεν είναι δυνατόν να αρνηθεί το γεγονός ότι έστειλε το μήνυμα.
- Οι εμπιστευτικές πληροφορίες προστατεύονται από μη εξουσιοδοτημένη αποκάλυψη.
- Οι υπολογιστές διαθέτουν ικανοποιητική προστασία από ιούς που μεταδίδονται μέσω του Διαδικτύου.
- Οι ευαίσθητες πληροφορίες (όπως για παράδειγμα αριθμοί πιστωτικών καρτών, θέματα εξετάσεων κλπ) προστατεύονται επαρκώς όταν διακινούνται μέσω του Διαδικτύου (για παράδειγμα με επαρκή κρυπτογράφηση).

Προβλήματα κατά την Εισαγωγή Ασφάλειας

Η εισαγωγή (προσθήκη μηχανισμών) ασφάλειας σε ένα πληροφοριακό σύστημα είναι ένα δύσκολο και περίπλοκο έργο. Η δυσκολία οφείλεται κυρίως στο ότι:

- Τα σύγχρονα πληροφοριακά συστήματα περιέχουν συχνά ένα τεράστιο σε όγκο και πολυπλοκότητα όγκο λογισμικού, και τα μεγάλα έργα λογισμικού έχει ιστορικά αποδειχθεί ότι είναι σχεδόν αδύνατο να υλοποιηθούν χωρίς λάθη.
- Η ασφάλεια συνήθως δεν περιλαμβάνεται στο αρχικά σχεδιασμένο ή υλοποιημένο σύστημα αλλά προστίθεται κατόπιν.
- Η ασφάλεια κοστίζει, συνήθως, αρκετά.
- Πολύ συχνά το πρόβλημα έγκειται στους ανθρώπους που χρησιμοποιούν το σύστημα και όχι στην τεχνολογία που χρησιμοποιείται.

Αναγκαιότητα και Σκοπιμότητα της Ασφάλειας

Είναι γεγονός ότι , παρά την προφανή της χρησιμότητα, η λήψη των απαραίτητων μέτρων ασφαλείας δημιουργεί πολλές φορές κάποια πρόσθετη επιβάρυνση στην απόδοση και το κόστος λειτουργίας του πληροφοριακού συστήματος του οργανισμού. Θα πρέπει ακόμα να αποδεχτούμε το κόστος της ασφάλειας και ως κόστος χρόνου και ως κόστος χρήματος. Συνεπώς, μπορεί να θεωρηθεί ότι η ασφάλεια βρίσκεται σε σχέση αντιστρόφως ανάλογη με την αποδοτικότητα του πληροφοριακού συστήματος του οργανισμού. Αυτό όμως δεν είναι σωστό γιατί η ασφάλεια είναι κόστος αναγκαίο για την ομαλή και εύρυθμη λειτουργία του.

Το συγκεκριμένο κόστος για την ασφάλεια των πληροφοριακών συστημάτων ενός οργανισμού, εξαρτάται και προκύπτει από την εκάστοτε ακολουθούμενη πολιτική ασφάλεια. Απαιτείται συνεπώς μια πολιτική ασφαλείας η οποία θα πρέπει να εξισορροπεί το κόστος εισαγωγής ασφάλειας από την μία πλευρά και το κόστος ζημιών από πιθανολογούμενο κίνδυνο από την άλλη. Επίσης, θα πρέπει να δημιουργούνται τέτοιες συνθήκες ασφάλειας ώστε να μην παρεμποδίζεται η ευελιξία και η ανάπτυξη του οργανισμού.

Η αναγκαία πολιτική ασφάλειας καθορίζεται από μία δυναμική εκτίμηση του κόστους των μέτρων ασφάλειας σε σχέση με τις συνέπειες που θα έχει για τον οργανισμό οποιαδήποτε πρόκληση δυσλειτουργίας. Ο βασικός αυτός κανόνας ισχύει για όλους τους τομείς και όλα τα επίπεδα ασφαλείας. Έτσι, σε κάθε περίπτωση όπου απαιτείται η λήψη κάποιου μέτρου ασφαλείας, πρέπει να εξετάζεται η πιθανότητα να συμβεί κάποιο γεγονός/πρόβλημα ασφάλειας, σε σχέση με τις συνέπειες που αυτό θα δημιουργήσει. Εάν η τιμή των δύο αυτών παραμέτρων είναι υψηλή, τότε πρέπει απαραίτητα να ληφθούν μέτρα, ανεξάρτητα από το κόστος πρόληψης.

Τέλος, πρέπει να σημειωθεί ότι η ασφάλεια χαρακτηρίζεται από τη φύση της ως δυναμική παράμετρος και όχι στατική, καθώς η τεχνολογία , ο ανταγωνισμός, η πολυπλοκότητα των πληροφοριακών συστημάτων και η ολοένα βελτιούμενη επιτηδειότητα των «επιτιθέμενων», απαιτούν τη λήψη νέων και συνεχώς αυστηρότερων μέτρων ασφαλείας, συνεπώς, η ακολουθούμενη πολιτική ασφαλείας θα πρέπει να επανεξετάζεται τακτικά και να διορθώνεται όπου αυτό κρίνεται απαραίτητο.

Κρυπτογραφία

Καθώς η περιοχή έρευνας που σχετίζεται με την κρυπτογραφία εξελίσσεται συνεχώς, οι διαχωριστικές γραμμές του τι είναι πραγματικά η κρυπτογραφία και τι όχι καθίστανται όλο και πιο δυσδιάκριτες. Ως *κρυπτογραφία* μπορεί να ορισθεί ο επιστημονικός κλάδος που ασχολείται με την μετατροπή των πληροφοριών, με σκοπό τη διαφύλαξη του απορρήτου τους. σκοπός της είναι να διασφαλίσει την ιδιωτικότητα ενός μηνύματος με το να κρατά την πληροφορία «κρυφή» από οποιοδήποτε άτομο, το οποίο δεν έχει ορισθεί ως αποδέκτης του μηνύματος, ακόμα και εάν έχει πρόσβαση στα κρυπτογραφημένα δεδομένα. Στην ορολογία της κρυπτογραφίας, το αρχικό μήνυμα που προορίζεται για κρυπτογράφηση ονομάζεται *απλό κείμενο (plaintext* ή *cleartext).* Η διαδικασία μετατροπής του περιεχομένου του μηνύματος σε μορφή τέτοια που να μην είναι κατανοητή για μη εξουσιοδοτημένους αποδέκτες ονομάζεται *κρυπτογράφηση*, ενώ το κρυπτογραφημένο μήνυμα ονομάζεται *κρυπτογράφημα (ciphertext).* Η κρυπτογράφηση ενός μηνύματος πραγματοποιείται με τη χρήση μιας μαθηματικής συνάρτησης, η οποία ονομάζεται *κλειδί.*

Σε ορισμένους κρυπτογραφικούς μηχανισμούς χρησιμοποιείται τι ίδιο κλειδί τόσο για τη διαδικασία της κρυπτογράφησης, όσο και της αποκρυπτογράφησης ενώ σε άλλους έχουμε διαφορετικά κλειδιά. Ως *αποκρυπτογράφηση* ορίζεται η αντίστροφη διαδικασία κατά την οποία το κρυπτογραφημένο μήνυμα μετατρέπεται στο αρχικό απλό μήνυμα με τη βοήθεια ενός κλειδιού.

Εκτός από την κρυπτογραφία που έχει στόχο τη διατήρηση της μυστικότητας των μηνυμάτων, υπάρχει και η *κρυπτανάλυση*, η οποία ορίζεται ως η τεχνική της παραβίασης του κρυπτογραφημένου μηνύματος, χωρίς να είναι γνωστό το κλειδί της αποκρυπτογράφησης. Η τεχνική της επινόησης κρυπτογραφημάτων και της παραβίασης αυτών είναι συνολικά γνωστή ως *κρυπτολογία.*

Ιστορικά, το πλέον γνωστό κρυπτογράφημα είναι αυτό του Ιουλίου Καίσαρα, ο οποίος δεν εμπιστευόταν τους αγγελιοφόρους που χρησιμοποιούσε για να μεταφέρουν τα μηνύματά του. Έτσι αντικαθιστούσε κάθε γράμμα Α με το γράμμα D, κάθε Β με το Ε κ.ο.κ. μόνο κάποιος

που γνώριζε τον κανόνα της «μετατόπισης κατά 3», που ουσιαστικά ήταν το κλειδί, μπορούσε να αποκρυπτογραφήσει τα μηνύματα.

Παλαιότερα χρησιμοποιούσαν την κρυπτογράφηση αποκλειστικά για στρατιωτικούς σκοπούς. Στην σημερινή κοινωνία της πληροφορίας. Η κρυπτογράφηση είναι ένα από τα βασικά εργαλεία διατήρησης του απορρήτου των μηνυμάτων με όλα τα προφανή πλεονεκτήματα. Ως αποτέλεσμα, η σύγχρονη κρυπτογραφία αποτελεί κάτι περισσότερο από απλή κρυπτογράφηση και αποκρυπτογράφηση δεδομένων. Για παράδειγμα, η πιστοποίηση αποτελεί μια εξίσου θεμελιώδη έννοια που συνδέεται άμεσα με την κρυπτογραφία. Όταν υπογράφεται ένα έγγραφο, είναι απαραίτητο να υπάρχουν μηχανισμοί με τους οποίους να μπορούμε να πιστοποιήσουμε τον κάτοχο του εγγράφου. Η κρυπτογραφία μας παρέχει μηχανισμούς για τέτοιες διαδικασίες. Η ψηφιακή υπογραφή «συνδέει» ένα έγγραφο με το χρόνο της δημιουργίας του.

Γενικότερα, η κρυπτογραφία μπορεί να χρησιμοποιηθεί σε μια πληθώρα εφαρμογών, όπως:

- Προστασία δεδομένων, αποθηκευμένων στον υπολογιστή, από μη εξουσιοδοτημένη πρόσβαση.
- Προστασία δεδομένων κατά τη μεταφορά τους ανάμεσα σε δύο υπολογιστικά συστήματα.
- Ανίχνευση τυχαίας ή εσκεμμένης αλλαγής σε δεδομένα.
- Πιστοποίηση της ταυτότητας του συντάκτη/εκδότη ενός κειμένου ή μηνύματος.

Βέβαια, η κρυπτογράφηση έχει και μειονεκτήματα, όπως το γεγονός ότι δε μπορεί να αποτρέψει τη διαγραφή δεδομένων από ένα εισβολέα του συστήματος. Επίσης, κατά τη διάρκεια μιας επίθεσης μπορεί να μεταβληθεί το πρόγραμμα κρυπτογράφησης, ώστε να χρησιμοποιεί διαφορετικό κλειδί από αυτό που έχει καθοριστεί από το νόμιμο χρήστη ή να καταγραφούν όλα τα κλειδιά για μελλοντική χρήση. Επιπλέον, μπορεί να βρεθεί ένας εύκολος και όχι ευρέως γνωστός τρόπος για την αποκωδικοποίηση μηνυμάτων και, τέλος, μπορεί ένα αρχείο να προσπελασθεί πριν την κωδικοποίησή του ή μετά την αποκωδικοποίησή του. Οι παραπάνω λόγοι συντελούν στο να χρησιμοποιείται η κρυπτογράφηση ως μέρος της «αρχιτεκτονικής ασφάλειας» ενός συστήματος και όχι ως υποκατάστατο όλων των υπαρχόντων μηχανισμών ασφάλειας.

Δημιουργία και διακίνηση των κλειδιών

Ο σχεδιασμός ενός αξιόπιστου κρυπτογραφήματος είναι απλά και μόνο το πρώτο βήμα για την ασφάλειά του. Αποτελεί όμως ανάλογη πρόκληση και ο τρόπος διαχείρισής του, στον οποίο ανήκουν η δημιουργία, η διακίνηση, η αποθήκευση και η επιδιόρθωση των μυστικών κλειδιών του.

Τα προγράμματα δημιουργίας κλειδιών, χρησιμοποιούν τυπικά μια ψευδοτυχαία διαδικασία η οποία περιλαμβάνει την ανάγνωση πληροφοριών, που αφορούν την κατάσταση του συστήματος, όπως για παράδειγμα το χρόνο που αυτό δείχνει. Εκτός και αν οι συγκεκριμένες τιμές είναι απρόβλεπτες και έχουν μεγάλη ποικιλία, ένας αντίπαλος μπορεί να εντοπίσει ένα κλειδί εξετάζοντας το σύστημα.

Σε ορισμένες εφαρμογές, οι χρήστες δημιουργούν τα δικά τους κλειδιά ή συμμετέχουν στη διαδικασία δημιουργίας ενός κλειδιού. Ενώ η κρυπτογράφηση χρησιμοποιείται για την προστασία των επικοινωνιών, απαιτείται κάποια μέθοδος, με την οποία ο αποστολέας και ο λήπτης θα μπορούν να συμφωνήσουν για το κρυφό κλειδί που θα χρησιμοποιούν. Ακόμα και για προφανείς λόγους, ο αποστολέας δε μπορεί να στείλει το κλειδί στο λήπτη σε ανοιχτή γλώσσα.

Εάν το σχετικό κανάλι ήταν ασφαλές, τότε δε θα χρειαζόταν να γίνει καμία κρυπτογράφηση. Μια πρώτη λύση του προβλήματος θα μπορούσε να είναι η εκτός γραμμής συνεννόηση των ενδιαφερομένων, δηλαδή μια πρόσωπο με πρόσωπο συνάντησή τους. ωστόσο, κάτι τέτοιο δεν είναι πάντα πρακτικό. Οι ενδιαφερόμενοι μπορεί να βρίσκονται σε διαφορετικά και απομακρυσμένα μεταξύ τους μέρη της ηπείρου τους ή της γης. Μια δεύτερη λύση, είναι να σταλεί το κλειδί μέσω ενός άλλου καναλιού που είναι ασφαλές, για παράδειγμα με κοινής εμπιστοσύνης ιδιωτικό ταχυδρομείο. Το μειονέκτημα της περίπτωσης αυτής είναι η καθυστέρηση. Σε πολλές περιπτώσεις, όπως το ηλεκτρονικό εμπόριο, οι χρήστες και τα προγράμματα που τρέχουν για λογαριασμό τους χρειάζονται έναν τρόπο άμεσης κατοχύρωσης του κλειδιού που χρησιμοποιούν.

Ψηφιακές υπογραφές

Μια ψηφιακή υπογραφή είναι ένα μπλοκ δεδομένων προσαρτημένων σε ένα μήνυμα ή σε ένα έγγραφο και η οποία συνδέει τα δεδομένα αυτά με ένα συγκεκριμένο άτομο ή οντότητα. Ο σύνδεσμος αυτός, είναι τέτοιος, που η υπογραφή μπορεί να επιβεβαιωθεί από το λήπτη ή από ένα τρίτο ανεξάρτητο μέρος, ενώ πρακτικά δεν μπορεί να πλαστογραφηθεί. Εάν ακόμα και ένα μπιτ δεδομένων παραληφθεί από αυτή, η υπογραφή δε θα μπορεί να περάσει τη διαδικασία επιβεβαίωσής της με επιτυχία. Οι ψηφιακές υπογραφές διασφαλίζουν την αυθεντικότητα της πηγής ενός μηνύματος. Παρέχουν επίσης τη βεβαιότητα ότι δεν μπορεί κάποιος να αρνηθεί το ότι έχει υπογράψει ένα μήνυμα και να αποστασιοποιηθεί από αυτό. Εκτός και αν το ιδιωτικό κλειδί ενός προσώπου έχει υπεξαιρεθεί, κανείς άλλος δε θα μπορούσε να αναπαραγάγει τη συγκεκριμένη υπογραφή.

Κάτω από φυσιολογικές συνθήκες, μια ψηφιακή υπογραφή δεν αποδεικνύει το ότι ένα έγγραφο γράφτηκε από κάποιον, από το γεγονός και μόνο ότι ο δημιουργός του είχε πρόσβαση σε αυτό και το υπέγραψε. Το έγγραφο θα μπορούσε να είχε κλαπεί. Ωστόσο, σε συνθήκες όπου η διαδικασία υπογραφής του συνδυάζεται με τη δημιουργία του, μια υπογραφή μπορεί να αποτελεί απόδειξη για την προέλευση ενός εγγράφου. Εάν μια ψηφιακή φωτογραφική μηχανή περιέχει ένα ιδιωτικό κλειδί με σκοπό την υπογραφή των φωτογραφιών τη στιγμή της λήψης τους, η υπογραφή αυτή αποτελεί μια ισχυρή απόδειξη για το ότι μια φωτογραφία έχει ληφθεί με τη συγκεκριμένη φωτογραφική μηχανή. Αυτό μπορεί να μας προστατεύσει από τη διαμόρφωση με τον υπολογιστή των ψηφιακών φωτογραφιών, κάτι που γίνεται σχετικά εύκολα. Οι υπογεγραμμένες φωτογραφίες θα μπορούσαν να είναι ιδιαίτερα χρήσιμες σε μια ποινική δίκη στην οποία ο κατηγορούμενος προσπαθεί να ισχυριστεί πως μια ενοχοποιητική για τον ίδιο φωτογραφία έχει κατασκευαστεί.

Οι ψηφιακές υπογραφές μπορεί να χρησιμοποιηθούν για την αναγνώριση ατόμων που υπογράφουν σε υπολογιστές, που χρησιμοποιούν μηχανήματα ATM και που μπαίνουν σε κτίρια.

Έλεγχοι της πρόσβασης

Η πρόσβαση στην πηγή πληροφοριών μπορεί να ελεγχθεί είτε μέσω μιας παθητικής συσκευής που ίσως είναι μια συμβατική κλειδαριά ή μέσω ενός ενεργού συστήματος παρακολούθησης. Ένα τέτοιο σύστημα ελέγχου της πρόσβασης, εξετάζει το εάν κάποιος είναι εξουσιοδοτημένος να χρησιμοποιήσει μια πηγή με τον τρόπο που επιθυμεί. Εάν η σχετική εξέταση αποβεί θετική, τότε η πρόσβαση του επιτρέπεται, διαφορετικά του απαγορεύεται. Προτού ληφθεί οποιαδήποτε απόφαση, το σύστημα μπορεί να επιβεβαιώσει την ταυτότητα κάθε

ενδιαφερομένου. Σε ορισμένες περιπτώσεις, η διαδικασία προσδιορισμού της εξουσιοδότησης συνδυάζεται με την αντίστοιχη της επαλήθευσης. Η κατοχή μιας ειδικής κάρτας, για παράδειγμα, μπορεί να σημαίνει πως αυτός που την έχει είναι εκείνος που έχει δικαίωμα να μπαίνει σε ένα κτίριο με αυτή ή να έχει πρόσβαση σε έναν υπολογιστή. Μετά τη λήψη της σχετικής απόφασης, το σύστημα ελέγχου μπορεί να γράψει μια αναφορά για το συμβάν σε ένα ημερολόγιο που τηρεί. Αυτή η ενέργειά του μπορεί να βοηθήσει ένα σύστημα εντοπισμού εισβολών, το οποίο ψάχνει να βρει ενέργειες που γίνονται από μη εξουσιοδοτημένα πρόσωπα. Εφόσον έχει διαπιστωθεί μια τέτοια ενέργεια, θα μπορεί να δώσει αποδεικτικά στοιχεία για την πραγματοποίησή της.

Πολιτικές εξουσιοδότησης: οι έλεγχοι της πρόσβασης χρησιμεύουν για τον καθορισμό της πολιτικής που θα ακολουθηθεί στο θέμα της εξουσιοδότησης, η οποία προσδιορίζει με ακρίβεια της δραστηριότητες που είτε επιτρέπονται είτε απαγορεύονται. Η πολιτική αυτή μπορεί να καθορίσει της ενέργειες που γίνονται, όχι μόνο από ανθρώπους αλλά και από προγράμματα υπολογιστών. Μπορεί να εφαρμοστεί σε κάθε μέσο – στο περιβάλλον, σε έντυπο υλικό, σε δισκέτες και μαγνητοταινίες, της τηλεπικοινωνίες, της ραδιοφωνικές εκπομπές και φυσικά, της υπολογιστές και τα δίκτυά της. λαμβάνοντας υπόψη της πηγές των υπολογιστών για παράδειγμα, η πολιτική εξουσιοδότησης που ακολουθεί μια επιχείρηση μπορεί να προσδιορίσει το ποιοι έχουν δικαίωμα πρόσβασης σε της, να τρέχει κάποια συγκεκριμένα προγράμματα, να διαβάζει συγκεκριμένα αρχεία ή μηνύματα ηλεκτρονικού ταχυδρομείου, να απαντά σε κάποια από αυτά για παροχή πληροφοριών, να στέλνει ηλεκτρονικά δελτία τύπου για της δραστηριότητές της καθώς και να δημιουργεί, να τυπώνει ή να διαγράφει επίσημα έγγραφα. Λαμβάνοντας υπόψη δε της εγκαταστάσεις της, στα πλαίσια της πολιτικής της μπορεί να καθορίζει το ποιος μπορεί να εισέρχεται σ' αυτές και το εάν οι επισκέπτες της θα συνοδεύονται από υπαλλήλους της.

Πολλά ζητήματα της ιδιωτικής ζωής ξεκινούν από πολιτικές ή από τη μη ύπαρξή της. για να ικανοποιήσουν τα συμφέροντα των καταναλωτών, οι οργανισμοί μπορεί να λένε της πελάτες της το πώς θα χρησιμοποιούν της προσωπικές της πληροφορίες και να υιοθετήσουν πολιτικές που απαγορεύουν τη δευτερεύουσα χρήση. Ορισμένοι οργανισμοί δημοσιεύουν την πολιτική της αυτή της ιστοσελίδες της, έτσι ώστε οι επισκέπτες της να γνωρίζουν το πώς πληροφορίες (που συνέλεξαν από την επίσκεψή της σε αυτές με τη συμπλήρωση αιτήσεων ή με cookies) θα χρησιμοποιηθούν.

Υπάρχουν αρκετοί λόγοι για της οποίους της οργανισμός θα πρέπει να καθιερώσει μια πολιτική, η οποία θα αφορά τη χρήση του Διαδικτύου. Εκτεταμένη χρήση, η οποία δε

σχετίζεται με δραστηριότητες που αφορούν την εργασία, μπορεί να έχει σαν αποτέλεσμα τη μείωση της παραγωγικότητας. Η ίδια μπορεί να επιβαρύνει της πηγές του δικτύου, προκαλώντας έτσι την παραγωγική του χρήση. Ο συγκεκριμένος οργανισμός μπορεί να θεωρηθεί ποινικά ή αστικά υπεύθυνος για δραστηριότητες που προκύπτουν από της πράξεις αυτές και οι οποίες μπορεί να αφορούν την αποστολή δυσφημιστικών μηνυμάτων, παιδική πορνογραφία κλπ. Η πολιτική μιας εταιρίας στο Internet μπορεί να εμποδίσει την πρόσβαση σε ιστοσελίδες, των οποίων το περιεχόμενο δεν έχει καμία σχέση με τον κύκλο των εργασιών της. Αυτή μπορεί να επιβάλλει τη συγκεκριμένη πολιτική της, μπλοκάροντας την πρόσβαση σε αυτές.

Πολιτικές Ασφάλειας Υψηλού Επιπέδου

Οι πολιτικές ασφάλειας υψηλού επιπέδου (high level security policies – HLSP) είναι διαχειριστικές οδηγίες που υποδεικνύουν πώς πρέπει να λειτουργεί της οργανισμός. Πρόκειται για εντολές υψηλού επιπέδου που αποσκοπούν στην παροχή καθοδήγησης στο τμήμα του προσωπικού που πρέπει να παίρνει τωρινές και μελλοντικές διαχειριστικές αποφάσεις. Της φορές, οι πολιτικές ασφάλειας υψηλού επιπέδου, θεωρούνται ως το ισοδύναμο των γενικευμένων απαιτήσεων.

Οι πολιτικές ασφάλειας υψηλού είναι τα πρωταρχικά δομικά στοιχεία για κάθε προσπάθεια εφαρμογής ασφάλειας πληροφοριών. Προκειμένου να είναι αποτελεσματικός, της τεχνικός ασφάλειας πληροφοριών (που μπορεί να είναι είτε της επαγγελματίας πληροφορικής, είτε της διαχειριστής) πρέπει να ακολουθεί μια πολιτική που να παρέχει υποστήριξη και της τη διεύθυνση και της τη διαχείριση. Οι πολιτικές ασφάλειας υψηλού επιπέδου περιλαμβάνουν γενικές εντολές για σκοπούς, αντικείμενα, σχέδια, υπευθυνότητες, ήθη και γενικές διαδικασίες.

Οι πολιτικές ασφάλειας υψηλού επιπέδου χρησιμοποιούνται ως αναφορά για μια ευρεία ποικιλία ενεργειών ασφάλειας και απορρήτου πληροφοριών, οι οποίες περιλαμβάνουν:

- Τον προσδιορισμό των δικαιωμάτων ελέγχου προσπέλασης
- Την εκτέλεση αναλύσεων κινδύνων
- Την καθοδήγηση ερευνών για κινδύνους ασφάλειας κλπ.

Η πολιτική ασφάλειας υψηλού επιπέδου είναι υποχρεωτική για όλα τα μέλη του προσωπικού της οργανισμού. Παρ' όλ' αυτά, πρέπει να επανεξετάζεται περιοδικά από τη διαχείριση της οργανισμού για να εντοπίζονται τα σημεία αναθεώρησής της.

Μια πολιτική ασφάλειας υψηλού επιπέδου αναφέρεται πρωταρχικά σε δύο βασικούς συντελεστές:

- Τα δρώντα υποκείμενα (για παράδειγμα ασθενείς, γιατροί παθολόγοι, ειδικοί ιατρικής πληροφορικής, διαχειριστές, νοσοκομειακές αρχές, ασφαλιστικές εταιρείες κλπ).
- Τα αντικείμενα δεδομένα που πρέπει να προστατευθούν (για παράδειγμα οι ιατρικές εγγραφές, δεδομένα επικοινωνίας κλπ).

Σύμφωνα με την εννοιολογική προσέγγιση για πολιτικές ασφάλειας υψηλού επιπέδου, η ασφάλεια και η μυστικότητα πληροφοριακών συστημάτων μπορεί εννοιολογικά να θεωρηθεί στα εξής ξεχωριστά επίπεδα:

- *Γενικές αρχές*, οι οποίες κυβερνούν την ασφάλεια και μυστικότητα των δεδομένων και των πληροφοριακών συστημάτων που επεξεργάζονται αυτά τα δεδομένα. Αυτές οι γενικές αρχές είναι κοινωνικά και πολιτιστικά εξαρτημένες.
- *Αρχές*, οι οποίες προκύπτουν όταν οι γενικές αρχές εξετάζονται στα πλαίσια της συγκεκριμένου διαχειριστικού περιβάλλοντος.
- *Οδηγίες*, οι οποίες είναι συγκεκριμένα λειτουργικά βήματα που θα πρέπει να ακολουθούνται από τα μέλη του προσωπικού με σκοπό την ικανοποίηση μιας συγκεκριμένης αρχής. Οι οδηγίες προκύπτουν όταν οι αρχές εξετάζονται στα πλαίσια της συγκεκριμένου τεχνολογικού περιβάλλοντος.
- *Κανόνες*, οι οποίοι προκύπτουν όταν οι οδηγίες εξετάζονται μέσα σε ένα συγκεκριμένο περιβάλλον εγκατάστασης.

Μια πολιτική ασφάλειας υψηλού επιπέδου αφορά τα δύο μεσαία επίπεδα και επομένως αποτελείται από ένα σύνολο αρχών, κάθε μια από της οποίες αναλύεται σε ένα σύνολο οδηγιών. Η πολιτική ασφάλειας υψηλού επιπέδου ορίζει με αυτόν τον τρόπο τη γενική προσέγγιση που της οργανισμός θα πρέπει να έχει της την κατεύθυνση της υλοποίησης ασφάλειας. Με άλλα λόγια, καθορίζει τι θα πρέπει να γίνει προκειμένου να έχουμε αποτελεσματική υλοποίηση ασφάλειας, χωρίς να παρέχει τεχνικές λεπτομέρειες για το πώς θα γίνει αυτό. Αυτές οι λεπτομέρειες μπορούν να βρεθούν της επιμέρους πολιτικές ασφάλειας που θα αναπτυχθούν. Επιπλέον, η πολιτική ασφάλειας υψηλού επιπέδου παρέχει σε αυτή τη φάση ένα σύνολο υποχρεωτικών συνθηκών για να διασφαλίζεται μια ικανοποιητική ασφάλεια των πληροφοριών που επεξεργάζονται από το πληροφοριακό σύστημα.

Τέλος, της από της πλέον υπεύθυνους στόχους σε έναν οργανισμό είναι η λειτουργική ποιότητα και φήμη και κατ' επέκταση η εμπιστοσύνη και η αποδοχή των χρηστών. Αυτοί οι στόχοι μπορούν να επιτευχθούν εφόσον η πολιτική ασφάλειας του πληροφοριακού συστήματος, αντικατοπτρίζει της προσωπικές απαιτήσεις ασφάλειας όλων των ατόμων που

επηρεάζονται. Ως εκ τούτου η πολιτική ασφάλειας που θα ορισθεί δεν μπορεί να είναι ανεξάρτητη από το τεχνικό σύστημα που χρησιμοποιείται, αφού είναι φανερό ότι δεν εμπιστεύονται όλα τα επηρεαζόμενα άτομα το τεχνικό σύστημα με τον ίδιο τρόπο και στο ίδιο μέτρο. Ακόμη και αν το εμπιστεύονται το ίδιο, η εμπιστοσύνη της αφορά διαφορετικά και επιτηρούμενα συστατικά (υλικό ή λογισμικό) της μεγάλου διαδικτυωμένου και κατανεμημένου πληροφοριακού συστήματος. Έτσι, η πολιτική ασφάλειας πρέπει να υιοθετεί μια κατά το δυνατόν αποκεντρωμένη άποψη για το ποια υποκείμενα ή ομάδες της πρέπει να έχουν δικαίωμα προσπέλασης στα αντικείμενα του πληροφοριακού συστήματος.

Φίλτρα

Ένα φίλτρο είναι ένα πρόγραμμα ή μια συσκευή, που παρακολουθεί τα εισερχόμενα και τα εξερχόμενα πακέτα από ένα δίκτυο υπολογιστών, με σκοπό να προσδιορίσει το εάν στα πακέτα αυτά θα πρέπει να επιτρέπεται η είσοδος ή η έξοδος από ένα σύστημα υπολογιστών. Οι αποφάσεις που θα αφορούν το πέρασμα ή μη της πακέτου μπορεί να στηριχθούν στην επικεφαλίδα του ή στα περιεχόμενά του. Οι πληροφορίες της επικεφαλίδας περιλαμβάνουν τον προσδιορισμό του δικτυακού πρωτοκόλλου, τη διεύθυνση στο Internet ή τη διεύθυνση προορισμού IP.

Φίλτρα για το ανεπιθύμητο ταχυδρομείο: ορισμένοι χρήστες και οργανισμοί απαντούν στα ανεπιθύμητα διαφημιστικά, κυρίως, μηνύματα ηλεκτρονικού ταχυδρομείου (spam) που λαμβάνουν με την εγκατάσταση προγραμμάτων που τα φιλτράρουν. Τα προγράμματα αυτά χρησιμοποιούν διάφορες στρατηγικές προκειμένου να αποφασίσουν για το ποια μηνύματα θα επιτρέψουν να περάσουν. Μια τέτοια στρατηγική ελέγχει τα «Από», «Χ-Αποστολέας» και «Αποστολέας» πεδία της επικεφαλίδας ενός μηνύματος. Εάν τα στοιχεία οποιουδήποτε από τα πεδία αυτά περιλαμβάνεται σ' ένα κατάλογο γνωστών spammers, τότε το μήνυμα αυτό διαγράφεται. Μια άλλη στρατηγική εξετάζει το πεδίο «Χ-Αποστολέας» και απορρίπτει μηνύματα που προέρχονται από αποστολείς που στέλνουν συνήθως ανεπιθύμητα διαφημιστικά μηνύματα. Μια Τρίτη στρατηγική απορρίπτει μηνύματα που στέλνονται από συγκεκριμένη διεύθυνση ενός αποστολέα. Όλες αυτές οι στρατηγικές διαγράφουν σε κάθε περίπτωση νόμιμα κυκλοφορούντα μηνύματα ηλεκτρονικού ταχυδρομείου.

Ορισμένοι παροχείς υπηρεσιών Internet προσπαθούν να φιλτράρουν τα ανεπιθύμητα μηνύματα που απευθύνονται στα μέλη τους, εξαιτίας της σχετικής επιβάρυνσης των υπολογιστών τους αλλά και της ενόχλησης που προξενούν σ' αυτά.

Φίλτρα του Ιστού: τα φίλτρα στον Ιστό χρησιμοποιούνται για να εμποδίσουν την εισαγωγή κάποιων θεμάτων σ' ένα σύστημα, την ώρα που οι χρήστες σερφάρουν σ' αυτόν. Ο σκοπός άλλης είναι η προστασία του πληροφοριακού χώρου των σέρφερς του Ιστού από υλικό το οποίο θα μπορούσε να υποβαθμίσει άλλης σκοπούς. Μια επιχείρηση, για παράδειγμα, θα μπορούσε να φιλτράρει πορνογραφικό υλικό έτσι ώστε οι υπάλληλοί άλλης να μην σπαταλούν τον εργασιακό άλλης χρόνο παρατηρώντας το.

Με ήδη πάνω από 200 εκατομμύρια σελίδες στον Ιστό και με συνεχώς νέες να εμφανίζονται, δεν είναι πρακτικό για άλλης δημιουργούς φίλτρων του Ιστού να ψάχνουν κάθε σελίδα για να δουν αν είναι κόσμια. Επομένως, τα συγκεκριμένα προϊόντα μπλοκάρουν την πρόσβαση στη βάση του ελέγχου μιας περιοχής σελίδων και όχι στη βάση του ελέγχου καθεμιάς σελίδας. Το αποτέλεσμα άλλης τακτικής άλλης είναι το ότι κάποιες σελίδες μπλοκάρονται σαν υποπροϊόντα μιας άλλης απαγορευμένης σελίδας.

Φίλτρα Προστασίας (Firewalls): γενικά η λέξη firewall αποδίδεται σε πυρίμαχους τοίχους που εμποδίζουν την εξάπλωση της φωτιάς από δωμάτιο σε δωμάτιο ή μεταξύ διαμερισμάτων. Στην περίπτωση των υπολογιστικών συστημάτων, τα firewalls αποτελούν την αναγκαία λύση προστασίας τους, καθώς αυτά συνδέονται ολοένα και περισσότερο σε δίκτυα τα οποία επίσης είναι συνδεδεμένα στο διαδίκτυο.

Από τη στιγμή που ένα δίκτυο αποκτήσει σύνδεση στο Internet, ανοίγει ένα κανάλι αμφίδρομης επικοινωνίας: οι χρήστες του δικτύου (insiders) αποκτούν επαφή με τον έξω κόσμο, αλλά ταυτόχρονα και οι outsiders, δηλαδή οι εξωτερικοί χρήστες ως αυτό το δίκτυο, αποκτούν πλέον δυνατότητα πρόσβασης σε αυτό. Ο τρομακτικός ρυθμός αύξησης του Διαδικτύου, προκαλεί ανάλογη αύξηση των πιθανών κινδύνων στα ιδιωτικά (private) δίκτυα που συνδέονται μαζί του. Για την προστασία τους από διάφορες εισβολές απαιτείται ένας κατάλληλος φράκτης. Ο φράκτης αυτός που καλείται firewall, πρέπει να είναι ικανός να επεξεργάζεται όλη την κυκλοφορία μηνυμάτων ανάμεσα σε ένα συγκεκριμένο τοπικό ή ιδιωτικό δίκτυο και στο Internet. Στην πραγματικότητα ένα σύστημα firewall ανορθώνει έναν εξωτερικό τοίχο ασφαλείας, οριοθετώντας μία περίμετρο προστασίας. Έτσι, προκαλεί ένα σαφή διαχωρισμό ανάμεσα στο προστατευμένο-εσωτερικό δίκτυο ενός οργανισμού (το οποίο θεωρείται ασφαλές και έμπιστο) και στο εξωτερικό διαδίκτυο (το οποίο θεωρείται μη ασφαλές και μη έμπιστο).

Ο πρωταρχικός σκοπός των firewalls είναι να προστατεύσουν τα δίκτυα από εξωτερικούς εισβολείς, περιορίζοντάς τους τα δικαιώματα προσπέλασης σε αυτό, χωρίς να

περιορίζουν την προσπέλαση στο εξωτερικό περιβάλλον. Για αυτό τα firewalls παρέχουν ένα περίβλημα προστασίας του δικτύου που το προστατεύουν από απειλές, όπως:

- *Μη εξουσιοδοτημένη προσπέλαση των δικτυακών πόρων*, όταν οι επίδοξοι εισβολείς προσπαθούν να εισχωρήσουν στο δίκτυο και να αποκτήσουν μη εξουσιοδοτημένη προσπέλαση στα αρχεία.
- *Άρνηση εξυπηρέτησης*, όταν κάποιος εξωτερικός παράγοντας γεμίζει τους διαθέσιμους ελεύθερους χώρους των δίσκων ή υπερφορτώνει τις γραμμές του δικτύου στέλνοντας μυριάδες μηνυμάτων σε έναν από τους ξενιστές του δικτύου.
- *Προσποίηση*, όταν τα μηνύματα του ηλεκτρονικού ταχυδρομείου φαίνονται ότι προέρχονται από κάποιον νόμιμο χρήστη ενώ έχουν παραποιηθεί από άλλον με σκοπό την πρόκληση παρεξηγήσεων ή ζημιών.

Ως λύση στα παραπάνω προβλήματα, πέρα από την ολοκληρωτική αποσύνδεση του δικτύου από τον έξω κόσμο, προτείνεται η υλοποίηση μηχανισμών προστασίας, όπως τα firewalls, τα οποία από τη μια φιλτράρουν την προσπέλαση στο δίκτυο, ενώ από τη άλλη επιτρέπουν την επικοινωνία με τον έξω κόσμο.

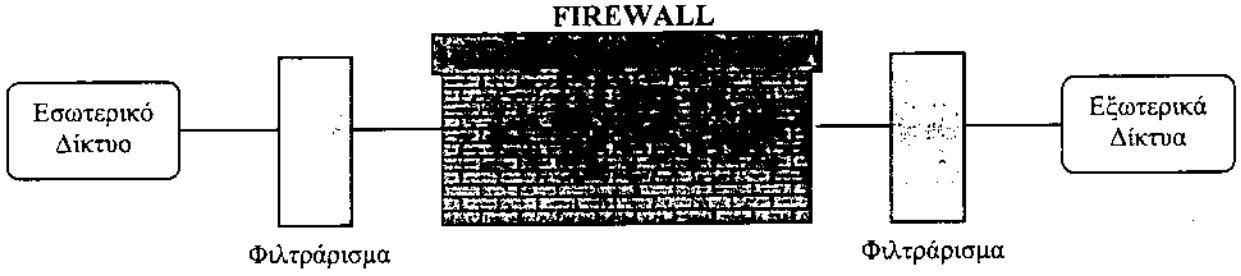
Ορισμοί

Ένα σύστημα firewall ορίζεται ως το λογισμικό και ο εξοπλισμός που τοποθετούμενος ανάμεσα στο διαδίκτυο και στο υπό προστασία δίκτυο, επιτρέπει την προσπέλαση των εξωτερικών χρηστών στο προστατευμένο δίκτυο, μόνο εφόσον διαθέτουν συγκεκριμένα χαρακτηριστικά. Έτσι, ένα τυπικό σύστημα firewall μπορεί να επιτρέπει επιλεκτικά την πρόσβαση στους εξωτερικούς χρήστες, βασιζόμενο σε ονόματα χρηστών και συνθηματικά ή σε IP διευθύνσεις ή ακόμη και σε ονόματα επικρατειών (domain names). Αυτός είναι ο κύριος σκοπός του: *να κρατήσει τις επικίνδυνες δραστηριότητες μακριά από το προστατευμένο περιβάλλον.*

Ένα firewall μπορεί να θεωρηθεί σαν ένα ζευγάρι μηχανισμών που ο ένας μπλοκάρει την κυκλοφορία των δεδομένων και ο άλλος επιτρέπει την ροή τους. Το ποια δεδομένα επιτρέπονται και ποια απορρίπτονται είναι ζήτημα της πολιτικής ελέγχου (control policy) που υποστηρίζει και εξαρτάται από τη συγκεκριμένη διαμόρφωσή του. Ένα σύστημα firewall δεν είναι απλά και μόνο ένας δρομολογητής, ένας διανομέας ή διακομιστής (server), ένας οικοδεσπότης ή ένα σύνολο εξοπλισμού και λογισμικού που παρέχει ασφάλεια στα δίκτυα. Οι αληθινές δυνατότητές του γίνονται εμφανείς αν το θεωρήσουμε ως ένα ισχυρό μέσο υλοποίησης μιας πολιτικής ασφαλείας που καθορίζει τις παρεχόμενες υπηρεσίες και τις

επιτρεπτές προσπελάσεις ανάμεσα σε έμπιστες και μη έμπιστες επικράτειες. Η υλοποίηση της πολιτικής ελέγχου προσπέλασης δικτύων γίνεται με την υποχρεωτική κατεύθυνση όλων των επικοινωνιών μέσω του firewall, ώστε να αποτελούν αντικείμενο για παραπέρα εξέταση και καταγραφή από αυτό.

Μια τυπική διάταξη firewalls παρουσιάζεται στην ακόλουθη εικόνα:



Σε αυτή τη διάταξη, το εσωτερικό δίκτυο χωρίζεται από τα εξωτερική δίκτυα με μια πύλη firewall. Η πύλη χρησιμοποιείται για την παροχή:

- υπηρεσιών αναμετάδοσης μεταξύ των δικτύων και
- υπηρεσιών φιλτραρίσματος για περιορισμό των πληροφοριών που διέρχονται με προορισμό/αφετηρία τους ξενιστές του εσωτερικού δικτύου.

Παρεχόμενη ασφάλεια

Καθώς τα τοπικά δίκτυα (local networks) συνδέονται στο Internet, αποτελεί ζήτημα μεγάλης σημασίας η διασφάλισης της κανονικής λειτουργίας τους από τους νόμιμους και παράνομους χρήστες τους. Η τοποθέτηση ενός firewall συστήματος ανάμεσα στο τοπικό δίκτυο ενός οργανισμού και το διαδίκτυο, παρέχει δυνατότητες ελέγχου στη ροή των πληροφοριών και διασφαλίζει τη σύνδεσή του με το διαδίκτυο, προστατεύοντας εκ μέρους του οργανισμού:

- τους πόρους του (υλικό, λογισμικό, δεδομένα) από φθορά, κατάχρηση και κλοπή.
- την υπόληψή του από τη δημοσιοποίηση αδυναμιών στην ασφάλεια του δικτύου του.
- την επικρατούσα πολιτική ορθής χρήσης των υπηρεσιών του διαδικτύου από τους εργαζομένους του.

Ο πιο συνηθισμένος πάντως λόγος ύπαρξης ενός συστήματος firewall σε έναν οργανισμό είναι η παροχή ενός μηχανισμού ελέγχου προσπέλασης (access control), πρώτου επιπέδου, για τον Web server. Ένα firewall πρέπει να ελέγχει και να καταγράφει τη ροή των επικοινωνιών που διέρχονται μέσα από το διακομιστή Web. Δηλαδή, πρέπει να παρεμβάλλεται και να αποκόπτει όλη την κίνηση των δεδομένων ανάμεσα στον Web server και το Internet,.

Έτσι, είναι σε θέση να προστατεύει τα δεδομένα που ανεπιθύμητες αλλαγές και να ελέγχει τη πρόσβαση στο διακομιστή Web, αποκλείοντας τους μη εξουσιοδοτημένους χρήστες από ευαίσθητους πόρους του διαδικτύου.

Ακόμη, ένας οργανισμός μπορεί να χρησιμοποιήσει ένα firewall για να απομονώσει τις επικοινωνίες ανάμεσα στα δίκτυα των επιμέρους τμημάτων του. Για παράδειγμα, ένα νοσοκομείο ενδεχομένως να θελήσει να διαχωρίσει το δίκτυο διακίνησης των δεδομένων των ασθενών από το δίκτυο των οικονομικών στοιχείων για να παρέχουν απομόνωση και ελεγχόμενη προσπέλαση ανάμεσα στα διάφορα μέρη ενός οργανισμού.

Ως ένα σύστημα firewall μπορεί να θεωρηθεί μια διάταξη δρομολόγησης (router), ένας προσωπικός υπολογιστής, ένας διακομιστής ή ένα σύνολο από διακομιστές, διαμορφωμένοι με τέτοιο τρόπο ώστε να οχυρώνουν μια δικτυακή τοποθεσία (site) ή ένα υποδίκτυο (subnet) από πρωτόκολλα και υπηρεσίες (π.χ υπηρεσίες e-mail) οι οποίες μπορούν να προσβληθούν από διακομιστές εκτός του υποδικτύου. Η συνηθισμένη θέση του είναι ως πύλη υψηλού επιπέδου ακριβώς στο σημείο σύνδεσης του οργανισμού με το Internet. Όπως έχει ήδη αναφερθεί, μπορεί να τοποθετηθεί και ως πύλη χαμηλότερων επιπέδων πρόσβασης, με σκοπό την προστασία επιμέρους τμημάτων του υποδικτύου.

Η εγκατάσταση επιμέρους προγραμμάτων firewall ως διαχωριστικά των επιμέρους τμημάτων ενός οργανισμού, προσφέρει δυνατότητες διαχωρισμού των εξουσιοδοτήσεων που προσφέρονται στους εσωτερικού χρήστες, λεπτομερέστερη επίβλεψή τους και γενικότερα υποστήριξη υπευθυνότητας με περισσότερη διακριτικότητα. Με άλλα λόγια, παρέχει μέτρα προστασίας από τους νόμιμους και εσωτερικούς χρήστες του δικτύου, που σύμφωνα και με τις περισσότερες έρευνες αποτελεί τον σημαντικότερο κίνδυνο για την ασφάλεια ενός οργανισμού.

Γενικές κατευθύνσεις Πολιτικής Ασφάλειας των Firewalls

Τα κύρια σημεία μιας πολιτικής ασφάλειας μέσω firewalls είναι:

- Ένα firewall να διαμορφώνεται έτσι ώστε να αποτελεί τη μόνη ορατή διεύθυνση διακομιστή προς το έξω δίκτυο, ενώ ταυτόχρονα να απαιτεί όλες οι συνδέσεις προς και από το εσωτερικό δίκτυο να διέρχονται μέσα από αυτό.
- Οι ισχυροί μηχανισμοί πιστοποίησης χρηστών να εφαρμόζονται σε επίπεδο εφαρμογής .
- Οι υπηρεσίες διαμεσολάβησης να παρέχουν λεπτομερείς πληροφορίες καταγραφής σε επίπεδο εφαρμογής.
- Να μην επιτρέπεται η άμεση προσπέλαση στις δικτυακές υπηρεσίες του εσωτερικού δικτύου. Όλες οι αιτήσεις που φτάνουν για υπηρεσίες να διέρχονται μέσω της κατάλληλης

υπηρεσίας διαμεσολάβησης στο firewall, ανεξάρτητα από το ποιος εσωτερικός διακομιστής είναι ο τελικός προορισμός τους.

- Όλες οι νεοεισερχόμενες υπηρεσίες οφείλουν να διεκπεραιώνονται από υπηρεσίες διαμεσολάβησης του firewall. Αν μια νέα υπηρεσία ζητηθεί, αυτή δε θα είναι διαθέσιμη έως ότου διατεθεί το αντίστοιχο λογισμικό υπηρεσίας διαμεσολάβησης και γίνουν οι έλεγχοι από το διαχειριστή ασφάλειας.
- Όλη η διαχείριση του συστήματος firewall να διενεργείται από ένα τοπικό τερματικό. Δεν επιτρέπεται προσπέλαση στο λογισμικό λειτουργίας του firewall, από απομακρυσμένη τοποθεσία. Η φυσική προσπέλαση προς το τερματικό του firewall να επιτρέπεται μόνο στο διαχειριστή του και στον εφεδρικό διαχειριστή.
- Ένας διαχειριστής συστημάτων firewalls οφείλει να έχει πολύ καλή εμπειρία στα δικτυακά ζητήματα ασφάλειας, καθώς και στη σχεδίαση και υλοποίηση firewalls. Έτσι μπορεί να επιτύχει τη σωστή ρύθμιση και εγκατάστασή του, ενώ ακόμη μπορεί να το διαχειρίζεται με ασφαλή τρόπο. Επιπλέον, οι διαχειριστές οφείλουν σε περιοδική φάση, να επιμορφώνονται και να ενημερώνονται πάνω σε πρακτικές ασφάλειας δικτύων και λειτουργίας συγχρόνων διατάξεων firewalls.
- Να δημιουργούνται σε καθημερινή, εβδομαδιαία και μηνιαία βάση ασφαλή (εφεδρικά) αντίγραφα (backups) του λογισμικού και των δεδομένων του συστήματος firewall, δηλαδή του λογισμικού συστήματος, των αρχείων ρυθμίσεων, των αρχείων της βάσης δεδομένων, των αρχείων καταγραφής κ.α, έτσι ώστε σε περίπτωση αποτυχίας του συστήματος (system failure) να υπάρχει η δυνατότητα αποκατάστασης της λειτουργίας του χωρίς σημαντικές απώλειες. Τα εφεδρικά αρχεία να φυλάσσονται με ασφάλεια σε αξιόπιστα μέσα που κατόπιν μπορούν να χρησιμοποιηθούν μόνο για ανάγνωση, για να αποφευχθεί η ακούσια διαγραφή ή καταστροφή τους. μόνο το κατάλληλο προσωπικό να έχει φυσική πρόσβαση σε αυτά.
- Τουλάχιστον ένα ακόμη σύστημα firewall, έτοιμο προς χρήση και με τις σωστές ρυθμίσεις να κρατείται εκτός λειτουργίας ως εφεδρεία.

Πλεονεκτήματα από τη χρήση Firewalls

Ένα firewall σε λειτουργία, δεν είναι μόνο ένα απλό συστατικό του δικτύου, αλλά αποτελεί την υλοποίηση μια στρατηγικής για την προστασία των συνδεδεμένων στο διαδίκτυο πόρων ενός οργανισμού, εξασφαλίζοντας ότι όλες οι επικοινωνίες από και προς το Internet είναι σύμφωνες με την προκαθορισμένη πολιτική ασφάλειας του οργανισμού. Αυτό αποτελεί την

πρώτη και σημαντικότερη ωφέλεια από την χρήση τους. όμως σπουδαίες είναι και οι υπόλοιπες επιμέρους ωφέλειες που παρέχει ένα πρόγραμμα firewall, όπως το ότι:

- Επιτρέπει αποτελεσματικά την επιβολή της πολιτικής ασφάλειας (policy enforcement) που θέλουμε να εφαρμόσουμε στο σύστημά μας. Η διαμόρφωση και η παραμετροποίηση που υποστηρίζει μας βοηθά να ορίσουμε ποιος χρήστης θα έχει πρόσβαση σε ποιο πόρο. Παράλληλα μέσω των διαθέσιμων εργαλείων του για καταγραφή και επίβλεψη, έχουμε μια πλήρη εικόνα των προσπαθειών (επιτυχών και ανεπιτυχών) σύνδεσης η οποία θα χρησιμεύσει στη συντήρηση ή και μετατροπή της πολιτικής ασφάλειας, ειδικότερα για χρήστες με «ύποπτη» συμπεριφορά. Χωρίς firewalls, η εφαρμογή της πολιτικής εξαρτάται από τη διάθεση συνεργασίας των χρηστών, αφού η ασφάλεια ενός δικτύου αντιμετωπίζεται ξεχωριστά από το κάθε τμήμα του. Βέβαια, η ασφάλεια ενός οργανισμού λίγο πολύ εξαρτάται από τους χρήστες του και τη συμμόρφωσή τους στους προβλεπόμενους κανόνες, αλλά με κανένα τρόπο δεν πρέπει να εξαρτάται από τους εξωτερικούς χρήστες του διαδικτύου.
- Προστατεύει από ευπαθείς υπηρεσίες δικτύων. Είναι γνωστό ότι τα πρωτόκολλα επικοινωνίας του διαδικτύου παρουσιάζουν εγγενή προβλήματα ασφάλειας. Η εγκαθίδρυση ενός συστήματος firewall προσφέρει δυνατότητες φιλτραρίσματος που ελαχιστοποιούν τους κινδύνους. Ακόμη, μπορεί και καλύπτει γνωστές ρωγμές ασφαλείας (όπως οι επιθέσεις αδυναμίας εξυπηρέτησης) στο κατώτερο επίπεδο των λειτουργικών συστημάτων. Έτσι, κάποια αδύνατα σημεία για την ασφάλεια του δικτύου, που έχουν ήδη τύχει εκμετάλλευσης από διάφορους εισβολείς, έρχεται να τα προστατέψει η χρήση των firewalls.
- Αποτελεί μέσο καταγραφής (logging) για τη χρήση και συναγερμού (alarming) για την παράνομη χρήση του δικτύου. Οι πληροφορίες που καταγράφονται είναι πολύτιμες λόγω της θέσης του firewall (καθώς είναι το μοναδικό σημείο σύνδεσης με το έξω δίκτυο) και γι' αυτό είναι ακριβείς και αξιόπιστες, καθώς τεκμηριώνουν την ικανότητα ή όχι του ίδιου του firewall για αποτροπή των επιθέσεων που συνέβησαν και κρίνουν την καταλληλότητα της πολιτικής ασφάλειας που εφαρμόζεται. Επιπλέον, τα στατιστικά χρήσης του δικτύου είναι χρήσιμα και στις διαδικασίες ανάλυσης κινδύνων (risk analysis) και ανάλυσης απαιτήσεων δικτύου (network requirement analysis). Ένα firewall μπορεί ακόμη με τις δυνατότητες επεξεργασίας των πληροφοριών αυτών που διαθέτει, να εντοπίσει ύποπτες δραστηριότητες και να αντιδράσει με προαποφασισμένες ενέργειες, όπως το κλείσιμο της σύνδεσης ή η ενημέρωση του διαχειριστή ασφάλεια με e- mail.

- Επιβάλλει *ελεγχόμενη προσπέλαση* (controlled access) στους πόρους ενός εσωτερικού δικτύου. Για παράδειγμα, κάποιοι διακομιστές ενδέχεται να προσφέρονται για επικοινωνία με το Internet, ενώ άλλοι όχι.
- Προσφέρει διευρυμένη ιδιωτικότητα. Για παράδειγμα αποκρύπτει λεπτομέρειες σχετικές με τη διάρθρωση του εσωτερικού δικτύου. Έτσι, οι εξωτερικοί παρατηρητές (intruders) δυσκολεύονται στις ενδεχόμενες προσπάθειές τους να «ξεφύγουν» από τα όρια χρήσης του δικτύου που έχουν καθορισθεί. Γενικότερα, υπάρχουν πάντοτε πληροφορίες που ενώ θεωρούνται αβλαβείς, περιέχουν σημαντικά στοιχεία για έναν επιδέξιο εισβολέα που θέλει να επιχειρήσει επίθεση. Έτσι, μέσω του firewall, πολλοί οργανισμοί σταματούν τις προσπάθειες για κακόβουλες χρήσεις των υπηρεσιών, όπως Finger και DNS (Domain Name Service). Η πρώτη δίνει πληροφορίες σχετικά με τους χρήστες ενός δικτύου, όπως το πότε συνδέθηκαν για τελευταία φορά, αν διάβασαν το ηλεκτρονικό τους ταχυδρομείο κλπ, οι οποίες παρέχουν πληροφορίες στους εισβολείς σχετικά με το πόσο συχνά ένα σύστημα χρησιμοποιείται ή αν εκείνη τη στιγμή υπάρχουν συνδεδεμένοι ενεργοί χρήστες. Η υπηρεσία DNS από την άλλη, παρέχει πληροφορίες για τις δικτυακές τοποθεσίες του συστήματος, όπως τα ονόματα των τόπων και τις δικτυακές τοποθεσίες του συστήματος, όπως τα ονόματα των τόπων και οι IP διευθύνσεις του. Η μη δημοσιοποίησή τους στο διαδίκτυο, αφαιρεί σίγουρα χρήσιμα στοιχεία από όσους τα επιβουλεύονται.
- Συγκεντρώνει υπηρεσίες ασφάλειας σε μια καλά ορισμένη και οχυρωμένη περιοχή. Ελαχιστοποιεί τη ζώνη κινδύνου (zone risk) ενός οργανισμού εφόσον μια ευρεία περιοχή των μηχανημάτων του παύει να απειλείται άμεσα. Ουσιαστικά, το ίδιο το firewall αποτελεί τη μοναδική ζώνη κινδύνου για τον οργανισμό. Άμεση συνέπεια του γεγονότος αυτού, είναι ευκολία διαχείρισης ασφάλειας και γενικότερα μια οικονομία κλίμακας αφού δεν απαιτούνται επεμβάσεις σε όλους τους διακομιστές κάθε φορά που γίνονται ρυθμίσεις λόγω αλλαγών στο λογισμικό των εφαρμογών ή της ασφάλειας. Η ενημέρωση-συντήρηση αφορά κυρίως το σύστημα firewall. Για παράδειγμα, η εγκατάσταση πρόσθετου λογισμικού πιστοποίησης (όπως τα συστήματα συνθηματικών μιας χρήσης) δε χρειάζεται να γίνει σε κάθε διακομιστή ξεχωριστά, αλλά να γίνει μια φορά στο firewall.
- Αρκετά σύγχρονα συστήματα firewall προσφέρουν ως επιπλέον υπηρεσία τη λειτουργία τους ως πύλες κρυπτογράφησης. Δηλαδή, παρέχουν ταυτόχρονα δυνατότητες κρυπτογράφησης των επικοινωνιών μεταξύ των διακομιστών που προστατεύουν. Ακόμη και εξωτερικά συστήματα μπορούν να συνομιλήσουν σε κρυπτογραφημένη μορφή, αρκεί να εγκαταστήσουν το ανάλογο λογισμικό πελάτη και να παρουσιάσουν τα σχετικά διαπιστευτήρια που προέρχονται από το διαχειριστή του firewall. Ένας τέτοιος λογικός

διαχωρισμός των δικτύων μέσω firewalls και τεχνικών κρυπτογράφησης δημιουργεί τα λεγόμενα *εικονικά ιδιωτικά δίκτυα* (Virtual Private Networks – VPN). Η κρυπτογράφηση μπορεί να είναι επιλεκτική, ανάλογα με την απαιτούμενη από το διαδίκτυο υπηρεσία και η διαχείρισή της να είναι ενσωματωμένη με τα υπόλοιπα χαρακτηριστικά του firewall, έτσι ώστε να είναι δυνατή η εκμετάλλευση όλων των βοηθημάτων που υποστηρίζονται για την κατασκευή των κανόνων ελέγχου προσπέλασης, η καταγραφή-παρακολούθηση των ενεργειών κλπ.

Περιορισμοί των firewalls

Τα συστήματα firewalls δεν αποτελούν πανάκεια για τα προβλήματα ασφάλειας στο διαδίκτυο. Υπάρχουν κίνδυνοι που ξεφεύγουν από τις δυνατότητές τους:

- Δεν προστατεύουν από τους εσωτερικούς χρήστες (πχ από τους υπαλλήλους του οργανισμού). Εφόσον ένα εσωτερικό μηχάνημα μπορεί να επικοινωνήσει με ένα άλλο, κάνοντας χρήση πρωτοκόλλου Internet, χωρίς να «περάσει» μέσα από το firewall, οποιαδήποτε ζημιά μπορεί να προκληθεί χωρίς να γίνει αντιληπτό από αυτό. Απαιτούνται επιπλέον μηχανισμοί πιστοποίησης και ελέγχου προσπέλασης για τους χρήστες και τις δραστηριότητες των συστημάτων τους. τα intranet firewalls ελαχιστοποιούν ανάλογους κινδύνους, παρακολουθώντας την κυκλοφορία ανάμεσα στα διάφορα τμήματα ενός οργανισμού.
- Μπορούν να προστατεύσουν ένα περιβάλλον, μόνον όταν ελέγχουν πλήρως την περίμετρό του. Δηλαδή, δεν πρέπει να υπάρχουν συνδέσεις (πχ μέσω modem) που να μην διοχετεύονται μέσω του firewall. Στην περίπτωση που έστω και ένας εσωτερικός διακομιστής μπορέσει να αποκτήσει τέτοια εξωτερική σύνδεση, ολόκληρο το εσωτερικό δίκτυο τίθεται σε κίνδυνο.
- Δεν είναι εντελώς άτρωτα, μπορούν να διαπεραστούν. Οι κατασκευαστές των συστημάτων firewalls τα κρατούν μικρά και απλά έτσι ώστε ο πιθανός εισβολέας να μην αποκτήσει στη συνέχεια τον έλεγχο επικίνδυνων εργαλείων όπως τα προγράμματα μεταγλώττισης, τα προγράμματα σύνδεσης κλπ. Όμως, σε καμιά περίπτωση δεν πρέπει να θεωρείται ότι είναι ικανά μόνα τους να εξασφαλίσουν την απόκρουση όλων των εξωτερικών επιθέσεων. Πρέπει να θεωρούνται απλώς σαν μια ισχυρή πρώτη γραμμή άμυνας.
- Αποτελούν για ένα οργανισμό, το πιο ορατό σημείο του προς τον έξω κόσμο. Έτσι μοιραία είναι και ο πιο ελκυστικός στόχος επίθεσης. Απαραίτητη επομένως είναι η οργάνωση άμυνας εις βάθος, με επιπλέον επίπεδα προστασίας.

- Διαθέτουν από περιορισμένο έως ελάχιστο έλεγχο πάνω στο περιεχόμενο των εισερχόμενων μηνυμάτων. Έτσι, σε επιθέσεις όπως αυτές των ιών και παρόμοιου επικίνδυνου κώδικα, χρειάζονται επιπλέον μέτρα προστασίας.
- Απαιτούν σωστή εγκατάσταση, προσεκτικές ρυθμίσεις και συνεχείς ενημερώσεις στη διαμόρφωσή τους ανάλογα με τις αλλαγές που παρουσιάζουν το εσωτερικό δίκτυο και οι συνδέσεις του με τον έξω κόσμο. Ακόμη, πρέπει να μελετώνται οι εγγραφές των αρχείων καταγραφής για τον έλεγχο απόδοσής τους και τον εντοπισμό πιθανών δυσλειτουργιών τους. αλλιώς, δημιουργείται μια εσφαλμένη αίσθηση ασφάλειας με αποτέλεσμα μια σχετικά εύκολη διείσδυση να αφήνει απροστάτευτους τους θεωρούμενους ασφαλείς εσωτερικούς πόρους.

Αποδεκτή λειτουργικότητα συστημάτων Firewalls

Ένα σύστημα firewall θα πρέπει να ικανοποιεί τις ακόλουθες προϋποθέσεις:

- Να απορρίπτει κάθε πακέτο που ρητά κάποιος κανόνας δεν επιτρέπει να περάσει. Αυτή είναι η εξ ορισμού (by default) ρύθμιση για τα περισσότερα firewalls και επιβάλλει στο διαχειριστή τους να διευκρινίσει ποιες ακριβώς επικοινωνίες είναι αποδεκτές.
- Να κρατά τους εξωτερικούς χρήστες έξω από το προστατευμένο δίκτυο. Αν για παράδειγμα, πρέπει κάποια αρχεία να γίνουν προσιτά μέσω του διαδικτύου, τότε το πιο σίγουρο είναι αυτά να τοποθετηθούν έξω από το firewall. Εναλλακτικά, απαιτούνται ισχυροί μηχανισμοί αυθεντικοποίησης σε επίπεδο εφαρμογών για την παρεμπόδιση των μη εξουσιοδοτημένων χρηστών.
- Να διαθέτει προηγμένα εργαλεία καταγραφής, επίβλεψης και πρόκλησης συναγερμού, ικανά να αναλύοντας πραγματοποιημένες συναλλαγές με σκοπό την εξαγωγή συμπερασμάτων σχετικά με το είδος και τη φύση των επιθέσεων και τη συνακόλουθη προσαρμογή της υφιστάμενης πολιτικής ασφάλειας.

Συνοπτικά ένα firewall πρέπει να είναι ικανό να προσφέρει υπηρεσίες ασφάλειας ελέγχου προσπέλασης (access control), συνδυάζοντας μηχανισμούς αυθεντικοποίησης (authentication), εξουσιοδότησης (authorization), επίβλεψης (auditing) και όπου είναι δυνατόν κρυπτογράφησης (encryption).

Ανάλογα με τα συστατικά που περιλαμβάνει ένα σύστημα firewall, παρέχει και διαφορετική βαθμίδα ασφάλειας. Ουσιαστικά πρόκειται για μια σχέση αντιστρόφως ανάλογη ανάμεσα στην παρεχόμενη ελευθερία σύνδεσης και στην ασφάλεια. Πλήρης ελευθερία σύνδεσης σημαίνει καθόλου ασφάλεια, ενώ αντίθετα πλήρης ασφάλεια σημαίνει καθόλου

ελευθερία σύνδεσης. Οι ενδιάμεσες βαθμίδες στη συνδεσιμότητα εξαρτώνται από τις υπηρεσίες και το βάθος ασφάλειας που υποστηρίζονται.

Η διαβάθμιση της παρεχόμενης ασφάλειας από ένα firewall εξαρτάται επιπλέον από το εάν αυτό παρέχει εμπιστευτικότητα και ακεραιότητα μέσω μηχανισμών κρυπτογράφησης. Η παρεχόμενη ασφάλεια καλείται Internet Layer Security γιατί η κρυπτογράφηση γίνεται μέσα στο χαμηλό IP κανάλι επικοινωνίας (IP layer). Υποστηρίζει εμπιστευτικότητα και ακεραιότητα από οικοδεσπότη σε οικοδεσπότη (host-to-host). Η δυνατότητα αυτή διακίνησης κρυπτογραφημένων δεδομένων μέσα στο πρωτόκολλο IP, καλείται και *ασφαλές πρωτόκολλο IP* (secure IP).

Ενημέρωση για Θέματα Ασφαλείας και Εκπαίδευση

Δεδομένου ότι μια από τις σημαντικότερες αδυναμίες των συστημάτων είναι ο ανθρώπινος παράγοντας, ο αμυντικός πληροφοριακός πόλεμος διαθέτει επίσης στο οπλοστάσιό του και το όπλο της εκπαίδευσης. Προγράμματα που ενημερώνουν για θέματα ασφαλείας και ανάλογη εκπαίδευση μπορούν να χρησιμεύσουν στην πληροφόρηση των υπαλλήλων ενός οργανισμού για την πολιτική ασφαλείας που αυτός ακολουθεί, να τους ευαισθητοποιήσουν για τους κινδύνους και τις πιθανές ζημιές και να τους εκπαιδεύσουν στην χρήση πρακτικών και τεχνολογιών ασφαλείας. Τα προγράμματα αυτά μπορούν να παρέχουν εκπαίδευση στους τομείς της ασφάλειας των εγκαταστάσεων και του προσωπικού, όπως επίσης και του κυβερνοχώρου.

Οι υπάλληλοι θα πρέπει να ενημερώνονται για τις τακτικές της κοινωνικής χειραγώγησης και για το πώς θα τις ανακαλύπτουν και θα τις αποφεύγουν. Οι διαχειριστές συστημάτων θα πρέπει να εκπαιδεύονται σε θέματα ασφάλειας πληροφοριών έτσι, ώστε να μπορούν να διαμορφώνουν κατάλληλα και να παρακολουθούν τα συστήματά τους. Αυτοί και τα άλλα μέλη του προσωπικού, θα πρέπει να διδάσκονται τις αρμοδιότητές τους που αφορούν τις πρακτικές και τα περιστατικά που έχουν σχέση με την ασφάλεια των πληροφοριών.

Η εκπαίδευση και η κατάρτιση επεκτείνονται στους καταναλωτές, οι οποίοι είναι ευάλωτοι στην κλοπή ταυτότητας, στη λήψη ενοχλητικών διαφημίσεων καθώς και σε άλλα είδη επιχειρήσεων επιθετικού πληροφοριακού πολέμου.

Αντιμετώπιση των Περιστατικών

Εάν συμβεί ένα περιστατικό πληροφοριακού πολέμου, η οντότητα που δέχθηκε την επίθεση μπορεί να απαντήσει σ' αυτή με αρκετούς τρόπους. Στη συνέχεια, θα γίνει παρουσίαση ορισμένων από αυτούς, χωρίς αυτό να σημαίνει ότι είναι και οι μοναδικοί.

Διερεύνηση και Εκτίμηση: το πρώτο βήμα που θα πρέπει να γίνει θα πρέπει να είναι μια εσωτερική διερεύνηση του περιστατικού, προκειμένου να ανακαλυφθεί ο δράστης καθώς και η προέλευση και η έκταση της επίθεσης. Η φύση του περιστατικού θα μπορούσε να διερευνηθεί με βάση τις αδυναμίες εκμετάλλευση των οποίων έγινε, τις μεθόδους που χρησιμοποιήθηκαν, τις ζημιές που προκλήθηκαν και τις δυνατότητες αντιμετώπισης. Όλα αυτά θα ήταν δυνατό να γίνουν είτε μετά το τέλος της επίθεσης ή ενώ αυτή βρίσκεται σε εξέλιξη. Στρατηγικές επίσης για παραπέρα ενέργειες, θα μπορούσαν να διαμορφωθούν και να προσδιοριστούν.

Περιορισμός και Ανάκαμψη: για να μετριαστεί η επίδραση μιας επίθεσης, θα πρέπει να ληφθούν μέτρα για τον περιορισμό της και για την επιδιόρθωση των ζημιών που προξένησε. Όπου αυτό είναι εφικτό, επιθέσεις που βρίσκονται σε εξέλιξη θα πρέπει να επιδιωχθεί να σταματήσουν αμέσως για να αποφευχθούν παραπέρα ζημιές.

Εάν έχει γίνει εισβολή σε ένα υπολογιστή, θα πρέπει να διακοπεί η σύνδεσή του με το δίκτυο, να απενεργοποιηθούν οι λογαριασμοί και να κλείσουν και οι υπόλοιποι υπολογιστές του δικτύου. Προσβεβλημένα ή διαγραμμένα αρχεία θα μπορέσουν να ανακληθούν από τα εφεδρικά τους αντίγραφα. Εάν το σύνολο των εγκαταστάσεων των υπολογιστών έχει καταστεί μη λειτουργικό, οι διαδικασίες επεξεργασίας των πληροφοριών θα πρέπει να γίνονται αλλού.

Εάν το σχετικό περιστατικό αποδίδεται σε κάποιο υπάλληλο, ο υπάλληλος αυτός θα πρέπει να απολυθεί ή να τεθεί σε διαθεσιμότητα κατά τη διάρκεια της διερεύνησής του. Σε υποθέσεις υπολογιστών, οι λογαριασμοί του ύποπτου υπαλλήλου θα πρέπει να απενεργοποιούνται, ειδικά αν υπάρχει περίπτωση αντεκδίκησης από την πλευρά του.

Εάν ένα περιστατικό έχει δημιουργήσει αρνητική δημοσιότητα ή αποτέλεσε το ίδιο μια πράξη διαμόρφωσης απόψεων, θα πρέπει να βγει ένα δελτίο τύπου, που να δίνει απαντήσεις στις φήμες και στην κριτική που ασκείται. Το δελτίο τύπου θα πρέπει να διορθώνει κάθε είδος παραπληροφόρησης.

Βελτιώνοντας την Ασφάλεια: όπου είναι εφικτό και οικονομικά πρακτικό, οι αδυναμίες εκμετάλλευση των οποίων γίνεται από ένα κακοποιό μπορεί να εξαλειφθούν ή να ελαχιστοποιηθούν. Η φυσική ασφάλεια μπορεί να επεκταθεί, για παράδειγμα, με την αύξηση

του αριθμού των φρουρών ή με καλύτερες κλειδαριές. Στους υπαλλήλους θα πρέπει να παραδίδονται μαθήματα για το πώς θα φυλάξουν καλύτερα τις πληροφορίες και δε θα αποτελούν τη λεία κακοπροαίρετων ατόμων.

Μετά από περιστατικά που αφορούν υπολογιστές, τα συστήματα θα πρέπει να επαναδιαμορφώνονται για να αποτρέψουν ανάλογες μελλοντικές επιθέσεις. Οι τρύπες στην ασφάλεια θα πρέπει να επιδιορθώνονται, εφόσον υπάρχουν διορθωτικά ή νέα προγράμματα και θα πρέπει να εγκαθίστανται και νέα προγράμματα ασφαλείας.

Γνωστοποίηση: εάν ο δράστης μιας επίθεσης μπορεί να αναγνωριστεί ή τουλάχιστον να γίνει κάποια επαφή μαζί του, το πρόσωπο αυτό θα πρέπει να γίνει ευρύτερα γνωστό και θα πρέπει να του ζητηθεί να σταματήσει τις πράξεις του. Το πρόσωπο αυτό θα πρέπει να απειληθεί με την άσκηση ποινικής δίωξης σε βάρος του ή με την υποβολή αγωγής αποζημίωσης, εφόσον δε σταματήσει αμέσως την επίθεσή και δεν επιδιορθώσει τις ζημιές που προξένησε. Για παράδειγμα, αναφέρουμε πως από κάποιον που έστειλε υβριστικό υλικό θα πρέπει να του ζητηθεί να το ανακαλέσει και να ζητήσει συγνώμη γι' αυτό. Σ' 'έναν πειρατή λογισμικού θα πρέπει να του σημειωθεί ότι θα πρέπει να πληρώσει την πραγματική αξία του προγράμματος διαφορετικά θα διωχθεί ποινικά. Σε έναν hacker θα πρέπει να γίνει σύσταση να αποσυρθεί και οι άλλες οντότητες που έχουν προσβληθεί από την εισβολή του, όπως τόποι του Διαδικτύου, θα πρέπει να ενημερωθούν.

Νόμιμες και Αστικές Επανορθώσεις: εάν μια επίθεση είναι παράνομη, το σχετικό περιστατικό μπορεί να αναφερθεί σα μία υπηρεσία επιβολής του νόμου, με την πιθανή απαίτηση της διενέργειας ανάκρισης και την άσκηση ποινικής δίωξης. Οι αξιωματικοί της υπηρεσίας αυτής με τη σειρά τους, μπορεί να χρησιμοποιήσουν μεθόδους επιθετικού πληροφοριακού πολέμου.

Πολλά περιστατικά δεν αναφέρονται ποτέ στις υπηρεσίες επιβολής του νόμου. Υπάρχουν αρκετοί λόγοι γι' αυτό. Μια εταιρεία θα πρέπει να ενδιαφέρεται για την αρνητική δημοσιότητα, η οποία μπορεί να έχει σαν αποτέλεσμα την απώλεια της εμπορικής της πίστης ή τη μείωση της αξίας των μετοχών της. Θα πρέπει, έτσι, να αποφασίσει για το αν αξίζει ο χρόνος και τα έξοδα που είναι υποχρεωμένη να κάνει για να υποστηρίξει την ανάκριση και την ποινική δίωξη για το εις βάρος της περιστατικό. Θα μπορούσε βέβαια να επιλέξει να ακολουθήσει την αστική διαδικασία για την αποζημίωσή της ή, εάν ο δράστης είναι υπάλληλός της, να πάρει πειθαρχικά μέτρα εναντίον του που μπορούν να φτάσουν μέχρι και την απόλυσή του.

Οι υπηρεσίες επιβολής του νόμου, αντιμετωπίζουν πολλές προκλήσεις όσον αφορά την απάντηση που θα πρέπει να δώσουν στις επιθέσεις του επιθετικού πληροφοριακού πολέμου, και ιδιαίτερα σε εκείνες από αυτές που ξεπερνούν τα εθνικά και τοπικά όρια και οι οποίες εκμεταλλεύονται τις δυνατότητες των σημερινών τεχνολογιών. Μπορεί να είναι δύσκολος ο εντοπισμός ενός hacker, ο οποίος έχει περάσει από πολλά συστήματα, χρησιμοποίησε ανώνυμες υπηρεσίες ή μπήκε στο σύστημα μέσω μιας ασύρματης σύνδεσης από μια κινητή μονάδα. Μια άλλη πρόκληση είναι η συλλογή και διατήρηση των αποδεικτικών στοιχείων. Αυτά μπορεί να είναι κρυπτογραφημένα ή να βρίσκονται διασκορπισμένα σε διάφορες χώρες. Η καταγραφή ενός εισβολέα και η συγκέντρωση αποδεικτικών στοιχείων, ίσως απαιτεί έρευνες και συλλήψεις ή τηλεφωνικές υποκλοπές κάτω από διαφορετικές νομοθεσίες. Μια Τρίτη πρόκληση, είναι ότι οι νόμοι δεν είναι ίδιοι σε όλες τις χώρες. Ορισμένες από αυτές έχουν ελαστικούς νόμους ή δεν κάνουν καμιά νομοθετική πρόβλεψη εναντίον των δραστηριοτήτων των hackers. Ακόμα και αν υπάρχουν οι σχετικοί νόμοι, η έκδοση ενός υπόδικου μπορεί να απαγορεύεται, κάτι που εξαρτάται από τις διακρατικές συμφωνίες.

Δ΄ Μέρος

Έρευνα CSI/FBI

Ανάλυση S.W.O.T* της χρήσης του Internet από τις επιχειρήσεις

«Το Internet είναι για την επερχόμενη οικονομική έκρηξη, της Βρυχώμενης Δεκαετίας του 2000, ότι ήταν η γραμμή παραγωγής κατά τη Βρυχώμενη Δεκαετία του '20. Είναι το κλειδί της μοχλοποίησης της παραγωγικότητας που θα προσδώσει νέες τεχνολογικές εφαρμογές, προϊόντα και υπηρεσίες στη δεσπόζουσα τάση της οικονομίας». (Harry S. Ned – The Roaring 2000s).

Η χρήση του Internet έχει παρουσιάσει παγκοσμίως σημαντική άνοδο από τη στιγμή της εμφάνισής του. Έρευνες δείχνουν πως μόνο ένα 10% του αμερικανικού πληθυσμού είχε πρόσβαση στο Internet το 1994. Πέντε χρόνια μετά, το 28% των σπιτιών είχε πρόσβαση στο Internet και η κίνησή του διπλασιάζεται κάθε 100 μέρες. Το δημόσιο περιεχόμενο πληροφορίας του WWW υπολογίζεται πρόχειρα σε 15 terabytes. Ως συνέπεια το 2003 περισσότερο από το 50 % είχε πρόσβαση στο Internet.

Οι πωλήσεις των υπολογιστών και η κίνηση στο Internet θα ωθήσουν το ένα την ανάπτυξη του άλλου. Ο Ned προέβλεψε ότι μέχρι το 2006, το 90% των σπιτιών στη Β.Αμερική θα έχει ηλεκτρονικό υπολογιστή. Καθώς η δημοτικότητα του Internet αυξάνεται και οι τιμές των υπηρεσιών του μειώνονται, είναι βέβαιο ότι η χρήση του θα αυξηθεί παράλληλα με τους ηλεκτρονικούς υπολογιστές.

Το 1999, η Ελλάδα είχε ποσοστά διείσδυσης Η/Υ και Internet 11% και 6% αντίστοιχα, ενώ οι αντίστοιχοι μέσοι όροι στις χώρες της Ε.Ε ήταν 34% και 20%. Το ποσοστό των χρηστών Η/Υ που έκανε και χρήση Internet στην Ε.Ε ήταν 56% το 1999. (Πηγή: Information Society Indicators in the Middle States of the European Union, an ESIS report, ISPO). Το 2000 ο μέσος όρος διείσδυσης Internet στην Ε.Ε ήταν 25,7% και τον Ιούνιο του 2001 έφτασε το 34,3%. Μέχρι το τέλος του παρόντος έτους η διείσδυση του Internet στην Ε.Ε προβλέπεται ότι θα φτάσει το 66%, δηλαδή τα 2/3 του πληθυσμού θα έχουν σύνδεση στο Internet.

Παρακάτω παρατίθεται μια μέθοδος εκτίμησης της ανταγωνιστικής θέσης-χρήσης του Internet.

* S.W.O.T = Strengths/Weaknesses/Opportunities/Threats

Στη γλώσσα μας ο όρος μεταφράζεται ως Δ.Α.Ε.Α = Δυνάμεις/Αδυναμίες/Ευκαιρίες/Απειλές.

Απειλές	**Ευκαιρίες**
➢ Ανταγωνιστές ➢ Νομικά θέματα που αφορούν το λογισμικό και τα δικαιώματα πνευματικής ιδιοκτησίας ➢ Ασφάλεια στο Internet ➢ Ιοί ➢ Hacking (παράνομη πρόσβαση)	➢ Αύξηση των χρηστών ➢ Τεχνολογική πρόοδος και νέες εφαρμογές ➢ Εμφάνιση νέων αγορών ➢ Ανάπτυξη νέας αγοράς ➢ Πρόσφατη αναδιοργάνωση επιχειρήσεων που δραστηριοποιούνται στο Διαδίκτυο
Δυνάμεις	**Αδυναμίες**
➢ Ικανότητα να προσελκύει αγοραστές και αντίστροφα ➢ Όγκος των συναλλαγών και ικανότητα επιλογής των αγαθών ➢ Κοινοτική συνοχή και αλληλεπίδραση των συναλλαγών ➢ Αξιοπιστία συστήματος ➢ Εξυπηρέτηση καταναλωτών ➢ Αξιοπιστία παράδοσης και πληρωμής από τους χρήστες ➢ Αναγνώριση φίρμας ➢ Ευκολία στη χρήση του δικτύου και γρήγορη πρόσβαση ➢ Εξυπηρέτηση πληρωμών ➢ Ποιότητα μηχανών αναζήτησης ➢ Περιττοί οι αποθηκευτικοί χώροι ➢ On-line κοινότητες	➢ Θέματα που σχετίζονται με την προσφορά ή ζήτηση παράνομων προϊόντων ➢ Κυβερνητικές έρευνες που αφορούν πιθανές παραβάσεις δικτύου ➢ Ιδιωτική πολιτική ➢ Νέοι και υπάρχοντες κανονισμοί Internet

Αρνητικές συνέπειες του Internet στις επιχειρήσεις

Θα ήταν ίσως περισσότερο ενδιαφέρον να αναφερθούμε στις αρνητικές συνέπειες του Internet στις επιχειρήσεις, αφού μιλάμε για ασφάλεια και διότι ο καθένας μας αντιλαμβάνεται σε γενικές γραμμές τα πλεονεκτήματά του.

Όπως όλα τα διαφημιστικά μέσα που υπάρχουν στη σημερινή εποχή όπως ΜΜΕ, αφίσες, κινηματογράφος, τα διαφημιστικά φυλλάδια κλπ, έτσι και το Internet έχει τα τρωτά του σημεία έναντι στα υπόλοιπα μέσα. Αυτά είναι τα εξής:

1) σε αντίθεση με τα διαφημιστικά φυλλάδια, αφίσες πινακίδες που τις συναντάμε καθημερινά, για να δει κάποιος μια διαφήμιση στο Internet πρέπει να βρεθεί μπροστά σε έναν Η/Υ.

2) έστω μια εταιρεία Χ έχει ένα site που διαφημίζει τα προϊόντα της. Στο site αυτό θα μπουν οι χρήστες που ενδιαφέρονται για τα προϊόντα αυτά, ωστόσο θα πρέπει να γνωρίζουν τη διεύθυνση για να μπουν στο συγκεκριμένο site. Το πρόβλημα αυτό που αποτελούσε πρόβλημα για τη διαφήμιση στο Internet, λύθηκε με τα Cyberads (διαφημιστικές καταχωρήσεις). Με λίγα λόγια, εννοούμε την ενοικίαση χώρου στην εισαγωγική σελίδα ενός πολυσύχναστου Website και η παράθεση σε κάποιο ευδιάκριτο σημείο της σελίδας μιας εμβόλιμης καταχώρησης με τη μορφή κάποιας εικόνας. Φυσικά η γραφική αυτή εικόνα είναι ένα hyperlink που οδηγεί σε αναλυτικές σελίδες της διαφημιζόμενης εταιρείας.

3) το μεγαλύτερο ίσως μειονέκτημα είναι η χρησιμοποίηση του Internet κυρίως από μεγάλες επιχειρήσεις και όχι από τις μικρομεσαίες, το οποίο χρησιμοποιείται τόσο για την προβολή τους όσο και για την ανάπτυξη του ηλεκτρονικού εμπορίου. Αυτό οφείλεται κυρίως στη μη καλή ενημέρωση των μικρομεσαίων επιχειρηματιών, γύρω από τις εξελίξεις και τα νέα δεδομένα της κοινωνίας των πληροφοριών και την έγκαιρη δραστηριοποίησή τους.

Ένας άλλος λόγος είναι η εξασφάλιση μεγαλύτερης πρόσβασης σε φθηνότερου κόστους υποδομές για το Internet (ιδιαίτερα στην Ελλάδα αφού η υποδομή και η πρόσβαση σ' αυτή κοστολογούνται ακριβότερα απ' ότι σε ολόκληρη την Ευρώπη).

Πώς το Διαδίκτυο αλλάζει τον ανταγωνισμό

Εγείρονται πολλά ερωτήματα για το επιχειρείν στο Διαδίκτυο. Όσοι δραστηριοποιούνται στο χώρο, αλλά και όχι μόνο, αναρωτιούνται για τις διαστάσεις που αυτό θα πάρει. Αλλά από τη σκοπιά του μάνατζερ υπάρχει ένα ουσιώδες επίμαχο θέμα: εάν και κατά πόσο μια οποιαδήποτε επιχείρηση είναι ικανή να σταθεί και να ανταγωνιστεί σε αυτή την κατά πολλούς άναρχα δομημένη αγορά. Αυτό το ερώτημα αναδεικνύει ζητήματα στρατηγικής και οργανωτικής ευελιξίας που πολλές εταιρείες καλούνται και οφείλουν να αντιμετωπίσουν πλέον. Ο ανταγωνισμός της αγοράς, θεμιτός ή αθέμιτος, κρυφός ή φανερός, υπάρχει και στον τομές του

Διαδικτύου κάτω από ορισμένες συνθήκες το Διαδίκτυο μπορεί να μετατραπεί από επιχειρηματική ευκαιρία σε επιχειρηματική απειλή, γι' αυτό πρέπει να υπάρχει διερεύνηση όχι μόνο στο χώρο των παραδοσιακών ανταγωνισμών, αλλά και πέρα από αυτούς.

Το Διαδίκτυο έχει αλλάξει τους ρυθμούς του ανταγωνισμού. Από αγορά σε αγορά, οι τιμές πέφτουν και τα επιχειρηματικά μοντέλα αλλάζουν με γοργούς ρυθμούς. Σιγά σιγά το Διαδίκτυο αλλάζει και την ίδια τη δομή του ανταγωνισμού. Ο «Παγκόσμιος Ιστός», διαφοροποιεί τον τρόπο με τον οποίο οι εταιρείες προσδιορίζουν τους ανταγωνιστές τους. Παραδοσιακά οι εταιρείες ανταγωνίζονταν κυρίως τις υπόλοιπες εταιρείες του κλάδου τους μόνο, και κάθε κλάδος ήταν απόλυτα διαχωρισμένος από τους άλλους. Το Διαδίκτυο όμως έχει μπερδέψει τα «όρια» των αγορών, με αποτέλεσμα μια αγορά να εισέρχεται εύκολα σε μια άλλη. Μπορεί κανείς, χωρίς να το αντιλαμβάνεται και χωρίς τη παραμικρή δυσκολία, να αλλάξει αγορά και ξαφνικά να βρίσκεται αντιμέτωπος με άλλες αγορές, δημιουργώντας ασυναίσθητα έτσι ανταγωνισμό μεταξύ τους.

Για παράδειγμα, ένας πιστωτικός οργανισμός μπορεί να βρει μπροστά του μια εταιρεία πληροφορικής ή ακόμα και μια εταιρεία παραδόσεων σαν πιθανούς ανταγωνιστές. Αυτό συμβαίνει σήμερα και στην Αμερική, αλλά και στην Ευρώπη. Ένα χαρακτηριστικό παράδειγμα αποτελεί το Amazon.com, το μεγαλύτερο on-line βιβλιοπωλείο. Το Amazon σίγουρα συναγωνίζεται την Barns and Noble, το μεγαλύτερο παραδοσιακό βιβλιοπωλείο. Πολλοί όμως από τον χώρο των ηλεκτρονικών υπολογιστών πιστεύουν ότι το Yahoo (κέντρο πληροφοριών και προσφοράς προϊόντων του Διαδικτύου) σύντομα θα είναι ο μεγάλος ανταγωνιστής του Amazon.

Και οι δύο είναι αξιόπιστες πηγές που χρησιμοποιούν οι αναγνώστες-καταναλωτές για να αποφασίσουν ποιο βιβλίο θα αγοράσουν. Κάποιοι πιστεύουν ότι το Amazon εξελίσσεται σε εταιρεία διεξαγωγής χρηματικών συναλλαγών, που κάποια στιγμή θα ανταγωνίζεται χρηματοοικονομικούς οργανισμούς και τράπεζες.

Καθώς το Internet επιτρέπει σε κάθε επιχείρηση να ιδιοποιείται εμπορικές και οικονομικές δραστηριότητες, νέες και μικρές επιχειρήσεις με υψηλό βαθμό τεχνογνωσίας μπορούν να κατακτήσουν μεγάλο μερίδιο αγοράς σε βάρος παλαιών επιχειρήσεων ή ακόμη και καθιερωμένων προϊόντων. Αν παρ' όλ' αυτά κάποιος επιχειρηματολογήσει και ισχυριστεί ότι η επιχείρησή του δε χρειάζεται να σπαταλά το χρόνο της με το Διαδίκτυο και ως εκ τούτου δεν είναι αναγκαία η δημιουργίας ενός εταιρικού Web site, εκ των πραγμάτων θα διαψευστεί.

Οι επιχειρήσεις απέναντι στο ηλεκτρονικό εμπόριο

Εξετάζοντας διεξοδικά την παρουσία των εταιρειών στο Διαδίκτυο, σε μια προσπάθεια κατηγοριοποίησης των εφαρμογών αυτών που απευθύνονται κυρίως στον καταναλωτή, μπορούμε να διακρίνουμε τρεις βασικές κατηγορίες επιχειρηματικής δραστηριότητας στο Internet:

➢ *Παρουσίαση-διαφήμιση προϊόντων και υπηρεσιών.* Στην κατηγορία αυτή ανήκουν επιχειρήσεις που χρησιμοποιούν το Internet, ως ένα εναλλακτικό μέσο διαφήμισης και προβολής της επιχείρησης. Για να χαρακτηριστεί ότι μια επιχείρηση εκμεταλλεύεται το Internet ως μέσο διαφήμισης και προβολής, θα πρέπει να έχει τα εξής χαρακτηριστικά: α) με τη χρήση πολυμέσων να δώσει έμφαση στην εμφάνιση και ποιοτική παρουσίασή της, β) να παρέχει στην ιστοσελίδα της πληροφορίες για την εταιρεία, γ) να δημοσιεύει ειδήσεις/πληροφορίες που αφορούν την επιχείρηση καθώς και τον κλάδο της, δ) να επικοινωνούν οι πελάτες με την εταιρεία κυρίως μέσω ηλεκτρονικού ταχυδρομείου και τέλος ε) να υπάρχει δυνατότητα σύνδεσης με άλλους κόμβους.

➢ *Παροχή πληροφοριών και υπηρεσιών.* Η κατηγορία αυτή περιλαμβάνει επιχειρήσεις που χρησιμοποιούν το Internet, για την παροχή πληροφοριών και υπηρεσιών στους χρήστες. Εδώ ανήκουν επιχειρήσεις όπως δημοσιογραφικοί οργανισμοί, επιχειρήσεις που παρέχουν συμβουλές σε νομικά, λογιστικά, ιατρικά κλπ θέματα, τουριστικοί οργανισμοί κοκ. Αυτό βέβαια μπορούν να το επιτύχουν με τη χρησιμοποίηση εξελιγμένων μηχανών αναζήτησης πληροφοριών, κατηγοριοποιώντας τις πληροφορίες καθώς και προσφέροντας στους χρήστες τη δυνατότητα εγγραφής σε μία υπηρεσία παροχής πληροφοριών ώστε να έχουν πρόσβαση σε μεγαλύτερο όγκο πληροφοριών ή να απολαμβάνουν υπηρεσίες προστιθέμενης αξίας.

➢ *Εμπορικές συναλλαγές.* Οι εφαρμογές αυτές αφορούν στην πώληση προϊόντων και υπηρεσιών. Αντιπροσωπευτικό παράδειγμα, αποτελούν τα ηλεκτρονικά καταστήματα στο χώρο του λιανεμπορίου, όπως είναι τα ηλεκτρονικά βιβλιοπωλεία ή οι εφαρμογές στο χώρο του τουρισμού. Ουσιαστικά, οι εφαρμογές αυτές, αποτελούν κόμβους προβολής και διαφήμισης των επιχειρήσεων, όπου επιπρόσθετα εκτελούνται εμπορικές συναλλαγές. Οι επιχειρήσεις αυτές προσφέροντας ασφάλεια κατά τις συναλλαγές, εξειδικεύοντας τις εργασίες τους στις απαιτήσεις των πελατών, παρέχοντας on-line πληροφορίες σχετικά με τα προϊόντα, την ύπαρξη αποθέματος κλπ και τέλος παρέχοντας on-line service μετά την αγορά, καταφέρνουν να μεγιστοποιούν τον όγκο των εμπορικών τους συναλλαγών.

Πλεονεκτήματα του ηλεκτρονικού εμπορίου

Για τον πελάτη

- Τα ηλεκτρονικά καταστήματα είναι ανοιχτά 24 ώρες το 24ωρο. Με άλλα λόγια οποιαδήποτε στιγμή το επιθυμεί κανείς, μπορεί να αγοράσει πχ ένα CD, ένα αεροπορικό εισιτήριο κλπ.
- Το κόστος των προϊόντων που πωλούνται μέσω Internet είναι κατά γενικό κανόνα πολύ χαμηλότερο από τις τιμές του εμπορίου, αφού ένα ηλεκτρονικό κατάστημα είναι απαλλαγμένο από ένα μεγάλο μέρος του λειτουργικού κόστους ενός πραγματικού καταστήματος (ενοικίαση χώρου και «αέρα», ηλεκτρικό, νερό κλπ) και γενικά απαιτεί πολύ λιγότερο υπαλληλικό προσωπικό.
- Η αγορά είναι πραγματικά παγκόσμια. Με άλλα λόγια, μπορείτε μέσω του υπολογιστή μας να αγοράσουμε ακόμα και κάτι το οποίο δεν κυκλοφορεί στην Ελλάδα, χωρίς να πρέπει πια να περιμένουμε πότε κάποιος φίλος μας θα ταξιδέψει στο εξωτερικό για να μας το φέρει.
- Η συναλλαγή είναι γρήγορη και άμεση. Με άλλα λόγια, από τη στιγμή που ολοκληρώνεται κάποια παραγγελία, το αργότερο σε 3-4 ημέρες έχει ληφθεί, ακόμα και αν εκείνη τη στιγμή το προϊόν βρίσκεται στην άλλη άκρη του πλανήτη. Αλλά το πιο πρακτικό και πιο σημαντικό όφελος για τον καταναλωτή από το ηλεκτρονικό εμπόριο είναι το ότι: καθένας βρίσκει αυτό που θέλει, χωρίς να κάνει βήμα, χωρίς δηλαδή κόπο και χωρίς καμιά σπατάλη χρόνου. Με άλλα λόγια απλά και εύκολα ψώνια από το σπίτι ή το γραφείο.

Για την εταιρεία

- Κάθε εταιρεία που έχει ηλεκτρονική παρουσία μπορεί να διευρύνει τον κύκλο εργασιών της επεκτείνοντας τα γεωγραφικά όρια των συναλλαγών της. Αυτό σημαίνει πως κάθε επιχείρηση που διαθέτει τα προϊόντα της on line μπορεί και αποκτά πελάτες σε περιοχές που βρίσκονται μακριά από την έδρα της, ακόμα και στο εξωτερικό. Με άλλα λόγια, κάθε επιχείρηση που έχει ένα ηλεκτρονικό κατάστημα, είναι σαν να έχει υποκαταστήματα σε πολλές περιοχές και μάλιστα με ελάχιστο λειτουργικό κόστος. Κάθε εταιρεία που χρησιμοποιεί τις νέες τεχνολογίες, όπως το Internet, γίνεται πιο ανταγωνιστική αφού μπορεί να ενημερώνεται πιο εύκολα για τις τρέχουσες εξελίξεις στο χώρο της. Με άλλα λόγια και με δεδομένο το ότι
- σε λίγα χρόνια όλες οι εμπορικές δραστηριότητες θα γίνονται μέσω Internet, το ηλεκτρονικό εμπόριο είναι η νέα μεγάλη πρόκληση για κάθε εταιρεία που θέλει να είναι ανταγωνιστική.

- ❖ Οι ηλεκτρονικές συναλλαγές επιτρέπουν την αμφίδρομη σχέση μεταξύ επιχείρησης και καταναλωτή. Αυτό σημαίνει πως κάθε εταιρεία μέσω των ηλεκτρονικών συναλλαγών μπορεί να συλλέξει πολλά στοιχεία για τις συνήθειες, τις ανάγκες και τα γούστα των καταναλωτών και σύμφωνα με αυτά να αναπροσαρμόσει την πολιτική της προς το θετικότερο.
- ❖ Τέλος, γνωρίζοντας τις συγκεκριμένες ανάγκες των πελατών τους, οι εταιρείες μπορούν να προσχωρήσουν στη δημιουργία συγκεκριμένων προϊόντων είτε ανταποκρινόμενων σε έναν καταναλωτή, είτε σε μια ομάδα καταναλωτών που χρειάζονται ένα νέο προϊόν το οποίο δεν υπάρχει ακόμα στην αγορά.

Μειονεκτήματα ηλεκτρονικού εμπορίου

Το σημαντικότερο μειονέκτημα του ηλεκτρονικού εμπορίου σχετίζεται με την ασφάλεια των συναλλαγών, που μας απασχολεί σε όλη την παρούσα εργασία. Στο Internet δύσκολα μπορεί κανείς να εγγυηθεί απόλυτη ασφάλεια, φράση που επίσης επαναλαμβάνεται συνεχώς στην εργασία. Αυτό λειτουργεί ως ένας ψυχολογικός φραγμός στον καταναλωτή που διστάζει να δώσει τον αριθμό της πιστωτικής του κάρτας σε έναν τόπο του Internet, ακόμη και αν του είναι γνωστός και καθιερωμένος. Βέβαια, είναι γεγονός ότι με την κρυπτογράφηση των δεδομένων και την υιοθέτηση ψηφιακών υπογραφών οι περιπτώσεις ηλεκτρονικής απάτης γίνονται ένα ασήμαντο στατιστικό ποσοστό των συναλλαγών.

Για τις μικρές χώρες η παγκοσμιοποίηση της αγοράς είναι επίσης μειονέκτημα. Οι ΗΠΑ είναι μια τεράστια αγορά, αλλά το κόστος για την δημιουργία του μηχανισμού πώλησης παραμένει συγκρίσιμο, με αποτέλεσμα η Amazon να πουλά διεθνώς ελληνικά βιβλία πολύ ευκολότερα από το να πουλήσει πχ ο Ελευθερουδάκης διεθνώς αγγλικά βιβλία. Πολέμιοι του ηλεκτρονικού εμπορίου προβάλλουν και τα ακόλουθα μειονεκτήματά του:

- Απαίτηση γρήγορων υπολογιστών οι οποίοι θα είναι ικανοί να επεξεργαστούν απαιτητικά γραφικά.
- Ακριβές διεθνείς τηλεπικοινωνίες.
- Περιορισμένη ροή πληροφοριών και περιορισμένες εγγραφές.
- Εξάρτηση από τυχόν δυσλειτουργία του υπολογιστή.
- Έλλειψη ασφάλειας.
- Ανεργία του ανθρώπινου δυναμικού.
- Έλλειψη ειδικευμένου προσωπικού.

Οι εταιρείες του ηλεκτρονικού επιχειρείν και εμπορίου έχουν δημιουργήσει τεράστιες υπεραξίες σε ελάχιστο χρονικό διάστημα και έχουν κάνει πλούσιους τους βασικούς τους μετόχους και τους απλούς επενδυτές. Με αυτή τη λογική, οι εταιρείες αυτές είναι πολύ επιτυχημένες πχ η εταιρεία Yahoo! έχει υψηλότερη χρηματιστηριακή αξία από την Apple ή τους New York Times. Σε ότι αφορά τις εταιρείες που πουλούν είναι δύσκολο να πει κανείς ότι δεν είναι επιτυχημένες, διότι δε θα είχαν επιβιώσει αλλιώς. Εταιρείες, όπως η Dell Computer, κάνουν ένα 30% του τζίρου τους μέσω του Internet και δημιουργούν σημαντικές συνεργασίες με τα κλασικά τους κανάλια διάθεσης. Είναι εντυπωσιακό ότι η Dell, η Intell και η Cisco (με τηλεπικοινωνιακό υλικό σε ποσοστό 75% on line) πουλούν μαζί πάνω από 70 εκατομμύρια δολάρια ημερησίως.

Αυτό που σίγουρα απαιτείται είναι μια επιχείρηση να μπορεί να αξιολογήσει σωστά τις ευκαιρίες και τους κινδύνους που μπορεί να συνεπάγεται η υιοθέτηση του ηλεκτρονικού εμπορίου, αλλά και να επιλέξει τη σωστή στρατηγική και το πλάνο εφαρμογής της.

Η επιρροή του ηλεκτρονικού εμπορίου στην απασχόληση και γενικότερα στον τρόπο ζωής μας.

Η άνθηση του ηλεκτρονικού εμπορίου έχει σημαντικό αντίκτυπο στην απασχόληση σε ολόκληρη την Ευρωπαϊκή Ένωση δεδομένου ότι πάνω από 22 εκατ. άνθρωποι εργάζονται στο εμπόριο. Κατά τη 10ετία 1984-1994 το εμπόριο δημιούργησε περίπου 2,3 εκατ. θέσεις εργασίας στα μέλη-κράτη της τότε ευρωπαϊκής ένωσης, αριθμός που ισοδυναμεί με το 12% της συνολικής αύξησης. Πλέον το ηλεκτρονικό εμπόριο αποτελεί αναπόσπαστο κομμάτι σχεδόν για όλες τις επιχειρήσεις. Οι καταναλωτές προτιμούν να ψάχνουν στις «ηλεκτρονικές βιτρίνες» παρά να χάνουν χρόνο ψάχνοντας στους δρόμους αφού με το πάτημα ενός πλήκτρου μπορούν να δουν πράγματα που τους ενδιαφέρουν μέσα σε λίγα λεπτά. Αντιθέτως, χρησιμοποιώντας τον παραδοσιακό τρόπο θα έχαναν αρκετές ώρες.

Το ηλεκτρονικό εμπόριο αποτελεί σήμερα το πιο δημοφιλές αντικείμενο συζήτησης μεταξύ των στελεχών επιχειρήσεων και των κρατικών αξιωματούχων στην Ελλάδα (πρώτο παραμένει ακόμα το Χρηματιστήριο). Κάθε τόσο ακούμε κυβερνητικές και ευρωπαϊκές εξαγγελίες για μέτρα ενθάρρυνσης των επενδύσεων σε αυτό το χώρο, ενώ ο τύπος δημοσιεύει συνεχώς μελέτες, σύμφωνα με τις οποίες η επιχειρηματική δραστηριότητα μετακομίζει στο δίκτυο και σύντομα όλες οι εργασίες και οι αγοραπωλησίες θα γίνονται μέσα από αυτό.

Όπως είναι φυσικό, υπάρχει μια δόση υπερβολής σε όλες αυτές τις προβλέψεις (μέχρι σήμερα σχεδόν καμία νέα τεχνολογία δεν εγκατέστησε εντελώς τις προηγούμενες). Είναι όμως γεγονός, πως βρισκόμαστε μπροστά σε μια πραγματική επανάσταση.

Μέσα σε αυτόν τον κυκεώνα προφητειών, ιδεών και προειδοποιήσεων, κάθε επενδυτής καλείται να προβλέψει ποια είναι εκείνα τα δεδομένα που θα μεταβληθούν στο άμεσο ή το απώτερο μέλλον και ποιες από τις παρουσιαζόμενες ως επαναστατικές αλλαγές θα αποδειχθούν επιτυχημένες και δε θα προστεθούν στον κατάλογο των πολυδιαφημιζόμενων εργαλείων του δικτύου, τα οποία τελικά αποδείχθηκαν άχρηστα και παραδόθηκαν στον Καιάδα των αποτυχημένων τεχνολογιών μαζί με τα εκατομμύρια δολάρια που δαπανήθηκαν για την ανάπτυξή τους.

Δυστυχώς, αυτό το άγχος για την καλύτερη κατανόηση και πρόβλεψη της εξέλιξης των τεχνολογιών Internet μας κάνει συχνά να ξεχνάμε πως η επιχειρηματική δραστηριότητα στο δίκτυο έχει τις ίδιες απαιτήσεις ανάλυσης, σχεδιασμού, κοστολόγησης, οικονομικής διαχείρισης, έρευνας αγοράς και διαφήμισης με κάθε ανάλογη προσπάθεια στην «παραδοσιακή» οικονομία.

Ηλεκτρονική τραπεζική (Web banking)

Το Web banking, δηλαδή η τραπεζική συναλλαγή μέσω της οθόνης του υπολογιστή με τη βοήθεια του Internet, αποτελεί μια καινοτομία στην κοινωνία που ζούμε, μια ιδέα επαναστατική που συμβάλλει στην αναβάθμιση της καθημερινής μας ζωής. Το Web banking αποτελεί το πρώτο σημαντικό βήμα στην ολοκλήρωση του κύκλου των εμπορικών και άλλων συναλλαγών μέσα από το Internet προκειμένου να καταργηθούν ΜΙΑ ΓΙΑ ΠΑΝΤΑ οι άσκοπες μετακινήσεις και η εκνευριστική αναμονή στις ουρές των ταμείων των διαφόρων τραπεζών. Οι τραπεζικές συναλλαγές μέσω Internet βοηθούν τον χρήστη-πελάτη να αποφύγει την ταλαιπωρία των μετακινήσεων από τη μια τράπεζα στην άλλη, την αναμονή σε συχνά ατελείωτες ουρές στα ταμεία τους, προσφέροντας του ταυτόχρονα άμεση πληροφόρηση και πληθώρα εναλλακτικών λύσεων σε όσα θέματα των απασχολούν. Το E-Banking μεταφέρει την τράπεζα στην οθόνη του υπολογιστή μας. Το παρεχόμενο φάσμα των υπηρεσιών θα περιλαμβάνει σταδιακά όλο το σύνολο των τραπεζικών εργασιών.

Μέσω του Internet ο χρήστης μπορεί να συνδεθεί με την τράπεζα στην οποία διατηρεί λογαριασμό, να ρωτήσει για το υπόλοιπο του λογαριασμού του, να πληρώσει την πιστωτική του κάρτα ή τις υποχρεώσεις του προς τρίτους, να υπολογίζει τους τόκους των καταθέσεών του ή να προχωρήσει ακόμα και σε στη διαχείριση του χαρτοφυλακίου του, στην εκτέλεση για το Χρηματιστήριο, στη λήψη και την αποπληρωμή των δανείων του.

Από την ησυχία του σπιτιού του ο κάθε χρήστης μπορεί να παρακολουθεί ότι ώρα θέλει και όσο θέλει τα επιτόκια όλων των τραπεζών και να υπολογίζει στα δικά του λογιστικά φύλλα, τα συν και τα πλην τους προκειμένου να προβεί στις πιο συμφέρουσες γι' αυτόν

επιλογές. Μπορεί να αποφασίσει αμερόληπτα όχι μόνο για το τραπεζικό του προϊόν αλλά και για την τράπεζα με την οποία συνεργάζεται.

Το Internet banking χρησιμοποιεί λογισμικό που είναι εγκατεστημένο στον υπολογιστή της τράπεζας, δίνοντας τη δυνατότητα στον πελάτη να έχει πρόσβαση στους λογαριασμούς του από οποιοδήποτε υπολογιστή που είναι συνδεδεμένος με το Διαδίκτυο.

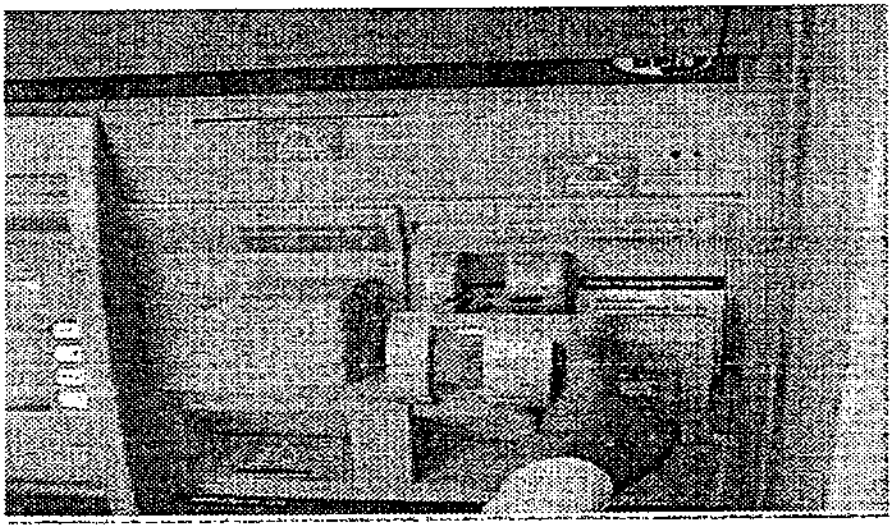
Το Web banking προϋποθέτει την ύπαρξη ενός τουλάχιστον λογαριασμού, στον οποίο μπορεί ο χρήστης-πελάτης να έχει την πρόσβαση να δίνει εντολές ή να παρακολουθεί το υπόλοιπό του. Αφού λοιπόν ο χρήστης-πελάτης εξασφαλίσει τη σύνδεση του υπολογιστή του με το Διαδίκτυο, πράγμα που αποτελεί το πρώτο βήμα, θα πρέπει αμέσως να προχωρήσει στο δεύτερο, δηλαδή στο άνοιγμα ενός λογαριασμού στην τράπεζα της προτίμησής του.

Για να γίνει αυτό, θα πρέπει να επισκεφθεί το πλησιέστερο υποκατάστημα της εκάστοτε τράπεζας έχοντας μαζί του την αστυνομική του ταυτότητα. Ορισμένες τράπεζες «απαιτούν» η αστυνομική ταυτότητα να συνοδεύεται και από μια κατάθεση της τάξης των 300€. Μετά το άνοιγμα του λογαριασμού και της σύνδεσης με το Internet ακολουθεί η συμπλήρωση της αίτησης για το Web banking. Αυτό μπορεί να γίνει και από το σπίτι, καθώς όλες οι τράπεζες διαθέτουν τις αντίστοιχες αιτήσεις μέσα από το Internet. Η συμπλήρωση και αίτηση με τα προσωπικά στοιχεία με τα προσωπικά στοιχεία του πελάτη γίνεται μέσα από το πρόγραμμα αναζήτησης και αποστέλλεται στην τράπεζα ηλεκτρονικά. Η αίτηση, η οποία είναι ψηφιακή, δεν είναι δυνατό να περιλαμβάνει την υπογραφή του πελάτη. Έτσι ο πελάτης θα πρέπει είτε να πάει στο κοντινότερο υποκατάστημα της τράπεζας όπου υπογράφει κάποια σύμβαση και παίρνει τους κωδικούς πρόσβασης για σύνδεση με το Web banking, είτε να περιμένει το συστημένο γράμμα του ταχυδρομείου με το φάκελο και τους κωδικούς πρόσβασης για να ολοκληρώσει τη διαδικασία και να ξεκινήσει τις συναλλαγές του μέσω Internet.

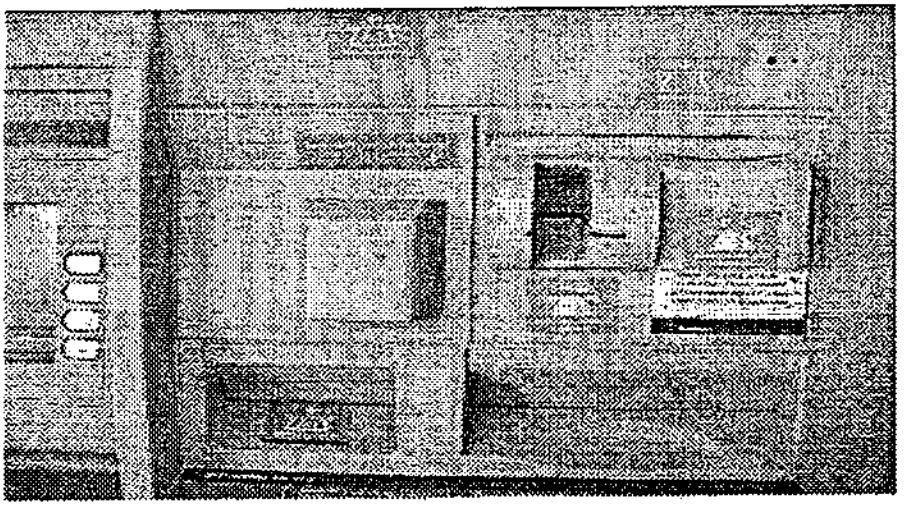
Ασφάλεια δεδομένων: η ασφάλεια των δεδομένων είναι φυσικό να αποτελεί ένα από τα πιο σημαντικά σημεία της λειτουργίας ενός συστήματος Διαδικτυακής Τραπεζικής. Όπου υπάρχουν προσωπικά στοιχεία, είναι εύλογο ο καθένας να θέλει να διασφαλίσει το απόρρητο, πόσο μάλλον όταν περιλαμβάνονται οικονομικά στοιχεία και στοιχεία λογαριασμών. Αυτή ακριβώς η ασφάλεια των συναλλαγών είναι το μεγαλύτερο πρόβλημα των υπεύθυνων μηχανογράφησης και ασφάλειας των τραπεζών. Κάτι παρόμοιο συμβαίνει και στο ηλεκτρονικό εμπόριο, σε μικρότερη όμως κλίμακα. Δεν είναι το ίδιο να μπορεί κανείς να έχει πρόσβαση σε μια πιστωτική κάρτα και στους λογαριασμούς της τράπεζας. Η πιστωτική κάρτα έχει περιορισμένη χρήση, μόνο για αγορές, και με συγκεκριμένο πιστωτικό όριο. Αντίθετα, η

πρόσβαση στον τραπεζικό λογαριασμό μπορεί να έχει πολλαπλά αποτελέσματα, καθώς, θεωρητικά, μπορεί κάποιος να κάνει διάφορες συναλλαγές, να πιστώσει και να χρεώσει άλλους λογαριασμούς ή να στείλει εμβάσματα στο εξωτερικό.

Οι συναλλαγές που πραγματοποιούνται κάνοντας χρήση των υπηρεσιών Web banking δε διαφέρουν από τις συμβατικές συναλλαγές μέσω πιστωτικών καρτών ή συναλλαγές με ATM. Αν μια πιστωτική κάρτα κλαπεί ή πέσει σε λάθος χέρια μαζί με το μυστικό αριθμό PIN, τότε υπάρχει άμεσος κίνδυνος να χάσει κάποιος τα χρήματά του. Ένα τέτοιο περιστατικό συνέβη πρόσφατα σε ελληνική τράπεζα (Φεβρουάριος 2004) και παρακάτω παρουσιάζεται η μέθοδος που χρησιμοποιήθηκε έτσι ώστε να υποκλέπτονται οι μυστικοί αριθμοί των πελατών που έκαναν χρήση του ATM, με αποτέλεσμα πολλοί από αυτούς να χάσουν σημαντικά ποσά από τους τραπεζικούς τους λογαριασμούς.

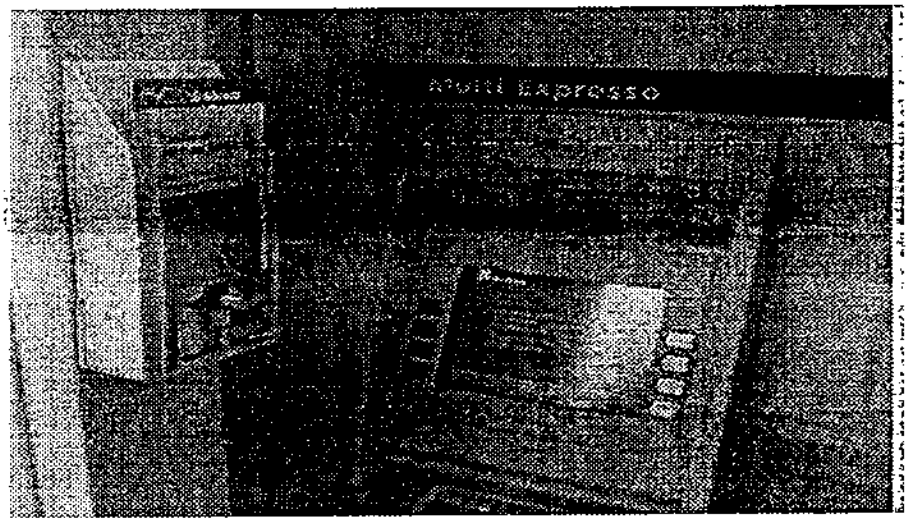


Εικόνα 1: ο ασύρματος μαγνητικός αντιγραφέας μπαίνει επάνω από το στόμιο υποδοχής της κάρτας και αποθηκεύει όλα τα στοιχεία της κάρτας.

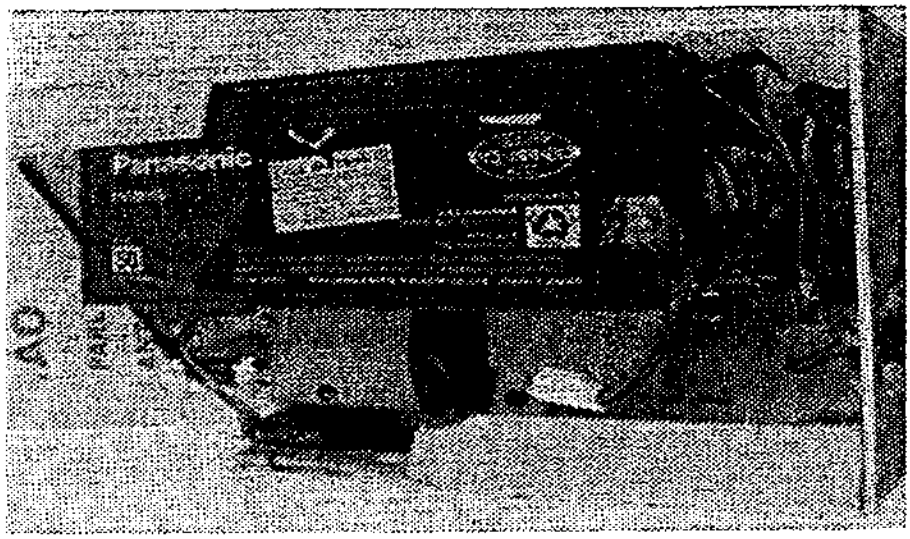


Εικόνα 2: εγκαθίσταται με τέτοιο τρόπο ώστε ο πελάτης να μην καταλαβαίνει τη διαφορά

Εικόνα 3: τοποθετούνται από δύο μικροκάμερες οι οποίες σημαδεύουν την οθόνη και το πληκτρολόγιο (για να βλέπουν το pin).



Εικόνα 4: οι ασύρματες αυτές συσκευές (κάμερες και μαγνητικός αντιγραφέας) έχουν εμβέλεια που φτάνει τα 200 μέτρα.

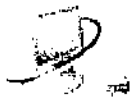


Εικόνα 5: το εσωτερικό του κουτιού που περιέχει την ασύρματη κάμερα.

Παρόμοιος κίνδυνος υπάρχει και στην περίπτωση των υπηρεσιών του Web banking, αν οι μυστικοί κωδικοί που αναφέραμε παραπάνω πέσουν σε λάθος χέρια. Ένα επιπλέον στοιχείο που πρέπει να ληφθεί υπόψη είναι το γενικότερο πρόβλημα της ασφάλειας του Διαδικτύου, όπως επανειλημμένως έχει αναφερθεί στην παρούσα εργασία. Οι τράπεζες πάντως, λαμβάνουν μια σειρά από μέτρα για την ασφάλεια των συναλλαγών, όπως είναι η χρησιμοποίηση του πρωτοκόλλου SSL (Secure Socket Layer), η κωδικοποίηση των στοιχείων, η χρησιμοποίηση πιστοποιητικών και οι κωδικοί αριθμοί που χρησιμοποιούνται σε κάθε συναλλαγή.

Η προστασία των συναλλαγών από πιθανούς «εισβολείς» είναι το ένα σκέλος του προβλήματος. Το άλλο, η τήρηση του τραπεζικού απορρήτου, πρέπει να θεωρείται αυτονόητο. Οι ίδιες βασικές αρχές που διέπουν τις κλασσικές τραπεζικές συναλλαγές ισχύουν και στην περίπτωση των συναλλαγών μέσω του Διαδικτύου. Όλες οι πληροφορίες που διαβιβάζονται από τον πελάτη στην τράπεζα είναι εμπιστευτικές και η κάθε τράπεζα λαμβάνει όλα τα απαραίτητα μέτρα, ώστε να γίνεται χρήση τους μόνο στα πλαίσια των παρεχόμενων υπηρεσιών. Ένα από αυτά, για παράδειγμα, είναι ότι μόνο εξουσιοδοτημένοι υπάλληλοι με την κατάλληλη εκπαίδευση στο χειρισμό πληροφοριών των πελατών έχουν πρόσβαση στις πληροφορίες των ηλεκτρονικών συναλλαγών, όπως άλλωστε γίνεται και με τις κανονικές συναλλαγές. Είναι αυτονόητο, ότι όπως δεν πρέπει κανείς να χάσει την κάρτα ανάληψης και τον κωδικό PIN, έτσι και ο χρήστης της υπηρεσίας Web banking δεν πρέπει να χάσει τους κωδικούς αριθμούς πρόσβασης, τον αριθμό κάρτας ή τους κωδικούς που συνοδεύουν τις συναλλαγές. Συνήθως, η διαδικασία που ακολουθείται σε περίπτωση απώλειας των στοιχείων αυτών είναι παρόμοια με αυτή που ακολουθείται όταν χάσει κανείς την πιστωτική του κάρτα ή την κάρτα ATM.

Ε΄ Μέρος



Παράρτημα

Εισαγωγή (του Robert Richardson)

Η έρευνα για το Έγκλημα και την Ασφάλεια στους Υπολογιστές διεξάγεται από την CSI (Computer Security Institute) με τη συμμετοχή του FBI (San Francisco Federal Bureau of Investigations). Η έρευνα, ούσα στο 8° έτος διεξαγωγής της, έχει το προνόμιο να είναι η μακροβιότερη έρευνα στον τομέα της ασφάλειας των πληροφοριών. Όπως και στα προηγούμενα χρόνια, η έρευνα παρουσιάζει μια αποκρουστική εικόνα του πόσο συχνά συμβαίνουν εγκλήματα σε δίκτυα υπολογιστών και απλά πόσο ακριβά είναι τέτοιου είδους εγκλήματα.

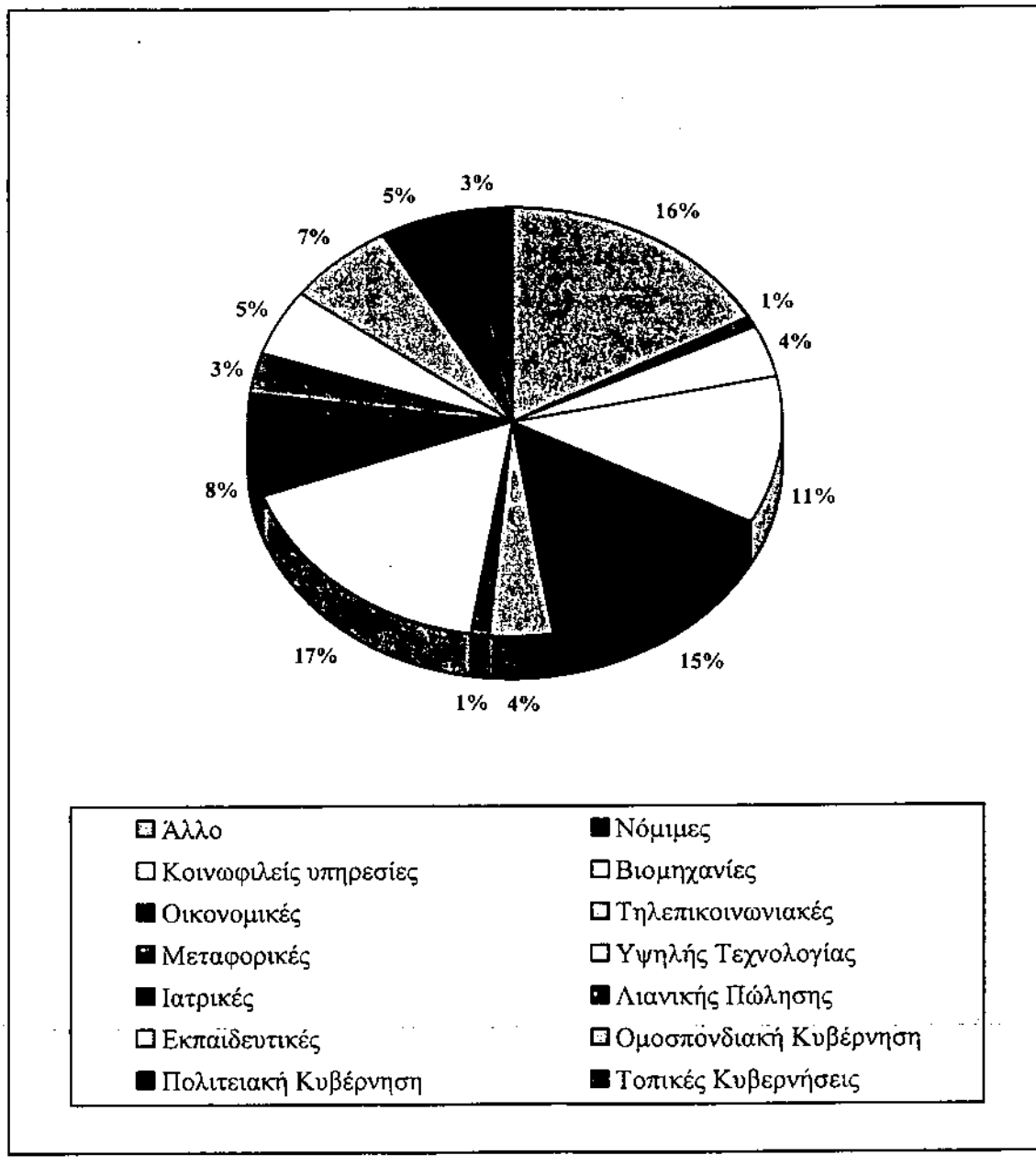
Βασισμένα στις απαντήσεις 530 ειδικών στην ασφάλεια υπολογιστών στις Ηνωμένες Πολιτείες, οργανισμών, κυβερνητικών οργανώσεων, οικονομικών ιδρυμάτων, ιατρικών ιδρυμάτων και πανεπιστημίων, τα ευρήματα του 2003 για άλλη μία φορά δείχνουν ότι δεν υπάρχει έλλειψη στις επιθέσεις, αλλά δείχνει ότι αυτό το χρόνο η ένταση και το κόστος αυτών των επιθέσεων παρουσίασε πτώση, για πρώτη φορά μετά το 1999.

Παρά τα χαμηλότερα νούμερα του συνόλου των οικονομικών απωλειών που αναφέρουν οι απαντηθέντες, το πιο σημαντικό συμπέρασμα που πρέπει κάποιος να βγάλει από την έρευνα παραμένει το ότι το ρίσκο των επιθέσεων παραμένει υψηλό. Ακόμα και οργανισμοί οι οποίοι έχουν προσλάβει μια πλατιά γκάμα τεχνολογιών ασφάλειας, μπορεί να πέσουν θύματα σημαντικών απωλειών. Επιπλέον, το ποσοστό αυτών των περιστατικών που αναφέρονται στις αρμόδιες αρχές παραμένει χαμηλό. Έτσι, δικαιολογημένα οι επιτιθέμενοι μπορούν να πιστεύουν ότι οι πιθανότητες να πιαστούν και να καταδικαστούν είναι καθαρά με το μέρος τους.

Σχετικά με τους απαντηθέντες

Αυτοί που απαντούν στην έρευνα, αποτελούνται από εταιρείες και οργανισμούς του φάσματος της μοντέρνας ζωής. Ένα 17% είναι από υψηλής τεχνολογίας εταιρείες, ένα πρόσθετο 15% προέρχεται από τον οικονομικό τομέα. Οι κυβερνητικές υπηρεσίες φτάνουν συνολικά, περίπου, ένα 15% των απαντήσεων της έρευνας.

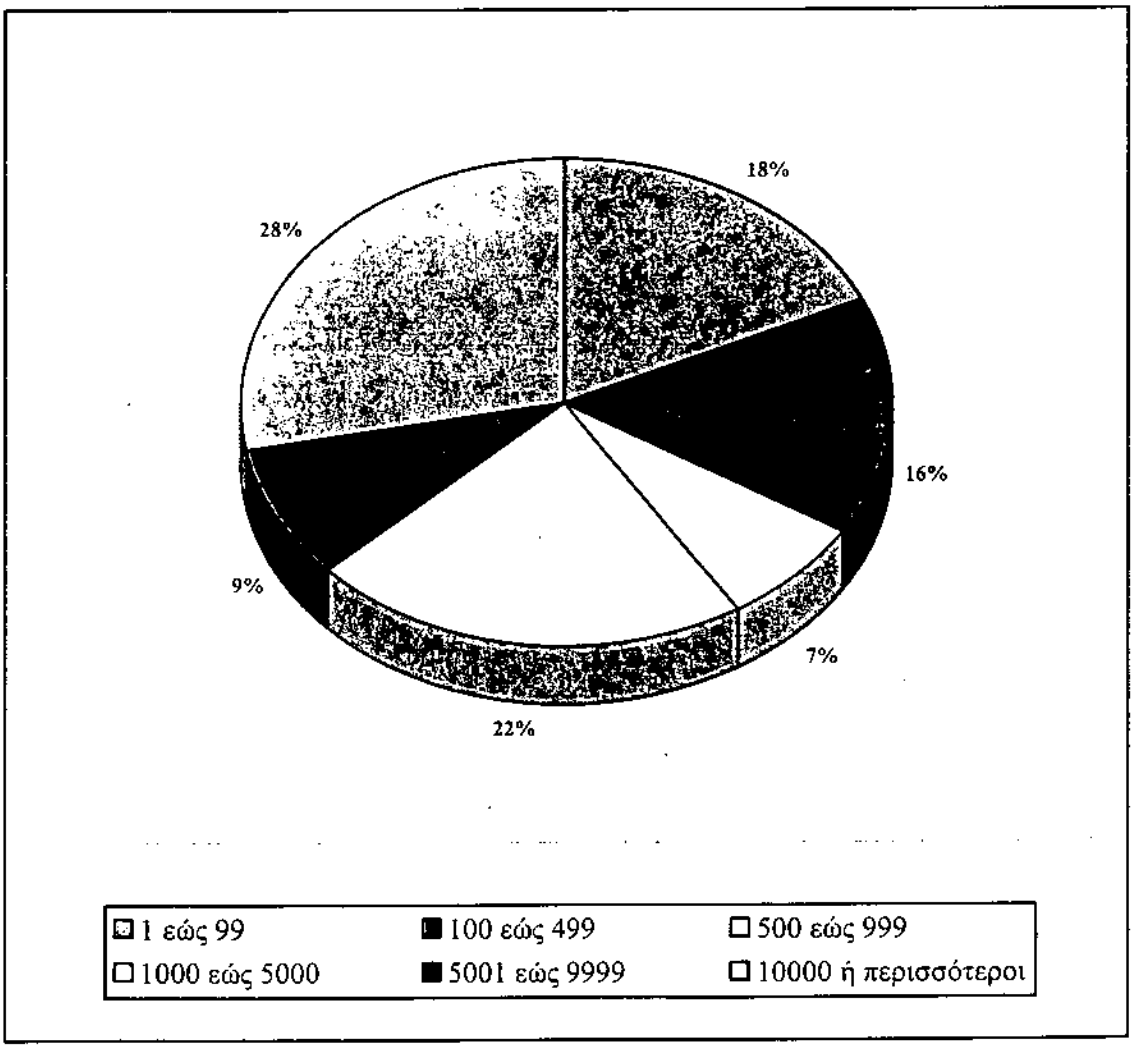
Απαντηθέντες από τον Βιομηχανικό Τομέα



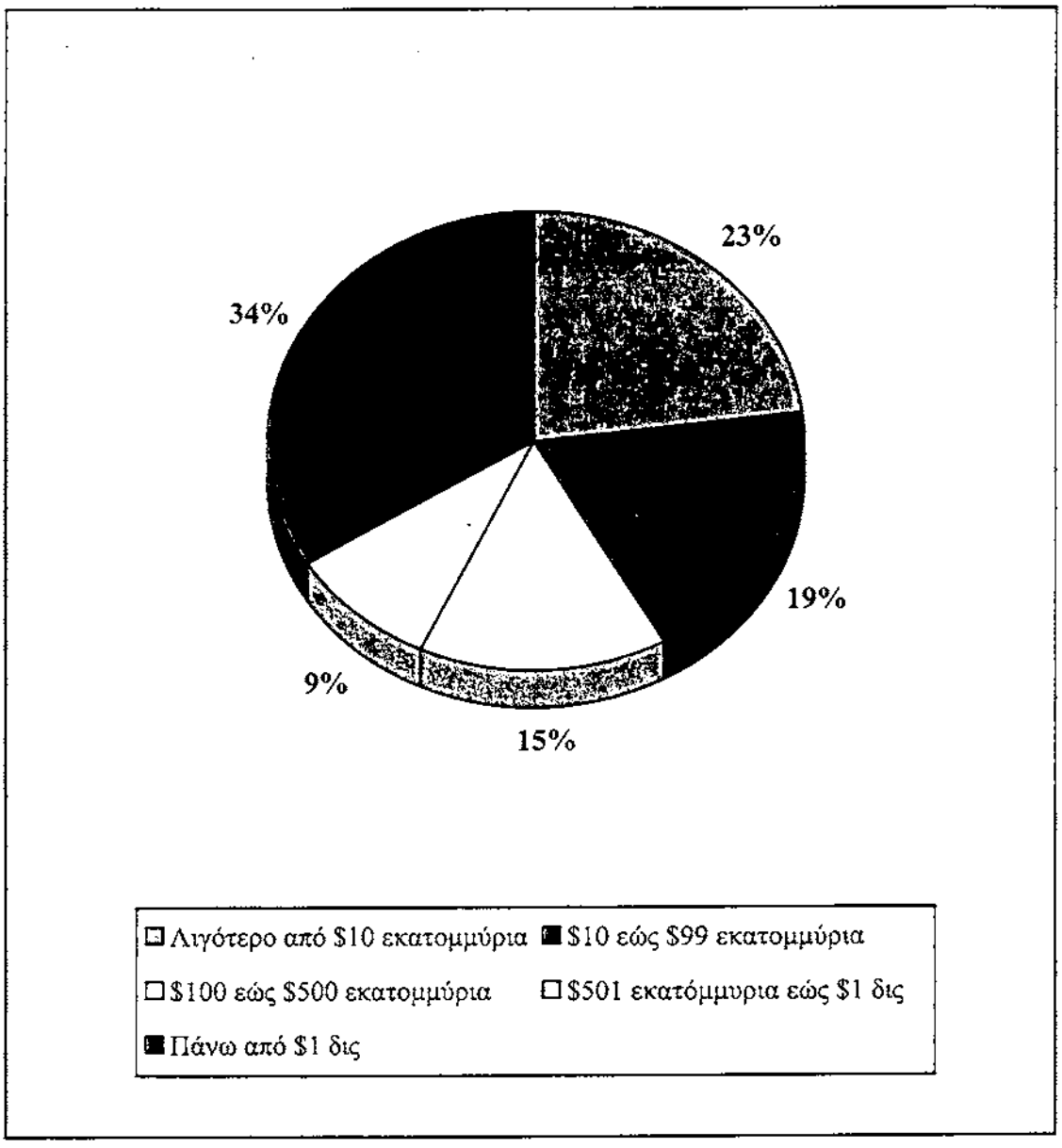
Παραπάνω από τους μισούς οργανισμούς που παρουσιάζονται στην έρευνα απασχολούν περισσότερους από 1.000 υπαλλήλους, ενώ περίπου το !/4 των απαντηθέντων (δηλαδή ένα ποσοστό 28%) αναφέρει ότι απασχολεί περισσότερους από 10.000 υπαλλήλους. Αυτό πρόχειρα αντιστοιχεί σε εισοδήματα, όπως: το 34% δηλώνει περισσότερο από ένα δις δολάρια σε ετήσια βάση.

Τα ποσοστά αυτά δείχνουν ξεκάθαρα ότι όχι μόνο οι υψηλής κλίμακας εταιρείες, αλλά και οι μικρότερες επιχειρήσεις έχουν θέση στην έρευνα. Συγκεκριμένα, το 18% των απαντηθέντων εργάζονται σε οργανισμούς με 99 ή λιγότερους υπαλλήλους και ένα 23% εργάζεται σε οργανισμούς που δηλώνουν εισοδήματα λιγότερα από δέκα εκατομμύρια δολάρια.

Απαντηθέντες και Αριθμός Υπαλλήλων



Απαντηθέντες και Εισόδημα (χονδρικά)

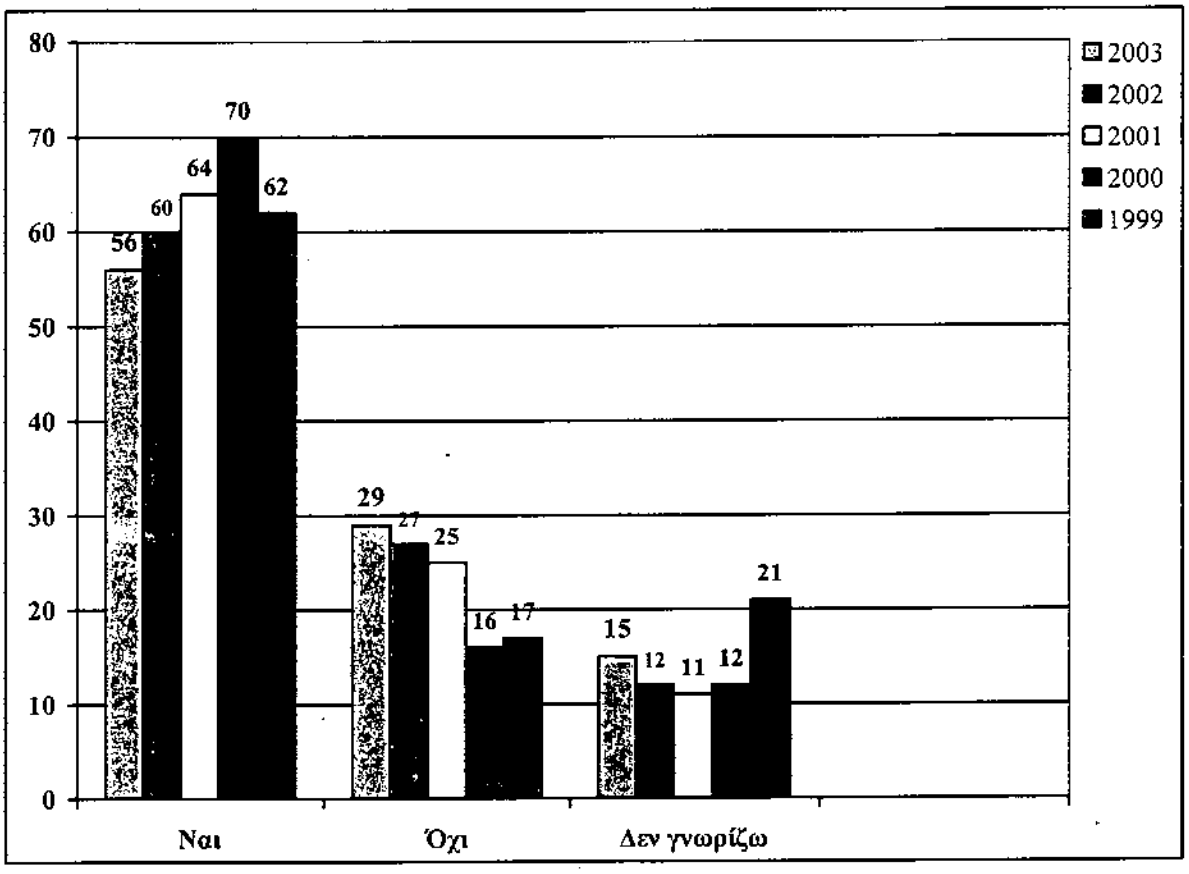


Τα «Highlights» της Έρευνας

Ενώ το ποσοστό των απαντηθέντων που αναφέρουν κάποια μορφή μη εξουσιοδοτημένης χρήσης υπολογιστή παρέμεινε περίπου το ίδιο με τις προηγούμενες χρονιές, οι οικονομικές απώλειες από αυτές τις επιθέσεις που αναφέρθηκαν έπεσαν κατακόρυφα. 56% των απαντηθέντων ανέφεραν μη εξουσιοδοτημένη χρήση, συγκρινόμενη με το 60% του 2002 (και σε σύγκριση με έναν μέσο όρο 59% κατά τα προηγούμενα 7 χρόνια της έρευνας). Οι συνολικές ετήσιες απώλειες που αναφέρθηκαν στην έρευνα του 2003 ήταν $201.797.340, αριθμός μειωμένος κατά 56% των $455 εκατομμυρίων που αναφέρθηκαν το 2002. Θα πρέπει να σημειωθεί, παρ' όλ' αυτά, ότι αυτό το νούμερο είναι ευθυγραμμισμένο με τα νούμερα που

αναφέρθηκαν πριν το 2001. Επίσης, είναι σημαντικό να θυμόμαστε ότι αυτό το ποσό είναι απλά οι συνολικές απώλειες που αναφέρθηκαν από συγκεκριμένο αριθμό οργανισμών (251 από αυτούς) και δεν χρήζει παραπέρα έρευνας.

Μη εξουσιοδοτημένη χρήση των Συστημάτων κατά τους τελευταίους 12 μήνες

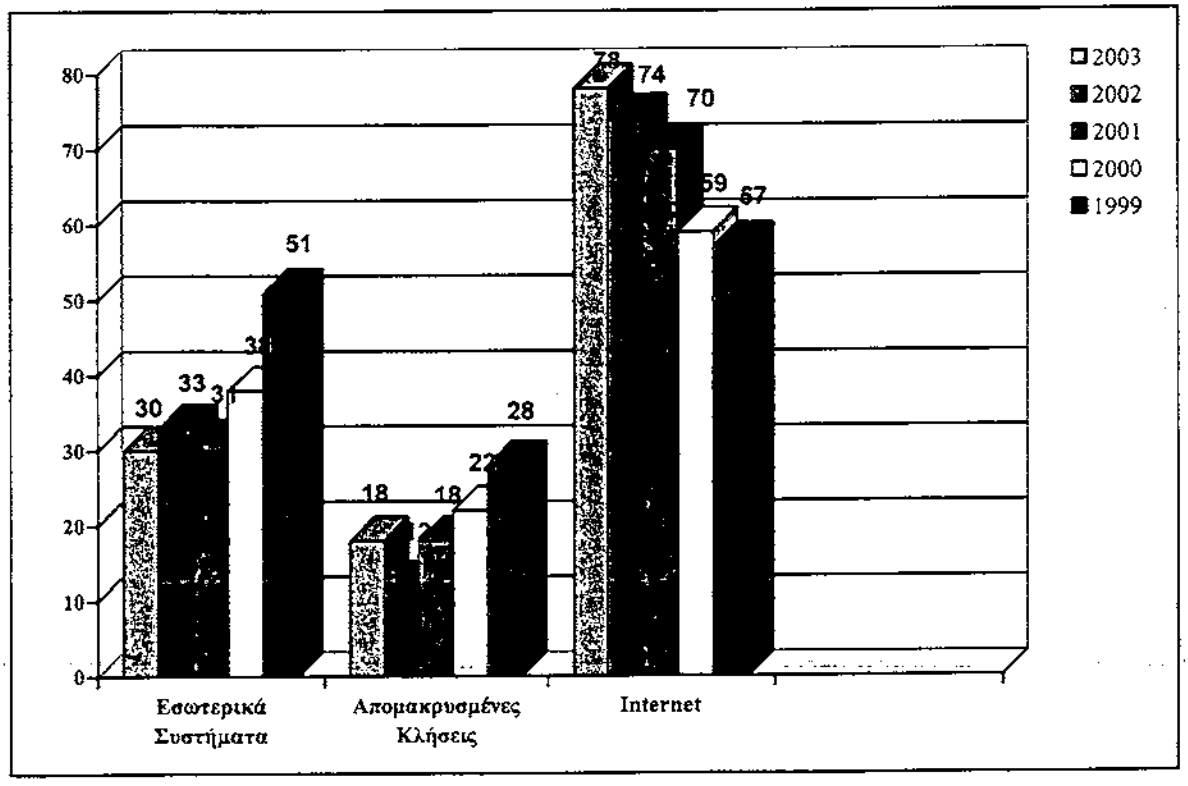


Αποκλειστικά Ιδιωτικές Πληροφορίες

Σύμφωνα με την ιστορία της έρευνας, η κλοπή αποκλειστικά ιδιωτικών πληροφοριών έχει αποτελέσει μία από τις πιο ακριβοπληρωμένες μορφές εγκλήματος των υπολογιστών. Πραγματικά, από το 1999 εκτοξεύει επίμονα τις κλίμακες των αναφερόμενων οικονομικών απωλειών στα ύψη. Αυτό δε θα έπρεπε να προκαλεί έκπληξη σε μια οικονομία όπου ένα μεγάλο μέρος της συνολικής παραγωγικότητας εξαρτάται από πληροφορίες και υψηλά τεχνικές γνώσεις πραγμάτων.

Μέσα στον κόσμο του Internet, θέματα που περιβάλλουν την πνευματική ιδιοκτησία ήταν στο επίκεντρο το 2002. Τα υψηλού προφίλ πακέτα νέων δεν αφορούσαν απαραίτητα την κλοπή εμπορικών μυστικών, η οποία είναι η σημαντικότερη απειλή για τις περισσότερες εταιρείες, αλλά επικεντρώνονται ακόμα και στην καταπάτηση της αποκλειστικότητας που έχει δημιουργήσει ένα κλίμα μες στο οποίο οι έλεγχοι που βασίζονται στην κρυπτογραφία (όπως τα νέα ψηφιακά δικαιώματα του Management Server της Microsoft) αυξάνονται σταθερά.

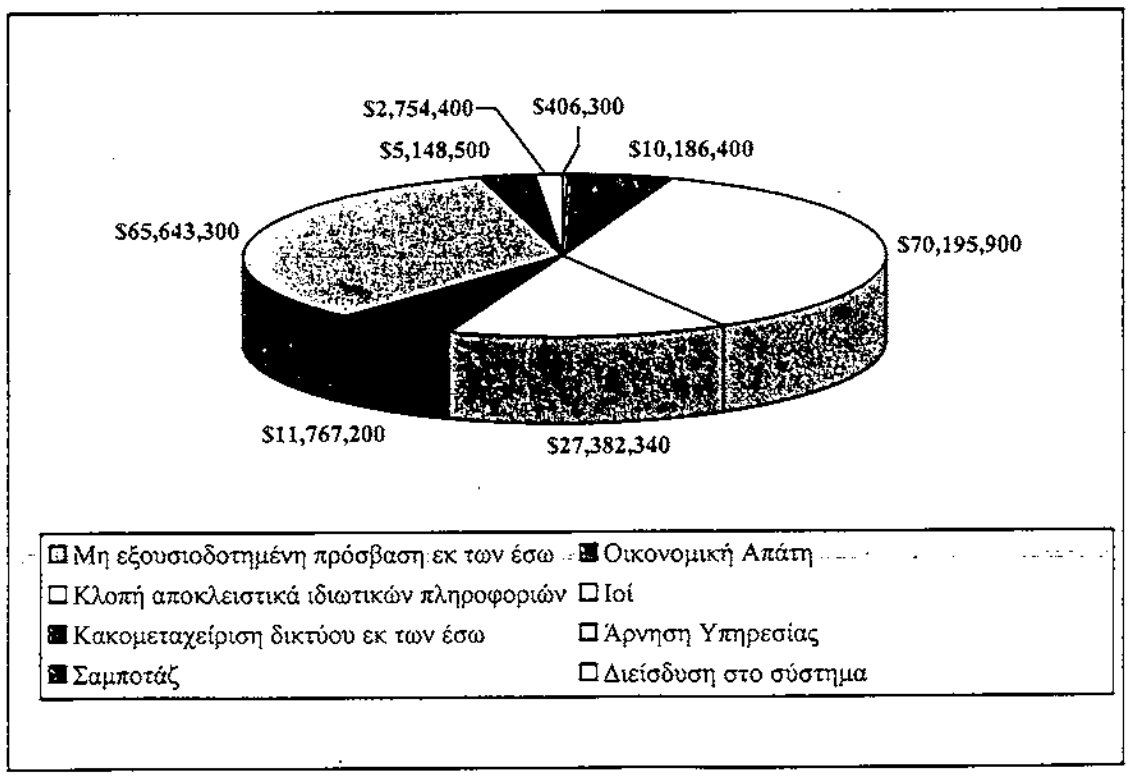
Οι Συνδέσεις Internet επιδεικνύονται συνεχώς ως το συχνότερο σημείο επίθεσης



Άλλα καίρια ευρήματα

- Ο αριθμός αυτών των σημαντικών περιστατικών παρέμειναν περίπου ο ίδιος με του προηγούμενου έτους, παρά την πτώση στις οικονομικές απώλειες.
- Όπως και στα προηγούμενα χρόνια, η κλοπή αποκλειστικά ιδιωτικών πληροφοριών προκάλεσε τις μεγαλύτερες οικονομικές απώλειες ($70.195.900 χάθηκαν, με το μέσο όρο που αναφέρθηκε να κυμαίνεται περίπου στα $2.7 εκατομμύρια).
- Σε μετατόπιση από τα προηγούμενα χρόνια, το δεύτερο πιο ακριβό έγκλημα με υπολογιστές, σύμφωνα με τις απαντήσεις της έρευνας, ήταν η άρνηση υπηρεσίας (denial of service), με κόστος που έφτασε τα $65.643.300.
- Απώλειες που αναφέρθηκαν για οικονομική απάτη μειώθηκαν δραστικά στα $10.186.400.
- Όπως και στα προηγούμενα χρόνια, τα περιστατικά με ιούς (82%) και η κακομεταχείριση του δικτύου εκ των έσω (80%) ήταν οι πιο συχνές μορφές επίθεσης ή κακοποίησης.
- Οι απαντηθέντες ξανά έκλιναν αρνητικά στην ιδέα της πρόσληψης κάποιου έμπειρου hacker (68% ήταν κατά).
- Το ποσοστό αυτών που ανέφεραν ότι υπέστησαν κάποιο πλήγμα τον προηγούμενο χρόνο και που είπαν ότι ανέφεραν αυτά τα περιστατικά στις αρχές, παρέμεινε ιδιαίτερα χαμηλό (30%).

Απώλειες (σε δολάρια) βάσει τύπου απάτης



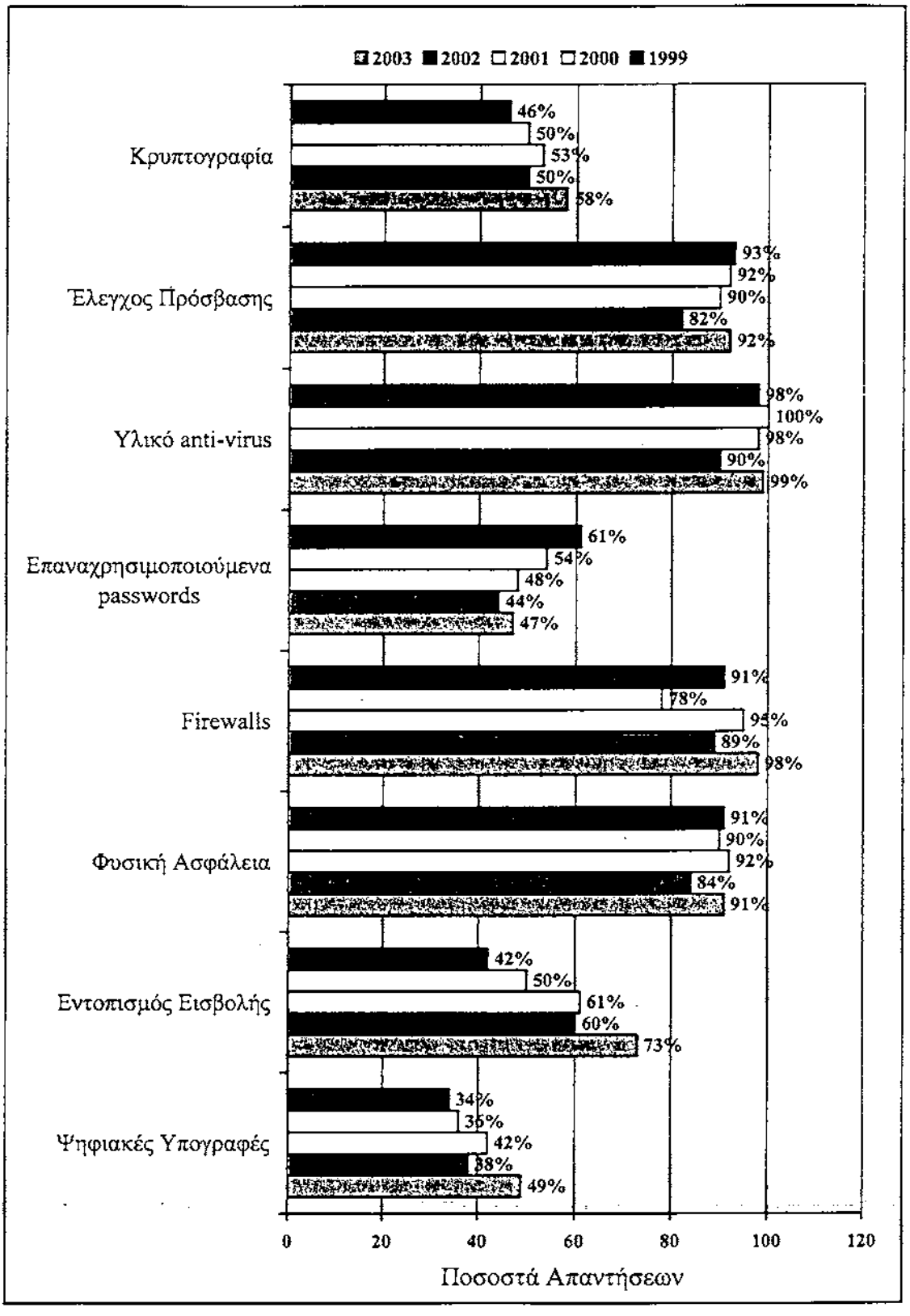
Χρησιμοποιούμενες τεχνολογίες ασφαλείας

Για 6° διαδοχικό έτος, οι συμμετέχοντες στην έρευνα ρωτήθηκαν για τα είδη της τεχνολογικής ασφάλειας που έχουν προσλάβει, για να προστατεύουν τους οργανισμούς τους. Παρ' όλο που στην έρευνα δεν απαντήθηκαν όλες οι απαντήσεις από όλους τους ερωτηθέντες, η ερώτηση που αφορά τη χρήση διαφόρων μορφών τεχνολογίας απαντάται από το 99% (525 από 530) των ερωτηθέντων.

Ουσιαστικά, όλοι οι οργανισμοί χρησιμοποιούν υλικό anti-virus (99%) και firewalls (98%). Όπως θα περίμενε κάποιος, οι περισσότεροι (το 91%) υιοθετούν κάποιου είδους φυσική ασφάλεια για να προστατεύσουν τους υπολογιστές και τις πληροφορίες τους και οι περισσότεροι υιοθετούν κάποια μέτρα ελέγχου πρόσβασης (92%).

Αυτές οι δύο τελευταίες κατηγορίες είναι, ίσως, μια καλή αφορμή για να πούμε κάτι σχετικά με τη φύση αυτών των απαντήσεων. Η ίδια η έρευνα διατηρείται εσκεμμένα πολύ μικρή και έχει παραμείνει σε μεγάλο βαθμό ίδια, κατά τη διάρκεια της οκταετούς της ζωής. Συνεπώς, από τους ερωτηθέντες ζητείται να ερμηνεύσουν ποικίλες πιθανές απαντήσεις της έρευνας, βάσει της δικής τους κατανόησης της βιομηχανικής ασφάλειας και της ορολογίας της. Επί το πλείστον, αυτή είναι μια λογική προσέγγιση- η περισσότερη ορολογία της βιομηχανίας είναι αρκετά τακτοποιημένη ώστε να μη γεννιούνται ερωτήματα σχετικά με το τι σημαίνει όταν η έρευνα ρωτά, για παράδειγμα, εάν χρησιμοποιούνται firewalls. Δεν υπάρχουν αμφιβολίες για το τι είναι ένα firewall.

Χρησιμοποιούμενες Τεχνολογίες Ασφάλειας



2003: 525 απάντησαν (99%)

2002:500 απάντησαν (99%)

2001: 530 απάντησαν (99%)

2000: 629 απάντησαν (97%)

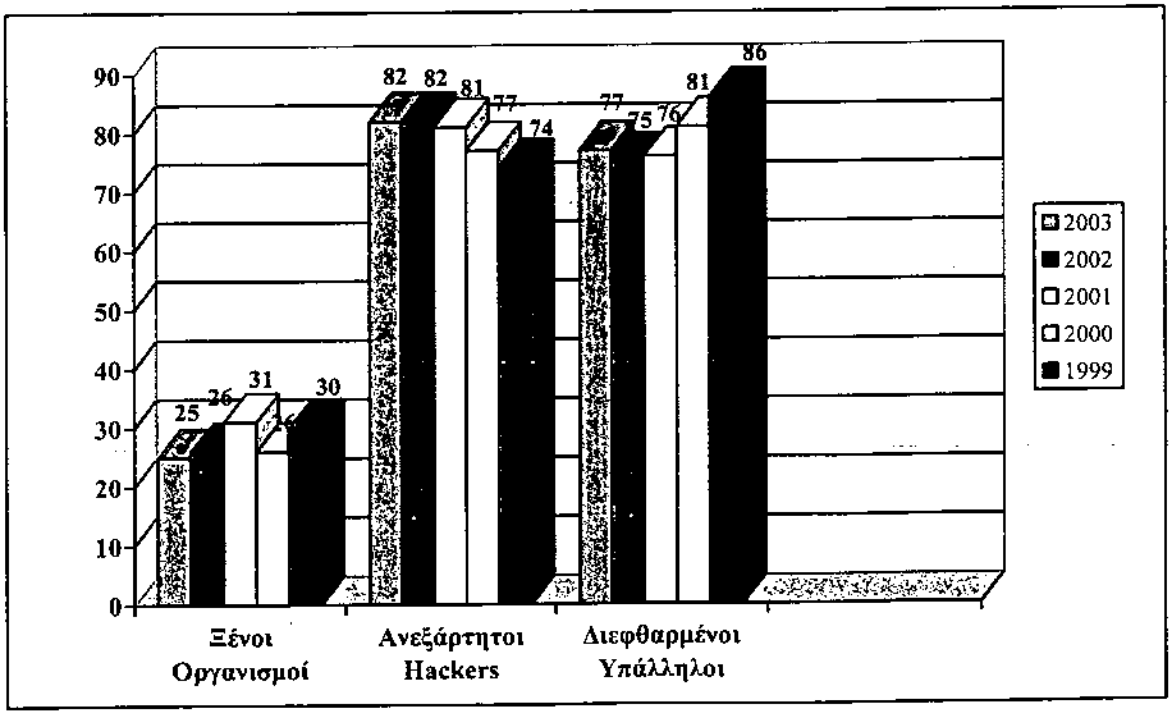
1999: 501 απάντησαν (96%)

Παρ' όλο που ο έλεγχος πρόσβασης είναι μια καλά κατανοητή κατηγορία, διεγείρει μια σειρά ερωτήσεων. Θα περιμέναμε πως κάθε οργανισμός που ζητά από τους χρήστες κάποιο password για την είσοδό του στο σύστημα, θα απαντούσε καταφατικά. Έτσι, ξανά είναι ενδιαφέρον που το 8% των απαντηθέντων λένε «όχι», στο ότι δεν υιοθετούν έλεγχο πρόσβασης. Από τους 48 απαντηθέντες που είπαν ότι δεν χρησιμοποιούν έλεγχο πρόσβασης, μόνο οι 6 είπαν ότι παρήγαγαν εισοδήματα παραπάνω του ενός εκατομμυρίου δολαρίων, με 2 από αυτούς να απαντούν ότι χρησιμοποίησαν επαναχρησιμοποιούμενα passwords. Αντιθέτως, 23 (ή σχεδόν οι μισοί) από τους απαντηθέντες που είπαν ότι δεν χρησιμοποιούν έλεγχο πρόσβασης, προέρχονταν από οργανισμούς με εισόδημα λιγότερο των $100 εκατομμυρίων.

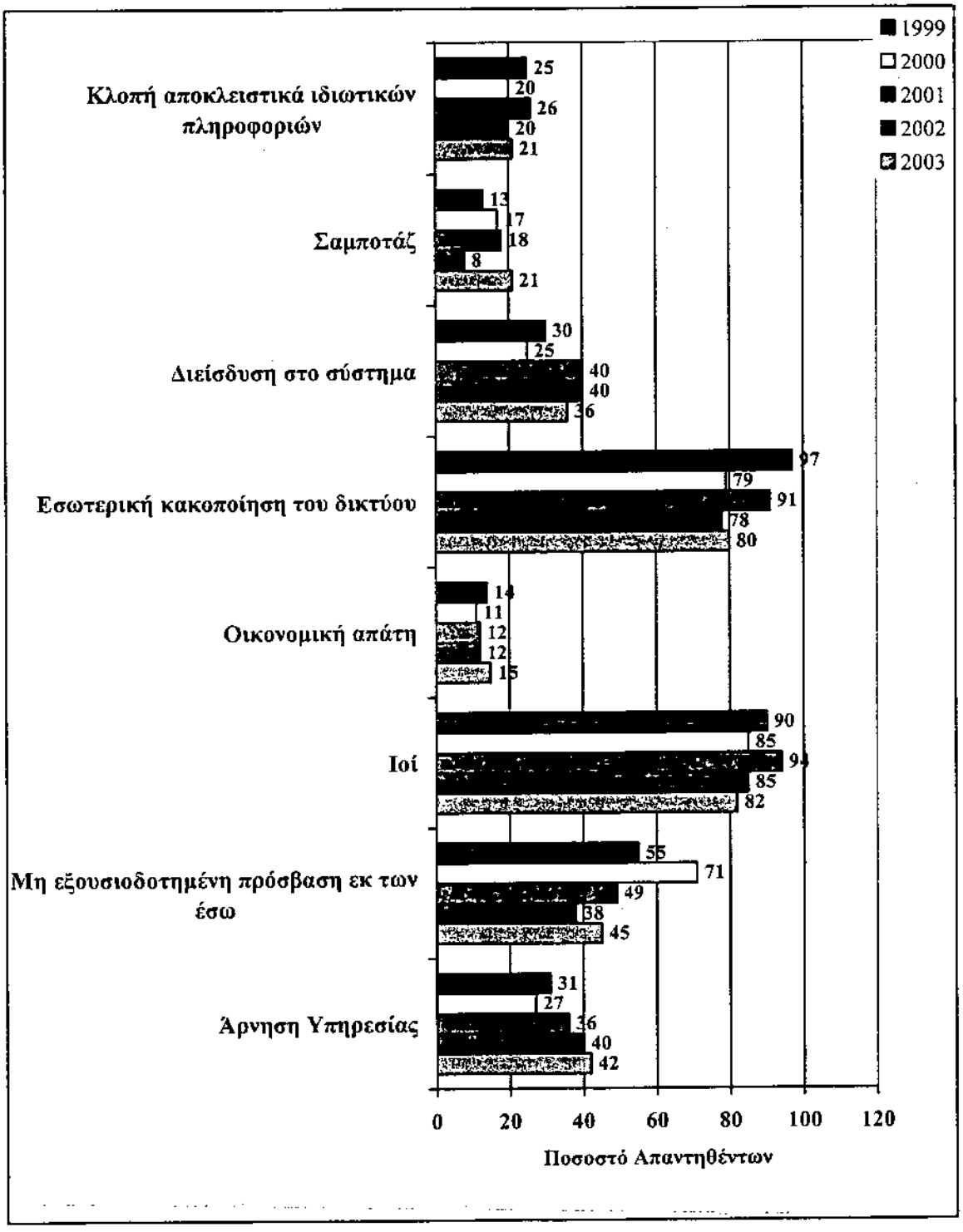
Προφανώς, αυτοί που δεν χρησιμοποιούν έλεγχο πρόσβασης έχουν πάρει τις αποφάσεις τους περί ασφάλειας με κατάλληλη διορατικότητα: δεν είναι ανάμεσα σε αυτούς που αναφέρουν οικονομικές απώλειες. Πραγματικά, κανείς από αυτούς τους 48 απαντηθέντες δεν αναφέρει μια σημαντική οικονομική απώλεια ιδιωτικών πληροφοριών.

Ανεξάρτητα από τα χρησιμοποιούμενα εργαλεία, το θέμα εξακολουθεί να είναι ότι πολλοί απαντηθέντες πολύ απλά δεν γνωρίζουν τι συμβαίνει με τα δίκτυά τους. 15% των απαντηθέντων δηλώνει ότι δεν γνωρίζει εάν υπήρξε κάποια μη εξουσιοδοτημένη χρήση του συστήματός τους κατά το τελευταίο έτος. Αυτό είναι ενοχλητικό, θα έλεγε κανείς. Ταυτόχρονα, παρ' όλ' αυτά, είναι περίπου το ίδιο ποσοστό όπως συνήθως: ο μέσος όρος για τα 7 τελευταία χρόνια της έρευνας ήταν ότι ένα 16.3% δε γνώριζε.

Πιθανές Πηγές Επίθεσης



Είδη επιθέσεων ή κακομεταχείρισης που εντοπίστηκαν τους τελευταίους 12 μήνες (έτος 2003)



2003: 490 απαντήσεις (92%)

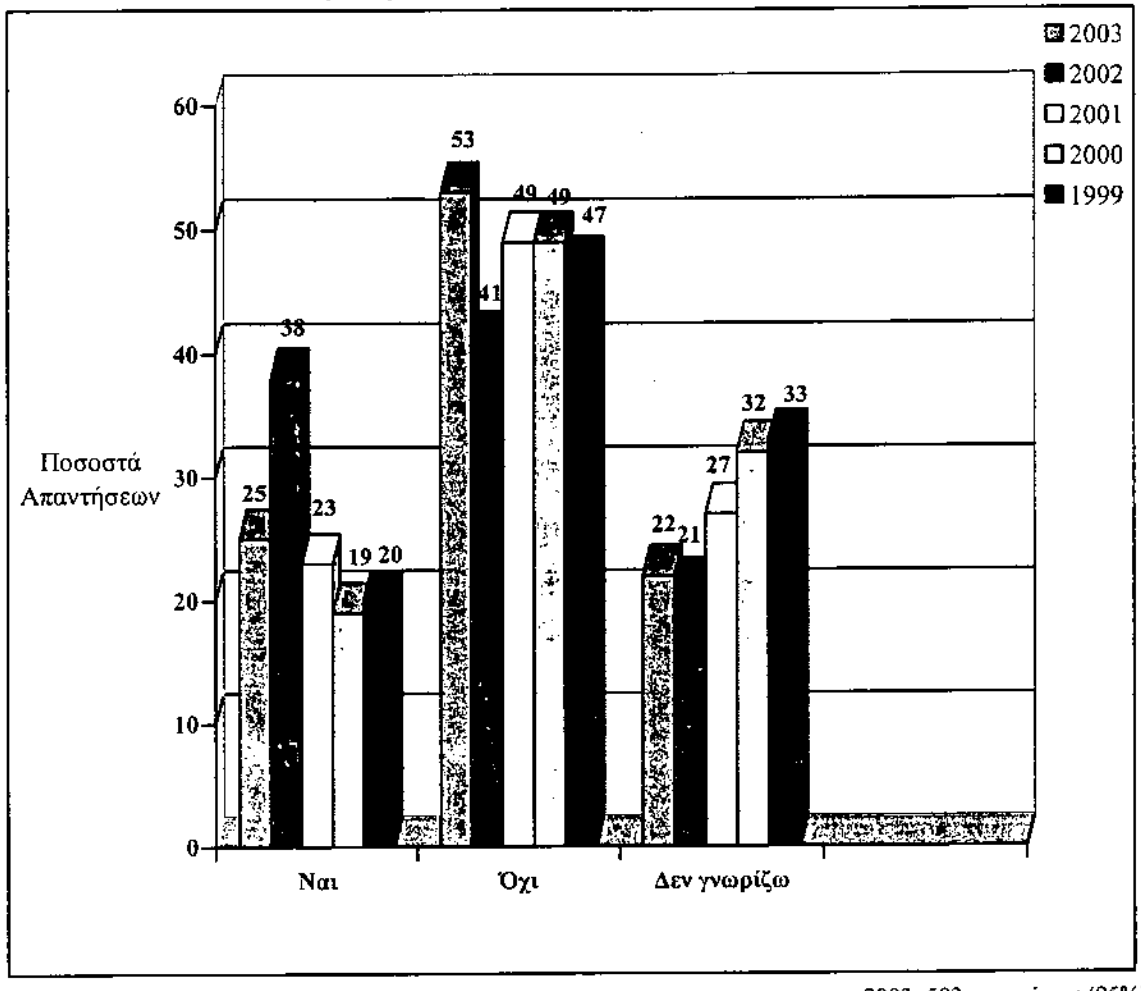
2002: 455 απαντήσεις (90%)

2001: 484 απαντήσεις (91%)

2000: 580 απαντήσεις (90%)

1999: 480 απαντήσεις (89%)

Έχει το WWW site σας υποστεί μη εξουσιοδοτημένη πρόσβαση ή κακομεταχείριση κατά τη διάρκεια των τελευταίων 12 μηνών;



2003: 503 απαντήσεις (95%)
2002: 472 απαντήσεις (94%)
2001: 509 απαντήσεις (95%)
2000: 603 απαντήσεις (90%)
1999: 479 απαντήσεις (92%)

Οικονομική απάτη

Η έρευνα πρώτα ρώτησε για τις απώλειες που οφείλονταν στην οικονομική απάτη το 1997, κατά την οποία 12% των απαντηθέντων γνωστοποίησαν οικονομική απάτη. Αυτού του έτους (2003) το 15% που αναφέρει οικονομική απάτη, είναι το υψηλότερο επίπεδο που έχει καταγραφεί στην ιστορία της έρευνας, αλλά είναι μόνο 1% υψηλότερο από το προηγούμενο «ρεκόρ», που δηλώθηκε το 1999. Έτσι, ενώ είναι πιθανό ότι η αύξηση σηματοδοτεί την αρχή μιας ανοδικής τάσης, φαίνεται κατά κάποιο τρόπο πιο πιθανό η κλίμακα των απωλειών από οικονομικές απάτες να παραμένει λιγότερο συνεχής, ταλαντευόμενη γύρω στο 13 με 14%.

Αυτό που προκαλεί πραγματική έκπληξη στα νούμερα της οικονομικής απάτης αυτό το χρόνο, παρ' όλ' αυτά, είναι οι αναφερόμενες οικονομικές απάτες, οι οποίες φτάνουν μετά βίας

το 1/10 αυτών που αναφέρθηκαν τον προηγούμενο χρόνο. Πιθανότατα, δεν είναι λογικό να υποθέσουμε ότι κάτι τέτοιο καλύπτει όλο το εύρος των επιχειρήσεων των Ηνωμένων Πολιτειών, αλλά σίγουρα μπορεί να είναι η περίπτωση όπου το δείγμα στην έρευνα έχει απολαύσει μια εμπειρία καλύτερη του μέσου όρου κατά το προηγούμενο έτος. Ενώ 15% των απαντηθέντων αναφέρουν οικονομική απώλεια -ελαφρώς μεγαλύτερο ποσοστό σε σύγκριση με τα προηγούμενα έτη- είναι επίσης η υπόθεση ότι η πιο μεγάλη αναφερόμενη απώλεια ήταν $4 εκατομμύρια. Αυτό είναι ένα μέρος της μεγαλύτερης αναφερόμενης οικονομικής απώλειας του περασμένου έτους, η οποία ήταν $50 εκατομμύρια. Αυτό το μοναδικό περιστατικό του προηγούμενου έτους, ήταν σχεδόν πέντε φορές υψηλότερο από όλες τις αναφερόμενες απώλειες που οφείλονταν σε οικονομική απάτη, για αυτό το έτος (2003).

Όπως θα περίμενε κάποιος, ο μέσος όρος των απωλειών από οικονομική απάτη αυτό το έτος, σε αντιστοιχία με αυτόν του προηγούμενου έτους, ήταν χαμηλότερος. Ο μέσος όρος των $328.594 αυτού του έτους ήταν κυριολεκτικά εκατομμύρια λιγότερος από τα προηγούμενα τρία έτη, όταν οι μέσοι όροι ήταν $4.632.000 το 2002, $4.420.738. το 2001 και $1.646.941 το 2000.

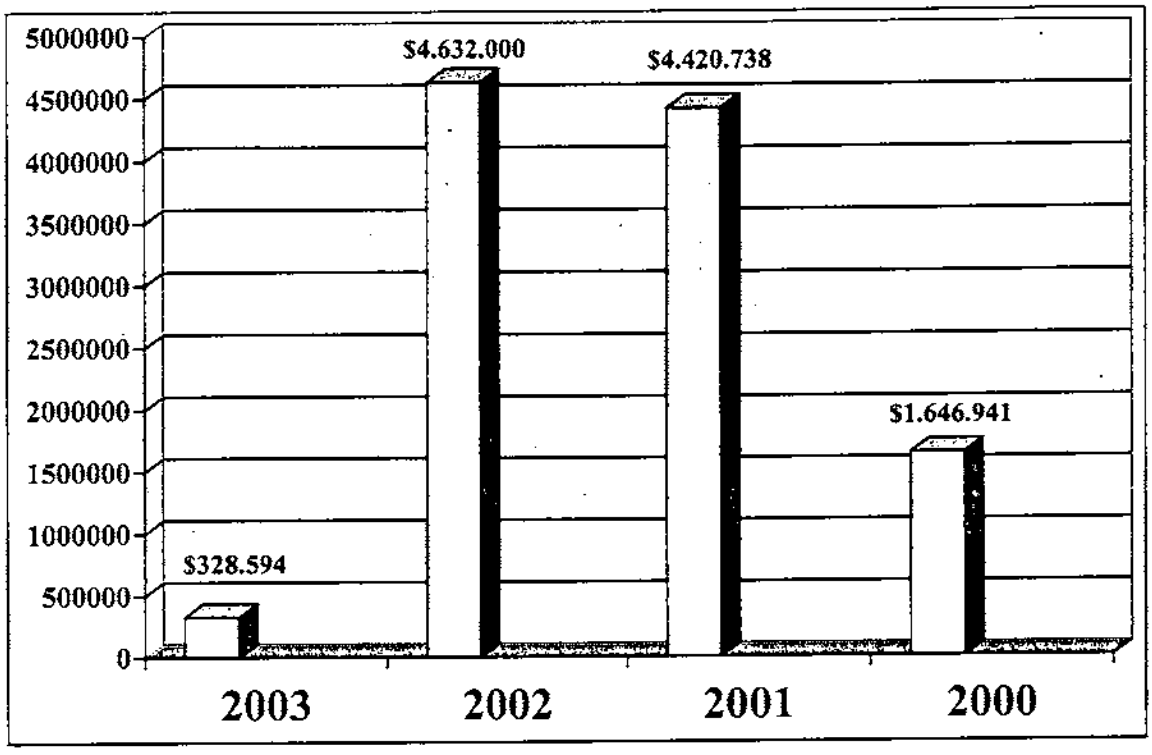
Πόσα περιστατικά; Πόσα από έξω; Πόσα από μέσα;

Πόσα περιστατικά;						
Ανά ποσοστό (%)	1 έως 5	6 έως 10	11 έως 30	31 έως 60	>από 60	Δεν ξέρω
2003	38	20	>από 16	0	0	26
2002	42	20	8	2	5	23
2001	33	24	5	1	5	31
2000	33	23	5	2	6	31
1999	34	22	7	2	5	29
2003: 355 απαντήσεις, 2002: 321 απαντήσεις, 2001: 348 απαντήσεις, 2000: 392 απαντήσεις, 1999: 327 απαντήσεις						
Πόσα από έξω;						
Ανά ποσοστό (%)	1 έως 5	6 έως 10	11 έως 30	31 έως 60	>από 60	Δεν ξέρω
2003	46	10	13	0	0	31
2002	49	14	5	0	4	27
2001	41	14	3	1	3	39
2000	39	11	2	2	4	42
1999	43	8	5	1	3	39
2003:336 απαντήσεις, 2002: 301 απαντήσεις, 2001: 316 απαντήσεις, 2000: 341 απαντήσεις, 1999: 280 απαντήσεις						
Πόσα από μέσα;						
Ανά ποσοστό (%)	1 έως 5	6 έως 10	11 έως 30	31 έως 60	>από 60	Δεν ξέρω
2003	45	11	12	0	0	33
2002	42	13	6	2	1	35
2001	40	12	3	0	4	41
2000	38	16	5	1	3	37
1999	37	16	9	1	2	35
2003: 328 απαντήσεις, 2002:299 απαντήσεις, 2001: 348 απαντήσεις, 2000:392 απαντήσεις, 1999: 327 απαντήσεις						

CSI/FBI 2003 Computer Crime Security Survey

Source: Computer Security Service

Απώλειες που οφείλονταν σε οικονομική απάτη



Πού βρίσκουμε πραγματογνωμοσύνη;

Μία από τις υφιστάμενες διαμάχες στην προστασία των πληροφοριών αφορά την αποτελεσματικότητα της πρόσληψης hacker που ισχυρίζονται ότι έχουν αναμορφωθεί. Το έτος 2002 ήταν πολύ ενδιαφέρον, όσον αφορά αυτή την άποψη, επειδή είδε την επιστροφή στο ενεργό (νόμιμο) καθήκον ενός εκ των πιο γνωστών hacker της κοινωνίας, του Kevin Mitnick. Μετά τη σύλληψη και καταδίκη του το 1995 για σειρά εγκλημάτων με Η/Υ, αφήνεται ελεύθερος το 2000. Πολυάριθμοι περιορισμοί βάσει της ελευθέρωσής του τον κράτησαν σε ησυχία για λίγο, αλλά το 2002 δημοσίευσε ένα βιβλίο πάνω στην κοινωνική μηχανική επιστήμη, που λεγόταν *Η τέχνη της απάτης*, και ξεκίνησε μια εταιρεία συμβούλων, την *Αμυντική Σκέψη*. Η σκέψη μεταξύ των περισσοτέρων από τους απαντηθέντες της έρευνας, παρ' όλ' αυτά, φαίνεται να είναι ότι η καλύτερη άμυνα είναι η σαφής κατεύθυνση των αναμορφωμένων hackers.

Το επιχείρημα απέναντι στους ασκούντες την ασφάλεια φαίνεται να είναι το ότι οι hackers μπορεί να αναμορφώνουν τους εαυτούς τους, αλλά δεν υπάρχει αναγκαστικός λόγος για να στηριχτούμε σε αυτό το γεγονός, δεδομένου ότι υπάρχουν πολλοί ειδικευμένοι εξασκούντες το επάγγελμα που δεν έχουν σχέση με τους hackers. Όντως, μπορεί να θολώσει τα νερά το γεγονός ότι μερικοί hackers έχουν καταδικαστεί, όταν πολλοί άλλοι διαπράττουν

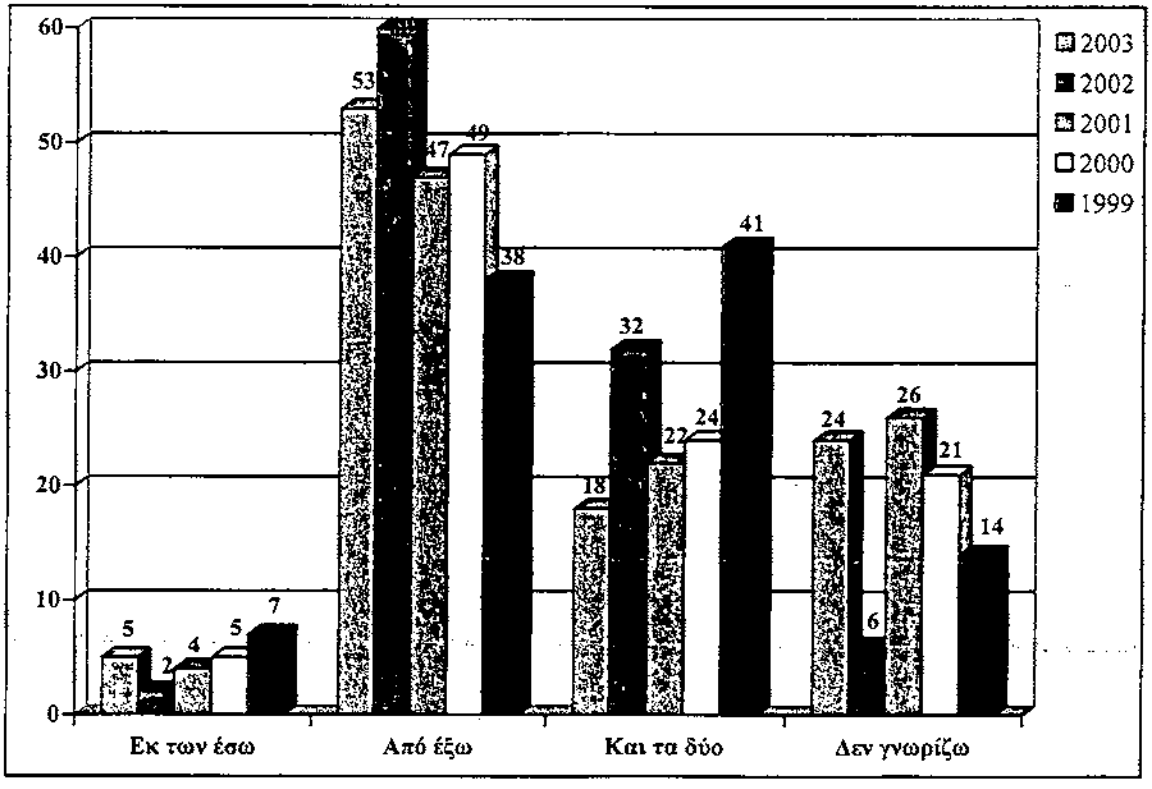
τα ίδια εγκλήματα χωρίς να συλληφθούν, και συνεπώς μπορεί να παρουσιάζει καθαρά διαπιστευτήρια. Και ναι, μπορεί να είναι πιθανό μια επιχείρηση να προσλάβει πρώην hackers σε πόστα όπου δεν τους αναθέτονται προσβάσεις σε ευαίσθητα παραγωγικά συστήματα. Αλλά οι περισσότεροι απαντηθέντες δεν φαίνεται να αγχώνονται και πολύ γι' αυτές τις διακρίσεις.

Η έρευνα ρωτά για το αν οι απαντηθέντες θα σκέφτονταν σοβαρά να προσλάβουν έναν αναμορφωμένο hacker και οι απαντήσεις είναι εμφατικές. Οι απαντηθέντες συνηθίζουν να απαντούν σε αυτή την ερώτηση με υπεκφυγές, και σημειώνουν κακογραφίες στο περιθώριο του να υποστηρίξουν την θέση τους (αυτό δε συμβαίνει πουθενά αλλού στην έρευνα).

Μόνο 15% λέει ότι θα προσλάμβανε πρώην hackers. Αντιθέτως, 68% λένε ότι δε θα το έκαναν, με 17% να μην είναι σίγουροι για τη θέση τους σχετικά με το θέμα.

Σαν γενική υπόθεση, παρ' όλ' αυτά, θα φαινόταν ότι το να έχεις συλληφθεί και επιτυχώς καταδικαστεί σαν εγκληματίας των υπολογιστών, *δεν είναι* σίγουρο εισιτήριο για μετέπειτα επιτυχία στην βιομηχανία της ασφάλειας, καθώς τα ¾ της αγοράς θα προτιμούσε καλύτερα να μη σε προσλάβει.

Θα σκεφτόταν ο Οργανισμός σας να προσλάβει αναμορφωμένους Hackers σαν συμβούλους;



Σχετικά με την έρευνα

Η έρευνα για τα Εγκλήματα των Υπολογιστών και την Ασφάλεια (CSI/FBI), ιστορικά έχει υπάρξει μια ελαφρώς ανεπίσημη δέσμευση, και δεν αποτελεί εξαίρεση για αυτό το έτος. Στόχος της είναι να αυξήσει τον προβληματισμό σχετικά με την ασφάλεια, να προωθήσει πληροφορίες για την προστασία και να ενθαρρύνει τη συνεργασία μεταξύ της εφαρμογής του νόμου και του ιδιωτικού τομέα.

Ανεπίσημα παρ' όλ' αυτά, υπάρχουν λόγοι ύπαρξης ενός βαθμού εμπιστοσύνης στη στατιστική αυστηρότητα των ευρημάτων της έρευνας. Πρώτον, η ίδια έρευνα έχει εκτελεστεί για οκτώ συνεχόμενα χρόνια και τα αποτελέσματα αυτού του έτους είναι φυσικά ιδιαιτέρως εύλογα όταν συγκρίνονται με μέσους όρους και κατευθυντήριες γραμμές προηγούμενων ετών.

Ένα δεύτερο σημείο, σημείο έχει να κάνει με τη φύση του δείγματος που χρησιμοποιείται σε αυτή την έρευνα. Είναι σίγουρα αληθές το ότι οι δείκτες της έρευνας δεν επιλέγονται στην τύχη. Προέρχονται από μια ομάδα επαγγελματιών της ασφάλειας και, ανάμεσα σε αυτό το ευρύτερο γκρουπ, επιλέγονται από μόνοι τους.

Εάν ρωτήσουμε ποιο θα είναι το αποτέλεσμα αυτού του είδους επιλογής, παρ' όλ' αυτά, φαίνεται πιθανό ότι δεν θα υποτιμά την εγκυρότητα όσων αναφέρονται. Αυτοί είναι άνθρωποι που δίνουν μεγάλη προσοχή στις καταστάσεις ασφάλειας και τις εμπειρίες των οργανισμών τους. Είναι σαφώς σε καλύτερη θέση από τους περισσότερους, με άλλα λόγια, το να ξέρουν τι περιστατικά έχουν υποστεί τα προηγούμενα χρόνια. Δεν είναι πάντα εμφανές το ότι ένα σύστημα Η/Υ έχει δεχθεί επίθεση -σημειώστε σαν απόδειξη αυτού ότι το 22% των απαντηθέντων δεν γνωρίζει εάν τα Web sites τους έχουν δεχθεί επίθεση από hackers κατά το προηγούμενο έτος- έτσι, δικαιολογείται το ότι αυτοί που δίνουν μεγάλη προσοχή μπορούν να παρέχουν καλύτερα ενημερωμένες απαντήσεις από αυτούς που δεν προσέχουν.

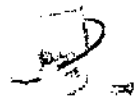
Βέβαια, είναι επίσης πιθανό ότι αυτή η ομάδα ατόμων να έχει κάποιο λόγο που μεγαλοποιεί τις απώλειές της, χρησιμοποιώντάς τις σαν τρόπο άμυνάς τους προς τα αφεντικά τους όταν τα κέρδη του οργανισμού όπου εργάζονται μειώνονται.. Ενώ αυτό θα φαινόταν πιθανό στα χρόνια όπου οι συνολικές οικονομικές απώλειες κινούνταν αμείλικτα ανοδικά, εν τούτοις είναι δυσκολότερο να υποστηριχθεί αυτή η θεωρία, δεδομένου της σημαντικής πτώσης στις αναφερόμενες απώλειες στη φετινή έρευνα. Εκτός αυτού, η «αυτοενδιαφερόμενη» θεωρία (εάν μπορούμε να την αποκαλέσουμε έτσι) είναι κτισμένη στην ιδέα ότι οι απαντηθέντες έχουν κάποιου είδους ικανότητα να πλαστοποιούν τους αριθμούς και να κινούνται σε αυτή την ιδέα. Εάν ήταν έτσι τα πράγματα, κάποιος θα περίμενε από τους περισσότερους απαντηθέντες να αναφέρουν απώλειες στις περισσότερες από τις κατηγορίες των ερωτήσεων (και γιατί άλλωστε να μην ωθήσουν προς τα πάνω όλες τις απώλειες;). Αλλά δεν είναι έτσι οι ατομικές απαντήσεις

-οι περισσότεροι απαντηθέντες δηλώνουν μόνο τρεις ή τέσσερις κατηγορίες όπου σημειώνονται απώλειες. Επιπλέον, ιδιαιτέρως πολλοί απαντηθέντες υποστηρίζουν ποικίλα είδη επιθέσεων παρά αναφέρουν το ύψος των απωλειών που προήλθαν από αυτές τις επιθέσεις. Κάποιος θα περίμενε κάθε επίθεση να έχει και μία αξία εάν το συμπεριληπτικό ενδιαφέρον γέμιζε τα νούμερα.

Υποθέτοντας ότι οι απαντηθέντες είναι τίμιοι και τα νούμερα νόμιμα, το βασικό πρόβλημα των ερευνών εξακολουθεί να υπάρχει -ποτέ δεν είναι όσο αδιάσειστες όσο θα τις ήθελες. Αυτή η έρευνα, όπως και πολλές άλλες, είναι κατά το πλείστο μια σειρά στιγμιότυπων του πως οι άνθρωποι βλέπουν τις καταστάσεις τους σε συγκεκριμένη στιγμή, εν ώρα υπηρεσίας.

Η CSI προσφέρει τα αποτελέσματα της έρευνας για δημόσια εξυπηρέτηση και μπορεί κανείς να τα βρει στο www.gocsi.com).

Ε' Μέρος



Παράρτημα

Ποιες είναι οι κυριότερες μορφές ηλεκτρονικών συναλλαγών που διενεργούν οι εταιρείες;

Οι περισσότερες εταιρείες, ακόμη και αν δεν ασχολούνται αμιγώς με το ηλεκτρονικό εμπόριο, πραγματοποιούν ήδη συναλλαγές μέσω του Internet με διάφορους τρόπους, όπως ενδεικτικά:

- Με την ανταλλαγή ηλεκτρονικών μηνυμάτων μέσω e-mail με τους συνεργάτες τους, και τους προμηθευτές τους (για να δώσουν κάποια εντολή, να κάνουν κάποια παραγγελία κλπ).
- Με την αποστολή ηλεκτρονικών μηνυμάτων στους καταναλωτές/πελάτες τους, με στόχο την εμπορική επικοινωνία.
- Με την απλή παρουσίαση των προϊόντων/υπηρεσιών τους μέσω μιας ιστοσελίδας στο Διαδίκτυο, έστω και αν η σελίδα αυτή υφίσταται απλώς για διαφημιστικούς σκοπούς, χωρίς να πραγματοποισύνται (ακόμα) πωλήσεις.
- Με τη διασύνδεσή τους στον Παγκόσμιο Ιστό, απλά και μόνο για την απόκτηση ηλεκτρονικής διεύθυνσης για την διοίκηση, τους υπαλλήλους κλπ.
- Με την ολοένα και αυξανόμενη διεκπεραίωση συναλλαγών με τον ευρύτερο δημόσιο τομέα (πχ ΔΟΥ, ΙΚΑ κλπ).

Γίνεται επομένως αντιληπτό, ότι είναι απαραίτητο να γνωρίσει ο εμπορικός κόσμος τις ρυθμίσεις που διέπουν τις ηλεκτρονικές συναλλακτικές τους σχέσεις. Το Διαδίκτυο έχει πάψει προ πολλού να αποτελεί έναν άναρχο και εντελώς ανασφαλή χώρο για τη διενέργεια συναλλαγών. Σταδιακά δημιουργούνται τα νόμιμα μέτρα και σταθμά που ρυθμίζουν τις ηλεκτρονικές συναλλακτικές σχέσεις, αυξάνοντας έτσι την εμπιστοσύνη των χρηστών. Η δημιουργία, εξάλλου, σταθερής νομικής υποδομής συνάδει και με τη φυσική ανάγκη των εταιρειών να μπορούν να προβλέπουν κατά το δυνατό τις συνέπειες των πράξεών τους και να μην εκτίθενται σε ένα επικίνδυνο περιβάλλον.

Νομικό πλαίσιο για τις ηλεκτρονικές συναλλαγές

Ένας από τους σημαντικότερους παράγοντες που συντέλεσε στη συρρίκνωση της επιχειρηματικότητας στο Διαδίκτυο, ήταν η έλλειψη ξεκάθαρων νομοθετικών ρυθμίσεων για ζωτικά θέματα των ψηφιακών συναλλαγών. Η απότομη τεχνολογική ανάπτυξη και η αρχική ραγδαία εξάπλωση του ηλεκτρονικού εμπορίου βρήκαν απροετοίμαστη τη νομοθεσία σε παγκόσμιο επίπεδο, η οποία αποδείχθηκε ελλιπής και αδύναμη να προσαρμοστεί τόσο γρήγορα στα νέα δεδομένα.

Η ίδια η φύση του Διαδικτύου είναι η αιτία που προκάλεσε το μεγάλο αυτό νομικό κενό. Τα κυριότερα χαρακτηριστικά του, τα οποία εμποδίζουν την καθολική εφαρμογή της

ισχύουσας νομοθεσίας και την επίκληση της υπάρχουσας νομολογίας στις ηλεκτρονικές συναλλαγές, είναι:

- Η παγκόσμια παρουσία του Internet, που καταλύει τα σύνορα και δημιουργεί μια νέα, κοινή αγορά, προσβάσιμη από κάθε πλευρά του πλανήτη και έρχεται σε κατάφορη αντίθεση με την εδαφικότητα των νομοθετικών ρυθμίσεων (κάθε χώρα έχει το δικό της δίκαιο που ρυθμίζει με διαφορετικό τρόπο τις έννομες σχέσεις).
- Η αποϋλοποίηση όλων των αντικειμένων, εφόσον τα πάντα μετατρέπονται, πλέον, σε δεδομένα τα οποία μεταφέρονται στον Παγκόσμιο Ιστό σε ηλεκτρονική μορφή (bits και bytes). Επομένως, παύει να υπάρχει η παραδοσιακή έννοια του «πράγματος» και δημιουργείται ένα καινούριο αγαθό που χρήζει ιδιαίτερης νομικής προστασίας.
- Η χρησιμοποίηση της τεχνολογίας σε όλο ή στο μεγαλύτερο κομμάτι της συναλλαγής που τροποποιεί πλήρως τα υφιστάμενα συναλλακτικά ήθη. Παράλληλα αποκλείεται η σύγκριση με παλαιότερες πρακτικές και η αναλογική εφαρμογή προγενέστερων δικαστικών αποφάσεων καθότι, συνήθως, η συναλλαγή διενεργείται με εντελώς καινούριο τρόπο χωρίς να υπάρχει συγκρίσιμο προηγούμενο.

Άρα, ενώ δεν καθίστανται πλήρως ανενεργείς οι ισχύουσες νομικές διατάξεις, οι περισσότερες από αυτές δεν είναι σε θέση να ανταποκριθούν στις ανάγκες και στις τεχνικές προδιαγραφές του κυβερνοχώρου, με αποτέλεσμα πρακτικά να είναι ανεφάρμοστες και παρωχημένες.

Όπως ήταν λογικό, το γεγονός αυτό προκάλεσε ανασφάλεια δικαίου που όχι μόνον φόβισε το, ούτως ή άλλως, δικαστικό καταναλωτικό κοινό, αλλά συνέβαλε και στην αναδίπλωση των εταιρειών που θέλησαν να πρωτοπορήσουν στο συγκεκριμένο χώρο. Εξάλλου, ποιος επιθυμεί να συναλλάσσεται χρησιμοποιώντας ένα μέσο χωρίς καν να γνωρίζει ποια είναι ακριβώς τα δικαιώματα και οι υποχρεώσεις των μερών και από πότε ξεκινούν.

Η Ευρωπαϊκή και Ελληνική Νομοθεσία για τις ηλεκτρονικές συναλλαγές σήμερα

Μέσα στο πλαίσιο αυτό, η Ευρωπαϊκή Ένωση πραγματοποιεί σταδιακά μια συντονισμένη προσπάθεια αντιμετώπισης του προβλήματος, θέλοντας να θέσει σταθερές νομικές βάσεις που να δημιουργούν ένα δίχτυ ασφαλείας για τις ηλεκτρονικές συναλλαγές. Βασικός γνώμονας είναι η αύξηση των συναλλαγών (εμπορικών και μη) στο Internet με τις απαραίτητες, όμως, υποδομές που να αποδίδουν την κατάλληλη νομική ισχύ σε κάθε επίπεδο ηλεκτρονικής συναλλαγής, ενώ παράλληλα να ανοίγουν το δρόμο για την πλήρη αποδοχή τους.

Η Ελληνική έννομη τάξη προσπαθεί να προσαρμοστεί στις προσταγές της νέας εμπορικής πραγματικότητας κυρίως με την προσαρμογή των ευρωπαϊκών νομοθετημάτων στο εσωτερικό δίκαιο. Παρόλο που παρουσιάζεται γενικά μια καθυστέρηση στην υιοθέτηση κάποιων επιμέρους Οδηγιών και σε πολλά σημεία χρειάζεται η δημιουργία πιο λεπτομερειακών ρυθμίσεων, αρχίζει και παίρνει μορφή το νομοθετικό εκείνο καθεστώς που να αρμόζει στο ηλεκτρονικό εμπόριο. Η ειδική νομοθεσία, σε συνδυασμό με τις προγενέστερες γενικές διατάξεις παρέχουν, στις μέρες μας, τη βάση για την προστασία των ηλεκτρονικών συναλλαγών, ενώ παράλληλα τις αναγνωρίζουν ως νόμιμη συναλλακτική πρακτική (με ελάχιστες εξαιρέσεις).

Το κυρίως ζητούμενο σε αυτό το στάδιο είναι η έκδοση από τις Αρμόδιες Αρχές, όπως Ανεξάρτητες Διοικητικές Αρχές, Υπουργεία, ΝΠΔΔ κα, των εξειδικευμένων εκείνων κανονισμών που θα δώσουν ώθηση στην ευρεία εφαρμογή των ηλεκτρονικών συναλλαγών. Παράλληλα, η περαιτέρω διάδοση των ηλεκτρονικών συναλλαγών θα καθορίσει τα νέα «ηλεκτρονικά» συναλλακτικά ήθη. Εξάλλου, με ενδιαφέρον αναμένονται και οι δικαστικές αποφάσεις που θα δώσουν το στίγμα για το πώς αντιμετωπίζει η νομολογία τις ηλεκτρονικές συναλλαγές και πώς ερμηνεύουν τα δικαστήρια τις σχετικές νομοθετικές ρυθμίσεις.

Κοινοτικό πρόγραμμα δράσης για την προώθηση της ασφαλούς χρήσης του Internet:

1. Στόχος

Η ενθάρρυνση της δημιουργίας ενός περιβάλλοντος που να ευνοεί την ανάπτυξη της βιομηχανίας που συνδέεται με το Διαδίκτυο, προωθώντας την ασφαλή χρήση του και καταπολεμώντας το παράνομο και βλαβερό περιεχόμενό του.

2. Πράξη

Απόφαση αριθ.276/1999/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 25ης Ιανουαρίου 1999, για ένα πολυετές πρόγραμμα δράσης για την προώθηση της ασφαλέστερης χρήσης του Internet μέσω της καταπολέμησης του παράνομου και βλαβερού περιεχομένου στα παγκόσμια δίκτυα [Επίσημη Εφημερίδα L33, 06.02.1999].

3. Σύνοψη

Ορισμοί

Το «παράνομο περιεχόμενο» σχετίζεται με μια μεγάλη ποικιλία ζητημάτων (εθνική ασφάλεια, προστασία ανηλίκων, προστασία ανθρώπινης αξιοπρέπειας, οικονομική ασφάλεια, προστασία πληροφοριών, προστασία ιδιωτικής ζωής, προστασία φήμης, πνευματική ιδιοκτησία).

«Βλαβερό περιεχόμενο» σημαίνει τόσο περιεχόμενο που επιτρέπεται, αλλά του οποίου η διανομή είναι περιορισμένη (για παράδειγμα μόνο για ενήλικες) όσο και περιεχόμενο που

μπορεί να ενοχλήσει ορισμένους χρήστες, αν και η δημοσίευσή του δεν είναι περιορισμένη λόγω της αρχής της ελευθερίας της έκφρασης.

Η διάκριση μεταξύ παράνομου και βλαβερού περιεχομένου είναι σημαντική, διότι οι δύο κατηγορίες αντιμετωπίζονται διαφορετικά:

- Το παράνομο περιεχόμενο πρέπει να αντιμετωπίζεται στην πηγή από τις αστυνομικές και δικαστικές αρχές, οι δραστηριότητες των οποίων καλύπτονται από τους κανόνες της εθνικής νομοθεσίας και τις συμφωνίες δικαστικής συνεργασίας. Η βιομηχανία πάντως μπορεί να προσφέρει σημαντική βοήθεια για τη μείωση της κυκλοφορίας παράνομου περιεχομένου (ιδιαίτερα περιεχομένου σχετικού με παιδική πορνογραφία, ρατσισμό και αντισημιτισμό) μέσω της θέσπισης αποτελεσματικών μηχανισμών αυτορύθμισης, που θα διέπονται και θα υποστηρίζονται από νομικές διατάξεις και θα έχουν την υποστήριξη των καταναλωτών.
- Για την αντιμετώπιση του βλαβερού περιεχομένου, οι δράσεις προτεραιότητας θα πρέπει να είναι: η παροχή στους χρήστες της δυνατότητας να αρνούνται το βλαβερό περιεχόμενο με την ανάπτυξη τεχνολογικών λύσεων (συστήματα φιλτραρίσματος και βαθμολόγησης περιεχομένου), η αύξηση της ευαισθητοποίησης των γονέων και η ανάπτυξη της αυτορύθμισης, η οποία μπορεί να προσφέρει ένα επαρκές πλαίσιο, ιδιαίτερα για την προστασία των ανηλίκων.

Προστασία των πληροφοριών και των δεδομένων προσωπικού χαρακτήρα (δημόσια ψηφιακά δίκτυα τηλεπικοινωνιών):

1. Στόχος

Η διατήρηση του δικαιώματος στην ιδιωτική ζωή, όσον αφορά την επεξεργασία δεδομένων προσωπικού χαρακτήρα στον τομέα των ηλεκτρονικών επικοινωνιών.

2. Πράξη

Οδηγία 2002/58/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 12ης Ιουλίου 2002, σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών (οδηγία για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες) [Επίσημη Εφημερίδα αριθ.L201, 31η Ιουλίου 2002].

3. Σύνοψη

Η Οδηγία 2002/58/ΕΚ αποτελεί μέρος της δέσμης ρυθμίσεων για τις τηλεπικοινωνίες και συνιστά τη νέα νομοθετική πράξη που θα καλύψει τον τομέα των ηλεκτρονικών επικοινωνιών και θα αντικαταστήσει την υφιστάμενη νομοθεσία που διέπει τον τομέα τηλεπικοινωνιών. Η

δέσμη ρυθμίσεων για τις τηλεπικοινωνίες περιλαμβάνει τέσσερις ακόμα οδηγίες για το γενικό πλαίσιο, την πρόσβαση και την διασύνδεση, τις εξουσιοδοτήσεις και τις άδειες καθώς και για τις παγκόσμιες υπηρεσίες.

Η παρούσα οδηγία καταργεί την οδηγία 97/66/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 15ης Δεκεμβρίου 1997. Σ' αυτή προσεγγίζονται ορισμένα θέματα περισσότερο ή λιγότερο ευαίσθητα, όπως η φύλαξη των δεδομένων σύνδεσης από τα κράτη-μέλη για την εξυπηρέτηση της αστυνομικής επιτήρησης (κατακράτηση δεδομένων), η αποστολή αυτόκλητων ηλεκτρονικών μηνυμάτων, η χρήση «cookies», και η αναγραφή προσωπικών δεδομένων στους δημόσιους καταλόγους συνδρομητών.

- *Απόρρητο των επικοινωνιών*: η οδηγία υπενθυμίζει ως βασική αρχή ότι τα κράτη-μέλη οφείλουν να εγγυώνται μέσω της εθνικής νομοθεσίας, το απόρρητο των επικοινωνιών που πραγματοποισύνται μέσω δημόσιου δικτύου ηλεκτρονικών επικοινωνιών. Οφείλουν, ειδικότερα, να απαγορεύουν σε κάθε άλλο πρόσωπο εκτός των χρηστών την ακρόαση, την υποκλοπή, την αποθήκευση των επικοινωνιών χωρίς τη συγκατάθεση των ενδιαφερομένων χρηστών.
- *Κατακράτηση των δεδομένων*: όσον αφορά το ευαίσθητο θέμα της κατακράτησης των δεδομένων, η οδηγία ορίζει ότι τα κράτη-μέλη δεν επιτρέπεται να αίρουν την προστασία των δεδομένων παρά μόνο όταν πρόκειται για τη διενέργεια ερευνών ποινικού χαρακτήρα ή για τη διαφύλαξη της εθνικής ασφάλειας, της εθνικής άμυνας και της δημόσιας ασφάλειας. Ένα τέτοιο μέτρο μπορεί να θεσπιστεί μόνο όταν αποτελεί «αναγκαίο, κατάλληλο και ανάλογο μέτρο σε μια δημοκρατική κοινωνία».
- *Αυτόκλητα ηλεκτρονικά μηνύματα (spamming)*: η οδηγία πραγματοποιεί μια προσέγγιση «συγκατάθεσης» έναντι των αυτόκλητων ηλεκτρονικών μηνυμάτων εμπορικού χαρακτήρα, σύμφωνα με την οποία οι χρήστες οφείλουν να παρέχουν την συγκατάθεσή τους προτού λάβουν τα εν λόγω μηνύματα. Το συγκεκριμένο σύστημα συγκατάθεσης καλύπτει επίσης τα σύντομα μηνύματα (SMS) και τα λοιπά ηλεκτρονικά μηνύματα που λαμβάνονται σε οποιοδήποτε κινητό ή σταθερό τερματικό.
- *Cookies*: συνίστανται σε κρυφές πληροφορίες που ανταλλάσσονται μεταξύ χρήστη του Διαδικτύου και ενός διακομιστή ιστού (web server) και αποθηκεύονται σε αρχείο στο σκληρό δίσκο του χρήστη. Οι πληροφορίες αυτές επέτρεπαν αρχικά τη διατήρηση των πληροφοριών μεταξύ δύο συνδέσεων, αλλά αποδεικνύονται και εργαλείο ελέγχου της δραστηριότητας του χρήστη του διαδικτύου, που συχνά αποδοκιμάζεται. Η οδηγία προβλέπει σχετικά ότι οι χρήστες πρέπει να έχουν τη δυνατότητα να αρνηθούν την τοποθέτηση κάποιου cookie ή παρόμοιας διάταξης, στον τερματικό τους εξοπλισμό. Για να γίνει κάτι τέτοιο,

πρέπει να δοθούν στους χρήστες σαφείς και ακριβείς πληροφορίες για τον προορισμό και το ρόλο των cookies.

- *Δημόσιοι κατάλογοι συνδρομητών*: σύμφωνα με την οδηγία, οι Ευρωπαίοι πολίτες πρέπει να παρέχουν τη συγκατάθεσή τους προτού οι αριθμοί τηλεφώνου τους (σταθερού ή κινητού), η ηλεκτρονική διεύθυνσή τους και η διεύθυνση κατοικίας τους αναγραφούν στους δημόσιους καταλόγους συνδρομητών.

Επιθέσεις κατά των συστημάτων πληροφόρησης:

1. Στόχος

Η ενίσχυση της δικαστικής συνεργασίας στον ποινικό τομέα σε περιπτώσεις επιθέσεων κατά των συστημάτων πληροφόρησης, χάρη στη διαμόρφωση αποτελεσματικών μέσων και διαδικασιών.

2. Πρόταση

Πρόταση απόφασης πλαισίου του Συμβουλίου για τις επιθέσεις κατά των συστημάτων πληροφόρησης [Επίσημη Εφημερίδα C203 E, 27.08.2002].

3. Περίληψη

Στο Ευρωπαϊκό Συμβούλιο του Tampere τον Οκτώβριο του 1999, τα κράτη-μέλη είχαν αναγνωρίσει την ανάγκη να καταλήξουν σε συμφωνία όσον αφορά τους ορισμούς (και τις εφαρμοστέες κυρώσεις) ενός ορισμένου αριθμού εγκληματικών πράξεων. Η εγκληματικότητα η οποία χρησιμοποιεί τις τεχνολογίες αιχμής ήταν μία από τις κατηγορίες εγκληματικών πράξεων που συμπεριλήφθηκαν σε αυτόν τον κατάλογο. Εν συνεχεία, το Ευρωπαϊκό Συμβούλιο της Λισσαβόνας τον Μάρτιο του 2000, είχε υπογραμμίσει τη σημασία μιας ανταγωνιστικής οικονομίας βασισμένης στη γνώση. Προς αυτή την κατεύθυνση, η Επιτροπή παρουσίασε το σφαιρικό σχέδιο δράσης eEurope για την ανάπτυξη όλων των δυνατοτήτων τις οποίες προσφέρουν οι νέες τεχνολογίες και για τη βελτίωση της ασφάλειας των δικτύων πληροφορικής. Επιπλέον, η παρούσα απόφαση-πλαίσιο περιλαμβανόταν ήδη στη σειρά των δράσεων που προβλεπόταν στην ημερήσια διάταξη που είχε παρουσιάσει η Επιτροπή αποβλέποντας στη δημιουργία ενός χώρου ασφάλειας, ελευθερίας και δικαιοσύνης.

4. Πεδίο εφαρμογής

Σκοπός της παρούσας πρότασης είναι να καλύψει όχι μόνο τις πράξεις που διαπράττονται έχοντας ως στόχο τα κράτη-μέλη, αλλά επίσης και τις πράξεις που διαπράττονται στο έδαφος των κρατών-μελών έχοντας σα στόχο συστήματα που βρίσκονται στο έδαφος τρίτων χωρών. Θα καλύπτει κάθε πράξη που διαπράττεται κατά μιας υποδομής πληροφορικής με σκοπό την καταστροφή, την τροποποίηση ή την αλλοίωση των πληροφοριών που περιλαμβάνονται στους

υπολογιστές ή στα δίκτυα υπολογιστών. Εντούτοις, οι συμπεριφορές ήσσονος σημασίας δε θα καλυφθούν από την παρούσα απόφαση πλαίσιο. Εν πάση περιπτώσει, η δράση της Ένωσης θα πρέπει να λάβει υπόψη τη Συνέλευση για την εγκληματικότητα στον Κυβερνοχώρο του Συμβουλίου της Ευρώπης η οποία άνοιξε προς υπογραφή των Κρατών το Νοέμβριο του 2001.

Κοινοτικό πλαίσιο για τις ηλεκτρονικές υπογραφές:

1. Στόχος

Η διασφάλιση της καλής λειτουργίας της εσωτερικής αγοράς στο πεδίο των ηλεκτρονικών υπογραφών με τη δημιουργία εναρμονισμένου νομικού πλαισίου, κατάλληλου για τη χρήση ηλεκτρονικών υπογραφών στην Ευρωπαϊκή Κοινότητα.

2. Μέτρο

Οδηγία 1999/93/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 13ης Δεκεμβρίου 1999, σχετικά με ένα κοινό πλαίσιο για τις ηλεκτρονικές υπογραφές.

3. Περιεχόμενο

Τα ανοικτά δίκτυα, όπως το Internet, καθίστανται διαρκώς σημαντικότερα για τις παγκόσμιες επικοινωνίες. Επιτρέπουν διαλογική επικοινωνία μεταξύ ατόμων, τα οποία ενίοτε δεν είχαν έως τότε συνάψει κανενός είδους σχέση. Παρέχοντας εργαλεία για την αύξηση της παραγωγικότητας και τη μείωση των δαπανών, καθώς και νέα μέσα προσέγγισης των πελατών, τα δίκτυα παρέχουν νέες οικονομικές δυνατότητες. Αξιοποιούνται από τις επιχειρήσεις που επιθυμούν να εκμεταλλευθούν νέους τρόπους διεξαγωγής συναλλαγών και νέους μεθόδους εργασίας. Για τη βέλτιστη αξιοποίηση των δυνατοτήτων αυτών είναι απαραίτητη η εγκατάσταση ασφαλούς περιβάλλοντος όσον αφορά την ηλεκτρονική επαλήθευση ταυτότητας. Οι ηλεκτρονικές υπογραφές επιτρέπουν στον αποστολέα ηλεκτρονικώς μεταδιδόμενων δεδομένων να επαληθεύει την προέλευση των δεδομένων και επίσης να επιβεβαιώνει ότι τα δεδομένα είναι πλήρη και αμετάβλητα, ότι δηλαδή έχει διαφυλαχθεί η ακεραιότητά τους.

Με την παρούσα οδηγία καθιερώνονται κριτήρια που συναποτελούν τη βάση της νομικής αναγνώρισης των ηλεκτρονικών υπογραφών, επικεντρωμένα στις υπηρεσίες πιστοποίησης. Πρόκειται συγκεκριμένα για:

- κοινές υποχρεώσεις για τους παροχείς υπηρεσιών πιστοποίησης με σκοπό τη διασφάλιση της διασυνοριακής αναγνώρισης των υπογραφών και των πιστοποιητικών στην Ευρωπαϊκή Κοινότητα.
- κοινούς κανόνες ευθύνης για υποστήριξη της διαδικασίας οικοδόμησης εμπιστοσύνης, τόσο όσον αφορά τους καταναλωτές που βασίζονται στα πιστοποιητικά όσο και ως προς τους παροχείς υπηρεσιών

- μηχανισμούς συνεργασίας για διευκόλυνση της διασυνοριακής αναγνώρισης των υπογραφών και των πιστοποιητικών με τρίτες χώρες

Δημιουργία ενός ευρωπαϊκού οργανισμού επιφορτισμένου με την ασφάλεια των δικτύων και των πληροφοριών:

1. Στόχος

Η διευκόλυνση της εφαρμογής των κοινοτικών μέτρων που αφορούν την ασφάλεια των δικτύων και των πληροφοριών και ενίσχυση της συνεργασίας στον τομέα αυτό ώστε να κατοχυρωθεί ο υψηλότερος δυνατός βαθμός ασφάλειας για τους χρήστες.

2. Πρόταση

Πρόταση κανονισμού του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 11ης Φεβρουαρίου 2003, για τη δημιουργία του Ευρωπαϊκού Οργανισμού για την ασφάλεια δικτύων και πληροφοριών [δεν έχει ακόμη δημοσιευθεί στην επίσημη εφημερίδα].

3. Πλαίσιο

Η πληροφορική και τα δίκτυα αποτελούν πλέον σημαντικό στοιχείο της καθημερινής ζωής των ευρωπαίων πολιτών. Πάνω από το 90% των εταιρειών της Ευρωπαϊκής Ένωσης έχουν σύνδεση με το Internet και η πλειονότητα αυτών διαθέτει δικό της ιστότοπο. Το 2002, περίπου το 40% των νοικοκυριών της ΕΕ διέθετε δική του σύνδεση με το Internet. Η χρήση του Internet για εκπαιδευτικούς σκοπούς αποτελεί αναπόσπαστο μέρος της λειτουργίας των σχολείων και των πανεπιστημίων, ενώ η δημόσια διοίκηση μεταβαίνει γρήγορα προς την ηλεκτρονική κυβέρνηση. Επιπλέον, υποδομές όπως τα συστήματα ηλεκτροδότησης και ύδρευσης ή τα δίκτυα δημοσίων συγκοινωνιών ελέγχονται από συστήματα πληροφορικής και δίκτυα επικοινωνίας.

Λόγω της γενικευμένης παρουσίας των δικτύων επικοινωνίας και των συστημάτων πληροφοριών, η ασφαλής λειτουργία τους αποτελεί πλέον ζήτημα αυξανόμενης σημασίας για το κοινωνικό σύνολο, ιδίως μετά τα γεγονότα της 11ης Σεπτεμβρίου 2001. οι απαιτήσεις ασφάλειας θα γίνουν εξάλλου ακόμη και πιο πιεστικές στο μέλλον λόγω του πολλαπλασιασμού των συνδέσεων με το Internet και της ανάπτυξης των δικτύων.

Ο αυξανόμενος αριθμός παραβιάσεων της ασφάλειας των δικτύων έχει ήδη προκαλέσει σοβαρές οικονομικές ζημιές, έχει κλονίσει την εμπιστοσύνη των χρηστών και έχει ζημιώσει την ανάπτυξη του ηλεκτρονικού εμπορίου. Οι ιδιώτες, οι δημόσιες αρχές και οι επιχειρήσεις αντέδρασαν προσφεύγοντας σε τεχνολογίες ασφάλειας και σε διαδικασίες διαχείρισης της ασφάλειας. Εν τούτοις, όπως αποδείχθηκε, οι αντιδράσεις των κρατών-μελών είναι διάσπαρτες και όχι επαρκώς συντονισμένες ώστε να αντιμετωπισθούν αποτελεσματικά τα προβλήματα

ασφάλειας. Εκτός από ορισμένα διοικητικά δίκτυα, δεν υπάρχει συστηματική διασυνοριακή συνεργασία για την ασφάλεια δικτύων και πληροφοριών μεταξύ των κρατών-μελών, μολονότι τα θέματα ασφαλείας δε μπορεί να θεωρηθούν μεμονωμένο πρόβλημα που αφορά μία μόνο χώρα.

4. Στόχοι

Πρωταρχικός στόχος της δημιουργίας ενός ευρωπαϊκού οργανισμού επιφορτισμένου με την ασφάλεια των δικτύων και των πληροφοριών είναι να διευκολυνθεί και να ενισχυθεί ο ευρωπαϊκός συντονισμός στον τομέα της ασφάλειας των πληροφοριών και, με αυτό τον τρόπο, να επιτευχθεί υψηλό επίπεδο ασφάλειας στα κράτη-μέλη. Ο οργανισμός προβλέπεται συνεπώς να ενισχύσει την ικανότητα απόκρισης της Ευρωπαϊκής Κοινότητας και των κρατών-μελών στα προβλήματα ασφάλειας των δικτύων και των πληροφοριών.

Ένας άλλος στόχος του οργανισμού είναι να διευκολύνει την εφαρμογή των κοινοτικών μέτρων που αφορούν την ασφάλεια των δικτύων και των πληροφοριών και να συμβάλλει στην κατοχύρωση της διαλειτουργικότητας των λειτουργιών ασφάλειας των δικτύων και συστημάτων πληροφοριών, συνεισφέροντας με τον τρόπο αυτό στη λειτουργία της εσωτερικής αγοράς της ΕΕ.

5. Διάρκεια λειτουργίας

Ο οργανισμός θα λειτουργήσει από την 1η Ιανουαρίου 2004 έως την 31η Δεκεμβρίου 2008.

Πηγές

❖ **Βιβλιογραφία**

«Ασφάλεια Δικτύων Υπολογιστών»
Πομπόρτσης Ανδρέας - Παπαδημητρίου Γεώργιος (Εκδόσεις ΤΖΙΟΛΑ)

«Ασφάλεια Πληροφοριακών Συστημάτων και Δικτύων»
Πάγκαλος Γ. - Μαυρίδης Ι. (Εκδόσεις ΑΝΙΚΟΥΛΑ)

«Πληροφοριακός Πόλεμος και Ασφάλεια Πληροφοριών των Επιχειρήσεων»
Dorothy E. Denning (Εκδόσεις ΙΩΝ)

❖ **Περιοδικά**

«INTERNET για όλους»
(Τεύχη από Οκτώβριο 2003 έως Απρίλιο 2004)

«PC MAGAZINE»
(Τεύχη Ιανουαρίου 2004 και Μαρτίου 2004)

❖ **Πτυχιακές Εργασίες**

«Ηλεκτρονικό Εμπόριο»
Κονταράκης Γεώργιος – Κούκα Μαρία (2002)

«Το ηλεκτρονικό εμπόριο, πλεονεκτήματα, μειονεκτήματα»
Μίτσιγγα Έφη – Κάρδαρη Ροδαλία (2002)

❖ **Internet**

www.howstuffworks.com
www.ciac.org
www.cookiecentral.com
www.csi/fbi.com
www.ebusinessforum.gr
www.europa.gr