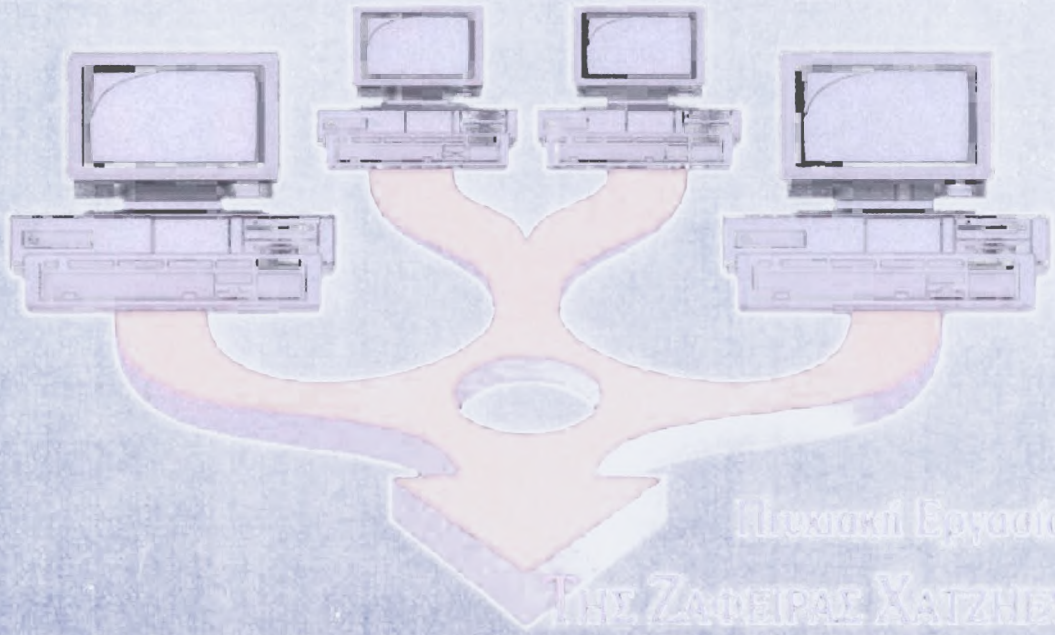
Τ.Ε.Ι. ΜΕΣΟΛΟΓΓΙΟΥ
ΣΧΟΛΗ ΔΙΟΙΚΗΣΗΣ ΟΙΚΟΝΟΜΙΑΣ
ΤΜΗΜΑ: ΣΤΕΛΕΧΩΝ ΣΥΝΕΤΑΙΡΙΣΤΙΚΩΝ ΟΡΓΑΝΩΣΕΩΝ & ΕΚΜΕΤΑΛΛΕΥΣΕΩΝ

Η ΗΛΕΚΤΡΟΝΙΚΗ ΠΡΟΩΘΗΣΗ ΠΡΟΪΟΝΤΩΝ ΤΩΝ ΠΑΝΕΠΙΣΤΗΜΙΑΚΩΝ ΕΠΙΧΕΙΡΗΣΕΩΝ



Πτυχιακή Εργασία
Των Ζαφείρας Χατζηευστρατίου

Επιβλέπων Καθηγητής
Δρ. Χρήστος Τσουραμάνης

ΜΕΣΟΛΟΓΓΙ 2000

***Ε**υχαριστώ, του καθηγητή κ. Χρήστο Τσουραμάνη*

για την πολύτιμη βοήθειά του στην προετοιμασία αυτής της εργασίας. Το πνεύμα συνεργασίας που τον διακατέχει, οι ιδέες του και οι υποδείξεις του υπήρξαν ιδιαίτερα χρήσιμες για την συγγραφή της.

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

ΕΙΣΑΓΩΓΗ

Η πτυχιακή εργασία με αντικείμενο την «Ηλεκτρονική προστασία πληροφοριών των συνεταιριστικών επιχειρήσεων» αναφέρεται σε μεγάλο μέρος της στους Hackers διότι αυτοί είναι ο μοναδικός κίνδυνος διαρροής των πληροφοριών μιας συνεταιριστικής επιχείρησης μέσα από ένα ηλεκτρονικό σύστημα πληροφοριών.

Τεράστια ανάπτυξη του Internet, του διεθνούς διαδικτύου, που σημειώθηκε τα τελευταία χρόνια είχε μεταξύ άλλων και μια σημαντική παρενέργεια : τη χρησιμοποίησή του για παράνομη διείσδυση σε διάφορα μικρότερα δίκτυα ακόμη και συνεταιριστικών επιχειρήσεων που είναι συνδεδεμένες με αυτό.

Στοχεύοντας στην παραπέρα διερεύνηση του θέματός μας θα ασχοληθούμε με την παράνομη διείσδυση στα συστήματα Η/Υ, γενικότερα των επιχειρήσεων και ειδικότερα των συνεταιριστικών επιχειρήσεων, που αναπτύσσουν τις δραστηριότητές τους στο Internet.

Ειδικότερα θα εξετάσουμε τα εξής :

- Την **πράξη** της παράνομης διείσδυσης (hacking) στο σύστημα Η/Υ μιας συνεταιριστικής επιχείρησης και τους σκοπούς που αυτή μπορεί να εξυπηρετεί,
- Την προσωπικότητα και τα κίνητρα των **δραστών** καθώς και τον τρόπο δράσης τους και τέλος
- Την **αντιμετώπιση** της παράνομης αυτής συμπεριφοράς δηλ τα μέτρα ασφάλειας που θα πρέπει να λαμβάνονται για την προστασία πληροφοριών που μια συνεταιριστική επιχείρηση θεωρεί ότι δεν θα πρέπει να γνωρίζουν το ευρύτερο κοινό και οι ανταγωνιστές της.

Η σύνδεση μιας συνεταιριστικής επιχείρησης με το internet χωρίς τη λήψη των απαραίτητων μέτρων για την ασφάλεια των πληροφοριών

αυτών είναι πολύ πιθανό να συντελέσει στην εύκολη θυματοποίησή της. Στην αντίθετη περίπτωση οι πιθανότητες να είναι ένα ακόμη εύκολο θύμα hacking, μειώνονται σημαντικά. Η μέχρι σήμερα πρακτική όμως έχει αποδείξει δυστυχώς την ανεπάρκεια των μέτρων αυτών σε σημείο που η παραβίασή τους να είναι σε πολλές περιπτώσεις εφικτή ακόμη και από έναν περιστασιακό "δράστη".

Η γνώση λοιπόν των κινδύνων που πιθανότατα διατρέχει κάθε συνεταιριστική επιχείρηση με την δραστηριοποίησή της μέσα στον χώρο του internet καθώς και των μέτρων που θα πρέπει να λάβει για την αποτροπή τους είναι βέβαιο ότι αποσκοπεί αποκλειστικά και μόνο στην προστασία των συμφερόντων της.

Στην εργασία αυτή γίνεται συνεχώς αναφορά στις συνεταιριστικές επιχειρήσεις διότι αυτό είναι και το αντικείμενό της, παρόλα αυτά θέλω να διευκρινίσω πως τα παραπάνω ισχύουν για όλες τις επιχειρήσεις είτε του ιδιωτικού είτε του δημόσιου τομέα καθώς και των διαφόρων οργανισμών, με απαραίτητη προϋπόθεση φυσικά να έχουν σύνδεση με το Internet.

ΚΕΦΑΛΑΙΟ 1

Η ΠΑΡΑΝΟΜΗ ΠΡΟΣΒΑΣΗ ΣΕ ΣΤΟΙΧΕΙΑ Η/Υ ΤΩΝ ΣΥΝΕΤΑΙΡΙΣΤΙΚΩΝ ΕΠΙΧΕΙΡΗΣΕΩΝ

Το αγαθό με την μεγαλύτερη αξία που κυκλοφορεί στις σημερινές «υπερλεωφόρους της πληροφορικής» είναι η ίδια η πληροφορία. Είναι φυσικό επακόλουθο να γίνονται "μάχες" για την απόκτησή της.

Η κάθε συνεταιριστική επιχείρηση, που έχει σύνδεση με το Internet αντιμετωπίζει κάποιους κινδύνους οι οποίοι έχουν ως στόχο την παραβίαση της ασφάλειας του συστήματος των Η/Υ. Στα συστήματα Η/Υ μιας συνεταιριστικής επιχείρησης βρίσκονται πληροφορίες, για την ίδια την επιχείρηση που ενδιαφέρουν μια μερίδα επιτήδειων ανθρώπων, των hackers.

Η παράνομη πρόσβαση σε στοιχεία Η/Υ μπορεί να θεωρηθεί από τον ποινικό νόμο μιας χώρας ως έγκλημα και οι δράστες αυτοί να τιμωρούνται με τις αντίστοιχες ποινές. Η προστασία του νόμιμου κατόχου της πληροφορίας αποτελεί υποχρέωση και καθήκον κάθε σύγχρονης έννομης τάξης. Για την δίωξη των εισβολέων εκπαιδεύονται κατάλληλα κάποιοι άνθρωποι. Η εκπαίδευση αυτή μπορεί να θεωρηθεί ιδιαίτερα κρίσιμη λόγου του εξειδικευμένου χαρακτήρα των εγκλημάτων. Χρειάζονται ειδικές γνώσεις όχι μόνο για την εξυγίανσή τους αλλά και την τεκμηριωμένη παραπομπή του δράστη τους στην δικαιοσύνη.

Η σημερινή ευρύτατη διάδοση του Internet έχει αυξήσει τις δυνατότητες εγκλημάτων κατά της ασφάλειας των συστημάτων πληροφοριών, μιας συνεταιριστικής επιχείρησης που είναι συνδεδεμένη με αυτό, δεδομένου ότι η πρόσβαση στα συστήματα αυτά έχει γίνει περισσότερο εύκολη από ποτέ άλλοτε.

Ποια όμως είναι η εγκληματική δραστηριότητα που απειλεί τις συνεταιριστικές επιχειρήσεις οι οποίες είναι στο Internet και κινούνται στον λεγόμενο «κυβερνοχώρο»;

Η δραστηριότητα αυτή είναι γνωστή ως Hacking και προσδιορίζεται στον ποινικό μας κώδικα ως η

«Πρόσβαση σε στοιχεία που έχουν εισαχθεί σε υπολογιστή ή περιφερειακή μνήμη υπολογιστή ή μεταδίδονται σε συστήματα τηλεπικοινωνιών, εφόσον οι πράξεις αυτές έγιναν χωρίς δικαίωμα, ιδίως με παραβίαση μέτρων ασφαλείας που είχε λάβει ο νόμιμος κάτοχός τους ...».

Βλέπουμε λοιπόν εδώ ότι η συγκεκριμένη εγκληματική συμπεριφορά αφορά την παράνομη διείσδυση σε συστήματα και επικοινωνίες υπολογιστών η οποία τελείται με την παραβίαση των μέτρων ασφαλείας που είχε λάβει ο νόμιμος κάτοχός τους.

Νόμιμοι κάτοχοι των συστημάτων αυτών μπορεί να είναι τόσο άτομα (φυσικά πρόσωπα) όσο και συνεταιριστικές επιχειρήσεις (νομικά πρόσωπα) που μας ενδιαφέρουν στην προκειμένη περίπτωση.

Όταν μιλάμε για «επικοινωνία υπολογιστών» εννοούμε το διαδεδομένο πια μέσο της εποχής μας, το Internet.

Ο δράστης – εισβολέας σ' αυτές τις περιπτώσεις μπορεί να ανήκει στο προσωπικό ή να ενεργεί για λογαριασμό των ανταγωνιστών της συνεταιριστικής επιχείρησης – θύματος. Όταν πλέον ο Hacker αποκτά πρόσβαση στις πληροφορίες της επιχείρησης – θύματος, θεωρείται ιδιαίτερα επικίνδυνος εφόσον επιδιώκει το προσωπικό του οικονομικό όφελος, κάτι που μπορεί να το πετύχει με :

Α. Την πειρατεία λογισμικού δηλ. προγραμμάτων Η/Υ

Η πειρατεία αυτή ουσιαστικά συνιστά κλοπή λογισμικού, γίνεται από το δράστη με σκοπό να χρησιμοποιήσει το συγκεκριμένο πρόγραμμα ο ίδιος ή να το πουλήσει σε τρίτους. Το πρόγραμμα αυτό ο δράστης είναι δυνατό να το κατεβάσει στο δικό του Η/Υ από το Site της συνεταιριστικής επιχείρησης στην οποία ανήκει η Εμπορική εκμετάλλευσή του.

Β. Την μεταβολή ή την καταστροφή πληροφοριών ή αρχείων

Αποκτώντας πρόσβαση στο δίκτυο ο δράστης – εισβολέας έχει την ευχέρεια να μεταβάλλει ή να καταστρέψει αρχεία πληροφοριών ή προγραμμάτων, να εισαγάγει ιούς σ' αυτό και γενικά να κάνει οποιαδήποτε άλλη ενέργεια θα το αχρηστεύσει μόνιμα ή προσωρινά, ενεργώντας έτσι προς όφελος των ανταγωνιστών της επιχείρησης αυτής.

Γ. Τη βιομηχανική κατασκοπεία

Τόσο τα άτομα όσο και οι Συνεταιριστικές επιχειρήσεις – καθώς και οι κυβερνήσεις – σπάνια δεν επιθυμούν την κατασκοπεία των ανταγωνιστών τους.

Τα νέα ηλεκτρονικά σύνορα, τους προσφέρουν πολλές ευκαιρίες για να έχουν πρόσβαση σε μέχρι τώρα απρόσιτες πληροφορίες των αντιπάλων τους. Έτσι πολλές επιχειρήσεις επιδιώκουν την απόκτηση τέτοιων πληροφοριών οι οποίες ξεκινούν από τον τρόπο παραγωγής των προϊόντων των ανταγωνιστών τους, και τις εμπορικές τους συμφωνίες με τρίτους και φτάνουν μέχρι τις στρατηγικές marketing που χρησιμοποιούν. Πολύ συχνά λοιπόν η παράνομη διείσδυση στο δίκτυο Η/Υ μιας συνεταιριστικής επιχείρησης μέσω του Internet μπορεί να είναι έργο

ανταγωνιστών της που στοχεύουν με τον τρόπο αυτό στο να τις αποσπάσουν κρίσιμα εμπορικά μυστικά της για προσωπικό τους οικονομικό όφελος.

Δ. Την κλοπή οικονομικών δεδομένων

Στην περίπτωση αυτή το θύμα είναι χρηματοπιστωτικό ίδρυμα δηλ. Τράπεζα κατά κύριο λόγο. Ο δράστης με την είσοδό του στο σύστημα επιδιώκει το σπάσιμο των κωδικών λογαριασμών των πελατών με σκοπό τη μεταφορά του περιεχομένου τους στο δικό του λογαριασμό. Για το θέμα αυτό ο Donald Pipkin παρατηρεί τα εξής :

> «Σημειώνεται πως εάν κάποιος ληστεύσει μια Τράπεζα με πιστόλι θα διωχθεί με κάθε μέσο οπουδήποτε κι αν πάει. Αλλά αν την ληστεύσει με τον Η/Υ του, είναι πάρα πολύ πιθανό η Τράπεζα να μην παραδεχθεί τη ληστεία αυτή προκειμένου να αποφύγει τη δημοσιότητα.
>
> Τα παρακάτω στατιστικά στοιχεία αποδεικνύουν του λόγου το αληθές. Κατά μέσον όρο ένας ένοπλος ληστής αποκομίζει από 2500 έως 7500 δολ. διατρέχοντας τον κίνδυνο να τον πυροβολήσουν και να τον σκοτώσουν. Ποσοστό πενήντα έως 60% από τους ένοπλους ληστές συλλαμβάνεται και από αυτούς το 80% καταδικάζεται και φυλακίζεται κατά μέσο όρο για πέντε χρόνια. Ο μέσος ηλεκτρονικός εγκληματίας θα αποκομίσει από 50 έως 500.000 δολ. και ο μεγαλύτερος κίνδυνος που διατρέχει είναι να χάσει τη δουλειά του και να πάει φυλακή. Ποσοστό 10% από τους εγκληματίες αυτούς ανακαλύπτεται και μόνο το 15% από αυτούς παραδίδεται στις αρχές. Πάνω από 50% από αυτούς τους τελευταίους δεν δικάζονται ποτέ γιατί δεν μπορεί να θεμελιωθεί κατηγορία σε βάρος τους

ελλείψει αποδείξεων ή επειδή το θύμα τους δεν επιθυμεί τη δημοσιότητα. Το 50% αυτών που τελικά δικάζονται και καταδικάζονται μένει στη φυλακή για χρονικό διάστημα όχι μεγαλύτερο των 5 ετών».

Το Hacking στην νομοθεσία μας θεωρείται πλημμέλημα και γι' αυτό τιμωρείται μόνο όταν τελείται με δόλο και η ποινή που μπορεί να επιβληθεί σ' ένα hacker είναι φυλάκιση από 10 ημέρες μέχρι 3 μήνες ή χρηματική ποινή από 10.000 μέχρι 1.000.000 δρχ. Επιβαρυντική για τον δράστη θεωρείται η περίπτωση κατά την οποία ενήργησε με σκοπό να βλάψει τις διεθνείς σχέσεις ή την ασφάλεια του ελληνικού κράτους. Η δίωξη κατά του δράστη γίνεται μετά από έγκληση του παθόντος. Συνήθως όμως σ' αυτά τα περιστατικά δεν έχουμε πλήρη καταγραφή διότι οι επιχειρήσεις – θύματα στις περισσότερες περιπτώσεις αποκρύπτουν το πάθημά τους επειδή πιστεύουν – και όχι άδικα – ότι η κοινοποίησή του στο ευρύ κοινό θα φανερώσει την ανεπάρκεια των συστημάτων ασφαλείας τους, γεγονός που πιθανότατα θα έχει επιπτώσεις στην εμπορική τους πίστη.

ΚΕΦΑΛΑΙΟ 2

HACKER :
Ο ΕΓΚΛΗΜΑΤΙΑΣ ΤΟΥ ΚΥΒΕΡΝΟΧΩΡΟΥ

Αυτός που διεισδύει παράνομα στο σύστημα Η/Υ, είναι ευρύτατα γνωστός στο κοινό και στα Μ.Μ.Ε. με την αγγλική λέξη hacker.

«Hacker είναι μια λέξη της αγγλικής αργό που αναφέρεται σε κάποιον που δεν έχει εκπαιδευτεί στη χρήση του Η/Υ, για τους οποίους όμως επιδεικνύει πολύ μεγάλο ενδιαφέρον. Το άτομο αυτό (hacker) μαθαίνει πειραματιζόμενο με τους Η/Υ κάτι που συνεπάγεται συχνά την θέλησή του να μπει σε βάσεις δεδομένων ή σε συστήματα Η/Υ χωρίς να έχει σχετική εξουσιοδότηση από τον ιδιοκτήτη τους. Ένας hacker μπορεί ή δεν μπορεί να ενδιαφέρεται να αποκτήσει πληροφορίες στις οποίες δεν έχει νόμιμη πρόσβαση».

Για άλλους ο ορισμός για την λέξη hacker έχει ως εξής :

«Hacker είναι ένα πρόσωπο που με πρόθεση εισβάλλει σ' ένα σύστημα Η/Υ, χωρίς προηγούμενη εξουσιοδότηση» και πως :

«ο όρος αυτός χρησιμοποιείται επίσης για να δηλώσει εκείνον που λατρεύει τους Η/Υ και ο οποίος απολαμβάνει τα υπέρ και τα κατά της ενασχόλησής του αυτής».

Από τους παραπάνω ορισμούς προκύπτει ότι σαν **hacker μπορούμε να χαρακτηρίσουμε είτε εκείνον που εισβάλλει παράνομα (χωρίς εξουσιοδότηση) σ' ένα σύστημα Η/Υ ανεξάρτητα για ποιο σκοπό το κάνει αυτό, είτε εκείνον που του αρέσει πολύ να ασχολείται γενικά με τους Η/Υ**. Από τις έννοιες αυτές μας ενδιαφέρει φυσικά η

πρώτη γιατί αυτή είναι εκείνη που μπορεί να χαρακτηρισθεί ως εγκληματική.

Ταυτόσημη είναι και η έννοια του όρου **cracker** η οποία όμως χρησιμοποιείται περισσότερο για να περιγράψει **εκείνον που ασχολείται αποκλειστικά με τη διαγραφή ή την καταστροφή των αρχείων του συστήματος στο οποίο απέκτησε παράνομη πρόσβαση**. Στην περίπτωση αυτή δηλ. θεωρείται δεδομένη η πρόθεση του εισβολέα να βλάψει τα αρχεία του συστήματος αυτού.

Είναι διαπιστωμένο ότι οι hackers αγαπούν την πρόκληση και ότι ασκούν πάνω τους μια παράξενη γοητεία και οι παραμικρές λεπτομέρειες από την τεχνολογία των Η/Υ. Πολλές φορές η γοητεία αυτή τους παρασύρει και έτσι το νόμο χρησιμοποιώντας τους Η/Υ τους.

Ένα συνηθισμένο slogan των hackers είναι το : «Η γνώση αποτελεί δύναμη» και το οποίο αποδίδεται στον Άγγλο φιλόσοφο και πολιτικό του $17^{ου}$ αιώνα Francis Bacon, εκφράζει με τον καλύτερο τρόπο τις αντιλήψεις τους. Η γνώση είναι βέβαιο ότι δίνει τη μεγαλύτερη δύναμη σ' όσους των κατέχουν και μάλιστα στη σημερινή εποχή με τις χιλιάδες βάσεις δεδομένων τις οποίες διαχειρίζονται κυβερνητικοί οργανισμοί και οι Συνεταιριστικές επιχειρήσεις και για την πρόσβαση των οποίων είναι απαραίτητο το Internet. Ιδού λοιπόν ο χώρος στον οποίο ο hacker θα ξεδιπλώσει σήμερα τις απεριόριστες – όπως υποστηρίζει – ικανότητές του !

Πως όμως ξεκίνησαν οι hackers ;

Η σημερινή πορεία των hackers ξεκίνησε από τους νεαρούς Αμερικάνους «Phone phreaks» της δεκαετίας του '60 και του '70 οι οποίοι προσπαθούσαν να ξεγελάσουν ηλεκτρονικά τα συστήματα της

αμερικανικής τηλεφωνικής εταιρείας AT & T με σκοπό να κάνουν μακράς διάρκειας υπεραστικά τηλεφωνήματα χωρίς φυσικά και να τα πληρώνουν.

Η συναρπαστική τέχνη της διερεύνησης ενός συστήματος Η/Υ με σκοπό την διαπίστωση του τρόπου λειτουργίας του ξεκίνησε ουσιαστικά στις αρχές της δεκαετίας του '70 από τους προγραμματιστές που εργάζονταν στα τμήματα Η/Υ και ηλεκτρονικής μηχανικής του M.I.T. (Massachusetts Institute of Technology) του Stanford καθώς και άλλων Πανεπιστημίων. Ο μοναδικός σκοπός των ατόμων αυτών ήταν να μάθουν εξερευνώντας τους Η/Υ, κάθε τι που αφορούσε τον χειρισμό τους και γενικότερα τις αλλαγές που θα μπορούσαν να τους κάνουν για να αυξήσουν την υπολογιστική ισχύ τους. Αυτοί μπορούμε να πούμε πως ήταν και οι πρώτοι hackers, η βασική φιλοσοφία των οποίων ήταν να μην κλέψουν ή να καταστρέψουν τίποτα από ένα σύστημα αλλά να μάθουν τα πάντα γι' αυτό!

Άποψή τους ήταν πως είχαν κάθε δικαίωμα να μπαίνουν σ' ένα σύστημα, χωρίς κανένα περιορισμό εφόσον είχαν τη δυνατότητα να κάνουν κάτι τέτοιο. Δεν είχαν πρόθεση να προξενήσουν καμία βλάβη στη λειτουργία στη λειτουργία του και το μόνο σημάδι που άφηναν για την εισβολή τους ήταν συνήθως ένα μήνυμα για τον υπεύθυνο ασφαλείας με το οποίο του επεσήμαναν τις αδυναμίες του συστήματος. Συνήθως δε, τους τόνιζαν ότι χάρις σ' αυτές πέτυχαν να εισβάλλουν σ' αυτό και πως οποιαδήποτε ενέργειά του για να αποτρέψει μια μελλοντική εισβολή τους δεν θα είχε καμία πιθανότητα επιτυχίας !

Έτσι το hacking θεωρήθηκε αρχικά σαν μια ενδιαφέρουσα «περιπέτεια» η οποία όχι μόνο δεν προξενούσε καμία ζημιά σε κανένα αλλά αντίθετα μπορούσε ίσως να εξυπηρετήσει ακόμα και εκπαιδευτικούς σκοπούς.

Η εμπορευματοποίηση όμως της πληροφορίας και η ανακάλυψη των διαφόρων ιών των Η/Υ δεν άργησε να σημάνει το τέλος της ρομαντικής εποχής των πρώτων hackers – γύρω στις αρχές της δεκαετίας του '80 – ίχνη της οποίας συναντούμε ακόμη και σήμερα με τις εισβολές που γίνονται σε κυβερνητικές υπηρεσίες – κυρίως στις ΗΠΑ – με σκοπό να αποδείξουν την ανεπάρκεια των συστημάτων ασφαλείας τους.

ΚΕΦΑΛΑΙΟ 3

ΚΑΤΗΓΟΡΙΕΣ HACKERS

Ο Othmar Kyas υποστηρίζει ότι μία επιχείρηση ή ένας οργανισμός μπορούν να αναζητήσουν τους hackers που έχουν τη δυνατότητα να προσβάλλουν τα συστήματά τους, σε μία από τις ακόλουθες έξι κατηγορίες ατόμων :

α. Στους φοιτητές Πανεπιστημίων και Κολεγίων καθώς και στους μαθητές μέσης εκπαίδευσης.

β. Ανάμεσα στους υπαλλήλους τους.

γ. Στους ανταγωνιστές τους.

δ. Σε εκείνους που κινούνται στον υπόκοσμο των Η/Υ.

ε. Σε παλιούς εγκληματίες από τον κόσμο των ναρκωτικών και του οργανωμένου εγκλήματος και τέλος

στ. Στους επαγγελματίες που έχουν ως αντικείμενό τους τη βιομηχανική κατασκοπεία.

Για τις πέντε από τις ομάδες αυτές ο Othman Kyas παρατηρεί σε γενικές γραμμές τα ακόλουθα :

α. Για τους φοιτητές και τους μαθητές

Σ' αυτούς οφείλονται οι περισσότερες απόπειρες εισβολών σε δίκτυα επιχειρήσεων, χωρίς αυτό να σημαίνει πως οι ενέργειές τους είναι πάντα επιτυχής.

Το γεγονός ότι έχουν στη διάθεσή τους τα πανίσχυρα υπολογιστικά συστήματα του Πανεπιστημίου τους με ελεύθερη και δωρεάν πρόσβαση στο Internet, το ότι γνωρίζουν πολύ καλά το χειρισμό τους καθώς και το ότι διαθέτουν αρκετό ελεύθερο χρόνο, σε συνδυασμό με μια χιουμοριστική διάθεση που είναι ένα από τα βασικά χαρακτηριστικά της ηλικίας τους, τους καθιστά ίσως τους πιο επικίνδυνους hackers. **Στις περισσότερες περιπτώσεις βέβαια τα άτομα αυτά κάνουν hacking ορμώμενα από ένα συνδυασμό χιούμορ, περιέργειας και επίδειξης των ικανοτήτων τους στους συνομήλικούς τους.**

Η αναζήτηση συγκεκριμένων πληροφοριών δεν είναι το ζητούμενο από αυτά. Αυτό που τους ενδιαφέρει ιδιαίτερα είναι αυτή η ίδια η παράνομη είσοδός τους σ' ένα σύστημα για την οποία θα μπορούν στη συνέχεια να υπερηφανεύονται στους φίλους τους.

Η λήψη των καταλλήλων μέτρων από τον υπεύθυνο ασφαλείας ενός δικτύου μπορεί να αποτρέψει πολλές από τις εισβολές αυτών των hackers για τους οποίους το hacking αποτελεί θα λέγαμε ένα είδος χόμπι, στο οποίο μάλιστα δεν επιδίδονται και πολύ συχνά. Εξάλλου αυτό που τους ενδιαφέρει και που τους καθιστά παράλληλα και κάπως ακίνδυνους για τα θύματά τους είναι το γεγονός ότι νοιάζονται κυρίως για το πώς θα σπάσουν τους κωδικούς ενός συστήματος και θα μπουν σ' αυτό χωρίς παράλληλα να τους ενδιαφέρουν και οι πληροφορίες που αυτό διαθέτει. Εξαιρούνται φυσικά οι περιπτώσεις εκείνες όπου το hacking αφορά τα αρχεία του σχολείου τους και με τις βαθμολογίες που όπως είναι φυσικό η «διορθωτική παρέμβαση» τους αποτελεί και τον κύριο στόχο τους !

β. Για τους υπαλλήλους της επιχείρησης

Έχει διαπιστωθεί ότι οι μεγαλύτερες ζημιές σε συστήματα Η/Υ των επιχειρήσεων οφείλονται σε υπαλλήλους τους οι οποίοι είναι

υπεύθυνοι για τη λειτουργία τους. Σε πολλές περιπτώσεις υπάλληλοι δυσαρεστημένοι από την απέναντί τους πολιτική της επιχείρησης στην οποία εργάζονται – χαμηλοί μισθοί, παράλειψη από προαγωγές, εύνοια σε συναδέλφους τους κ.λ.π – αντιδρούν καταστρέφοντας αρχεία ή σαμποτάροντας το δίκτυο των Η/Υ της επιχείρησης. Οι τρόποι που μεταχειρίζονται γι' αυτό ξεκινούν από το ανοιγοκλείσιμο του ηλεκτρικού ρεύματος στο τμήμα Η/Υ όταν δεν βρίσκεται κανείς άλλος εκεί και φτάνουν μέχρι τις κλοπές αρχείων και την εισαγωγή στο σύστημα καταστρεπτικών ιών. Δεν είναι όμως λίγες και οι περιπτώσεις όπου υπάλληλοι είναι εκείνοι που βοηθούν με την αθέλητη μη λήψη των κατάλληλων μέτρων ασφαλείας, εξωτερικούς εχθρούς της επιχείρησης να αποκτήσουν πρόσβαση σ' αυτό. Μια από τις μεθόδους που χρησιμοποιεί ένας εξωτερικός hacker είναι και η γνώση σαν «Social hacking». Αντί να ξοδεύει το χρόνο του προσπαθώντας να βρει το password για την είσοδό του στο δίκτυο προσποιείται πως είναι ένας δυσαρεστημένος χρήστης ή πελάτης και ζητάει από τον υπάλληλο να το αλλάξει ή να φτιάξει ένα νέο προσωρινό τρόπο εισόδου. Ευκολόπιστοι ή αφελείς οι υπάλληλοι χαλαρώνουν τα μέτρα ασφαλείας δίνοντας έτσι την ευκαιρία στον hacker να μπει στο δίκτυο αποφεύγοντας με τον τρόπο αυτό τα περίπλοκα συστήματα ασφαλείας που έχουν θεσπισθεί για την προστασία του.

γ. Για τους hackers που κινούνται στον υπόκοσμο των Η/Υ

Στην προκειμένη περίπτωση έχουμε να κάνουμε με την αφρόκρεμα των hackers. Πολλοί από αυτούς είναι αυτοδίδακτοι, δεν έχουν κάνει πανεπιστημιακές σπουδές και βασικά προέρχονται από τους λεγόμενους «Phone – phreakers» οι οποίοι στις δεκαετίες 1960 και 1970 έσπαζα κωδικούς τηλεφώνων στις ΗΠΑ με σκοπό βέβαια την αποφυγή της πληρωμής τηλεφωνικών τελών. Απαραίτητη προϋπόθεση για να γίνει

κάποιος hacker είναι η ικανότητά του να μπαίνει σε δίκτυα. Έτσι λοιπόν όποιος ενδιαφέρεται να ενταχθεί σε μια κοινότητα hackers θα πρέπει να εντοπίσει μια σχετική BBS (Bulletin Board Systems) και να κερδίσει έτσι την εμπιστοσύνη των μελών της αναφέροντας τις περιπτώσεις hacking που έχει κάνει και απαντώντας σε «τεχνικές» ερωτήσεις πάνω σε σχετικά ζητήματα. Το μεγαλύτερο επίτευγμα όμως των υποψήφιων μελών είναι η είσοδός τους σ' ένα σύστημα υψηλής ασφάλειας και η έξοδός τους από αυτό χωρίς να τους πάρει είδηση κανένας. Κανόνας είναι στην περίπτωση αυτή η μη διαγραφή ή καταστροφή αρχείων.

Στις δεκαετίες του '60 και του '70 οι hackers είχαν τις ακόλουθες έξι «αρχές» οι οποίες όμως με τα σημερινά δεδομένα θεωρούνται ξεπερασμένες :

« **1)** Η πρόσβαση στα συστήματα Η/Υ (και σε οτιδήποτε δείχνει πως ο κόσμος δουλεύει) θα πρέπει να είναι ελεύθερη και απεριόριστη για όλους.

2) Όλες οι πληροφορίες είναι ελεύθερες.

3) Μην εμπιστεύεσαι τις αρχές, υποστήριξε την αποκέντρωση.

4) Οι hackers θα πρέπει να κρίνονται από αυτά που κάνουν και όχι από την ηλικία, τη φυλή ή την κοινωνική τους θέση.

5) Οι Η/Υ μπορούν επίσης να χρησιμοποιηθούν για να δημιουργήσουν τέχνη και ομορφιά.

6) Οι Η/Υ μπορούν να αλλάξουν τη ζωή προς το καλύτερο.»

Ένας από τους σκοπούς που επιδιώκει ο σημερινός υπόκοσμος των hackers έχει να κάνει με την άποψη που λεει ότι η κοινωνία θα πρέπει να αλλάξει τη στάση της απέναντι στη σύγχρονη τεχνολογία και να κατανοήσει τους κινδύνους που αυτή περικλείει. Αυτό θα έχει σαν συνέπεια ότι θα πρέπει να δείξει κανείς στο κοινό και σε κάθε επιχείρηση

τα προβλήματα που παρουσιάζουν τα συστήματα ασφαλείας των δικτύων Η/Υ που χρησιμοποιούν.

Οι **crackers** αποτελούν την πιο επικίνδυνη κατηγορία του υπόκοσμου των hackers. Έχουν ως σκοπό τους όχι μόνο την πρόσβαση σ' ένα σύστημα αλλά και την προσωρινή ή μόνιμη αχρήστευσή του. Τα άτομα αυτά έχει παρατηρηθεί πως είναι νεαρά αγόρια με ηλικία που ξεκινάει από την εφηβική και φτάνει τα 30 το πολύ χρόνια, μαθαίνουν εύκολα και εγκαταλείπουν συχνά το σχολείο εξαιτίας της υπερβολικής αγάπης τους για ότι έχει σχέση με τους Η/Υ. Κατά τη μετεφηβική τους ηλικία καταφέρνουν συνήθως να βρουν μια δουλειά που σχετίζεται με το μεγάλο πάθος τους, τους Η/Υ και φυσικά δεν προκαλούν καμία υποψία για την ιδιότητά τους δεδομένου ότι είναι πολύ δύσκολο μέχρι τότε να έχουν ήδη καταδικασθεί για κάποια σχετική παράνομη πράξη. Οι crackers έχουν μια φοβερή ικανότητα να παραβιάζουν ακόμα και τα περισσότερο περίπλοκα από άποψη ασφαλείας συστήματα. Οι τεράστιες τεχνικές τους γνώσεις σε συνδυασμό με την ικανότητά τους να κερδίζουν την εμπιστοσύνη των άλλων, τους δίνουν την δυνατότητα να αποσπάσουν τις απαραίτητες πληροφορίες από τους ανύποπτους υπαλλήλους συνεταιριστικής επιχείρησης, οι οποίες θα τους βοηθήσουν στη συνέχεια να αποκτήσουν εύκολη πρόσβαση στα συστήματά της.

δ. Για τους εγκληματίες από τον κόσμο των ναρκωτικών και του οργανωμένου εγκλήματος

Κίνητρα για τα χρησιμοποίηση του Internet από τα άτομα αυτά είναι η ευρύτατη διάδοσή του αλλά και η αδυναμία των διωκτικών αρχών να παρακολουθήσουν εύκολα τα «εγκλήματα» που μπορούν να γίνουν μέσα σ' αυτό.

Οι επαφές για τη διακίνηση ναρκωτικών αλλά και για την τέλεση και άλλων αξιόποινων πράξεων – όπως π.χ. κυκλοφορία πορνογραφικού υλικού – βρίσκουν πρόσφορο έδαφος στον κυβερνοχώρο. Η περαιτέρω δε ενασχόληση των εγκληματικών οργανώσεων με εγκλήματα που τελούνται με την χρήση Η/Υ καθιστά πιθανούς στόχους τους τις συναλλαγές των συνεταιριστικών επιχειρήσεων με τους πελάτες τους. Σαν τέτοιες περιπτώσεις θα μπορούσαν να αναφερθούν π.χ. η υποκλοπή του αριθμού μιας πιστωτικής κάρτας μέσω της οποίας ένας πελάτης πληρώνει την οφειλή του on-line ή η οποιαδήποτε συναλλαγή με μια επιχείρηση – μαϊμού η οποία εισπράττει το οικονομικό αντίτιμο προϊόντων ή υπηρεσιών τις οποίες ουδέποτε παρέχει. Πρέπει να έχουμε υπόψη μας πως πίσω από κάποιες επιχειρήσεις μέσα στο Internet μπορεί να κρύβονται και εγκληματικές οργανώσεις που συναλλασσόμενες κάνουν ξέπλυμα βρώμικου χρήματος.

ε. Για τους επαγγελματίες hackers – βιομηχανικούς κατασκόπους

Η όλο και μεγαλύτερη διείσδυση του Internet στον εμπορικό χώρο έχει ανοίξει την όρεξη των επαγγελματικών κλεπτών διαφόρων δεδομένων. Ορισμένοι από αυτούς προέρχονται από τον υπόκοσμο των Η/Υ και οι υπόλοιποι είναι ειδικοί που εργάζονται στους Η/Υ. Τα άτομα αυτά συνήθως ψάχνουν σε BBS για να βρουν πληροφορίες που θα τα οδηγήσουν στο σπάσιμο των κωδικών ενός συστήματος, με σκοπό να τις πουλήσουν. Άλλες ανάλογες πληροφορίες που θα πέσουν κατά τύχη στα χέρια τους τις πουλούν σε όποιον τους προσφέρει τα περισσότερα. Τα άτομα αυτά πιστεύεται πως στρατολογούνται είτε από κυβερνητικές υπηρεσίες είτε από επιχειρήσεις προκειμένου να κάνουν βιομηχανική κατασκοπεία.

Θα πρέπει να σημειώσουμε ακόμη πως η επικινδυνότητα των hackers εξαρτάται από τα κίνητρά τους. Αν τα κίνητρά τους είναι η διασκέδαση ή η επιθυμία τους να αναγνωριστούν στον κύκλο τους ως αυθεντίες στους Η/Υ ή να μάθουν τον τρόπο λειτουργίας του συστήματος μιας επιχείρησης η παράνομη πρόσβασή τους σ' αυτό σταματάει μέχρις εκεί και εκείνο που έχει υποστεί βλάβη πραγματικά είναι το ..... γόητρο του συστήματος ασφαλείας της συγκεκριμένης επιχείρησης. Αν όμως το κίνητρό τους είναι το κέρδος το οποίο μπορούν να επιτύχουν βλάπτοντας με οποιοδήποτε τρόπο το σύστημα ή τα αρχεία δεδομένων της συνεταιριστικής επιχείρησης – θύματός τους ή πουλώντας σε τρίτους τις πληροφορίες που απεκόμισαν από αυτά, τότε οι ζημιές της συνεταιριστικής επιχείρησης μπορεί να είναι ανυπολόγιστες.

Δυστυχώς ένας αρκετά μεγάλος αριθμός από τους σημερινούς hackers έχει οικονομικά κίνητρα πράγμα που αυτόματα αυξάνει τον επικίνδυνο χαρακτήρα τους.

Η ολοένα και μεγαλύτερη εκμετάλλευση του Internet για εμπορικούς σκοπούς με την αλματώδη τα τελευταία χρόνια ανάπτυξη του ηλεκτρικού εμπορίου έχει καταστήσει τις επιχειρήσεις περισσότερο προσιτούς και συνάμα οικονομικά ελκυστικούς στόχους.

Η λήψη μέτρων αντιμετώπισης του hacking από οποιονδήποτε κι αν προέρχεται – εφόσον είναι αδύνατη η από πριν γνώση των κινήτρων του – καθίσταται επιτακτική ανάγκη για την συνεταιριστική επιχείρηση που ενδιαφέρεται να μην υποστεί μεγαλύτερες ζημιές από τα οφέλη που αποκομίζει από τη σύνδεσή της με το διεθνές δίκτυο δηλ. το Internet.

Οι αδυναμίες του δικτύου καθιστούν προβληματική την ασφάλειά του και ο προσδιορισμός των τρόπων επίθεσης των hackers εναντίον του είναι τα θέματα που θα μας απασχολήσουν στη συνέχεια.

ΚΕΦΑΛΑΙΟ 4

ΑΔΥΝΑΜΙΕΣ ΤΟΥ INTERNET ΚΑΙ ΜΕΣΑ ΕΠΙΘΕΣΗΣ ΤΩΝ HACKERS

Δεδομένου ότι το Internet σαν σύστημα είναι ιδιαίτερα περίπλοκο είναι αδύνατο να μην παρουσιάζει αρκετά προβλήματα που συχνά κάνουν κάθε άλλο παρά ομαλή την λειτουργία του. Αυτό έχει σαν βασική συνέπεια ότι οποιαδήποτε αρχεία ή προγράμματα διακινούνται μέσω αυτού να διατρέχουν τον κίνδυνο να φτάσουν σε αποδέκτη ο οποίος δεν έχει δικαίωμα να τα χρησιμοποιήσει.

Ένας από τους κυριότερους λόγους για τους οποίους παρουσιάζονται πολλά προβλήματα ασφάλειας στο Internet είναι η βασική αρχιτεκτονική των πρωτοκόλλων TCP/IP και UDP που χρησιμοποιούνται σ' αυτό. Κανένα από αυτά δεν σχεδιάστηκε αρχικά με σκοπό να παράσχει αληθινά ασφαλή επικοινωνιακά μονοπάτια. Έτσι όταν στέλνει κανείς στοιχεία χρησιμοποιώντας το πρωτόκολλο TCP/IP, δεν μπορεί να γνωρίζει ποιους ακριβώς επικοινωνιακούς διαύλους θα ακολουθήσουν αυτά για να φτάσουν στον προορισμό τους. Αν κάποιος hacker καταφέρει να εγκαταστήσει σε κάποιον από τους διαύλους αυτούς ένα πρόγραμμα γνωστό σαν "sniffer" τότε θα μπορέσει να υποκλέψει όλα τα διαβιβαζόμενα με τον τρόπο αυτό στοιχεία.

Ένας ακόμη λόγος για τον οποίο οι hackers έχουν σοβαρές πιθανότητες να επιτυγχάνουν τον στόχο τους είναι η ίδια η διαμόρφωση του συστήματος η οποία δεν προϋποθέτει προληπτικά μέτρα ασφαλείας έτσι ώστε να ελέγχεται η είσοδος κάποιου στο Internet.

Σε γενικές γραμμές θα μπορούσαμε να εντοπίσουμε τις αδυναμίες των διαφόρων συστημάτων στα εξής :

α. Στην ανυπαρξία μέτρων ασφαλείας

β. Στην ατελή διαμόρφωση και διαχείρισή τους

γ. Σε βασικά προβλήματα ασφάλειας σε σχέση με τα πρωτόκολλα επικοινωνίας που χρησιμοποιούν

δ. Σε προβλήματα ασφαλείας σε σχέση με τις υπηρεσίες του Internet που χρησιμοποιούν και

ε. Στο μη ικανοποιητικό service που τους παρέχεται.

Εκτός από τα παραπάνω προβλήματα ασφάλειας πρέπει να αναφέρουμε και τις αδυναμίες των συνεταιριστικών επιχειρήσεων να αντιμετωπίσουν αποτελεσματικά μια εισβολή στα συστήματά τους είναι δυνατό να εντοπισθούν και στην ίδια την οργάνωσή τους. Δεν είναι λίγες οι περιπτώσεις όπου λείπει το εξειδικευμένο προσωπικό ασφαλείας και η διαχείριση των συστημάτων τους έχει ανατεθεί σε μη ειδικούς γι' αυτά τα θέματα.

Επίσης δεν υπάρχει συγκεκριμένη στρατηγική για την αντιμετώπιση των επιθέσεων των hackers έτσι ώστε να πιστοποιείται η πετυχημένη διείσδυσή τους στο σύστημα.

Σημείωση : Sniffer είναι ένα μικρό πρόγραμμα το οποίο χωρίς να γίνεται αντιληπτό εισχωρεί σ' ένα σύστημα όπου ψάχνει και αναλύει τα αρχεία του με σκοπό τη συλλογή συγκεκριμένων πληροφοριών τις οποίες διαβιβάζει στην συνέχεια στον χρήστη της.

ΚΕΦΑΛΑΙΟ 5

Ο ΤΡΟΠΟΣ ΔΡΑΣΗΣ ΤΩΝ HACKERS

Η πρόσβαση ενός hacker στο σύστημα του υποψήφιου θύματός του προϋποθέτει δύο στάδια : ένα προπαρασκευαστικό και ένα κύριο. Στο πρώτο ο hacker κάνει όλες εκείνες τις ενέργειες οι οποίες του είναι απαραίτητες για να αποκτήσει πρόσβαση στο σύστημα που τον ενδιαφέρει ενώ στο δεύτερο συλλέγει τις πληροφορίες που αναζητούσε και αποχωρεί από αυτό προσπαθώντας να μην αφήσει ίχνη της εισβολής του, διατηρώντας παράλληλα το «δικαίωμα» της επαναεισόδου του.

Έτσι στο **προπαρασκευαστικό στάδιο** ο hacker :

α. Συγκεντρώνει πληροφορίες για το σύστημα που επιθυμεί να προσβάλλει και

β. Προσπαθεί να αποκτήσει πρόσβαση σ' αυτό «σπάζοντας» τους κωδικούς εισόδου αποκτώντας έτσι τα δικαιώματα ενός νόμιμου χρήστη του συστήματος.

Στο **κύριο στάδιο** ο hacker επιδιώκει την εκπλήρωση των σκοπών για τους οποίους μπήκε παράνομα στο συγκεκριμένο σύστημα και αποχωρεί από αυτό προσπαθώντας να μην αφήσει ίχνη που θα μπορούν να οδηγήσουν στην ανακάλυψη της ταυτότητάς του, ενώ παράλληλα φροντίζει να διατηρήσει το δικαίωμα επανεισόδου του στο σύστημα, οπότε πάλι ο ίδιος το επιθυμήσει

Για καθένα από τα βήματα αυτά του hacker θα μπορούσαμε να πούμε τα ακόλουθα :

Α. Συλλογή πληροφοριών για το σύστημα

Το βήμα αυτό αποτελεί ίσως το βασικότερο σκαλοπάτι στην κλίμακα ενός πετυχημένου hacking. Η ρήση του Francis Bacon ότι «η πληροφορία αποτελεί δύναμη», βρίσκει την πλήρη εφαρμογή της στους hackers. Όσα περισσότερα γνωρίζει ένας hacker για ένα σύστημα τόσο περισσότερο αυξάνονται οι πιθανότητες που έχει για να διεισδύσει σ' αυτό χωρίς μάλιστα να γίνει αντιληπτός.

Οι πιθανές ερωτήσεις για τις οποίες οι απαντήσεις που θα πάρει να αποδειχθούν σημαντικές έχουν να κάνουν συνήθως τόσο με το ανθρώπινο δυναμικό (διαχειριστές, μηχανικούς, χειριστές, χρήστες) του συστήματος όσο και με το ίδιο το σύστημα (hardware, λειτουργικό που χρησιμοποιεί, ενδεχόμενες ιδιομορφίες του κλπ). Τις πληροφορίες αυτές ο hacker μπορεί να τις πάρει από :

- Το ίδιο το σύστημα
- Την επιχείρηση στην οποία αυτό ανήκει
- Ειδικούς (τεχνικούς, επιστήμονες) των Η/Υ και
- Άλλους συναδέλφους του.

Σχετικά με το **ίδιο το σύστημα** οι πληροφορίες διακρίνονται σ' εκείνες που μπορεί να πάρει ο hacker προτού εισβάλλει σ' αυτό και σ' εκείνες που μπορεί να πάρει μετά την εισβολή του. Οι πρώτες πιθανόν να μην είναι ιδιαίτερα σημαντικές γι' αυτόν δεδομένου ότι είτε απευθύνονται γενικότερα στο κοινό είτε περιέχουν ένα μήνυμα με το οποίο δηλώνεται ότι για να προχωρήσει κανείς παρακάτω θα πρέπει να δώσει το password, δηλαδή η πρόσβαση αφορά μόνο εξουσιοδοτημένους χρήστες. Εάν ο hacker βρει το password και καταφέρει να διεισδύσει στο σύστημα οι πληροφορίες που μπορεί να πάρει πλέον γι' αυτό είναι

δυνατό να αποκαλύπτουν το hardware του, τον τρόπο διαχείρισής του, τα δικαιώματα των νόμιμων χρηστών του κλπ.

Στη δεύτερη αυτή περίπτωση ο hacker θα έχει στη διάθεσή του μια σειρά εντολών για να εξερευνήσει το συγκεκριμένο σύστημα. Θα προσπαθήσει φυσικά η εξερεύνηση αυτή να μην τραβήξει την προσοχή των υπευθύνων για την ασφάλειά του. Βασικά όμως εκείνο το οποίο θα κάνει θα είναι να ελέγξει τα μέτρα ασφαλείας του συστήματος, κάτι που θα του καθορίσει αποφασιστικά και την παραπέρα δράση του.

Έχει επανειλημμένα αποδειχθεί ότι είναι πιο εύκολο να αποκτήσει κανείς μια πληροφορία που χρειάζεται εκμεταλλευόμενος τις γνωριμίες που έχει παρά προσπαθώντας να την κλέψει. Γιατί λοιπόν ένας hacker να προσπαθήσει να κλέψει μια πληροφορία που τον ενδιαφέρει για το σύστημα-στόχο του και να μην την πάρει δημιουργώντας απλά το κατάλληλο φιλικό περιβάλλον με εκείνον που πιθανότατα την κατέχει ; Έτσι λοιπόν ο hacker μπορεί να πλησιάσει κάποιον από τους **υπαλλήλους της επιχείρησης-στόχου** που του αρέσει ίσως να μιλάει πολύ τόσο για τα προσωπικά του όσο και για τα επαγγελματικά του θέματα. Αν μάλιστα ήταν πρώην υπάλληλος που κατά την γνώμη του απολύθηκε άδικα τότε σίγουρα θα διακατέχεται από μια διάθεση εκδίκησης ως προς τους εργοδότες διευκολύνοντας έτσι τη "συνεργασία" του με τον hacker. Ο εντοπισμός του προσώπου αυτού από τον hacker και **η στα πλαίσια μιας κοινωνικής επαφής απόκτηση της εμπιστοσύνης του** - γνωστά στη γλώσσα των hackers σαν **Social engineering** (κοινωνική χειραγώγηση) - μπορεί να αποτελέσει γι' αυτόν μια σημαντικότατη πηγή πληροφόρησης. Το πρόβλημα που υπάρχει στη συγκεκριμένη περίπτωση είναι ότι αρκετοί hackers κάθε άλλο παρά σαν κοινωνικά άτομα θα μπορούσαν να χαρακτηρισθούν, πράγμα που όπως είναι φυσικό εμποδίζει αρκετά στις κοινωνικές τους επαφές. Θα πρέπει πάντως να σημειώσουμε πως οι περισσότερες περιπτώσεις χρήσης της

μεθόδου **Social engineering** παίρνουν απαρατήρητες δεδομένου ότι οι ερωτήσεις πού απευθύνει ο hacker είναι συνήθως αποσπασματικές δεν αφορούν δηλ. όλα τα στοιχεία της λειτουργίας ενός συστήματος ενώ στη συνέχεια ο ερωτών φροντίζει να εξαφανισθεί. Με τον τρόπο αυτό φυσικά, σπάνια δημιουργεί υποψίες για το άτομό του και τον σκοπό τον οποίο επιδιώκει.

Social engineering μπορεί επίσης να θεωρηθεί ότι γίνεται και μέσω software με την χρήση «Δούρειων ίππων». Έτσι μέσω παιχνιδιών που ζητούν από τον νόμιμο χρήστη τους password ο hacker που παίζει με τον υπάλληλο της συνεταιριστικής επιχείρησης μπορεί να πάρει μια ιδέα και για τα passwords που ενδεχόμενα χρησιμοποιούνται στην εργασία αυτού του τελευταίου.

Δεν είναι και οι περιπτώσεις που ο hacker προσπαθώντας να μάθει τα μυστικά του συστήματος από το προσωπικό της συνεταιριστικής επιχείρησης που τον ενδιαφέρει επιδιώκει με κάποια πρόφαση - π.χ. ότι έρχεται να κάνει συντήρηση από την εταιρία που έχει εγκαταστήσει το δίκτυο ή ότι είναι υπάλληλος της ηλεκτρικής ή της τηλεφωνικής εταιρείας και ήλθε για να επιδιορθώσει μια βλάβη κλπ - να περιηγηθεί στους χώρους της, να συζητήσει για τη λειτουργία των διαφόρων μηχανημάτων και ίσως να πάρει για ... επιδιόρθωση στο εργαστήριό του κάποιους Η/Υ, όπου βέβαια θα τους «δει» με όλη του την άνεση. Σχετικές οδηγίες για το πώς μπορεί να προσληφθεί κανείς σε μια συνεταιριστική επιχείρηση που κάνει συντήρηση Η/Υ έχουν δοθεί επανειλημμένα από hackers.

Τέλος σημαντικές πληροφορίες από την **ίδια την συνεταιριστική επιχείρηση στόχο** μπορεί να πάρει ο hacker - όσο κι αν φαίνεται απίθανο - ψάχνοντας στα ... σκουπίδια της. Είναι συνηθισμένο φαινόμενο πολλές πληροφορίες να πετιούνται στα σκουπίδια, με τη μορφή άχρηστων σημειωμάτων που περιέχουν μισοσβησμένους κωδικούς ή αντίγραφα

αναφορών για διάφορα εμπιστευτικά ζητήματα που έχουν τυπωθεί σε εκτυπωτή ή αποδείξεων πληρωμής λογαριασμών πιστωτικών καρτών ή αποκομμάτων εφημερίδων και περιοδικών ή εγχειριδίων Η/Υ που δεν περιέχουν μόνο οδηγίες για τη χρήση τους αλλά και σημειώσεις που γράφτηκαν στο περιθώριο από τους χρήστες τους κλπ. Οι πληροφορίες που περιλαμβάνονται σ' όλα αυτά είναι πολύ πιθανό να αναφέρονται σε χαρακτηριστικά του συστήματος σε passwords καθώς και σε κάθε είδους ζητήματα λειτουργίας των διαφόρων μηχανημάτων. Η αξία τους για τον hacker μπορεί φυσικά να θεωρηθεί ανυπολόγιστη όπως μπορεί να είναι και οι ζημιές που ίσως προκληθούν στην επιχείρηση από την αμέλεια των υπαλλήλων της να τηρήσουν τους κανόνες ασφαλείας που επιβάλλονται για την συγκεκριμένη περίπτωση.

Οι δημοσιεύσεις για θέματα ασφάλειας συστημάτων Η/Υ που γίνονται σε επιστημονικά περιοδικά, σε βιβλία, σε newsgroups και σε mailing lists από **επιστήμονες της πληροφορικής και από ειδικούς** του χώρου αυτού αποτελούν μία ακόμη σημαντική πηγή πληροφόρησης για τους hackers. Όσο χρήσιμη είναι η πληροφόρηση αυτή για τους υπεύθυνους ασφαλείας των διαφόρων συστημάτων άλλο τόσο είναι και για τους ίδιους τους hacker's. Γνωρίζοντας με τον τρόπο αυτό οι hacker's τα μέτρα που παίρνονται για την αντιμετώπισή τους, μπορούν εύκολα να πάρουν τα κατάλληλα αντι-μέτρα.

Οι hacker's περνούν αρκετό από το χρόνο τους ψάχνοντας να βρουν Sites στο Web ή ανεξάρτητες BBS με πληροφορίες που τους αφορούν και τις οποίες έχουν με τον τρόπο αυτό θέσει στη διάθεσή τους άλλοι **συνάδελφοί τους**. Είναι γεγονός πως Sites με πληροφορίες και εργαλεία για hacking αφθονούν στο Web. Η ανεύρεσή τους μάλιστα δεν είναι διόλου δύσκολη παρότι, δεν μένουν σταθερά για πολύ χρόνο στην ίδια διεύθυνση. Ακόμα πολλοί hacker's συνεργάζονται μεταξύ τους ανταλλάσσοντας πληροφορίες με ηλεκτρονικό ταχυδρομείο (e-mail) ή

συνομιλώντας σε ειδικά chat rooms. Βεβαίως και υπάρχει επίσημο (!) έντυπο των hacker's, το «**2600 : The hacker's Quarterly**», που κυκλοφορεί από το 1984 – μηνιαία κυκλοφορία 20.000 εντύπων το 1995 – (σήμερα και σε ηλεκτρονική μορφή **(http://www.2600.com.)** καθώς και άλλα παρόμοια περιοδικά σε ηλεκτρονική κυρίως μορφή. Τέλος, οποιοσδήποτε χρήστης PC μπορεί να βρει εύκολα συναλλαγές προγραμμάτων για hacking σε CD-ROM που κυκλοφορούν ελεύθερα στο εμπόριο – και στη χώρα μας – σε προσιτή τιμή.

Β. Εισβολή στο σύστημα : «Σπάσιμο των κωδικών εισόδου και απόκτηση των δικαιωμάτων ενός νόμιμου χρήστη».

Σχεδόν όλοι οι hackers γνωρίζουν ότι ένα από τα βασικά μυστικά της επιτυχίας τους είναι η αδυναμία των διαφόρων συστημάτων να εμποδίσουν την εισβολή τους σ' αυτά. Ένα σύστημα λειτουργεί σωστά από τη στιγμή που ο μηχανισμός αναγνώρισης της ταυτότητας (πιστοποίηση) των νόμιμων χρηστών του είναι αξιόπιστος. Για το λόγο αυτό η εξουδετέρωση του μηχανισμού αυτού αποτελεί το κύριο μέλημα κάθε hacker που σέβεται τον εαυτό του !

Η μέθοδος που χρησιμοποιείται περισσότερο για την **πιστοποίηση** ενός χρήστη είναι αυτή που στηρίζεται στο **όνομά του (user's ID)** σε συνδυασμό μ' ένα **συνθηματικό (password)**, τα οποία θα πρέπει να δώσει ο χρήστης προκειμένου να του επιτραπεί η είσοδός του στο σύστημα. Εννοείται ότι και τα δύο θα πρέπει να είναι «γνωστά» σ' αυτό για να καταστεί δυνατή η σχετική αναγνώριση. Τα στοιχεία αυτά βρίσκονται συνήθως αποθηκευμένα στο αρχείο «**passwd**» που υπάρχει στο σύστημα, εφόσον αυτό χρησιμοποιεί Unix, κάτι που ισχύει για τους Servers των περισσότερων συστημάτων που είναι στο Internet. Επιδίωξη

του hacker είναι να μάθει τα στοιχεία αυτά. Πως μπορεί να το πετύχει αυτό ;

Σύμφωνα με τον O. Kyas υπάρχουν πέντε τρόποι για να μάθει ένας hacker το password (και το ID) που θέλει :

1. **Να το μαντέψει**
2. **Να διερευνήσει συστηματικά το αρχείο «passwd» με ειδικά για την αποκάλυψη passwords προγραμμάτων που υπάρχουν άφθονα στο Web**
3. **Αναλύοντας πρωτόκολλα επικοινωνίας με ειδικά προγράμματα διερεύνησης δικτύων**
4. **Απομονώνοντας τα passwords με τη χρήση προγραμμάτων που μένουν στη μνήμη**
5. **Με «Social hacking (engineering)».**

Παρενθετικά θα πρέπει να παρατηρήσουμε πως η επιλογή των passwords είναι ένα θέμα πολύ μεγάλης σημασίας για την ασφάλεια ενός συστήματος. **Ασφαλές passwords είναι εκείνο που δεν μπορεί να ανακαλύψει ένας hacker οποιαδήποτε μέθοδο κι αν χρησιμοποιήσει και το οποίο δεν μπορεί να απομνημονευθεί εύκολα.** Οι οδηγίες που θα πρέπει να δίνονται στους χρήστες όταν επιλέγουν το Id και το password που θα χρησιμοποιούν για την είσοδό τους στο σύστημα θα πρέπει να τους συνιστούν να αποφεύγουν :

- Το μικρό τους όνομα ή το επώνυμο ή ακόμα οποιονδήποτε συνδυασμό αυτών των δύο, το παρωνύμιο τους, τα ονόματα των παιδιών τους, των συζύγων τους, των συντρόφων τους, των στενών τους φίλων, των συγγενών τους, ονόματα από μυθιστορήματα, από σειρές της τηλεόρασης ή από γνωστά κινηματογραφικά έργα, ονόματα τοποθεσιών, χωρών, πόλεων, μάρκες αυτοκινήτων κ.λ.π.

- Αριθμούς τηλεφώνων, ημερομηνίες γέννησης, αριθμούς αυτοκινήτων και άδεια οδήγησης, σειρά αριθμών π.χ. 4, 5, 6, 7, 8 κ.λ.π.
- Λέξεις που βρίσκονται σε λεξικό οποιασδήποτε γλώσσας ή που δεν τις συναντά κανείς στα συνηθισμένα λεξικά.
- Συνηθισμένες φράσεις ή αρχή κάποιας παροιμίας.
- Σειρά γραμμάτων του πληκτρολογίου π.χ. ζ, χ, ψ, ω κ.λ.π.
- Ένα μόνο γράμμα ή αριθμό.
- Λέξεις ή συνθήματα που εκφράζουν τις πολιτικές, αθλητικές κ.λ.π. προτιμήσεις τους ή τα hobbies τους και
- Passwords που είχαν χρησιμοποιήσει στο παρελθόν.

Οι δυσκολίες που θα συναντήσει ένας hacker, ενδεχόμενα θα είναι αρκετές εάν ο χρήστης :

- Αλλάζει το password του κάθε 3 ή 6 μήνες το πολύ,
- Χρησιμοποιεί password αποτελούμενο από μικρά και από κεφαλαία γράμματα ή από διαφορετικά αλφάβητα ή από αριθμούς και ειδικούς χαρακτήρες π.χ. 3,8@$-9,^!#6*.
- Χρησιμοποιεί σαν password μια φράση χωρίς διαστήματα π.χ. «φίλοιμουκαληνύχτα».
- Δεν χρησιμοποιεί passwords με λιγότερους από 8 χαρακτήρες.

Ακόμα όμως και τα πιο δύσκολα passwords και τα προστατευόμενα με τον ασφαλέστερο τρόπο αρχεία «password» ενός συστήματος δεν είναι δυνατό να μην αποκαλυφθούν στον hacker που έχει καταφέρει να εγκαταστήσει σ' αυτό ένα πρόγραμμα sniffer, με το οποίο θα έχει τη

δυνατότητα να καταγράφει όλα τα πατήματα του πληκτρολογίου του χρήστη.

Ο hacker χρησιμοποιώντας ακόμα ειδικά προγράμματα που περιέχουν καταλόγους με λέξεις (word lists) - που μπορεί να βρει εύκολα στο Internet - αυξάνει σημαντικά τις πιθανότητες να ανακαλύψει το password και το Id που θα το επιτρέψουν να κινηθεί μέσα σ' ένα σύστημα αποκτώντας τελικά όλα τα δικαιώματα ενός νόμιμου χρήστη του.

Γ. Ο hacker μέσα στο σύστημα

Από τη στιγμή που ο hacker θα αποκτήσει πρόσβαση στο σύστημα της συνεταιριστικής επιχείρησης - στόχου του το τι θα κάνει στη συνέχεια εξαρτάται από το σκοπό για τον οποίο έκανε το hacking. Ανεξάρτητα από το ποιο είναι πάντως το βασικό του κίνητρο είναι βέβαιο πως μεταξύ άλλων θα συγκεντρώσει πληροφορίες **και** για τη λειτουργία του συστήματος αυτού καθώς και ότι θα προσπαθήσει να εκμεταλλευτεί τις δυνατότητές του και γενικότερα τα δικαιώματα που παρέχονται στους νόμιμους χρήστες του. Ολοκληρώνοντας ο hacker την «επίσκεψή» του θα προσπαθήσει να εξαφανίσει τα ίχνη της και παράλληλα να αφήσει «ανοικτή την πόρτα» και για μελλοντικές ανάλογες δραστηριότητες στο ίδιο σύστημα.

Ο hacker λοιπόν, ευρισκόμενος μέσα στο σύστημα της συνεταιριστικής επιχείρησης - στόχου του θα έχει την ευχέρεια :

- να συγκεντρώσει τις πληροφορίες που τον ενδιαφέρουν,
- να διαστρεβλώσει πληροφορίες που ήδη υπάρχουν εκεί,
- να το χρησιμοποιήσει γενικά όπως ο ίδιος επιθυμεί,
- να εγκαταστήσει σ' αυτό πρόγραμμα που θα το βλάψουν,

- να εξαφανίσει τα ίχνη της «επίσκεψής» του και
- να δημιουργήσει **backdoors** χρήσιμες για ανάλογες μελλοντικές δραστηριότητές του.

Εφόσον ο hacker «επισκέπτεται» ένα σύστημα για να **πάρει συγκεκριμένες πληροφορίες**, μόλις τις βρει τις παίρνει και φεύγει. Υπάρχει βέβαια και η πιθανότητα ανάλογες πληροφορίες να εισάγονται περιοδικά στο σύστημα, οπότε στην περίπτωση αυτή το επισκέπτεται σε τακτά χρονικά διαστήματα, προσπαθώντας να μην αφήνει κάθε φορά ίχνη των επισκέψεών του ατών ή έχει εγκαταστήσει σ' αυτό ειδικά προγράμματα τα οποία του επιτρέπουν να παρακολουθεί την κίνηση των δεδομένων. Εφόσον τα αρχεία που τον ενδιαφέρουν δεν έχουν μεγάλη έκταση και εμφανίζονται με την μορφή απλού κειμένου (text), η μεταφορά τους στον Η/Υ του, γίνεται καθώς εμφανίζονται στην οθόνη του υπολογιστή του θύματός του και μάλιστα σε ελάχιστο χρόνο. Αν όμως η έκτασή τους είναι μεγάλη τότε η μεταφορά τους θα πρέπει να γίνει είτε μ' ένα πρόγραμμα μεταφοράς αρχείων ή ο hacker θα τα στείλει με e - mail στον εαυτό του. Εάν όμως είναι υπάλληλος της συνεταιριστικής επιχείρησης - θύματος, πράγμα που σημαίνει ότι μπορεί να χειρίζεται και ο ίδιος κάποιον υπολογιστή της, τότε δεν έχει παρά να αντιγράψει τα σχετικά αρχεία σε δισκέτες ή σε οποιοδήποτε άλλο μέσο μεταφοράς αρχείων.

Υπάρχει ενδεχόμενο ένας hacker να θέλει να **διαστρεβλώσει** το περιεχόμενο πληροφοριών ενός συστήματος με σκοπό να ζημιώσει τις συναλλαγές της συνεταιριστικής επιχείρησης στην οποία αυτό ανήκει. Η επέμβασή του στα σχετικά αρχεία μετά την αναγνώρισή τους μπορεί να είναι καταλυτική και οι ζημιές που θα επέλθουν από την χρήση εσφαλμένων στοιχείων που θα έχει εισαγάγει σ' αυτά θα είναι σημαντική για το ανύποπτο θύμα του.

Η χρησιμοποίηση των δυνατοτήτων ενός συστήματος από τον ίδιο τον hacker έχει συνήθως να κάνει με την επιθυμία του αφενός μεν να το ελέγξει - έστω και για λίγο - αφετέρου δε να εμποδίσει τη χρήση του από τους νόμιμους χρήστες του. Και στις δύο περιπτώσεις οι ζημιές του θύματος είναι δεδομένο πως μπορεί να είναι πολύ μεγάλες.

Ανεξάρτητα για ποιο λόγο ένας hacker εισβάλλει σ' ένα σύστημα, προκειμένου να επιτύχει τους στόχους του θα χρειασθεί να χρησιμοποιήσει σε πολλές περιπτώσεις, κάποια **προγράμματα** τα οποία εγκαθιστώμενα σ' αυτό θα του προσφέρουν σημαντική βοήθεια. Τέτοια προγράμματα μπορεί να είναι τα εξής :

- **Spoofs** : τα οποία είναι προγράμματα που υποδύονται ότι είναι άλλα, κρύβοντας έτσι την πραγματική τους ταυτότητα. Σκοπός τους είναι η συλλογή πληροφοριών. Γενικότερα δε **spoofing** είναι η απόπειρα που κάνει κάποιος να διεισδύσει σ' ένα σύστημα προσποιούμενος πως είναι μόνιμος χρήστης του.
- **Logic bombs** : που είναι προγράμματα που παραμένουν ανενεργά στη μνήμη ενός Η/Υ και ενεργοποιούνται είτε σε προκαθορισμένη χρονική στιγμή (time bombs) είτε μετά από κάποιο συγκεκριμένο χειρισμό. Σκοπός τους είναι η καταστροφή αρχείων εξαιτίας της οποίας προκαλείται η σταδιακή κατάρρευση ενός συστήματος.
- **Trojan horses** : τα οποία είναι τα προγράμματα που ενώ φαίνεται ότι λειτουργούν κανονικά, παράλληλα εκτελούν και κάποιες μη επιτρεπόμενες ενέργειες. Οι hackers χρησιμοποιούν συνήθως τα προγράμματα αυτά για να κάνουν έμμεσα ενέργειες που δεν μπορούν να κάνουν άμεσα, παραπλανώντας έτσι για τις πραγματικές τους προθέσεις, τα θύματά τους.
- **Worms** : τα οποία είναι προγράμματα που χρησιμοποιούνται σαν ένας μηχανισμός μεταφοράς άλλων προγραμμάτων. Για το λόγο αυτό χρησιμοποιούν τις δυνατότητες κυκλοφορίας που τους παρέχει ένα

δίκτυο με σκοπό να μεταφέρουν κάποιο καταστρεπτικό πρόγραμμα στα διάφορα συστήματα του δικτύου αυτού.

- **Snoopers** : τα οποία είναι προγράμματα που παρακολουθούν δεδομένα (data) που διακινούνται μέσα σ' ένα σύστημα, ψάχνοντας να βρουν ένα συγκεκριμένο είδος πληροφοριών. Ένα τέτοιο πρόγραμμα μπορεί να εγκατασταθεί στον κεντρικό Server ενός δικτύου ή στον σκληρό δίσκο ενός Η/Υ και να παρακολουθεί με τον τρόπο αυτό τα δεδομένα που διακινούνται σ' αυτά και τέλος
- **Viruses** : οι γνωστοί ιοί των Η/Υ για τους οποίους έχει γίνει πολύς λόγος από τότε που εμφανίστηκαν. Δεδομένης της σπουδαιότητάς τους θα ασχοληθούμε ειδικά μαζί τους στο επόμενο τμήμα της εργασίας μας αυτής.

Ευρισκόμενος ο hacker μέσα στο σύστημα της συνεταιριστικής επιχείρησης - στόχου του επιθυμεί να αφήσει όσο το δυνατό λιγότερα **ίχνη** από την εκεί παρουσία του. Βασικό του μέλημα λοιπόν είναι να σβήσει όσα περισσότερα από αυτά μπορεί αλλά και όσα απομένουν να τα περιπλέξει με τέτοιο τρόπο έτσι ώστε να μην μπορούν να οδηγήσουν σ' αυτόν. Γνωρίζοντας ότι η αποκάλυψη της ταυτότητάς του θα καταστρέψει το «έργο» του οι προσπάθειές του για την εξάλειψη των ιχνών της προστασίας του ξεκινούν από τη στιγμή της εισόδου του στο σύστημα και ολοκληρώνονται με την έξοδό του από αυτό.

Τέλος από την στιγμή που ένας hacker αποκτά τη δυνατότητα πρόσβασης σ' ένα σύστημα επιθυμία του είναι να εξακολουθήσει να έχει πρόσβαση στο σύστημα αυτό ακόμα κι αν αποκαλυφθεί η παράνομη είσοδός του. Για να το πετύχει αυτό θα πρέπει να δημιουργήσει τις λεγόμενες «**backdoors**» δηλ. εναλλακτικούς τρόπους παράνομης επαναδιείσδυσής του στο σύστημα. Για το λόγο αυτό πολλοί hackers έχουν στη διάθεσή τους τα κατάλληλα προγράμματα με τα οποία θα μπορέσουν να εκμεταλλευτούν τα προβλήματα ασφαλείας του

συστήματος και γενικότερα τις ατέλειές του έτσι ώστε με τον τρόπο αυτό να μπορέσουν να ανοίξουν και άλλες διόδους πρόσβασης σ' αυτό.

Ολοκληρώνοντας στο σημείο αυτό την περιγραφή του τρόπου δράσης των hackers δεν τρέφουμε την ψευδαίσθηση ότι έχουμε καλύψει τα πάντα γι' αυτό. Η μεθοδολογία του hacking ανανεώνεται καθημερινά και στους «κατοίκους» του κυβερνοχώρου η φαντασία περισσεύει γιατί είναι απαραίτητο στοιχείο για την επιβίωσή τους μέσα στα όριά του !

Στη συνέχεια και προτού ασχοληθούμε με τους τρόπους αντιμετώπισης του hacking και των hackers κρίνουμε απαραίτητη την αυτοτελή αναφορά μας σ' ένα από τα περισσότερο συζητημένα όπλα τους : τους **ιούς (viruses)** των υπολογιστών.

συστήματος και γενικότερα τις ατέλειές του έτσι ώστε με τον τρόπο αυτό να μπορέσουν να ανοίξουν και άλλες διόδους πρόσβασης σ' αυτό.

Ολοκληρώνοντας στο σημείο αυτό την περιγραφή του τρόπου δράσης των hackers δεν τρέφουμε την ψευδαίσθηση ότι έχουμε καλύψει τα πάντα γι' αυτό. Η μεθοδολογία του hacking ανανεώνεται καθημερινά και στους «κατοίκους» του κυβερνοχώρου η φαντασία περισσεύει γιατί είναι απαραίτητο στοιχείο για την επιβίωσή τους μέσα στα όριά του !

Στη συνέχεια και προτού ασχοληθούμε με τους τρόπους αντιμετώπισης του hacking και των hackers κρίνουμε απαραίτητη την αυτοτελή αναφορά μας σ' ένα από τα περισσότερο συζητημένα όπλα τους : τους **ιούς (viruses)** των υπολογιστών.

ΚΕΦΑΛΑΙΟ 6

ΟΙ ΙΟΙ ΤΩΝ Η/Υ

Οι ιοί των υπολογιστών δεν ξεκίνησαν στην αρχή σαν εργαλεία (tools) των hackers αλλά σαν πνευματικά παιχνίδια των ερευνητών σε επιστημονικά εργαστήρια αμερικάνικων πανεπιστημίων όπως του M.I.T. ή εταιρειών προϊόντων υψηλής τεχνολογίας.

Οι ερευνητές και οι προγραμματιστές των ερευνητικών αυτών κέντρων, κατά τη διάρκεια του ελεύθερου χρόνου τους διασκέδαζαν τους εαυτούς τους και τους συναδέλφους τους μπαίνοντας στην κεντρική μνήμη των υπολογιστικών μηχανημάτων τους. Αλλάζοντας όμως τον κώδικα της μνήμης αυτής διαπίστωσαν ότι προγράμματα τα οποία είχαν σχεδιασθεί για να ταξινομήσουν αρχεία μπορούσαν επίσης και να τα καταστρέψουν ! Στην ανακάλυψη αυτή στηρίχθηκε και το παιχνίδι «**Core wars**» στο οποίο οι προγραμματιστές δοκίμαζαν την εξυπνάδα τους γράφοντας προγράμματα τα οποία μπορούσαν να αναπαράγουν τον εαυτό τους και στη συνέχεια να καταστρέψουν τα προγράμματα των αντιπάλων παικτών.

Οι ιοί που δημιουργήθηκαν μέσα στα πλαίσια των «core wars» δεν έγιναν ευρύτερα γνωστοί έξω από τους υπολογιστές των εργαστηρίων επειδή οι προγραμματιστές που τους χρησιμοποιούσαν κρατούσαν τις λεπτομέρειες της κατασκευής τους μόνο για τον εαυτό τους. Έτσι δεν αποτελούσαν απειλή για τον εξωτερικό κόσμο.

Όλα αυτά μέχρι το 1983. Τη χρονιά αυτή ο δημιουργός του λειτουργικού συστήματος UNIX, Ken Thompson μιλώντας στην «Association for Computing Machines» έκανε λόγο για τα «core wars».

Αυτό ήταν το πρώτο λάθος. Την επόμενη χρονιά έγινε το δεύτερο και πιο αποφασιστικό. Το περιοδικό **Scientific American** δημοσίευσε ένα άρθρο που αναφερόταν στους ιούς και στο οποίο περιλαμβανόταν λεπτομέρειες για το πώς θα μπορούσε κανείς να γράψει τέτοια προγράμματα που αντέγραφαν τον εαυτό τους. Η ραγδαία ανάπτυξη των ιών που επακολούθησε ήταν πια θέμα χρόνου. Τα πλαίσια των επιστημονικών εργαστηρίων ήταν πλέον πολύ στενά γι' αυτούς.

Στην αρχή βέβαια εμφανίστηκαν σαν ακίνδυνα προγράμματα που έδειχναν ένα μήνυμα στην οθόνη του Η/Υ ή έπαιζαν κάποιο ήχο σε συγκεκριμένη ώρα κάθε ημέρας. Ακίνδυνα μεν ενοχλητικά δε, θα μπορούσε να παρατηρήσει κανείς. Όπως ακριβώς όμως συνέβη και με τους hackers που ξεκίνησαν τη δράση τους για να διευρύνουν τις γνώσεις τους εξελίχθηκαν στο να κάνουν παράνομες πράξεις, έτσι και οι δημιουργοί ιών από κάποιο σημείο και μετά κατάλαβαν τη δύναμη που είχαν στα χέρια τους και άρχισαν να δημιουργούν ιούς που προξενούσαν καταστροφές όχι μόνο σε αρχεία αλλά και σε ολόκληρα δίκτυα υπολογιστών. Δεν ήταν δε λίγες οι περιπτώσεις που ζήτησαν οικονομικά ανταλλάγματα για να μην τους χρησιμοποιήσουν.

Οι καταστροφικές τους δυνατότητες υπογραμμίστηκαν μεταξύ άλλων και από τον Δρ. Peter S. Tippet, διευθυντή παραγωγής προϊόντων ασφαλείας της Symantec Corporation, ο οποίος καταθέτοντας σε μια υποεπιτροπή του Αμερικάνικου Κογκρέσου το 1993, υπογράμμισε πως :

> «... μια εταιρεία που έχει 1000 υπολογιστές προσβάλλεται από έναν ιό κάθε τέταρτο της ώρας, το κόστος για την αντιμετώπιση των ιών αυτών ανέρχεται σε 170.000 $ το χρόνο τώρα και σε 500.000 $ για τον επόμενο χρόνο και ότι εάν προσθέσουμε τα κόστη αυτά από το 1990 και μετά θα δούμε πως η μάχη κατά των ιών των υπολογιστών έχει κοστίσει στους Αμερικάνους πολίτες περισσότερο από 1 δισεκατομμύριο δολάρια».

Τι είναι όμως ο ιός των υπολογιστών ; **Ο ιός είναι ένα πρόγραμμα που έχει σχεδιασθεί με σκοπό να μολύνει άλλα προγράμματα με αντίγραφά του.** Επειδή δε έχει τη δυνατότητα να αναπαράγεται συνεχώς μπορεί να μεταδοθεί από το ένα σύστημα σ' ένα άλλο, με σκοπό να εκτελέσει την αποστολή του η οποία περιλαμβάνει την δυσλειτουργία ή και την καταστροφή ολόκληρων συστημάτων, τη διαγραφή αρχείων ή το σβήσιμο του συνόλου του περιεχομένου σκληρών δίσκων.

Οι περισσότεροι ιοί έχουν σαν στόχο τους προγράμματα των υπολογιστών. Εξαιτίας δε των διαφόρων μορφών που μπορεί να πάρει ένας ιός από τις παρεμβάσεις που κάνει συνήθως στη δομή του ένας hacker, είναι αρκετά δύσκολη η ακριβής περιγραφή του και η κατάταξή του σε συγκεκριμένη κατηγορία. Ωστόσο ο **John McAfee** της «Computer Virus Industry Association», γνωστός για τα anti-virus προγράμματα που έχει κυκλοφορήσει στη διεθνή αγορά, υποστηρίζει την άποψη πως σαν **κριτήρια διάκρισης των ιών μπορούν να θεωρηθούν η δομή του προγράμματος που προσβάλλουν, το μέγεθος της καταστροφής που προξενούν και η περιοχή του συστήματος στο οποίο εγκαθίστανται.**

Ο **O. Kyas** εξάλλου, με κριτήρια το μέρος του υπολογιστή που προσβάλλουν για να μην γίνονται αντιληπτοί, διαχωρίζει τους ιούς σε εκείνους :

- **Που μολύνουν τον τομέα εκκίνησης ενός σκληρού δίσκου (ή των δισκετών) ο οποίος περιέχει εντολές εκκίνησης του υπολογιστή,**
- **Που μολύνουν το σύστημα και οι οποίοι προσκολλώνται σε διάφορα τμήματα του λειτουργικού ή στο πρόγραμμα ελέγχου εφαρμογών.**
- **Που μεταβάλλουν προγράμματα υπολογιστών και οι οποίοι βρίσκονται κρυμμένοι μέσα σε εκτελέσιμα αρχεία και τρέχουν μόλις ξεκινήσει το πρόγραμμα που έχουν μολύνει.**

- **Που έχουν τη δυνατότητα να αναπαράγονται με πολλούς και διαφορετικούς τρόπους έτσι ώστε να είναι ανθεκτικοί στα διάφορα anti - virus προγράμματα.**
- **Που έχουν τη δυνατότητα να καμουφλάρουν τις αλλαγές που κάνουν στον τομέα εκκίνησης ενός συστήματος ή ενός αρχείου επεμβαίνοντας στο λογισμικό του συστήματος που προσβάλλουν.**
- **Που προσπαθούν να καταστρέψουν ή αν σβήσουν εντελώς προγράμματα anti-virus και**
- **Που προσβάλλουν τις μακρο-εντολές σύγχρονων προγραμμάτων των εφαρμογών.**

Ο καλύτερος τρόπος αντιμετώπισης των ιών είναι η **πρόληψη**. Το πρώτο βήμα προς την κατεύθυνση όλων των τρόπων με τους οποίους μπορούν αυτοί να διεισδύσουν σ' ένα σύστημα. Το μπλοκάρισμα των τρόπων αυτών αποτελεί το επόμενο βήμα. **Έτσι συστήματα ευάλωτα στην προσβολή τους από ιούς - όπως είναι εκείνα που έχουν σύνδεση με το Internet ή εκείνα που έχουν πολλούς χρήστες - θα πρέπει να διασφαλίζονται με την χρήση του κατάλληλου διερευνητικού software ή με τη δημιουργία backups των αρχείων τους.** Η χρήση προγραμμάτων διαγνωστικών των ιών που θα ενεργοποιούνται με την έναρξη της λειτουργίας του συστήματος είναι απαραίτητη στην προκειμένη περίπτωση δεδομένου ότι έτσι μειώνονται και οι πιθανότητες ενεργοποίησης ιών που το έχουν ήδη μολύνει.

Από τη στιγμή που μέσω ενός τέτοιου προγράμματος - (κυκλοφορούν άφθονα στην αγορά) - διαπιστωθεί η ύπαρξη ιού ή ιών η λειτουργία του συστήματος σταματάει και με ειδικά πάλι anti-virus προγράμματα θα πρέπει να καταστραφούν οι ιοί που το έχουν ήδη μολύνει. Η διαγραφή όλων των μολυσμένων αρχείων και η αντικατάστασή τους με «καθαρά» αντίγραφά τους συνιστάται στη

συγκεκριμένη περίπτωση.

Οι ενέργειες αντιμετώπισης ενός ιού ολοκληρώνονται με τη διερεύνηση του τρόπου και του λόγου εισόδου του στο σύστημα. Η απάντηση στα σχετικά ερωτήματα θα βοηθήσει στη θεραπεία των αδυναμιών του συστήματος και στην μη επανάληψή τους στο μέλλον.

Σημειώνουμε τέλος πως υπάρχουν πολλοί οργανισμοί που ειδικεύονται στην παραγωγή προγραμμάτων διάγνωσης και καταστροφής ιών (π.χ. **IBM Anti-Virus research, EINET computer Virus and Security informations** κ.λ.π.) και πως τα σχετικά προγράμματα (**anti-virus software**) ανανεώνονται συνεχώς ακολουθώντας την ανάλογη ανανεωτική τάση των διάφορων ιών.

ΚΕΦΑΛΑΙΟ 7

ΑΝΤΙΜΕΤΩΠΙΖΟΝΤΑΣ ΤΗΝ ΕΙΣΒΟΛΗ ΤΩΝ HACKERS

Όσα μέχρι τώρα έχουμε πει αποτελούν το υπόβαθρο με βάση το οποίο θα πρέπει να δούμε ποια θα είναι η πολιτική που θα πρέπει να ακολουθήσει μια συνεταιριστική επιχείρηση προκειμένου να προστατεύσει το σύστημά της από την εισβολή κάθε επίδοξου hacker.

Η πολιτική αυτή θα πρέπει να χαρακτηρίζεται από τα ακόλουθα :

⇒ Τον προσδιορισμό των κινδύνων που απειλούν την ασφάλεια των δεδομένων του συγκεκριμένου δικτύου,

⇒ Την οριοθέτηση των ευπαθών σημείων του και

⇒ Την επισήμανση των αναγκών εκείνων που το χρησιμοποιούν.

Η καταγραφή των παραπάνω θα πρέπει να οδηγήσει στη λήψη συγκεκριμένων μέτρων τα οποία θα πρέπει να στοχεύουν :

⇒ Στην προληπτική προστασία του συστήματος,

⇒ Στην διαπίστωση της εισβολής και

⇒ Στις ενέργειες που θα πρέπει να γίνουν για την αποκατάσταση της «τάξης» στο σύστημα - θύμα.

Για κάθε ένα από αυτά θα πρέπει να παρατηρήσουμε σε γενικές γραμμές, τα ακόλουθα :

Α. Η προληπτική προστασία του συστήματος

Με σκοπό την εκ των προτέρων προστασία του συστήματός της μία συνεταιριστική επιχείρηση οφείλει :

1. **Να προστατεύει με κάθε δυνατό μέσο τη διαρροή πληροφοριών σε τρίτους, οι οποίες αφορούν την ίδια, το σύστημά της, τους χρήστες του καθώς και τα προγράμματα που τρέχουν σ' αυτό.**

Όπως ήδη έχουμε σημειώσει το μεγαλύτερο και σπουδαιότερο όπλο των hackers είναι η πληροφόρηση για ο,τι αφορά τον μελλοντικό τους στόχο. Έτσι μεταξύ των ζητημάτων που τους ενδιαφέρουν περιλαμβάνεται π.χ. το είδος του συστήματος, τα προγράμματα που τρέχουν σ' αυτό τα ονόματα και τα passwords των χρηστών που το χρησιμοποιούν και φυσικά ο,τιδήποτε έχει σχέση με τη συνεταιριστική επιχείρηση στην οποία αυτό ανήκει. Όλες αυτές οι πληροφορίες θα αποτελέσουν τμήματα του σταυρολέξου που θα πρέπει να λύσει ο hacker προκειμένου να φτάσει στο στόχο του. Ειδικότερα κάθε είδους πληροφορία - εμπιστευτική ή μη, για το ιδιοκτησιακό καθεστώς ή για το προσωπικό (ονόματα, διευθύνσεις κατοικίας, ημερομηνίες γέννησης, μισθολόγιο) της συνεταιριστικής επιχείρησης - στόχου μπορεί να αποδειχθεί χρήσιμη για τον hacker, εφόσον του δίνεται η δυνατότητα να την αξιοποιήσει για την εισβολή του. Επομένως θα πρέπει να γίνεται μια εκ των προτέρων κατάταξη και διαβάθμιση των πληροφοριών αυτών που θα έχει να κάνει με την βαρύτητά τους και να λαμβάνονται τα κατάλληλα μέτρα για την αποτροπή της διαρροής τους σε κάθε τρίτο μη εξουσιοδοτημένο πρόσωπο. Είναι ακόμη εύλογο πως πληροφορίες που αφορούν τα ονόματα και τα passwords των χρηστών δεν θα πρέπει να είναι γνωστές σε κανένα άλλο εκτός από τον διαχειριστή του συστήματος. Επίσης θα πρέπει να δοθεί ιδιαίτερη προσοχή σε προγράμματα που με την αρχική σύνδεση δίνουν κάποια από τα χαρακτηριστικά του συστήματος ακόμα και σε μη εξουσιοδοτημένους χρήστες. Γι' αυτά θα πρέπει να γίνει ειδική ρύθμιση έτσι ώστε να πάψουν να λειτουργούν με τον τρόπο αυτό.

2. **Να περιορίζει την ελεύθερη και χωρίς καμμιά διάκριση πρόσβαση στο σύστημά της ακόμα και από τους ίδιους τους χρήστες της.** Αυτό θα το πετύχει επιτρέποντας στους χρήστες - εξωτερικούς ή εσωτερικούς - να το χρησιμοποιήσουν αποκλειστικά και μόνο μέσα στα πλαίσια των δικαιωμάτων ή των καθηκόντων που τους έχουν ανατεθεί από την ίδια την συνεταιριστική επιχείρηση. Έτσι ο κάθε χρήστης θα έχει τη δυνατότητα να χρησιμοποιεί το σύστημα μόνο για υπηρεσίες για τις οποίες εκ των προτέρων θα του έχει επιτραπεί η πρόσβαση σ' αυτό. Η υπέρβαση των δικαιωμάτων του θα πρέπει να καταγράφεται και στη συνέχεια να του ζητούνται εξηγήσεις γι' αυτή.

3. **Να στηρίζει τη λειτουργία του συστήματός της σε συγκεκριμένο software.**

   Ο βαθμός ασφάλειας ενός συστήματος εξαρτάται σε μεγάλο βαθμό από το πόσο νέο είναι το software που χρησιμοποιείται για τη λειτουργία του. Παλαιά προγράμματα που έχουν ήδη αποδειχθεί ευάλωτα σε επιθέσεις hackers δεν αποτελούν αξιόπιστη λύση, δεδομένου ότι αυτοί οι τελευταίοι γνωρίζουν το πώς να εκμεταλλευτούν τις αδυναμίες που έχουν παρουσιάσει στο παρελθόν. Μόνο η εγκατάσταση του πλέον σύγχρονου software θα είναι δυνατό να εγγυηθεί σε ικανοποιητικό σημείο την ασφάλεια ενός συστήματος.

4. **Να διαγράψει από κάθε τι (αρχείο, πρόγραμμα κλπ) που δεν χρησιμοποιείται πια.**

   Ο γενικός κανόνας λεει πως αν κάτι δεν το χρησιμοποιείς πλέον, θα πρέπει να το πετάξεις. Αυτό στην προκειμένη περίπτωση ισχύει για τα αρχεία, για δεδομένα, για προγράμματα και για λογαριασμούς χρηστών που δεν είναι πλέον ενεργοί. Η διαγραφή όλων αυτών θα δυσκολέψει τις προσπάθειες των hackers που ενδεχόμενα να ήξεραν και τα είχαν χρησιμοποιήσει στο παρελθόν. Ιδιαίτερη προσοχή θα

πρέπει να δίνεται στους λογαριασμούς των χρηστών. Η γνώση ενός από αυτούς από έναν hacker του δίνει την δυνατότητα να χρησιμοποιεί το σύστημα για αρκετό χρονικό διάστημα χωρίς να γίνεται αντιληπτός από κανέναν.

5. **Να χρησιμοποιεί firewalls ή / και μεθόδους κρυπτογράφησης δεδομένων.**

Τα firewalls θα πρέπει να πούμε πως είναι προγράμματα ασφαλείας που βρίσκονται σε κάποιο κόμβο του δικτύου. Σκοπός τους είναι η προστασία των δεδομένων του Server από κάθε ανεπιθύμητη επέμβαση. Στα μειονεκτήματά τους καταλογίζονται το υψηλό οικονομικό τους κόστος, η δυσκολία να ρυθμιστούν με τρόπο αποτελεσματικό για την εκπλήρωση της αποστολής τους και τέλος το γεγονός ότι η προστασία που παρέχουν είναι εντελώς σχετική. Είναι γνωστό π.χ. πως τα modems είναι ένα σημείο εισόδου στο δίκτυο.

Η μέθοδος της κρυπτογράφησης των δεδομένων όμως μπορεί να δώσει ικανοποιητικά αποτελέσματα εφόσον συνδυασθεί με τη δημιουργία καταλόγου νόμιμων χρηστών οι οποίοι θα αποκτούν πρόσβαση στο δίκτυο με τη χρήση passwords.

Β. Η διαπίστωση της εισβολής

Άσχετα με τα μέτρα που λαμβάνονται για την εκ των προτέρων προστασία ενός συστήματος, το σύστημα αυτό δεν είναι σε κάθε περίπτωση άτρωτο. Τα μέτρα αυτά αποτελούν απλώς το πρώτο βήμα που πρέπει να γίνει για την προστασία των δεδομένων που κινούνται σ' αυτό: Αυτό το οποίο μπορούν (μόνο) να πετύχουν τα μέτρα αυτά είναι το να **περιορίσουν** τις πιθανότητες προσβολής του συστήματος από ένα hacker, ιδίως αν αυτός δεν είναι και ιδιαίτερα έμπειρος !

Γ. Η αποκατάσταση της «τάξης» στο σύστημα - θύμα

Μετά τη διαπίστωση της εισβολής hackers σ' ένα σύστημα και της καταμέτρησης των ζημιών που προκλήθηκαν σ' αυτό θα πρέπει να επακολουθήσει μια σειρά ενεργειών οι οποίες θα αποσκοπούν στο α επαναφέρουν τα πράγματα στην πριν από την επίθεση κατάσταση. Οι ενέργειες αυτές θα πρέπει κατά τον Pipkin να περιλαμβάνουν τα εξής :

1. Αποκατάσταση των αρχείων που καταστράφηκαν.
2. Επαναλειτουργία του συνόλου των υπηρεσιών του συστήματος προς τους χρήστες του.
3. Διάγνωση και επιδιόρθωση του προβλήματος ασφαλείας του συστήματος με σκοπό να αποφευχθεί η επανάληψή του στο μέλλον.
4. Προσπάθεια για τον εντοπισμό των hackers για να παραδοθούν στις διωκτικές αρχές με τελικό σκοπό την παραπομπή τους στην δικαιοσύνη.
5. Παρουσίαση του περιστατικού στο κοινό με τέτοιο τρόπο ώστε να μην βλάπτεται το καλό όνομα της επιχείρησης - θύματος και
6. Ανάλυση των επιμέρους στοιχείων του όλου συμβάντος με την οποία θα διαπιστωθούν τα κενά στην πολιτική της ασφάλειας του συστήματος με προοπτική την απόκτηση εμπειριών οι οποίες είναι χρήσιμες για την αντιμετώπιση ανάλογων περιστατικών στο μέλλον.

Ολοκληρώνοντας οφείλουμε να επισημάνουμε πως υπάρχει και ένας μεγάλος αριθμός εφαρμογών software που χρησιμοποιούνται σήμερα από τις διάφορες επιχειρήσεις προκειμένου να ελέγξουν την ασφάλεια του δικτύου τους. Στην κατηγορία αυτή ανήκουν μεταξύ άλλων τα προγράμματα SATAN, Pingware, Netprobe κ.α.

Είναι γεγονός πως καθημερινά σ' ένα σύστημα ανακαλύπτονται και νέα προβλήματα ασφαλείας, πράγμα που απαιτεί τη συνεχή βελτίωση των τρόπων αντιμετώπισής τους. Το γεγονός αυτό καθιστά την προστασία ενός συστήματος μια συνεχή διεργασία με αρχή αλλά χωρίς τέλος. Ο «πόλεμος» ανάμεσα στους επίδοξους hackers και στους administrators των συστημάτων έχει ημερομηνία έναρξης εκείνη που άρχισε να λειτουργεί το σύστημα και ημερομηνία λήξης εκείνη που το σύστημα αυτό παύει να είναι ενεργό ! Ανάμεσα σ' αυτές όμως που είναι σημαντική η καταγραφή των ημερομηνιών των «μαχών – εισβολών» που διαδραματίζονται στο συγκεκριμένο σύστημα.

Η **καταγραφή** κάθε απόπειρας - επιτυχημένης ή μη - παράνομης εισόδου ή χρησιμοποίησης του συστήματος μιας επιχείρησης η διαπίστωση δηλ. της εισβολής που επιχειρείται στα δεδομένα της, αποτελεί το αμέσως μετά τα προληπτικά μέτρα που ήδη αναφέραμε, αναγκαίο για την ασφάλειά της μέτρο. Χωρίς αυτήν δεν μπορεί να γνωρίζει ούτε ότι δέχθηκε επίθεση, ούτε πότε την δέχθηκε και σε τελική ανάλυση θα αγνοεί το ότι το σύστημά της δεν είναι πλέον ασφαλές.

Για να γίνει η καταγραφή αυτή θα πρέπει **να παρακολουθείται σε 24ωρη βάση** η λειτουργία του συστήματος και να σημειώνεται κάθε τι που δεν συμβαίνει συνήθως σ' αυτό. Η διαπίστωση μιας ασυνήθιστης λειτουργίας του είναι δυνατό να αποκαλύψει μια επίθεση που δέχθηκε το σύστημα από hackers. Ανάλογη παρακολούθηση των χαρακτηριστικών των αρχείων του συστήματος που θα δείξει την οποιαδήποτε αδικαιολόγητη μεταβολή τους μπορεί να οδηγήσει στο ίδιο συμπέρασμα.

Η παρακολούθηση τόσο του συστήματος όσο και των αρχείων του, γίνεται με την χρήση του κατάλληλου κατά περίπτωση λογισμικού. Η διαπίστωση της συγκεκριμένης εισβολής θα αποδώσει περισσότερο, εφόσον παράλληλα αποκαλυφθούν οι ζημιές που είχε προξενήσει για να καταστεί δυνατή η άμεση αποκατάστασή τους.

ΒΙΒΛΙΟΓΡΑΦΙΑ

- Βασιλάκη ΕΕ (1993). Η καταπολέμηση της εγκληματικότητας μέσω ηλεκτρονικών υπολογιστών, Ποινικά 40, Αθήνα, Σάκκουλας.
- Kyas O., (1997) Internet Security : Risk Analysis, strageties and firewalls, London, International Thomson Computer Press.
- Pipkin L.D., (1997) Halting the Hacker: A practical Guide to Computer Security, New Jersey, Prentice Hall.
- Quarantiello E.E., (1997), Cyber Crime: How to protect yourself from computer criminals.
- Τσουραμάνης Χρ. (1996), Οικονομική Παραβατικότητα, Αθήνα, Ελλην.