LionHeartsPointOfView

INTERNET – ΗΛΕΚΤΡΟΝΙΚΟ ΕΓΚΛΗΜΑ – ΔΙΩΞΗ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

Δευτέρα, 27 Αυγούστου 2007

Κυρίες και Κύριοι καλημέρα σας.

Αφορμή για το κείμενο που θα διαβάσετε πιο κάτω, αποτέλεσε κάποιο πρόσφατο γεγονός που συνέβη στο forum και αφορούσε εμένα. Σκεφτόμουν πολλές φορές να καθίσω να γράψω κάτι ανάλογο, όμως τόσο ο φόρτος εργασίας, όσο και η περιορισμένη αντίληψη του μεγαλύτερου μέρους των χρηστών ενός forum, με απέτρεπαν. Όταν αναφέρομαι σε μειωμένη αντίληψη μη με παρεξηγείτε.

Είναι γνωστό εξάλλου ότι η χώρα μας κατατάσσεται στις τελευταίες χώρες, στη λίστα με τους χρήστες Internet, πράγμα το οποίο φυσικά σημαίνει, ότι και οι γνώσεις μας γύρω από το θέμα, είναι εκ των πραγμάτων περιορισμένες.

Λόγω επαγγέλματος, λόγω ειδικότητας αλλά και λόγω της καθημερινής μου ενασχόλησης με το «άθλημα» για περίπου 18 χρόνια, έχοντας διατελέσει χρήστης-διαχειριστής (administrator) διαφόρων ειδών δικτύων πολιτικών-στρατιωτικών, της παλαιότερης ενασχόλησης μου ως Operator στο MIRC, παρακολούθηση διαφόρων σεμιναρίων και η χρήσιμες συνομιλίες που είχα με cyber cop νομίζω πως μπορώ, με την βοήθεια φυσικά και ορισμένων sites, να σας βοηθήσω τόσο με ορισμούς, όσο και με το πώς μπορείτε να προφυλαχτείτε, από τις διάφορες «απειλές» που προκύπτουν με τη χρήση του δικτύου. Και φυσικά να γνωρίσετε όλοι, τόσο τα δικαιώματά μας όσο και τις υποχρεώσεις μας που απορρέουν από την χρήση του.

- Αλήθεια ποιοι από εσάς ξέρουν τι είναι Internet;
- Τι είναι sites;
- Τι είναι fora;
- Ποιες είναι οι υποχρεώσεις μας, όταν κάνουμε χρήση των παραπάνω;
- Ποια τα δικαιώματά μας;
- Υπάρχει ανωνυμία στο παγκόσμιο διαδίκτυο;
- Τι ονομάζουμε Ηλεκτρονικό Έγκλημα;
- Πόσο ασφαλείς είμαστε, χρησιμοποιώντας το;
- Τι είναι η Δίωξη Ηλεκτρονικού Εγκλήματος;

Πολλά ερωτηματικά, τα περισσότερα από τα οποία δύσκολα κανείς τα έχει σκεφτεί. Πόσο μάλλον να έχει σκεφτεί τρόπους αντιμετώπισης εκβιασμών, απειλών, hacking, fishing κτλ.

Ας ξεκινήσουμε εν συντομία όμως με μερικά ιστορικά στοιχεία για το παγκόσμιο Διαδίκτυο. Πώς ξεκίνησε και πώς εξελίχθηκε ως σήμερα.

Όλα ξεκίνησαν κατά την περίοδο του Ψυχρού Πολέμου μεταξύ της τότε ΕΣΣΔ και των ΗΠΑ. Στη σκέψη των Αμερικανών, υπήρχε η σχεδίαση ενός δικτύου, το οποίο σε περίπτωση πυρηνικού πολέμου, δεν θα κατέρρεε. Η σκέψη αυτή υλοποιήθηκε από την εταιρεία ***ARPA*** *(Advance Research Projects Agency)*, η οποία ανέπτυξε ένα δίκτυο υπολογιστών στα τέλη της δεκαετίας του 1960. Το όνομα αυτού ***ARPAnet***.

Το δίκτυο αυτό αποτελείτο αρχικά από τέσσερις (4) υπολογιστές, 3 εκ των οποίων βρίσκονταν στην Καλιφόρνια και ένας (1) στην πολιτεία της Γιούτα. Το πρωτόκολλο που χρησιμοποιήθηκε για την κατασκευή του συγκεκριμένου δικτύου ήταν το ***NCP*** *(Network Control Protocol)*. Κάπως έτσι λοιπόν ξεκίνησε το Διαδίκτυο.

Αργότερα με το πέρασμα των χρόνων εξελίχθηκε, εμφανίστηκαν οι όροι *TCP/IP* ως πλέον το πιο προσφιλή πρωτόκολλο εν χρήση, *BITNET (because its time network)*, *CSNET (Computer Science Networks)*, *NSFNET (National Foundation Network)* το μεγαλύτερο backbone δίκτυο στην εποχή του. Η ARPANET αργότερα διασπάστηκε σε *ARPANET* και σε *MILnet (Military Network).*

Παρακάτω θα βρείτε μια λίστα με τις ημερομηνίες που αποτέλεσαν σταθμό στην ιστορία του Internet.

- '60 Εφεύρεση της μεταγωγής δεδομένων.
- 1967 – Σχέδια υλοποίησης της θεωρίας μεταγωγής πακέτων.
- 1969 – Ορίζεται η ARPAnet από το Υ.ΕΘ.Α των ΗΠΑ, να ερευνήσει την δυνατότητα διαδικτύωσης των υπολογιστών – Σύνδεση των πρώτων 4 κέντρων.
- 1970 – Χρήση του Network Control Protocol (NCP) των κόμβων (nodes) του ARPAnet.
- 1972 – Ίδρυση του InterNetworking Working Group (INWG) με σκοπό τον ορισμό των standards.
- 1973 – Πρώτες διεθνές συνδέσεις του ARPAnet. Σύνδεση με Νορβηγία και Βρετανία.
- 1976 – Αναπτύχθηκε το UUCP (Unix to Unix Copy Protocol) από την AT&T Bell Labs.
- 1979 – Γέννηση του USEnet που κάνει χρήση του UUCP.
- 1981 – Ίδρυση των BITNET και CSNET.
- 1982 – Το INWG ορίζει το TCP/IP ως το πρωτόκολλο του ARPAnet. Το Υπουργείο Άμυνας των ΗΠΑ το υιοθετεί.
- 1983 – Δημιουργία του Name Server από το Πανεπιστήμιο του Wisconsin. Οι χρήστες δεν χρειάζεται να ξέρουν την διαδρομή για να βρουν τα άλλα συστήματα. Διάσπαση του ARPAnet σε ARPAnet και MILnet.
- 1984 – Εγκατάσταση του DNS (Domain Name Server). 1.000 hosts.
- 1986 – Ίδρυση του NSFnet με κορμό στα 56Kbps
- 1989 – Αναβάθμιση του κορμού του NSFnet σε T1, 1,544 Mbps. 100.000 hosts.
- 1990 – Κατάργηση του ARPAnet. Ίδρυση της Electronic Frontier Foundation (EFF). Ανακοινώνεται η υπηρεσία Archie.
- 1991 – Ίδρυση του Commercial Internet Exchange (CIX). Δημιουργία των υπηρεσιών WAIS και Gopher.
- 1992 – Ίδρυση της Internet Society. Το CERN δημιουργεί το World-Wide-Web. Ο κορμός του NSFnet αναβαθμίζεται σε T3 δηλ. 44.736Mbps. Πάνω από 1.000.000 hosts στο Internet.
- 1993 – Ιδρύεται το InterNIC από την NSF με σκοπό την παροχή πληροφοριών στους χρήστες. Τα ΜΜΕ δίνουν σημασία στο Internet.
- 1994 – Αλλαγή πολιτικής του NSF. Ο έλεγχος του κορμού περνάει σε ιδιώτες ενώ αίρονται οι περιορισμοί που αφορούσαν τις διεθνείς συνδέσεις.

Τι Είναι Λοιπόν το Internet

Internet ή αλλιώς Διαδίκτυο είναι ένα δίκτυο υπολογιστών συνδεδεμένων μεταξύ τους. Οι κυριότεροι λόγοι ύπαρξης ενός δικτύου είναι : 1ον να μπορούν οι χρήστες των υπολογιστών να επικοινωνούν μεταξύ τους και 2ον να χρησιμοποιούν από απόσταση τις υπηρεσίες που προσφέρει κάποιος υπολογιστής του δικτύου.

Ένα σύνολο από κανόνες που ονομάζεται πρωτόκολλο δικτύωσης, καθορίζει το πώς επικοινωνούν μεταξύ τους οι υπολογιστές του δικτύου. Η φυσική διάταξη των συνδέσεων του δικτύου ονομάζεται τοπολογία. Οι τρεις πιο συνηθισμένες τοπολογίες είναι οι εξής :

Αστέρας (star)
Υπάρχει ένας κεντρικός υπολογιστής στον οποίον συνδέονται οι υπόλοιποι υπολογιστές του δικτύου.

Δακτύλιος (ring)
Όλοι οι υπολογιστές είναι συνδεδεμένοι σ' έναν πλήρη κλειστό δακτύλιο.

Δίαυλος (bus)
Όλοι οι υπολογιστές συνδέονται κατά μήκος ενός κεντρικού αγωγού.

Τα δίκτυα, ανάλογα με το εύρος της περιοχής που καλύπτουν, χωρίζονται σε τρεις κατηγορίες :

Τοπικά Δίκτυα (Local Area Network – LAN)
Συνδέουν υπολογιστές που απέχουν μεταξύ τους μικρές αποστάσεις, π.χ. υπολογιστές που βρίσκονται στο ίδιο ή σε γειτονικά κτίρια.

Δίκτυα Μητροπολιτικής Περιοχής (Metropolitan Area Network – MAN)
Συνδέουν υπολογιστές που απέχουν μεταξύ τους μεσαίες αποστάσεις, π.χ. υπολογιστές που βρίσκονται σε διαφορετικά σημεία της ίδιας πόλης.

Δίκτυα Ευρείας Περιοχής (Wide Area Network – WAN)
Συνδέουν υπολογιστές που απέχουν μεταξύ τους μεγάλες αποστάσεις, π.χ. υπολογιστές που βρίσκονται σε διαφορετικές πόλεις.

Τι είναι η IP Address
Κάνοντας μια απλουστευμένη ανάλυση, η IP Address είναι ένα σύνολο αριθμών το οποίο συνήθως αποτελείται από 3αδες νούμερων διαχωρισμένα με μια τελεία. Ο κάθε Ηλεκτρονικός Υπολογιστής που θέλει να «βγει» στο δίκτυο, πρέπει να έχει μια τέτοια διεύθυνση, η οποία είναι ΜΟΝΑΔΙΚΗ. Η διεύθυνση αυτή αποτελείται από 4 ψηφία, τριών αριθμών από το 0 έως το 255. Έχει τη μορφή xxx.xxx.xxx.xxx.

Τι είναι τα Domains
Επίσης επιχειρώντας μια απλουστευμένη ανάλυση, domains είναι οι καταλήξεις μια ιστοσελίδας. Δηλαδή, στην ιστοσελίδα http://www.metropolisradio.gr το .gr αποτελεί το domain του site. Παρακάτω φαίνονται μερικά domain names που κυκλοφορούν και μας είναι γνωστά.

- .edu = educational (Εκπαιδευτικό Ίδρυμα ΗΠΑ)
- .gov = government (Κυβέρνηση ΗΠΑ)
- .mil = military (Υ.ΕΘ.Α. ΗΠΑ)
- .com = commercial (Εμπορικό ΗΠΑ)
- .us = άλλα των ΗΠΑ
- .net = network (Δίκτυο)
- .gr = Greece (domain Ελλάδας)
- .it = Italy (domain Ιταλίας)
- .uk = United Kingdom (domain Βρετανίας)

Σας κούρασα; Σ' αυτό το σημείο τελειώνει η αναφορά μου στα του Διαδικτύου (Internet). Ο στόχος εξάλλου δεν ήταν αυτός. Απλά θεώρησα καλό ορισμένες βασικές έννοιες του δικτύου να τις έχουμε συγκεντρωμένες. Είμαι σίγουρος, πως πολλοί από εσάς είχατε ακούσει κατά καιρούς, όλες αυτές τις λέξεις-όρους, αλλά οι περισσότεροι δεν θα ήσασταν σε θέση να δώσετε τους ορισμούς τους.

Προχωράμε λοιπόν....

Το παρακάτω κείμενο είναι ιδιαιτέρως κατατοπιστικό. Προέρχεται από την ιστοσελίδα του Υπουργείου Δημοσίας Τάξης και είναι ένα δημοσίευμα του Ανθ/μου Κωνσταντίνου Γ. Κούρου.

Το Ηλεκτρονικό Έγκλημα

Η ραγδαία εξέλιξη της τεχνολογίας, η ανάπτυξη της πληροφορικής και η ευρύτατη χρήση του Διαδικτύου έχουν επιφέρει επαναστατικές αλλαγές στο σύνολο των καθημερινών δραστηριοτήτων, στην παραγωγική διαδικασία, στις συναλλαγές, στην εκπαίδευση, στη διασκέδαση, ακόμα και στον τρόπο σκέψεως του σύγχρονου ανθρώπου.

Μαζί μ' αυτές τις αλλαγές, οι οποίες κατά κανόνα βελτιώνουν την ποιότητα της ζωής μας, υπεισέρχονται και οι παράμετροι που ευνοούν την ανάπτυξη νέων μορφών εγκληματικότητας. Οι νέες αυτές μορφές εγκληματικότητας θεσμοθετούνται με τον όρο «Ηλεκτρονικό Έγκλημα».

Η πληροφορική τεχνολογία κατέστησε δυνατή τη διάπραξη ενός ευρέως φάσματος εγκληματικών πράξεων, οι οποίες απαιτούν εξειδίκευση και αυξημένη κατάρτιση. Ως «Ηλεκτρονικό Έγκλημα», λοιπόν, θεωρούνται οι αξιόποινες εγκληματικές πράξεις που τελούνται με τη χρήση ηλεκτρονικών υπολογιστών και συστημάτων επεξεργασίας δεδομένων και τιμωρούνται με συγκεκριμένες ποινές από την ελληνική νομοθεσία.

Ανάλογα με τον τρόπο τέλεσης διαχωρίζονται σε εγκλήματα τελούμενα με τη χρήση Ηλεκτρονικών Υπολογιστών (computer crime) και σε Κυβερνοεγκλήματα (cyber crime), εάν τελέσθηκαν μέσω του Διαδικτύου.

Η Συνθήκη της Βουδαπέστης

Οι μορφές του Ηλεκτρονικού Εγκλήματος είναι ποικίλες και με τη συνεχή ανάπτυξη της τεχνολογίας και του Διαδικτύου πολλαπλασιάζονται. Για την αντιμετώπιση του κινδύνου αυτού ήταν απαραίτητη η διακρατική συνεννόηση και η εκπόνηση μιας αναλυτικής και αποτελεσματικής στρατηγικής.

Ο στόχος αυτός επετεύχθη στο *Συνέδριο για το Ηλεκτρονικό Έγκλημα (Convention on Cybercrime)*, που έγινε το 2001 στη Βουδαπέστη του οποίου όλα τα συμπεράσματα αποκρυσταλλώνονται στη Συνθήκη που υπεγράφη μετά το πέρας των εργασιών του Συνεδρίου στις 23.11.2001.

Στη Συνθήκη της Βουδαπέστης, υπέγραψαν 26 υπουργοί ευρωπαϊκών κρατών, μεταξύ των οποίων και της Ελλάδας, και υπάρχουν επεξηγήσεις και ρυθμίσεις γι' όλα τα Ηλεκτρονικά Εγκλήματα.

Μορφές Κυβερνοεγκλήματος

Σύμφωνα με τα αποτελέσματα έρευνας που διεξήγαγε η McConnell International σε 52 χώρες, με τίτλο «Cyber Crime ... and Punishment?» κατατάσσει τα αδικήματα που διαπράττονται στον Κυβερνοχώρο στις παρακάτω δέκα κατηγορίες :

- Παρεμπόδιση (κυβερνο)κυκλοφορίας
- Τροποποίηση και Κλοπή δεδομένων
- Εισβολή και Σαμποτάζ σε δίκτυο
- Μη εξουσιοδοτημένη πρόσβαση
- Διασπορά ιών
- Υπόθαλψη αδικημάτων
- Πλαστογραφία και
- Απάτη

Κύριες μορφές Κυβερνοεγκλημάτων που εξιχνιάσθηκαν στην Ελλάδα από το Τμήμα Ηλεκτρονικού Εγκλήματος/ΔΑΑ :

1. Απάτες μέσω Διαδικτύου
2. Παιδική πορνογραφία
3. Cracking και hacking
4. Διακίνηση-πειρατεία λογισμικού
5. Πιστωτικές κάρτες
6. Διακίνηση ναρκωτικών
7. Έγκλημα στα chat rooms

Η Ελληνική Νομοθεσία

Ο Ν. 1805/88, αφορά τα εγκλήματα που διαπράττονται με ηλεκτρονικούς υπολογιστές (computer crimes) και στο βαθμό που τα προβλεπόμενα εγκλήματα (370Β, 370Γ, 386Α) διαπράττονται και σε περιβάλλον Διαδικτύου (Internet), τότε τα άρθρα αυτά εφαρμόζονται και στις συγκεκριμένες περιπτώσεις.

Στην ελληνική νομοθεσία, όμως, δεν υπάρχει νόμος που να αναφέρεται αποκλειστικά σε θέματα Διαδικτύου και να ρυθμίζει τη συμπεριφορά των χρηστών του Διαδικτύου από άποψη Ποινικού Δικαίου. Ως εκ τούτου, η Ελλάδα συνεργάζεται με τα άλλα κράτη της Ευρωπαϊκής Ένωσης, του Συμβουλίου της Ευρώπης, καθώς και άλλων διεθνών οργανισμών, για την αντιμετώπιση των σχετικών θεμάτων.

Ανεξάρτητα, όμως, από το εάν ο ανωτέρω νόμος και οι διεθνείς συνεργασίες επαρκούν ή όχι για την ποινική κάλυψη των θεμάτων που προκύπτουν από την ανάπτυξη της Πληροφορικής, το βέβαιο είναι ότι, δεν επαρκούν για την τέλεια αντιμετώπιση των εγκλημάτων που έχουν τελεστεί με τη χρήση του Διαδικτύου.

Πρόσφατα τέθηκε σε ισχύ το Π.Δ. 47/2005, από την Α.Δ.Α.Ε. (Αρχή Διασφάλισης Απορρήτου των Επικοινωνιών), το οποίο αφορά τις διαδικασίες, τεχνικές και οργανωτικές εγγυήσεις για την άρση του απορρήτου των επικοινωνιών και τη διασφάλισή του. Ενώ, σύντομα αναμένεται να τεθεί σε ισχύ η Συνθήκη της Βουδαπέστης.

Άρθρο 370Β

1. Όποιος αθέμιτα αντιγράφει, αποτυπώνει, χρησιμοποιεί, αποκαλύπτει σε τρίτον ή οπωσδήποτε παραβιάζει στοιχεία ή προγράμματα υπολογιστών τα οποία συνιστούν κρατικά, επιστημονικά ή επαγγελματικά απόρρητα ή απόρρητα επιχείρησης του δημοσίου ή ιδιωτικού τομέα, τιμωρείται με φυλάκιση τουλάχιστον 3 μηνών. Ως απόρρητα θεωρούνται κι εκείνα που ο νόμιμος κάτοχός τους από δικαιολογημένο ενδιαφέρον τα μεταχειρίζεται ως απόρρητα, ιδίως όταν έχει λάβει μέτρα για να παρεμποδίζονται τρίτοι να λάβουν γνώση τους.
2. Αν ο δράστης είναι στην υπηρεσία του κατόχου των στοιχείων, καθώς και αν το απόρρητο είναι ιδιαίτερα μεγάλης οικονομικής σημασίας, επιβάλλεται φυλάκιση τουλάχιστον ενός έτους.
3. Αν πρόκειται για στρατιωτικό ή διαπλαστικό απόρρητο ή για απόρρητο που αναφέρεται στην ασφάλεια του κράτους, η κατά την παρ. 1 πράξη τιμωρείται κατά τα άρθρα 146 και 147.
4. Οι πράξεις που προβλέπονται στις παρ.1 και 2 διώκονται ύστερα από έγκληση.

Άρθρο 370Γ

1. Όποιος χωρίς δικαίωμα αντιγράφει ή χρησιμοποιεί προγράμματα υπολογιστών, τιμωρείται με φυλάκιση μέχρι έξι μήνες και με χρηματική ποινή διακοσίων ενενήντα (290) ευρώ έως πέντε χιλιάδων εννιακοσίων (5.900) ευρώ.
2. Όποιος αποκτά πρόσβαση σε στοιχεία που έχουν εισαχθεί σε υπολογιστή ή σε περιφερειακή μνήμη υπολογιστή ή μεταδίδονται με συστήματα τηλεπικοινωνιών, εφόσον οι πράξεις αυτές έγιναν χωρίς δικαίωμα ιδίως με παραβίαση απαγορεύσεων ή μέτρων ασφαλείας που είχε λάβει ο νόμιμος κάτοχός τους, τιμωρείται με φυλάκιση μέχρι τρεις μήνες ή με χρηματική ποινή τουλάχιστον

είκοσι εννέα ευρώ. Αν η πράξη αναφέρεται στις διεθνείς σχέσεις ή την ασφάλεια του κράτους, τιμωρείται κατά το άρθρο 148.

3. Αν ο δράστης είναι στην υπηρεσία του νόμιμου κατόχου των στοιχείων, η πράξη της προηγούμενης παραγράφου τιμωρείται μόνο αν απαγορεύεται ρητά από εσωτερικό κανονισμό ή από έγγραφη απόφαση του κατόχου ή αρμοδίου υπαλλήλου του.
4. Οι πράξεις των παρ. 1 έως 3 διώκονται ύστερα από έγκληση.

Άρθρο 386Α - Απάτη με υπολογιστή

Όποιος, με σκοπό να προσπορίσει στον εαυτό του ή σε άλλο παράνομο περιουσιακό όφελος, βλάπτει ξένη περιουσία, επηρεάζοντας τα στοιχεία υπολογιστή είτε με μη ορθή διαμόρφωση του προγράμματος είτε με επέμβαση κατά την εφαρμογή του είτε με χρησιμοποίηση μη ορθών ή ελλιπών στοιχείων είτε με οποιονδήποτε άλλο τρόπο, τιμωρείται με τις ποινές του προηγούμενου άρθρου. Περιουσιακή βλάβη υφίσταται και αν τα πρόσωπα που την υπέστησαν είναι άδηλα. Για την εκτίμηση του ύψους της ζημιάς είναι αδιάφορο αν παθόντες είναι ένα ή περισσότερα πρόσωπα.

Νομοθεσία Διαδικτυακών Εγκλημάτων στο Εξωτερικό

Στην Αγγλία από τον Φεβρουάριο του 2001, οι hackers, αναλόγως με τη σημασία του χτυπήματος θεωρούνται και τρομοκράτες. Στην Αμερική θεωρείται τρομοκρατική οποιαδήποτε πράξη μη εξουσιοδοτημένης πρόσβασης σε Η/Υ, και τιμωρείται με φυλάκιση ως και ισόβια (ανάλογα με τη σημασία της εισβολής), χωρίς δυνατότητα μείωσης τις ποινής.

Αδυναμίες της Νομοθεσίας

Ο Προϊστάμενος του Τμήματος Ηλεκτρονικού Εγκλήματος της Δ/νσης Ασφάλειας Αττικής, Αστυνόμος Α΄ κ. *Εμμανουήλ Σφακιανάκης* παρατηρεί ότι *«οι νομοθετικές ρυθμίσεις που αφορούν το ηλεκτρονικό έγκλημα παρουσιάζουν εγγενείς αδυναμίες, τόσο στην Ελλάδα όσο και στις υπόλοιπες χώρες. Αυτό συμβαίνει διότι το Ηλεκτρονικό Έγκλημα αποτελεί εγκληματική δραστηριότητα αρκετά εξειδικευμένη και ανεπτυγμένη τεχνολογικά, με αποτέλεσμα να παρουσιάζονται προβλήματα στην οριοθέτηση των πράξεων που θα πρέπει να διώκονται ποινικά. Επιπλέον, οι νομοθέτες είναι αναγκασμένοι να ενημερώνονται διαρκώς για τις εξελίξεις στον τομέα της τεχνολογίας των υπολογιστών, προκειμένου να εξοικειωθούν με τον τρόπο διάπραξης αδικημάτων μέσω αυτών»*.

Σε ειδική έρευνα που έγινε στη Βρετανία από την Επιτροπή Πρόβλεψης και Πρόληψης Εγκλήματος (Foresight Crime Prevention Panel) διαπιστώθηκε ότι το έτος 2020 οι κακοποιοί θα γνωρίζουν στην εντέλεια τη λειτουργία των συστημάτων ασφαλείας των τραπεζικών κωδικών και των τεχνικών αναγνώρισης και θα έχουν την τεχνογνωσία να υπερκεράσουν οποιοδήποτε ηλεκτρονικό εμπόδιο.

Διάρκεια της Διαδικτυακής Έρευνας

Η έρευνα των Ηλεκτρονικών Εγκλημάτων είναι αρκετά δύσκολη και ιδιαίτερα χρονοβόρος είναι και η διαδικασία του εντοπισμού των «ηλεκτρονικών ιχνών». Μια έρευνα μπορεί να διαρκέσει από έναν μήνα έως και δύο χρόνια. Ο λόγος της μεγάλης διάρκειας είναι διότι οι χρήστες του Διαδικτύου που ερευνώνται και που έχουν καταγγελθεί στην υπηρεσία μας ότι έχουν διαπράξει μια αξιόποινη πράξη λαμβάνουν διάφορα διαδικτυακά μέτρα προστασίας, έτσι ώστε ο εντοπισμός του να καθίσταται αρκετά δύσκολος.

Σε κάθε διαδικτυακή έρευνα γίνεται προσπάθεια εντοπισμού του ***«ηλεκτρονικού ίχνους»*** του δράστη, το οποίο για κάθε χρήστη του Internet είναι μοναδικό, και αποτελεί σημαντικό στοιχείο για την αποδεικτική διαδικασία στο δικαστήριο. Η λεγομένη ηλεκτρονική απόδειξη (electronic evidence) δεν ταυτίζεται με τα παραδοσιακά αποδεικτικά μέσα. Τα τελευταία, έχουν κατά κανόνα υλική υπόσταση και μπορούν να εντοπιστούν σε συγκεκριμένο τόπο και χρόνο. Αντίθετα, τα ηλεκτρονικά αποδεικτικά μέσα είναι ψηφιακά!

Σύμφωνα με τον Προϊστάμενο του Τμήματος Ηλεκτρονικού Εγκλήματος/ΔΑΑ, Αστυνόμο Α' κ. Εμμανουήλ Σφακιανάκη *«ο σωστός συνδυασμός των τεχνικών μέσων μαζί με τον ανθρώπινο παράγοντα είναι η χρυσή συνταγή για καλά αποτελέσματα. Εάν υπάρχουν τα τεχνολογικά μέσα (Η/Υ μαζί με λογισμικό) χωρίς την κατάλληλη εξειδίκευση του αστυνομικού προσωπικού, τότε τα αποτελέσματα δεν θα είναι τα αναμενόμενα. Στην υπηρεσία μας πιστεύω ότι υπάρχει η σωστή αναλογία σε τεχνικά μέσα και προσωπικό».*

Χαρακτηριστικά Γνωρίσματα του Κυβερνοεγκλήματος

- Το έγκλημα στον Κυβερνοχώρο είναι γρήγορο, διαπράττεται σε χρόνο δευτερολέπτων και πολλές φορές δεν το αντιλαμβάνεται ούτε το ίδιο το θύμα.
- Είναι εύκολο στην διάπραξή του, φυσικά για όσους το γνωρίζουν, ενώ τα ίχνη που αφήνει είναι ψηφιακά.
- Για την τέλεσή του απαιτούνται άριστες και εξειδικευμένες γνώσεις.
- Μπορεί να διαπραχθεί χωρίς την μετακίνηση του δράστη, ο οποίος ενεργεί από το γραφείο ή το σπίτι του, μέσω του υπολογιστή του.
- Δίνει τη δυνατότητα σε άτομα με ιδιαιτερότητες όπως οι παιδόφιλοι (child pornography) να επικοινωνούν γρήγορα ή και σε πραγματικό χρόνο, χωρίς μετακίνηση, εύκολα, ανέξοδα, να βρίσκονται πολλοί μαζί στις ίδιες ομάδες συζητήσεων (news groups) ή μέσα σε chat rooms.
- Οι "εγκληματίες του Κυβερνοχώρου" πολλές φορές δεν εμφανίζονται με την πραγματική τους ταυτότητα και αποστέλλουν ηλεκτρονικά μηνύματα (e-mails) με ψευδή στοιχεία.
- Είναι έγκλημα διασυνοριακό και τα αποτελέσματά του μπορεί να πραγματοποιούνται ταυτόχρονα σε πολλούς τόπους.
- Είναι πολύ δύσκολο να προσδιοριστεί ο τόπος τελέσεώς του και επίσης είναι αρκετά δύσκολη η διερεύνηση και ο εντοπισμός του δράστη. Υπάρχει ενδεχόμενο ο δράστης να εντοπισθεί στην Α χώρα και τα αποδεικτικά στοιχεία μπορεί να βρίσκονται σε διαφορετική και απομακρυσμένη χώρα ή και να βρίσκονται ταυτόχρονα σε πολλές διαφορετικές χώρες.

- Η έρευνα απαιτεί κατά κανόνα συνεργασία δύο τουλάχιστον κρατών (του κράτους στο οποίο έγίνε αντιληπτό το αποτέλεσμα της εγκληματικής συμπεριφοράς, και του κράτους όπου βρίσκονται τα αποδεικτικά στοιχεία). Περιπτώσεις εγκληματικής συμπεριφοράς στα όρια ενός μόνον κράτους είναι σπάνια.
- Η καταγραφή της εγκληματικότητας στον Κυβερνοχώρο δεν ανταποκρίνεται στην πραγματικότητα διότι ελάχιστες περιπτώσεις εγκλημάτων του Κυβερνοχώρου καταγγέλλονται διεθνώς. Κατά συνέπεια, το μέγεθος της εγκληματικότητας στο χώρο του Διαδικτύου είναι «ακόμα πιο σκοτεινό», απ' ότι στον «κοινό» εγκληματικό χώρο.

Οι Hackers και οι Crackers

Τους "εγκληματίες του Κυβερνοχώρου" μπορούμε να τους διακρίνουμε σε δύο κατηγορίες ανάλογα με τον τρόπο διείσδυσης και το επιδιωκόμενο αποτέλεσμα :

α) Σ' αυτούς που "επιτίθενται" στα computers απλώς από ευχαρίστηση ή περιέργεια, χωρίς όμως να επιδιώκουν κάποιο οικονομικό όφελος. Στην κατηγορία αυτή ανήκουν, οι δράστες που "εισβάλουν" σε υπολογιστή δια της χρήσεως του Διαδικτύου (hackers) για να μάθουν απλώς, κάποια προσωπικά στοιχεία, ή για να εντοπίσουν κάποιο πρόβλημα στην πληροφοριακή υποδομή εταιριών, τραπεζών κ.ά. (τρύπα συστήματος), και στη συνέχεια να κοινοποιήσουν αυτό με σκοπό την αμοιβή τους η την πρόσληψή τους στην εταιρία.

β) Σ' αυτούς που ενεργούν από οικονομικό όφελος (crackers). Στην κατηγορία αυτή ανήκουν αυτοί που δεν "εισβάλουν" απλώς για να μάθουν κάτι, αλλά μόλις μάθουν το στοιχείο που επιθυμούν (π.χ. τον αριθμό της πιστωτικής κάρτας) δίνουν και την κατάλληλη εντολή στην Τράπεζα για την μεταφορά ενός ποσού στον λογαριασμό τους.

Ο Νομικός Ορισμός του Hacker

Ως hacker μπορεί να ορισθεί το άτομο εκείνο το οποίο χωρίς δικαίωμα αποκτά πρόσβαση σε στοιχεία που έχουν εισαχθεί σε υπολογιστή ή σε περιφερειακή μνήμη υπολογιστή ή μεταδίδονται με συστήματα τηλεπικοινωνιών. (Οι hackers εμφανίστηκαν για πρώτη φορά κατά τη δεκαετία του 1970 στις ΗΠΑ, ως δράστες σε τηλεπικοινωνιακά συστήματα).

Ιοί – Προστασία των Δεδομένων από Ιούς

Μια ιδιαίτερα συχνή και επικίνδυνη μορφή εγκληματικότητας που εμφανίζεται στο Διαδίκτυο είναι η αλλοίωση ή διαγραφή των δεδομένων με ιούς. Οι ιοί (viruses) των υπολογιστών είναι ειδικά προγράμματα που έχουν την ικανότητα να εξαπλώνονται από μόνα τους. Διακρίνονται σε δύο μορφές : στους ιούς των προγραμμάτων και στους ιούς των συστημάτων. Οι δράστες τιμωρούνται σύμφωνα με το άρθρο 381 του Π.Κ. αλλά έχουν και αστικές ευθύνες.

Μέτρα Προστασίας

Προληπτικά μέτρα προστασίας πρέπει πάντα να λαμβάνονται από τους χρήστες Διαδικτύου, διότι οι κίνδυνοι από ιούς, παράνομες εισβολές και υπερβολικές χρεώσεις σε τηλεφωνικούς λογαριασμούς είναι συχνότατοι.

Κατά προτίμηση, ο χρήστης που εισέρχεται στο Διαδίκτυο από dial up σύνδεση θα πρέπει να κλείνει με κωδικό που θα προμηθευτεί από τον ΟΤΕ τις εξερχόμενες διεθνείς κλήσεις, καθόσον υπάρχει ο κίνδυνος του dialer (πρόγραμμα που συνδέει τον Η/Υ του χρήστη σε ISP της αλλοδαπής με αποτέλεσμα την υπερβολική τηλεφωνική χρέωσή του). Επίσης, ο χρήστης θα πρέπει να έχει εγκαταστήσει προγράμματα για την προστασία από ιούς και ηλεκτρονικές επιθέσεις.

Κίνδυνοι για τα Παιδιά

- Τα παιδιά μπορούν να εκτεθούν σε ακατάλληλο πορνογραφικό ή προσβλητικό περιεχόμενο.
- Τα παιδιά μπορούν να έρθουν σε επαφή με αγνώστους που μπορούν να τα βλάψουν.
- Τα παιδιά υπόκεινται σε πιέσεις από τις έμμεσες αλλά επιβλητικές διαφημίσεις στο Διαδίκτυο.
- Τα παιδιά μπορούν να εθιστούν στη χρήση του Διαδικτύου και έτσι κινδυνεύουν να παραμελήσουν τις κοινωνικές τους δραστηριότητες, τις σχολικές τους υποχρεώσεις και τα παιχνίδια τους με φίλους.

Συμβουλές για τα Παιδιά

- Εξηγείτε στους γονείς σας τις εμπειρίες σας κατά την περιπλάνησή σας στο Διαδίκτυο.
- Πάντα να μιλάτε στους γονείς σας ή σε κάποιον ενήλικα για εικόνες ή κείμενα που βρήκατε στο Διαδίκτυο και σας ανησυχούν ή σας φοβίζουν.
- Διαφυλάσσετε τις προσωπικές σας πληροφορίες. Ποτέ μην δίνετε το όνομα σας, την διεύθυνσή σας, την διεύθυνση και το όνομα του σχολείου σας, το τηλέφωνό σας, φωτογραφίες σας σε αγνώστους που συναντάτε στο Διαδίκτυο ακόμη και αν σας το ζητήσουν.
- Κρατάτε τον κωδικό εισόδου στον υπολογιστή σας μυστικό. Είναι σαν το κλειδί του σπιτιού σας που δεν θα το δανείζετε σε κανέναν.
- Μόνο με την άδεια και την παρουσία των γονιών σας μπορείτε να συμφωνήσετε να συναντήσετε κάποιον/κάποια που γνωρίσατε στο Διαδίκτυο.
- Προσέχετε όταν μιλάτε διαμέσου chatroom ή e-mail. Διακόψτε τη συνομιλία όταν κάποιοι σας κάνουν να νιώθετε άβολα.
- Μην εμπιστεύεστε ό,τι διαβάζετε στο Διαδίκτυο. Μάθετε να βλέπετε το περιεχόμενο με κριτικό μάτι.

Συμβουλές για τους Γονείς

- Κρατήστε τον ηλεκτρονικό υπολογιστή σε χώρους όπως το σαλόνι και όχι σε υπνοδωμάτια. Ασχοληθείτε με τον τρόπο που δουλεύει το Διαδίκτυο και αφιερώστε χρόνο να περιηγηθείτε μαζί με τα παιδιά σας στον Κυβερνοχώρο και μάθετε απ' αυτά.
- Σιγουρευτείτε ότι τα παιδιά σας είναι ενήμερα, ότι πρέπει να ανησυχούν για αγνώστους που συναντούν μέσω του ηλεκτρονικού υπολογιστή. Όπως ακριβώς είμαστε ανήσυχοι όταν άγνωστοι χτυπάνε την πόρτα του σπιτιού μας, έτσι δεν πρέπει τα παιδιά να δίνουν προσωπικές πληροφορίες για τους εαυτούς τους.
- Να είστε ιδιαίτερα προσεχτικοί όταν τα παιδιά χρησιμοποιούν τα chatrooms (δωμάτια συνομιλίας), χωρίς την επίβλεψή σας. Μην αφήσετε τα παιδιά σας να συναντήσουν κάποιον που γνώρισαν μέσω του Διαδικτύου χωρίς να είστε και εσείς μαζί.
- Ενθαρρύνετε τα παιδιά σας να προτιμούν τις ιστοσελίδες που εσείς θέλετε και όχι αυτές που θεωρείτε ανάρμοστες.
- Εγκαταστήσετε στον υπολογιστή σας κάποιο λογισμικό φίλτρο που απαγορεύει την προσπέλαση σε συγκεκριμένες σελίδες του Διαδικτύου.
- Συζητήστε με τα παιδιά σας για την ασφάλεια του Διαδικτύου. Συζητώντας τους μελλοντικούς κινδύνους μέσω του Διαδικτύου με τα παιδιά χρειάζεται να δείξετε ευαισθησία και έγνοια έτσι ώστε να κατανοήσουν και τα ίδια τους κινδύνους.
- Γνωρίστε ποιους πρέπει να ενημερώσετε και εν ανάγκη να καταγγείλετε σε περίπτωση που συναντήσετε βλαβερό και παράνομο περιεχόμενο στο Διαδίκτυο.

Τα Λογισμικά Φίλτρα

Ένα φίλτρο είναι ένα πακέτο λογισμικού το οποίο μπορεί να αποκλείσει την προσπέλαση σε τόπους του Κυβερνοχώρου με παράνομο ή επιβλαβές περιεχόμενο. Η αποτελεσματικότητα ενός φίλτρου εξαρτάται από την επινοητικότητα του λογισμικού καθώς και από το πόσο ανανεωμένες είναι οι λίστες με τους απαγορευμένους τόπους. Διαφορετικά φίλτρα είναι αποτελεσματικά στο να αποκλείουν την πρόσβαση σε τόπους με διαφορετικό περιεχόμενο.

Για παράδειγμα, κάποιο φίλτρο μπορεί να είναι πιο αποτελεσματικό στο να αποκλείει την πρόσβαση σε τόπους με πορνογραφικό περιεχόμενο, ενώ κάποιο άλλο να είναι πιο αποτελεσματικό σε περιεχόμενο με βία η ρατσισμό.

Κάποιοι από τους παροχείς υπηρεσιών Ίντερνετ έχουν ήδη εγκαταστήσει λογισμικά φίλτρα στις υπηρεσίες τους. Σ' αυτήν την περίπτωση δεν είναι αναγκαία η εγκατάσταση άλλων φίλτρων.

Εν κατακλείδι

Έχει γίνει σαφές ότι η απεριόριστη χρήση των Ηλεκτρονικών Υπολογιστών και η λειτουργία του Διαδικτύου δίνουν απεριόριστες δυνατότητες και συμβάλλουν στην οικονομική ανάπτυξη των κρατών.

Ο Προϊστάμενος του Τμήματος Ηλεκτρονικού Εγκλήματος/ΔΑΑ, Αστυνόμος Α' κ. Εμμανουήλ Σφακιανάκης -τον οποίο ευχαριστούμε για κάθε δυνατή πληροφορία που μας παρείχε για την ολοκλήρωση της παρουσίασης- συνοψίζοντας, θεωρεί ότι : *«Η τεχνολογική υποδομή μαζί με τη νομοθεσία είναι απολύτως αναγκαίες για την σωστή τεκμηρίωση των εξιχνιασθέντων υποθέσεων που αφορούν ηλεκτρονικά εγκλήματα.*

Στην περίπτωση που θα υπάρχει τεχνολογική υποδομή χωρίς την κατάλληλη νομοθεσία, μέσα από την οποία θα οριοθετούνται οι εγκληματικές συμπεριφορές, τότε θα έχουμε πρόβλημα ως προς την απονομή δικαιοσύνης.

Σύμφωνα με έρευνα μέσω των πληροφοριακών δικτύων (κυρίως του Διαδικτύου) και με χρήση των συστημάτων ηλεκτρονικής μεταφοράς οικονομικών μεγεθών (electronic funds transfer systems ή EFTS) διακινούνται καθημερινά πάνω από 2 τρισεκατομμύρια δολάρια μόνο στις ΗΠΑ σε 700.000 συναλλαγές, ενώ στον κόσμο η εκτίμηση ανεβάζει το ποσό στα 5 τρισεκατομμύρια.

Κατά μέσο όρο λοιπόν στον κόσμο διακινούνται ηλεκτρονικά πάνω από 3,5 δισεκατομμύρια δολάρια το λεπτό. Αυτά τα ποσά εποφθαλμιούν οι crackers, οι οποίοι διαθέτουν τις γνώσεις για να τολμήσουν να επιτεθούν και ίσως να σπάσουν τους κωδικούς προστασίας των συστημάτων, αποκτώντας πρόσβαση σ' αυτά τα ποσά.

Μέσω της δυναμικής εισβολής του ηλεκτρονικού υπολογιστή και της λειτουργίας του Διαδικτύου αναπτύσσονται τεράστιες δυνατότητες χρήσης και κατάχρησης που αφορούν την ηλεκτρονική επεξεργασία δεδομένων. Η ηλεκτρονική εγκληματικότητα συνεχώς εμπλουτίζεται και η πιθανότητα εμφάνισης νέων μορφών στο μέλλον, επιβάλλουν τη συντομότερη και καλύτερη αντιμετώπιση του θέματος, την πραγματοποίηση συλλογικής προσπάθειας και διασυνοριακής συνεργασίας».

Ανθ/μος Κωνσταντίνος Γ. Κούρος

Το παραπάνω άρθρο θα το βρείτε στο link
http://www.ydt.gr/main/Article.jsp?ArticleID=83890

Στο κείμενο είμαι σίγουρος ότι θα βρείτε χρήσιμες πληροφορίες για το ηλεκτρονικό έγκλημα. Όλοι όσοι υποπίπτουν σε τέτοιου είδους εγκλήματα είχαν την ψευδαίσθηση ότι το δίκτυο τους παρέχει ανωνυμία. Δυστυχώς γι' αυτούς, με τις σύγχρονες μεθόδους παρακολούθησης, τα πράγματα δεν είναι και τόσο ευχάριστα.

Παρακάτω σας παραθέτω ένα περιστατικό το οποίο έγραψε ο Γιώργος Επιτήδειος στην ιστοσελίδα http://www.eeei.gr/interbiz/articles/gunhus.htm

Μια περίπτωση συκοφαντικής δυσφήμισης μέσω Internet
22/6/2001 (Ενα παράδειγμα από τις ΗΠΑ, και ο τρόπος ανακάλυψης του ενόχου). Γιώργος Επιτήδειος, gepiti@gepiti.com

Η Ανωνυμία στο Internet

Ένα πολύ γνωστό ρητό υποστηρίζει ότι : *"In the Internet nobody knows you are a dog"*, θέλοντας έτσι να τονίσει ότι μέσα στο δίκτυο είναι πολύ εύκολο να κρατήσεις την ανωνυμία σου. Ωστόσο, κάθε ενέργειά μας στον κυβερνοχώρο αφήνει πίσω της ίχνη και μόνο ένας πολύ καλός γνώστης του δικτύου μπορεί να καλύψει αρκετά απ' αυτά, δυσκολεύοντας έτσι το έργο όσων τον αναζητούν.

Τα Συκοφαντικά e-mails

Αυτό το μάθημα έλαβαν (με πολύ σκληρό τρόπο) οι συνεργάτες ενός Γερουσιαστή από τη Μινεσότα των ΗΠΑ (του Rod Grams) οι οποίοι χρησιμοποίησαν ένα δωρεάν e-mail account από το Hotmail για να εξαπολύσουν μια σειρά από κατηγορίες εναντίον του αντιπάλου του κ. Mike Ciresi.

Στην αρχή οι συνεργάτες του Ciresi δεν αντιλήφθηκαν κάτι ύποπτο, θεωρώντας ότι τα e-mails (που υπέγραφε κάποια Katie Stevens) ήταν απλώς αυτό που ισχυρίζονταν (διαμαρτυρίες μιας ομάδας πολιτών). Έτσι, έγραψαν ένα ευγενικό γράμμα στην Stevens και ζήτησαν μια συνάντηση για να γνωριστούν μαζί της και να της εξηγήσουν τις θέσεις τους. Εκείνη όμως στην αρχή αρνήθηκε κάθε επαφή, δηλώνοντας μάλιστα : *"Please don't try to find out who we are"*, ενώ μετά από επίμονες εκκλήσεις συμφώνησε τελικά σε μια συνάντηση, αλλά δεν εμφανίστηκε ποτέ στο ραντεβού.

Από εκείνη τη στιγμή πλέον πολλοί άρχισαν να υποπτεύονται ότι υπήρχε κάτι ύποπτο σ' αυτή την υπόθεση και ξεκίνησαν έρευνες για να ανακαλύψουν τι ακριβώς συνέβαινε.

Η Ανακάλυψη του Ενόχου

Στοιχείο 1^{ο} :

Μια και τα e-mails περιείχαν συνημμένα αρχεία word κάποιος σκέφθηκε να επιλέξει File - Properties - Summary (Αρχείο - Ιδιότητες - Σύνοψη) και προς μεγάλη του έκπληξη διάβασε ότι ως συγγραφείς των αρχείων είχαν δηλωθεί μέλη της ομάδας του (πρώην και αγωνιζόμενου για την επανεκλογή του) Γερουσιαστή Grams μεταξύ των οποίων συμπεριλαμβανόταν και η διευθύντρια του γραφείου του και σύζυγός του Christine Gunhus!

Ακόμη περισσότερα ονόματα στελεχών του Grams ανακαλύφθηκαν στο ίδιο σημείο (File - Properties) μέσω της επιλογής Statistics (Στατιστικά Στοιχεία) όπου αναφέρεται ποιος ήταν ο τελευταίος χρήστης που αποθήκευσε το συγκεκριμένο αρχείο.

Στοιχείο 2^{ο} :

Φυσικά, οποιοσδήποτε θα μπορούσε να δημιουργήσει ένα αρχείο word, δηλώνοντας ως συγγραφέα κάποιον άλλον οπότε τα παραπάνω αποτελούσαν απλή ένδειξη και όχι απόδειξη. Έτσι, οι συνεργάτες του Ciresi επικοινώνησαν με το Hotmail και ζήτησαν να μάθουν από ποια IP διεύθυνση στάλθηκαν αυτά τα μηνύματα. Όπως αποδείχθηκε, το πρώτο είχε σταλεί από ένα Internet Cafe οπότε δεν ήταν δυνατόν να ανακαλυφθεί ο αποστολέας. Φαίνεται όμως ότι στη συνέχεια οι προφυλάξεις θεωρήθη-

καν περιττές και πολλά από τα υπόλοιπα μηνύματα είχαν αποσταλεί από υπολογιστές που βρίσκονταν στα γραφεία της προεκλογικής εκστρατείας του κ. Grams!

Στοιχείο 3° :

Το θέμα είχε αρχίσει τώρα να γίνεται τόσο σοβαρό ώστε μερικοί χρησιμοποίησαν τον όρο Wordgate για να περιγράψουν όσα είχαν συμβεί. Ωστόσο, η συλλογή των στοιχείων δεν είχε τελειώσει. Κάποιος θυμήθηκε ότι πριν από αρκετούς μήνες η Microsoft παραδέχθηκε πως έδινε έναν μοναδικό αριθμό (Globally Unique Identifier ή GUID) σε κάθε υπολογιστή και ότι τα Windows μετέδιδαν αυτό το νούμερο, που αποτελείται από 32 ψηφία, στην Microsoft κατά την ψηφιακή δήλωση του προϊόντος.

Αν και το Microsoft Word διαθέτει τον δικό του GUID δεν λήφθηκαν στοιχεία από τη Microsoft μια και η διαδικασία θα ήταν αρκετά χρονοβόρα, ενώ αν το προϊόν δεν είχε δηλωθεί ηλεκτρονικά ο αριθμός δεν θα είχε καταχωρηθεί στη βάση δεδομένων της εταιρείας. Λίγοι όμως γνωρίζουν ότι οι κάρτες δικτύου (Ethernet) διαθέτουν τις δικές τους μοναδικές διευθύνσεις τις οποίες το Word καταχωρεί μαζί με το GUID σε κάθε έγγραφο που δημιουργεί!

Οπλισμένοι με αυτό το στοιχείο οι άνθρωποι του υποψήφιου γερουσιαστή Mike Ciresi κατέφυγαν στην αστυνομία η οποία εξέδωσε ένταλμα και μετά από επί τόπου έλεγχο ανακάλυψε ότι η κάρτα δικτύου που αναφερόταν στο GUID των αρχείων Word βρισκόταν στον Η/Υ της διευθύντριας της εκστρατείας και συζύγου του Grams, Christine Gunhus!

Στοιχείο 4° :

Η ενοχή της Christine Gunhus έγινε ακόμη πιο εμφανής όταν η μελέτη των ηλεκτρονικών αρχείων του Hotmail (βλέπε στοιχείο 2) αποκάλυψε ότι μερικά e-mails είχαν σταλεί από το σπίτι της! Και εδώ η απόδειξη ήρθε από τις IP διευθύνσεις αποστολής οι οποίες ανήκαν στην ATT WorldNet. Μια μελέτη στα αρχεία (log files) της εταιρείας έδειξε ότι τις ώρες που στάλθηκαν τα e-mails η IP διεύθυνση αυτή χρησιμοποιείτο από έναν αριθμό τηλεφώνου ο οποίος όπως αποδείχθηκε ήταν εκείνος του σπιτιού της Christine Gunhus.

Συμπεράσματα

Αφήνοντας το ηθικό θέμα της υπόθεσης κατά μέρος (όχι γιατί δεν είναι σημαντικό, αλλά διότι δεν αφορά αυτό το άρθρο), το συγκεκριμένο περιστατικό μάς διδάσκει ότι : *"Ουδέν κρυπτόν υπό τον ήλιον"*. Κάθε μας ενέργεια καταγράφεται σε πολλαπλά σημεία τόσο στο Internet όσο και μέσα στον ίδιο τον υπολογιστή μας. Καλύτερα λοιπόν να μη βασιζόμαστε στην ανωνυμία του δικτύου διότι είναι περισσότερο ευάλωτη απ' ό,τι νομίζαμε.

Γιώργος Επιτήδειος

Ακολουθεί ένα δεύτερο άρθρο από την ιστοσελίδα http://www.go-online.gr και αφορά την ανωνυμία μέσω Internet.

«Πότε άλλοτε δεν υπήρξε μεγαλύτερη ανάγκη για ανωνυμία και προστασία ιδιωτικού απορρήτου στο Internet. Κυβερνήσεις, οργανισμοί και πολυεθνικές εταιρείες επιχειρούν -καθένας για τους δικούς τους λόγους- να καταγράψουν, να ελέγξουν ή ακόμα και να περιορίσουν τις διαδικτυακές συνήθειες των κυβερνοπολιτών. Ποιες όμως είναι οι επιλογές που έχετε ώστε να διώξετε από πάνω σας τα αδιάκριτα μάτια;

Ξεκινώντας σχεδόν από το 1995 και φθάνοντας κατά την τελευταία πενταετία στην ολοκλήρωση, το Internet γνώρισε μια μετεξέλιξη που το μεταμόρφωσε από ένα άκρως δημοκρατικό forum σ' ένα εμπορευματοποιημένο μέσο, που είναι στα χέρια κρατικών και ιδιωτικών φορέων. Φορέων, που στην πλειοψηφία τους επιχειρούν και συνήθως κατορθώνουν να καταγράφουν και να περιορίζουν δραστηριότητες και συνήθειες των χρηστών του Internet για εμπορικούς αλλά και πολιτικούς λόγους.

Η ίδια η αρχιτεκτονική του Internet (κυρίως η server – client φιλοσοφία που διέπει το Διαδίκτυο και όλα τα χρησιμοποιούμενα πρωτόκολλά του) καθιστά εύκολη την καταγραφή της συμπεριφοράς των χρηστών, ενώ η ανάπτυξη ολοένα πιο "έξυπνων" μηχανισμών παρακολούθησης σε συνδυασμό με την γνωστοποίησή τους λειτουργούν ανασταλτικά στην εξάσκηση του αναφαίρετου δικαιώματος της ελευθερίας του λόγου.

Σε μια ακραία περιγραφή της υπάρχουσας κατάστασης, μπορούμε να πούμε ότι έχει διαμορφωθεί ένας νέος ψηφιακός άγραφος νόμος σε ορισμένες χώρες του πλανήτη που έχει ως εξής: *"Είσαι ελεύθερος να πεις ό,τι θες, αρκεί να υποστείς τις συνέπειες"*. Οι κυριότερες απειλές που ενδέχεται να αντιμετωπίσετε ως χρήστες του Internet σήμερα, προέρχονται από : Το x άτομο που επικοινωνεί, είτε μέσω e-mail, σε chat rooms και message boards είτε μέσω instant messengers.

Αν δεν γνωρίζετε το άτομο στην πραγματική ζωή, καλό θα ήταν να αποφύγετε να του αποκαλύψετε την πραγματική σας ταυτότητα. Είναι απίστευτο το μέγεθος των πληροφοριών που μπορεί να συγκεντρώσει κάποιος μύστης απλά και μόνο γνωρίζοντας το όνομά σας. Πρόκειται για μια μορφή social engineering/phreaking (απόσπαση πληροφοριών μέσω κοινωνικής εξαπάτησης π.χ. μέσω τηλεφώνου) πολύ δημοφιλή στην τάξη των hackers.

- Άτομα που έχουν φυσική πρόσβαση στον υπολογιστή σας

Φροντίστε όταν έχετε κάποια δραστηριότητα που θέλετε να αποκρύψετε από το οικείο ή και το εταιρικό σας περιβάλλον :

α) να μην έχετε απρόσκλητη παρέα πάνω από το κεφάλι σας και

β) εφόσον κάποιος άλλος χρησιμοποιεί τον υπολογιστή, τίποτα να μην αποκαλύπτει τις συνήθειές σας.

- Διαχειριστές Web sites που επισκέπτεστε

Οι περισσότεροι Web administrators (και όχι μόνο) έχουν ως χόμπι την ανάλυση των logs (αρχεία καταγραφής δραστηριότητας) του Web site που διαχειρίζονται. Μέσα απ' αυτά τα logs παίρνουν πληροφορίες όπως αριθμός επισκέψεων διεύθυνση και αριθμός αιτήσεων ανά IP, τύπος αιτήσεων (ποια αρχεία) κ.ο.κ.

Το μόνο που χρειάζεται είναι ένα καλό πρόγραμμα ούτως ώστε να γίνει πλήρης ομαδοποίηση των "δραστηριοτήτων σας" και η ανάλυση των cookies που έχετε στον υπολογιστή σας για να δημιουργηθεί το προφίλ σας (ως ένα βαθμό βέβαια ατελές).

- ISPs και λοιπούς παροχείς δικτυακών υπηρεσιών

Οποιοσδήποτε σας παρέχει σε κάποιο βαθμό πρόσβαση στο Internet και πρόσβαση σε συγκεκριμένες υπηρεσίες μπορεί να σας ελέγξει. Απλοί μηχανισμοί επιτρέπουν την καταγραφή όλων των εισερχόμενων/εξερχόμενων δεδομένων στον server που λειτουργεί ως η προσωπική πύλη σας στο Internet.

- Crackers

Εκμεταλλευόμενοι τα κενά ασφάλειας του λειτουργικού συστήματος και του browser που χρησιμοποιείτε, οι crackers μπορούν να αποκτήσουν εύκολα πρόσβαση σ' όλα τα αρχεία του υπολογιστή σας, συγκεντρώνοντας μεγάλο αριθμό πληροφοριών για τις δικτυακές σας συνήθειες αλλά και όποια ευαίσθητα προσωπικά δεδομένα συνηθίζετε να διατηρείτε στον υπολογιστή σας.

- Πολυεθνικές και διαφημιστικές εταιρείες

Οι μεγάλες εταιρείες έχουν δύο λόγους για να ελέγχουν την αναπτυσσόμενη δικτυακή δραστηριότητα των χρηστών καθώς και τις δικτυακές του συνήθειες. Ο πρώτος είναι η συλλογή στατιστικών στοιχείων για (υπέρ το δέον) επιτυχημένη έρευνα αγοράς, ο δεύτερος είναι ο ίδιος ο πόλεμος των πληροφοριών – εξάλλου το παιχνίδι της εξουσίας έχει να κάνει με τον έλεγχο της γνώσης.

- Κυβερνήσεις

Οι κυβερνήσεις και ιδίως αυτές των μεγάλων χώρων του πλανήτη μπορούν να ασκήσουν πιέσεις στους ίδιους τους παροχείς της δικτυακής υποδομής του Internet, των εταιρειών δηλαδή που ευθύνονται για την κεντρική λειτουργία του Διαδικτύου και να ελέγξουν όλη την αναπτυσσόμενη δικτυακή δραστηριότητα.

Φημολογείται ότι τέτοια είδους παρακολούθηση ήδη υφίσταται ενώ ο αντίλογος ισχυρίζεται ότι είναι τέτοιος ο όγκος των πληροφοριών που είναι αδύνατη η επεξεργασία του, ωστόσο κανείς δεν μπορεί να είναι σίγουρος».

Το παραπάνω κείμενο θα το βρείτε στο link :
http://www.go-online.gr/ebusiness/specials/article.html?article_id=417

«Ουδέν κρυπτόν υπό τον ήλιο» γράφει ο κ. Επιτήδειος και μάλλον έχει δίκιο.

- Τι γίνεται όμως στη χώρα μας;
- Πώς μπορεί να προστατευθεί ο χρήστης του Διαδικτύου;

Τα τελευταία χρόνια λειτουργεί στη χώρα μας μια ιστοσελίδα, στην οποία ο χρήστης του διαδικτύου μπορεί να κάνει ανώνυμες ή επώνυμες καταγγελίες, για διάφορα θέματα που αφορούν το ηλεκτρονικό έγκλημα και υποπίπτουν στην αντίληψή του. Είναι η http://www.safeline.gr. Σ' αυτή τη σελίδα θα βρείτε χρήσιμες πληροφορίες για το ποια είναι η διαδικασία υποβολής της καταγγελίας, καθώς και τις ενέργειες αυτού του φορέα μόλις λάβει την καταγγελία σας.

Στην προσπάθεια αυτή, της συγκέντρωσης στοιχείων, με βοήθησαν ιδιαίτερα τα παρακάτω sites :

- http://www.go-online.gr
- http://news.pathfinder.gr/periscopio
- http://www.ydt.gr
- http://www.eeei.gr

Με τιμή,

lionheart

ΠΕΡΙΕΧΟΜΕΝΑ