1.1. Εισαγωγή

1.1.1. Μια σύντομη περιγραφή

Καθημερινά, πλέον, στην τηλεόραση ή το ραδιόφωνο, στις εφημερίδες και τα περιοδικά, υπάρχουν ειδήσεις που αφορούν στο ηλεκτρονικό έγκλημα. Το ηλεκτρονικό έγκλημα, ανέκαθεν μυστηριώδες, «γοητεύει» όλους όσους από εμάς ασχολούμαστε με την πληροφορική και τις εφαρμογές της.

Συχνά τα όρια του ηλεκτρονικού εγκλήματος, τόσο όσον αφορά στον τρόπο με τον οποίο διεξάγεται αυτό όσο και στην πράξη αυτή καθεαυτή, δεν είναι πολύ εύκολο να τεθούν. Για να είμαστε ακόμη περισσότερο ακριβείς, είναι πολύ δύσκολο να αναγνωριστεί μια τέτοια πράξη αλλά, ακόμη και αν αναγνωριστεί, είναι ακόμη πιο δύσκολο να «χωρέσει» μέσα στο υπάρχον νομικό πλαίσιο της κάθε χώρας ή πολιτείας, ώστε να μπορεί να αποδοθεί δικαιοσύνη. Για παράδειγμα, μπορεί κάποιος επίδοξος *hacker* να κατηγορηθεί για κλοπή, αν «υποκλέψει» με κάποιο τρόπο τα στοιχεία της πιστωτικής μας κάρτας και προβεί σε αγορές προς όφελός του; Προτού βιαστούμε να απαντήσουμε, ας σκεφτούμε πως αυτός ο επίδοξος *hacker* δεν έχει κλέψει την πιστωτική μας κάρτα, αφού αυτή βρίσκεται ακόμη στην κατοχή μας. Με τον όρο *hacker* θα υπονοούμε γενικά οποιονδήποτε επιτιθέμενο, κακόβουλο χρήστη ή επίδοξο «κλέφτη». Στις ενότητες που ακολουθούν θα αναλυθούν οι διάφορες κατηγορίες των *hackers*, ενώ θα επιχειρήσουμε να δώσουμε ένα σύντομο προφίλ τους για να γίνει περισσότερο κατανοητό το πρόβλημα.

Με το παραπάνω –αρκετά- απλουστευμένο παράδειγμα σαν αρχή, θα επιχειρήσουμε να ταξινομήσουμε βασικές έννοιες και κατηγορίες ενεργειών που συνιστούν πράξεις ηλεκτρονικού εγκλήματος. Επίσης, θα κάνουμε μια ιστορική αναδρομή στην παράλληλη πορεία της εξέλιξης της τεχνολογίας και των αντίστοιχων εγκλημάτων που σχετίζονται με αυτήν. Τέλος, θα αναφέρουμε αποσπάσματα του νομικού πλαισίου της χώρας μας, αλλά και αντίστοιχων διατάξεων στην Ευρωπαϊκή Ένωση, ώστε να μπορεί ο αναγνώστης να εξαγάγει τα δικά του συμπεράσματα σχετικά με το ηλεκτρονικό έγκλημα και τα δευτερεύοντα προβλήματα που δημιουργεί.

1.1.2. Απόψεις στο ηλεκτρονικό έγκλημα

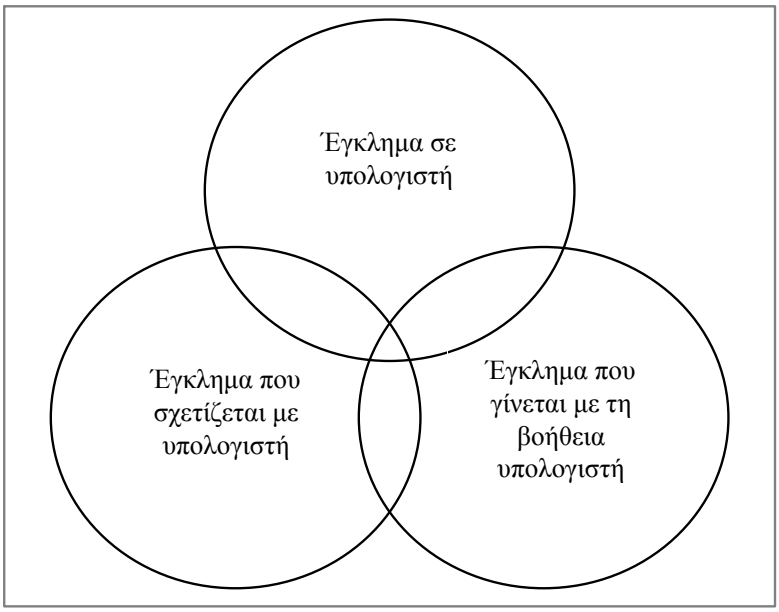
Σκοπός της συγκεκριμένης ενότητας είναι η παρουσίαση των θεμελιωδών εννοιών του ηλεκτρονικού εγκλήματος. Για να γίνει όμως σωστά αυτό, πάντοτε

μέσα στους σκοπούς και τους στόχους του συγκεκριμένου βιβλίου, ενθαρρύνουμε τον αναγνώστη να σκέφτεται όσο το δυνατόν ευρύτερα, ώστε να εξάγει τα δικά του συμπεράσματα και απόψεις. Η ευαισθησία του θέματος είναι πολύ μεγάλη και οποιαδήποτε άποψη θα πρέπει να είναι πολύ καλά διατυπωμένη και τεκμηριωμένη. Αναφορικά, ο αναγνώστης θα πρέπει να σκέφτεται σαν αστυνομικός ή κυβερνητικός υπάλληλος, σαν δημοσιογράφος, σαν *hacker* αλλά και σαν ειδικός στην ασφάλεια πληροφορικής, ώστε να μπορεί να εξετάζει όσο το δυνατόν πιο σφαιρικά το κάθε ζήτημα.

1.1.3. Κατηγορίες ηλεκτρονικού εγκλήματος

Η πρώτη μας προσέγγιση έχει να κάνει με τη διαίρεση της έννοιας «ηλεκτρονικό έγκλημα» σε περισσότερες, κάπως πιο ειδικές, κατηγορίες. Έτσι, όπως δείχνει και το σχήμα 1.1, μπορούμε να μιλάμε για:

- Έγκλημα σε υπολογιστή (*computer crime*)
- Έγκλημα που σχετίζεται με υπολογιστή (*computer related crime*)
- Έγκλημα που γίνεται με τη βοήθεια υπολογιστή (*computer aided crime*).



Σχήμα 1.1 *– Κατηγορίες ηλεκτρονικού εγκλήματος*

Στην πρώτη κατηγορία ανήκουν ενέργειες όπως η μη εξουσιοδοτημένη πρόσβαση σε υπολογιστικά συστήματα (*hacking* ή *cracking*), τα κακόβουλα προγράμματα (*malicious programs*) π.χ. ιοί (*viruses*), σκουλήκια (*worms*), δούρειοι ίπποι (*Trojan horses*) κτλ. Χαρακτηριστικά παραδείγματα αποτελούν οι *hackers*, το προφίλ των οποίων εξετάζεται στη συνέχεια, οι οποίοι παραδοσιακά «έσπαζαν» τα συστήματα ασφάλειας πολλών υπολογιστικών συστημάτων και είχαν πρόσβαση σε πληροφορίες που, υπό κανονικές συνθήκες, δεν έπρεπε να έχουν. Ακόμη, η δεύτερη μεγάλη υποκατηγορία, το κακόβουλο *software*, αποτελεί σήμερα τη μεγαλύτερη ίσως απειλή για τα υπολογιστικά συστήματα ολόκληρου του πλανήτη.

Στη δεύτερη κατηγορία, το έγκλημα που σχετίζεται με τους υπολογιστές, περιλαμβάνονται η ηλεκτρονική πορνογραφία (*computer pornography*), η πειρατεία λογισμικού (*software piracy*) ή ψηφιακού περιεχομένου γενικότερα κτλ. Η εξάπλωση του *Internet* σε όλα τα μήκη και τα πλάτη της Γης, σε συνδυασμό με το περιεχόμενο που μπορεί να φιλοξενήσει (γραφικά, *video*, ήχο κτλ.), επιτρέπει στα εκατομμύρια χρήστες του να ανταλλάσσουν πάσης φύσεως πληροφορίες.

Σε πάρα πολλές περιπτώσεις, δυστυχώς, οι πληροφορίες αυτές περιλαμβάνουν πορνογραφικό υλικό (και σε αρκετές περιπτώσεις υλικό παιδικής πορνογραφίας). Ακόμη χειρότερα, σήμερα κανείς μπορεί να βρει, μετά από ελάχιστες ώρες αναζήτησης, αναλυτικές οδηγίες κατασκευής εκρηκτικών μηχανισμών, ναρκωτικών ουσιών ή ακόμη και να παραγγείλει όπλα και ναρκωτικά μέσω του *Internet*. Προφανώς αυτές οι πληροφορίες δεν είναι και τόσο αθώες και σε πολλές περιπτώσεις οι συνέπειες είναι καταστροφικές. Επίσης, στην κατηγορία αυτή, περιλαμβάνονται -ευτυχώς[1] ή δυστυχώς- και οι πληροφορίες που υπάρχουν μέσα σε μηνύματα ηλεκτρονικής αλληλογραφίας (*email*). Τέλος, η περίπτωση παράνομης αντιγραφής λογισμικού αναφέρεται στη μη εξουσιοδοτημένη αντιγραφή λογισμικού το οποίο είναι πνευματικά κατοχυρωμένο, κυρίως για λόγους εμπορικής εκμετάλλευσης. Ειδικότερα τα τελευταία χρόνια, κυρίως λόγω της μείωσης του κόστους της τεχνολογίας, ανθεί η λεγόμενη «ψηφιακή πειρατεία» (*digital piracy*) που εμπορεύεται μουσικά *CDs*, ταινίες, εκπαιδευτικό υλικό, προγράμματα υπολογιστών κτλ.

Τέλος, στην τρίτη κατηγορία (έγκλημα με τη βοήθεια υπολογιστή) ανήκουν η απάτη στις ηλεκτρονικές συναλλαγές, η ψηφιακή αντιγραφή εντύπων κτλ. Χαρακτηριστικά παραδείγματα αποτελούν η υποκλοπή στοιχείων πιστωτικών καρτών και η πλαστογράφηση εντύπων (π.χ. χαρτονομίσματα μέσω *scanners*).

---

[1] Π.χ. περιπτώσεις τρομοκρατικών ενεργειών.

1.1.4. Μια σύντομη ιστορική αναδρομή

Αξίζει να κάνουμε μια σύντομη ιστορική αναδρομή στο ηλεκτρονικό έγκλημα μελετώντας κυρίως το τεχνολογικό και νομικό πλαίσιο κάθε εποχής. Ο στόχος είναι, αφενός, να προσπαθήσουμε να παρακολουθήσουμε την εξέλιξή του και, αφετέρου, να καταλάβουμε πως «πολλά προβλήματα στην ηλεκτρονική ασφάλεια είναι μετενσάρκωση παλαιών και γνωστών προβλημάτων». Τέλος, είναι απαραίτητο να δούμε πώς και με ποιο τρόπο αντιμετωπίζονταν οι πράξεις ηλεκτρονικού εγκλήματος κάθε εποχή αλλά και ποιος είναι, σε κάθε περίπτωση, ο πραγματικός επιτιθέμενος.

Στις αρχές της δεκαετίας του ’80 είχαμε την έλευση του δικτυακού πρωτοκόλλου X.25, μέσω του οποίου οι υπολογιστές εκείνης της εποχής (*Sinclair Spectrum*, *PC XT*/*PC AT* και *Apple*) μπορούσαν, με μια κατάλληλη συσκευή (του γνωστού σε όλους μας *modem*) καθώς και τη χρήση του τηλεπικοινωνιακού δικτύου, να επικοινωνήσουν μεταξύ τους. Σύντομα, πολλοί χρήστες ξεκίνησαν να μοιράζονται πληροφορίες μέσω των λεγόμενων *BBSs* (*Bulletin Board Service*). Ο τρόπος ήταν απλός: αρκούσε ένα τηλεφώνημα από το *modem* σε έναν συγκεκριμένο αριθμό.

Στην κλήση απαντούσε το *modem* του «απέναντι» υπολογιστή και η σύνδεση ήταν επιτυχής. Μετά, ο χρήστης που συνδεόταν στην *BBS,* μπορούσε να διαβάσει συγκεκριμένες πληροφορίες, να «κατεβάσει» (*download*) όποιες από αυτές ήθελε αλλά και να «ανεβάσει» (*upload*) δικές του με χρήση κατάλληλων πρωτοκόλλων.

Κύριοι φορείς των συγκεκριμένων υπηρεσιών ήταν τα πανεπιστήμια, διάφορες εμπορικές εταιρείες αλλά και πολλοί ιδιώτες. Ιστορικά και μόνο αναφέρουμε πως οι πρώτες πληροφορίες που έβρισκε ένας χρήστης που συνδεόταν σε μια *BBS* (στην εισαγωγική δηλαδή οθόνη), ήταν αναλυτικές οδηγίες για το πως μπορεί να συνδεθεί σε αυτήν.

Σύντομα εμφανίστηκαν και οι πρώτοι *hackers* οι οποίοι χρησιμοποιούσαν τα *modems* για να συνδεθούν σε υπολογιστές στους οποίους δεν έπρεπε κανονικά να έχουν πρόσβαση (π.χ. στρατιωτικούς υπολογιστές ή ακαδημαϊκά ιδρύματα, για εκείνους που δεν ήταν φοιτητές στη συγκεκριμένη σχολή). Καθώς τα μέτρα ασφάλειας ήταν ελάχιστα, την τριετία 1983-85 αναφέρονται στη Μεγάλη Βρετανία τα πρώτα κρούσματα *hacking*, τα οποία αφορούσαν κυρίως σε απόπειρες, πολλές φορές μάλιστα επιτυχημένες, για παράνομη αντιγραφή πληροφοριών καθώς και πρόκληση ζημιών σε υπολογιστικά συστήματα πανεπιστημίων. Την ίδια εποχή, και πιο συγκεκριμένα το 1984,

ιδρύεται το «τμήμα» δίωξης ηλεκτρονικού εγκλήματος στην *New Scotland Yard*[2]. Επίσης, η Μεγάλη Βρετανία γίνεται η πρώτη χώρα στην Ευρώπη η οποία εκδίδει νόμο περί προστασίας των ηλεκτρονικών δεδομένων (*Data Protection Act* 1984). Τέλος, κυκλοφορεί περιοδικό με το «εγχειρίδιο του *hacker*» (*the hacker's handbook*), το οποίο γίνεται ανάρπαστο.

Τα επόμενα χρόνια, μέχρι τα τέλη της δεκαετίας, σημαδεύονται από την άνθιση των λεγόμενων υπολογιστικών «ιών» (*computer viruses*). Ο ιός *Aids* κάνει θραύση καθώς πολλά περιοδικά υπολογιστών στην Ευρώπη κυκλοφορούν με δισκέτα μολυσμένη από το συγκεκριμένο ιό. Η περίπτωση αυτή είναι η πρώτη μαζική μόλυνση υπολογιστικών συστημάτων αλλά και η πρώτη περίπτωση εκβιασμού, από το συγγραφέα του «ιού», ο οποίος απαιτούσε συγκεκριμένο χρηματικό αντίτιμο, για να παρέχει το «αντίδοτο».

Το 1989 είναι η χρονιά στην οποία γίνεται η πρώτη σοβαρή προσπάθεια, σε Πανευρωπαϊκό επίπεδο, για τη νομική αντιμετώπιση του ηλεκτρονικού εγκλήματος. Εκείνη την εποχή υπήρχαν ελάχιστες χώρες στον κόσμο (Ηνωμένο Βασίλειο, Αυστρία, Δανία, Γερμανία, Γαλλία, Ομοσπονδιακή Δημοκρατία της Γερμανίας, Ελλάδα, Νορβηγία, Σουηδία, Ηνωμένες Πολιτείες, Αυστραλία, Ιαπωνία και Καναδάς), οι οποίες είχαν ήδη θεσπίσει νόμους που κάλυπταν και κάποια τμήματα του ηλεκτρονικού εγκλήματος. Οι στόχοι της συγκεκριμένες επιτροπής (*Legal Affairs Committee*), η οποία συγκροτήθηκε από εκπροσώπους όλων σχεδόν των Ευρωπαϊκών χωρών, ήταν η δημιουργία ενός κοινού πλαισίου για γρήγορη και αποτελεσματική αντίδραση σε περιστατικά ασφάλειας που υποδήλωναν πράξεις ηλεκτρονικού εγκλήματος. Οι νομικοί της συγκεκριμένης επιτροπής είχαν καταλάβει πως το ηλεκτρονικό έγκλημα είναι ένα πρόβλημα που δεν γνωρίζει σύνορα και η ανάγκη ύπαρξης ενός ενιαίου (κατά το δυνατόν) νομικού πλαισίου ήταν παραπάνω από απαραίτητη. Η σύσταση της συγκεκριμένης επιτροπής έγινε γνωστή με την ονομασία *Council of Europe Recommendation R*(89)9, τα περιεχόμενα της οποίας εξετάζονται σε επόμενη ενότητα. Τέλος, την εποχή εκείνη κυκλοφορεί το περιβόητο βιβλίο *The Cuckoo's Egg*, στο οποίο ο συγγραφέας περιγράφει την πρώτη καταγεγραμμένη περίπτωση διεθνούς κατασκοπείας μέσω υπολογιστών.

Η αρχή της δεκαετίας του '90, εκτός από το κίνημα *grunge*, φέρνει την ίδρυση του πρώτου παγκόσμιου κέντρου συντονισμού για περιστατικά ασφάλειας σε υπολογιστικά συστήματα στο *Software Engineering Institute* του πανεπιστημίου *Carnegie Melon*, στις ΗΠΑ. Το κέντρο αυτό, είναι γνωστό

[2] Για περισσότερο από 10 χρόνια, το «τμήμα» αυτό είχε έναν μόνο υπάλληλο, τον *John Austen*.

σήμερα σαν *CERT*/*CC* (*Computer Emergency Response Team*/*Coordination Center*).

Παράλληλα, το *Internet* εξαπλώνεται ραγδαία μέσω της υπηρεσίας *WWW* (*world wide web*) η οποία επιτρέπει τη φιλοξενία αρχείων ήχου, βίντεο, εικόνων και υπερκειμένου (*hypertext*) στις ιστοσελίδες των αντίστοιχων διακομιστών (*servers*). Η άνθιση αυτή συνοδεύεται, όμως, από χιλιάδες σελίδες με πορνογραφικό υλικό, τρομοκρατικές προκηρύξεις καθώς και από αμέτρητες σελίδες μέσα από τις οποίες προσφέρεται – με παράνομο τρόπο – πειρατικό λογισμικό για υπολογιστές. Από την άλλη πλευρά, καταγράφεται η πρώτη περίπτωση βιομηχανικής κατασκοπείας με δράστη τον περιβόητο αμερικανό *hacker Kevin Mitnick*, ο οποίος και φυλακίζεται με την κατηγορία πρόκλησης βλάβης σε υπολογιστικά συστήματα καθώς και για διαφυγόντα κέρδη 9 δισεκατομμυρίων δολαρίων.

Περίπου στα 1995 ξεκινά η ραγδαία αύξηση των Παρόχων *Internet* Υπηρεσιών (*Internet Service Providers – ISPs*), ενώ κάνουν δειλά-δειλά τα βήματά τους οι πρώτες εταιρείες οι οποίες προσφέρουν υπηρεσίες ηλεκτρονικού εμπορίου (*e-commerce*). Την ίδια εποχή, όμως, κυκλοφορεί, δωρεάν στο *Internet*, το εργαλείο *SATAN* (*Security Administrator Tool for Analyzing Networks*), το οποίο χρησιμεύει για να ανακαλύπτει αδυναμίες στη δικτυακή και υπολογιστική υποδομή διαφόρων οργανισμών και εταιρειών. Το *SATAN* κυκλοφόρησε αρχικά σαν ένα πολύτιμο εργαλείο για τους διαχειριστές δικτύων και συστημάτων (*network and systems administrators*) των διαφόρων εταιρειών, γρήγορα όμως οι *hackers* κατάλαβαν τη διττή σημασία του και άρχισαν να το χρησιμοποιούν εκτεταμένα. Παράλληλα, ξεκινά από τη Μεγάλη Βρετανία η πρώτη προσπάθεια, με το πρότυπο συμμόρφωσης *BS* 7799, για την έκδοση ενός «οδηγού» με κατάλληλες εταιρικές πολιτικές ασφάλειας[3].

Το δεύτερο μισό της δεκαετίας του ’90 επιφυλάσσει πολλές δυσάρεστες εκπλήξεις στον κόσμο της πληροφορικής. Κυκλοφορεί ο πρώτος *macro-virus*, ο οποίος προσβάλλει μη εκτελέσιμα αρχεία (π.χ. αρχεία κειμένου ή λογιστικά φύλλα), γνωστός με το όνομα *Melissa*. Ο ιός αυτός, όσο και οι κλώνοι του, προξενούν ζημιές εκατομμυρίων δολαρίων σε υπολογιστικά συστήματα σε όλα τα μήκη και πλάτη του πλανήτη. Παράλληλα με τους *macro-viruses*, ανθούν και τα διάφορα *freeware tools*, εργαλεία λογισμικού τα οποία διατίθενται ελεύθερα στο *Internet*, με τα οποία μπορεί κάποιος *hacker* να εκμεταλλευτεί τα όποια υπάρχοντα κενά ασφάλειας. Τέλος, οι σελίδες με σχετικό (με το παραπάνω) περιεχόμενο εκείνη την εποχή ανέρχονται σε μερικές χιλιάδες, ενώ

[3] Το πρότυπο αυτό, καθώς και η σημασία του, περιγράφονται σε επόμενη ενότητα του βιβλίου.

η παράνομη αντιγραφή ψηφιακού περιεχομένου γίνεται ολοένα και μεγαλύτερη με την έλευση των αντιγραφικών συσκευών οπτικών δίσκων (*CD-R*).

Η δεκαετία του '90 μας αφήνει με μια τεράστια αγωνία για τα υπολογιστικά συστήματα του πλανήτη τα οποία διακυβεύουν την ασφάλεια ολόκληρης της Γης. Ο «ιός του 2000» (*millennium bug*), σύμφωνα με τον οποίο θα σταματούσε η λειτουργία των περισσοτέρων υπολογιστικών συστημάτων, τελικά μάλλον προκάλεσε πολύ περισσότερη αναστάτωση παρά συνέπειες και ζημιές[4].

Όσες ζημιές, όμως, δεν προξένησε το συγκεκριμένο πρόβλημα μάλλον, παρά ιός, τις προξένησε ο πιο «ερωτικός» -μέχρι σήμερα- ιός, γνωστός με την ονομασία «*I Love You Virus*» ή «*Love Bug*», ο οποίος ταλαιπώρησε εκατομμύρια υπολογιστές σε ολόκληρο τον κόσμο[5].

Η καινούργια χιλιετηρίδα ξεκίνησε με την πρώτη διεθνή συνθήκη για το ηλεκτρονικό έγκλημα (*Cyber Crime Convention* 2001), την οποία προσυπέγραψε και η χώρα μας αλλά και με δύο πολύ καταστροφικούς ιούς (*Code Red* και *Nimda*[6]). Επίσης, οι φήμες για ένα παγκόσμιο σύστημα παρακολούθησης τηλεφωνικών συνομιλιών και μηνυμάτων ηλεκτρονικού ταχυδρομείου, από την κυβέρνηση των ΗΠΑ, (γνωστό με το κωδικό όνομα *Carnivore*) επιβεβαιώθηκαν από ορισμένους *hackers* οι οποίοι δημοσίευσαν απόρρητα έγγραφα της Υπηρεσίας Εθνικής Ασφάλειας των ΗΠΑ (*National Security Agency – NSA*). Κάτι ανάλογο έγινε και στην Ευρώπη, με το γνωστό πλέον -σε πολλούς- σύστημα παρακολούθησης *Echelon*.

Τέλος, τα δραματικά γεγονότα της 11ης Σεπτεμβρίου έμελλε να επηρεάσουν τα μέγιστα τις εξελίξεις σε όλα τα μήκη και πλάτη του πλανήτη. Σύσσωμος ο δυτικός κόσμος παραδέχθηκε πως οι τρομοκράτες χρησιμοποίησαν κρυπτογραφικές μεθόδους για να ανταλλάξουν πληροφορίες μεταξύ τους χωρίς να γίνονται αντιληπτοί, αλλά και ότι εισέβαλαν σε πολλά συστήματα των ΗΠΑ με σκοπό να αποκομίσουν πολύτιμες μυστικές πληροφορίες. Η ημερομηνία

---

[4] Αξίζει να τονισθεί όμως πως αντιμετωπίστηκε με συντονισμένο τρόπο παγκοσμίως

[5] Αν και για τον συγκεκριμένο ιό έχουν γραφτεί χιλιάδες απόψεις, ο τρόπος λειτουργίας του καθώς και οι ζημιές που προκαλούσε (αρκετά συγκεκριμένες) έβαλαν σε σκέψεις πολλούς ειδικούς σε θέματα ασφάλειας πληροφορικής ανά τον πλανήτη. Σύμφωνα μάλιστα με πολλούς από αυτούς, δεν αποκλείεται ο ιός αυτός να γράφτηκε κατά παραγγελία μεγάλης δισκογραφικής εταιρείας για να καταπολεμήσει το φαινόμενο *Napster* που εκείνη την εποχή επέτρεπε σε εκατομμύρια χρήστες να ανταλλάσσουν δωρεάν μουσικά αρχεία μεταξύ τους.

[6] Αναγραμματισμός της σύντμησης *admin* η οποία υπονοεί τον διαχειριστή (*administrator*) ενός συστήματος που τις περισσότερες φορές είναι και ο «κυρίαρχός» του.

αυτή μάλλον θα είναι η αρχή μιας σειράς εξελίξεων και στην ασφάλεια πληροφοριών[7].

1.2. Οι «γνωστοί-άγνωστοι» Hackers

1.2.1. Το Προφίλ των hackers

Για τους *hackers* έχουν χυθεί αρκετά κιλά μελάνης και όμως το πραγματικό τους προφίλ παραμένει ακόμη ανεξιχνίαστο. Διαισθητικά και μόνον καλούμε *hacker* οποιονδήποτε ασχολείται μανιωδώς με τους υπολογιστές, είτε περνώντας τον καιρό του παίζοντας παιγνίδια είτε γράφοντας χιλιάδες γραμμές κώδικα καθημερινά.

Το προφίλ του *hacker* που σχεδόν έχουμε στο μυαλό μας, έχει διαμορφωθεί κυρίως από τα μέσα μαζικής ενημέρωσης καθώς και από τον πλήρη σκοταδισμό που καλύπτει όλες σχεδόν τις ιστορίες ηλεκτρονικού εγκλήματος. Έρευνες που έχουν γίνει σε απλούς πολίτες δείχνουν πως η άποψη που επικρατεί κυρίως για τους *hackers* είναι πως είναι άτομα νεαρής ηλικίας (τις περισσότερες φορές ανήλικα), ιδιαίτερα ευφυή που παίζουν στα δάκτυλα τα συστήματα ασφάλειας οποιουδήποτε σχεδόν οργανισμού ή εταιρείας. Τέλος, οι *hackers* έχουν πολύ καλές γνώσεις (απο)συναρμολόγησης υπολογιστικών συστημάτων, δικτύων και προγραμματισμού.

Ιδιαίτερο ενδιαφέρον παρουσιάζει η εικόνα που έχουν οι ίδιοι οι *hackers* για τον εαυτό τους.

Ενισχύοντας όλα τα προηγούμενα, οι *hackers* πιστεύουν πως ανήκουν σε μια ελίτ, στην οποία λίγα μόνον άτομα έχουν θέση. Αν και οι κανόνες και οι διαδικασίες εισαγωγής σε αυτήν την ελίτ είναι ιδιαίτερα θολές, ωστόσο ακολουθείται κάποιο άγραφο τελετουργικό[8]. Από τη στιγμή που ένα άτομο γίνεται μέλος ενός *hacking* γκρουπ, είναι υποχρεωμένο να σέβεται αυτό το άτυπο τελετουργικό και να ακολουθεί τους άγραφους κανόνες με τα πιστεύω του. Οι *hackers* πιστεύουν επίσης πως είναι οι καλύτεροι υπερασπιστές της ελεύθερης διακίνησης πληροφοριών. Ακόμη περισσότερο, οι *hackers* πιστεύουν πως είναι οι πραγματικοί σύγχρονοι επαναστάτες απέναντι στον κρατικό

[7] Και για όσους λατρεύουν τα οικονομικά μεγέθη, η κυβέρνηση των ΗΠΑ αποφάσισε να αυξήσει από 5 σε 17 δισεκατομμύρια δολάρια το ποσό που δαπανάται ετησίως για την καταπολέμηση του ηλεκτρονικού εγκλήματος στο εσωτερικό της χώρας.

[8] Συνήθως περιλαμβάνει ζημιές σε υπολογιστικά συστήματα

μηχανισμό, ο οποίος επιβάλλει πρακτικές που πολλές φορές έρχονται σε σύγκρουση με τις προσωπικές ελευθερίες των πολιτών.

Χωρίς να θέλουμε να επεκτείνουμε σε βάθος τις παραπάνω περιγραφές και βασιζόμενοι σε πραγματικά στοιχεία, τα οποία τις περισσότερες φορές είναι σκόρπια, θα επιχειρήσουμε να δώσουμε εν συντομία το πραγματικό προφίλ ενός *hacker*, αν και ο αναγνώστης ενθαρρύνεται να ανατρέξει στη σχετική βιβλιογραφία που βρίσκεται στο τέλος της συγκεκριμένης ενότητας[9]. Ο κύριος λόγος που γίνεται αυτό είναι για να υπάρχει μια βάση για τις ενότητες που ακολουθούν. Το προφίλ αυτό προσπαθεί να συμπεριλάβει όλες τις απόψεις που αναφέρονται στην αντίστοιχη ενότητα προηγουμένως και σε καμιά περίπτωση δεν εκφράζει προσωπικές απόψεις ή υποθέσεις.

Έτσι λοιπόν, ο μέσος *hacker* είναι άνδρας, ηλικίας 15-35 χρόνων, απόφοιτος –τουλάχιστον- της μέσης εκπαίδευσης. Έχει μέτριες έως καλές γνώσεις υπολογιστών και δικτύων για τις οποίες μάλιστα καυχιέται ιδιαίτερα, όπου και όποτε μπορεί (συνήθως με τους «ομοίους» του[10]). Ο συνήθης *hacker* δεν έχει ιδιαίτερες κοινωνικές επαφές και σχέσεις – προτιμά τον όποιο ελεύθερο χρόνο του να τον περνά με τον υπολογιστή του. Επίσης, έχει μια ιδιαίτερη αγάπη στη νύχτα καθώς τότε μπορεί να δρα με λίγη περισσότερη άνεση και είναι έντονα μυστικοπαθής. Συνήθως ένας *hacker* δείχνει ατημέλητος εξωτερικά, είτε λόγω των άτυπων κανόνων που αναφέραμε στα προηγούμενα είτε λόγω του γεγονότος ότι η νυχτερινή του ενασχόληση με τους υπολογιστές του επιτρέπει να κοιμάται ελάχιστα. Τέλος, λόγω του τελευταίου γεγονότος, ένας *hacker* είναι περισσότερο επιρρεπής σε «ουσίες» που του επιτρέπουν να μένει ξύπνιος όσο περισσότερο γίνεται.

1.2.2. Τα διάφορα είδη των hackers

Αν υπήρχε στις μέρες μας ένα κατάλληλο λεξικό με όρους σχετικούς με το ηλεκτρονικό έγκλημα, ο όρος *hacker* θα περιγράφονταν κάπως έτσι:

[9] Υπάρχουν ολόκληρα βιβλία τα οποία περιγράφουν λεπτομερώς διάφορες ιστορίες ηλεκτρονικού εγκλήματος και τους πρωταγωνιστές τους, επιχειρώντας να δώσουν το πραγματικό κοινωνικό προφίλ ενός *hacker* – σε αρκετές περιπτώσεις αυτό γίνεται με ιδιαίτερη επιτυχία.

[10] Δεν είναι λίγες όμως οι φορές που οι περισσότεροι *hackers* έχουν αποκαλυφθεί κυρίως για αυτή την τάση τους.

Hacker: αυτός που ασχολείται μανιωδώς με τους ηλεκτρονικούς υπολογιστές για οικονομικό ή πολιτικό όφελος, εγκληματίας, κλέφτης - αυτός που αποκτά ή επιχειρεί να αποκτήσει πρόσβαση σε υπολογιστικούς πόρους χωρίς την κατάλληλη εξουσιοδότηση

Όπως αναφέραμε και στα προηγούμενα, ο όρος *hacker* είναι γενικός και χρησιμοποιείται για να περιγράψει έναν κακόβουλο χρήστη. Αξίζει τον κόπο να επιχειρήσουμε μια ταξινόμηση των διαφόρων κατηγοριών των *hackers*, σύμφωνα με τους στόχους τους καθώς και τις ζημιές που προκαλούν, για να γνωρίζουμε καλύτερα πώς μπορούμε να προστατεύσουμε τα πληροφοριακά μας αγαθά (συμπεριλαμβανομένων και των δεδομένων μας).

1.2.2.1. Εσωτερικοί χρήστες (Insiders)

Σύμφωνα με το Ινστιτούτο Τεχνολογίας Λογισμικού του Πανεπιστημίου *Carnegie Melon* των ΗΠΑ (γνωστό και ως *CERT/CC*), οι εσωτερικοί χρήστες προκαλούν το 66% των περιστατικών ασφάλειας σε ένα πληροφοριακό σύστημα. Με τον όρο περιστατικό ασφάλειας ορίζεται οποιαδήποτε ενέργεια βάζει σε κίνδυνο τα αγαθά ενός πληροφοριακού συστήματος.

Υπάρχουν αρκετές περιπτώσεις που οι εσωτερικοί χρήστες προκαλούν περιστατικά ασφάλειας λόγω της περιέργειας ή της άγνοιάς τους, χωρίς όμως αυτό να είναι η πιο συνηθισμένη περίπτωση. Για παράδειγμα ένας υπάλληλος που θέλει να γνωρίζει κάποια εμπιστευτικά στοιχεία (π.χ. το μισθό συναδέλφου του) μπορεί να προσπαθήσει να βρει το κατάλληλο αρχείο (π.χ. *misthoi.xls misthologia.xls*) και στη συνέχεια να το διαβάσει. Πιο συνηθισμένη περίπτωση είναι όμως ένας υπάλληλος να αντιγράφει εμπιστευτικές πληροφορίες της εταιρείας σε αποθηκευτικά μέσα (π.χ. δισκέτες, *CD-ROMs* κτλ.), ή να τις στέλνει μέσω *email* σε έναν δικό του *email* λογαριασμό και να τις «κατεβάζει» αργότερα από το σπίτι του[11].

Στην κατηγορία αυτή κατατάσσονται και οι πρώην χρήστες ενός πληροφοριακού συστήματος. Με τον όρο «πρώην» εννοούμε υπάλληλους μιας εταιρείας οι οποίοι έχουν απολυθεί ή παραιτηθεί και θέλουν να εκφράσουν τη δυσαρέσκειά τους σε αυτήν, προκαλώντας ζημιές στα πληροφοριακά της

[11] Πολλοί από αυτούς χρησιμοποιούν κρυπτογραφικά προγράμματα για να «κρύψουν» τις πληροφορίες αυτές ή χρησιμοποιούν έξυπνα φορητά αποθηκευτικά μέσα (π.χ. *USB Hard Disks*).

αγαθά. Δεν θα πρέπει να αγνοούμε, επίσης, την περίπτωση ένας πρώην υπάλληλος να έχει σαν στόχο να υποκλέψει εταιρικές πληροφορίες και να τις χρησιμοποιήσει για δικό του όφελος.

Τα περιστατικά ασφάλειας που προκαλούνται από εσωτερικούς χρήστες αποτελούν ένα σημαντικό πρόβλημα σε κάθε υπεύθυνο ασφάλειας ενός πληροφοριακού συστήματος. Ο κίνδυνος είναι ιδιαίτερα μεγάλος μια και έχουν γνώση του συστήματος καθώς και ένα συγκεκριμένο επίπεδο πρόσβασης στις εταιρικές πληροφορίες. Επίσης, σε πολλές χώρες του κόσμου, υπάρχουν νόμοι που περιορίζουν την επίβλεψη (*monitoring*) των πράξεων των υπαλλήλων μιας εταιρείας.

1.2.2.2. Κατάσκοποι (Spies)

Υπάρχουν πολλές περιπτώσεις που οι υπολογιστές χρησιμοποιούνται από κατασκόπους: είτε κυβερνητικούς, είτε στρατιωτικούς, είτε βιομηχανικούς. Με τον όρο «βιομηχανικός κατάσκοπος» περιγράφεται ένας χρήστης ο οποίος πληρώνεται και εξοπλίζεται από μια εταιρεία για να προκαλέσει ζημιά σε μια άλλη ανταγωνιστική εταιρεία[12]. Τα κίνητρα των κατασκόπων ποικίλλουν, από υποκλοπή συγκεκριμένων εταιρικών δεδομένων μέχρι πλήρη «καταστροφή» πληροφοριακών συστημάτων ή/και δικτύων.

Οι κατάσκοποι έχουν συγκεκριμένους στόχους και πληρώνονται πολύ καλά για αυτό. Για τους λόγους αυτούς είναι ιδιαίτερα επίμονοι. Στις περισσότερες των περιπτώσεων, οι κατάσκοποι, είναι πολύ καλά εξοπλισμένοι με ό,τι τελευταίο έχει να επιδείξει η τεχνολογία. Επίσης, διαθέτουν κατάλληλη τεχνογνωσία, είναι ιδιαίτερα ικανοί και υπομονετικοί και έχουν – σχεδόν πάντα – μια αρχική γνώση του πληροφοριακού συστήματος στο οποίο επιτίθενται. Τέλος, οι κατάσκοποι, είναι ιδιαίτερα προσεκτικοί και προσπαθούν να περνούν απαρατήρητοι από τα συστήματα ασφάλειας τα οποία υπάρχουν. Η δουλειά τους μπορεί να απαιτεί απόλυτη προσήλωση στο στόχο τους για πολλούς μήνες (μερικές φορές ίσως και χρόνια!).

1.2.2.3. Βάνδαλοι (Vandals)

Οι «Βάνδαλοι» είναι οι περισσότερο κακόβουλοι χρήστες: χωρίς να έχουν συγκεκριμένο κίνητρο προσπαθούν να προκαλέσουν όσο το δυνατόν περισσότερη ζημιά σε ένα υπολογιστικό σύστημα. Συχνά, μάλιστα, είναι πρώην (και αρκετά δυσαρεστημένοι) υπάλληλοι μιας εταιρείας. Στις

[12] Φαινόμενο το οποίο λαμβάνει επιδημικές διαστάσεις, κυρίως στις ανεπτυγμένες χώρες του δυτικού κόσμου.

περισσότερες των περιπτώσεων, οι βάνδαλοι εξαπολύουν «επιθέσεις άρνησης εξυπηρέτησης» (*Denial Of Service – DoS – attack*) που υποχρεώνουν σε προσωρινή (..) διακοπή τα υπολογιστικά συστήματα μιας εταιρείας. Οι επιθέσεις αυτής της κατηγορίας γίνονται ολοένα και περισσότερο επικίνδυνες καθώς, ιδιαίτερα τα τελευταία χρόνια, οι πιο δημοφιλείς εταιρείες του πλανήτη έχουν πέσει θύματα μιας τέτοιας επίθεσης[13]. Τέλος, οι βάνδαλοι δεν λαμβάνουν οι ίδιοι κανένα μέτρο προστασίας και καυχώνται ιδιαίτερα για τα κατορθώματά τους.

1.2.2.4. Οι «ανένταχτοι»

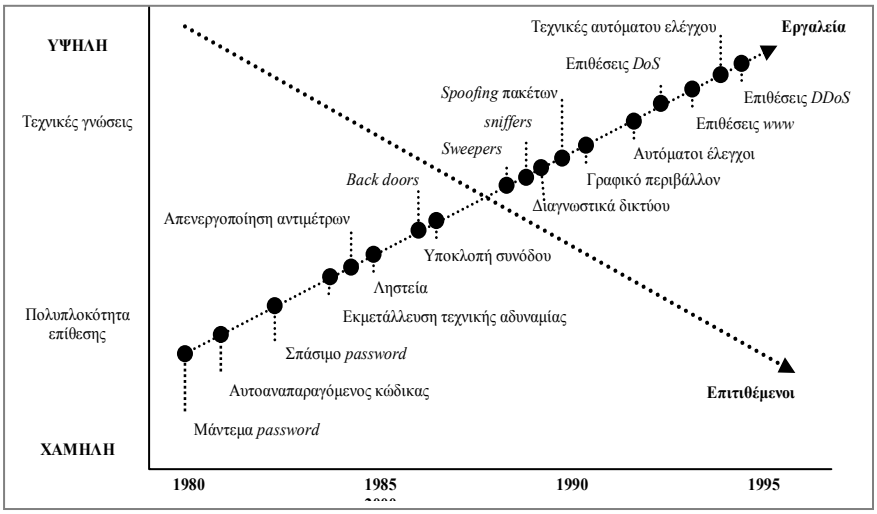
Υπάρχουν, βέβαια, και πολλές άλλες κατηγορίες κακόβουλων χρηστών οι οποίοι έχουν διάφορες ονομασίες στην «αργκό» του *Internet*: *script kiddies*, *anklebiters*, *crackers* κτλ. Οι χρήστες αυτοί συνήθως έχουν λίγους υπολογιστικούς πόρους και γνώσεις αλλά τον περισσότερο χρόνο. Επίσης, δεν έχουν και αυτοί κάποιο συγκεκριμένο κίνητρο ή στόχο – είναι απλά η επιθυμία τους να αποδείξουν (τις περισσότερες φορές στους υπόλοιπους) πως είναι ικανοί να παρακάμψουν τα συστήματα ασφάλειας ενός πληροφοριακού συστήματος που τους προτρέπει να προκαλούν ζημιές.

Συνήθως οι χρήστες αυτοί χρησιμοποιούν το *Internet* για να βρουν τα κατάλληλα εργαλεία και προγράμματα με τα οποία μπορούν και εξαπολύουν διάφορες επιθέσεις. Τα εργαλεία αυτά είναι πλήρως αυτοματοποιημένα, χωρίς να χρειάζεται απολύτως καμία γνώση των πολύπλοκων δικτυακών πρωτοκόλλων και των διαφόρων γλωσσών προγραμματισμού. Αν και γενικά επικρατεί η άποψη ότι τα εργαλεία αυτά είναι πανάκεια και οποιοσδήποτε μπορεί να τα βρει εύκολα και να τα χρησιμοποιήσει κατά βούληση, εμείς θα υποστηρίξουμε πως κάτι τέτοιο δεν είναι 100% αληθές. Τα συγκεκριμένα εργαλεία από μόνα τους δεν μπορούν να προκαλέσουν ζημιές σε ένα σύστημα, μπορούν όμως να γίνουν πραγματικά όπλα (ίσως και μαζικής καταστροφής) αν χρησιμοποιηθούν από άτομα που έχουν τις σχετικές γνώσεις.

Το παρακάτω σχήμα παρουσιάζει μια εικόνα των τεχνικών γνώσεων των *hackers* σε σχέση με την ολοένα και μεγαλύτερη «αυτοματοποίηση» των εργαλείων που χρησιμοποιούν.

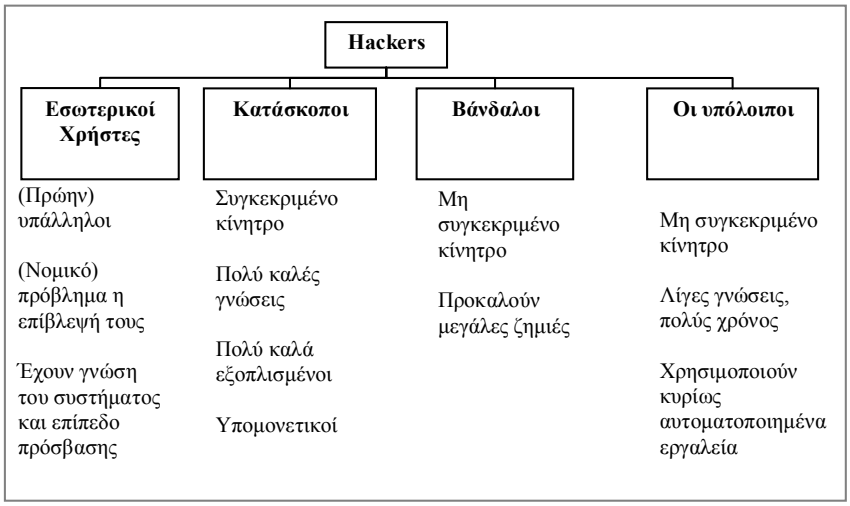
---

[13] Πιο συγκεκριμένα, οι βάνδαλοι συνεργάζονται κατά δεκάδες (ή ακόμα και εκατοντάδες) ώστε η επίθεση αυτή να γίνει με κατανεμημένο τρόπο (*Distributed Denial of Service Attacks – DDoS*) ώστε να μην μπορέσουν, με κανέναν τρόπο, να αντισταθούν τα συστήματα στα οποία επιτίθενται.



Σχήμα 1.2 *– Η πολυπλοκότητα των επιθέσεων σε σχέση με τις τεχνικές γνώσεις των επιτιθέμενων (Πηγή: Carnegie Melon – Software Engineering Institute)*

Τέλος, μια και πάντοτε μια εικόνα ισοδυναμεί με χίλιες λέξεις[14], στο παρακάτω διάγραμμα δίνεται μια οπτική περίληψη των διαφόρων κατηγοριών *hackers* με τα βασικά τους χαρακτηριστικά.



Σχήμα 1.3 *– Τα είδη και τα χαρακτηριστικά των hackers*

[14] Για την ακρίβεια 1387 λέξεις στη συγκεκριμένη ενότητα (!)

1.3. Οι στόχοι των hackers

Οι πρώτοι *hackers*, στα μέσα της δεκαετίας του '70, ήθελαν να βρουν τρόπους ώστε να μπορούν να κάνουν «δωρεάν»[15] τηλεφωνήματα σε ολόκληρο τον κόσμο. Στην Αμερική, και πιο συγκεκριμένα στο τηλεφωνικό δίκτυο ενός από τους μεγαλύτερους τηλεπικοινωνιακούς οργανισμούς των ΗΠΑ, αυτό ήταν δυνατό αναπαράγοντας μια συγκεκριμένη συχνότητα (την περιβόητη συχνότητα των 2600 *Hz*) κοντά στο ακουστικό του τηλεφώνου, ξεγελώντας έτσι το τηλεφωνικό κέντρο το οποίο δεν κατέγραφε και δεν χρέωνε την κλήση. Δυστυχώς, η ιστορία δεν συγκράτησε το όνομα του εμπνευστή αυτής της ιδέας, ο οποίος όμως σύντομα διέδωσε το μυστικό στο στενό του κύκλο[16]. Σύντομα, χιλιάδες άνθρωποι στις ΗΠΑ αναπαρήγαγαν (με την επίσης περιβόητη «μπλε σφυρίχτρα» η οποία εκείνη την εποχή κόστιζε μόλις 5 δολάρια) τη συγκεκριμένη συχνότητα και απολάμβαναν τη χαρά μιας εντελώς δωρεάν τηλεφωνικής συνομιλίας.

Το μυστικό ήταν πως η συγκεκριμένη συχνότητα χρησιμοποιούνταν από τους μηχανικούς του συγκεκριμένου τηλεπικοινωνιακού οργανισμού για διαγνωστικούς σκοπούς, όταν εκείνοι έκαναν εγκαταστάσεις τηλεφωνικών κέντρων. Έπρεπε, για λόγους κόστους, να μπορούν να κάνουν δωρεάν δοκιμαστικά τηλεφωνήματα σε ολόκληρη την Αμερικανική επικράτεια για να διαπιστώνουν αν η συγκεκριμένη εγκατάσταση ήταν επιτυχημένη ή όχι. Μάλιστα η τεχνική αυτή (το περιβόητο μυστικό) περιγράφονταν αναλυτικά στο βιβλίο οδηγιών (*manual*) των συγκεκριμένων τηλεφωνικών συσκευών!

Αν και σήμερα οι στόχοι των *hackers* έχουν κατά πολύ αλλάξει, τα δωρεάν τηλεφωνήματα (με τα οποία εξασφαλίζεται δωρεάν πρόσβαση στο *Internet*) παραμένουν ένας από τους βασικούς στόχους των απανταχού *hackers*.

Η πληροφορία στις μέρες μας έχει ιδιαίτερη αξία. Η πληροφορία κατά πολλούς είναι δύναμη στα χέρια του κατόχου. Καθώς όλα σχεδόν στις μέρες μας διακινούνται και ελέγχονται με ηλεκτρονικά μέσα, οι πληροφορίες αποκτούν ακόμη μεγαλύτερη αξία. Αυτή ακριβώς την αξία των πληροφοριών επιζητούν οι *hackers*, μέσω της οποίας θα μπορέσουν να αποκτήσουν περισσότερη δύναμη (και χρήματα και δόξα και πολλά άλλα). Το πώς μπορεί να γίνει αυτό είναι αρκετά απλό.

---

[15] είτε τελείως δωρεάν, είτε βρίσκοντας μια μέθοδο ώστε να πληρώνει κάποιος άλλος τα τηλεφωνικά κόστη αντί αυτών.

[16] Η τεχνική αυτή ονομάστηκε *phreaking*. Ανεπίσημα, οι *Phreakers*, παραδέχονται ως εμπνευστή αυτής της ιδέας τον *John Draper*, γνωστό επίσης με το παρατσούκλι *Captain Crunch* ο οποίος χρησιμοποιούσε μια σφυρίχτρα την οποία βρήκε μέσα στη συσκευασία γνωστής μάρκας δημητριακών!

Για παράδειγμα, πολλοί από εμάς θα πληρώναμε ένα μικρό ποσό για κωδικούς δωρεάν πρόσβασης στο *Internet* ή για κωδικούς με τους οποίους θα μπορούσαμε να κάνουμε δωρεάν τηλεφωνήματα σε ολόκληρο τον πλανήτη. Κάποιοι άλλοι, πιθανόν οι ιδιοκτήτες μιας εταιρείας, θα πλήρωναν ένα μεγαλύτερο ποσό για να έχουν στα χέρια τους τα σχέδια ενός προϊόντος που θα κατασκεύαζε μια ανταγωνιστική εταιρεία. Τέλος, μια κυβέρνηση θα πλήρωνε πολλά περισσότερα χρήματα για να αποκτήσει πληροφορίες σχετικά με τις «αμυντικές» δυνατότητες της αντιπάλου χώρας. Ο κατάλογος είναι πραγματικά ανεξάντλητος, όπως και τα είδη των πληροφοριών τα οποία διακινούνται.

Κατά κάποιον τρόπο, οι *hackers* λειτουργούν σαν *information brokers*. Πωλούν και αγοράζουν διάφορους κωδικούς, πειρατικό λογισμικό, προσωπικά στοιχεία πολιτών, πελατολόγια, μουσικά αρχεία, αρχεία βίντεο, κρατικές πληροφορίες, δημόσια έγγραφα, πορνογραφικό υλικό κτλ. Επίσης, σε πολλές περιπτώσεις, οι *hackers* είναι ωμοί εκβιαστές: καταφέρνουν και κλέβουν πολύτιμες πληροφορίες από μια επιχείρηση ή έναν οργανισμό και μετά απαιτούν τεράστια ποσά για να μην πωλήσουν τις συγκεκριμένες πληροφορίες στον άμεσο ανταγωνιστή ή να τις δημοσιοποιήσουν ελεύθερα στο *Internet*.

1.4. Μέθοδοι απόκτησης και διακίνησης πληροφοριών

Αν και στις υπόλοιπες ενότητες παρουσιάζονται αναλυτικά οι απανταχού τεχνολογικές αδυναμίες, τόσο στα τηλεπικοινωνιακά δίκτυα όσο και στα υπολογιστικά συστήματα, που η εκμετάλλευσή τους οδηγεί στη διακύβευση της ασφάλειάς τους, θα πρέπει εν συντομία να αναφέρουμε τις κλασικές και παραδοσιακές τεχνικές που χρησιμοποιούν οι απανταχού *hackers* προκειμένου να αποσπάσουν τις πολυπόθητες εκείνες πληροφορίες που επιθυμούν.

1.4.1. Passwords

Όπως τονίζεται και στο κεφάλαιο της κρυπτογραφίας, ο συνδυασμός ενός ονόματος και ενός συνθηματικού (*username and password*) είναι ο περισσότερο δημοφιλής τρόπος για να την πιστοποίηση της ταυτότητας ενός χρήστη σε ένα πληροφοριακό σύστημα.

Συνήθως οι *hackers* προσπαθούν να μαντέψουν ή να "σπάσουν" έναν κατάλληλο τέτοιο συνδυασμό ώστε να εισχωρήσουν σε ένα πληροφοριακό σύστημα. Αν και σε καμία περίπτωση δεν θέλουμε να δώσουμε αναλυτικές

οδηγίες για το πώς γίνεται αυτό, ωστόσο υπάρχουν πολλά χαρακτηριστικά που αποκαλύπτουν πολύ εύκολα το συνθηματικό μας. Οι περισσότεροι από εμάς, για να μπορέσουμε εύκολα να το θυμόμαστε, συσχετίζουμε το συνθηματικό μας με κάτι δικό μας. Τις περισσότερες φορές αυτό το «κάτι σχετικό» είναι η ημερομηνία γεννήσεώς μας, μια άλλη σημαντική ημερομηνία για εμάς, το όνομα του συντρόφου μας ή του παιδιού μας[17], ο αριθμός της πινακίδας του αυτοκινήτου μας, το όνομα του κατοικίδιου ζώου μας, το όνομα του μέρους που περάσαμε τις διακοπές μας κτλ. Το αναγνωριστικό μας όνομα (*username*), τις περισσότερες φορές, είναι ταυτόσημο με το όνομα του λογαριασμού ηλεκτρονικού ταχυδρομείου (*email address*) που χρησιμοποιούμε, κυρίως για λόγους ευκολίας και εξυπηρέτησης του διαχειριστή του συστήματος (*system administrator*). Αυτό ακριβώς εκμεταλλεύονται και οι *hackers*. Αφού μπορέσουν και βρουν ένα αναγνωριστικό όνομα δοκιμάζουν, με χρήση κατάλληλων εργαλείων, διαδοχικά *passwords* μέχρι να βρουν το κατάλληλο.

Αν ο *hacker* είναι κάποιος εσωτερικός χρήστης μπορεί να αντιγράψει ολόκληρο το αρχείο των συνθηματικών (*passwords*) σε κάποιο αποθηκευτικό μέσο. Στη συνέχεια μπορεί να το αντιγράψει στον προσωπικό του υπολογιστή στον οποίο βρίσκονται εγκατεστημένα ειδικά εργαλεία τα οποία μπορούν και δοκιμάζουν διαδοχικούς κωδικούς μέχρι πάλι να βρουν τον κατάλληλο. Για παράδειγμα, αναφέρουμε πως αυτή τη στιγμή υπάρχει, ελεύθερα διαθέσιμο στο *Internet*, πρόγραμμα το οποίο μπορεί και δοκιμάζει 2,930,000 *passwords* το δευτερόλεπτο[18]. Τα προγράμματα αυτά, στην πλειοψηφία τους, χρησιμοποιούν ένα λεξικό, τα περιεχόμενα του οποίου χρησιμοποιούν είτε λεξικογραφικά είτε με τυχαία σειρά (δηλ με αναγραμματισμούς). Επίσης, χρησιμοποιούν τελείως τυχαίους συνδυασμούς αριθμών, γραμμάτων και ειδικών συμβόλων (τεχνική *brute force*).

1.4.2. Shoulder surfing

Μια άλλη, εξίσου δημοφιλής, τεχνική υποκλοπής *passwords* είναι εκείνη του *shoulder surfing*. Πολλοί υπάλληλοι μιας εταιρείας, κυρίως όσοι δεν έχουν ιδιαίτερα καλές σχέσεις με τους υπολογιστές, συχνά καταγράφουν το συνθηματικό τους σε χαρτιά ή σε άλλα εμφανή μέρη, τα οποία μπορεί να τα δει οποιοσδήποτε έχει φυσική πρόσβαση στο συγκεκριμένο χώρο.

---

[17] Θυμηθείτε ότι στην ταινία *War Games* (1984), η ασφάλεια όλου του πλανήτη κρεμόταν από ένα *password* (*Joshua*) το οποίο ήταν το όνομα του παιδιού του επιστήμονα που κατασκεύασε την πολεμική αυτή εφαρμογή.

[18] Σε έναν *Pentium III* 700*MHz* υπολογιστή με 384*MB* μνήμης *RAM*, χρησιμοποιώντας συνδυασμό των μεθόδων *brute force* και *Xieve*.

Για παράδειγμα, έχει παρατηρηθεί πολλές φορές το φαινόμενο οι υπάλληλοι να γράφουν το προσωπικό τους συνθηματικό σε ένα κομμάτι χαρτί το οποίο κολλούν στη συνέχεια πάνω στην οθόνη τους (για να μην το ξεχάσουν). Επίσης, σε μέσα αποθήκευσης ή εφεδρικά αντίγραφα ασφάλειας (*backups*) έχουν παρατηρηθεί αυτοκόλλητες ετικέτες με το *password* που απαιτείται για να μπορέσει το εξουσιοδοτημένο προσωπικό να διαχειριστεί τα αρχεία που περιλαμβάνονται σε αυτά. Ακόμη χειρότερα, σε μηνύματα ηλεκτρονικού ταχυδρομείου, ανταλλάσσονται πολύτιμες πληροφορίες σε μη κρυπτογραφημένη μορφή αλλά ακόμη και στις περιπτώσεις που χρησιμοποιείται κρυπτογραφία ή κάποιο συνθηματικό έχει παρατηρηθεί να μεταδίδεται το κλειδί αποκρυπτογράφησης ή το απαιτούμενο *password* (σε μη κρυπτογραφημένη μορφή) στο ίδιο *email*.

Τα παραπάνω παραδείγματα ίσως φαίνονται ιδιαίτερα «τραβηγμένα από τα μαλλιά», είναι όμως πέρα για πέρα αληθή και αποτελούν έναν από τους μεγαλύτερους πονοκεφάλους των απανταχού *managers*. Δυστυχώς, η πλειονότητα των χρηστών δεν ενδιαφέρεται άμεσα για την ασφάλεια των πληροφοριών που διακινούνται μέσα από ένα πληροφοριακό σύστημα – ενδιαφέρονται περισσότερο για την ευχρηστία, την ταχύτητα και τη λειτουργικότητα μιας εφαρμογής. Είναι συνεπώς αυτονόητο, καθώς οποιοδήποτε μέτρο ασφάλειας δεν προσθέτει τίποτα στα παραπάνω αλλά αντίθετα περιορίζει τις συγκεκριμένες παραμέτρους, πως οι χρήστες θα προσπαθούν πάντοτε να το παρακάμπτουν.

Οι *hackers* λοιπόν από την άλλη πλευρά εκμεταλλεύονται αυτήν ακριβώς την τάση των χρηστών για προσωπικό τους όφελος ώστε να εκμεταλλευτούν τις ίδιες πληροφορίες με κάποιους από τους τρόπους που περιγράψαμε παραπάνω.

Προσοχή λοιπόν σε:

- αυτοκόλλητα χαρτιά σε οθόνες ή άλλα εμφανή μέρη στο γραφείο ενός υπαλλήλου[19]
- ετικέτες που περιέχουν το συνθηματικό ή την τιμή ενός κρυπτογραφικού κλειδιού και είναι κολλημένες σε αποθηκευτικά μέσα
- ετικέτες που περιέχουν το *password* συγκεκριμένων συσκευών (π.χ. *servers*, *routers*, κτλ.)

[19] Στην ίδια πάλι ταινία, *War Games*, ο ήρωας της ταινίας βρήκε ένα άλλο *password* (*pencil*) που χρειαζόταν κοιτάζοντας κάτω από το γραφείο ενός υπαλλήλου.

- ετικέτες σε καλώδια ή σε κάρτες δικτύου ή ακόμη και στα ίδια μηχανήματα που περιέχουν την IP διεύθυνση του μηχανήματος ή άλλες χρήσιμες πληροφορίες για αυτό
- χρήστες που ανταλλάσσουν *passwords* σε μη κρυπτογραφημένη μορφή μέσω *email*
- χρήστες που ανακοινώνουν οποιοδήποτε *password* δημόσια ή μέσω τηλεφώνου, *fax* κτλ.

Επίσης, οποιοδήποτε *password* δεν θα πρέπει να ανακοινώνεται ΠΟΤΕ ΚΑΙ ΣΕ ΚΑΜΙΑ ΠΕΡΙΠΤΩΣΗ, ακόμα αν και η σημασία του δεν είναι μέγιστη για την ασφάλεια ενός συστήματος. Πιθανόν να αποτελεί το πρώτο βήμα εισόδου σε ένα πληροφοριακό σύστημα ή σημάδι μιας μεγαλύτερης επίθεσης (*escalation attacks*).

1.4.3. Dustbin diving

Πολύ σημαντικό, επίσης, θέμα σε όλα τα πληροφοριακά συστήματα είναι ο τρόπος καταστροφής σημαντικών πληροφοριών και αρχείων που τηρούνται σε χειρόγραφη ή ηλεκτρονική μορφή. Για παράδειγμα, πολλές τράπεζες κρατούν αρχείο των καθημερινών συναλλαγών και κινήσεων των λογαριασμών των πελατών τους. Μετά από κάποιο χρονικό διάστημα, το αρχείο αυτό πρέπει να καταστραφεί καθώς περιέχει παλαιότερες πληροφορίες οι οποίες έχουν αλλάξει με την πάροδο του χρόνου (π.χ. το ποσό στον λογαριασμό καταθέσεων ενός πελάτη της τράπεζας), κάποια όμως από αυτά (π.χ. το όνομα, ο αριθμός καθώς και οι τελευταίες «κινήσεις» του λογαριασμού και πιθανόν και η διεύθυνση ή το τηλέφωνο ενός πελάτη) παραμένουν ακόμη ακριβή. Το αρχείο αυτό πρέπει λοιπόν να καταστραφεί με τέτοιο τρόπο ώστε να μην μπορεί κανείς να αναπαράγει τις πληροφορίες και τα δεδομένα που περιέχονται σε αυτό. Δυστυχώς, σε πολλές περιπτώσεις, η εμπειρία μάς έχει δείξει πως οι συγκεκριμένες εκτυπώσεις πετιούνται στον κάδο απορριμμάτων ακριβώς έξω από το κατάστημα!

Πολλές εταιρείες επίσης, ανά τακτά χρονικά διαστήματα, κάνουν αλλαγή του πληροφοριακού τους εξοπλισμού (π.χ. στα *desktop* συστήματά τους) και πετούν τα παλαιά σε τυχαία σημεία ή τα δωρίζουν σε φιλικά ή συγγενικά τους πρόσωπα ή τα χορηγούν σε άλλες υπηρεσίες (ή σχολεία, εκπαιδευτικά ιδρύματα κτλ.). Η συνήθης τακτική για τα δεδομένα που περιλαμβάνονται στα παλαιά συστήματα είναι να κρατούνται σε εφεδρικά αντίγραφα ασφάλειας (*backups*) ώστε να μπορούν να αναπαραχθούν (*restore*) στα καινούργια συστήματα. Μετά από αυτό συνήθως γίνεται *format* στα παλαιά συστήματα ώστε να διαγραφούν τα δεδομένα. Δυστυχώς αυτό δεν είναι αλήθεια! Ακόμη και μετά

από διαδοχικές διαδικασίες *format* είναι δυνατόν να αναπαραχθούν συγκεκριμένα ή ακόμη και όλα τα δεδομένα που υπήρχαν σε ένα σύστημα. Υπάρχουν εργαλεία λογισμικού με τα οποία είναι δυνατόν να ανακτηθούν δεδομένα που υπήρχαν σε ένα σύστημα μήνες ή ακόμη και χρόνια πριν, ακόμη και αν οι δίσκοι έχουν διαγραφεί, ξαναγραφτεί ή φορμαριστεί (*formatted*).

Ένας *hacker* λοιπόν μπορεί να αποκτήσει χρήσιμες πληροφορίες από τα σκουπίδια μας! Όσο περίεργο και αν μας φαίνεται αυτό...

Οι τρόποι αντιμετώπισης των κινδύνων αυτού του είδους είναι θέμα τόσο σωστού ελέγχου και διαχείρισης (*management*) όσο και αποτελεσματικών τεχνικών. Αναφορικά, για τα κρίσιμα δεδομένα καθώς και τα προγράμματα που είναι αποθηκευμένα σε σκληρούς δίσκους, συνήθως ακολουθείται η παρακάτω αλληλουχία ενεργειών:

- Απεγκατάσταση (*uninstall*) των εφαρμογών
- Ασφαλής διαγραφή (*secure delete*) των εφαρμογών, η οποία συχνά περιλαμβάνει κρυπτογραφικές μεθόδους
- Ασφαλής διαγραφή των δεδομένων με τις ίδιες τεχνικές
- Διαγραφή των τμημάτων (*partitions*) του σκληρού δίσκου
- Μορφοποίηση σε χαμηλό επίπεδο (*low level format*)

Τα δύο τελευταία βήματα μπορεί να χρειάζεται να επαναληφθούν περισσότερες από μία φορές.

Ανάλογες τεχνικές χρησιμοποιούνται και για μαγνητικές ταινίες (όπου υπάρχουν ακόμη) καθώς και *backup cartridges*. Για τους οπτικούς δίσκους απαιτείται η πλήρης καταστροφή τους (χάραγμα της επιφάνειας εγγραφής και τεμαχισμός σε πολλά κομμάτια). Τέλος, για τα δεδομένα που τηρούνται σε χαρτί (π.χ. εκτυπώσεις) απαιτείται πολλές φορές κάψιμο, πολτοποίηση ή τεμαχισμός τους (*shredding*) με ανάλογες συσκευές.

1.4.4. Social engineering (Κοινωνική Μηχανική)

Μια από τις πιο δημοφιλείς αλλά και ιστορικά παλαιότερες τεχνικές ανεύρεσης πληροφοριών είναι η τεχνική του *social engineering*. Θα προσπαθήσουμε από τα παρακάτω – πραγματικά - παραδείγματα να εξηγήσουμε τη συγκεκριμένη τεχνική.

Παράδειγμα 1ο:

Ένας (εσωτερικός) *hacker* χρησιμοποιεί μια τυχαία διεύθυνση ηλεκτρονικού ταχυδρομείου (χρησιμοποιώντας πολλές υπηρεσίες που προσφέρουν δωρεάν διευθύνσεις ηλεκτρονικού ταχυδρομείου – π.χ *hotmail*, *yahoo*, κτλ.) και τροποποιεί τα στοιχεία της με τέτοιο τρόπο ώστε να εμφανίζεται το ονοματεπώνυμο ενός υψηλά ιστάμενου προσώπου μέσα στην εταιρεία (π.χ. του διαχειριστή συστημάτων (*systems administrator*) ή ενός διευθυντή κτλ.). Στη συνέχεια στέλνει ένα μήνυμα σε κάποιον ανυποψίαστο χρήστη και τον παρακαλεί να «αλλάξει το *password* σε 12345». Στην οθόνη του υπαλλήλου-θύματος εμφανίζεται ένα μήνυμα ηλεκτρονικού ταχυδρομείου με τα στοιχεία του υποτιθέμενου προσώπου (π.χ. του διευθυντή) που τον παρακαλεί να προβεί σε αλλαγή του συνθηματικού του. Σε πολλές περιπτώσεις, ο χρήστης-θύμα - κυρίως λόγω φόρτου εργασίας ή υπακοής στις εντολές των ανωτέρων- αλλάζει το *password*. Στη συνέχεια, ο *hacker* χρησιμοποιεί το συγκεκριμένο *password* και συνδέεται στο σύστημα του χρήστη-θύματος αλλά και στα συστήματα στα οποία ο χρήστης-θύμα έχει δικαίωμα να συνδεθεί. Με λίγα λόγια, ο *hacker* αποκτά τα δικαιώματα χρήσης (*user privileges*) και το βαθμό εξουσιοδότησης (*user's clearance*) που έχει ο χρήστης-θύμα.

Οι πιο συνηθισμένοι στόχοι είναι οι γραμματείς, κυρίως λόγω του φόρτου εργασίας αλλά και των στοιχείων που διαχειρίζονται, καθώς και άλλο βοηθητικό προσωπικό που είναι σε γενικές γραμμές ανυποψίαστο[20].

Παράδειγμα 2ο:

Ένας (εξωτερικός) *hacker* τηλεφωνεί στο τηλεφωνικό κέντρο μιας εταιρείας και προσποιούμενος κάποιον υπάλληλο της εταιρείας ζητά από την τηλεφωνήτρια να του πει το τηλεφωνικό νούμερο του *computer room* καθώς, όπως ισχυρίζεται, έχει κάποιο πρόβλημα με το σύστημά του και χρειάζεται τη βοήθεια του διαχειριστή (*administrator*). Με τον τρόπο αυτό κατορθώνει να μάθει το νούμερο του *computer room*, καθώς και το όνομα του διαχειριστή (πιθανόν και άλλες πληροφορίες, αν η τεχνική του δουλεύει αποτελεσματικά).

Στη συνέχεια, καλεί στο *computer room* και ζητά να συνομιλήσει με το διαχειριστή. Εδώ αρχίζει το πραγματικό παιχνίδι. Αν ο διαχειριστής λείπει (που λόγω φόρτου εργασίας συνήθως λείπει από το *computer room*) και

[20] Χωρίς να υποβαθμίζουμε, με κανέναν τρόπο, τον πραγματικά πολύτιμο ρόλο των γραμματέων ή του βοηθητικού προσωπικού σε μια εταιρεία. Είναι γνωστή όμως η ρήση πως «όσα ξέρει η γραμματέας δεν τα ξέρει ο κόσμος όλος».

απαντήσει κάποιος από το βοηθητικό προσωπικό ζητά να μάθει πού είναι καθώς και το όνομα και την ιδιότητα του προσώπου με το οποίο συνομιλεί, προσποιούμενος κάποιον χρήστη ο οποίος έχει πρόβλημα με το σύστημά του. Κλείνει το τηλέφωνο και ξανακαλεί. Προσποιούμενος το διαχειριστή, ζητά από τον υπάλληλο που απάντησε στο τηλέφωνο προηγουμένως (τον οποίο μάλιστα μπορεί να καλεί και με το μικρό του όνομα) να πληκτρολογήσει κάποιες συγκεκριμένες εντολές και να αλλάξει κάποια *passwords*. Η συνέχεια αφήνεται ως άσκηση της φαντασίας του αναγνώστη...

Δυστυχώς η συγκεκριμένη τεχνική είναι από τις πιο αποδοτικές, κυρίως γιατί οι άνθρωποι θέλουν πάντοτε να βοηθούν και να φαίνονται χρήσιμοι σε θέματα που είναι μέσα ή πολλές φορές πέρα από τις αρμοδιότητές τους προκειμένου να είναι σωστοί και τυπικοί στη δουλειά τους. Επίσης, η συγκεκριμένη τεχνική είναι τελείως διάφανη καθώς δεν μπορεί να αποδειχθεί εύκολα ότι κάτι τέτοιο έγινε (οι εμπλεκόμενοι υπάλληλοι όταν καταλάβουν το λάθος τους θα προσπαθήσουν να αποφύγουν οποιαδήποτε ανάμειξη).

Τα αντίμετρα για τη συγκεκριμένη τεχνική επίθεσης, καθώς και για τους κινδύνους που ελλοχεύουν σε αυτήν, έχουν κυρίως να κάνουν με το επίπεδο επαγρύπνησης του προσωπικού σχετικά με θέματα ασφάλειας (*security awareness*) το οποίο πάντοτε χρειάζεται τη σχετική εκπαίδευση. Για παράδειγμα, όποτε ζητούνται –μέσω τηλεφώνου- στοιχεία όπως εσωτερικοί αριθμοί κλήσης ή άλλα προσωπικά στοιχεία, το προσωπικό πρέπει να ζητά τον αριθμό τηλεφώνου του προσώπου που καλεί και στη συνέχεια να καλεί εκείνος πίσω. Επίσης, όσον αφορά στα *email* που μας παρακαλούν να αλλάξουμε τον κωδικό μας ή να προβούμε σε συγκεκριμένες ρυθμίσεις, χρειάζεται να ελέγχουμε την επικεφαλίδα (*header*) του μηνύματος, ώστε να δούμε την αληθινή προέλευσή του.

1.5. Το νομικό πλαίσιο

1.5.1. Το Ευρωπαϊκό νομικό πλαίσιο

1.5.1.1. Council of Europe Recommendation R(89)9

Στις προηγούμενες ενότητες αναφερθήκαμε στην πρώτη διεθνή προσπάθεια να επιβληθεί ένα πλαίσιο νόμου ώστε να μπορεί να αντιμετωπιστεί κατάλληλα το φαινόμενο του ηλεκτρονικού εγκλήματος.

Την εποχή εκείνη, όπως προαναφέραμε, ελάχιστες χώρες στον κόσμο είχαν θεσπίσει κάποιους νόμους (ή είχαν τροποποιήσει κάποιους παλαιότερους) για να μπορέσουν να αντιμετωπίσουν το ολοένα και αυξανόμενο φαινόμενο. Οι ανησυχίες των πολιτικών εστιάζονταν κυρίως στα κυβερνητικά και στρατιωτικά συστήματα πληροφορικής αλλά σύντομα επεκτάθηκαν. Πολλά ακόμη συστήματα απειλούνταν άμεσα, με χαρακτηριστικά παραδείγματα τα συστήματα υγείας, τα συστήματα μεταφορών, τα ηλεκτρονικά συστήματα των εφοριών και των δημοσίων υπηρεσιών γενικότερα. Η ασφάλεια πληροφοριών ήταν μείζον θέμα όπως ακόμη και τα προσωπικά δεδομένα πολιτών.

Ένα άλλο μεγάλο πρόβλημα στην αντιμετώπιση του ηλεκτρονικού εγκλήματος ήταν οι δικαστές, οι οποίοι δεν είχαν την απαραίτητη εκπαίδευση πάνω στα συγκεκριμένα αδικήματα με αποτέλεσμα, πολλές φορές, οι υπαίτιοι να αθωώνονται στα δικαστήρια. Δεν θα πρέπει να ξεχνάμε πως τα συγκεκριμένα αδικήματα δεν ήταν κάτι συνηθισμένο για τους δικαστές εκείνης της εποχής, οι οποίοι δεν μπορούσαν αφενός να καταλάβουν ποιο είναι το έγκλημα και αφετέρου κάτω από ποιους νόμους μπορεί ο υπαίτιος να δικαστεί. Επίσης, ένα τεράστιο πρόβλημα για τους κατήγορους ήταν η συλλογή και η προσκόμιση στο δικαστήριο ηλεκτρονικών αποδεικτικών στοιχείων και πειστηρίων.

Για να καταλάβουμε τι σημαίνει αυτό, αρκεί να υπενθυμίσουμε πως σε ένα φόνο, για παράδειγμα, χαρακτηριστικά αποδεικτικά στοιχεία αποτελούν τα δακτυλικά αποτυπώματα στο όπλο με το οποίο έγινε το συγκεκριμένο έγκλημα. Το ποιο είναι βέβαια το όπλο του φόνου το δείχνει με τη σειρά της μια κατάλληλη (βαλλιστική) έρευνα, η οποία συγκρίνει χαρακτηριστικά του όπλου με τα πειστήρια που βρέθηκαν στον χώρο του εγκλήματος και συλλέχθηκαν από την υπηρεσία σήμανσης (*forensics*). Σε τέτοιες περιπτώσεις, η σήμανση ακολουθεί συγκεκριμένους κανόνες του ποινικού κώδικα προκειμένου να μην αλλοιώσει κανένα πειστήριο (π.χ. αν κάποιος αστυνομικός της σήμανσης πιάσει το όπλο με γυμνά χέρια πιθανόν να χαθούν τα δακτυλικά αποτυπώματα του δράστη). Ανάλογες πρακτικές και διαδικασίες δεν ήταν εύκολο να βρεθούν για τις περιπτώσεις που το έγκλημα γινόταν με (ή σε) ηλεκτρονικά μέσα.

Οι τυπικοί νόμοι αδυνατούν να αντιμετωπίσουν κατάλληλα τα αδικήματα αυτού του είδους. Για παράδειγμα, σε πολλές περιπτώσεις υπάρχει πρόβλημα στη σύνταξη εντάλματος ώστε να μπορούν οι αστυνομικές αρχές να ψάξουν και να κατασχέσουν ηλεκτρονικούς υπολογιστές. Επίσης, ανοικτό παραμένει, ακόμη και σήμερα, το θέμα των μαρτύρων υπεράσπισης ή κατηγορίας, καθώς και η υποχρέωσή τους να καταθέσουν αλλά και η αξιοπιστία της κατάθεσής τους. Συχνά, στις μέρες μας, σε δίκες που αφορούν σε τέτοιου είδους

αδικήματα καλούνται διακεκριμένοι επιστήμονες της ασφάλειας πληροφοριών ως ειδικοί μάρτυρες[21] (*expert witness*). Τέλος, παραμένει ακόμη και σήμερα ανοικτό το θέμα της δικαιοδοσίας των αρχών να παρακολουθούν τηλεφωνικές συνδιαλέξεις, μηνύματα ηλεκτρονικού ταχυδρομείου ή άλλου είδους υπολογιστικές τεχνικές με σκοπό την πρόληψη ή την καταπολέμηση του ηλεκτρονικού εγκλήματος.

Ένα άλλο μεγάλο πρόβλημα είναι η διασυνοριακή φύση του ηλεκτρονικού εγκλήματος. Σε πολλές τέτοιες περιπτώσεις, παραμένει ανοικτό το θέμα της δικαιοδοσίας των νόμων ενός κράτους[22]. Επιπροσθέτως, πρόβλημα υπάρχει και με την έκδοση ατόμων που διαπράττουν τέτοιου είδους εγκλήματα σε χώρες του εξωτερικού.

Για τους λόγους αυτούς συντάχθηκε από την Ευρωπαϊκή Επιτροπή Νομικών Ζητημάτων (*Legal Affairs Committee*) η Σύσταση *R*(89)9.

Η σύσταση αυτή προτείνει δύο μεγάλες κατηγορίες οι οποίες περιγράφουν αναλυτικά συγκεκριμένες πράξεις με σκοπό να έχουν την ίδια σημασία σε όλες τις χώρες που θα αποδέχονταν τη συγκεκριμένη σύσταση. Οι κατηγορίες αυτές είναι γνωστές σαν η ελάχιστη (*minimum*) και η προαιρετική (*optional*) λίστα.

Η ελάχιστη λίστα περιέγραφε με αρκετή λεπτομέρεια τα διάφορα αδικήματα του συγκεκριμένου είδους με σκοπό την πλήρη κατανόησή τους από τους δικαστές. Χαρακτηριστικά, αναφέρουμε τα παρακάτω παραδείγματα:

- Ως «Απάτη που σχετίζεται με υπολογιστές» ορίζεται η εισαγωγή (*input*), διαγραφή (*erasure*) ή η απόκρυψη (*suppression*) δεδομένων ή προγραμμάτων η οποία προκαλεί οικονομικές ή άλλου είδους απώλειες.
- Ως «Υπολογιστική Κλοπή» ορίζεται η διαγραφή (*erasure*), καταστροφή (*damaging*) ή η απόκρυψη (*suppression*) δεδομένων ή προγραμμάτων η οποία θα συνιστούσε κλοπή και με τον παραδοσιακή τρόπο
- Ως «Ζημιά σε Προγράμματα ή Δεδομένα» ορίζεται η διαγραφή (*erasure*), καταστροφή (*damaging*) ή η απόκρυψη (*suppression*) δεδομένων ή προγραμμάτων χωρίς πρότερη εξουσιοδότηση

[21] Συνήθως ως μάρτυρες κατηγορίας.

[22] Για παράδειγμα, με τους νόμους ποιας χώρας δικάζεται ένας Αυστραλός *hacker* ο οποίος κλέβει πληροφορίες από ένα αμερικάνικο υπολογιστικό σύστημα, χρησιμοποιώντας IP διεύθυνση η οποία αντιστοιχεί στο αγγλικό πεδίο διευθύνσεων και χρησιμοποιεί ως ενδιάμεσους σταθμούς την Ελλάδα, την Τουρκία και το Ιράκ ;

Η προαιρετική λίστα περιελάμβανε περιγραφές συγκεκριμένων αδικημάτων κυρίως για περιπτώσεις που το έγκλημα αυτής της μορφής ξεπερνά τα σύνορα μιας χώρας. Για παράδειγμα, η έκδοση ενός τέτοιου εγκληματία σε χώρες του εξωτερικού, συμφωνήθηκε με διμερείς συμφωνίες μεταξύ των χωρών που τελικά αποδέχθηκαν τη συγκεκριμένη σύσταση.

Στη λίστα αυτή, επίσης, ορίζονται έννοιες σαν την αλλοίωση (*alteration*) δεδομένων ή προγραμμάτων, την κατασκοπία με ηλεκτρονικά μέσα, τη μη εξουσιοδοτημένη χρήση ενός υπολογιστικού συστήματος καθώς και τη μη εξουσιοδοτημένη χρήση προστατευόμενου λογισμικού.

1.5.1.2. Η διεθνής σύμβαση για το ηλεκτρονικό έγκλημα (Convention on Cyber Crime)

Η δεύτερη μεγάλη προσπάθεια έγινε 12 χρόνια, περίπου μετά. Η Ευρωπαϊκή Επιτροπή Εγκλημάτων (*European Committee on Crime Problems*) ανέθεσε σε μια ομάδα ειδικών επιστημόνων και νομικών να διερευνήσει τις εξελίξεις της τεχνολογίας αλλά και τις επιπτώσεις που έχουν αυτές στην αύξηση κάθε μορφής εγκλήματος. Η συγκεκριμένη ομάδα βασίστηκε επίσης στα πορίσματα της έκθεσης του Καθηγητή *H.W. K. Kaspersen*, σύμφωνα με την οποία τα θέματα που σχετίζονται με κάθε μορφή ηλεκτρονικού εγκλήματος θα πρέπει να αντιμετωπίζονται από ένα άλλο επίσημο νομικό έγγραφο, το οποίο προβλέπει περισσότερες υποχρεώσεις από εκείνες που ορίζονται σε μια πρόταση (κάτι δηλ. σαν μια σύμβαση). Μια τέτοια σύμβαση, κατά τον *Kaspersen*, θα πρέπει να ασχολείται επίσης, πέρα από τα ουσιαστικά ποινικά ζητήματα, με τυπικές και διαδικαστικές ποινικές πράξεις καθώς και με διεθνείς ποινικές διαδικασίες και συμφωνίες.

Για να μην αναλωθούμε σε άλλες ιστορικές αναδρομές ή βιβλιογραφικές παραπομπές, η σύμβαση αυτή υπογράφτηκε από τις περισσότερες χώρες-μέλη της Ευρωπαϊκής Ένωσης, στην Βουδαπέστη, το Νοέμβριο του 2001 και είναι γνωστή σαν *Convention on Cyber Crime* 2001.

Η σύμβαση αυτή στοχεύει κυρίως στην εναρμόνιση των εθνικών νομοθεσιών σχετικά με τα ποινικά στοιχεία κατηγορίας αλλά και σχετικές προβλέψεις για πράξεις ηλεκτρονικού εγκλήματος. Επίσης, στη σύμβαση αυτή ορίζονται οι (αστυνομικές ή άλλες) Αρχές οι οποίες είναι απαραίτητες για την ποινική δίωξη των υπευθύνων ενός ηλεκτρονικού εγκλήματος κάθε μορφής αλλά και την διερεύνηση πειστηρίων και αποδεικτικών στοιχείων που διατηρούνται σε ηλεκτρονική μορφή. Τέλος, η συνθήκη αυτή ορίζει ένα

γρήγορο και αποτελεσματικό καθεστώς (*regime*) για μια διεθνή συνεργασία σε θέματα που αφορούν στο ηλεκτρονικό έγκλημα.

Η σύμβαση «*Convention on Cyber Crime* 2001» περιλαμβάνει τέσσερα (4) κεφάλαια, τα οποία είναι αντίστοιχα:

1. **Ορισμός και χρήση εννοιών**, όπου περιγράφονται αναλυτικά όλοι οι ορισμοί των όρων που χρησιμοποιούνται στη συνθήκη αυτή

2. **Μέτρα σε εθνικό επίπεδο**

Το πρώτο μέρος του 2ου κεφαλαίου (νομικά διαδικαστικά θέματα) καλύπτει τη λήψη των αναγκαίων μέτρων για τις πράξεις ηλεκτρονικού εγκλήματος. Πρωτίστως περιγράφει εννέα (9) κύριες παραβάσεις που ομαδοποιούνται σε τέσσερις (4) κύριες κατηγορίες και, κατά δεύτερο λόγο, καλύπτει τις δευτερεύουσες ευθύνες και τις αντίστοιχες κυρώσεις. Οι κύριες παραβάσεις είναι:

- Παράνομη πρόσβαση (*illegal access*)
- Παράνομη υποκλοπή (*illegal interception*)
- Παρεμβολή σε δεδομένα (*data interference*)
- Παρεμβολή σε συστήματα (*system interference*)
- Κακή χρήση συσκευών (*misuse of devices*)
- Κλοπή που σχετίζεται με υπολογιστή (*computer-related forgery*)
- Απάτη που σχετίζεται με υπολογιστή (*computer-related fraud*)
- Παιδική πορνογραφία (*child pornography*)
- Προστασία πνευματικών δικαιωμάτων ηλεκτρονικών πληροφοριών (*offences related to copyrights*)

Το δεύτερο μέρος του 2ου κεφαλαίου της σύμβασης καλύπτει παραβάσεις που δεν καλύπτονται στο 1ο μέρος, υπό την έννοια ότι περιγράφει κατηγορίες για πράξεις οι οποίες έγιναν με τη χρήση υπολογιστή. Επίσης, στην ενότητα αυτή, καλύπτονται ζητήματα που αφορούν στα αποδεικτικά στοιχεία τα οποία διατηρούνται σε ηλεκτρονική μορφή (*electronic evidence* ή απλώς *evidence*). Κατά κύριο λόγο εξετάζονται οι τρέχουσες συνθήκες αλλά και τα κατάλληλα αντίμετρα για τις ποινικές διαδικασίες που περιγράφονται στο 1ο μέρος.

Επίσης, περιγράφονται, για πρώτη φορά, οι ακόλουθες έννοιες:

- Προφύλαξη από αποστολή αποθηκευμένων δεδομένων (*expedited preservation of stored data*)
- Προφύλαξη από αποστολή και μερική αποκάλυψη αποθηκευμένων δεδομένων (*expedited preservation and partial disclosure of stored data*)
- Σειρά παρουσίασης αποδεικτικών στοιχείων (*production order*)
- Έρευνα και κατάσχεση δεδομένων ηλεκτρονικού υπολογιστή (*search and seizure of computer data*)
- Συλλογή δικτυακών δεδομένων σε πραγματικό χρόνο (*real-time collection of traffic data*)
- Υποκλοπή σημασίας και περιεχομένου δεδομένων (*interception of content data*)

Τέλος, στο δεύτερο κεφάλαιο εξετάζονται θέματα δικαιοδοσίας (*jurisdiction*).

3. Διεθνής συνεργασία

Στο κεφάλαιο αυτό περιγράφονται οι ανάγκες για τη λήψη κατάλληλων μέτρων που αφορούν στη σχέση μεταξύ εγκλημάτων που γίνονται με τον παραδοσιακό τρόπο αλλά και εκείνων που γίνονται με τη βοήθεια υπολογιστή. Αναλυτικότερα, προβλέπονται δυο τρόποι συνεργασίας:

- Χωρίς νομική βάση συνεργασίας (π.χ. συμφωνία, συμπληρωματική νομοθεσία κτλ.) μεταξύ των χωρών που εμπλέκονται.
- Με νομική βάση συνεργασίας μεταξύ των χωρών που εμπλέκονται (όπως π.χ. με τη συγκεκριμένη σύμβαση).

Επιπροσθέτως , η συγκεκριμένη ενότητα της σύμβασης αυτής, προβλέπει συγκεκριμένους τρόπους πρόσβασης των Αρχών μιας χώρας σε αποθηκευμένα δεδομένα που βρίσκονται σε κάποια άλλη (είτε με συγκατάθεση της τελευταίας είτε για εκείνα τα δεδομένα τα οποία είναι διαθέσιμα στο ευρύ κοινό). Τέλος, προβλέπεται η δημιουργία ενός Δικτύου Συνεργασίας, το οποίο θα επιτυγχάνει τη βέλτιστη δυνατή συνεργασία μεταξύ των μερών που υπογράφουν τη συγκεκριμένη σύμβασης.

4. Τελικά συμπεράσματα, τα οποία –ως επί το πλείστον- επαναλαμβάνουν τα συμπεράσματα τα οποία περιέχονται σε κάθε σύμβαση που εκδίδεται από το Ευρωπαϊκό Συμβούλιο.

1.5.2. Το Ελληνικό νομικό πλαίσιο

Στην Ελλάδα υπάρχουν αρκετοί νόμοι οι οποίοι ασχολούνται με περιπτώσεις ηλεκτρονικού εγκλήματος αλλά και με την προστασία των δεδομένων που τηρούνται σε ηλεκτρονική μορφή. Στις επόμενες υποενότητες θα παρουσιαστούν εν συντομία οι κυριότερες νομικές διατάξεις με σκοπό να παρέχουμε στον αναγνώστη μια όσο το δυνατόν ευρύτερη προσέγγιση του θέματος. Σε πολλές από αυτές αποφεύγεται –σκόπιμα- κάθε μορφή σχολιασμού ως προς τους ορισμούς που δίδονται σε αυτές ενώ συσχετίζονται άμεσα, όπου αυτό είναι δυνατό, με τεχνικά ζητήματα της ασφάλειας πληροφοριών ώστε να μπορέσει ο αναγνώστης να βγάλει τα δικά του συμπεράσματα. Επίσης, είναι πέρα από τους στόχους του συγκεκριμένου βιβλίου να εντρυφήσει περισσότερα σε νομικά ζητήματα.

1.5.2.1. Ποινικός κώδικας – Άρθρο 370Α

Κατά το Άρθρο 370Α του ποινικού κώδικα:

«Όποιος αθέμιτα παγιδεύει ή με οποιονδήποτε τρόπο παρεμβαίνει σε τηλεφωνική σύνδεση ή συσκευή με σκοπό να πληροφορηθεί ή να μαγνητοφωνήσει το περιεχόμενο τηλεφωνικής συνδιάλεξης μεταξύ τρίτων, τιμωρείται με φυλάκιση. Η χρησιμοποίηση από το δράστη των πληροφοριών ή μαγνητοταινιών, που αποκτήθηκαν με αυτόν τον τρόπο, θεωρείται επιβαρυντική περίπτωση[23]*»* (Άρθρο 370Α, παράγραφος 1).

Χαρακτηριστικές περιπτώσεις εφαρμογής της παραγράφου 1 του συγκεκριμένου άρθρου είναι η εγκατάσταση ενός κατάλληλου προγράμματος ή μιας συσκευής η οποία μπορεί να καταγράφει τηλεφωνικές συνδιαλέξεις.

Ας δώσουμε όμως ένα παράδειγμα το οποίο -ίσως- εξηγήσει καλύτερα μια τέτοια πιθανή περίπτωση.

Συνήθως, στο ισόγειο των πολυκατοικιών υπάρχουν (ξύλινες) ντουλάπες οι οποίες περιέχουν τον λεγόμενο «κατανεμητή του ΟΤΕ». Εκεί καταλήγουν οι τηλεφωνικές γραμμές από το πλησιέστερο κέντρο του οργανισμού στους συνδρομητές της συγκεκριμένης πολυκατοικίας. Στους κατανεμητές αυτούς, κυρίως για λόγους διαχείρισης των δεκάδων κυκλωμάτων, υπάρχουν τοποθετημένες ετικέτες οι οποίες αναγράφουν τον αριθμό του τηλεφώνου του

[23] όπως αποτυπώνεται στις παραγράφους 4 και 5 από το άρθρο 33, παράγραφο 7 του νόμου 2172/1993 (ΦΕΚ Α' 207) οι οποίες αντικατέστησαν και συμπλήρωσαν το συγκεκριμένο άρθρο.

αντίστοιχου συνδρομητή[24]. Κάποιος «περίεργος» λοιπόν μπορεί εύκολα να τοποθετήσει τα δικά του καλώδια[25], καθώς και μια αντίστοιχη συσκευή που μπορεί να καταγράφει τηλεφωνικές συνδιαλέξεις (τίποτα περισσότερο από ένα απλό δημοσιογραφικό κασετόφωνο) για όσο χρονικό διάστημα θέλει ή του επιτρέπεται λόγω των συνθηκών.

Σε πιο εξελιγμένες επιθέσεις χρησιμοποιούνται μικροσκοπικοί «κοριοί» οι οποίοι παγιδεύουν την τηλεφωνική συσκευή του θύματος. Η συγκεκριμένη τεχνολογία μάλιστα επιτρέπει σε ένα τέτοιο εξάρτημα να μεταδίδει πληροφορίες με ασύρματο τρόπο (!) σε μια συγκεκριμένη συχνότητα, ενώ μπορεί να λειτουργήσει αρκετούς μήνες προτού εξαντληθεί η ισχύς της μπαταρίας του.

Βέβαια, καθώς πάρα πολλοί χρήστες του *Internet* χρησιμοποιούν ως μέσο σύνδεσης το τηλεφωνικό δίκτυο, το άρθρο αυτό μπορεί επίσης να εφαρμοστεί σε περιπτώσεις όπου ένας δράστης χρησιμοποιεί ένα κατάλληλο πρόγραμμα (*sniffer*) και καταγράφει όλη τη δικτυακή κίνηση που εισέρχεται ή εξέρχεται προς/από ένα δίκτυο υπολογιστών.

Τέλος, παρεμβολή σε μια τέτοια σύνδεση μπορεί, επίσης, να γίνει και με τη χρήση προγραμμάτων *Trojan Horse* που -με κάποιον από τους πολλούς πιθανούς τρόπους- έχει εγκατασταθεί στον ηλεκτρονικό υπολογιστή ενός χρήστη από το δράστη. Πολλά από τα προγράμματα αυτά μπορούν να καταγράφουν συγκεκριμένες πληροφορίες (π.χ. αριθμούς πιστωτικών καρτών, *passwords* κτλ.) και να τις μεταδίδουν (πολλές φορές και κρυπτογραφημένα) στο δράστη. Ο τρόπος λειτουργίας των προγραμμάτων αυτών καθώς και τεχνικές προστασίας από αυτά εξετάζονται σε επόμενες ενότητες.

Τέλος, το άρθρο 370Α του ποινικού κώδικα σχετίζεται, μεταξύ άλλων, με:

- Το άρθρο 19 του Συντάγματος της Ελλάδας
- Το άρθρο 250 του Ποινικού Κώδικα («Παραβάσεις των Τηλεφωνικών Υπαλλήλων»)

---

[24] Στις περισσότερες των περιπτώσεων, πάντως, υπάρχουν αναγεγραμμένοι κάποιοι κωδικοί αριθμοί. Βέβαια, έχουν αναφερθεί περιπτώσεις όπου οι δράστες καλούν το τεχνικό τμήμα του ΟΤΕ (προσποιούμενοι πως είναι και εκείνοι τεχνικοί και θέλουν να επιλύσουν μια βλάβη) ζητώντας να μάθουν σε ποιο τηλεφωνικό νούμερο αντιστοιχούν οι κωδικοί αυτοί (χαρακτηριστικό παράδειγμα της τεχνικής *social engineering*)

[25] Τα καλώδια αυτά είναι γνωστά και ως «ραζίμι» στην «αργκό» των τεχνικών και μπορούν να τοποθετηθούν πάνω στο αντίστοιχο ζεύγος καλωδίων με τη χρήση ενός κατάλληλου εξαρτήματος («καρφωτικό *KRONE*»), το οποίο έχει κόστος μερικών μόνον ευρώ!

- Το άρθρο 25 ,παράγραφος 2, του νόμου 2075/1992 («Οργάνωση και λειτουργία του τομέα των τηλεπικοινωνιών»)
- Το άρθρο 33, παράγραφος 8, του νόμου 2172/1993 («Τροποποίηση και αντικατάσταση διατάξεων κλπ.»).
- Τα άρθρα 3,4 καθώς και το άρθρο 5 παράγραφοι 10-11 του νόμου («Για την προστασία της ελευθερίας, ανταπόκρισης και επικοινωνίας κ.ά. δ/ξεις»)
- Ποινικός κώδικας – Άρθρο 370Β
- Το άρθρο 370Β του ποινικού κώδικα εξετάζει περιπτώσεις μη εξουσιοδοτημένης πρόσβασης σε απόρρητα δεδομένα ηλεκτρονικών υπολογιστών. Αναλυτικότερα:

«Όποιος αθέμιτα αντιγράφει, αποτυπώνει, χρησιμοποιεί, αποκαλύπτει σε τρίτο ή οπωσδήποτε παραβιάζει στοιχεία ή προγράμματα υπολογιστών, τα οποία συνιστούν κρατικά, επιστημονικά ή επαγγελματικά απόρρητα ή απόρρητα επιχείρησης του δημόσιου ή ιδιωτικού τομέα, τιμωρείται με φυλάκιση τουλάχιστο τριών μηνών. Ως απόρρητα θεωρούνται και 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.

Αν ο δράστης είναι στην υπηρεσία του κατόχου των στοιχείων καθώς και αν το απόρρητο είναι ιδιαίτερα μεγάλης οικονομικής σημασίας, επιβάλλεται φυλάκιση τουλάχιστο ενός έτους.

Αν πρόκειται για στρατιωτικό ή διπλωματικό απόρρητο ή για απόρρητο που αναφέρεται στην ασφάλεια του κράτους, η κατά την παράγραφο 1 πράξη τιμωρείται κατά τα άρθρα 146 και 147.» (Άρθρο 370Β, παράγραφοι 1,2,3)

Το άρθρο αυτό είναι ιδιαίτερα σημαντικό[26], καθώς περικλείει ποινές για μια πλειάδα εγκληματικών πράξεων όπως, μη εξουσιοδοτημένη πρόσβαση σε συστήματα υπολογιστών, μη εξουσιοδοτημένη αντιγραφή απόρρητων δεδομένων, μη εξουσιοδοτημένη διακίνηση απόρρητων δεδομένων κτλ.

Επίσης, το άρθρο 370Β του ποινικού κώδικα σχετίζεται, μεταξύ άλλων, με:

- Το άρθρο 2, παράγραφος 4, εδάφιο Β του νόμου 1599/1986 («Σχέσεις κράτους-πολίτη, καθιέρωση νέου δελτίου ταυτότητας κ.ά. διατάξεις»)
- Το άρθρο 16 του νόμου 146/1914 («Περί αθέμιτου ανταγωνισμού»)

[26] Το άρθρο 370Β προστέθηκε με το άρθρο 3 του νόμου 1805/1988

- Το άρθρο 35, παράγραφος 1, του νόμου 2172/1993 («Για την προστασία της κοινωνίας από το οργανωμένο έγκλημα»)
- Το νόμο 2068/1992 «Κύρωση της Ευρωπαϊκής Σύμβασης για την προστασία του ατόμου από την αυτοματοποιημένη επεξεργασία πληροφοριών προσωπικού χαρακτήρα»)
- Άρθρο 18, παράγραφος 4 και άρθρο 22, παράγραφοι 1-8, του νόμου 2472/1997 («προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα»)

1.5.2.2. Ποινικός κώδικας – Άρθρο 370Γ

Ανάλογες περιπτώσεις εξετάζονται και στο Άρθρο 370Γ, στο οποίο καλύπτονται και θέματα παράνομης αντιγραφής και διακίνησης προστατευόμενου λογισμικού (*software*). Αναλυτικότερα:

«Όποιος χωρίς δικαίωμα αντιγράφει ή χρησιμοποιεί προγράμματα υπολογιστών, τιμωρείται με φυλάκιση μέχρι έξι μηνών και με χρηματική ποινή εκατό χιλιάδες έως δυο εκατομμυρίων δραχμών[27].

Όποιος αποκτά πρόσβαση σε στοιχεία που έχουν εισαχθεί σε υπολογιστή ή σε περιφερειακή μνήμη υπολογιστή ή μεταδίδονται με συστήματα τηλεπικοινωνιών, εφ' όσον οι πράξεις αυτές έγιναν χωρίς δικαίωμα, ιδίως με παραβίαση απαγορεύσεων ή μέτρων ασφάλειας που είχε λάβει ο νόμιμος κάτοχός τους, τιμωρείται με φυλάκιση μέχρι τριών μηνών ή με χρηματική ποινή τουλάχιστο δέκα χιλιάδων δραχμών[28]. Αν η πράξη αναφέρεται στις διεθνείς σχέσεις ή στην ασφάλεια του κράτους, τιμωρείται κατά το άρθρο 148.

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 αρμόδιου υπαλλήλου του.» (Άρθρο 370Γ, παράγραφοι 1,2,3)

Τονίζεται πως, σύμφωνα με το νόμο αυτό δεν χρειάζεται να έχουν χαρακτηριστεί ως «απόρρητα» τα δεδομένα (στοιχεία) που τηρούνται στην κύρια (*RAM*) ή την περιφερειακή μνήμη (σκληροί δίσκοι, δισκέτες, οπτικοί δίσκοι κτλ.) ενός υπολογιστή.

---

[27] €293,47 - €5869,41αντίστοιχα (για να συμβαδίζουμε με την νέα τάξη πραγμάτων, τουλάχιστο σε ό,τι αφορά στη νέα νομισματική μονάδα)
[28] €29,35

Επίσης, αξίζει να τονίσουμε τη σημασία της παραγράφου 3 για την ύπαρξη κατάλληλων εταιρικών πολιτικών ασφάλειας (*corporate security policy*). Αν και είναι μάλλον απίθανο να περιγράψουμε το τι ακριβώς είναι μια τέτοια πολιτική σε λίγες γραμμές, για τους σκοπούς της συγκεκριμένης ενότητας, ωστόσο εν συντομία, ο αναγνώστης θα πρέπει να σκέφτεται μια εταιρική πολιτική ασφάλειας σαν «ένα έγγραφο το οποίο περιγράφει αναλυτικά ποιος δικαιούται πρόσβαση, τι τύπου πρόσβαση, σε τι τύπου δεδομένα και πιθανόν πότε, για πόσο καθώς και για ποιο λόγο[29]». Το έγγραφο αυτό είναι υψίστης σημασίας για μια επιχείρηση η οποία διατηρεί αυτοματοποιημένα συστήματα επεξεργασίας δεδομένων.

Η πολιτική ασφάλειας, όπως θα τονιστεί κατ' επανάληψη στις επόμενες ενότητες, αποτελεί το Α και το Ω των αντίστοιχων μέτρων προστασίας από τους κινδύνους που αντιμετωπίζουν τα πληροφοριακά αγαθά μιας εταιρείας. Επίσης, σε ένα τέτοιο έγγραφο περιγράφονται και οι κατάλληλοι μηχανισμοί ασφάλειας (*security mechanisms*) οι οποίοι ακολουθούνται (ή πρέπει να ακολουθούνται) για να επιτευχθεί αυτός ο στόχος.

Η σύνταξη κατάλληλων πολιτικών ασφάλειας είναι μια ιδιαίτερα επίπονη δουλειά, καθώς χρειάζεται πρωτίστως να αποτιμηθούν σωστά τα πληροφοριακά αγαθά μιας εταιρείας ή ενός οργανισμού (μέσω μιας διαδικασίας που ονομάζεται *risk analysis*), να συσχετισθούν τα αγαθά αυτά με τους πιθανούς κινδύνους που αντιμετωπίζουν (μέσω διαδικασιών που ονομάζονται *risk assessment*) καθώς και να προταθούν -και να ακολουθηθούν με ευλάβεια- συγκεκριμένοι μηχανισμοί-αντίμετρα με τα οποία πρέπει να προστατεύονται αυτά (*countermeasures*) όσο και οι πιθανές τους αδυναμίες (μέσω μιας αντίστοιχης διαδικασίας που ονομάζεται *vulnerability assessment*). Η σύνταξη μιας σωστής πολιτικής ασφάλειας απαιτεί κατάλληλες γνώσεις για την εσωτερική δομή του οργανισμού ή της εταιρείας και γίνεται πάντοτε με στενή συνεργασία μεταξύ κατάλληλα ειδικευμένων αναλυτών και συμβούλων ασφάλειας πληροφορικής με στελέχη του οργανισμού.

Επίσης, μια πολιτική ασφάλειας είναι δυναμική και γι' αυτό το λόγο θα πρέπει να εξετάζεται και να αναθεωρείται τακτικά για να μπορεί να αντιμετωπίζει τις όποιες εξελίξεις. Τέλος, μια τέτοια πολιτική αποτελεί θεμέλιο για όποια εταιρεία ή οργανισμό σέβεται τον εαυτό της (όσον αφορά στη χρήση πληροφορικής και δικτύων). Η σύνταξη σωστών πολιτικών ασφάλειας εξετάζεται αναλυτικά σε επόμενη ενότητα του συγκεκριμένου βιβλίου.

---

[29] κάτι δηλαδή σαν έναν εσωτερικό κανονισμό

Το παραπάνω άρθρο προστέθηκε, όπως και το άρθρο 370Β, με το άρθρο 4 του νόμου 1805/1988.

Τέλος, το άρθρο 370Γ του ποινικού κώδικα σχετίζεται, μεταξύ άλλων, με:

- Το άρθρο 16, του νόμου 146/1914 («Περί αθέμιτου ανταγωνισμού»)
- Το άρθρο 30, του νόμου 1806/1988 («Τροποποίηση νομοθεσίας για τα Χρηματιστήρια κ.ά. διατάξεις»)
- Το άρθρο 35, παράγραφος 1, του νόμου 2172/1993 (ο οποίος αντικατέστησε το άρθρο 12 του νόμου 1916/1990 «Για την προστασία της κοινωνίας από το οργανωμένο έγκλημα»)
- Το νόμο 2068/1992 («Κύρωση της Ευρωπαϊκής Σύμβασης για την προστασία του ατόμου από την αυτοματοποιημένη επεξεργασία πληροφοριών προσωπικού χαρακτήρα»)
- Το άρθρο 18, παράγραφος 4 καθώς και το άρθρο 22, παράγραφοι 1-8, του νόμου 2472/1998 («Για την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα»)

1.5.2.3. Νόμος 2672/1998, Άρθρο 14 (Διακίνηση εγγράφων με ηλεκτρονικά μέσα)

Σύμφωνα με το παραπάνω άρθρο:

«Επιτρέπεται η διακίνηση εγγράφων μεταξύ των υπηρεσιών του Δημοσίου, των Ν.Π.Δ.Δ. και των οργανισμών τοπικής αυτοδιοίκησης ή μεταξύ αυτών και των ενδιαφερομένων φυσικών προσώπων με τηλεμοιοτυπία και ηλεκτρονικό ταχυδρομείο.

Για την εφαρμογή του παρόντος άρθρου ορίζονται:

- *Ως τηλεμοιοτυπία, η πιστή αναπαραγωγή από απόσταση εγγράφων με βοήθεια κατάλληλων τερματικών συσκευών*
- *Ως τηλεμοιότυπο, το λαμβανόμενο αντίγραφο στην τερματική συσκευή λήψης*
- *Ως ηλεκτρονικό ταχυδρομείο, το σύστημα αποστολής και λήψης μηνυμάτων μέσω δικτύου, από και προς την ηλεκτρονική διεύθυνση των χρηστών*
- *Ως μήνυμα ηλεκτρονικού ταχυδρομείου, η πληροφορία, το κείμενο ή αρχείο δεδομένων ή άλλο έγγραφο που μεταδίδεται με σύστημα ηλεκτρονικού ταχυδρομείου.*

- *Ως ψηφιακή υπογραφή, η ψηφιακής μορφής υπογραφή σε δεδομένα ή συνημμένη σε δεδομένα ή λογικά συσχετιζόμενη με αυτά, που χρησιμοποιείται από τον υπογράφοντα ως ένδειξη αποδοχής του περιεχομένου αυτών, εφόσον η εν λόγω υπογραφή:*
    - *συνδέεται μονοσήμαντα με τον υπογράφοντα*
    - *ταυτοποιεί τον υπογράφοντα»*

Ο συγκεκριμένος νόμος ίσως, εκ πρώτης όψεως, δεν σχετίζεται άμεσα με το ηλεκτρονικό έγκλημα – θα λέγαμε όμως πως είναι ιδιαίτερα σημαντικός για τις ενότητες που θα ακολουθήσουν και ιδιαίτερα για την ενότητα της κρυπτογραφίας καθώς νομιμοποιεί τη χρήση ψηφιακών υπογραφών για τη διακίνηση ηλεκτρονικών πληροφοριών και δεδομένων μέσω μηνυμάτων ηλεκτρονικού ταχυδρομείου (*email*).

Η χρήση των ψηφιακών υπογραφών για συναλλαγές που γίνονται με ηλεκτρονικά μέσα αποτελεί ουσιαστικά ένα συμβολαιογραφικό ισοδύναμο της φυσικής μας υπογραφής στον ηλεκτρονικό κόσμο. Σίγουρα όλοι μας διαισθητικά μπορούμε να καταλάβουμε τις συνέπειες που υπάρχουν από την παράνομη πλαστογράφηση της υπογραφής μας. Κάτι αντίστοιχο, σε μεγαλύτερη έκταση ίσως, μπορεί να γίνει και με την «πλαστογράφηση» της ψηφιακής μας υπογραφής. Πιστεύουμε πως ο αναγνώστης θα μπορεί να καταλάβει πλήρως το πρόβλημα που δημιουργείται μόλις διαβάσει και κατανοήσει τις βασικές αρχές της κρυπτογραφίας στην αντίστοιχη ενότητα.

1.5.2.4. Νόμος 2472/1997, (Προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα)

Ο νόμος 2472/1997 αποτελεί μια από τις πιο σοβαρές προσπάθειες των Ελλήνων νομικών για την προστασία του απλού πολίτη από την επεξεργασία δεδομένων προσωπικού χαρακτήρα. Σύμφωνα με το νόμο αυτό, ως δεδομένα προσωπικού χαρακτήρα ορίζονται «κάθε πληροφορία που αναφέρεται στο υποκείμενο των δεδομένων».

Η δομή του συγκεκριμένου νόμου έχει ως εξής:

Στο Κεφάλαιο Α’, με τίτλο «Γενικές Διατάξεις», περιλαμβάνονται γενικές πληροφορίες περί του νόμου, δηλ. Αντικείμενο, Ορισμοί και Πεδίο Εφαρμογής (στα άρθρα 1,2 και 3 αντίστοιχα).

Στο Κεφάλαιο Β', με τίτλο «Επεξεργασία Δεδομένων Προσωπικού Χαρακτήρα» περιλαμβάνονται τα άρθρα 4-10, στα οποία περιγράφονται οι εξής έννοιες

Άρθρο 4 – Χαρακτηριστικά δεδομένων προσωπικού χαρακτήρα
Άρθρο 5 – Προϋποθέσεις Επεξεργασίας
Άρθρο 6 – Γνωστοποίηση αρχείων
Άρθρο 7 – Επεξεργασία ευαίσθητων δεδομένων
Άρθρο 7α – Απαλλαγή υποχρέωσης γνωστοποίησης και λήψης άδειας
Άρθρο 8 – Διασύνδεση Αρχείων
Άρθρο 9 – Διασυνοριακή ροή δεδομένων προσωπικού χαρακτήρα
Άρθρο 10 – Απόρρητο και ασφάλεια της επεξεργασίας

Στο Κεφάλαιο Γ, με τίτλο «Δικαιώματα του υποκειμένου των δεδομένων», περιγράφονται τα δικαιώματα που έχει στα δεδομένα ο κάτοχός τους. Αναλυτικότερα:

Άρθρο 11 – Δικαίωμα ενημέρωσης
Άρθρο 12 – Δικαίωμα πρόσβασης
Άρθρο 13 – Δικαίωμα αντίρρησης
Άρθρο 14 – Δικαίωμα προσωρινής δικαστικής προστασίας

Τέλος, τα κεφάλαια Δ', Ε' και ΣΤ, «Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα», «Κυρώσεις» και «Τελικές Μεταβατικές Διατάξεις» αντίστοιχα, πραγματεύονται κυρίως με διαδικαστικά θέματα για την πληρότητα του συγκεκριμένου νόμου.

1.6. Computer Forensics

1.6.1. Ηλεκτρονικά αποδεικτικά στοιχεία και πειστήρια (electronic evidence)

Όπως αναφέραμε στα προηγούμενα, ένα από τα μεγαλύτερα προβλήματα που αντιμετωπίζουν οι νομικοί -αλλά και οι δικαστές που ασχολούνται με πράξεις ηλεκτρονικού εγκλήματος- είναι η συλλογή κατάλληλων πειστηρίων και αποδεικτικών στοιχείων από υπολογιστικά συστήματα, ώστε αυτά να μπορούν να στηρίξουν κατάλληλα μια τέτοια υπόθεση. Επίσης, τα στοιχεία αυτά πρέπει να είναι ακριβώς εκείνα που συλλέχθηκαν κατά τη διάρκεια μιας έρευνας και δεν πρέπει σε καμία περίπτωση να έχουν τροποποιηθεί.

Ο κλάδος της ασφάλειας πληροφοριών που ασχολείται με τα συγκεκριμένα ζητήματα ονομάζεται *computer forensics*. Τα *computer forensics* είναι οι διαδικασίες εφαρμογής επιστημονικών και αναλυτικών τεχνικών σε λειτουργικά συστήματα υπολογιστών καθώς και στις αντίστοιχες δομές αρχείων (*file structures*) για την ανεύρεση ηλεκτρονικών αποδείξεων (*electronic evidence*). Με τον όρο «ηλεκτρονική απόδειξη» θα εννοούμε οποιαδήποτε πειστήρια και αποδεικτικά στοιχεία που τηρούνται σε ηλεκτρονική μορφή μέσα σε ένα υπολογιστικό σύστημα. Τα στοιχεία αυτά είναι απαραίτητα για να υποστηρίξουν κάποιον ισχυρισμό σε μια πιθανή δίκη.

Μια τέτοια ανάλυση (*computer forensics analysis*) μπορεί να ζητηθεί από τις αστυνομικές –ή τις δικαστικές- αρχές (καθώς μπορεί να το επιβάλλει η σχετική νομοθεσία), από ασφαλιστικές εταιρείες οι οποίες προασπίζονται τα συμφέροντα ιδιωτών ή εταιρειών που πιθανόν να εμπλέκονται σε ένα ηλεκτρονικό έγκλημα, καθώς και από απλούς ιδιώτες[30].

Οι λόγοι που συνήθως επιβάλλουν μια τέτοιου είδους ανάλυση εστιάζουν κυρίως στο να βρουν τον υπαίτιο (ή τους υπαίτιους) ενός ηλεκτρονικού εγκλήματος αλλά και στο να ανακαλύψουν τη μέθοδο που χρησιμοποίησε αυτός προκειμένου να αποκτήσει πρόσβαση στο συγκεκριμένο σύστημα. Επίσης, μια τέτοια ανάλυση μπορεί να δώσει μιαν αποτίμηση της ζημιάς που έχει προξενήσει. Τέλος, η συγκεκριμένη ανάλυση, αν γίνει σωστά, μπορεί να παρέχει τα αποδεικτικά στοιχεία που πιθανόν να χρειαστούν σε μια δίκη.

Στην ενότητα αυτή θα εστιάσουμε περισσότερο στην τεχνική πλευρά του θέματος παρά στη νομική του. Δεν θα πρέπει να ξεχνάμε, όμως, την τεράστια σημασία των νομικών διατάξεων για τη συλλογή ηλεκτρονικών πειστηρίων και αποδεικτικών στοιχείων, καθώς οποιαδήποτε παρέκκλιση από αυτές θα μπορούσε να καταστήσει την όλη διαδικασία άχρηστη. Οποιαδήποτε ενέργεια που σχετίζεται με τη συλλογή τέτοιων δεδομένων, αλλά και την εξαγωγή ανάλογων συμπερασμάτων, πρέπει να γίνεται αλλά και να τεκμηριώνεται με τέτοιο τρόπο ώστε να μην μπορεί από κανέναν, αλλά και με κανένα μέσο, να αμφισβητηθεί η ακεραιότητα της όλης διαδικασίας.

1.6.2. Η επιστήμη των computer forensics

Πολλοί από εμάς είμαστε λάτρεις των αστυνομικών ταινιών. Σε πολλές από αυτές, έχουμε παρατηρήσει πως στον τόπο ενός εγκλήματος φθάνουν

[30] αν και κάτι τέτοιο σπανίζει (για να είμαστε ειλικρινείς).

άμεσα διάφοροι υπεύθυνοι αστυνομικοί, ντέτεκτιβς καθώς και η Σήμανση (*forensics*), η οποία είναι υπεύθυνη για τη διερεύνηση και τη συλλογή πιθανών αποδεικτικών στοιχείων. Τα στοιχεία αυτά συλλέγονται με συγκεκριμένες διαδικασίες και προφυλάσσονται από κάθε ακούσια ή εσκεμμένη αλλοίωση. Επίσης, τοποθετούνται αμέσως ειδικές ταινίες που απαγορεύουν την πρόσβαση σε μη εξουσιοδοτημένα άτομα στο χώρο στον οποίο έγινε το έγκλημα αλλά και όλη η περιοχή φωτογραφίζεται λεπτομερώς. Τέλος, τα αποδεικτικά στοιχεία παραδίδονται στους υπεύθυνους ειδικούς (με συγκεκριμένες πάλι διαδικασίες) οι οποίοι θα προχωρήσουν σε σχετικές έρευνες προκειμένου να βρουν τον ή τους υπαίτιους.

Κάτι αντίστοιχο εφαρμόζεται και στις περιπτώσεις που το έγκλημα γίνεται με ηλεκτρονικό τρόπο. Βασιζόμενοι στη σχετική βιβλιογραφία, η επιστήμη αυτή ονομάζεται *computer forensics* και εστιάζει στη συλλογή αποδεικτικών στοιχείων που τηρούνται σε ηλεκτρονική μορφή από έναν ηλεκτρονικό υπολογιστή, η ανάλυση των οποίων μπορεί να παρέχει πληροφορίες για τον (ή τους) υπαίτιους καθώς και για την τεχνική την οποία ακολούθησαν.

Πριν το 1990 η επιστήμη των *computer forensics* ήταν σχεδόν ανύπαρκτη, κυρίως λόγω της έλλειψης κατάλληλων εργαλείων υλικού (*hardware*) και λογισμικού (*software*). Από τα μέσα περίπου εκείνης της χρονιάς άρχισαν να εμφανίζονται τα πρώτα προγράμματα τα οποία μπορούσαν να αντιγράψουν *bit*-προς-*bit* το σκληρό δίσκο ενός υπολογιστή. Τα προγράμματα αυτά εκτελούν διεργασίες «κλωνοποίησης» των περιεχομένων ενός σκληρού δίσκου και είναι γνωστά σαν *disk image*, *disk cloning* ή *bistream image software*.

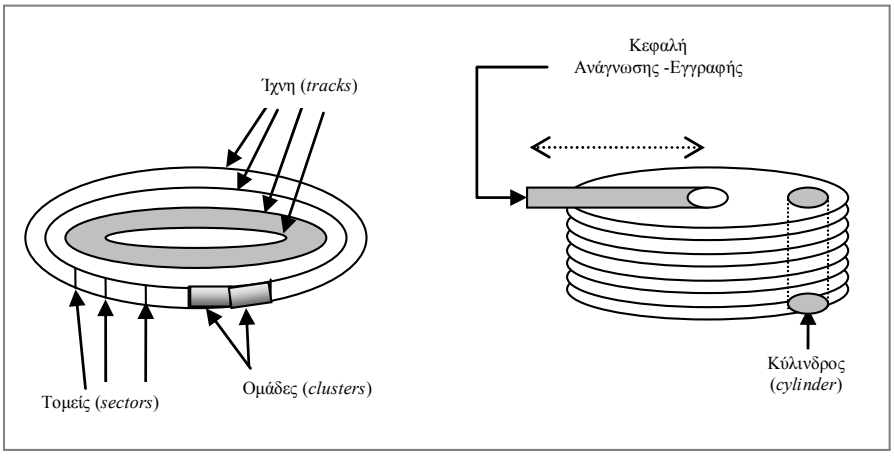
Τα εργαλεία αυτά βοηθούν στο να μπορούμε να έχουμε ένα ακριβές αντίγραφο (κλώνο) του σκληρού δίσκου του συστήματος για το οποίο θέλουμε να διεξάγουμε μια τέτοια ανάλυση. Για παράδειγμα, όταν έχει περιέλθει στην κατοχή των αστυνομικών αρχών (ή άλλων υπευθύνων) το υπολογιστικό σύστημα ενός ατόμου που είναι ύποπτο πως έχει προβεί σε πράξεις που οδήγησαν σε κάποιο ηλεκτρονικό έγκλημα, η αυτοψία αυτού του συστήματος μπορεί να οδηγήσει στην εξαγωγή χρήσιμων συμπερασμάτων. Ο σκληρός δίσκος ενός υπολογιστή είναι το μέρος στο οποίο αποθηκεύεται κάθε σχεδόν ενέργεια που κάνει ο χρήστης του και αποτελεί μια έξοχη πηγή για ανεύρεση ηλεκτρονικών πειστηρίων και αποδεικτικών στοιχείων. Επίσης, άλλη συνηθισμένη περίπτωση είναι να εξετάζεται ο σκληρός δίσκος ενός υπολογιστή ο οποίος έχει πέσει θύμα των *hackers*.

1.6.3. Πού βρίσκονται οι (ηλεκτρονικές) αποδείξεις

Χρειάζεται να τονίσουμε πως πάντοτε, σε τέτοιες περιπτώσεις, εξετάζεται το αντίγραφο του σκληρού δίσκου και ποτέ ο σκληρός δίσκος αυτός καθαυτός. Τα δεδομένα τα οποία περιέχονται στον σκληρό δίσκο ενός -προς έρευνα- υπολογιστή δεν θα πρέπει σε καμία περίπτωση να αλλοιωθούν, καθώς είναι πιθανόν είτε να καταστραφούν τα όποια αποδεικτικά στοιχεία περιέχονται, είτε να κατηγορηθούν τα άτομα τα οποία διεξάγουν την έρευνα για εσκεμμένη αλλοίωση των περιεχομένων του. Τέλος, σε οποιαδήποτε περίπτωση χρειάζεται να ακολουθούνται πάντοτε οι σχετικές νομικές διατάξεις.

Για να καταλάβουμε καλύτερα πού μπορούν να βρεθούν πειστήρια και αποδεικτικά στοιχεία που τηρούνται σε ηλεκτρονική μορφή, χρειάζεται να κάνουμε, εν συντομία, μια περιγραφή του σκληρού δίσκου ενός υπολογιστή.

Ένας σκληρός δίσκος αποθηκεύει δεδομένα σε λογικά αρχεία τα οποία με τη σειρά τους αποθηκεύονται, στο φυσικό μέσο, οργανωμένα κατά ομάδες (*clusters*), ίχνη (*tracks*), τομείς (*sectors*) και κυλίνδρους (*cylinders*) όπως φαίνεται και στο σχήμα 1.4.



***Σχήμα 1.4** – Η αρχιτεκτονική ενός σκληρού δίσκου*

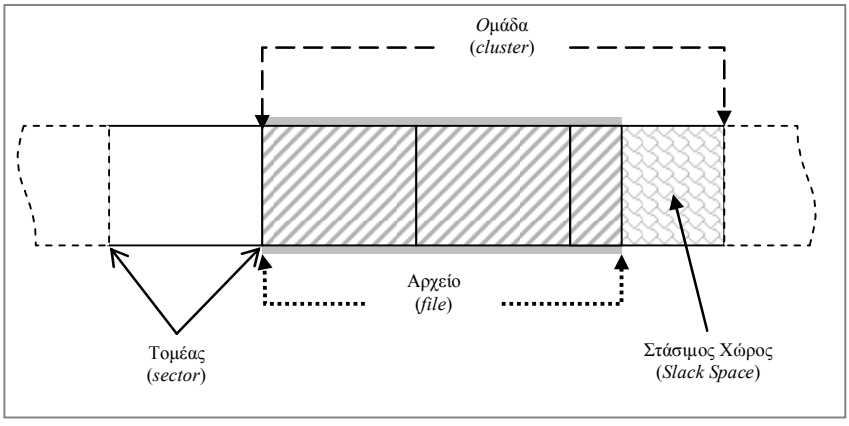
Τα λογικά αρχεία που βρίσκονται αποθηκευμένα σε ένα σκληρό δίσκο δεν εξαφανίζονται «μια για πάντα» (ευτυχώς ή δυστυχώς, ανάλογα με την περίπτωση) όταν διαγράφονται. Αντίθετα, παραμένουν στο φυσικό μέσο

(σκληρό δίσκο) μέχρις ότου η συγκεκριμένη περιοχή επανεγγραφεί ή ο σκληρός δίσκος μορφοποιηθεί ξανά (*formatted*)[31].

Ο σκληρός δίσκος, σε λογικό επίπεδο, περιέχει αρχεία, στάσιμο χώρο (*slack space*), κενό χώρο (*free space*) και, ανάλογα με το λειτουργικό σύστημα που χρησιμοποιείται (π.χ. την οικογένεια λειτουργικών συστημάτων *Windows* της *Microsoft*), μπορεί να περιέχει και το λεγόμενο *swap file*. Ένα *bitstream image* είναι λοιπόν μια πλήρης αντιγραφή όλων αυτών των δεδομένων.

1.6.3.1. Στάσιμος χώρος (Slack Space)

Όταν ένα αρχείο αποθηκεύεται στο σκληρό δίσκο ενός υπολογιστικού συστήματος αποθηκεύεται σε κάποια ομάδα (*cluster*). Ανάλογα με το λειτουργικό σύστημα που χρησιμοποιεί το συγκεκριμένο σύστημα, το μέγεθος της κάθε μιας από αυτές τις ομάδες ποικίλει από 512 *bytes* μέχρι 32 *Kbytes* (32*1024 *bytes*). Οι *clusters*, λοιπόν, που περιέχουν αρχεία μικρότερα από το προκαθορισμένο μέγεθός τους θα περιέχουν κάποιο στάσιμο χώρο (*slack space*) μεταξύ του τέλους του αρχείου και το τέλος του *cluster*, όπως δείχνει το σχήμα 1.5. Στο χώρο αυτό μπορεί να βρίσκονται αποθηκευμένα τμήματα αρχείων που έχουν διαγραφεί, παλαιότερες εκδόσεις αρχείων που είναι ακόμη αποθηκευμένα στο σύστημα κτλ. Ο στάσιμος χώρος αποτελεί μια πολύ καλή πηγή για την εύρεση ηλεκτρονικών πληροφοριών που μπορούν να χρησιμεύσουν σαν πειστήρια.



***Σχήμα 1.5** – Ο στάσιμος χώρος (slack space)*

[31] αν και αυτό δεν είναι 100% αληθές, καθώς υπάρχουν προγράμματα, σήμερα, στο εμπόριο τα οποία μπορούν να βρουν «ξεχασμένα» αρχεία σε ένα σκληρό δίσκο ακόμη και μετά από διαδοχικές διαδικασίες μορφοποίησης. Ωστόσο, χάριν ευκολίας, θα βασιστούμε στην παραπάνω υπόθεση.

1.6.3.2. Ελεύθερος χώρος (Free Space)

Αντίστοιχα, ο ελεύθερος χώρος (*free space*) ενός σκληρού δίσκου θεωρείται σαν το «νεκροταφείο των αρχείων». Στο χώρο αυτό βρίσκονται, σχεδόν πάντα, αρχεία που έχουν διαγραφεί, προσωρινά αρχεία (*temporary files*) καθώς και οι μη χρησιμοποιούμενες περιοχές ενός σκληρού δίσκου (ειδικότερα αν στο σύστημα υπάρχει και το λεγόμενο *swap file*). Ο ελεύθερος χώρος ενός σκληρού δίσκου είναι επίσης μια πάρα πολύ καλή πηγή για τη συλλογή πληροφοριών.

1.6.3.3. Το αρχείο ανταλλαγής (swap file)

Το αρχείο ανταλλαγής χρησιμοποιείται από την οικογένεια των λειτουργικών συστημάτων *Windows* της εταιρείας *Microsoft*. Το *swap file* (γνωστό και ως *page file*[32]) είναι ένα κρυφό (*hidden*) αρχείο στο σκληρό δίσκο ενός υπολογιστή το οποίο διατηρεί προγράμματα και δεδομένα τα οποία δεν χωρούν στην κύρια μνήμη. Το αρχείο αυτό χρησιμοποιείται για να μεταφέρει προγράμματα και δεδομένα από και προς την κύρια μνήμη. Για να απλουστεύσουμε λίγο τα πράγματα και να μην μπερδέψουμε τον αναγνώστη με αρχές θεωρίας μοντέρνων λειτουργικών συστημάτων, το *swap file* είναι κάτι σαν το «σημειωματάριο» του υπολογιστή που κρατά αναλυτικές σημειώσεις σχετικά με τις ενέργειες που κάνει ο χρήστης. Το *swap file* αποτελεί μια έξοχη περιοχή για ανεύρεση χρήσιμων πληροφοριών καθώς εκεί τηρούνται τα *emails* τα οποία έχει διαχειριστεί ο χρήστης, τα *login names* και *passwords* που έχει χρησιμοποιήσει ο χρήστης καθώς και οι τοποθεσίες των ιστοσελίδων που έχει επισκεφθεί[33].

1.6.3.4. Άλλες πιθανές πηγές ανεύρεσης τέτοιων πληροφοριών

Ο σκληρός δίσκος ενός υπολογιστή δεν είναι η μόνη πηγή σε μια πιθανή ανάλυση *computer forensics*. Μεταξύ άλλων, σημεία τα οποία ερευνούν οι ειδικοί των *computer forensics*, για τη συλλογή κατάλληλων στοιχείων, είναι:

- Οι υπηρεσίες (*services*), οι εφαρμογές (*applications*) και οι διεργασίες (*processes*) οι οποίες είναι ενεργές κατά την ώρα που το μηχάνημα περνά στην κατοχή των ειδικών, αν αυτό είναι δυνατό. Με αυτό τον

[32] Το αρχείο αυτό βρίσκεται στο *root directory* του *partition* που έχει εγκατασταθεί το λειτουργικό σύστημα *Windows*, με όνομα *pagefile.sys*

[33] ένα αντίγραφο αυτών των πληροφοριών μπορεί επίσης να βρεθεί στους καταλόγους *Temporary Internet Files* και *History* σε κάθε σύστημα που χρησιμοποιεί λειτουργικό σύστημα *Windows*.

τρόπο μπορούν να βρεθούν προγράμματα η χρήση των οποίων έχει κυρίως κακόβουλο σκοπό (π.χ. *port scanners*)

- Το υλικό του συστήματος (*Hardware*) καθώς και όλοι οι αντίστοιχοι *drivers* που είναι εγκατεστημένοι στο σύστημα. Σε πολλές περιπτώσεις οι χρήστες συνδέουν εξωτερικές συσκευές αποθήκευσης σε ένα σύστημα για να μπορούν να αντιγράφουν δεδομένα (π.χ. εξωτερικά *zip drivers*, *cd-recorders*, *usb disks* ή *tokens* κτλ.)
- Τα αρχεία ελέγχου και καταγραφής του συστήματος (*audit log files*). Στα αρχεία αυτά μπορούν να βρεθούν χρήσιμες ενέργειες του χρήστη και σε πολλές περιπτώσεις αποτελούν τη βάση για την εξομοίωση μιας επίθεσης. Στα συστήματα που χρησιμοποιούν λειτουργικό *Microsoft Windows NT*/2000 τα αρχεία αυτά ονομάζονται αντίστοιχα *System*, *Security*, και *Application audit files*.
- Το λογισμικό (*software*) το οποίο είναι εγκατεστημένο στο συγκεκριμένο σύστημα. Σχεδόν στις περισσότερες περιπτώσεις, οι *hackers* χρησιμοποιούν συγκεκριμένα εργαλεία λογισμικού για να «αυτοματοποιήσουν» πολλά τμήματα μιας επίθεσης.
- Κρυπτογραφικό Λογισμικό (*Encryption Software*) το οποίο είναι εγκατεστημένο στο σύστημα. Υπάρχουν πολλές περιπτώσεις που ένας εσωτερικός (κυρίως) χρήστης αντιγράφει εμπιστευτικά ή απόρρητα δεδομένα, τα κρυπτογραφεί και τα στέλνει μέσω *email* (ή τα αντιγράφει σε αποθηκευτικά μέσα) σε μια συγκεκριμένη τοποθεσία (π.χ. σε ένα δικό του *FTP site*).
- Ύπαρξη *Published Shares*/*Permissions* σε ένα δίκτυο υπολογιστών. Η χρήση κατάλληλων δικτυακών πρωτοκόλλων (π.χ. *NetBIOS* στα *Windows* συστήματα) επιτρέπουν τον εύκολο διαμοιρασμό αρχείων (*file sharing*). Η ανεύρεση τέτοιων *shares*, σε συνδυασμό με τα αρχεία ελέγχου και καταγραφής της δικτυακής κίνησης μπορούν να δώσουν χρήσιμα συμπεράσματα για το ποιος είχε πρόσβαση σε τι, πώς, πότε και γιατί34.
- Αρχεία συνθηματικών (*Password Files*) τα οποία μπορεί να είναι αποθηκευμένα. Σε πολλές περιπτώσεις, οι *hackers* αντιγράφουν ολόκληρα *password files* στον υπολογιστή τους και χρησιμοποιούν κατάλληλο λογισμικό για να τα «σπάσουν».
- Δικτυακή Αρχιτεκτονική, η οποία μπορεί να «μαρτυρήσει» τα λεγόμενα «κρίσιμα συστήματα», τα συστήματα δηλαδή που τηρούν εμπιστευτικά ή απόρρητα δεδομένα και είναι ιδιαίτερα ελκυστικά στους *hackers*.

[34] Όπως αναφέρει χαρακτηριστικά ο *Gollman*, «*who had access to what*, *when and how*».

- Σύνδεση με «*X-Drives*» ή άλλα *FTP sites* στο *Internet*. Από την μελέτη των υποκαταλόγων *\Temporary Internet Files* και *\History* μπορεί, πολλές φορές, να βρεθεί αν ένας χρήστης έχει «ανεβάσει» (*upload*) δεδομένα σε εξωτερικούς δικτυακούς αποθηκευτικούς τόπους. Με τον όρο «*X-Drive*» εννοούμε (δωρεάν συνήθως) αποθηκευτικό χώρο στο *Internet*, ο οποίος προσφέρεται από διαφημιστικές εταιρείες.

1.6.4. Επιλογή του κατάλληλου εξοπλισμού για computer forensics

Σήμερα, όπως προαναφέραμε, υπάρχουν κατάλληλα εργαλεία λογισμικού τα οποία μπορούν να βοηθήσουν τους ειδικούς που διενεργούν μια *computer forensics* ανάλυση. Για παράδειγμα, υπάρχουν προγράμματα τα οποία μπορούν να απαριθμήσουν όλα τα αρχεία που υπάρχουν στο σκληρό δίσκο καθώς και στη μνήμη ενός υπολογιστή (ακόμη και διαγεγραμμένα).

Επίσης, κάποια από τα προγράμματα αυτά μπορούν να δώσουν αναλυτικές περιγραφές και πληροφορίες για τα αρχεία αυτά, όπως την ημερομηνία/ώρα της δημιουργίας ή της αλλαγής ή της διαγραφής τους καθώς και την ημερομηνία/ώρα που προσπελάστηκαν για τελευταία φορά.

Επιπλέον, μπορούν να ψάξουν μέσα στα αρχεία αυτά για την ύπαρξη συγκεκριμένων λέξεων ή φράσεων (*keywords* και *keyphrases* αντιστοίχως). Αυτό είναι ιδιαίτερα χρήσιμο καθώς τα αρχεία που θα ερευνηθούν είναι, τις περισσότερες φορές, αρκετές χιλιάδες και ένα σειριακό ψάξιμο θα έπαιρνε αιώνες μέχρι να ολοκληρωθεί. Τέλος, υπάρχουν αρκετά εργαλεία τα οποία διαχωρίζουν τον στάσιμο από τον ελεύθερο χώρο και το αρχείο ανταλλαγής, κάνοντας αρκετά πιο εύκολη τη δουλειά του ειδικού.

Είναι πέρα από τους σκοπούς του βιβλίου αυτού να αξιολογήσει τα υπάρχοντα εργαλεία λογισμικού που υπάρχουν σήμερα στην παγκόσμια αγορά ή να προτείνει κάποιο συγκεκριμένο. Σίγουρα όμως η επιλογή ενός τέτοιου προγράμματος πρέπει να πληροί συγκεκριμένα κριτήρια, πέρα από τις τεχνολογικές του αρετές, ώστε να μπορεί να σταθεί αξιοπρεπώς σε μια δικαστική διαμάχη. Θυμηθείτε πως ένας από τους πιο σημαντικούς λόγους για τους οποίους πολλές δίκες με αντικείμενο το ηλεκτρονικό έγκλημα χάνονται είναι γιατί αλλοιώνονται –ηθελημένα ή (τις περισσότερες φορές) αθέλητα –τα αποδεικτικά στοιχεία.

Ενδεικτικά, το λογισμικό αυτό, πρέπει να είναι κατάλληλο για το λειτουργικό σύστημα (και την έκδοση) του υπολογιστή που εξετάζεται.

Επίσης, πρέπει να υποστηρίζει τον τύπο και τις ρυθμίσεις της προς ανάλυση πλατφόρμας (π.χ. να υποστηρίζει τη διάταξη *RAID* των σκληρών δίσκων καθώς και δικτυακό περιβάλλον).

Σήμερα κυκλοφορούν πολλά τέτοια εργαλεία στο *Internet*, τα οποία πολλές φορές είναι δωρεάν διαθέσιμα. Αυτά τα εργαλεία είναι χρήσιμα μόνο για εκπαιδευτικούς σκοπούς και σε καμία περίπτωση δεν θα πρέπει να χρησιμοποιούνται σε σοβαρές περιπτώσεις. Αντιθέτως, το χρησιμοποιούμενο λογισμικό πρέπει να προέρχεται από έναν αξιόπιστο οίκο που να το υποστηρίζει (ενημερώνει) και να το τεκμηριώνει κατάλληλα. Υπάρχουν μάλιστα πολλές περιπτώσεις που στο δικαστήριο έχει κληθεί ο δημιουργός ενός τέτοιου προγράμματος για να επιλύσει διαφωνίες.

Αντιστοίχως, το χρησιμοποιούμενο υλικό (*hardware*) περιλαμβάνει πολλούς συνδυασμούς και επιλογές. Μπορεί να χρησιμοποιηθούν τόσο *desktop* συστήματα όσο και φορητοί υπολογιστές (*laptops*), ανάλογα με την περίπτωση. Απαραίτητη προϋπόθεση είναι τα συστήματα αυτά να είναι ιδιαίτερα ισχυρά[35] και να έχουν αρκετή διαθέσιμη μνήμη. Επιπροσθέτως, απαιτούνται εξωτερικές συσκευές αποθήκευσης (*CD-R*, *DVD-R* ή ακόμη και *tape streamers*), εξωτερικοί σκληροί δίσκοι (χωρητικότητας 80*G*B ή και μεγαλύτερης), καλώδια *UTP* ("*cross*" και "*straight*36"), καλώδια σύνδεσης υπολογιστών μέσω της σειριακής, παράλληλης, *USB* ή/και *Firewire* θύρας, *hubs* και *switches* κτλ.

Ακόμη, σε πολλές περιπτώσεις, χρειάζονται ψηφιακές φωτογραφικές μηχανές για να αποτυπώσουν την ακριβή κατάσταση και θέση στην οποία οι ειδικοί παραλαμβάνουν έναν υπολογιστή (π.χ. την εικόνα που έχει η οθόνη του υπολογιστή τη συγκεκριμένη στιγμή, φωτογραφίες[37] του χώρου ή του δωματίου στο οποίο βρίσκεται κτλ.).

Επίσης, χρειάζεται πάντοτε το κατάλληλο λογισμικό υποστήριξης, το οποίο μεταξύ άλλων περιλαμβάνει:

---

[35] Για παράδειγμα, για το έτος 2002, ένα τυπικό τέτοιο σύστημα, πρέπει να απαρτίζεται, μεταξύ άλλων, από 1 (ή 2 ή περισσότερους) επεξεργαστές *Pentium* 4 με συχνότητα 2.6*GHz* (ή μεγαλύτερη), 2*GB* μνήμης *RAM* (ή περισσότερη) και (τουλάχιστον) 80*GB* σκληρό δίσκο. Επίσης, πρέπει να διαθέτει πολλαπλές θύρες επικοινωνίας και να υποστηρίζει όλες τις κατηγορίες αποθηκευτικών μέσων. Τα μεγέθη αυτά αυξάνουν – δραματικά- κάθε χρόνο.

[36] Που συμβολίζονται συνήθως "*X*" & "*Str*8" αντίστοιχα

[37] Οι φωτογραφίες αυτές αποθηκεύονται ψηφιακά και στη συνέχεια υπολογίζεται το κρυπτογραφικό άθροισμά τους για να τις προφυλάξουν από εσκεμμένο μοντάζ.

- Προγράμματα που παρέχουν *bitstream images* του σκληρού δίσκου
- Προγράμματα που να μπορούν να υπολογίσουν ή/και να επιβεβαιώσουν κρυπτογραφικά αθροίσματα ελέγχου (*cryptographic checksums*) με σκοπό να διαφυλάξουν την ακεραιότητα των δεδομένων που εξετάζονται
- Προγράμματα ανεύρεσης κωδικών για αρχεία διαφόρων μορφοτύπων (π.χ. συμπιεσμένα *–zipped-* αρχεία, αρχεία *Word*, *Excel*, *Powerpoint* κτλ.)
- Προγράμματα ανεύρεσης άλλων κωδικών (π.χ. *system password*, *boot password* κτλ.)
- Προγράμματα *sniffer* για να αναλύσουν αρχεία τα οποία έχουν καταγράψει τη δικτυακή κίνηση σε ένα τοπικό δίκτυο υπολογιστών
- Προγράμματα *antivirus* για την ανίχνευση τέτοιων ή παρεμφερών αρχείων (π.χ. *viruses* ή *Trojan horses*)
- Προγράμματα που μπορούν να παράγουν εκθέσεις (*reports*) των δεδομένων που αναλύονται

Τέλος, έχουν αναφερθεί περιπτώσεις στις οποίες χρειάστηκε πλήρης εξομοίωση του προς εξέταση συστήματος, όσον αφορά στο υλικό του, αλλά και του τμήματος του δικτύου[38] στο οποίο ανήκε.

1.6.5. Πώς δημιουργείται ένα κατάλληλο αντίγραφο ενός σκληρού δίσκου

Το πρώτο βήμα και ίσως ένα από τα πιο σημαντικά, που πρέπει να γίνει σε μια *computer forensics* ανάλυση, είναι η δημιουργία ενός αντιγράφου του σκληρού δίσκου του συστήματος που πρέπει να εξεταστεί. Στη συνέχεια, το αντίγραφο αυτό «κοπιάρεται» ξανά στο σταθμό ανάλυσης (*forensics workstation*) στον οποίο λαμβάνει χώρα όλη η διαδικασία ανίχνευσης και συλλογής των ζητουμένων πληροφοριών.

Στη σχετική βιβλιογραφία συναντάμε τρεις –κυρίως- διαφορετικούς τρόπους για τη δημιουργία τέτοιων αντιγράφων (γνωστών, επίσης, και σαν *forensic duplicates*):

- Αφαίρεση του σκληρού δίσκου του προς εξέταση συστήματος, προσθήκη του στο σύστημα ανάλυσης (*forensic workstation*) και δημιουργία ενός (ή περισσοτέρων) αντιγράφων. Με αυτόν τον τρόπο

[38] Του *VLAN* (*Virtual Local Area Network*) στο οποίο ανήκε για να είμαστε πιο συγκεκριμένοι.

δεν χρειάζεται η εγκατάσταση ειδικού λογισμικού στο υπό εξέταση σύστημα αλλά δεν μπορεί να αποτυπωθεί η τρέχουσα κατάστασή του[39], καθώς το σύστημα θα πρέπει να τεθεί εκτός λειτουργίας.

- Προσθήκη ενός σκληρού δίσκου στο προς εξέταση σύστημα και δημιουργία του αντιγράφου. Με τον τρόπο αυτό δημιουργούνται μικρές αλλαγές στο *BIOS* (*Basic Input Output System*) του συστήματος. Επίσης, δεν μπορεί να αποτυπωθεί η τρέχουσα κατάστασή του. Τέλος, πρέπει να εγκατασταθεί ειδικό λογισμικό δημιουργίας αντιγράφων (*disk cloning software*) στο συγκεκριμένο σύστημα. Παρ' όλα αυτά, ο τρόπος αυτός προτιμάται όταν υπάρχουν περιορισμοί σε υλικό ή όταν η διαδικασία γίνεται για εκπαιδευτικούς σκοπούς.
- Σύνδεση του υπό εξέταση συστήματος με το σύστημα ανάλυσης (συνήθως μέσω της παράλληλης θύρας επικοινωνίας), δημιουργία του αντιγράφου και αποστολή του σε ένα απομακρυσμένο σύστημα (μέσω ενός κλειστού δικτύου) ή αποθήκευση στο σύστημα ανάλυσης. Ο τρόπος αυτός είναι και ο περισσότερο ασφαλής, αν όμως υπάρχει εγκατεστημένο ειδικό λογισμικό στο σύστημα ανάλυσης και αρκετός αποθηκευτικός χώρος σε αυτό (ίσος ή μεγαλύτερος από εκείνον του υπό εξέταση συστήματος). Μοναδικός –και σε κάποιες περιπτώσεις σημαντικός- περιορισμός είναι η ταχύτητα με την οποία δημιουργείται το αντίγραφο του σκληρού δίσκου, κυρίως λόγω της ταχύτητας της παράλληλης θύρας[40].

1.6.6. Συνηθισμένα λάθη στο χειρισμό ηλεκτρονικών αποδεικτικών στοιχείων

Σύμφωνα με τους *Mandia* και *Prosise*, τα παρακάτω είναι τα πιο συνηθισμένα λάθη –από μια μεγάλη σειρά- που καταστρέφουν την όλη διαδικασία συλλογής και επεξεργασίας ηλεκτρονικών αποδεικτικών στοιχείων:

- Αλλοίωση της ημερομηνίας ή/και της ώρας στους σταθμούς εργασίας που χρησιμοποιούνται για την εξέταση ενός σκληρού δίσκου ή ενός ολόκληρου συστήματος. Χρειάζεται να τονίσουμε πως η όλη η διαδικασία μιας *computer forensics* ανάλυσης γίνεται σε απόλυτους –και όχι σχετικούς- χρόνους. Όπως θα εξηγήσουμε και στην επόμενη ενότητα, η διατήρηση μιας αλληλουχίας επιτήρησης (*chain of custody*)

---

[39] Τρέχουσες εφαρμογές (*applications*), διαδικασίες (*procedures*), διεργασίες (*processes*), «δαίμονες» (*daemons*), προγράμματα (*programs*), ανοικτά ή προσωρινά αρχεία (*open*/*temporary files*) καθώς και τα περιεχόμενα της μνήμης *RAM*.

[40] Ενδεικτικά, για ένα σκληρό δίσκο 40*GB* ο οποίος αντιγράφεται με αυτόν τον τρόπο απαιτούνται:
(40*1024*1024*1024) *bytes* / (115,200) *bytes*/*sec* = 372827 *sec* (ή 4 1/2 περίπου ημέρες!)

των αποδεικτικών στοιχείων είναι κρίσιμος παράγοντας για την ακεραιότητα της όλης διαδικασίας

- Τερματισμός των τρεχουσών διεργασιών του υπό εξέταση συστήματος. Αυτό μπορεί να οδηγήσει σε πιθανή διαγραφή προσωρινών αρχείων, αρχείων που είναι ανοικτά εκείνη τη στιγμή, ανοικτών συνδέσεων κτλ. και μπορεί, επίσης, να οδηγήσει σε αλλοίωση των αποτελεσμάτων της ανάλυσης.
- Μη καταγραφή των εντολών που δίδονται στο υπό εξέταση σύστημα. Η καταγραφή οποιασδήποτε τέτοιας εντολής πρέπει να γίνεται με θρησκευτική ευλάβεια καθώς ο αναλυτής μπορεί να κατηγορηθεί για εσκεμμένη αλλοίωση των αποτελεσμάτων.
- Εγκατάσταση και χρήση εργαλείων με γραφικό περιβάλλον (*graphical user interface – GUI*) στο υπό εξέταση σύστημα. Τα προγράμματα αυτά, τις περισσότερες φορές, πρέπει να εγκαταστήσουν, στο σκληρό δίσκο του συστήματος, μια σειρά από απαραίτητες βιβλιοθήκες (*software libraries*) και αρχεία τα οποία μπορεί να αλλοιώσουν τα πιθανά αποδεικτικά στοιχεία.
- Χρησιμοποίηση λάθος εντολών και αρχείων[41]
- Εγκατάσταση προγραμμάτων στο υπό εξέταση σύστημα που αλλοιώνουν τα πιθανά αποδεικτικά στοιχεία (για τους ίδιους λόγους που αναφέρθηκαν παραπάνω).
- Χρήση προγραμμάτων που αποθηκεύουν τα αποτελέσματα στο σκληρό δίσκο του υπό εξέταση συστήματος (παρομοίως...)

Οι παραπάνω λόγοι αναφέρθηκαν με τυχαία σειρά. Ο πιο δημοφιλής λόγος, όπως τονίσαμε προηγουμένως, είναι η εξέταση του (σκληρού δίσκου του) συστήματος αυτού καθαυτού και όχι του αντιγράφου του (*bistream image*).

1.6.7. Η αλληλουχία επιτήρησης (chain of custody) των ηλεκτρονικών στοιχείων

Σε μια *computer forensics* ανάλυση πρέπει να ακολουθούνται συγκεκριμένες διαδικασίες και πρακτικές για τη δημιουργία αλλά και την κατάλληλη τεκμηρίωση μιας αλληλουχίας επιτήρησης.

Ενδεικτικά, αναφέρουμε πως για κάθε σύστημα ή/και αποθηκευτικό μέσο το οποίο εξετάζεται πρέπει να δημιουργούνται κατάλληλες ετικέτες (*tags*), παρόμοιες με αυτές που φαίνονται στο σχήμα 1.6 και 1.7 αντιστοίχως.

---

[41] Χωρίς ιδιαίτερα σχόλια...(!)

ΗΜΕΡΟΜΗΝΙΑ	**ΟΝΟΜΑ ΣΥΣΤΗΜΑΤΟΣ**	
ΟΝΟΜΑ ΥΠΕΥΘΥΝΟΥ ΑΝΑΛΥΣΗΣ	ΥΠΟΓΡΑΦΗ ΥΠΕΥΘΥΝΟΥ ΑΝΑΛΥΣΗΣ	ΟΝΟΜΑ ΚΑΙ ΑΡΙΘΜΟΣ ΔΙΚΑΣΤΙΚΗΣ ΥΠΟΘΕΣΗΣ
ΟΝΟΜΑ ΚΑΤΟΧΟΥ ΠΕΙΣΤΗΡΙΩΝ	ΥΠΟΓΡΑΦΗ	

***Σχήμα 1.6** – Ετικέτα για κάθε αποθηκευτικό μέσο που εξετάζεται (μπροστινή όψη)*

Κατά τη διάρκεια μιας τέτοιας ανάλυσης χρειάζεται πολλές φορές να αλλάζουν κάτοχο ή/και τοποθεσία τα αποδεικτικά στοιχεία τα οποία συλλέγονται. Κάθε τέτοια «συναλλαγή» πρέπει να τεκμηριώνεται κατάλληλα. Πέρα από τις ετικέτες που προαναφέραμε, κάθε πληροφορία που αφορά στις συγκεκριμένες πληροφορίες πρέπει να καταγράφεται και να περιγράφεται αναλυτικά. Παραδοσιακά, ο πιο δημοφιλής τρόπος είναι ένα σημειωματάριο[42] αν και σήμερα τον ίδιο ρόλο μπορεί να παίξει και ένας φορητός υπολογιστής.

ΑΛΛΗΛΟΥΧΙΑ ΕΠΙΤΗΡΗΣΗΣ			
ΑΠΟ: ΠΕΡΙΟΧΗ:	ΗΜΕΡΟΜΗΝΙΑ	ΑΙΤΙΑ	ΠΡΟΣ: ΠΕΡΙΟΧΗ:
ΑΠΟ: ΠΕΡΙΟΧΗ:	ΗΜΕΡΟΜΗΝΙΑ	ΑΙΤΙΑ	ΠΡΟΣ: ΠΕΡΙΟΧΗ:
ΑΠΟ: ΠΕΡΙΟΧΗ:	ΗΜΕΡΟΜΗΝΙΑ	ΑΙΤΙΑ	ΠΡΟΣ: ΠΕΡΙΟΧΗ:
ΑΠΟ: ΠΕΡΙΟΧΗ:	ΗΜΕΡΟΜΗΝΙΑ	ΑΙΤΙΑ	ΠΡΟΣ: ΠΕΡΙΟΧΗ:
ΑΠΟ: ΠΕΡΙΟΧΗ:	ΗΜΕΡΟΜΗΝΙΑ	ΑΙΤΙΑ	ΠΡΟΣ: ΠΕΡΙΟΧΗ:
ΤΕΛΙΚΗ ΚΑΤΑΣΤΑΣΗ ΠΕΙΣΤΗΡΙΩΝ		ΗΜΕΡΟΜΗΝΙΑ	

***Σχήμα 1.7** – Ετικέτα για κάθε αποθηκευτικό μέσο που εξετάζεται (οπίσθια όψη)*

---

[42] Όσο παράξενο και αν φαίνεται αυτό στην εποχή μας, πολλές φορές έχει σώσει από δύσκολες καταστάσεις. Για τη σημασία ενός τέτοιου σημειωματάριου, ο αναγνώστης ενθαρρύνεται να ανατρέξει στο *Cuckoo's Egg*.

Για παράδειγμα, οι παρακάτω πληροφορίες είναι οι ελάχιστες από εκείνες που πρέπει να διατηρούνται:

- Τοποθεσία του υπό εξέταση συστήματος
- Τα ονόματα των ατόμων που ήταν παρόντα όταν άρχισε η εξέταση του συγκεκριμένου συστήματος
- Τα ονόματα των ατόμων που μπορούν να έχουν πρόσβαση στο χώρο στον οποίο βρίσκεται το υπό εξέταση σύστημα
- Η κατάσταση του υπό εξέταση συστήματος (πιθανόν μια φωτογραφία, η οποία δείχνει όλες τις «ορατές» πληροφορίες)
- Οι σειριακοί αριθμοί (*serial numbers*), το μοντέλο και η μάρκα κάθε μέρους του συστήματος που εξετάζεται
- Τα περιφερειακά που βρίσκονται συνδεδεμένα με το συγκεκριμένο σύστημα.