

Γ.Ε.Ι. ΜΕΣΟΛΟΓΓΙΟΥ  
Σ.Δ.Ο.-Σ.Σ.Ο.Ε.



# ΕΓΚΛΗΜΑΤΑ ΣΤΟ INTERNET ΤΟ 1999

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ:  
ΧΡΗΣΤΟΣ ΤΣΟΥΡΑΜΑΝΗΣ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ ΤΗΣ:  
ΕΥΑΓΓΕΛΙΑΣ ΜΠΑΣΑΚΑΡΗ

Μεσολόγι 2001

**ΕΓΚΛΗΜΑΤΑ ΣΤΟ INTERNET  
ΤΟ 1999**

# ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

<b><u>ΠΡΟΛΟΓΟΣ</u></b>	3
<b><u>ΜΕΡΟΣ ΠΡΩΤΟ</u></b>	
<b>1. ΤΟ INTERNET: ΤΟ ΔΙΕΘΝΕΣ ΔΙΑΔΙΚΤΥΟ</b>	5
Α. ΤΙ ΕΙΝΑΙ ΤΟ INTERNET	7
Β. ΧΡΗΣΕΙΣ ΚΑΙ ΧΡΗΣΙΜΟΤΗΤΑ ΤΟΥ INTERNET	9
Γ. ΓΕΝΝΗΣΗ ΚΑΙ ΕΞΕΛΙΞΗ	12
Δ. ΤΟ INTERNET ΣΤΗΝ ΕΛΛΑΔΑ	16
<b><u>ΜΕΡΟΣ ΔΕΥΤΕΡΟ</u></b>	
<b>2. ΤΟ ΗΛΕΚΤΡΟΝΙΚΟ ΕΓΚΛΗΜΑ (ΠΑΡΑΒΑΤΙΚΟΤΗΤΑ ΣΤΟ ΔΙΑΔΙΚΤΥΟ)</b>	18
Α. ΕΝΝΟΙΑ	18
Β. ΜΟΡΦΕΣ	20
Γ. ΔΡΑΣΤΕΣ	24
Δ. ΘΥΜΑΤΑ	28
Ε. ΑΝΤΙΜΕΤΩΠΙΣΗ	31
<b><u>ΜΕΡΟΣ ΤΡΙΤΟ</u></b>	
<b>3. ΠΑΡΑΒΑΤΙΚΟΤΗΤΑ ΣΤΟ ΔΙΑΔΙΚΤΥΟ ΤΟ 1999</b>	33
Α. ΜΕΘΟΔΟΛΟΓΙΑ ΣΥΛΛΟΓΗΣ	33

Β. ΠΑΡΟΥΣΙΑΣΗ	34
Γ. ΚΡΙΤΙΚΕΣ ΠΑΡΑΤΗΡΗΣΕΙΣ	112
<b><u>ΕΠΙΛΟΓΟΣ</u></b>	114
<b><u>ΠΗΓΕΣ</u></b>	116
Α. ΒΙΒΛΙΑ	116
Α.1. ΕΛΛΗΝΙΚΑ	116
Α.2. ΞΕΝΑ	116
Β. ΑΡΘΡΑ	116
Β.1. ΕΛΛΗΝΙΚΑ	116
Β.2. ΞΕΝΑ	118
Γ. ΙΣΤΟΣΕΛΙΔΕΣ	118
<b><u>ΠΑΡΑΡΤΗΜΑ</u></b>	119
Α. ΓΛΩΣΣΑΡΙΟ	119

## ΠΡΟΛΟΓΟΣ

Η τεχνολογία των ηλεκτρονικών υπολογιστών έχει μπει στη ζωή μας και έχει κατακτήσει ρόλο αναντικατάστατο όσον αφορά τις ευκολίες και τις δυνατότητες που προσφέρει σε όλους τους τομείς, από την πληροφόρηση, την επικοινωνία και τη διασκέδαση μέχρι τη διεξαγωγή των περισσότερων συναλλαγών μεταξύ επιχειρήσεων, τραπεζών, δημόσιων υπηρεσιών κ.α. Ο κυβερνοχώρος με τη σημερινή του μορφή είναι μία μικρογραφία της κοινωνίας όπου αναπόφευκτα κάθε είδους παράνομη δραστηριότητα βρίσκει πρόσφορο έδαφος. Στο καινούριο θαυμαστό περιβάλλον του Διαδικτύου, φιλοξενούνται όλα τα είδη των ανθρώπων, μεταξύ των οποίων απατεώνες και εγκληματίες, με αποτέλεσμα απέναντι στα προτερήματα του κυβερνοχώρου να αντιπαραβάλλονται και πολλά «δεινά». Σκοπός αυτής της πτυχιακής εργασίας είναι να παρουσιάσει τη «σκοτεινή πλευρά» του Internet, αναφέροντας συγκεκριμένα παραδείγματα.

Ακολουθεί μία σύντομη περίληψη των περιεχομένων της πτυχιακής εργασίας:

- **ΜΕΡΟΣ ΠΡΩΤΟ: «Το Internet: Το Διεθνές Διαδίκτυο».** Εξηγείται τι ακριβώς είναι το Internet, περιγράφονται οι χρήσεις και η χρησιμότητά του. Περιλαμβάνεται μία ιστορική αναδρομή με αφετηρία την πνευματική σύλληψη της ιδέας του «γαλαξιακού δικτύου» μέχρι τη σημερινή του μορφή και τέλος, μία μικρή αναφορά στην εξέλιξη του Internet στον ελλαδικό χώρο.
- **ΜΕΡΟΣ ΔΕΥΤΕΡΟ: «Το Ηλεκτρονικό Έγκλημα (Παραβατικότητα στο Διαδίκτυο)».** Δίνεται ο εννοιολογικός προσδιορισμός της Ηλεκτρονικής Παραβατικότητας και παραθέτονται οι μορφές της, με τη βοήθεια παραδειγμάτων. Παρουσιάζονται το προφίλ των δραστών και οι κατηγορίες των θυμάτων, με ειδική αναφορά στα πρώτα κρούσματα παραβάσεων στην Ελλάδα. Τέλος, μπορεί κανείς να διαβάσει απλούς

τρόπους προκειμένου να προστατευτεί όταν σερφάρει ή δραστηριοποιείται στο Internet.

- **ΜΕΡΟΣ ΤΡΙΤΟ: «Παραβατικότητα στο Διαδίκτυο το 1999».** Γίνεται παρουσίαση των περιπτώσεων παραβατικότητας στο Διαδίκτυο έτσι όπως καταγράφηκαν στην ιστοσελίδα [www.apbnews.com](http://www.apbnews.com) για το έτος 1999 – 2000. Πρόκειται για περιπτώσεις όλων των μορφών παραβατικής συμπεριφοράς που έφτασαν στις αίθουσες των δικαστηρίων ή είδαν το φως της δημοσιότητας. Ολοκληρώνοντας, παρατίθεται η προσωπική μου άποψη για τις παραπάνω περιπτώσεις.

Θα ήθελα να εκφράσω τις ευχαριστίες μου προς τον καθηγητή κ. Χρ. Τσουραμάνη και την παιδική μου φίλη Ε. Παναγοπούλου για την πρακτική και ηθική υποστήριξή τους σ' όλη τη διάρκεια συγγραφής της πτυχιακής μου εργασίας.

# 1. ΤΟ INTERNET: ΔΙΕΘΝΕΣ ΔΙΑΔΙΚΤΥΟ

Το Internet, όσο τίποτε άλλο, προκάλεσε επανάσταση στον κόσμο των ηλεκτρονικών υπολογιστών και των επικοινωνιακών μέσων. Οι ανακαλύψεις του τηλέγραφου, του τηλεφώνου, του ραδιοφώνου και των ηλεκτρονικών υπολογιστών, έθεσαν τις βάσεις για αυτήν την άνευ προηγουμένου ολοκλήρωση μέσω των ιδιοτήτων που διαθέτουν.

Αυτός ο παγκόσμιος αναμεταδότης, το Internet, εμπεριέχει πολλαπλές ιδιότητες ανάμεσα στις οποίες: αποτελεί ένα θαυμάσιο μηχανισμό για την εύρεση πληροφοριών, ένα μέσο για συνεργασία και επιχειρηματική δράση σε παγκόσμιο επίπεδο, αφού μέσω αυτού παύουν να υφίστανται γεωγραφικά όρια και εμπόδια μεταξύ ατόμων και επιχειρήσεων.

Το Internet, αντιπροσωπεύει ένα από τα επιτυχημένα παραδείγματα από τα οφέλη που μπορεί να προσφέρει η σύγχρονη τεχνολογία. Ο όρος Υπερλεωφόρος της Πληροφόρησης που δίνεται από πολλούς για το Internet αποτελεί ανεπαρκή χαρακτηρισμό του αναφορικά με την ποικιλία των λειτουργιών που δύναται να εκτελέσει.

Θέτοντας σαν αφετηρία την πρώιμη έρευνα αναφορικά με τη διαδικτύωση ηλεκτρονικών υπολογιστών το κράτος, η βιομηχανία και ο ακαδημαϊκός χώρος ανάπτυξης συνεργάστηκαν στην εξέλιξη και ανάπτυξη αυτής της νέας εντυπωσιακής τεχνολογίας. Στις μέρες μας όροι όπως «bleiner@computer.org» και «http://www.acm.org» είναι συνηθισμένοι στις καθημερινές ομιλίες μεταξύ απλών ανθρώπων.

Η ιστορία του Internet περιστρέφεται γύρω από τέσσερις άξονες:

- Ο πρώτος είναι της τεχνολογικής εξέλιξης που άρχισε με την πρώιμη έρευνα των συμπιεσμένων μεταγωγέων πακέτων και το APRANET (παρόμοια τεχνολογία), όπου η τρέχουσα έρευνα συνεχίζει να επεκτείνει τους ορίζοντες της όσον αφορά την υποδομή προς διάφορες κατευθύνσεις, όπως στις αναλογίες μεταξύ διαφόρων διαστάσεων των



μερών που συναποτελούν το σύστημα του Internet, την απόδοση και τη λειτουργικότητα σε υψηλότερο επίπεδο.

- Υπάρχει ο άξονας των κέντρων ελέγχου των επιχειρήσεων και της διοίκησης για μια παγκόσμια και πολύπλοκη υποδομή λειτουργίας.
- Ο κοινωνικός άξονας από τον οποίο απορρέει (προκύπτει) το όραμα για μια φιλελεύθερη κοινωνία «Ίντερναυτών» που μέσω της κοινής συνεργασίας θα δημιουργούσαν και θα ανέπτυσαν τεχνολογία.
- Τέλος, είναι ο άξονας της εμπορευματοποίησης, ο οποίος καταλήγει σε μια εκπληκτικά αποτελεσματική μεταλλαγή των αποτελεσμάτων της έρευνας σε πλατιά αναπτυσσόμενη και διαθέσιμη υποδομή πληροφοριών.

Σήμερα το Internet αποτελεί μια υποδομή πληροφοριών παγκοσμίως διαδεδομένη που συχνά αποκαλείται Διεθνής Υποδομή Πληροφοριών (National Information Infrastructure). Η ιστορία του είναι περίπλοκη, επειδή εμπεριέχει πολλές όψεις – τεχνολογική, οργανωτική, κοινωνική. Η δυναμική του επίδραση πλησιάζει όχι μόνο τον τεχνολογικό χώρο των επικοινωνιών μέσω των υπολογιστών αλλά και την κοινωνία όσο η εξέλιξη προχωρά στη χρησιμοποίηση άμεσα συνδεδεμένων εργαλείων για την διεκπεραίωση του ηλεκτρονικού εμπορίου, την πρόσκτηση (απόκτηση) πληροφοριών και την κοινή δράση μεταξύ των επιχειρήσεων.

Χωρίς αμφιβολία βρισκόμαστε στην εποχή του Internet και της Πληροφορικής. Είναι απίστευτο το μέγεθος της προσφοράς αυτής της τεχνολογίας στην ανθρωπότητα. Ο 20<sup>ος</sup> αιώνας είναι ο αιώνας της ανάπτυξης της τεχνολογίας η οποία εισέβαλε στην καθημερινή ζωή του ανθρώπου με σκοπό να τη βελτιώσει.

Στη συνέχεια θα ακολουθήσει μια συνοπτική ανασκόπηση στα κυριότερα στάδια της εξελικτικής πορείας του Διαδικτύου η οποία ξεκινά από τα τέλη της δεκαετίας του 1950.



## A. ΤΙ ΕΙΝΑΙ ΤΟ INTERNET

Ο θαυμάσιος κόσμος του Internet παρά την ταχεία διάδοσή του είναι άγνωστος σε αρκετούς ανθρώπους, και ιδίως στη χώρα μας όπου άρχισε να διαδίδεται τα τελευταία χρόνια. Για τον παραπάνω λόγο θεωρώ σκόπιμο να δώσω απάντηση στο ερώτημα «Τι είναι το Internet;».

Ο συγγραφέας Noel Estabrook παρομοίασε πολύ πετυχημένα το σύστημα Internet με το σύστημα τηλεφώνου. Πράγματι τα κοινά των δύο αυτών συστημάτων είναι πολλά: Και τα δύο έχουν δημιουργηθεί με σκοπό τη μετάδοση δεδομένων όπως ήχο και κείμενο. Προκειμένου να γίνει η διεκπεραίωση της μεταφοράς των δεδομένων χρησιμοποιούν πολύπλοκα μέσα που αλληλοσυνεργάζονται. Καθώς το τηλεφωνικό σύστημα απαιτεί για κάθε ένα που θέλει μία τηλεφωνική σύνδεση, έναν μοναδικό αριθμό, έτσι και η σύνδεση στο Internet απαιτεί από κάθε συμμετέχον μία μοναδική διεύθυνση ηλεκτρονικού ταχυδρομείου. Τέλος και τα δύο συστήματα χρησιμοποιούν τύπους συσκευών όπως η τηλεφωνική συσκευή ή ένα μόντεμ αντίστοιχα.

Αρκεί να σκεφτούμε μόνο πως ένα τηλεφώνημα από την Ελλάδα φτάνει σε μία πολιτεία της Αμερικής. Περίπου με τον ίδιο τρόπο μπορούν να επικοινωνήσουν μέσω του Internet δύο άνθρωποι από διαφορετικά σημεία του πλανήτη.

Στην περίπτωση βέβαια του Internet χρησιμοποιούνται διαφορετικά μέσα και τύποι συσκευών για την εκτέλεση της παραπάνω λειτουργίας. Τον ρόλο των τηλεφωνικών σταθμών όσον αφορά το Internet έχουν οι κόμβοι, οι οποίοι εκτελούν λειτουργίες παρόμοιες με εκείνες που εκτελούν οι σταθμοί δρομολόγησης των τηλεφωνημάτων. Η βασική διαφορά αφορά τον τρόπο μεταφοράς των δεδομένων. Ενώ στο τηλεφωνικό σύστημα ένα τηλεφώνημα μεταδίδεται σε μια σταθερή ροή, στο σύστημα του Internet τα δεδομένα μεταδίδονται ψηφιακά και αποτελούνται από σειρές 0 και 1 σε συνδυασμούς.

Η παραπάνω παρομοίωση δεν αποτελεί παρά ένα υπεραπλουστευμένο παράδειγμα και παρά το γεγονός ότι τα δύο

αυτά συστήματα έχουν πολλά κοινά δεν θα πρέπει να συγχέονται στο μυαλό μας.

Αποτελούν δύο διαφορετικά συστήματα που λειτουργούν με παρόμοιο αλλά διαφορετικό τρόπο.

## **B. ΧΡΗΣΕΙΣ ΚΑΙ ΧΡΗΣΙΜΟΤΗΤΑ ΤΟΥ INTERNET**

Η εκπληκτική αύξηση του αριθμού των χρηστών του Internet από την αρχική σύλληψή του στις αρχές της δεκαετίας του '70 μέχρι σήμερα οφείλεται σαφώς στη χρησιμότητά του. Η διάδοση του Internet δεν είναι τυχαίο γεγονός αφού οι χρήσεις του είναι πολλές και καλύπτουν σχεδόν όλο το φάσμα των ανθρώπινων ενδιαφερόντων.

### **Επικοινωνία**

Μία από τις πιο δημοφιλείς χρήσεις του είναι η επικοινωνία μέσω του ηλεκτρονικού ταχυδρομείου γνωστό ως e-mail. Αποτελεί τον πιο γρήγορο και εύκολο τρόπο επικοινωνίας που υπάρχει στη διάθεσή μας σήμερα μαζί με το τηλέφωνο. Μια διεύθυνση e-mail είναι ζωτικής σημασίας όσον αφορά την επικοινωνία σε μια κοινωνία που χρησιμοποιεί όλο και περισσότερο το Internet. Δίνει ένα πλεονέκτημα όσον αφορά τη συνεργασία και την επικοινωνία τόσο σε προσωπικό όσο και σε κοινωνικό επίπεδο. Επιπλέον το e-mail είναι η φθηνότερη μορφή επικοινωνίας και παρέχει μεγάλη εξοικονόμηση χρόνου.

Το Internet δίνει τη δυνατότητα στους χρήστες του να προσπελάσουν εκατοντάδες ανθρώπους μέσω μιας και μόνης διεύθυνσης ηλεκτρονικού ταχυδρομείου που αποκαλείται ταχυδρομική λίστα (mailing list). Συμμετοχή σε μια ταχυδρομική λίστα σημαίνει δυνατότητα άμεσης πρόσβασης σε όλους όσους συμμετέχουν σ' αυτή.

Η ταχυδρομική λίστα είναι διαμορφωμένη ώστε να προωθεί κάθε μήνυμα που λαμβάνει και υπάρχουν διαθέσιμες ταχυδρομικές λίστες για εκατοντάδες θέματα και συγκεκριμένα ενδιαφέροντα.

Άλλος τρόπος επικοινωνίας με μεγάλες ομάδες ανθρώπων μέσω του Internet είναι οι ομάδες νέων (newsgroups). Στις ομάδες νέων τα μηνύματα δημοσιεύονται σε έναν ηλεκτρονικό πίνακα ανακοινώσεων τον οποίο πρέπει να επισκεφτεί ο χρήστης για να διαβάσει τα μηνύματα.

Όσον αφορά την χρήση του ως επικοινωνιακό μέσο το Internet προσφέρει τώρα πια και επικοινωνία σε πραγματικό χρόνο. Το κατάλληλο λογισμικό μπορεί και ψηφιοποιεί τη φωνή σε πακέτα δεδομένων τα οποία μεταδίδονται μέσω του μόντεμ, μεταβαίνουν από server σε server για να φτάσουν τελικά στο μόντεμ του ατόμου που επιθυμούμε να επικοινωνήσουμε, να περάσουν από το λογισμικό του και να μετατραπούν σε ηχητικό σήμα – φωνή. Το ίδιο συμβαίνει και με τη μετάδοση εικόνας – βίντεο. Για έναν χρήστη ιδιώτη ή οργανισμό ο οποίος έρχεται σε επαφή με ανθρώπους απ' όλο τον κόσμο, η επικοινωνία «πρόσωπο με πρόσωπο» σε τακτική βάση γίνεται εφικτή μέσω του Internet.

### **Πληροφόρηση**

Το Internet είναι η ίδια η πληροφορία. Ο όγκος των διαθέσιμων πληροφοριών που μπορεί να βρει κάποιος στο Internet είναι τεράστιος, ενώ η αναζήτηση κάποιας συγκεκριμένης πληροφορίας γίνεται εύκολη με τη χρησιμοποίηση κάποιας από τις διαθέσιμες μηχανές αναζήτησης (όπως π.χ. altavista, yahoo, lycos κλπ. και των ελληνικών portals: in.gr, thea.gr, κλπ).

### **Εκπαίδευση**

Παρέχει πολλές ευκαιρίες για εκπαίδευση σε διάφορα Πανεπιστήμια, αφού σχεδόν όλα τα εκπαιδευτικά ιδρύματα διατηρούν δικές τους σελίδες στο WWW (World Wide Web) και λειτουργούν προγράμματα εκπαίδευσης μέσω του Internet (βλ. τη διεύθυνση «[www.gunet.gr](http://www.gunet.gr)» για τα ελληνικά ΑΕΙ και ΤΕΙ). Υπάρχουν εκπαιδευτικά ιδρύματα που παρέχουν ακόμη και ζωντανές διαλέξεις απευθείας μέσω του Internet.

### **Ηλεκτρονικό Εμπόριο**

Μια ακόμη χρησιμότητα του Internet είναι η διεξαγωγή του ηλεκτρονικού εμπορίου (e-commerce). Στον οικονομικό τομέα ισχύει η φράση: «ο χρόνος είναι χρήμα», ακόμη και τα δευτερόλεπτα μπορούν να σημαίνουν πολύ χρήμα συνεπώς το Internet είναι ο ιδανικός χώρος για να κινηθεί κανείς όταν σκοπεύει να ξεκινήσει μία επιχείρηση ή όταν επιθυμεί να βρει συνεργάτες, υπαλλήλους και πελάτες. Το Internet με τη σημερινή

του μορφή αποτελεί εκτός των άλλων και μία αγορά. Οι σελίδες που φιλοξενεί κατακλύζονται από διαφημίσεις και ο καθένας μπορεί να αγοράσει ή να πουλήσει μέσω Internet βιβλία, δίσκους, ρούχα, αυτοκίνητα, μετοχές και ότι άλλο μπορεί να φανταστεί κανείς. Με λίγα λόγια αποτελεί το μέλλον των επιχειρήσεων.

### Διασκέδαση – Ψυχαγωγία

Το Internet κατακλύζεται από ιδιόμορφα και περίεργα πράγματα με τα οποία μπορούν οι χρήστες να διασκεδάσουν. Γέλιο μπορούν να προσφέρουν οι σελίδες με ανέκδοτα οι οποίες είναι αρκετά διασκεδαστικές (π.χ. Η σελίδα Joke of the Day / Netcenter, <http://netcenter.com/daily.html>). Στη διεύθυνση <http://www.yahoo.com/Entertainment/Humor Jokes and Fun/Jokes/> μπορεί κανείς να βρει πολλούς συνδέσμους που οδηγούνε προς διευθύνσεις με διαφόρων ειδών ανέκδοτα.

Ο χρήστης μπορεί στο Internet να βρει πληροφορίες για ταινίες, κριτικές κινηματογραφικών έργων και κάθε είδους άλλης μορφής ψυχαγωγίας. Μέσω του Internet θα μπορούσε κανείς να σχεδιάσει ακόμη και ταξίδια βρίσκοντας τη διαδρομή ή κλείνοντας εισιτήρια. Ψυχαγωγία και διασκέδαση προσφέρουν και οι ταχυδρομικές λίστες οι οποίες υπάρχουν σε αναρίθμητο πλήθος και ο κάθε χρήστης θα βρει κάποια από αυτές ενδιαφέρουσα.

Το όνομα του World Wide Web δεν είναι τυχαίο (world=κόσμος), ο Παγκόσμιος αυτός Ιστός δίνει τη δυνατότητα στο χρήστη να βρει οποιαδήποτε πληροφορία από οποιοδήποτε μέρος του κόσμου.

## Γ. ΓΕΝΝΗΣΗ ΚΑΙ ΕΞΕΛΙΞΗ

Η πρώτη καταγεγραμμένη περιγραφή για το πώς θα μπορούσε να καταστεί εφικτό το δίκτυο (networking) δίνεται μέσα από μια σειρά υπομνήματα γραμμένα από τον I.C.R. Licklider του MIT, τον Αύγουστο του 1962, τα οποία περιείχαν και περιέγραφαν την πνευματική του σύλληψη για το «γαλαξιακό δίκτυο» (Galactic Network). Ο Licklider οραματιζόταν μία αλληλοσυνδεόμενη σειρά υπολογιστών μέσα από τους οποίους, οποιοσδήποτε θα μπορούσε να έχει γρήγορη πρόσβαση σε δεδομένα και προγράμματα από οποιαδήποτε τοποθεσία. Η ιδέα αυτή ταυτίζεται πολύ με τη μορφή που έχει σήμερα το Internet. Ο Licklider ήταν ο επικεφαλής της DARPA<sup>1</sup> (Υπηρεσία Προηγμένων Ερευνητικών Προγραμμάτων), που αφορούσε στο ερευνητικό πρόγραμμα με θέμα την εύρεση τεχνικών και τεχνολογιών για τη σύνδεση διαφόρων τύπων δικτύων, που ξεκίνησε τις εργασίες του τον Οκτώβριο του 1962. Το χρονικό διάστημα που συμμετείχε στη DARPA κατάφερε να πείσει για τη σημασία της ιδέας του, τους διαδόχους του στην υπηρεσία αυτή, τον Ivan Sutherland, τον Bob Taylor και τον ερευνητή του MIT, Lawrence G. Roberts.

Ένα χρόνο νωρίτερα, τον Ιούλιο του 1961, ο Leonard Kleinrock, του MIT, είχε εκδώσει την πρώτη επιστημονική ανακοίνωση σχετικά με τη θεωρία των συμπιεσμένων μεταγωγέων πακέτων με διακόπτη και το πρώτο βιβλίο με το ίδιο θέμα το 1964. Ο Kleinrock, έπεισε τον Roberts για τη θεωρητική επιτευξιμότητα των επικοινωνιών χρησιμοποιώντας δέσμες (πακέτα) αντί για ηλεκτρικά κυκλώματα (circuits), πράγμα το οποίο αποτέλεσε ένα τεράστιο βήμα προς την κατεύθυνση της δικτυακής σύνδεσης. Το επόμενο βήμα «κλειδί» ήταν να κάνουν τους ηλεκτρονικούς υπολογιστές να «συνομιλούν». Προκειμένου να ερευνηθούν κάτι τέτοιο, το 1965 με τη συνεργασία του Thomas Merrill, ο Roberts συνέδεσε τον ηλεκτρονικό υπολογιστή TX-2 σε λειτουργία με έναν ηλεκτρονικό υπολογιστή Q-32 στην Καλιφόρνια με μία χαμηλής ταχύτητας τηλεφωνική γραμμή, δημιουργώντας το πρώτο (μικρό) εκτεταμένης έκτασης δίκτυο ηλεκτρονικού υπολογιστή. Το αποτέλεσμα του πειράματος αυτού ήταν ότι οι συνδεδεμένοι ηλεκτρονικοί

<sup>1</sup> Advanced Research Projects Agency.

υπολογιστές, μπορούσαν να συνεργάζονται με επιτυχία, τρέχοντας προγράμματα και ανακτώντας δεδομένα όταν χρειαζόταν στη μηχανή καθοδήγησης, όμως η αλυσίδα διακοπών του τηλεφωνικού συστήματος ήταν τελείως ακατάλληλη γι' αυτή τη δουλειά επιβεβαιώνοντας την πεποίθηση του Kleinrock για την ανάγκη χρησιμοποίησης συμπιεσμένων διακοπών.

Σχεδόν παράλληλα (1963) το Εθνικό Εργαστήριο Φυσικής Middlesex της Βρετανίας σε συνεργασία με την Επιτροπή Τηλεπικοινωνιών της Γαλλίας ξεκινούν έρευνες με στόχο τη δικτύωση με τη βοήθεια κοινών τηλεπικοινωνιακών γραμμών που θα παρείχε την δυνατότητα μεταφοράς και ανταλλαγής δεδομένων.

Στα τέλη του 1966 ο Roberts πήγε στη DARPA για να αναπτύξει την ιδέα του δικτύου υπολογιστών και γρήγορα συνέταξε το σχέδιο του για το «APRANET», το οποίο εξέδωσε το 1967. Στη διάσκεψη στην οποία παρουσίασε την εργασία του υπήρχε επίσης μια ανάλογη εργασία του Donald Davies και του Roger Scantlebury (NPL). Ο τελευταίος είπε στον Roberts για τις εργασίες του NPL.

Το 1968, το Υπουργείο Άμυνας των Η.Π.Α. διασυνδέει τους ηλεκτρονικούς υπολογιστές που περιείχαν στρατιωτικά δεδομένα στο πλαίσιο του ARPA<sup>2</sup>, (Δίκτυο Προηγμένων Ερευνητικών Σχεδίων). Η εταιρεία BBN<sup>3</sup> ανέλαβε τη σχεδίαση του πρωτοκόλλου IMP<sup>4</sup> (Information Message Protocol) προκειμένου να επιτευχθεί η δικτύωση των ηλεκτρονικών υπολογιστών.

Το 1969 η εταιρεία AT & Bell δημιουργεί το λειτουργικό σύστημα UNIX που συνέβαλε καθοριστικά στην εξέλιξη των δικτύων.

Η πρώτη δικτύωση γίνεται το 1970 όταν τέσσερα πανεπιστήμια της νοτιοδυτικής Αμερικής ενώνουν τα υπολογιστικά τους συστήματα. Η μεταφορά των δεδομένων γίνεται με πρωτόκολλο NCP (Network Control Protocol). Ο

---

<sup>2</sup> Advanced Research Projects Agency.

<sup>3</sup> Bolt Beranek and Newman.

<sup>4</sup> Το IMP είναι ο πρόδρομος του γνωστού σε όλους σήμερα ISDN – Integrated Services Digital Network- Δίκτυο Ολοκληρωμένων Ψηφιακών Υπηρεσιών.



αριθμός των δικτυωμένων υπολογιστών αυξάνεται σε 40 μέσα στα επόμενα 2 χρόνια και γεννιέται το Ηλεκτρονικό Ταχυδρομείο (e-mail).

Το 1972 συγκαλείται το Α' Διεθνές Συνέδριο για τις Ηλεκτρονικές Επικοινωνίες στην Ουάσινγκτον, στο οποίο αποφασίστηκε η δημιουργία μίας ομάδας (INWG – International Network Working Group) η οποία δημιούργησε το Διεθνές Πρότυπο Επικοινωνιών X.25. Ακολούθησε το αντίστοιχο ευρωπαϊκό δίκτυο X.25Euronet.

Η ίδια ομάδα (INWG) σχεδιάζει και τα πρωτόκολλα επικοινωνίας IP (Internetworking Protocol) και TCP (Transmission Control Protocol) που συνεχίζουν να χρησιμοποιούνται στις μέρες μας, ως ενιαίο πρωτόκολλο TCP/IP. Το TCP/IP βοηθά στην αποφυγή της κατάρρευσης του δικτύου και τη συνέχιση της λειτουργίας του σε περίπτωση που κάποιος κόμβος τεθεί εκτός λειτουργίας.

Η Υπηρεσία DARPA (είναι η Υπηρεσία ARPA που μετονομάστηκε σε DARPA), μελετά την διαδικτύωση μέσω του προγράμματος Internetting Project και αποφασίζει την ελεύθερη διάθεση του TCP/IP στο εμπόριο.

Το 1976 έρχεται στο προσκήνιο για μία ακόμη φορά η εταιρεία AT & Bell δημιουργώντας το λογισμικό UUCP (UNIX – to – UNIX Copy Program) το οποίο απλοποιεί τη σύνδεση των υπολογιστών με τη χρήση ενός modem και μιας κοινής τηλεφωνικής γραμμής.

Ένα χρόνο αργότερα τα δίκτυα APRAnet, SATnet και Prnet συνδέονται μεταξύ τους μέσω δορυφόρου. Λίγο μετά προστίθεται ένα νέο δίκτυο το (Snet Computer Science Research) και μια υπηρεσία παροχής υπηρεσιών η CompuServe<sup>5</sup>.

Το 1982 δημιουργείται το δίκτυο Usenet μέσω του οποίου εμφανίζονται για πρώτη φορά τα μηνύματα μεταξύ των newsgroups.

---

<sup>5</sup> Η CompuServe εξαγοράστηκε από την America On Line η οποία είναι μία γιγάντια επιχείρηση σήμερα με κόμβους σε όλο τον κόσμο και εκατομμύρια συνδρομητές.

Άλλα δίκτυα που ιδρύονται την ίδια δεκαετία είναι: Το BITnet (Because it's Time Network) αντίστοιχο του Usenet, το οποίο παρέχει μεταξύ άλλων υπηρεσιών και μηνύματα στους συνδρομητές του. Το FidoNet το οποίο παρέχει στους συνδρομητές του τη δυνατότητα να συνομιλούν. Τέλος το 1985 μπαίνει δυναμικά στο χώρο της δικτύωσης των ηλεκτρονικών υπολογιστών η AOL (America On Line).

Προσπάθειες επέκτασης του Διαδικτύου γίνεται το 1998 από το Ομοσπονδιακό Συμβούλιο Δικτύωσης των ΗΠΑ που κατέληξαν στην υλοποίηση του e-mail.

Εκείνη τη χρονιά εμφανίζονται και τα πρώτα προβλήματα από εισβολές στο Διαδίκτυο που έχουν ως αποτέλεσμα διαφοροποιήσεις στα ήδη υπάρχοντα λειτουργικά προγράμματα και τη δημιουργία νέων.

Το WWW-World Wide Web ή αλλιώς Παγκόσμιος Ιστός δημιουργείται το 1989 στην Ελβετία στο Ευρωπαϊκό Κέντρο Πυρηνικών Ερευνών (CERN)<sup>6</sup>. Ο Tim Berners Lee, ήταν αυτός που συνέλαβε την ιδέα για τον WWW, κατάφερε να υλοποιήσει και να το βάλει στην καθημερινή μας ζωή.

Εξελίξεις έχουμε και στις Η.Π.Α. Το Πανεπιστήμιο της Μινεάπολης δημιουργεί το λογισμικό Gopher για την εύκολη ταξινόμηση των πληροφοριών στο Διαδίκτυο ενώ το 1989 ιδρύεται στην πολιτεία της Virginia η ISOC (Internet Society) μια εθελοντική παροχή υπηρεσιών στο Διαδίκτυο.

Μέχρι το 1995 τα τέσσερα πρώτα δίκτυα που δημιουργήθηκαν έχουν παύσει να λειτουργούν, όμως το Διαδίκτυο είναι πιο δυνατό και επιτυχημένο από τότε που ξεκίνησε τα πρώτα βήματα.

Στις 5 Σεπτεμβρίου 1995 για πρώτη φορά το δίκτυο ABC Radio News, μεταδίδει ζωντανά στο Internet αγώνα μπίτζμπωλ. Το Internet είναι πλέον παγκόσμιος κατακτητής. Ως ημερομηνία γέννησης του Internet θεωρείται από πολλούς η 1η Ιανουαρίου 1983 όταν η APRAnet παύει να λειτουργεί κάτω από τη δικαιοδοσία του στρατού και αυτονομείται στο Διαδίκτυο.

---

<sup>6</sup> European Laboratory for Particle Physics.

## Δ. ΤΟ INTERNET ΣΤΗΝ ΕΛΛΑΔΑ

Το πρώτο βήμα προς την Διαδικτύωση γίνεται στη χώρα μας το 1984. Το πρώτο μήνυμα ηλεκτρονικού ταχυδρομείου λαμβάνει το (ΙΤΕ) Ίδρυμα Τεχνολογίας και Έρευνας της Κρήτης μέσω σύνδεσης UUCP. Τότε ο ΟΤΕ συνδέεται με το Ευρωπαϊκό δίκτυο X.25 Euronet. Λιγοστές διασυνδέσεις υπήρχαν και νωρίτερα, αλλά περιορίζονταν αποκλειστικά μεταξύ ακαδημαϊκών ιδρυμάτων ανάμεσα στα οποία και το ίδρυμα «Δημόκριτος» στην Αγία Παρασκευή.

Το 1992 δημιουργείται στο Ηράκλειο το Network Operation Center (NOC) και το 1994 το FORTHnet<sup>7</sup>. Το τελευταίο παρέχει ταχύτητα δικτύωσης 2Mbps από 19.200bps που παρείχε η σύνδεση X.25. Μέχρι το 1995 μόνο οι πόλεις Αθήνα, Θεσσαλονίκη και Ηράκλειο είχαν την δυνατότητα Διαδικτύωσης. Από το 1995 όμως η λειτουργία της Διαδικτύωσης επεκτείνεται και ολοκληρώνεται σ' όλη την ελληνική επικράτεια παρέχοντας πρόσβαση στο Internet.

Ταυτόχρονα, δραστηριοποιείται και το ίδρυμα του «Δημόκριτου» με το πρόγραμμα «Αριάδνη». Το δίκτυο «Αριάδνη» διασυνδέει όλα τα μεγάλα ερευνητικά κέντρα και τα πανεπιστημιακά ιδρύματα μεταξύ τους και με ιδιώτες.

Το ΙΤΕ δημιουργεί νέο δίκτυο με το όνομα ΕΔΕΤ (Εθνικό Δίκτυο Έρευνας & Τεχνολογίας) μέσω του Ευρωπαϊκού φορέα DANTE.

Το 1995 κάνει την εμφάνιση ο ΟΤΕ μέσω της θυγατρικής εταιρίας ΟΤΕnet. Το 1996 νέες εταιρείες παροχής Internet δημιουργούνται μεταξύ των οποίων και οι: HellasNet, GroovnyNet, Acropolis Net, Compulink.

Σήμερα το Internet έχει εισρεύσει, τόσο στην ζωή των Ελλήνων που αποτελεί καθημερινότητα. Οι Έλληνες χρήστες, μπορούν με οικονομία και ασφάλεια να σερφάρουν στο Internet αρκεί να διαθέτουν ένα PC, ένα modem και μία τηλεφωνική γραμμή.

<sup>7</sup> Το δίκτυο FORTHnet δημιουργήθηκε και λειτουργεί στο (ΙΤΕ) Ινστιτούτο Πληροφορικής του Ιδρύματος Τεχνολογίας και Έρευνας.

Έχουν δε τη δυνατότητα να επιλέξουν ανάμεσα σε μια πληθώρα συνδέσεων. Κι αν πριν ήταν απαραίτητη η γνώση της Αγγλικής γλώσσας για μία επίσκεψη στα sites του Παγκόσμιου Ιστού (World Wide Web) σήμερα υπάρχει το Ελληνικό Web προσαρμοσμένο στην ελληνική πραγματικότητα και γλώσσα, με ελληνικούς θεματικούς καταλόγους.

## **2. ΤΟ ΗΛΕΚΤΡΟΝΙΚΟ ΕΓΚΛΗΜΑ (ΠΑΡΑΒΑΤΙΚΟΤΗΤΑ ΣΤΟ ΔΙΑΔΙΚΤΥΟ)**

### **A. ΕΝΝΟΙΑ**

Ο κυβερνοχώρος με τη μορφή που έχει σήμερα, αποτελεί μια μικρογραφία της κοινωνίας. Αναπόφευκτα, λοιπόν, κάθε είδους παράνομη δραστηριότητα βρίσκει πρόσφορο έδαφος στο Internet. Η σύγχρονη τεχνολογία των ηλεκτρονικών υπολογιστών προσφέρει στους παραβάτες τη δυνατότητα να ελίσσονται εύκολα για την πραγματοποίηση των στόχων τους, χωρίς να διατρέχουν μεγάλο κίνδυνο. Το εύρος των χρήσεων των ηλεκτρονικών υπολογιστών και του Διαδικτύου, καθώς, και η συνεχώς αυξανόμενη χρησιμοποίησή τους σε ακόμη περισσότερους τομείς, καθιστά δύσκολο τον ακριβή προσδιορισμό της έννοιας της παράβασης.

Πρόσθετη δυσκολία όσον αφορά τον εννοιολογικό προσδιορισμό των παραβάσεων είναι το γεγονός ότι ενώ το Internet αποτελεί μία παγκόσμια κοινότητα, από κράτος σε κράτος οι ισχύοντες νόμοι διαφέρουν. Για παράδειγμα η αποστολή και η κατοχή πορνογραφικού υλικού αποτελεί αδίκημα με ποινικές κυρώσεις για κάποια κράτη, ενώ για άλλα κράτη είναι νόμιμη πράξη και κάθε ενέργεια εντοπισμού του υλικού αυτού θεωρείται αντισυνταγματική γιατί παραβιάζει το δικαίωμα του απορρήτου προσωπικών δεδομένων.

Χαρακτηριστικό παράδειγμα είναι επίσης και η διακίνηση ναρκωτικών ουσιών που γίνεται μέσω Internet, για όλα σχεδόν τα κράτη είναι παράνομη πράξη και συνεπάγεται ποινικές κυρώσεις, για την Ολλανδία όμως, όπως είναι γνωστό ισχύει η αποποινικοποίηση της διακίνησης των μαλακών ναρκωτικών ουσιών.

Ένεκα της ανεκτικότητας που διακρίνει το Internet, υπάρχει χώρος μέσα σ' αυτό σε οποιονδήποτε το θελήσει να εκφράσει ελεύθερα τις απόψεις του. Έτσι λοιπόν στο Internet συναντάμε ακροδεξιές οργανώσεις και ακραίες ομάδες (hate

groups), αναρχικούς και ακροαριστερές οργανώσεις, τρομοκράτες και ρατσιστές, κάθε λογής ανθρώπους ή ομάδες ανθρώπων, οι οποίοι εξασκώντας το δικαίωμα τους για «ελευθερία του λόγου» συχνά παραβιάζουν συνταγματικά δικαιώματα άλλων ανθρώπων. Σ' αυτές τις περιπτώσεις είναι δύσκολο να ορίσει κανείς που ξεκινούν τα όρια της παράνομης πράξης. Ένα παράδειγμα είναι αυτό της 25χρονης Γερμανίδας, μέλος του αριστερού κόμματος του Δημοκρατικού Σοσιαλισμού, η οποία κατηγορήθηκε ότι προέτρεπε μέσω του Internet τους πολίτες της Γερμανίας στην τέλεση αξιόποινων πράξεων, δηλαδή στην ανάγνωση ενός αριστερού περιοδικού του Radikal, του οποίου η έκδοση έχει απαγορευτεί στη Γερμανία.

Παρ' όλα αυτά, ένας ευρύτερος ορισμός των παραβάσεων με ηλεκτρονικούς υπολογιστές είναι ο εξής: «κάθε παράνομη πράξη για την τέλεση της οποίας είναι απαραίτητη η γνώση της τεχνολογίας των ηλεκτρονικών υπολογιστών». (Βλ. Χ. Τσουραμάνης, Οικονομική Παραβατικότητα, 1996, σελ. 86).

Στις παράνομες πράξεις περιλαμβάνονται εκτός από τις ποινικοποιημένες μορφές παραβατικής συμπεριφοράς και κάθε άλλη πράξη που αντιβαίνει στο νόμο, η οποία δεν συνεπάγεται υποχρεωτικά ποινικές αλλά και αστικές ή διοικητικές κυρώσεις. (Βλ. Χ. Τσουραμάνης, Οικονομική Παραβατικότητα, 1996, σελ. 86).

## **B. ΜΟΡΦΕΣ**

Η ραγδαία ανάπτυξη των ηλεκτρονικών υπολογιστών και του Διαδικτύου έχει προσφέρει στους «κακούς» τη δυνατότητα της χρησιμοποίησης αυτής της τεχνολογίας για την επίτευξη των στόχων τους. Ο χώρος του Internet είναι γεμάτος από hackers, παιδεραστές, ρατσιστές, εμπόρους ναρκωτικών και κάθε είδους παραβάτες. Είναι δύσκολο να πει κανείς πότε ακριβώς άρχισαν να εμφανίζονται οι πρώτες παράνομες πράξεις στο Internet, υποθετικά άρχισαν με την γέννηση του διαδικτύου. Ασφαλώς τότε η κατάσταση ήταν ελεγχόμενη εξαιτίας του περιορισμένου αριθμού των χρηστών του Internet. Στις μέρες μας όμως η κατάσταση είναι πιο περίπλοκη, αφού στην on-line κοινότητα ανήκει σχεδόν ολόκληρος ο πληθυσμός του πλανήτη.

Το γεγονός αυτό της μεγάλης αύξησης των χρηστών του Internet καθιστά τις απόπειρες ελέγχου ιδιαίτερα δύσκολες. Η νέα αυτή τεχνολογία επιπλέον προσφέρει κάλυψη στους παραβάτες που συνήθως διαφεύγουν τον κίνδυνο του εντοπισμού τους και της τιμωρίας.

Και δεν είναι λίγες οι περιπτώσεις όπου ο έλεγχος αυτών των πράξεων έρχεται αντιμέτωπο με κρίσιμα ερωτήματα όπως η ελευθερία του λόγου, το δικαίωμα του απόρρητου και άλλες δημοκρατικές αρχές, ακροβατώντας στα όρια της λογοκρισίας.

Οι περιπτώσεις στις οποίες εντοπίζονται οι παράνομες δραστηριότητες στο χώρο του Internet, σύμφωνα με ανακοίνωση της Επιτροπής της Ευρωπαϊκής Ένωσης προς το Συμβούλιο και την Οικονομική και Κοινωνική Επιτροπή στα τέλη του 1997 είναι οι εξής:(Βλ. Ν.Κουράκη, Το οικονομικό έγκλημα στην Ελλάδα σήμερα, Ποινική Δικαιοσύνη,Τ6 2000,σελ.649-651

- **Θέματα Εθνικής ασφάλειας.** Όπως για παράδειγμα η αποκωδικοποίηση απόρρητων στρατιωτικών πληροφοριών, οδηγίες για κατασκευή βομβών ή εκρηκτικών μηχανισμών, παρασκευή ναρκωτικών. (σχετικές αναπτύξεις στο βιβλίο της Μ. Μπόση, Ζητήματα Ασφάλειας στη Νέα Τάξη πραγμάτων, Αθήνα: Παπαζήσης, 1999, σελ. 229 .).



κυκλώματος παιδεραστών στο Βέλγιο το καλοκαίρι του 1997 όπου διαπιστώθηκε ότι το Internet χρησιμοποιείται για τη διανομή υλικού σεξουαλικού περιεχομένου με ανήλικους. Σε πολλές χώρες η κατοχή τέτοιου είδους υλικού συμπεριλαμβανομένου και αυτών με ψηφιοποιημένο περιεχόμενο διώκεται ποινικά και συχνά γίνονται επιδρομές από τις διωκτικές αρχές. Παρ' όλα αυτά οι διανομές και οι παραλήπτες του πορνογραφικού υλικού εντοπίζονται εξαιρετικά δύσκολα αφού αλλάζουν διαρκώς ονόματα και διευθύνσεις e-mail. Μέχρι τώρα οι μέθοδοι που έχουν χρησιμοποιηθεί για τον εντοπισμό αυτών των ανθρώπων αποδείχτηκαν πρακτικά ανίσχυρες, αφήνοντας σχεδόν ανενόχλητους τους παραβάτες να διακινούν «υπογείως» τέτοιου είδους υλικό.

- **Θέματα προστασίας της ανθρώπινης αξιοπρέπειας.** Π.χ. υποκίνηση μέσω ιστοσελίδων του Internet σε φυλετικό μίσος ή φυλετικές διακρίσεις, όπου μπορεί να βρει κανείς ακροδεξιές οργανώσεις που αμφισβητούν το Ολοκαύτωμα και μιλούν για την ανωτερότητα των λευκών. Στην on-line σύνδεση υπάρχουν εκπρόσωποι κάθε κατηγορίας ανθρώπων, όπως αναρχικών, ακραίες ομάδες (hate group), ακροαριστερές οργανώσεις, απελευθερωτικά κινήματα, τρομοκρατικές οργανώσεις, ρατσιστές οι οποίοι χρησιμοποιούν την υψηλή τεχνολογία για να προωθήσουν τις απόψεις τους πολλές φορές σε βάρος άλλων ανθρώπων!
- **Θέματα προστασίας της ιδιωτικής ζωής.** Π.χ. ηλεκτρονική σεξουαλική παρενόχληση, παράνομη διακίνηση προσωπικών στοιχείων. Στην Ελλάδα ισχύει ο Ν. 2472/1997 σύμφωνα με τον οποίο προστατεύεται το άτομο από την επεξεργασία δεδομένων προσωπικού χαρακτήρα. Το θέμα περί προστασίας της προσωπικής ζωής είναι λεπτό και οι αντιπαραθέσεις σχετικά μ' αυτό δεν φαίνεται να έχουν τέλος. Παρ' όλα αυτά αντίστοιχος νόμος ισχύει και την Ευρωπαϊκή Κοινότητα.
- **Θέματα φθοράς ιδιοκτησίας.** Π.χ. προσβολή των προγραμμάτων ηλεκτρονικών υπολογιστών με ιούς, πνεύμα ανταγωνιστικότητας ή διάθεση «πλάκας». Σ' αυτές τις περιπτώσεις οι δράστες προέρχονται συχνά μέσα από τους κόλπους των επιχειρήσεων και επιδιώκουν οικονομικά

οφέλη, είτε διοχετεύοντας μυστικά της επιχείρησης σε ανταγωνιστικές επιχειρήσεις, είτε εκβιάζοντας την ίδια την επιχείρηση. Τις περισσότερες φορές οι δράστες είναι οι ονομαζόμενοι «hackers», οι οποίοι σπάζοντας τους κωδικούς, παραβιάζουν ηλεκτρονικά συστήματα και αποκτούν παράνομη πρόσβαση σ' αυτά. Πολλές φορές το μοναδικό κίνητρο είναι μόνο η «πλάκα».

- **Θέματα προστασίας της καλής φήμης και της υπόληψης.** Π.χ. δυσφήμιση, παράνομη συγκριτική διαφήμιση. Η συκοφαντική δυσφήμιση συγκριτικά με τα αδικήματα που διαπράττονται στο Internet αποτελεί «πταίσμα».
- **Θέματα πνευματικής ιδιοκτησίας.** Π.χ. παράνομη διακίνηση κατοχυρωμένων λογοτεχνικών έργων, μουσικών ακουσμάτων κλπ.
- **Θέματα βιομηχανικής κατασκοπείας,** με στόχους εταιρείες που παράγουν προϊόντα υψηλής τεχνολογίας και όχι μόνο.
- **Θέματα ηλεκτρονικής κλοπής πιστωτικών καρτών:** Η αρπαγή των στοιχείων των χρηστών που προβαίνουν μέσω πιστωτικών καρτών σε συναλλαγές με επιχειρήσεις μέσω του ηλεκτρονικού εμπορίου, χρησιμοποίηση των στοιχείων αυτών για την πραγματοποίηση συναλλαγών με τράπεζες και επιχειρήσεις σε βάρος των νόμιμων ιδιοκτητών τους. Αυτή είναι η συνηθέστερη μορφή σύγχρονου οικονομικού εγκλήματος στο Internet με άπειρα παραδείγματα. Ωστόσο στην Ευρωπαϊκή Ένωση ισχύει νόμος ο οποίος δίνει το δικαίωμα στον κάτοχο της πιστωτικής κάρτας να αρνηθεί χρέωση, που έχει γίνει χωρίς την υπογραφή του, δηλαδή μέσω τηλεφώνου ή διεύθυνσης e-mail.
- **Θέματα ηλεκτρονικής κλοπής τραπεζικών κωδικών.** Χαρακτηριστική η περίπτωση ρώσων hackers, οι οποίοι έκλεψαν κωδικούς πελατών της αμερικανικής τράπεζας Citibank και μετέφεραν 10 εκατομμύρια δολάρια σε λογαριασμό του εξωτερικού.
- **Θέματα ηλεκτρονικής απάτης σε χρηματιστηριακές συναλλαγές,** κυρίως με παραπλάνηση χρηστών του

Διαδικτύου, στους οποίους παρέχονται ψευδείς πληροφορίες. Οι επιτήδαιοι παραπλανούν τα θύματά τους με σκοπό να πλουτίσουν σε βάρος τους.

Με την γέννηση του Διαδικτύου και την εξέλιξή του έχουμε και την παράλληλη γέννηση και εξέλιξη μορφών παραβατικότητας και εγκλήματος. Τα οικονομικά αδικήματα είναι σύνηθες φαινόμενο και γι' αυτό από τις παραπάνω περιπτώσεις οι επτά τελευταίες αποτελούν μορφές σύγχρονου οικονομικού εγκλήματος.

## **Γ. ΔΡΑΣΤΕΣ**

### **Οι hacker: Ποιοι είναι, ποια η δεοντολογία του hacking, ποια τα κίνητρό τους, τι ικανότητες έχουν.**

Έχουν περάσει 30 χρόνια από την εμφάνιση του Internet και όμως πολλοί είναι αυτοί που δεν γνωρίζουν τι ακριβώς είναι ένας hacker.

Οι hacker περιγράφονται ως ακίνδυνοι φαρσέρ, μανιακοί με την τεχνολογία των ηλεκτρονικών υπολογιστών, υπέρμαχοι της ελευθερίας ή ως επικίνδυνοι τρομοκράτες. Όπως είναι φανερό αυτοί οι άνθρωποι έφεραν σε αμηχανία τον κόσμο αφού δεν υπάρχει ακριβής περιγραφή του τι είναι hacker. Συνήθως για τον όρο hacker στα λεξικά υπάρχει και η εξής περιγραφή: «Αυτός που επεμβαίνει καταχρηστικά στη μνήμη ή το πρόγραμμα ενός άλλου υπολογιστή». Ο όρος hacker εμφανίστηκε στην πρώιμη περίοδο της τεχνολογίας των ηλεκτρονικών υπολογιστών και χρησιμοποιούταν για το θετικό χαρακτηρισμό ατόμων με ιδιαίτερες γνώσεις γύρω από τους ηλεκτρονικούς υπολογιστές. Η εξέλιξη της τεχνολογίας οφείλεται σε μεγάλο βαθμό στους hackers, οι οποίοι προσπαθούσαν πάντα να ξεπεράσουν τον εαυτό τους προκειμένου να επιτύχουν το στόχο τους.

### **Τι είναι όμως ο hacker**

Κάπως έτσι αυτοσυστήνονται: «Hacker είναι εκείνος που γνωρίζει για τους ηλεκτρονικούς υπολογιστές περισσότερα από ότι ο μέσος χρήστης. Με έναν ηλεκτρονικό υπολογιστή μπορεί να κάνει πράγματα που βρίσκονται πέραν των δυνατοτήτων ενός μέσου χρήστη. Όμως το βασικό ενδιαφέρον εστιάζεται στη διαχείριση της πληροφορίας. Δεν είναι εγκληματικοί τύποι. Δεν καταστρέφουν ένα σύστημα στο οποίο διεισδύουν. Εξετάζουν τις πληροφορίες που βρίσκονται σ' αυτό, αφήνουν ένα επισκεπτήριο για να αποδείξουν τη διείσδυσή τους και μετά αποχωρούν παίρνοντας μαζί τους τα αρχεία που ήθελαν». Αυτά αναφέρει κάποιος «botkil 131» στη σελίδα του (<http://www.concentric.net~tang/hack.html>). Μία περισσότερο αναλυτική περιγραφή δίνει κάποιος άλλος: «Υπάρχει μία κοινότητα, μία κοινή κουλτούρα ανάμεσα στους ειδικούς προγραμματιστές και τους γκουρού του Διαδικτύου, που

πιστεύουν στην κοινοκτημοσύνη της πληροφορίας. Αυτή η κοινότητα γέννησε τον όρο hacker. Hackers έστησαν το Internet, αυτοί δημιούργησαν το Unix, αυτοί έτρεξαν το Usenet, αυτοί κάνουν το WWW να λειτουργεί όπως λειτουργεί σήμερα. Όποιος ανήκει ενεργά σ' αυτή την κουλτούρα και οι άλλοι τον αναγνωρίζουν ως hacker, αυτός είναι hacker». (Διεύθυνση άρθρου: <http://www.tuxedo.org/~esr/fags/hacker-howto.htm>).

Οι hacker μπορεί να είναι είτε επαγγελματίες είτε ερασιτέχνες στον τομέα της πληροφορικής, κάθε είδους άνθρωποι κυρίως νεαρής ηλικίας. Κάθε τους παράνομη ενέργεια βασίζεται στο σκεπτικό ότι γι' αυτούς καμία πόρτα δεν μπορεί να μείνει για πάντα κλειστή, κατά την διάρκεια των περιηγήσεών τους στο διαδίκτυο. Η νοοτροπία τους αυτή έχει διαμορφώσει ορισμένους κανόνες κοινά αποδεκτούς από όλους τους hackers.

Για τους hackers ο κόσμος της πληροφορικής είναι γεμάτος προβλήματα τα οποία πρέπει να λυθούν. Αυτό τους συναρπάζει και αποτελεί κίνητρο για τις δραστηριότητές τους. Βρίσκοντας λύσεις στα διάφορα προβλήματα βελτιώνουν τις ικανότητές τους και αυξάνουν τις γνώσεις τους στον τομέα της πληροφορικής.

Άλλος κανόνας της κουλτούρας τους είναι ότι «κανένας δεν χρειάζεται να λύσει το ίδιο πρόβλημα δύο φορές». Πιστεύουν δηλαδή ότι πρέπει να μοιράζονται μεταξύ τους πληροφορίες έτσι ώστε να μην ξοδεύει ένας hacker χρόνο για να λύσει ένα πρόβλημα το οποίο ήδη έχει καταφέρει να λύσει κάποιος άλλος. Επιπλέον επειδή θεωρούν τον χρόνο τους πολύτιμο και επειδή ο κόσμος του Internet είναι πολύ μεγάλος η ίδια «αποστολή» δεν πρέπει να επαναλαμβάνεται από διαφορετικούς hacker. Εξαίρεση αποτελεί η περίπτωση όπου ένας hacker αναγκάζεται να ακολουθήσει μία ήδη γνωστή διαδικασία προκειμένου να φτάσει σε ένα νέο στόχο. Η ανία αλλά και η υπερβολική ενασχόληση χωρίς αποτελέσματα είναι κατακριτέα.

Θεμελιώδης κανόνας της κουλτούρας που έχουν αναπτύξει οι hackers είναι η ελευθερία σε όλες τους τις κινήσεις. Αποδοκιμάζουν τον απολυταρχισμό και τη λογοκρισία, τη βία, τη μυστικότητα και οποιονδήποτε είναι σε θέση να δίνει διαταγές.

Τελευταίος κανόνας που πρέπει να ακολουθήσει κάποιος προκειμένου να γίνει αποδεκτός από την κοινότητα των hackers

είναι η κατανόηση όλων των παραπάνω κανόνων. Η νοοτροπία και μόνο του hacker δεν είναι αρκετή, αλλά χρειάζεται ευστροφία, αφοσίωση και σκληρή εργασία.

Τα κίνητρα που ωθούν τους hackers στις παράνομες δραστηριότητές τους ποικίλλουν και σε σχέση με αυτά οι hackers μπορούν να χωριστούν σε ομάδες:

### **1η Ομάδα: Κοινωνικά Κίνητρα.**

Σ' αυτήν την ομάδα ανήκουν άτομα τα οποία κάνουν hacking προκειμένου να γίνουν γνωστοί και κοινωνικά αποδεκτοί. Είναι εμφανές ότι το μοναδικό κίνητρο για τις ενέργειές τους είναι η απόκτηση δημοσιότητας.

### **2η Ομάδα: Οικονομικά Κίνητρα.**

Τα άτομα αυτής της ομάδας έχουν σαν κίνητρο για τις παράνομες δραστηριότητές τους το κέρδος. Προσπαθούν να ωφεληθούν οικονομικά παραβιάζοντας τα δεδομένα επιχειρήσεων με υποκλοπές σε συστήματα ηλεκτρονικών υπολογιστών κ.α.

Σε αντίθεση με την 1η ομάδα δεν επιδιώκουν τη δημοσιότητα αλλά κρατούν κρυφή την ταυτότητά τους.

### **3η Ομάδα: Τεχνολογικά Κίνητρα.**

Είναι ένα από τα σπανιότερα «είδη» hacker, τα άτομα αυτής της ομάδας δρουν με το κίνητρο ότι μ' αυτό τον τρόπο βοηθούν στη διάδοση της τεχνολογίας. Πιστεύουν ότι παραβιάζοντας συστήματα ηλεκτρονικών υπολογιστών δείχνουν τις αδυναμίες που έχουν αυτά και βοηθούν τις εταιρείες να διορθώσουν τα λάθη. Λόγο του κοινωνικού χαρακτήρα των δραστηριοτήτων τους πολλές φορές ταυτίζονται με την 1η ομάδα.

### **4η Ομάδα: Πολιτικά Κίνητρα.**

Σ' αυτή την ομάδα ανήκουν άτομα με ισχυρές πολιτικές πεποιθήσεις ή άτομα που αισθάνονται καταπιεσμένα από το υπάρχον πολιτικό σύστημα στη χώρα τους. Συνηθίζουν να

παραβιάζουν τα συστήματα ηλεκτρονικών υπολογιστών αντίπαλων πολιτικών κομμάτων και φροντίζουν ώστε οι παραβιάσεις αυτές να γίνονται γνωστές μέσω των Μέσων Μαζικής Ενημέρωσης. Μ' αυτό τον τρόπο προβάλλουν και γνωστοποιούν τις θέσεις τους στο κοινό.

Σ' αυτή την ομάδα εντάσσεται ως υποομάδα και αυτή της «ψηφιακής τρομοκρατίας». Αυτό βέβαια δε σημαίνει ότι οποιοσδήποτε παραβιάζει ένα σύστημα με πολιτικά κίνητρα είναι και τρομοκράτης.

### **5η Ομάδα: Κατασκοπευτικά Κίνητρα.**

Θα μπορούσαμε να χαρακτηρίσουμε την ομάδα αυτή ως την εξέλιξη της 4ης Ομάδας. Σ' αυτήν την ομάδα ανήκουν οι κατάσκοποι που δουλεύουν για κυβερνήσεις χωρών οι οποίες στρέφονται εναντίον άλλων κυβερνήσεων.

Οι ονομαζόμενοι hackers είναι οι άνθρωποι που βρίσκονται πίσω από παράνομες δραστηριότητες στο χώρο του Internet. Υπάρχουν μορφές Ηλεκτρονικής Παραβατικότητας που παρατηρούνται όλο και συχνότερα στο Internet που θα ήταν άδικο να καταλογιστούν σ' αυτούς. Μία από αυτές η Αποπλάνηση και Έκθεση Ανηλίκων. Στον τεράστιο κυβερνοχώρο όπου με εντυπωσιακή ταχύτητα κινούνται οι πληροφορίες, ο δρόμος είναι ανοιχτός για κάθε λογής απατεώνες και εγκληματίες.

Είναι δύσκολο να βάλει κάποιος φραγμό και να διαχωρίσει τους ηλεκτρονικούς εγκληματίες από τους χρήστες.

Στην υπερλεωφόρο της πληροφορίας κινούνται και δρουν σχεδόν ανενόχλητοι εντοπίζοντας τα θύματά τους, κάθε είδους άνθρωποι, ανάμεσα τους και παιδεραστές και πορνογράφοι. Η πορνεία αποτελεί ένα από τα αρχαιότερα επαγγέλματα. Τώρα που οι ανθρώπινες δραστηριότητες μεταφέρονται και εκτελούνται μέσω του Internet θα ήταν απίθανο να μη καταλάβει και η πορνεία μία θέση στο Internet.

Ανησυχητική είναι η αύξηση κρουσμάτων αποπλάνησης ανηλίκων και ακόμη πιο ανησυχητικό είναι το ότι σπάνια σε τέτοιες περιπτώσεις αποδίδεται δικαιοσύνη.



## Δ. ΘΥΜΑΤΑ

Τα θύματα παραβάσεων στο δίκτυο είναι:

- α) εμπορικές επιχειρήσεις και βιομηχανίες,
- β) τράπεζες και πιστωτικοί οργανισμοί,
- γ) κρατικές υπηρεσίες,
- δ) ιδιώτες που είναι ιδιοκτήτες προϊόντων παροχής υπηρεσιών ή πνευματικής ιδιοκτησίας που προβάλλουν στο δίκτυο,
- ε) απλοί χρήστες του δικτύου συμπεριλαμβανομένων και των ανηλίκων.

Χαρακτηριστικό είναι ότι το θύμα στις περισσότερες περιπτώσεις είναι άγνωστο με τον θύτη και δυστυχώς, αδυνατεί να λάβει αποτελεσματικά προληπτικά μέτρα αφού η τεχνολογία των ηλεκτρονικών υπολογιστών διαρκώς εξελίσσεται και είναι ιδιαίτερα πολύπλοκη.

Στην Ελλάδα το πρώτο κρούσμα χάκινγκ (hacking) εντοπίζεται τον Ιανουάριο του 1994 σε σύστημα ηλεκτρονικών υπολογιστών του Δημόκριτου. Ένας νεαρός προκειμένου να διαμαρτυρηθεί για την αύξηση της τιμής της συνδρομής στο Internet, κατάφερε να βρει έναν κωδικό μέσω του οποίου τρέλανε το Δίκτυο και κατάφερε να το κλείσει για μία εβδομάδα. Μετά από αυτό, τον Δεκέμβριο του 1995 την τιμητική του έχει το Ωνάσειο, την περίοδο που ο Πρωθυπουργός νοσηλεύεται εκεί. Στις 14 Δεκεμβρίου η ηλεκτρονική σελίδα της «Ελευθεροτυπίας» ανακοινώνει στις 1:45 τα ξημερώματα το θάνατο του Πρωθυπουργού και την διακόμιση της συζύγου του στον Ευαγγελισμό με σοκ. Ο μηχανισμός της εφημερίδας κινητοποιείται για να κατεβάσει την ψευδή είδηση και τα καταφέρνει στις 4:29 έχει όμως ήδη προκληθεί πανικός. Η σύζυγος του Πρωθυπουργού δύο χρόνια αργότερα ξαναπέφτει θύμα κάποιου χάκερ (hacker) ο οποίος παραβιάζει τη σελίδα της στο Internet και τοποθετεί εκεί γυμνές φωτογραφίες της.

Το καλοκαίρι του 1997 δέχεται επίθεση η ιστοσελίδα της Αγγελικής Νικολούλη (εκπομπή: «Παιχνίδια Ζωής»). Οι hackers αντικαθιστούν τον τίτλο της εκπομπής με τη φράση «Έξω τα σκουπίδια της TV από το Δίκτυο» που συνοδευόταν από ένα υποτιμητικό κείμενο για την παρουσιάστρια.

Το 1998, τον Νοέμβριο το Υπουργείο Παιδείας δέχεται επίθεση από την οργάνωση «Δικτυακή Πάλη», οι οποίοι μετονομάζουν το Υπουργείο σε «Υπουργείο της Βίας και της Καταστολής» συμπληρώνοντας τη σελίδα με φωτογραφίες του φοιτητή Δημήτρη Κασούρη που χτυπήθηκε από την οργάνωση «Χρυσή Αυγή».

Πολλές ακόμη είναι οι περιπτώσεις ηλεκτρονικών παραβιάσεων οι παραπάνω δεν είναι παρά μόνο μερικά από τα πρώτα δείγματα τρανταχτού hacking στον ελλαδικό χώρο.

Εναντίον της Ελλάδας έχουν υποβληθεί στο έτος 2000 εβδομήντα οκτώ (78) αιτήσεις για παραβιάσεις στο Ευρωπαϊκό Δικαστήριο Ανθρωπίνων Δικαιωμάτων από πολίτες που ζουν στην χώρα μας. Πολλές από τις οποίες σχετίζονται με το χώρο του Internet.

Πρώτη στην καταπάτηση των Ανθρωπίνων Δικαιωμάτων έρχεται η Ρωσία με 953 αιτήσεις παραβιάσεως, έπειτα η Γαλλία με 703, η Ιταλία με 533, η Τουρκία με 497, η Ρουμανία με 456, η Πολωνία με 443 και η Ουκρανία με 432. Όσον αφορά τις υπόλοιπες ευρωπαϊκές χώρες ο αριθμός των αιτήσεων για παραβιάσεις ανθρωπίνων δικαιωμάτων προς το Δικαστήριο είναι μονοψήφιος. Συνολικά όμως, έχουν προγραμματιστεί για να εκδικαστούν 15.107 υποθέσεις στα 41 κράτη – μέλη του Συμβουλίου της Ευρώπης. Από τις 15.107 υποθέσεις που εκκρεμούν οι 2.661 αφορούν την Τουρκία. Ακολουθούν η Ιταλία (1.933), η Γαλλία (1.365), η Πολωνία (1.263), η Ρωσία (1.064), η Αυστρία (406), η Βουλγαρία (403), η Γερμανία (543), η Ρουμανία (824), η Αγγλία (858) και η Ουκρανία (492). Εναντίον της Ελλάδας έχουν προγραμματιστεί να εκδικαστούν μόνο 149 υποθέσεις, συγκριτικά μικρός αριθμός με τις άλλες Ευρωπαϊκές χώρες.

Αξίζει να σημειωθεί ότι το Δικαστήριο Ανθρωπίνων Δικαιωμάτων δέχεται καθημερινά 170 τηλεφωνήματα και 720

επιστολές περίπου από Ευρωπαίους πολίτες που επιθυμούν να αποδοθεί δικαιοσύνη. Ο φόρτος εργασίας του Δικαστηρίου αυξάνεται δυσανάλογα με τις δυνατότητές του και αν υποθέσουμε ότι ένα 5% των περιστατικών αυτών αφορούν κατάπαυση ανθρωπίνων δικαιωμάτων μέσω του Internet είναι φανερό ότι τα θύματα ηλεκτρονικών παραβιάσεων σπάνια δικαιώνονται.

## **E. ANTIMETΩΠΙΣΗ**

Στην Αμερική, όπου γίνονται οι περισσότερες ηλεκτρονικές απάτες, υπάρχει ένα δίκτυο προστασίας του χρήστη, μία υπηρεσία στο υπουργείο Δικαιοσύνης η οποία ελέγχει το δίκτυο για απάτες. Ονομάζεται Υπηρεσία Παρακολούθησης Απάτης στο Internet και αποτελεί τμήμα της Ένωσης Προστασίας Καταναλωτών (<http://www.fraud.org>). Στην διεύθυνση αυτή μπορούν χρήστες από όλο τον κόσμο να καταγγείλουν όποια παρανομία πέσει στην αντίληψή τους και να ζητήσουν συμβουλές ή πληροφορίες. Η Ένωση Καταναλωτών σε συνεργασία με την Ομοσπονδία Εισαγγελέων της Αμερικής, συμβουλεύει τα εξής στους χρήστες:

- 1) Προστατέψτε τον απόρρητο κωδικό πρόσβασης στο δίκτυο. Διαλέξτε έναν κωδικό που δύσκολα μαντεύετε και αλλάζετε τον συχνά.
- 2) Μη παρασύρεστε από υποσχέσεις για δώρα, δωρεάν ταξίδια, προσφορές και φανταχτερές ηλεκτρονικές σελίδες.
- 3) Μην αποκαλύπτετε λογαριασμούς τραπεζής, πιστωτικών καρτών ή άλλα προσωπικά οικονομικά στοιχεία σε κανένα Web site ή on line υπηρεσία, εκτός αν γνωρίζετε ότι οι πληροφορίες που αναφέρονται είναι αληθινές. Το Εθνικό Κέντρο Πληροφοριών για Απάτες διαθέτει βάση δεδομένων για καταγγελίες στο δίκτυο και μπορεί να σας δώσει πληροφορίες.
- 4) Καταγγείλατε όποια παρανομία πέσει στην αντίληψή σας.

Όσοι σχετίζονται με το Internet και κυρίως όσοι έχουν πέσει θύματα κάποιου επίδοξου η αδιάκριτου hacker, πιστεύουν ότι ιδιωτική ζωή δεν υπάρχει και αισθάνονται εκτεθειμένοι διαρκώς όταν βρίσκονται στο διαδίκτυο. Ο φόβος επεκτείνεται πέρα από τα φυσικά πρόσωπα και στις επιχειρήσεις και τις κυβερνήσεις κρατών, των οποίων η εξάρτηση από τους ηλεκτρονικούς υπολογιστές αυξάνεται συνεχώς. Χαρακτηριστική απόδειξη είναι οι επιθέσεις που δέχθηκε το Πεντάγωνο: στο διάστημα 1992-1994 καταγράφηκαν 38.000 εισβολές μέσω ηλεκτρονικών υπολογιστών οι οποίες σκόπευαν στην

καταστροφή κωδικών, φακέλων και συστημάτων ή απλά στην ανάγνωση απόρρητων στοιχείων. Το 65% αυτών των επιθέσεων στέφθηκαν με επιτυχία. Οι επιθέσεις αυξάνονται ταχύτατα παρά τα μέτρα προστασίας που λαμβάνονται κάθε φορά και τα οποία κοστίζουν πολλά εκατομμύρια δολάρια.

Ένας επίδοξος hacker μπορεί να αποκτήσει πρόσβαση σε οποιοδήποτε σύστημα, γι' αυτό πρέπει ο χρήστης να κάνει κάποιες βασικές ενέργειες προκειμένου να αποφύγει κάτι τέτοιο:

- 1) Συχνή αλλαγή του κωδικού με τον οποίο μπαίνει στο Internet.
- 2) Χρήση ενός καλού προγράμματος antivirus, το οποίο είναι ενημερωμένο ώστε να εντοπίζει τον ιό μελλοντικά.
- 3) Τοποθέτηση κάποιου από τα προγράμματα εντοπισμού και αφαίρεσης των ιών στον κατάλογο εκκίνησης των Windows ώστε να γίνεται έλεγχος κάθε φορά που ανοίγει το σύστημα.
- 4) Εγκατάσταση προγράμματος firewall με το οποίο εμποδίζονται εισβολές τρίτων σ'ένα δίκτυο ή μεμονωμένο Η/Υ (π.χ. το ZoneAlarm)

Στο χώρο του Internet το Web θεωρείται αρκετά ασφαλές σε αντίθεση με το usenet όπου γίνονται και οι περισσότερες ηλεκτρονικές απάτες. Καλό είναι να αποφεύγετε το usenet όσον αφορά τα ηλεκτρονικά κλαμπ συζήτησης και προσοχή στις αγγελίες για πώληση κάποιων προϊόντων, στους διαγωνισμούς και τα δώρα.

### 3. ΠΑΡΑΒΑΤΙΚΟΤΗΤΑ ΣΤΟ ΔΙΑΔΙΚΤΥΟ ΤΟ 1999

#### Α. ΜΕΘΟΔΟΛΟΓΙΑ ΣΥΛΛΟΓΗΣ ΣΤΟΙΧΕΙΩΝ

Οι περιπτώσεις που παραθέτονται στο κεφάλαιο «Παρουσίαση» προέρχονται από το Web site APBnews.com ([www.apbnews.com](http://www.apbnews.com)). Πρόκειται για τις περιπτώσεις παραβιάσεων που καταγράφηκαν καθ' όλη τη διάρκεια του έτους 1999 στο site.

Το site APBnews.com, με έδρα την πολιτεία New York, είναι αφιερωμένο στην παροχή πληροφοριών σχετικά με τα εγκλήματα, τη δικαιοσύνη και την ασφάλεια με σκοπό την ενημέρωση. Οι δημιουργοί του site πιστεύουν ότι το σύστημα ποινικής δικαιοσύνης ανήκει στους πολίτες και η ενημέρωσή τους σ' αυτό το θέμα θα βοηθήσει στην βελτίωσή του.

Το site APB έχει αναγνωριστεί από αμερικάνικους δημοσιογραφικούς κύκλους και από το μεταπτυχιακό τμήμα δημοσιογραφίας και MME του πανεπιστημίου Columbia. Έχει κερδίσει το βραβείο "Sigma Delta Chi", το 1999, το οποίο απονέμει η Ένωση Επαγγελματιών Δημοσιογράφων (Society Professional Journalists) και το έτος 2000 κέρδισε το πρώτο βραβείο διεθνής δημοσιογραφίας<sup>8</sup> για Web Reporting (=ανταπόκριση στο Διαδίκτυο).

Η μετάφραση των περιπτώσεων από τα Αγγλικά στα Ελληνικά είναι ελεύθερη και όχι ακριβής σε μία προσπάθεια να αποδοθεί το νόημα έτσι ώστε ο αναγνώστης να το κατανοήσει και να μην κουράζεται με περιττές λεπτομέρειες. Η επιλογή των πληροφοριών έγινε με γνώμονα να συμπεριληφθούν στην πτυχιακή οι σχετικές με το θέμα πληροφορίες.

<sup>8</sup> Το βραβείο απονέμει η Investigative Reporters and Editors (= Ερευνητικοί Ανταποκριτές και Συντάκτες).

## **B. ΠΑΡΟΥΣΙΑΣΗ**

### **ΠΕΡΙΠΤΩΣΗ 1<sup>η</sup> ( 1/1/99 )**

#### **Ενήλικη γυναίκα συλλαμβάνεται για ερωτική σχέση με ανήλικο**

Κατηγορίες από την Ομοσπονδιακή κυβέρνηση για σύναψη σεξουαλικών σχέσεων με δεκαπεντάχρονο αγόρι, αντιμετωπίζει μία γυναίκα από το Πιτσμπουργκ. Σύμφωνα με τον κυβερνητικό εκπρόσωπο Larrel σε συνέντευξή του στο κανάλι APB News, είναι παράνομο ένα άτομο εικοσιένα χρονών και πάνω να έχει σεξουαλική επαφή με άτομο από δεκαπέντε χρονών και κάτω. Είπε ακόμη ότι ειδοποιήθηκε το FBI γιατί η υπόθεση διαβαίνει τα σύνορα της πολιτείας.

Η μοναχική Adriane, τριάντα χρονών, κατηγορείται για σεξουαλικό αδίκημα τρίτου βαθμού με ποινή φυλάκισης δέκα χρόνια, πρόστιμο μέχρι \$2.500 ή και τα δύο, σύμφωνα με το Υπουργείου Δικαιοσύνης.

Η Smith γνώρισε τον νεαρό στο **Internet**. Σύμφωνα με τις αρχές, υπάρχουν αποδείξεις που δείχνουν ότι γνώριζε την ηλικία του αγοριού πριν το συναντήσει στη Maryland, στην περιοχή του Howard, όπου και πήγε το Σάββατο με σκοπό να συνάψει μαζί του σεξουαλική σχέση. Συνελήφθη την Κυριακή και προφυλακίστηκε με εγγύηση \$40.000 ως την 28η Ιανουαρίου, την ημέρα της ακρόασης.

#### **Μηνύματα E-mail**

Η μητέρα του αγοριού, πιστεύοντας ότι ο γιος της εξαφανίστηκε ειδοποίησε τις αστυνομικές αρχές την Κυριακή, αφού προηγουμένως είχε ανακαλύψει τα μηνύματα της “ερωμένης” στον υπολογιστή του παιδιού της στο διαμέρισμα της οικογένειάς τους. Βρήκε ένα μήνυμα που μιλούσε για μία απρόσμενη συνάντηση που θα είχαν οι δύο “εραστές”. Νόμιζε ότι πρόκειται για μία έφηβη κοπέλα. Στο τέλος του μηνύματος υπήρχε ένας τηλεφωνικός αριθμός. Τηλεφώνησε και απάντησε κάποιος άντρας. Του ζήτησε να μιλήσει στην κόρη του Adriane . Αυτός της απάντησε ότι δεν ήταν κόρη του αλλά γυναίκα του.



Ενώ οι αστυνομικές αρχές του Howard μιλούσαν με τη μητέρα του παιδιού η Smith βρισκόταν με το αγόρι. Ο αστυνομικός αντιπρόσωπος Morris Carol και ιδιωτικοί αστυνομικοί αποφάσισαν ότι αυτά που συνέβησαν βρίσκονταν πέρα από τις αρμοδιότητές τους και για αυτό επικοινωνήσαν με την αστυνομία της Laurel. Η Laurel είναι μία πόλη με πληθυσμό είκοσι χιλιάδες περίπου κατοίκους και βρίσκεται εννέα μίλια βόρεια του Silver Spring και δεκαεννέα μίλια νότια της Βαλτιμόρης.

Ο νεαρός στεναχωρήθηκε πολύ με τη σύλληψη της ερωμένης του. Το γεγονός αυτό, πιθανά θα επιφέρει βλαπτικές συνέπειες στο αγόρι το οποίο συμμετείχε με τη θέληση του, αλλά αυτό δεν παίζει κανένα ρόλο όσον αφορά την απόφαση της δικαιοσύνης εξαιτίας της ηλικίας του αγοριού.

## ΠΕΡΙΠΤΩΣΗ 2<sup>η</sup> ( 13/1/99 )

### Η πολιτεία της Nevada δίνει τη μάχη της στην αναζήτηση θυμάτων σεξουαλικής παρενόχλησης στο διαδίκτυο

#### Δύο άντρες, ύποπτοι για πιθανή σεξουαλική παρενόχληση

Η αστυνομία αναζητά περισσότερα θύματα των δύο αντρών που κατηγορούνται για σεξουαλική επίθεση σε ένα δεκαεφτάχρονο κορίτσι το οποίο γνώρισαν μέσω του Internet. Οι δύο άντρες που ονομάζονται Timothy Mobly και Aaron Cross, εικοσιπέντε χρονών και οι δύο, συνελήφθησαν στο διαμέρισμα του πρώτου στις 3 Ιανουαρίου 1999. Κρατούνται στις Κρατικές Σωφρονιστικές Εγκαταστάσεις στο Washoe μέχρι την προκαταρκτική ακρόαση της 21<sup>ης</sup> Ιανουαρίου στο δικαστήριο του Keno. Σύμφωνα με τις αρχές και οι δύο κατηγορούνται για σεξουαλική επίθεση και για κατοχή παιδικού πορνογραφικού υλικού. Επιπλέον ο Cross κατηγορείται για απρεπή και άσεμνη έκθεση ανηλίκου, παράνομη κατακράτηση και απαγωγή πρώτου βαθμού, ενώ η εγγύηση για την αποφυλάκιση του καθορίστηκε σε \$30.000. Όσον αφορά τον Mobly, η κατηγορία εναντίον του για παράνομη κατακράτηση αποσύρθηκε στις 8 Ιανουαρίου και η εγγύηση γι' αυτόν καθορίστηκε σε \$20.000.

## **Η κοπέλα απέδρασε**

Η αστυνομία πιστεύει ότι οι δύο άντρες χρησιμοποιώντας διάφορα αντικείμενα κράτησαν δια της βίας και επιτέθηκαν σεξουαλικά στο δεκαεφτάχρονο κορίτσι το οποίο πήγε στο διαμέρισμα του Mobly για επίσκεψη. Σύμφωνα με τον εκπρόσωπο της αστυνομίας Dave Zarubi , το επόμενο πρωί, όταν οι δύο άντρες άφησαν μόνη της την κοπέλα στο διαμέρισμα, εκείνη κατάφερε να απελευθερωθεί και άρχισε να καλεί σε βοήθεια φωνάζοντας. Σύμφωνα πάλι με τα λεγόμενα του Zarubi, η αστυνομία είναι γενική στις περιγραφές του περιστατικού σκόπιμα έτσι ώστε να μην προκαλέσουν σύγχυση σε άλλα τυχόν θύματα. Όπως είπε και στο κανάλι APB News : Αν κάποιος ήρθε πραγματικά σε επαφή με κάποιον από τους δύο άντρες πρέπει να γνωρίζει ειδικές λεπτομέρειες γι' αυτούς, τις οποίες δεν έχει αποκαλύψει η αστυνομία στο κοινό.

## **Λευκό ποινικό μητρώο**

Ο ιδιωτικός αστυνομικός Dave Adams περιέγραψε τον Mobly σαν έναν καλοκαμωμένο λευκό άντρα με ύψος 1,90μ., 60κιλά περίπου, με καστανά μαλλιά και πράσινα μάτια ο οποίος φοράει γυαλιά. Περιέγραψε τον Cross ως έναν επίσης καλοκαμωμένο νέγρο με ύψος 1,68μ., βάρος 65κιλά, με πολύ κοντά μαύρα μαλλιά και καστανά μάτια.

Κανένας από τους δύο δεν έχει στο ποινικό του μητρώο αξιόποινες πράξεις.

## **ΠΕΡΙΠΤΩΣΗ 3" (13/1/99 )**

### **Άντρας από την Florida εμπλέκεται σε διαδικτυακές σεξουαλικές σχέσεις με ανηλίκους**

Κατηγορίες για προσπάθεια σύναψης παράνομων σεξουαλικών σχέσεων με νεαρά κορίτσια μέσω του Internet, βαραίνουν τον πενηντατριάχρονο Edward Flagge, ο οποίος σέρφαρε στο Internet με το όνομα Winter Park. Μέσα σε λίγες ώρες μετά την αποφυλάκισή του με εγγύηση συνελήφθη εκ νέου αφού προσπαθούσε να κανονίσει μία ακόμη συνάντηση πρόσωπο με πρόσωπο με μία ανήλικη.

Στις 13.01.1999 εμφανίστηκε στο ομοσπονδιακό δικαστήριο, όπου αποφασίστηκε η κράτηση του χωρίς εγγύηση μέχρι τη δίκη της 1ης Μαρτίου. Όπως είπε η βοηθός Ana Escobar "Ο δικαστής τον χαρακτήρισε κίνδυνο για την κοινωνία".

Έρευνες για τον Flagge διεξάγονται από το FBI, από τρία αστυνομικά γραφεία της Florida και από ένα αστυνομικό τμήμα του Illinois.

Ομοσπονδιακό δικαστήριο απήγγειλε οκτώ κατηγορίες κατά του Flagge, ανάμεσα στις οποίες περιλαμβάνονται δύο κατηγορίες για απόπειρα προσέλκυσης παιδιών για σεξουαλικές πράξεις με δόλο, πέντε κατηγορίες για διακίνηση υλικού παιδικής πορνογραφίας & μία κατηγορία για την κατοχή παιδικής πορνογραφίας. Οι κατηγορίες αυτές από την πολιτεία Hillsborough είναι ακόμη σε εκκρεμότητα.

Το αστυνομικό γραφείο της πολιτείας του Hillsborough παρακολουθούσε τις δραστηριότητες του Flagge στο διαδίκτυο από τον Ιούνιο του 1998. Για μια χρονική περίοδο μεγαλύτερη των πέντε μηνών, ο Flagge χρησιμοποιούσε τον ηλεκτρονικό υπολογιστή του για να στέλνει υλικό παιδικής πορνογραφίας και απασχολήθηκε σε συζητήσεις σεξουαλικού περιεχομένου χρησιμοποιώντας γραφικά στην προσπάθειά του όπως νόμιζε να προσελκύσει ένα δεκατετράχρονο κορίτσι από την πόλη Tampa. Δεν γνώριζε όμως, ότι πίσω από το έφηβο κορίτσι βρίσκονταν η αστυνομία που παρακολουθούσε τα βήματά του.

Στις 24 Νοεμβρίου, ο Flagge πήγε στην πόλη Tampa με σκοπό να βρεθεί σεξουαλικά με τη «νεαρή σύντροφο» του. Αντί γι' αυτήν, τον υποδέχτηκαν οι απεσταλμένοι του αστυνομικού τμήματος. Ο Flagge οδηγήθηκε στη φυλακή του Hillsborough αλλά αφέθηκε ελεύθερος με εγγύηση λίγο αργότερα την ίδια μέρα.

Μέσα σε λίγες ώρες μετά την αποφυλάκισή του, σύμφωνα πάντα με τις αρχές, ο Flagge συνδέθηκε πάλι με το Internet για να ξεκινήσει σεξουαλικές συζητήσεις με κάποιο πρόσωπο από το Illinois, το οποίο πίστευε ότι ήταν ένα δωδεκάχρονο κορίτσι.

Στην πραγματικότητα το δωδεκάχρονο κορίτσι ήταν ένας αστυνομικός.

Μέρος της κατηγορίας για διαδικτυακή επικοινωνία σεξουαλικού χαρακτήρα με ανήλικο, είναι και το ότι απέστειλε εικόνες παιδικής πορνογραφίας.

Σε περίπτωση καταδίκης ο Flagge αντιμετωπίζει ποινή φυλάκισης μέχρι και δεκαπέντε χρόνια και πρόστιμο μέχρι \$250.000 για κάθε μία από τις αποπλανήσεις ανηλίκων που διέπραξε. Για την κατηγορία της κατοχής υλικού παιδικής πορνογραφίας, η ποινή είναι πέντε επιπλέον χρόνια φυλάκισης και μέχρι \$250.000.

#### **ΠΕΡΙΠΤΩΣΗ 4<sup>η</sup> ( 19/1/99 )**

##### **Την περιέργεια της αστυνομίας κέντρισε ένας τριαντάχρονος στρατιώτης**

Ο John C. Kania, ένας προγραμματιστής υπολογιστών και εθελοντής στρατιώτης του πυροβολικού από την Allentown, αρχικά τράβηξε την προσοχή της αστυνομίας σε ένα chat room όπου είχε στείλει μήνυμα αναζητώντας «συνάντηση σεξουαλικού χαρακτήρα με νεαρή κοπέλα», σύμφωνα με τον αντιπρόσωπο Al Della Feve.

Αστυνομικοί από το αστυνομικό τμήμα έρευνας εγκλημάτων στο χώρο της Υψηλής Τεχνολογίας του New Jersey, οι οποίοι παρακολουθούσαν διάφορα chat rooms με σκοπό να ανακαλύψουν άτομα που παρενοχλούσαν σεξουαλικά, παιδιά απάντησαν στο μήνυμα προσποιούμενοι ότι ήταν ένα δεκατριάχρονο κορίτσι.

Ο στρατιώτης παρουσιαζόταν στις συνομιλίες σαν έφηβος. Μετά από συνομιλίες που κράτησαν αρκετές εβδομάδες, ο Kania κανόνισε να συναντήσει την κοπέλα τη Δευτέρα στο τοπικό εμπορικό κέντρο και ύστερα να την πάει σε ένα γειτονικό ξενοδοχείο για να κάνουν έρωτα.

Ωστόσο στο εμπορικό κέντρο μία γυναίκα στρατιωτικός μεταμφιέστηκε σε μία «γλυκιά ανήλικη». Η ενδυμασία και η

εμφάνιση της γυναίκας ήταν τόσο πειστική με αποτέλεσμα να ξεγελαστεί ο Kania, ο οποίος πίστεψε πραγματικά ότι ήταν δεκατριών χρονών. Κατά τη διάρκεια της συνάντησης τους στο εμπορικό, αυτός της έκανε ασελγείς προτάσεις οι οποίες ηχογραφήθηκαν στον «κοριό» τον οποίο είχε η γυναίκα. Στο σημείο αυτό, εισέβαλαν οι στρατιώτες και ο Kania συνελήφθηκε. Κατηγορήθηκε για απόπειρα σεξουαλικής επίθεσης και διακινδύνευσης της ασφάλειας παιδιού.

### **Αποδεικτικά στοιχεία και στο ξενοδοχείο**

Αργότερα οι αστυνομικοί πήγαν στο σπίτι του Kania και έψαξαν τον υπολογιστή του όπου βρήκαν «απροσδιόριστες» αποδείξεις σύμφωνα με την αναφορά της αστυνομίας. Επίσης, στο δωμάτιο του ξενοδοχείου το οποίο είχε κρατήσει ο Kania βρήκαν προφυλακτικά.

Ο Kania, εθελοντής στρατιώτης πυροβολικού, παντρεμένος και πατέρας ενός παιδιού, βρίσκεται τώρα στη φυλακή με εγγύηση \$20.000.

## **ΠΕΡΙΠΤΩΣΗ 5<sup>η</sup> ( 29/1/99 )**

### **Απιστία μέσω Internet**

Ο Kolb, ένας εξηντατριάχρονος εργάτης εργοστασίου, προσπάθησε να σκοτώσει την εξηντάχρονη γυναίκα του Ida με ένα χασαπομάχαιρο σε μία έκρηξη ζήλιας, όταν ανακάλυψε ότι αυτή διατηρούσε ερωτική σχέση μέσω του Internet. Όπως είπε στην ομολογία του το γεγονός αυτό τον στεναχωρούσε με αποτέλεσμα να μην κοιμάται τα βράδια και να χάνει την όρεξη για δουλειά.

Σύμφωνα με την αστυνομία ο Kolb δεν άντεχε άλλο την πίεση. Η Ida μιλούσε στο Internet για μήνες με διάφορα πρόσωπα μεταξύ των οποίων ένας άντρας μεταξύ είκοσι πέντε και τριάντα πέντε χρονών. Όταν γύρισε από τη δουλειά ζήτησε από τον γιο του να ψάξει τον υπολογιστή. Ο γιος του βρήκε τη φωτογραφία του άντρα και τότε ο Kolb εξαγριώθηκε.

«Έκατσα σε μία καρέκλα και σκεφτόμουν την Ida και τη φωτογραφία. Όσο περισσότερο σκεφτόμουν τόσο μεγάλωνε ο θυμός μου. Ζούσα μία κόλαση». Όταν η Ida γύρισε στις 04:25 ο Kolb της μίλησε για τη σχέση της με τον άντρα. Εκείνη το αρνήθηκε. Τότε ο Kolb της επιτέθηκε με ένα μαχαίρι που βρήκε στην κουζίνα του σπιτιού. Ο γιος τους όταν αντιλήφθηκε τι γινόταν άρπαξε από τους ώμους τον πατέρα του και τον αφόπλισε. Αργότερα, όταν ηρέμησε, πήγε ο ίδιος τη γυναίκα του στο νοσοκομείο.

Ο γενικός εισαγγελέας Dennis Hawthorne είπε: «Είναι κρίμα, ήταν παντρεμένοι πολλά χρόνια. Ο Kolb δεν έχει βεβαρημένο ποινικό μητρώο. Είναι ένας απλός άνθρωπος ο οποίος σ' ολόκληρη τη ζωή του δούλεψε στο εργοστάσιο της περιοχής. Η απιστία της γυναίκας του ήταν πολύ βαρύ φορτίο για να το αντέξει».

Ο Kolb κατηγορείται για απόπειρα δολοφονίας και εγκληματική κατοχή όπλου. Διατάχθηκε η κράτησή του ενώ ορίστηκε εγγύηση αποφυλάκισης \$100.000 μετρητά.

### ΠΕΡΙΠΤΩΣΗ 6<sup>η</sup> ( 2/2/99 )

#### Άντρας χρησιμοποιούσε το Internet για αποπλάνηση αγοριών

Ο James Cleary, τριάντα έξι χρονών, από το Howard Beach κατηγορείται για σεξουαλική εκμετάλλευση δύο αγοριών τα οποία προσπάθησε να δελεάσει δίνοντάς τους υποσχέσεις για δώρα και βόλτες με τη μηχανή του.

Ο James γνώρισε τα δύο αγόρια δέκα και δώδεκα χρονών το καθένα, σε ένα chat room στο Internet. Προκειμένου να τον συναντήσουν τους υποσχέθηκε ότι θα τους αγόραζε παιχνίδια. Η συνάντηση κανονίστηκε για τις 11 Νοεμβρίου στο πάρκο Wantagh, στη δυτική ακτή του Long Island, ένα νέο προάστιο της New York.

Όταν τα παιδιά έφτασαν στο πάρκο τους έδωσε τα δώρα τους και λέγοντάς τους ότι θα τα πάει βόλτα με τη μηχανή του, τα οδήγησε σε ένα απομονωμένο σημείο της παιδικής χαράς, όπου και τα παρενόχλησε σεξουαλικά.

Η αστυνομία συνέλαβε τον Cleary στις 17 Δεκεμβρίου, όταν ένα από τα δύο αγόρια εκμυστηρεύτηκε στους γονείς του το γεγονός.

Τον Cleary βαραίνουν επτά κατηγορίες, τέσσερις από τις οποίες για σεξουαλική κακοποίηση και οι τρεις για τη θέση σε κίνδυνο της υγείας των παιδιών. Ο εναγόμενος κατηγορείται επίσης για την χρησιμοποίηση του Internet με σκοπό να πλησιάσει τα παιδιά και για την αποστολή άσεμνου υλικού σε νεαρά αγόρια μέσω αυτού.

Για τις παραπάνω κατηγορίες δήλωσε αθώος. Σε περίπτωση καταδίκης του αντιμετωπίζει επτά χρόνια φυλάκισης για κάθε μία από τις σεξουαλικές παρενοχλήσεις που διέπραξε.

### **ΠΕΡΙΠΤΩΣΗ 7<sup>η</sup> ( 2/2/99 )**

#### **Σχέση μέσω του Internet κατέληξε σε θάνατο**

Μια ερωτική σχέση που ξεκίνησε μέσω του Internet κατέληξε σε φόνο όταν ο άντρας πυροβόλησε την «αγαπημένη» του στο πίσω μέρος του κεφαλιού με καραμπίνα γιατί εκείνη δεν ήθελε να δώσει τέλος στη σχέση τους.

Ο τριανταεννιάχρονος William M. Miller από την πολιτεία Missouri, είχε γνωρίσει την Joann Marie Brown στο Internet πριν έξι μήνες. Η Joann μετακόμισε από το πατρικό της σπίτι στο Dearborn, Mich. στο σπίτι του το φθινόπωρο.

Ο William ισχυρίστηκε ότι είχε πυροβολήσει την εικοσιεπτάχρονη Brown λίγα μέτρα μπροστά από το εξοχικό του σπίτι, και ότι ήταν ατύχημα. Είπε ότι όταν έγινε αυτό πανικοβλήθηκε και τη μετέφερε σ' ένα πηγάδι κοντά στο σπίτι του. Ύστερα την σκέπασε και καθάρισε το αίμα από την περιοχή.

Δέκα ημέρες αργότερα η συνείδησή του και η συμβουλή της αδερφής του, τον οδήγησαν στην απόφαση να πάει στην αστυνομία.

Στην περιγραφή του όμως υπήρχαν πολλές ασάφειες. Εξάλλου η αυτοψία έδειξε ότι η γυναίκα είχε πυροβοληθεί εξ' επαφής και όχι από απόσταση. Ακόμη η αστυνομία που εξέτασε

το όπλο το βρήκε οπλισμένο. Εξάλλου είναι ασυνήθιστο οι άνθρωποι να περπατούν στους δρόμους με οπλισμένες караμπίνες.

Η αστυνομία έχοντας στη διάθεσή της αυτές τις πληροφορίες, ανέκρινε τον Miller, ο οποίος τελικά ομολόγησε ότι στις 20 Ιανουαρίου '99 σκότωσε την Brown γιατί δεν την άντεχε άλλο και εκείνη αρνιόταν να φύγει από το σπίτι του. Κατάφερε να την πείσει να βγουν έξω από το σπίτι έτσι ώστε να την σκοτώσει κοντά στο σημείο όπου θα έκρυβε το πτώμα της.

Η οικογένεια της γυναίκας δεν γνώριζε που ακριβώς είχε πάει και έτσι κανείς δεν κατάλαβε την απουσία της έως τη στιγμή που ο Miller πήγε στην αστυνομία.

Ο Miller κρατείται στη φυλακή της πολιτείας McDonald με την κατηγορία φόνου πρώτου βαθμού.

### **ΠΕΡΙΠΤΩΣΗ 8<sup>η</sup> ( 1/4/99 )**

#### **Το FBI στα ίχνη του δημιουργού του ιού Melissa**

Περιγράφεται ως ο πιο διαδεδομένος ιός, ο ιός «Melissa». Αναγνωρίστηκε για πρώτη φορά στις 26 Μαρτίου και ανάγκασε πολλές εταιρείες να θέσουν εκτός λειτουργίας τους ηλεκτρονικούς υπολογιστές τους. Ο ιός ενεργοποιείται μόνο μέσα στο λειτουργικό πρόγραμμα της Microsoft. Όταν ο υπολογιστής μολυνθεί, ο ιός ψάχνει και εντοπίζει το πρόγραμμα Microsoft Outlook. Ενεργοποιώντας μία σειρά εντολών δημιουργεί μηνύματα e-mail τα οποία στέλνει στα 50 πρώτα άτομα που βρίσκονται καταχωρημένα στο βιβλίο διευθύνσεων (address book) του προγράμματος. Κάθε μήνυμα κουβαλάει μαζί του τον ιό ο οποίος μολύνει τον υπολογιστή του παραλήπτη. Μ' αυτό τον τρόπο ο ιός εξαπλώνεται ταχύτατα.

Το FBI, που ασχολείται με την υπόθεση, κατάφερε να εντοπίσει τον δημιουργό του ιού Melissa σε ένα Web site που φιλοξενείται στην Access Orlando, μία εταιρεία παροχής υπηρεσιών δικτύου. Ο ιός δεν επηρέασε τους υπολογιστές της Access Orlando η εταιρεία χρησιμοποιεί το λειτουργικό σύστημα UNIX στο οποίο δεν ενεργοποιείται ο ιός.



Πράκτορες του FBI ζήτησαν άδεια από την εταιρεία α παρακολουθήσουν το Web site της, ενώ αναμένουν ένταλμα που θα τους επιτρέψει να ερευνήσουν το περιεχόμενο του σκληρού δίσκου του κεντρικού ηλεκτρονικού υπολογιστή της εταιρείας.

Σε περίπτωση που ο δημιουργός του ιού Melissa βρεθεί, αντιμετωπίζει πρόστιμο \$250.000 και μέχρι 10 χρόνια φυλάκιση.

Στα κεντρικά γραφεία του FBI στην Washington, ο εκπρόσωπος δημοσίων σχέσεων αρνήθηκε να σχολιάσει την έρευνα που διεξάγεται.

### **ΠΕΡΙΠΤΩΣΗ 9<sup>η</sup> ( 2/4/99 )**

#### **Συνελήφθη ο δημιουργός του ιού Melissa**

Ο David L. Smith, 30 χρονών, από την περιοχή Aberdeen, συνελήφθη στο σπίτι του αδερφού του κοντά στην περιοχή Eatontown με την κατηγορία ότι δημιούργησε τον ιό Melissa ο οποίος προκάλεσε τεράστια προβλήματα και μεταδόθηκε σ' ολόκληρο τον κόσμο με απίστευτη ταχύτητα. (βλ. ΠΕΡΙΠΤΩΣΗ 8η, 1 Απριλίου 1999, σελ: 42).

Ο Smith που ήταν υπό κράτηση στις φυλακές Monmouth County Jail βγήκε με εγγύηση \$100.000, την οποία πλήρωσε ο αδερφός του: (βλ. ΠΕΡΙΠΤΩΣΗ 52η, 9 Δεκεμβρίου 1999, σελ. 108).

### **ΠΕΡΙΠΤΩΣΗ 10<sup>η</sup> ( 28/5/99 )**

#### **Παιδίατρος κατηγορείται για κατοχή παιδικού πορνογραφικού υλικού**

Ένας παιδίατρος από τη Βόρεια Virginia κατηγορείται για κατοχή πορνογραφικού υλικού. Την κατηγορία αυτή του απήγγειλαν οι αρχές μετά από έρευνες που έκαναν στην America Online (AOL). Στα e-mail της σύνδεσής του με την AOL βρήκαν

αποκαλυπτικές εικόνες οι οποίες του είχαν αποσταλεί μέσω e-mail κατά τη διάρκεια των τελευταίων έξι μηνών. Επιπλέον υλικό παιδικής πορνογραφίας βρήκαν και στα αρχεία του ηλεκτρονικού του υπολογιστή.

Ο παιδίατρος παρουσιαζόταν στον άνθρωπο που του έστειλε τις εικόνες ως ένα 16χρονο κορίτσι. Η κατοχή πορνογραφικού υλικού αποτελεί έγκλημα για το οποίο ο παιδίατρος καλείται να απολογηθεί.

### **ΠΕΡΙΠΤΩΣΗ 11<sup>η</sup> ( 11/6/99 )**

#### **Το FBI διερευνά την προέλευση των ιών των υπολογιστών**

Το FBI διεξάγει έρευνες με σκοπό να βρει την προέλευση ενός επικίνδυνου ιού, ο οποίος επηρέασε δέκα χιλιάδες συνεργαζόμενα συστήματα ηλεκτρονικού υπολογιστή και πολλούς ατομικούς ηλεκτρονικούς υπολογιστές σ' όλο τον κόσμο.

Ο ιός διαδίδεται και πολλαπλασιάζεται μέσω του προγράμματος της Microsoft, Outlook, οδηγώντας πολλές μεγάλες εταιρείες στο να κλείσουν τα συστήματα των e-mail τους με στόχο την ελαχιστοποίηση της καταστροφικής δράσης του ιού.

Ο ιός έχει την ιδιότητα να καταστρέφει δεδομένα και να «τρώνει» έγγραφα και άλλα σημαντικά αρχεία. Σύμφωνα με τους ειδικούς ο τρόπος με τον οποίο δρα ο ιός τον καθιστά πιο επικίνδυνο ακόμη και από το γνωστό ιό «Melissa».

Τα πρώτα κρούσματα εμφανίστηκαν στη Γαλλία, στη Γερμανία, στο Ισραήλ, στη Νορβηγία, στην Ουγγαρία και στις ΗΠΑ ενώ τουλάχιστον πέντε ακόμη χώρες χτυπήθηκαν από τον ιό.

Σύμφωνα με το FBI και το NIPC (National Infrastructure Protection Center), ο ιός καταστρέφει μία σειρά αρχείων του ηλεκτρονικού υπολογιστή μετατρέποντάς τα σε 0 bytes και έχει τη δυνατότητα να καταστρέψει τεράστια ποσότητα δεδομένων.

Ο ιός παρουσιάζεται σαν ένα ακίνδυνο e-mail ως απάντηση από μία γνωριμία και γράφει: «Έλαβα το e-mail σου, και πρέπει να απαντήσω. Μέχρι τότε, ρίξε μια ματιά στα παρακάτω έγγραφα». Οι χρήστες οι οποίοι θα διαβάσουν το κείμενο θα επιτρέψουν στον ιό να εισχωρήσει στον ηλεκτρονικό τους υπολογιστή και να καταστρέψει καταρχήν το Outlook. Ταυτόχρονα δίνει στον ηλεκτρονικό υπολογιστή την εντολή να φτιάξει αντίγραφα του ιού τα οποία στην συνέχεια θα στείλει στις διευθύνσεις e-mail που υπάρχουν στη λίστα του Inbox.

Ένας ακόμη παρόμοιος ιός με το όνομα Chernobyl χτύπησε κυρίως τις Ευρωπαϊκές χώρες στα τέλη του Απρίλη.

### **ΠΕΡΙΠΤΩΣΗ 12<sup>η</sup> ( 16/6/99 )**

#### **Καταπέλτης αποδείχτηκαν οι περιπολίες για παιδική πορνογραφία στο Internet**

Μία ομάδα επιδοτούμενη από τις Η.Π.Α., δημιούργησε ένα πρόγραμμα το οποίο θα ελέγχει τους πορνογράφους και τους παιδόφιλους που χρησιμοποιούν το Internet για να εντοπίσουν θύματα σ' όλο τον κόσμο. Το πρόγραμμα αποκαλείται «Αθωότητα σε Κίνδυνο».

Η ομάδα αυτή κατάφερε να αποκαλύψει δύο ενήλικες οι οποίοι επιδίωκαν και επιδίδονταν σε ερωτικές σχέσεις με νεαρά άτομα μέσω του Internet. Τελικά όμως καμία κατηγορία δεν απαγγέλθηκε εναντίον τους.

### **ΠΕΡΙΠΤΩΣΗ 13<sup>η</sup> ( 28/7/99 )**

#### **Πρόσφατα hackers εισέβαλαν στο Website του FBI και άλλων ομοσπονδιακών υπηρεσιών**

Η κυβέρνηση Clinton πρότεινε στο Λευκό Οίκο ένα σχέδιο σύμφωνα με το οποίο το FBI θα μπορεί να επιβλέπει μέσω ενός συστήματος υπολογιστών, ψάχνοντας ενδείξεις για παράνομη δραστηριότητα στο Internet και το οποίο αποβλέπει στην προστασία των αρχείων του κράτους από τους εισβολείς. Το

σύστημα αυτό θα είναι έτοιμο το 2003 και πιθανότατα θα χρησιμοποιηθεί και στις τράπεζες, στις τηλεπικοινωνίες & στα μεταφορικά μέσα.

Σύμφωνα με τον πρόεδρο του Συμβουλίου Εθνικής Ασφάλειας Jeffrey Hunker, οι φόβοι για εισβολείς έχουν αυξηθεί δραματικά.

Ανησυχίες εκφράζονται όσον αφορά το δικαίωμα της ιδιωτικής ζωής των χρηστών του Internet, ενώ πολίτες εκφράζουν φόβους για την εισβολή σε δικά τους ιδιωτικά έγγραφα ή αρχεία, αφού το FBI θα μπορεί να παρακολουθεί κρυφά τα πάντα μέσα στο Internet.

### **ΠΕΡΙΠΤΩΣΗ 14<sup>η</sup> ( 30/7/99 )**

#### **Τουλάχιστον 200 θύματα αγορών μέσω του Internet ενός επαγγελματία απατεώνα**

Ο James R. Denlinger Jr., επαγγελματίας απατεώνας κατάφερε να εξαπατήσει περισσότερα από 200 άτομα από τα οποία απέσπασε περίπου \$200.000. Χρησιμοποιώντας sites στο Internet υποσχόταν να πουλήσει ή να ανταλλάξει συλλεκτικές κούκλες αντί \$200 η μία ενώ η πραγματική τιμή τους στη νόμιμη αγορά είναι \$6 η μία.

Το FBI παρακολουθούσε για χρόνια τις προσπάθειες του Denlinger να πουλήσει κούκλες Barbie, Transformers και κάρτες του baseball. Δεν κατάφερναν όμως να τον εντοπίσουν επειδή ο Denlinger μετακινούνταν πάρα πολύ και χρησιμοποιούσε κυρίως ταχυδρομικές θυρίδες για να κάνει τις συναλλαγές του.

Παρ' όλα αυτά μία από τις ταχυδρομικές θυρίδες που διατηρούσε οδήγησε την αστυνομία στην πόρτα του όταν ένας συλλέκτης ανέφερε στις αρχές ότι έστειλε \$220 σ' έναν άντρα για ένα παιχνίδι το οποίο δεν έλαβε ποτέ.

Τα περισσότερα θύματά του, προέρχονται από τη Florida, το Illinois, το Maine, το New Jersey, το Oregon, τη Δυτική Virginia, όπου διατηρούσε ταχυδρομικές θυρίδες και από 3 τουλάχιστον ακόμη μέρη.

Μερικά από τα θύματα ζήτησαν συστάσεις προκειμένου να γίνει η αγοραπωλησία, τις οποίες παρείχε ο ίδιος στα θύματά του χρησιμοποιώντας διάφορα ψευδώνυμα μέσω μηνυμάτων e-mail.

Θύμα ανέφερε ότι του είχε στείλει \$1000.

Μετά από κάθε απάτη ο Denlinger έβγαζε κοροϊδευτικές ανακοινώσεις στο Internet όπου ονόμαζε τα θύματά του «ηλίθιους».

Η αστυνομία συνέλαβε τον 28χρονο άντρα σ' ένα διαμέρισμα στο San Jose. Στην κατοχή του βρέθηκαν μία βαλίτσα με έγγραφα που απαριθμούσαν τα θύματά του, καθώς και δωδεκάδες συλλεκτικά αρκουδάκια.

Τον Denlinger βαραίνουν 7 κατηγορίες για απάτη μέσω του Internet και μία κατηγορία για παράνομη χρησιμοποίηση site. Σε βάρος του εκκρεμούν επιπλέον κατηγορίες για κλοπή και χρησιμοποίηση ξένης ταυτότητας. Αναφορικά με την τελευταία κατηγορία, είχε νοικιάσει ταχυδρομική θυρίδα στο όνομα μίας τραπεζικής υπαλλήλου με το όνομα Santa Rosa, την οποία είχε γνωρίσει στο δρόμο.

Ο Denlinger μετά τη σύλληψή του αφέθηκε ελεύθερος με εγγύηση \$200.000.

### ΠΕΡΙΠΤΩΣΗ 15<sup>η</sup> ( 9/8/99 )

#### Οι περισσότερες υποθέσεις παραβιάσεων στο Internet διαγράφονται

Ο Kevin Mitnick υπήρξε ένας από τους καταζητούμενους hackers στο διαδίκτυο. Η αστυνομία κατάφερε να τον συλλάβει. Ο Kevin δήλωσε ένοχος στις πέντε κατηγορίες που του απαγγέλθηκαν για απάτη και για κατάχρηση μέσω του Internet τον Απρίλιο του 1999.

Η υπόθεση του κατέληξε στην αίθουσα δικαστηρίου, στην California αυτόν τον μήνα, όπου αποφασίστηκε η αποφυλάκιση του με αναστολή 5 χρόνων.

Η υπόθεση του Kevin αποτελεί τρανταχτό παράδειγμα επιβολής ποινής στους hackers.

Μέσα στο 1998, το FBI και άλλες μυστικές υπηρεσίες αναφέρθηκαν σε 419 περιπτώσεις εγκληματικών πράξεων στο Internet, σχεδόν 4 φορές περισσότερες από αυτές του 1992, σύμφωνα με έρευνα του Υπουργείου Δικαιοσύνης που δημοσιεύτηκε στην εβδομαδιαία εφημερίδα που ασχολείται με θέματα Ποινικής Δικαιοσύνης. Παρ' όλα αυτά μόνο σε 83 δράστες απαγγέλθηκαν κατηγορίες ενώ οι υπόλοιποι αφέθηκαν ελεύθεροι λόγο έλλειψης αποδεικτικών στοιχείων. Εξαιτίας της νεαρής ηλικίας των δραστών και της ύπαρξης λευκού ποινικού μητρώου, πολλοί δράστες αφήνονται ελεύθεροι.

Παρ' ότι η αστυνομία έχει αυξήσει περισσότερο από ποτέ τις έρευνες για παραβάτες στο Internet τον προηγούμενο χρόνο μόνο το 20% των περιπτώσεων κατέληξε στα δικαστήρια.

### **ΠΕΡΙΠΤΩΣΗ 16<sup>η</sup> ( 16/8/99 )**

#### **Αγορά GHB\* στο Internet**

Ο Carl Corton, 63 ετών από το Merritt Island και ο John Hedrik, 22 ετών από το Colorado Springs κατηγορούνται ότι χρησιμοποιούσαν το Internet για να πουλήσουν υλικά και οδηγίες, για κατασκευή στο σπίτι ενός ισχυρού ναρκωτικού του GHB, γνωστό και ως "date rape" (=προκαθορισμένο βιασμό).

Ο Γενικός Εισαγγελέας του Michigan, Jennifer M. Granholm ανακοίνωσε το περιεχόμενο των κατηγοριών εναντίον των 2 αντρών.

Σύμφωνα με τον νόμο του Michigan η πώληση του GHB είναι παράνομη. Η υποκίνηση σε κατασκευή του αποτελεί κακούργημα. Σε περίπτωση καταδίκης τους αντιμετωπίζουν μέγιστη ποινή κάθειρξης 30 ετών.

Πρόταση για παύση των ενεργειών τους έγινε προς τους δύο άντρες. Σύμφωνα με τους όρους της πρότασης οι δύο άντρες έχουν στη διάθεσή τους 10 ημέρες για να σταματήσουν την

παροχή οδηγιών για την κατασκευή του GHB διαφορετικά θα αναγκαστούν να αντιμετωπίσουν τις κατηγορίες.

Η αποκάλυψη των δύο αντρών έγινε, όταν αυτοί προσπάθησαν να παρακινήσουν δύο μυστικούς αστυνομικούς μέσω Internet να κατασκευάσουν μόνοι τους το GHB, πουλώντας τους οδηγίες για τη χημική του σύνθεση, αντί \$200.

### **32 Θάνατοι από το GHB**

Ο Gorton και ο Hendrick είχαν δημιουργήσει μία σελίδα στο Internet για να προωθούν και να πουλούν χημικές ουσίες και οδηγίες για την κατασκευή του GHB. Ταυτόχρονα διαβεβαίωναν τους πελάτες τους για τη νομιμότητα της αγοραπωλησίας.

Η διαβεβαίωση αυτή βασιζόταν στο ότι δεν πωλούσαν αυτό κάθε αυτό το ναρκωτικό, αλλά μεμονωμένα υλικά και οδηγίες κατασκευής.

Σύμφωνα με σχετική έρευνα, το GHB από το 1990 οδήγησε 32 άτομα στο θάνατο, ενώ 3.500 άτομα υπέστησαν τις συνέπειες από υπερβολική δόση.

*\* Ναρκωτικό το οποίο περιέχει υδροξυβουτυρικό οξύ, γνωστό ως GHB διαμέσου Internet. Λίγες σταγόνες από το GHB μπορούν να προκαλέσουν λιποθυμία για 20 τουλάχιστον λεπτά, ενώ το επόμενο πρωί ο χρήστης δεν θυμάται το συμβάν.*

### **ΠΕΡΙΠΤΩΣΗ 17<sup>η</sup> ( 1/9/99 )**

#### **Γυναίκα χρησιμοποιεί το Internet για να καλέσει την αστυνομία**

#### **Στέλνει μήνυμα κατά την διάρκεια της αιχμαλωσίας της**

Η τεχνολογία στάθηκε αρωγός για μία γυναίκα, η οποία χρησιμοποίησε το Internet για να καλέσει την αστυνομία όταν ο σύζυγός της την φυλάκισε μέσα στο σπίτι της. Η 29χρονη γυναίκα κατόρθωσε να γράψει μια παράκληση για βοήθεια στο Internet η οποία ταξίδεψε από την Αριζόνα στην Καλιφόρνια και τελικά στο αστυνομικό τμήμα του West Valley. Αστυνομικοί

πήγαν στο σπίτι της και απελευθέρωσαν, την ίδια και τα 2 παιδιά της, 30 λεπτά αφού είχε στείλει το μήνυμα στον κυβερνήτο.

Σύμφωνα με την κατάθεση της γυναίκας, βρισκόταν στο σπίτι της μαζί με την 3χρονη κόρη της και τον 8χρονο γιο της. Όταν έφθασε ο άντρας της, της απαγόρευσε να βγει από το σπίτι και να χρησιμοποιήσει το τηλέφωνο, ενώ την απείλησε ότι θα έσβηνε το τσιγάρο του στο μάτι της και θα την κομμάτιαζε αν τηλεφωνούσε στην αστυνομία.

Η γυναίκα εκείνη τη στιγμή βρισκόταν σε ένα χώρο συζήτησης (chat room) στο Internet. Χωρίς να το καταλάβει ο άντρας της, έγραψε ένα μήνυμα σ' έναν άντρα στην Αριζόνα, ο οποίος με τη σειρά του επικοινωνήσε με μία γυναίκα στο Calaveras, και η οποία τελικά κάλεσε την αστυνομία.

Μετά την απελευθέρωση της γυναίκας εκδόθηκε ένταλμα σύλληψης για τον σύζυγο, ο οποίος όμως κατάφερε να ξεφύγει. Τελικά η αστυνομία, κατάφερε να τον οδηγήσει στη φυλακή του Salt Lake με την κατηγορία της παράνομης επίθεσης.

Τώρα είναι ελεύθερος με εγγύηση \$11.100. Προκειμένου να εξασφαλιστεί η ασφάλεια της τρομοκρατημένης γυναίκας εκδόθηκε εντολή για την επιτήρηση του συζύγου της.

### ΠΕΡΙΠΤΩΣΗ 18<sup>η</sup> ( 2/9/99 )

#### Προσφορά νεφρού στο Internet στην τιμή \$5,7 εκατομ.

Μία δημοπρασία ανθρώπινου νεφρού στο Internet στο site eBay, έφτασε τα \$5,7 εκατομ. Σύμφωνα με τον υπεύθυνο δημοσίων σχέσεων του eBay, Kevin Pursglove, ο ίδιος δεν γνώριζε αν η προσφορά ήταν αληθινή. Σταμάτησε όμως τη συναλλαγή γιατί ο πωλητής ήρθε σε αντίθεση με το νόμο, ο οποίος απαγορεύει την πώληση ανθρωπίνων οργάνων, και τιμωρεί τον παραβάτη με πρόστιμο μέχρι 5 χρόνια φυλακή και πρόστιμο \$50.000.

Ο πωλητής συστήθηκε ως «hnchego» και απέστειλε το εξής μήνυμα με την αρχική προσφορά των \$25.000: «Πλήρης λειτουργικό νεφρό για πώληση. Μπορείτε να επιλέξετε



οποιοδήποτε από τα δυο μου νεφρά. Ο αγοραστής θα πληρώσει επίσης όλα τα έξοδα της μεταμόσχευσης. Φυσικά μόνο το ένα νεφρό πωλείται, αφού χρειάζομαι το άλλο για να ζήσω. Σοβαρές προσφορές μόνο».

Ο διευθυντής της Αμερικάνικης Ιατρικής Ένωσης, όταν ενημερώθηκε για τα παραπάνω μίλησε για ανηθικότητα και παράνομη δράση γιατρών που συμμετέχουν σε παρόμοιες ενέργειες.

Σύμφωνα με τον Pursglove, προσφορές όπως αυτή τυχαίνει να γίνονται στο site του eBay, αφού δεν υπάρχει κάποιο σύστημα ελέγχου, απλά βασίζονται σε μία απλή δήλωση αξιοπιστίας από τους χρήστες του site.

Αναφέρεται ένα ακόμη τρανταχτό παράδειγμα μιας ομάδας μηχανικών οι οποίοι παρουσίασαν τους εαυτούς τους ως επαγγελματίες ιδιοφυΐες του κυβερνοχώρου, οι οποίοι δέχτηκαν προσφορές για συνεργασία που έφτασε τα \$3,14 εκατομ. Αναφέρονται και περιπτώσεις όπου κάποιοι προσπάθησαν να πουλήσουν στρατιωτικά όπλα όπως μπαζούκας, πυραύλους, ρουκέτες κ.α.

### ΠΕΡΙΠΤΩΣΗ 19<sup>η</sup> ( 2/9/99 )

#### Πειρατές ηγεμονεύουν στις πωλήσεις λογισμικού στο Internet

Σχεδόν στο 60% των πωλήσεων προγραμμάτων υπολογιστών στα τρία από τα μεγαλύτερα sites αγοράς διαπράττεται πειρατεία, σύμφωνα με έλεγχο που έγινε μεταξύ 15 και 20 Αυγούστου από την SIIA – Software and Information Industry Association (Ένωση Βιομηχανιών Λογισμικού και Πληροφόρησης), όπου βρέθηκε ότι προγράμματα υπολογιστών αξίας εκατοντάδων δολαρίων, πωλούνται σε εξευτελιστικές τιμές. Συνολικά 20 διαφορετικά προγράμματα εταιρειών όπως οι: Macromedia, FileMaker, Visio και Adobe, δέχτηκαν επίθεση από πειρατές σε 221 ξεχωριστές περιπτώσεις μέσα από τα sites: eBay, ZDNet Auctions και Excite Auction. Μετά από εξέταση των παραπάνω περιπτώσεων, 181 πωλήσεις διαπιστώθηκαν, από τις οποίες οι 109 κρίθηκαν παράνομες ενώ οι υπόλοιπες 72 νόμιμες. Για τις άλλες 40 περιπτώσεις δεν αναγνωρίστηκε η γνησιότητά

τους ή μη. Σύμφωνα με τα παραπάνω η πιθανότητα να εξαπατηθεί ο καταναλωτής αγοράζοντας λογισμικό μέσω του Internet αγγίζει το 60% και γίνεται εύκολα αφού οι πειρατές – πωλητές δεν παρουσιάζονται σαν μεμονωμένα άτομα αλλά και ως επιχειρήσεις.

Κόκκινη σημαία για τους καταναλωτές και ως αναφορά τις αντιγραφές προγραμμάτων σε CD. Αντιγραφή σημαίνει μεγάλη διαφορά στην τιμή. Για παράδειγμα το πρόγραμμα Director της Macromedia που κοστίζει νόμιμα \$999 πωλείται παράνομα \$28, ενώ το δημοφιλές Photoshop 5.5 είναι διαθέσιμο με \$11.99 αντί \$549 περίπου, που είναι η νόμιμη τιμή του.

### **Ζημία \$11 δισ.**

Στο τέταρτο ετήσιο συνέδριο με θέμα την παγκόσμια πειρατεία λογισμικού τον Μάιο, με διοργανωτή την εταιρεία Software Alliance και τη SIIA, αναφέρθηκε ότι από τις 615 εκατομ. νέες επιχειρήσεις λογισμικού που άνοιξαν παγκοσμίως στη διάρκεια του 1998, οι 231 εκατομ. ή το 38% δέχεται πειρατεία. Από το 1997, μέσα σ' ένα χρόνο, η πειρατεία αυξήθηκε σε 2,5 εκ. επιχειρήσεις, ενώ υπολογίζεται ότι η ζημία για το 1998 έφτασε τα \$11 δισ.: Τα 7,3 δισ. ή το 67% χάθηκαν στις ΗΠΑ, Κίνα, Ιαπωνία, Γερμανία, Ηνωμένο Βασίλειο, Γαλλία, Βραζιλία, Καναδά και Ρωσία. Ακόμη υπολογίζεται ότι μόνο στο Βιετνάμ το 97% των επιχειρήσεων λογισμικού δέχονται πειρατεία, το 95% στην Κίνα, το 92% στην Ινδονησία και το 92% στη Ρωσία.

### **ΠΕΡΙΠΤΩΣΗ 20<sup>η</sup> ( 11/9/99 )**

#### **Όνειρο ή Απάτη;**

Ο Lauzaras Long<sup>9</sup> από την Oklahoma, προσπάθησε να συγκεντρώσει \$ 350 εκ. μέσω ενός site στο Internet πουλώντας γη ή κατοικίες σε μία πολιτεία την οποία θα κατασκεύαζε στην Καραϊβική. Η νέα πολιτεία θα χτιζόταν 115 μίλια δυτικά των νήσων Cayman και θα αναδυόταν μέσα από τη θάλασσα πάνω σε γιγαντιαίες πλατφόρμες. Οι πλατφόρμες θα στηρίζονταν πάνω σε

<sup>9</sup> Το όνομα ενός από τους ήρωες βιβλίου επιστημονικής φαντασίας του Robert A. Heinlein. Το πραγματικό όνομα του Long είναι Howard Turney και το άλλαξε πριν τρία χρόνια.

ένα υποθαλάσσιο βουνό το οποίο απέχει 12 πόδια από την επιφάνεια της θάλασσας. Οι επενδυτές θα μπορούσαν να αγοράσουν κατοικίες αλλά και διάφορα κτίρια παροχής υπηρεσιών όπως νοσοκομεία και ξενοδοχεία.

Ο Long οραματιζόταν τη δημιουργία μίας δικιάς του χώρας, μίας «μοναρχίας», όπου θα «βασίλευε» ο ίδιος.

Μήνυση εναντίον του έκανε η επιτροπή SEC<sup>10</sup> όταν ανακάλυψε τις δραστηριότητές του για τη συγκέντρωση των χρημάτων. Τον Απρίλιο, Δικαστής από την Oklahoma, έδωσε εντολή σύμφωνα με την οποία ο Long έπρεπε να συμμορφωθεί και να παύσει κάθε ενέργεια για τη συγκέντρωση χρημάτων, ενώ ταυτόχρονα πάγωσε όλους του τραπεζικούς του λογαριασμούς.

Σύμφωνα με την επιτροπή SEC ο Long διέπραξε μια σειρά από παράνομες πράξεις. Προκειμένου να παραπλανήσει και να πείσει τους ενδιαφερόμενους, έλεγε ότι είχε κλείσει συμφωνία με μία μεγάλη Ευρωπαϊκή κατασκευαστική εταιρεία η οποία θα αναλάμβανε την κατασκευή του έργου.

Επιπλέον πρόσφερε στους ενδιαφερόμενους αγοραστές Αμερικάνικη υπηκοότητα αντί \$ 1.500.

Ακόμη και αν ο Long είχε ειλικρινείς προθέσεις, ο τρόπος με τον οποίο προσπάθησε να συγκεντρώσει τα χρήματα μέσω του Internet είναι παράνομος.

Η SEC υπολογίζει ότι κατάφερε να συγκεντρώσει \$ 20.000 με \$30.000 και ότι έχει ξοδέψει τα περισσότερα από αυτά τα χρήματα.

Ο Long σε συνέντευξή του στο κανάλι ABPnews είπε ότι το SEC τον χρησιμοποίησε προκειμένου να αποκτήσει δημοσιότητα ο αγώνας ενάντια στις απάτες που γίνονται στο Internet.

Αποδέχτηκε ότι έκανε κάποια νομικά λάθη, αλλά αρνήθηκε ότι έκανε συμβόλαιο με επενδυτές. Χαρακτήρισε τη SEC πολύ αυστηρή και είπε ακόμη ότι οι ενέργειές του στο Internet δεν αφορούν τη SEC γιατί το site του Internet που χρησιμοποιούσε διευθύνεται από την Αγγλία.

<sup>10</sup> SEC – Securities and Exchange Commission

Αν η υπόθεση φτάσει στην αίθουσα του δικαστηρίου και σε περίπτωση καταδίκης του, ο Long, θα πρέπει να καταβάλει μεγάλα χρηματικά πρόστιμα & επιπλέον θα πρέπει να επιστρέψει τα χρήματα στους δικαιούχους.

## **ΠΕΡΙΠΤΩΣΗ 21<sup>η</sup> ( 17/9/99 )**

### **Τυχερά παιχνίδια στο Internet**

Η ιδιωτική επιχείρηση OCR Associates Inc. διενεργούσε τυχερά παιχνίδια στο Internet μέσω του site [www.raffle.com](http://www.raffle.com) μέχρι τη στιγμή που η εισαγγελία του New Mexico έκρινε τη λειτουργία της παράνομη.

Ο Chris Corpin, βοηθός εισαγγελέα, απαίτησε από το Εποπτικό Συμβούλιο<sup>11</sup> της επιχείρησης να σταματήσει τις δραστηριότητές της. Σε αντίθετη περίπτωση θα ζητούσε άδεια από την εισαγγελία να καταφύγει σε νομικές διαδικασίες για τη δίωξη της επιχείρησης, για τη διεξαγωγή λοταρίας μέσω του Internet.

Ο Janice Ruth Mc Crary, μέλος του Εποπτικού Συμβουλίου δήλωσε ότι το Εποπτικό Συμβούλιο θα κληθεί σε συνεδρίαση στις 24 Σεπτεμβρίου προκειμένου να αποφασίσει αν θα συμμορφωθεί ή όχι με την απαίτηση της εισαγγελίας. Μεταξύ άλλων δόθηκε εντολή να επιστραφούν τα χρήματα στους ανθρώπους που είχαν αγοράσει λαχνούς και μετά από ψηφοφορία των μελών του Εποπτικού Συμβουλίου η επιχείρηση σταμάτησε εθελοντικά τις δραστηριότητές της.

Ο Hall, διευθυντής της επιχείρησης, υπερασπίζοντας την, είπε, ότι η επιχείρηση λειτουργούσε ως ανάδοχος πολλών φιλανθρωπικών οργανισμών οι οποίοι διευκόλυναν τη λειτουργία τους μέσω των φιλανθρωπικών λοταριών που διοργάνωνε η εταιρεία του. Ανάμεσα σε άλλα, η επιχείρηση αναλάμβανε για χάρη των τοπικών φιλανθρωπικών οργανισμών, τη διαφήμιση, την προβολή, το μάρκετινγκ και τη συγκέντρωση των χρημάτων μέσω πιστωτικών καρτών από τις λοταρίες.

---

<sup>11</sup> Gaming Control Bord της OCR Associates.

Σύμφωνα πάλι με τον Hall η πρόθεση της εισαγγελίας δεν ήταν να κλείσει την επιχείρηση αφού ενεργούσε για χάρη φιλανθρωπικών οργανισμών και απεκόμισε σ' αυτές τεράστια κέρδη.

Απλά αισθάνθηκαν την απειλή παραβίασης του νόμου και ανησυχούσαν ότι άλλες επιχειρήσεις ίσως ακολουθούσαν το δρόμο που χάραξε η OCR Associates Inc.

Ο Corrin επισήμανε σε δήλωσή του ότι η επιχείρηση θα μπορούσε να υπογράψει συμβόλαια με μεγάλο αριθμό φιλανθρωπικών οργανισμών έτσι ώστε αν υποτεθεί ότι διεξάγει δύο λοταρίες για κάθε έναν από αυτούς, λοταρίες θα διεξάγονται καθημερινά όλο το χρόνο. Είπε ακόμη ότι το κράτος δεν σχεδιάζει να στραφεί εναντίον αυτών που παίζουν χαρτιά, μπλακ τζακ και άλλα τυχερά παιχνίδια στον υπολογιστή τους, αλλά εναντίον αυτών που τα διοργανώνουν.

### Αύξηση του τζόγου

Επίσημα στοιχεία για τον αριθμό των sites που διεξάγουν τυχερά παιχνίδια δεν υπάρχουν. Ο Corrin έκανε λόγο για την αναγκαιότητα να υπάρξει σχετική νομοθετική ρύθμιση. Οι περισσότερες πολιτείες αποσιωπούν το θέμα γιατί το Internet είναι κάτι καινούργιο και υπερβαίνει τη δικαιοδοσία των εισαγγελέων.

Πρόσφατη καταμέτρηση στο New Mexico έδειξε ότι οι κάτοικοί του δαπανούν περίπου \$ 180 εκ. το χρόνο σε τυχερά παιχνίδια στο Internet μεταξύ των οποίων είναι και οι λοταρίες, στοιχήματα για σπορ, παιχνίδια μπιλιάρδου και ιππόδρομο.

Τα \$ 180 εκ. δεν είναι παρά μόνο το 20% από το \$ 886 εκ. τα οποία ξοδεύουν συνολικά οι κάτοικοι του New Mexico σε τυχερά παιχνίδια.

Ο William Cadington, καθηγητής Οικονομικών και Διευθυντής του Institute for Study of Gambling and Commercial Gaming στο Πανεπιστήμιο της Nevada, στο Reno, επισήμανε τις δυσκολίες που υπάρχουν όσον αφορά την απαγόρευση των

τυχερών παιχνιδιών και στοιχημάτων στο Internet αφού για κάποιες πολιτείες, είναι παράνομο και για άλλες όχι.

Χαρακτήρισε την απόφαση της εισαγγελίας αυταρχική και υποκριτική αφού τα τελευταία 23 χρόνια το ποσοστό των τζογαδόρων έχει αυξηθεί σημαντικά μέσα και έξω από το Internet.

Η νομιμότητα των τυχερών παιχνιδιών στο Internet παραμένει αδιευκρίνιστη στις περισσότερες πολιτείες αφού δεν υπάρχουν σχετικοί νόμοι και το Κογκρέσσο δεν έχει αποφασίσει ακόμη τη θέσπισή τους.

Σύμφωνα με έρευνες στα δύο επόμενα χρόνια προβλέπεται αύξηση του ποσού που διατίθεται σε τυχερά παιχνίδια από \$ 2.3 εκ. σε \$10 εκ.

### **Άλλες καταδικαστικές αποφάσεις**

Πρόσφατα, το Ανώτατο Δικαστήριο της New York έκρινε παράνομο το τζόγο στο Internet και καταδίκασε το καζίνο WIGIC στο Internet, παρότι η διοίκηση του καζίνου βρίσκεται στην Antigua όπου ο τζόγος είναι νόμιμος.

Τα τελευταία 2 χρόνια πολλά άλλα καζίνο στο Internet ήρθαν αντιμέτωπα με μηνύσεις και έρευνες.

Τον προηγούμενο χρόνο 22 ιδιοκτήτες, διευθυντές και υπάλληλοι σε επιχειρήσεις που διεξήγαγαν στοιχήματα για διάφορους αγώνες σε αθλήματα, κατηγορήθηκαν για παραβίαση του νόμου.

### **ΠΕΡΙΠΤΩΣΗ 22<sup>η</sup> ( 28/9/99 )**

#### **Πλαστά πτυχία μέσω Internet**

Ένα site πανεπιστημίου στο Internet διέκοψε, όταν η Γενική Εισαγγελέας του Kansas, άσκησε μήνυση με την κατηγορία ότι τα πτυχία που παρείχε δεν ήταν αναγνωρισμένα.

Η Γενική Εισαγγελέας, Carla J. Stovall, έκανε μήνυση στα μέσα του Αυγούστου, κατά τον Leslie Edwin Snell, τον

διευθυντή του Πανεπιστημίου Montirello και διευθυντή άλλων επιχειρήσεων, κατηγορώντας τον ότι η σχολή του πωλούσε πλαστά διπλώματα.

Σαν αποτέλεσμα το Web site του πανεπιστημίου Monticello αφαιρέθηκε από το Internet.

Αρχικά το site του πανεπιστημίου φιλοξενούσε η DeGauss Technology Specialists στο Kansas. Στη θέση του site τώρα υπάρχει μία ανακοίνωση που λέει πως το web site αφαιρέθηκε μετά από εντολή του Γενικού Εισαγγελέα του Kansas για παραβίαση της συμφωνίας «Φιλοξενίας» μεταξύ του πελάτη και της DeGauss.

Η Stovall έκδωσε προσωρινή περιοριστική εντολή κατά του Snell με σκοπό να αποτρέψει παρόμοιες επιχειρηματικές δραστηριότητες του στο Kansas και πάγωσε τους τραπεζικούς του λογαριασμούς.

Η μήνυση επιδόθηκε στον Snell πριν δύο εβδομάδες, όταν αστυνομικοί κατάφεραν να τον εντοπίσουν στο Texas.

Οι κατηγορίες κατά του Snell περιλαμβάνουν: παροχή διπλωμάτων χωρίς άδεια, παραβιάσεις των δικαιωμάτων κοινωφελών οργανισμών και παραπλανητική δράση, μη εξουσιοδοτημένη διοίκηση επιχείρησης & πρακτικής στο Kansas, παραπλάνηση καταναλωτών.

Η εισαγγελέας ισχυρίζεται ότι ο Snell ασκεί και δικηγορία και παρουσιάζεται με το όνομα "Leslie Snell, ID".

Ακόμη, ότι ενώ αρχικά το Πανεπιστήμιο είχε το όνομα Thomas Jeffreson, αργότερα άλλαξε σε Monticello. Επανήλθε στο Internet αυτή τη φορά φιλοξενούμενο από μία άλλη εταιρεία του Web την Bensalem Pa, και η σχολή τώρα έχει το όνομα «Master Educators LLC» στο Dallas.

Τη μήνυση στο Kansas εναντίον του Snell διαδέχεται νέα μήνυση από την πολιτεία της Hawaii για εξαπάτηση καταναλωτών.

Διαφημίσεις του Πανεπιστημίου υπήρξαν κατά καιρούς στις σελίδες του Web: USA Today, The Economist και American Way.

Σύμφωνα με δικαστικά έγγραφα περισσότερα από 200 άτομα πλήρωσαν μεταξύ \$ 2.000 και \$ 8.000 για εκπαιδευτικές υπηρεσίες και εκπαιδευτικό υλικό.

Ο Snell αντιμετωπίζει αν κριθεί ένοχος πρόστιμο \$ 5.000 για κάθε μία από τις παραβιάσεις που διέπραξε, επιστροφή χρημάτων στους ανθρώπους που εξαπάτησε και πληρωμή των δικαστικών εξόδων.

Το Πανεπιστήμιο Monticello με δήλωση αρνείται τις κατηγορίες ισχυριζόμενο ότι είναι καθ' όλα νόμιμα & αποδεκτό από την Ακαδημία του Lugano, στην Ελβετία. Αρνείται ακόμη την λειτουργία του στο Kansas. Ισχυρίζεται ότι διατηρεί μία μη κερδοσκοπική επιχείρηση στην πολιτεία Nevada.

### **Εκπαίδευση στο Internet**

Η εκπαίδευση από απόσταση μέσω του Internet είναι μία εξαιρετικά δημοφιλής & εύκολη μέθοδος εκμάθησης και απόκτησης ανώτερης εκπαίδευσης.

Σύμφωνα με έρευνα του Υπουργείου Παιδείας στις ΗΠΑ το 1998 το 90% των Πανεπιστημιακών Σχολών παρείχε εκπαίδευση από απόσταση μέσω του Internet σε περισσότερους από 10.000 φοιτητές το 85% των σχολείων σε 3.000 με 10.000 μαθητές.

Ενώ διεθνώς υπολογίζεται<sup>12</sup> ότι το 2002 το 85% των Ανώτατων σχολών θα παρέχουν ανώτατη εκπαίδευση μέσω του Internet.

---

<sup>12</sup> Σύμφωνα με στατιστική που έκανε η εταιρεία International Data Corp., που βρίσκεται στα Framingham, Mass.



## ΠΕΡΙΠΤΩΣΗ 23<sup>η</sup> ( 29/9/99 )

### Αστυνομικός δημοσιοποιεί τις προσωπικές του απόψεις σε κρατικό site του Internet

Ο αστυνομικός John J. McDougall από την Florida εμφανίστηκε στην τηλεόραση στο κανάλι NBC στο τηλεοπτικό πρόγραμμα «Today» με την πρόφαση ότι ήθελε να υπερασπιστεί τις απόψεις του. Σύμφωνα με τον McDougall οι δημόσιοι υπάλληλοι έχουν υποχρέωση να μιλούν δημόσια για θέματα που προκύπτουν από την νομοθεσία και από δικαστικές αποφάσεις.

Είπε ότι πολλά προβλήματα που αντιμετωπίζει η χώρα οφείλονται σε αποφάσεις των τελευταίων 30 χρόνων.

Διαμάχη προκάλεσαν οι επίμαχες απόψεις του για τους ομοφυλόφιλους, τις φεμινίστριες και τους φιλελεύθερους.

Σε μία πρόσφατη δημοσίευση ενός γράμματός του στο Web site Lee County Sheriff's Department με το οποίο επιτίθεται προς διάφορες ομάδες ανθρώπων όπως την Γυναικεία Οργάνωση<sup>13</sup>, την Ένωση Αμερικανών Φιλελεύθερων<sup>14</sup> και την Οργάνωση Οικογενειακού Προγραμματισμού<sup>15</sup>. Χαρακτήρισε τις ομάδες αυτές «διαβολικές δυνάμεις» και τις κατηγορήσε ότι δρουν με σκοπό να υπονομεύσουν το κράτος.

Παρ' ότι οι νόμοι στη Florida λένε ότι ένας δημόσιος υπάλληλος απαγορεύεται να χρησιμοποιεί τη θέση του με σκοπό να εξασφαλίσει προσωπική προβολή κανένας δεν φαίνεται να δραστηριοποιείται. Η Επιτροπή για θέματα Ηθικής είπε ότι δεν θα ενεργήσει αν δεν της ζητηθεί. Ακόμη ο Δικαστής James G. Yeager δήλωσε ότι δεν είναι θέμα που αφορά την πολιτεία αν ο McDougall μπορεί να δημοσιεύει τις προσωπικές του θέσεις σε Web site χρηματοδοτούμενο από το κράτος.

Η αστυνομία είναι στο πλευρό του McDougall. Η Beth Schell, εκπρόσωπος δημοσίων σχέσεων του Αστυνομικού Τμήματος στο οποίο ανήκει ο Dougall ανακοίνωσε ότι υπήρξαν

<sup>13</sup> National Organization for Women.

<sup>14</sup> American Civil Liberties Union.

<sup>15</sup> Planned Parenthood.

εκατοντάδες e-mail, τηλεφωνικές κλήσεις ακόμη και από άλλους αστυνομικούς που υποστηρίζουν τον McDougall.

Η πρόεδρος της CEO<sup>16</sup>, Οικογενειακού Προγραμματισμού, είπε ότι εξετάζουν κάθε νομική ενέργεια που μπορεί να γίνει & ζήτησε από το κράτος να ενεργήσει. Χαρακτήρισε τις δηλώσεις του αστυνομικού εξωφρενικές και είπε ότι διαστρεβλώνουν τις θέσεις της πολιτείας. Ακόμη θεώρησε απαραίτητο να αφαιρεθεί το γράμμα από το Web site.

### ΠΕΡΙΠΤΩΣΗ 24<sup>η</sup> ( 1/10/99 )

#### CIA και FBI κατηγορούν Ινδία και Ισραήλ

Το NIPC<sup>17</sup>, το κέντρο προστασίας διεθνούς υποδομής του FBI, προειδοποίησε για μία ενδεχόμενη εισβολή στους υπολογιστές των Η.Π.Α. από το Ισραήλ και την Ινδία. Οι δύο αυτές χώρες, με την πρόφαση ότι προετοιμάζουν τους ηλεκτρονικούς υπολογιστές για το μικρόβιο του 2000, δημιουργούν μυστικές «εισόδους» σε συστήματα υπολογιστών των Η.Π.Α., οι οποίες θα τους παρέχουν πρόσβαση σε κρατικά μυστικά.

Στέλεχος της CIA και βοηθός στην έρευνα του NIPC, αναφέρει σ' ένα άρθρο ότι τα κράτη ή οι βιομηχανίες 2 χωρών ίσως έχουν ήδη διεισδύσει σε συστήματα υπολογιστών.

Ένας αναλυτής στη CIA, ο Terrill D. Maynard, έγραψε σ' ένα περιοδικό, ότι πολλές εταιρείες των Η.Π.Α. και κρατικές υπηρεσίες αφήνονται για την τελευταία στιγμή την προετοιμασία των υπολογιστών τους για το 2000, προσέλαβαν ξένους προγραμματιστές χωρίς να ελέγχουν τις συστάσεις τους. Το αποτέλεσμα ήταν οι ξένες χώρες ή εταιρείες να έχουν εύκολη πρόσβαση σε υπολογιστές στις Η.Π.Α.

Φημολογείται ότι ασυνείδητοι τεχνικοί ηλεκτρονικών υπολογιστών οι οποίοι επισκευάζουν ηλεκτρονικούς υπολογιστές,

<sup>16</sup> South Palm Beach/ Broward County Planned Parenthood.

<sup>17</sup> (NIPC) National Infrastructure Protection Center του FBI.

τοποθέτησαν σ' αυτούς κρυφές «πόρτες – παγίδες», με στόχο να χρησιμοποιηθούν μετά το έτος 2000 για να παίρνουν παράνομα μυστικές πληροφορίες.

Εικάζεται ότι πολλές ξένες εταιρείες ηλεκτρονικών υπολογιστών κατασκευάστηκαν με το πρόσχημα να εξυπηρετήσουν εταιρείες που ζητούσαν απεγνωσμένα βοήθεια για να αποφύγουν τα προβλήματα που θα δημιουργούσε η αλλαγή του έτους σε 2000 στους υπολογιστές τους.

Ο εκπρόσωπος Δημοσίων Σχέσεων του FBI, υποστήριξε την άποψη ότι η Ινδία και το Ισραήλ έχουν εχθρικές διαθέσεις και ότι αποτελούν κίνδυνο στο χώρο του Internet.

Το Προξενείο του Ισραήλ, χαρακτήρισε αυτές τις δηλώσεις αστείες και είπε ότι οι δηλώσεις του εκπροσώπου του FBI δεν είναι τίποτε άλλο από ανεύθυνες δηλώσεις.

Ειδικός στην ασφάλεια των υπολογιστών ο Drew Williams<sup>18</sup>, είπε στο κανάλι APBnews ότι στο χώρο της εργασίας του είναι γνωστές οι παραπάνω χώρες για την επιθετικότητά τους. Όμως χαρακτήρισε τις κατηγορίες για τις χώρες αυτές «φημολογίες» λόγω έλλειψης αποδείξεων.

Ανάλογη δήλωση έκανε και ο John Pike<sup>19</sup>: «Είναι ευθύνη του σκύλου να γαβγίζει. Όμως κάθε φορά που γαβγίζει δε σημαίνει ότι υπάρχει κλέφτης». Δεν απέκλεισε όμως την πιθανότητα οι εικασίες να είναι πραγματικότητα.

## **ΠΕΡΙΠΤΩΣΗ 25<sup>η</sup> ( 6/10/99 )**

### **Έφηβος αποδέχεται κατηγορίες εις βάρος του για hacking**

Ένας 19χρονος hacker με το όνομα Jay Satira, δήλωσε ένοχος στο δικαστήριο στην πόλη Westchester για την κατηγορία εισβολής σε ξένους υπολογιστές. Αντιμετωπίζει να καταδικαστεί σε 15 χρόνια φυλάκισης.

<sup>18</sup> Ο Drew Williams ειδικεύεται σε θέματα ασφάλειας στα συστήματα ηλεκτρονικών υπολογιστών και είναι διευθυντής της εταιρείας «Axent Technologies» στην πόλη Rockville.

<sup>19</sup> John Pike: Επιστήμονας αναλυτής στην Ομοσπονδία Αμερικανών Επιστημόνων (Federation of American Scientists).

Ο Satira εισέβαλε στους υπολογιστές της εταιρείας America Online's Internal (AOL) από τον υπολογιστή του σπιτιού του και έκανε αλλαγές σε κάποια από τα προγράμματα της εταιρείας. Η εταιρεία AOL ισχυρίζεται ότι η ζημία που προκάλεσε ο Satira υπολογίζεται περίπου σε \$50.000.

Τον μήνα Μάρτιο, η εταιρεία AOL αφού ερεύνησε την εισβολή κατάφερε να εντοπίσει τα ίχνη που οδήγησαν στο Satira. Η αστυνομία τον συνέλαβε στο σπίτι του και κατάσχεσε τον υπολογιστή του.

Ο Satira είχε παλιότερα εργαστεί ως εθελοντής στο τμήμα τεχνικής υποστήριξης της AOL. Συνδυάζοντας τις γνώσεις που απέκρινε στην AOL με άλλες πληροφορίες που περισυνέλεξε από άλλους hackers κατάφερε να εισβάλει στους υπολογιστές της εταιρείας αυτής.

## **ΠΕΡΙΠΤΩΣΗ 26<sup>η</sup> (6/10/99)**

### **Επιθέσεις μέσω Internet**

Τα κράτη και οι επιχειρήσεις μπορεί να προετοιμάζονται μανιωδώς για τον ιό του 2000 (ΥΣΚ) αλλά μια νέα έρευνα λει οτι η αντιμετώπιση του προβλήματος δεν είναι παρά μόνο η αρχή της απειλής που θα αντιμετωπίσει το διαδίκτυο.

Σύμφωνα με αναφορά του Κέντρου Προστασίας Υποδομής ηλεκτρονικών υπολογιστών, οι υπολογιστές στις Η.Π.Α θα βρεθούν σε μεγάλο κίνδυνο. Θα δεχθούν επιθέσεις μέσω του Internet από hackers, ξένα έθνη και τρομοκρατικές ομάδες πολύ αργότερα από την έναρξη της χιλιετίας.

Σχετική έρευνα έγινε και από το Υπουργείο Οικονομικών<sup>20</sup> ύστερα από απαίτηση του γερουσιαστή Robert Bennett που ηγείται της διοικούσας επιτροπής της Γερουσίας για το πρόβλημα των ηλεκτρονικών υπολογιστών του 2000.

Σύμφωνα με την έρευνα οι υπολογιστές της χώρας βρίσκονται σε αυξημένο κίνδυνο σοβαρών παρεμβολών. Η πρόκληση του έτους 2000 έδειξε εμφανώς και έντονα τους

<sup>20</sup> General Accounting Office (GAO)

κινδύνους που απειλούν όλα τα συστήματα συμπεριλαμβανομένων και των συστημάτων ηλεκτρονικών υπολογιστών. Παρ'όλα αυτά σημαντικές απειλές θα συνεχίσουν να υπάρχουν για μεγάλο χρονικό διάστημα και μετά την επίλυση του προβλήματος του έτους 2000.

### **Η σύνδεση στο Internet κρύβει κινδύνους**

Σύμφωνα με την παραπάνω έρευνα μεγάλο μέρος της απειλής προέρχεται από τη χρησιμότητα και την άνεση που παρέχει η αλματώδης ανάπτυξη των διαδικτύων στο Internet αυξάνει τον κίνδυνο αφού προβλήματα που υπάρχουν σε ένα σύστημα ηλεκτρονικών υπολογιστών μπορούν να μεταδοθούν σε ένα άλλο μέσω Internet.

Σε πείσμα της απειλής του ιού του 2000, δίνεται η ευκαιρία στους προγραμματιστές ηλεκτρονικών υπολογιστών να διαπιστώσουν το πόσο καλά θα ανταποκριθεί η χώρα της Αμερικής σε μια μαζική καταστροφή των υπολογιστικών συστημάτων. Από πολλές πλευρές το πρόβλημα της χρονιάς 2000 μπορεί να θεωρηθεί ως μια σημαντική εξέταση της ικανότητας της χώρας να προστατεύει τα σημαντικά και κρίσιμα αρχεία του κράτους.

### **Οι απειλές διαβρώνουν την εμπιστοσύνη του κοινού**

Το κράτος, οι επιχειρήσεις και οι βιοτεχνίες, οι τηλεπικοινωνίες, η εθνική άμυνα, ο τομέας της δικαιοσύνης και άλλες δημόσιες υπηρεσίες αντιμετωπίζουν τον μεγαλύτερο κίνδυνο.

Οι απειλές προέρχονται από διάφορες πλευρές όπως από τρομοκράτες, εχθρικά κράτη, δολιοφθορείς, κατασκόπους, εγκληματίες, φαρσέρ ακόμη και από φυσικές καταστροφές.

Τα αποτελέσματα από τέτοιες επιθέσεις μπορεί να προκαλέσουν σημαντικές ζημιές όπως τη φανέρωση μυστικών δεδομένων, την εμπόδιση της διεξαγωγής σημαντικών λειτουργιών, τη διατάραξη των λειτουργιών διαφόρων υπηρεσιών και τέλος τη διάβρωση της εμπιστοσύνης του κοινού στο σύστημα.

Και ενώ ακόμη δεν έχουν σημειωθεί σημαντικές επιθέσεις προς το κράτος των Η.Π.Α. μέσω του Internet, οι περιπτώσεις hacking και μολύνσεων από ιούς διαφόρων sites στο Web αυξάνονται.

Η ομάδα Computer Emergency Response Team<sup>21</sup> αναφέρει μεγάλη αύξηση στις αναφερόμενες περιπτώσεις από 1.334 που ήταν το 1993 σε 4.398 κατά τη διάρκεια του πρώτου εξαμήνου του 1999.

Σε έρευνα που διεξήγαγαν το Ινστιτούτο Ασφάλειας ηλεκτρονικών υπολογιστών<sup>22</sup> και το FBI βρέθηκε ότι το 30% των 521 επιχειρήσεων που συμμετείχαν στην έρευνα δέχθηκαν παρεμβολές στα συστήματα των ηλεκτρονικών υπολογιστών τους. Επιπλέον σημειώθηκαν πολλά περισσότερα περιστατικά hacking τα οποία είτε είναι μικρά είτε περνούν απαρατήρητα.

### **Στόχος στρατιωτικά μυστικά**

Επίθεση δέχθηκε το Υπουργείο Άμυνας των Η.Π.Α. τον Φεβρουάριο του 1998. Η επίθεση ονομάστηκε «Solaris Sunrise» – το όνομα προέρχεται από το λειτουργικό σύστημα Solaris, μια έκδοση του UNIX που χρησιμοποιούσε το Υπουργείο. Η επίθεση ήταν δυσοίωνη αφού ο στόχος ήταν πληροφορίες – κλειδιά σε χρόνο που ο στρατός ετοιμαζόταν για πιθανή επίθεση εναντίον του Ιράκ.

Η αντίδραση του κράτους είχε αρχίσει από τα μέσα της δεκαετίας του '90 όταν διαπιστώθηκε η ανάγκη να λυθούν προβλήματα ασφάλειας.

Μεγάλη προσπάθεια προς την κατεύθυνση αυτή έγινε από το κράτος το 1998. Τότε ο Πρόεδρος Clinton ενέκρινε την κατευθυντήρια οδηγία Νο 63 (PDD-63)<sup>23</sup> με την οποία απαιτούσε από τις δημόσιες υπηρεσίες και τον ιδιωτικό τομέα να αντιμετωπίσουν τα θέματα ασφάλειας.

---

<sup>21</sup> Η ομάδα Computer Emergency Response Team χρηματοδοτείται από το Αμερικάνικο Κράτος με σκοπό να εκτελέσει προγράμματα ασφάλειας.

<sup>22</sup> Computer Security Institute.

<sup>23</sup> Κατευθυντήρια οδηγία Νο 63 ή αλλιώς PDD-63 (Presidential Decision Directive-63).

Μόλις την προηγούμενη εβδομάδα το Υπουργείο Θησαυροφυλακίου, μεγάλες τράπεζες και επώνυμες χρηματιστηριακές εταιρείες έφτιαξαν ένα κέντρο που στόχος του είναι να εντοπίζει τυχόν εγκληματικές πράξεις ή παραβιάσεις στο Internet με το οποίο θα μοιράζονται και θα ανταλλάσσουν εμπιστευτικές πληροφορίες για τυχόν απειλές.

### **10 Πολιτείες απροετοίμαστες για το 2000**

Το Υπουργείο Οικονομικών σε μια αναφορά 228 σελίδων, εκφράζει ανησυχίες για το σύστημα υγείας της χώρας και για τις μικρές επιχειρήσεις.

Ακόμη, 10 πολιτείες βρέθηκαν ανέτοιμες όσον αφορά το σύστημα υγείας μεταξύ των οποίων: Alaska, Alabama, Massachusetts, New Hampshire, New Mexico, North Carolina, North Dakota και Vermont.

Ελλείψεις βρέθηκαν και σε τοπικά συστήματα παροχής νερού και αστυνομικά τμήματα. Τον Αύγουστο του 1999 μόνο το 34% των αστυνομικών τμημάτων<sup>24</sup> και μόνο το 47% των κοινοτήτων ασχολούνται με την επίλυση του προβλήματος.

Τον Ιούλιο του 1999 η Ένωση Metropolitan Sewerage Agencies έφτιαξε μια ομάδα με αντικείμενο τη συνεχή παρακολούθηση και αξιολόγηση του ιού του 2000. Από τα 259 μέλη μόνο τα 51 ανταποκρίθηκαν και από αυτά μόνο το 14% είναι έτοιμα.

### **ΠΕΡΙΠΤΩΣΗ 27<sup>η</sup> ( 7/10/99 )**

#### **NOMOS GIA THN PROSTASIA TON ANHLIKON**

Ένας νέος νόμος που θεσπίστηκε στην πολιτεία Virginia και τέθηκε σε ισχύ από την 1η Ιουλίου προβλέπει την απαγόρευση κυκλοφορίας στο Internet υλικού που θεωρείται βλαβερό για τους νέους.

<sup>24</sup> Τα αστυνομικά τμήματα θα αντιμετωπίζουν προβλήματα όσον αφορά το σύστημα PSAPS. Ένα σύστημα ηλεκτρονικών υπολογιστών που χρησιμοποιείται για την λήψη και την επίσπευση των τηλεφωνικών κλήσεων προς και από τα αστυνομικά τμήματα.

Πολέμιοι του νόμου ισχυρίζονται ότι ο νόμος αυτός αντιτίθεται στο συνταγματικό δικαίωμα της ελευθερίας και της προστασίας του λόγου των ενηλίκων μέσα και έξω από τα σύνορα της πολιτείας εξαιτίας του διεθνούς χαρακτήρα του Internet, συμπεριλαμβανομένων και της αλληλογραφίας στο Internet (e-mail). Υποστηρίζουν ότι ο νόμος παραβιάζει άρθρα & διατάξεις των Συνταγμάτων των ΗΠΑ.

Το νομοθετικό σώμα μετά από συνεδρίαση ψήφισε το νόμο στις 7 Απριλίου, ο οποίος ενοχοποιεί την εν γνώση έκθεση στο Internet υλικού που θεωρείται βλαβερό για τους νέους στις εξής περιπτώσεις: όταν το υλικό είναι για διαφημιστικούς σκοπούς και σε κάθε άλλη περίπτωση όταν η πρόσβαση σ' αυτό είναι εύκολη.

Ο Robert Marshall, εξουσιοδοτημένος αντιπρόσωπος του κράτους και υποστηρικτής του νόμου, δήλωσε ότι πρέπει να αντιμετωπίσουν πολύ προσεκτικά τα εμπορικά sites που πωλούν υλικό για ενήλικες.

Αγωγή έκαναν με σκοπό να ανατρέψουν τον νέο νόμο ο συνδυασμός First Amendment advocates and Internet businesses και η εταιρεία Net Sex Biz. Άλλοι ενάγοντες στην υπόθεση (συνολικά 16) είναι: η εταιρεία PSINet Inc. (μεγάλη εταιρεία παροχής υπηρεσιών του Internet), εμπορικές και επιχειρηματικές ενώσεις όπως και Commercial Internet Exchange Association & η Virginia Internet Service Provider's Alliance. Ακόμη συγγραφείς και πωλητές λογοτεχνικών βιβλίων, καλλιτέχνες & άνθρωποι που παρέχουν πληροφορίες σε θέματα υγείας στο Internet.

Η αγωγή έγινε στο Δικαστήριο της Περιφέρειας της Ανατολικής Virginia. Συνήγοροι υπεράσπισης είναι ο James Gilmore και ο Γενικός Εισαγγελέας Mark L. Earley.

Τον Νοέμβριο η εταιρεία People for the American Way (PFAN), αναγκάστηκε να εφαρμόσει ένα μέτρο με το οποίο έπρεπε να ζητά πληροφορίες για τα στοιχεία όσων ήθελαν να επισκεφτούν τα sites της. Διαμαρτυρόμενη ζήτησε ένα λιγότερο αυστηρό μέτρο και πρότεινε ο έλεγχος της πρόσβασης των παιδιών στο Internet να γίνεται από τους γονείς και όχι από κράτος.



Ο πρόεδρος της PFAN, είπε ότι ευτυχώς το Σύνταγμα υπερिशύει. Πράγματι μέχρι τώρα κανείς δεν έχει κατηγορηθεί για παραβίαση του νόμου, ο οποίος προβλέπει για τον παραβάτη 12 μήνες φυλακή και πρόστιμο \$2.500.

Εξαιτίας του τρόπου με τον οποίο λειτουργεί το Internet ο νόμος αυτός θα επιβάλει περιορισμούς στην επικοινωνία μεταξύ ενηλίκων που συνομιλούν στο Internet, σε πολύτιμες εργασίες, στη λογοτεχνία, στην τέχνη και σε άλλους τομείς στο Internet. Αυτός είναι ο κύριος λόγος που έχει προκαλέσει τόσα κοινωνικά σχόλια. Άλλοι λόγοι διαμαρτυρίας είναι εμπορικοί, όπως αυτός του Glenn Hauman, πρόεδρο και εκδότη του BiblioBytes που είπε ότι νόμοι σαν αυτόν θα σκοτώσουν την αγορά του Internet. Οι άνθρωποι περνούν ώρες στο Internet διαβάζοντας, μιλώντας & αγοράζοντας πράγματα & βιβλία. Έχει γίνει τρόπος ζωής & πηγή εισοδήματος για πολλούς ανθρώπους. Οι ενήλικες θα πρέπει να περιορίσουν τη χρήση του Internet σε θέματα που η πολιτεία της Virginia θεωρεί αποδεκτά για τους νέους.

Σημαντικό είναι να σημειώσουμε εδώ ότι 2 συνταγματικοί νόμοι & 5 νόμοι πολιτειών που αφορούσαν την προστασία των ανηλίκων στο Internet έχουν κιάλας πάψει να ισχύουν με αποφάσεις δικαστηρίων.

### **ΠΕΡΙΠΤΩΣΗ 28<sup>η</sup> ( 9/10/99 )**

#### **Τα χρήματα του Αμερικάνικου κράτους κινδυνεύουν λόγω έλλειψης μέτρων ασφαλείας**

Σύμφωνα με το Υπουργείο Οικονομικών εκατομμύρια δολάρια από πληρωμές και φόρους βρίσκονται σε μεγάλο κίνδυνο να χαθούν ή να πέσουν στα χέρια απατεώνων. Επιπλέον, τεράστιες ποσότητες δεδομένων κινδυνεύουν από παράνομη διαγραφή τους και κρίσιμες λειτουργίες βασισμένες σε ηλεκτρονικό υπολογιστή είναι τρωτές σε σοβαρές παρεμβολές.

Το Υπουργείο Οικονομικών, ύστερα από εξέταση των 7 κύριων κεντρικών υπολογιστικών μονάδων που επεξεργάζονται ευαίσθητα δεδομένα στην Υπηρεσία Οικονομικής Διαχείρισης

του Θησαυροφυλακίου, για το διάστημα Αύγουστο 1998 – Φεβρουάριο 1999 διαπίστωσε:

- Ημιτελή προστασία ελέγχου στις εισόδους των κέντρων φύλαξης δεδομένων και εγκαταστάσεων των ηλεκτρονικών υπολογιστών.
- Ελλιπής έλεγχος στις ταυτότητες & τους κωδικούς πρόσβασης σε αρχεία υπολογιστών.
- Εκπρόθεσμα και ανακριβή δεδομένα.

Η σοβαρότητα των αποτελεσμάτων βαδίζει παράλληλα με την σοβαρότητα των ευθυνών της Υπηρεσίας Διαχείρισης Θησαυροφυλακίου που λειτουργεί ως λογιστής του κράτους, συνεργάζεται με το Υπουργείο Δικαιοσύνης και με 11.000 οικονομικά ιδρύματα. Το 1999 είχε υπό την εποπτεία του \$1,6 τρισεκατομμύρια σε πληρωμές και \$1,7 τρισεκατομμύρια από έσοδα. Σ' αυτά συμπεριλαμβάνονται η κοινωνική ασφάλιση (και συντάξεις βετεράνων), φόροι και επιστροφές, μισθοί δημοσίων υπαλλήλων, έσοδα από το τελωνείο και από πρόστιμα. Ακόμη διατηρεί αρχεία του ισολογισμού που χρησιμοποιεί το Κογκρέσο και του κρατικού προϋπολογισμού.

Υπεύθυνοι του Θησαυροφυλακίου είπαν ότι έκαναν τις απαραίτητες ενέργειες για τη διόρθωση των προβλημάτων ασφαλείας, ενώ διόρθωσαν άλλες αδυναμίες που διαπιστώθηκαν σε συστήματα υπολογιστών τα οποία διαχειρίζονται τις οικονομικές συναλλαγές του κράτους.

Ο Connie Craig, εκπρόσωπος Δημοσίων Σχέσεων της Υπηρεσίας Οικονομικής Διαχείρισης Θησαυροφυλακίου είπε, ότι με προσωπική του εκτίμηση η κατάσταση έχει βελτιωθεί ύστερα από την έκθεση των προβλημάτων. Πρόσθεσε ότι δεν αντιπροσωπεύουν τα παραπάνω την σημερινή πραγματικότητα, καθώς έχουν γίνει πολλά βήματα για να διορθωθούν οι αδυναμίες που διαπιστώθηκαν.

## ΠΕΡΙΠΤΩΣΗ 29<sup>η</sup> (10/10/99)

### Αστυνομικοί συλλαμβάνουν συμμορία κακοποιών ανηλίκων στο Internet

Ο Craig Luecke, πυροσβέστης και ενθουσιώδης χρήστης του Internet καθώς ήταν συνδεδεμένος στο Internet από το σπίτι του όπως συνήθιζε, ένα μήνυμα εμφανίστηκε στην οθόνη του. Ο αποστολέας του μηνύματος χρησιμοποιούσε το όνομα «chckrflag» και ήταν συνδρομητής της εταιρείας America On line. Ο Luecke δεν αναγνώρισε το όνομα παρόλα αυτά απάντησε και τότε ο «chckrflag» τον ρώτησε αν του άρεσαν ακόμη οι σεξουαλικές παρεκκλίσεις. Όταν ο Luecke ρώτησε γιατί, η απάντηση ήταν ότι «εγώ και η γυναίκα μου ψάχνουμε για ένα 3χρονο».

Έτσι άρχισε στις 26 Μαρτίου 1998 η συζήτηση που οδήγησε στις κατηγορίες σεξουαλικής εκμετάλλευσης παιδιών κατά τριών ατόμων.

Ο Luecke δεν έψαχνε για εκκεντρικές ερωτικές περιπέτειες, συνέχισε όμως τις συνομιλίες γιατί νόμιζε ότι κάποιος φίλος του έκανε κάποια ανώνυμη φάρσα. Όταν όμως οι σεξουαλικές συζητήσεις στράφηκαν σε παιδιά, κάλεσε την αστυνομία.

Εντός 30 λεπτών από την ώρα που κάλεσε την αστυνομία στις 29 Μαρτίου, ο Sgt Barry Lease, αστυνόμος και διοικητής της Αστυνομίας της πολιτείας Maryland και ηγέτης της ομάδας εγκλημάτων στο Internet άρχισε να καταγράφει τις συζητήσεις των 3 ατόμων στο Internet με την άδεια του Luecke.

Για 4 μέρες παρακολουθούσε τις συζητήσεις του Luecke με τον «chckrflag» και άλλων που απαντούσαν στα μηνύματα τους οι οποίες γινόντουσαν μέσω του Instant Messenger της AOL. Το Instant Messenger επιτρέπει στους συνδρομητές του να ανταλλάσσουν μηνύματα όταν βρίσκονται συνδεδεμένοι με το Internet.

Στις 29 Μαρτίου, ο Luecke επικοινωνήσε 5 φορές με τον «chckrflag» μεταξύ 5:14 π.μ. και 11:48μ.μ. Σε μια από τις συζητήσεις αυτές ο «chckrflag» έδωσε στον Luecke τη

διεύθυνση της φιλενάδας του και του είπε ότι θα μπορούσε να κάνει έρωτα στην κόρη της.

Σε άλλη συζήτηση περιέγραφε με λεπτομέρειες μια ερωτική πράξη μεταξύ του 5χρονου κοριτσιού και ενός άνδρα που χρησιμοποιούσε το όνομα «dad4fam» στο Internet και ο οποίος είχε αρχίσει επίσης συνομιλίες με τον Luecke.

Η μητέρα που συμμετείχε στις συζητήσεις, την 1η Απριλίου έστειλε μήνυμα στον Luecke ότι δεν θα επέτρεπε πια σε άνδρες να κάνουν έρωτα με την κόρη της γιατί το κοριτσάκι είχε εφιάλτες.

Την ίδια μέρα η αστυνομία μίλησε με τα κορίτσια στο σχολείο τους και πήγε στο διαμέρισμα του «chckrflag» όπου βρισκόταν αυτός και η μητέρα των παιδιών. Έψαξαν στον υπολογιστή του και βρήκαν εκατοντάδες μηνύματα και πορνογραφικό υλικό, φωτογραφίες και video clips με παιδιά.

Ο «chckrflag» το πραγματικό όνομα του οποίου είναι Scott Edward Yigling, 33χρονος σύμβουλος εταιρείας ηλεκτρονικών υπολογιστών κατηγορείται για σεξουαλική εκμετάλλευση του 5χρονου κοριτσιού και για παρενόχληση της 6χρονης αδελφής της. Στην κατάθεση του την προηγούμενη εβδομάδα αρνήθηκε τις κατηγορίες και κατέθεσε ότι είχε φυλάξει τα πορνό μηνύματα που είχε λάβει γιατί ήθελε να ξεσκεπάσει τους ανθρώπους που συμμετείχαν σ' αυτές τις πράξεις.

Σύμφωνα με τον δικηγόρο υπεράσπισης Thomas Barse δεν υπάρχουν αποδείξεις που να επιβεβαιώνουν τους ισχυρισμούς του.

Μειωμένες κατηγορίες σεξουαλικής παρενόχλησης αντιμετωπίζει και η μητέρα, η οποία δήλωσε ένοχη.

Το τρίτο πρόσωπο που εμπλέκεται στην υπόθεση είναι ο Daniel C. Benton, 41 χρόνων, προγραμματιστής ηλεκτρονικών υπολογιστών από την περιοχή Poolsevill ο οποίος παραδέχτηκε ότι κακοποίησε το παιδί στις 31 Μαρτίου και θα δικαστεί σύντομα.

Ο Luecke κατέθεσε ότι σκέφτηκε πως ίσως να υπήρχε κάποια πραγματικότητα σ' όλα αυτά γι' αυτό και κάλεσε την αστυνομία.

Η μητέρα και ο Benton κατέθεσαν εναντίον του Luecke.

### **ΠΕΡΙΠΤΩΣΗ 30<sup>η</sup> ( 11/10/99 )**

#### **Πρόγραμμα καταστροφής των ηλεκτρονικών μηνυμάτων σχεδιάστηκε για να βοηθήσει τις επιχειρήσεις**

Μία εταιρεία ηλεκτρονικών υπολογιστών ισχυρίζεται ότι σε μία προσπάθεια να προστατέψει τα μυστικά των επιχειρήσεων από τα περίεργα βλέμματα, κατασκεύασε έναν «αυτοκαταστρεφόμενο» μηχανισμό ο οποίος κάνει τα ηλεκτρονικά μηνύματα (e-mails) να εξαφανίζονται χωρίς να αφήνουν ίχνη.

Η νέα τεχνολογία που έχει το όνομα Disappearing<sup>25</sup> Inc., λειτουργεί με όλα τα προγράμματα e-mail για την αποκρυπτογράφηση, εύρεση και διαγραφή μηνυμάτων, συμπεριλαμβανομένων και αυτών που έχουν αποθηκευτεί σε δισκέτες ή σε άλλα μέρη του υπολογιστή.

MacIen Marvit, διευθυντικό στέλεχος της εταιρείας που κατασκεύασε το πρόγραμμα σε δήλωσή του παρομοίασε τα μη προστατευόμενα e-mail με καρτ-ποστάλ.

Είπε ότι λάθος άνθρωποι μπορούν να τα διαβάσουν και επιπλέον υπάρχουν για πάντα. Είπε ότι η πολιτική της εταιρείας του όσον αφορά τα e-mail είναι η ύπαρξη ενός συστήματος διαχείρισης και προστασίας των μηνυμάτων όσο βρίσκονται σε χρήση και η διαγραφή τους όταν το επιλέξει η κάθε επιχείρηση.

Το πρόγραμμα το οποίο θα βγει στην αγορά στις αρχές του έτους 2000, αποκρύπτει τα μηνύματα με ένα μοναδικό κλειδί έτσι ώστε να προλαμβάνει κάθε παράνομη πρόσβαση σ' αυτά. Οι παραλήπτες των μηνυμάτων θα πρέπει να δίνουν κάθε φορά κάποιες πληροφορίες για την ταυτότητά τους προκειμένου να

<sup>25</sup> Disappearing= Εξαφάνιση

διαβάσουν ένα μήνυμα. Όταν το κλειδί καταστραφεί, τότε τα μηνύματα είναι αδύνατον να διαβαστούν.

Όταν ένα μήνυμα διαγράφεται με την εντολή DELETE (=ΔΙΑΓΡΑΦΗ), όλα τα αντίγραφα και αυτά που βρίσκονται σε δισκέτες ή σε άλλα μέρη των υπολογιστών, δεν μπορούν να διαβαστούν. Αυτό μειώνει την ευθύνη που δημιουργείται από πρόχειρα και προσωρινά αρχειοθετημένα e-mails. Το software του προγράμματος επιτρέπει στις επιχειρήσεις τη δημιουργία και την εφαρμογή πολιτικής αυτόματου ελέγχου όσον αφορά το χρόνο που επιθυμούν να παραμένουν τα κάθε είδους μηνύματα στους υπολογιστές τους.

Μία δημόσια υπηρεσία για παράδειγμα μπορεί να προσαρμόσει το πρόγραμμα έτσι ώστε να υπάρχει μια κατηγορία μηνυμάτων μόνιμα αρχειοθετημένων και άλλη κατηγορία μηνυμάτων τα οποία θα διαγράφονται μετά την πάροδο 90 ημερών.

Ο εκδότης του Privacy Times, Evan Hendricks, είπε ότι είναι μια ακόμη προσπάθεια προστασίας της ιδιωτικής ζωής.

Το πρόγραμμα λειτουργεί ανεξάρτητα με το πρόγραμμα e-mail που χρησιμοποιούν ο αποστολέας και ο παραλήπτης. Στα προγράμματα e-mail συμπεριλαμβάνονται και τα παρακάτω: Web Mail, Microsoft Outlook, Netscape Mail και Eudora. Η εταιρεία διαβεβαιώνει ότι οι χρήστες αυτών των προγραμμάτων δεν θα διαπιστώσουν καμία αλλαγή στη λειτουργία των προγραμμάτων τους.

### **Κίνδυνοι από τη χρήση της νέας τεχνολογίας**

Η νέα αυτή τεχνολογία θέτει πιθανά μελλοντικά προβλήματα για την αστυνομία και για τους εισαγγελείς δίωξης οι οποίοι βασίζονται σε πληροφορίες από τα ηλεκτρονικά μηνύματα για να ανοίξουν μία υπόθεση, ιδιαίτερα σε μία περίοδο που παρατηρείται σημαντική αύξηση των εγκληματικών πράξεων στο Internet. Τα e-mails σε πολλές περιπτώσεις χρησιμοποιούνται ως αποδεικτικά στοιχεία και ως μέσο για τον εντοπισμό των υπόπτων.

Το πρόγραμμα που σχεδιάστηκε για να προστατέψει και να συμβάλλει θετικά στις κοινωνικές και εμπορικές συναλλαγές, πιθανόν να δημιουργήσει και κάποια ακούσια αποτελέσματα, όπως της προστασίας των απατεώνων και των παιδόφιλων στον κυβερνόχωρο.

Εισαγγελείς και πολίτες που καταφεύγουν στα δικαστήρια είχαν βρει ένα πραγματικό χρυσωρυχείο αποδεικτικών στοιχείων στα e-mails. Όμως η τεχνολογία τώρα τους παίρνει πίσω αυτό που τους έδωσε. Το αίτημα για προστασία της ιδιωτικής ζωής, οδήγησε στη δημιουργία ενός τεχνολογικού περιβάλλοντος που θα την προστατεύει, σχεδιασμένο να καταστρέφει ή να καλύπτει δεδομένα αποκλείοντας τη δυνατότητα να χρησιμοποιηθούν για δευτερεύοντες σκοπούς. Οι εισαγγελείς το μόνο που μπορούν να κάνουν είναι να προσαρμοστούν στη νέα πραγματικότητα.

### Νομικές απόψεις

Η Susan Brener, πρότανης και καθηγήτρια νομικής στην Ανωτάτη Σχολή Νομικής του Πανεπιστημίου Dayton στο Ohio, είπε ότι οι επιχειρήσεις πρέπει να είναι ιδιαίτερα προσεκτικές με τις πληροφορίες που καταστρέφουν.

Ας υποθέσουμε ότι μία εταιρεία κληθεί δικαστικά να παρουσιάσει στο δικαστήριο τα αρχεία της για τα τελευταία 5 χρόνια λειτουργίας της σε 2 εβδομάδες. Πιθανότατα θα θεωρηθεί ύποπτο αν η εταιρεία αρχίσει να καταστρέφει έγγραφα και αρχεία. Η μοναδική περίπτωση να μη φανεί ύποπτη η καταστροφή των αρχείων, είναι αν έχει τεθεί ένα χρονικό διάστημα 3 χρόνων παραμονής των αρχείων πριν την καταστροφή τους. Θέλησε η Brener μ' αυτό το παράδειγμα να τονίσει τη σημασία που έχει για τις επιχειρήσεις να επιλέξουν τη σωστή στρατηγική σχετικά με την καταστροφή των αρχείων τους, όσον αφορά τα e-mails, παρ' ότι το κράτος δεν έχει υπαγορεύσει το χρονικό διάστημα στο οποίο θα πρέπει να διατηρούνται τα αρχεία.

Σημαντικό είναι το ότι σε διάφορες περιπτώσεις ανακρίσεων, οι έρευνες αφορούν παρελθοντικές περιόδους και εκτείνονται ίσως ακόμη και σε πολλά χρόνια πριν. Προκειμένου να γίνει μία τέτοια έρευνα οι εισαγγελείς θα πρέπει να έχουν πρόσβαση στα αρχεία των χρονικών περιόδων που ερευνούν.

Ο Michael Froomkin, καθηγητής νομικής στο Πανεπιστήμιο του Miami και ειδικός στην ασφάλεια υπολογιστών, θεωρεί ότι έχει δοθεί μεγαλύτερη σημασία στο θέμα αυτό απ' ό τι πραγματικά έχει. Είπε ότι η ιδέα ότι το πρόγραμμα αυτό θα προστατέψει τους απατεώνες στο Internet μοιάζει με μία εκπληκτικά αποτελεσματική διαφήμιση του προϊόντος.

### **ΠΕΡΙΠΤΩΣΗ 31<sup>η</sup> ( 12/10/99 )**

#### **Νόμος καταστρατηγεί το δικαίωμα του απορρήτου για τους εργαζόμενους**

Ο Κυβερνήτης της πολιτείας της California πρόβαλε βέτο στο νοσοκομείο περί απορρήτου των ηλεκτρονικών μηνυμάτων και επέτρεψε στις επιχειρήσεις να παρακολουθούν τα μηνύματα των υπαλλήλων τους.

Αδικημένοι αισθάνονται οι υπέρμαχοι του νομοσχεδίου που δήλωσαν ότι η πολιτεία της California έχασε την ευκαιρία να εδραιώσει το δικαίωμα των υπαλλήλων να διατηρούν το απόρρητο της αλληλογραφίας τους.

Εξαιτίας του ότι εκατοντάδες επιχειρήσεις εφαρμόζουν μέτρα παρακολούθησης, το βέτο του κυβερνήτη David Sobel προβλέπεται η γραπτή ενημέρωση των υπαλλήλων από τους εργοδότες για τα μέτρα παρακολούθησης.

Σε δηλώσεις του ο κυβερνήτης παρομοίασε την παρακολούθηση των e-mails των υπαλλήλων με την παρακολούθηση για το αν κάνουν υπεραστικά τηλέφωνα. Σημείωσε ότι οι επιχειρήσεις κινδυνεύουν να μηνυθούν αν οι υπάλληλοι τους χρησιμοποιούν τους υπολογιστές με σκοπό να εξαπατήσουν ή να παρενοχλήσουν κάποιον. Είπε ακόμη ότι αφού οι ηλεκτρονικοί υπολογιστές και τα ηλεκτρονικά μηνύματα αποτελούν μέρος της ιδιοκτησίας των επιχειρήσεων, τότε έχουν το δικαίωμα να τα παρακολουθούν.

Οι εργοδότες ισχυρίζονται ότι επιδιώκουν με τα μέτρα παρακολούθησης να αυξήσουν την παραγωγικότητα, να προλάβουν τυχόν προβλήματα των υπολογιστών και να



αποφύγουν τα νομικά προβλήματα που μπορούν να δημιουργηθούν είτε από τη διαρροή μυστικών της επιχείρησης είτε από την αποστολή ρατσιστικών ή παρενοχλητικών μηνυμάτων.

Ο Γενικός σύμβουλος του Κέντρου Electronic Privacy Information<sup>26</sup> χαρακτήρισε το βέτο του Κυβερνήτη περίπλοκο. Είπε ότι καθώς ο βιομηχανικός τομέας αναπτύσσεται, αυξάνονται και οι θερμοί υποστηρικτές της μυστικής κατασκοπείας των υπαλλήλων.

Από το κόμμα των Δημοκρατικών, τη διαφωνία της με τις απόψεις του Κυβερνήτη δήλωσε η Debra Bowen η οποία είπε χαρακτηριστικά: «Το ότι ο εργοδότης σου παρέχει δωμάτιο για ανάπαυση δε σημαίνει ότι έχει και το δικαίωμα να βιντεοσκοπεί οτιδήποτε κάνεις εκεί μέσα».

Έρευνα της American Management Association αναφέρει ότι το 20% από δείγμα 1000 επιχειρήσεων στην πολιτεία της California και 6 δημόσιες υπηρεσίες, διαθέτουν προγράμματα παρακολούθησης στους ηλεκτρονικούς υπολογιστές τους.

Άλλη έρευνα που διεξήγαγε η εταιρεία στατιστικών ερευνών International Data Corp. στο Framingham, έδειξε ότι μέχρι το έτος 2001 υπολογίζεται ότι το 80% των μεγάλων επιχειρήσεων θα χρησιμοποιούν προγράμματα παρακολούθησης του ηλεκτρονικού ταχυδρομείου των υπαλλήλων τους.

### **ΠΕΡΙΠΤΩΣΗ 32<sup>η</sup> (14/10/99)**

#### **Η δολοφονία της JonBonet στο Internet**

Υστερα από τη δολοφονία της βασίλισσας της ομορφιάς JonBonet Ramsey το 1996, το Internet έχει γίνει μέρος ανταλλαγής απόψεων για τους πενθώντες, προσφέροντας παράλληλα και θεωρίες για το έγκλημα.

Διαμάχη δημιουργήθηκε όταν η εισαγγελία ανακοίνωσε ότι δεν θα αποδοθούν κατηγορίες στους ύποπτους για το φόνο της

---

<sup>26</sup> Μία μη κερδοσκοπική ερευνητική ομάδα.

κοπέλας. Πολλοί κατηγόρησαν την εισαγγελία ότι συνεργάζεται με την οικογένεια Ramsey προκειμένου να καλύψει το έγκλημα.

Στο Internet περιφέρονται θεωρίες για πολιτικές δολοπλοκίες και συνωμοσίες ενώ ανώνυμοι πολίτες εκφράζουν οργή για την υπόθεση.

Κάποια με το όνομα «Shirley» έγραψε στο alt.abuse com-recovery newsgroup: «Είμαι τόσο οργισμένη με τη δικαιοσύνη που θα μπορούσα να φτύσω νύχια. Κλείνουν την υπόθεση JonBenet Ramsey λόγω έλλειψης αποδεικτικών στοιχείων».

Άλλη με το όνομα «Linda» έγραψε στο alt.true-crime: «Νευρίασα τόσο που θα νόμιζε κανείς ότι συνδέομαι προσωπικά με την υπόθεση. Πίστευα ότι κάποια στιγμή το Ανώτατο Δικαστήριο θα έστελνε στο πειθαρχικό τον Εισαγγελέα για την απραξία του».

Εκατοντάδες ακόμη πολίτες κατηγορούν τον Γενικό Εισαγγελέα Alex Hunter ότι δεν χειρίστηκε καλά την υπόθεση.

### **Επικοινωνία με το φάντασμα της JonBenet**

Κατά τη διάρκεια που το Ανώτατο Δικαστήριο μάζευε αποδείξεις και έπαιρνε συνεντεύξεις από αυτόπτες μάρτυρες, χρήστες του Internet προσπαθούσαν να εξιγνιάσουν το έγκλημα.

Σε μία προσπάθεια να βοηθήσουν την αστυνομία και το FBI, ισχυρίζονται ότι ήρθαν σ' επαφή με το φάντασμα της JonBenet Ramsey. Σε μία από αυτές τις επαφές ειπώθηκαν τα εξής:

- Σου λείπει η ζωή σου;
- Ναι.
- Είναι ανακατεμένοι οι γονείς σου;
- Ναι.
- Σου λείπει η μητέρα σου;
- ... (καμία αντίδραση).
- Σου λείπει ο πατέρας σου;
- Λίγο.

Οι γνώμες για το συμβάν έχουν κατακλύσει πολλά Web sites που αφορούν εγκλήματα.

Κάποιος με το ψευδώνυμο «Jameson» δημιούργησε ένα Forum<sup>27</sup> με το δικό του όνομα domain<sup>28</sup> τον Ιούνιο του 1999. Ως πρόεδρος του Forum, δήλωσε ότι προσπαθεί να κατευθύνει με λογική τις συζητήσεις για την υπόθεση Ramsey. Είπε ότι το Internet έχει παίξει πολύ σημαντικό ρόλο στην ανταλλαγή απόψεων και έχει επιτρέψει στον κόσμο να συζητά την υπόθεση και να κρίνει τη δικαιοσύνη.

Ένα από τα πολλά sites που δημιουργήθηκαν με θέμα την υπόθεση Ramsey είναι και το site Ramsey Case Internet Resources που έφτιαξε ο Frank De Freitas. Σ' αυτό υπάρχει μία εκτεταμένη λίστα φωτογραφιών, video και ηχογραφήσεων με την JonBenet.

Στα video clips περιέχονται μεταξύ άλλων και οι πρόβες της JonBenet για τα καλλιστεία, η συνέντευξη τύπου των γονιών της και συνεντεύξεις του Αρχηγού της Αστυνομίας Tom Kolby για την υπόθεση.

### **ΠΕΡΙΠΤΩΣΗ 33<sup>η</sup> (15/10/99)**

#### **Νέος ιός ελίσσεται στο Internet εξαπλώνοντας πορνό**

Ο νέος ιός έχει την ιδιότητα να δημιουργεί δεσμούς σε Web sites για ενήλικες και αφού τα εμφανίσει στην οθόνη του υπολογιστή, ψάχνει εξονυχιστικά τις διευθύνσεις e-mails και στέλνει τα ίδια πορνό sites σε φίλους, συγγενείς και συνεργάτες του χρήστη.

Το παραπάνω πρόγραμμα, γνωστό ως «σκουλήκι» λειτουργεί όπως ο ιός Melissa που προκάλεσε όλεθρο στους ηλεκτρονικούς υπολογιστές τον περασμένο Μάρτιο. Τίθεται δηλαδή σε λειτουργία όταν ανοιχτεί το μήνυμα με θέμα «Δείτε αυτό!». Ο υπολογιστής έχει μολυνθεί. Όλα τα μελλοντικά e-mail που θα σταλούν από τον μολυσμένο ηλεκτρονικό υπολογιστή

<sup>27</sup> Forum: Τόπος διακίνησης ιδεών στο Internet σε πραγματικό χρόνο.

<sup>28</sup> Domain name (όνομα domain): Το όνομα που δίνεται σε οποιονδήποτε υπολογιστή καταγράφεται σαν επίσημος φορέας παροχής πληροφοριών και αρχείων.

περιέχουν ένα μυστηριώδη προσάρτημα με θέμα «Καλή διασκέδαση».

### **Περισσότερα για τον ιό**

Ο ιός ονομάζεται VBS/Freelink και ενεργοποιείται μόνο αν ανοιχτεί. Δουλεύει μόνο με τα Windows '98 και Windows 2000, τα οποία υποστηρίζουν έναν ειδικό μηχανισμό προγραμματισμού. Όταν ενεργοποιηθεί, εμφανίζονται στην οθόνη sites για ενήλικες. Έπειτα γλιστρά στο Outlook και βρίσκει τις διευθύνσεις e-mail με σκοπό να αυτοδιανεμηθεί και σε άλλους ηλεκτρονικούς υπολογιστές. Δεν διαγράφει αρχεία, δεν μολύνει έγγραφα του Word, ούτε σβήνει το περιεχόμενο του σκληρού δίσκου, είναι όμως αρκετά ενοχλητικός κυρίως για αυτούς που θα πρέπει να δώσουν εξηγήσεις γιατί έστειλαν μηνύματα που περιέχουν πορνό. Επιπλέον ο ιός εγκαθιστά ένα αρχείο με το όνομα "Rundll.vbs" στο σύστημα έναρξης του ηλεκτρονικού υπολογιστή. Έτσι κάθε φορά που ανοίγουν τα Windows το πρόγραμμα εκτελείται από την αρχή εμφανίζοντας τα πορνό sites. Στέλνεται κάθε φορά που εκτελείται.

### **Μεγάλο κόστος**

Για πρώτη φορά εντοπίστηκε στην Ευρώπη το καλοκαίρι.

Ο Bruce Hughes, διευθυντής στις έρευνες Anti-Virus του εργαστηρίου ICISA (International Computer Association) συμβούλεψε τους χρήστες ηλεκτρονικών υπολογιστών να μην εκτελούν προγράμματα που δέχονται από άτομα που δεν εμπιστεύονται.

Προειδοποιήσεις για τον ιό στάλθηκαν προς τις υπηρεσίες παροχής υπηρεσιών Internet, τις εταιρείες έρευνας καταστολής ιών και τις επιχειρήσεις Ασφάλειας ηλεκτρονικών υπολογιστών.

Πρόσφατη έρευνα που διενήργησε η ICISA σχετικά με ιούς ηλεκτρονικών υπολογιστών έδειξε ότι το ποσοστό των μολύνσεων από ιούς συνεχίζει να αυξάνεται παρά τα μέτρα προστασίας που υπάρχουν όσον αφορά τα PCs, τους servers και τα modem (83% από τους ηλεκτρονικούς υπολογιστές που εξετάστηκαν, μολύνθηκαν παρά τα μέτρα προστασίας που διέθεταν).

Υπολογίζεται ότι το κόστος για την επαναφορά των υπολογιστών μιας επιχείρησης μετά από χτύπημα ενός παρόμοιου ιού, ανέρχεται στα \$1.750. Σε ορισμένες περιπτώσεις επιχειρήσεις ξόδεψαν μέχρι και \$100.000 για καταστροφές που προκάλεσε ένας μόνο ιός.

### **ΠΕΡΙΠΤΩΣΗ 34<sup>η</sup> (20/10/99)**

#### **Μαθητής κάνει φάρσα σε καθηγητή του**

Σε ένα site που χρησιμοποιείται από καθηγητές σ' όλη την Αμερική, περιέχονταν μία σημείωση που έμοιαζε να προέρχεται από έναν καθηγητή, όπου παραδεχόταν ότι παρενοχλούσε σεξουαλικά παιδιά και σκυλιά.

Τελικά αποδείχτηκε ότι ήταν μία φάρσα από ένα μαθητή του καθηγητή στο γυμνάσιο που διδάσκει, στην περιοχή East Greenwich.

Στον δεκαπεντάχρονο μαθητή αποδόθηκε στις 6 Οκτωβρίου η κατηγορία για ψευδείς πληροφορίες που αποτελεί πλημμέλημα. Αφέθηκε ελεύθερος υπό την επιμέλεια των γονιών του και θα παρουσιαστεί στον δικαστή ανηλίκων μέσα σε μία εβδομάδα

Το site που λέγεται "SchoolNotes.com", χρησιμοποιείται από 25.000 καθηγητές και περιέχει βιογραφικά και εργασίες, γι' αυτό πολλοί ανησυχούν για την ασφάλεια των πληροφοριών που περιέχει.

Ο Ricardo Valencia, εκπρόσωπος δημοσίων σχέσεων της εταιρείας Copernicus Interactive, ιδιοκτήτριας του site "SchoolNotes.com", εξέφρασε την απέχθειά της για την πράξη του αγοριού.

Πρότεινε ένα μέτρο με το οποίο οι καθηγητές θα πρέπει να εγγράφονται στο site προκειμένου να μπορέσουν να τοποθετήσουν πληροφορίες και να έχουν πρόσβαση σ' αυτό.

## ΠΕΡΙΠΤΩΣΗ 35<sup>η</sup> ( 22/10/99 )

### Μηνύονται Φαρμακευτικές Εταιρείες που λειτουργούν στο Internet

Μήνυση εναντίον φαρμακευτικών εταιρειών στο Internet έκανε η πολιτεία του Illinois με την αιτιολογία ότι δεν έχουν άδεια λειτουργίας από την πολιτεία αυτή και συνεπώς δεν μπορούν να πωλούν φάρμακα σε αυτή.

Η μήνυση έγινε στο δικαστήριο της περιφέρειας του Γενικού Εισαγγελέα Jim Ryan, ο οποίος και αποφάσισε τη διακοπή των πωλήσεων στην πολιτεία του Illinois. Ο Εισαγγελέας δήλωσε ότι τα φάρμακα πρέπει να διανέμονται μόνο έπειτα από συνταγή γιατρού και από φαρμακεία που έχουν σχετική άδεια. Πρόσθεσε ότι οι επιχειρήσεις στο Internet αγνοούν το νόμο και θέτουν σε κίνδυνο την υγεία των καταναλωτών.

Τη μήνυση υποστηρίζουν η Ένωση Αμερικανών Γιατρών (American Medical Association), δύο (2) γιατροί του δημοσίου και ομάδες φαρμακοποιών.

Κατηγορούμενοι είναι: η Υπηρεσίες ExpressMed Service Co. και Express Today Inc. στο Chandler Ariz, η εταιρεία M.D. Healthline στο Phoenix, η επιχείρηση DVM Enterprises Inc. στο Midlothian και η Male Clinic στο Los Angeles.

Ένας από τους κατηγορούμενους, ο Gary Hengfelt, ο ιδιοκτήτης της Φαρμακευτικής Εταιρείας Plaza United Pharmacy που πωλούσε φάρμακα μέσω της M.D. Healthline στο Internet, δήλωσε άγνοια για την ύπαρξη νόμου που απαγορεύει τις πωλήσεις στο Illinois.

Ο Εισαγγελέας Ryan είπε ότι σερφάροντας στο Internet θέλησε να διαπιστώσει αν οι συνταγές των φαρμάκων δίνονταν μετά τη γνωστοποίηση του ιστορικού υγείας των πελατών. Σε μία περίπτωση ανακάλυψε ότι μία έγκυος γυναικά κατάφερε έναν πωλητή να της προμηθεύσει Viagra από το εξωτερικό.

Η Nancy Coles, εκπρόσωπος της Ένωσης Προστασίας των Δικαιωμάτων των Καταναλωτών, δήλωσε ότι η απαγόρευση των

πωλήσεων των εταιρειών αυτών θα μπορούσε να πλήξει τα δικαιώματα των καταναλωτών. Παρόλα αυτά είπε ότι έχουν ακουστεί παράπονα και προβλήματα που προέρχονται από αγοραστές φαρμάκων στο Internet.

### ΠΕΡΙΠΤΩΣΗ 36<sup>η</sup> ( 25/10/99 )

#### Ανάπηρος κατηγορείται για τρομοκρατία μέσω του διαδικτύου

Ένας 19χρονος παράλυτος από την πολιτεία του Missouri κατηγορείται ότι απειλούσε να σκοτώσει δεκάδες μαθητές, καθηγητές και να ανατινάξει ένα γυμνάσιο σε μία κοινότητα κοντά στα σύνορα με το New Hampshire.

Ο 19χρονος ονομάζεται Christian Hunold ομολόγησε ότι τρομοκρατούσε τα παιδιά και τους καθηγητές του Γυμνασίου Hawthorne Brook. Τις απειλές του τις έστειλε μέσω ενός chat room του σχολείου στο Internet.

Η αστυνομία του Missouri εισέβαλε στο σπίτι του, τον συνέλαβε και κατάσχεσε τον εξοπλισμό του ηλεκτρονικού υπολογιστή του καθώς και άλλα αποδεικτικά στοιχεία. Το Web site του σχολείου έκλεισε αφού ο 19χρονος Christian είχε τοποθετήσει εκεί οδηγούς για πορνογραφικά sites.

Ο Christian κατηγορείται για διάδοση βλαβερού υλικού σε ανηλίκους, έκθεση παιδιών και κατοχή παιδικής πορνογραφίας, έκθεση και διαφθορά του σχολείου. Ημερομηνία της δίκης ορίστηκε η 3<sup>η</sup> Νοεμβρίου και η δίκη θα γίνει στο Δικαστήριο Ayer District Court.

Τα γεγονότα που οδήγησαν στις απειλές θανάτου ξεκίνησαν πριν από ένα μήνα σε ένα chat room της America Online όπου η 8<sup>η</sup> τάξη του Γυμνασίου Hawthorne Brook συγκεντρώνονταν για να συζητήσουν τις δραστηριότητες του σχολείου και άλλα θέματα. Ο ύποπτος παρακολουθούσε τις συνομιλίες και συγκέντρωνε πληροφορίες για το σχολείο και κάποιους από τους μαθητές.

Αρχικά ο Christian προέτρεπε κάποιους μαθητές να μπουν σε sites που παρουσίαζαν παιδική πορνογραφία. Αργότερα άρχισε τις απειλές και οι συζητήσεις άρχισαν να γίνονται βίαιες. Λεπτομέρειες και η φύση των διαδικτυακών συζητήσεων έκαναν τους μαθητές να πιστεύουν ότι ο άντρας ζούσε κοντά τους. Το σχολείο ειδοποίησε τους γονείς των 650 μαθητών του σχολείου και συγκάλυψε συνέλευση γονέων και καθηγητών με σκοπό να τους καθησυχάσει, ενώ προηγουμένως έγινε έρευνα στο σχολείο και τις τσάντες των μαθητών για βόμβες.

Στις 20 Οκτωβρίου, ξεκίνησαν νέες απειλές με στόχο το Διευθυντή του σχολείου, 3 καθηγητές και 20 μαθητές. Το Web site του σχολείου παραβιάστηκε και τοποθετήθηκε εκεί μία φωτογραφία του διευθυντή που τον έδειχνε με τρύπες από σφαίρες στο κεφάλι και στο στήθος. Μετά από αυτό το γεγονός προγραμματίστηκε νέα σύσκεψη γονέων με στόχο να εξετάσουν την υπόθεση και να ενημερώσουν τους γονείς σχετικά με το τι πρέπει να γνωρίζουν όσον αφορά τη χρήση του Internet από τα παιδιά τους. Δύο μέρες αργότερα ο ύποπτος ανακαλύφθηκε και συνελήφθη.

Σύμφωνα με τον Tom Reilly, Γενικό Εισαγγελέα στην πολιτεία της Massachusetts: «Κανείς στο σχολείο δεν βρέθηκε σε κίνδυνο ή ρίσκο για φυσική βλάβη. Αυτό όμως δε μειώνει τις πράξεις αυτού του ατόμου. Ήταν πράξεις τρομοκρατικές μέσω του δικτύου και όπλο ήταν το Internet με στόχο να δημιουργήσει ένα αίσθημα πανικού στο σχολείο και στην κοινότητα».

### **ΠΕΡΙΠΤΩΣΗ 37<sup>η</sup> ( 26/10/99 )**

#### **Καταπολέμηση της παιδικής πορνογραφίας**

Με σκοπό την καταπολέμηση της παιδικής πορνογραφίας, βρέθηκαν στο Texas, ο Γενικός Εισαγγελέας της πολιτείας του Texas και εκπρόσωποι των υπηρεσιών παροχής Internet. Μια ασυνήθιστη συνεργασία μεταξύ δημόσιου και ιδιωτικού τομέα θα υπάρχει από εδώ και στο εξής αφού οι εκπρόσωποι των υπηρεσιών του Internet συμφώνησαν να προμηθεύουν με σχετικές αναφορές από τα sites τους περιστατικά παιδικής πορνογραφίας, τον Γενικό Εισαγγελέα, John Cornyn.



Με αυτή τη συμφωνία οι παιδικοί πορνογράφοι θα δυσκολευτούν να βρουν ασφαλή χώρο στο διαδίκτυο για την έκθεση του υλικού τους και οι υπηρεσίες του Internet δε θα έχουν το φόβο να κατηγορηθούν για συνενοχή στην κατοχή του απαγορευμένου υλικού ενημερώνοντας τις αρχές.

«Έχουμε ένα κοινό στόχο: να βγάλουμε την παιδική πορνογραφία από το Internet. Αυτές οι κατευθυντήριες γραμμές εξυπηρετούν τα συμφέροντα της πολιτείας γιατί θα βγάλουν αυτούς τους εγκληματίες από το Internet. Και τα συμφέροντα των εταιρειών του Internet αφού θα κερδίσουν την εμπιστοσύνη του καταναλωτή. Πρόκειται για μια ισόπαλη συμφωνία και ελπίζω να ακολουθήσουν και άλλες εταιρείες.»

Σύμφωνα με τους όρους αυτής της συμφωνίας όταν ένας χρήστης καταγγείλει ότι συνάντησε παιδική πορνογραφία σε κάποιο site, η υπηρεσία του Internet θα πρέπει να εξακριβώσει αν πραγματικά στο συγκεκριμένο site υπάρχει τέτοιου είδους υλικό και να μεταφέρει την πληροφορία στον Γενικό Εισαγγελέα. Ο Γενικός Εισαγγελέας θα εξετάσει την καταγγελία και μέσα σε δύο εβδομάδες θα πρέπει να ενημερώσει τους ενδιαφερόμενους αν υπάρχει υπόθεση που να στηρίζεται στις καταγγελίες.

Η εκπρόσωπος του γραφείου του Γενικού Εισαγγελέα, είπε ότι αυτή η συμφωνία θα μπορούσε να αποτελέσει εθνικό μοντέλο για άλλες συμφωνίες.

Μία από τις υπηρεσίες παροχής υπηρεσιών του Internet που έλαβε μέρος στη συμφωνία είναι η America On Line (AOL), ο μεγαλύτερος προμηθευτής του Internet για τις ΗΠΑ. Ο Don Colcolough, Γενικός Διευθυντής του Δικτύου Ασφαλείας και Παρακολούθησης της AOL, είπε ότι η εταιρεία δεν έχει καμία ανοχή απέναντι στην παράνομη συμπεριφορά: «Η προστασία και ασφάλεια των μελών είναι η πρώτη προτεραιότητα της America Online. Συνεργαζόμαστε στενά με υπηρεσίες εκτέλεσης του νόμου έτσι ώστε να εξασφαλίζουμε στα μέλη ασφάλεια. Τα μέλη μας ενδιαφέρονται και για την ανάγκη καταπολέμησης της παιδικής πορνογραφίας στο Internet και για την ανάγκη προστασίας του ιδιωτικού απορρήτου. Αισθανόμαστε ότι οι κατευθυντήριες γραμμές της συμφωνίας σκιαγραφούν μία διαδικασία η οποία επισπεύδει την εκτέλεση του νόμου και διαβεβαιώνουν ότι τα προσωπικά στοιχεία των πελατών μας θα

κρατηθούν μυστικά έως το βαθμό που ορίζει ο νόμος. Έτσι ενθαρρύνουμε όλες τις υπηρεσίες παροχής υπηρεσιών να υιοθετήσουν την ίδια διαδικασία αντιμετώπισης του προβλήματος».

Ο Ed Cavazos, Αντιπρόεδρος Νομικών και Επαγγελματικών Υποθέσεων, στο Internet, είπε: «Το Internet δε θα πρέπει να αποτελεί ένα ασφαλές καταφύγιο για τους παιδικούς πορνογράφους. Η συνεργασία με τις αρχές θα εξασφαλίσει να μη συμβεί αυτό».

### **ΠΕΡΙΠΤΩΣΗ 38<sup>η</sup> ( 01/11/99 )**

#### **Hackers επιτίθενται στο Web site του Associated Press**

Μία ομάδα από hackers η οποία χρησιμοποιεί το όνομα “United Loan Gummen” (ULG) είναι υπεύθυνη για τις παραμορφώσεις των Web sites νέων οργανισμών. Η ομάδα αυτή, η ULG, χτύπησε και το Web site του οργανισμού «Associated Press» του μεγαλύτερου παγκοσμίως οργανισμού συγκέντρωσης ειδήσεων. Κατάφερε να παραμορφώσει το site του οργανισμού τοποθετώντας σ’ αυτό ένα ποίημα του Edgar Allan Poe, το «Στοιχειωμένο Παλάτι», το οποίο κατέβαλε όλη την ιστοσελίδα, καθώς και μία ευχή για τη γιορτή του Halloween.

Κρυμμένη στην πηγή του κωδικού της ιστοσελίδας, βρισκόταν μία δήλωση της ομάδας ULG με την οποία αναλάμβανε την ευθύνη της επίθεσης στο site και έλεγε ότι σκοπός της ήταν να βγει στις ειδήσεις. Συγκεκριμένα έλεγε τα εξής: «Θα μπει η ULG στις ειδήσεις γι’ αυτό; Εμείς φτιάχνουμε τις ειδήσεις».

Ο Ruth Gerch, εκδότης της AP Multimedia Services, είπε ότι παρόλο που η επίθεση των hackers ήταν σοβαρή, το περιεχόμενο των ειδήσεων δεν επηρεάστηκε.

#### **Διαμαρτυρία για έναν φυλακισμένο hacker**

Πίσω από την παραμορφωμένη ιστοσελίδα του «Associated Press» υπήρχε επίσης και μία αναφορά στην HFG (Hacking for Girlies), μία άλλη ομάδα από hackers. Η ομάδα αυτή (HFG)

ισχυριζόταν ότι ήταν υπεύθυνη για το κλείσιμο και ξεχαρβάλωμα της ιστοσελίδας της εφημερίδας «The New York Times», τον Σεπτέμβριο του 1998. Τότε η ομάδα αυτή είχε τοποθετήσει στο site κάποιες άσεμνες φωτογραφίες θέλοντας να διαμαρτυρηθεί για ένα άρθρο της εφημερίδας σχετικά με τον super – hacker των ηλεκτρονικών υπολογιστών, του Kevin Mitnick.

Η ULG λανσάρισε μια διατριβή για τον δημοσιογράφο των “New York Times”, τον John Markoff ο οποίος ασχολείται με τεχνολογικά θέματα. Έγραψε επίσης το βιβλίο «Takedown» που εξιστορεί την καταδίωξη και τη σύλληψη του Mitnick. Απόσπασμα των όσων έγραψε η ULG είναι: «Η αδικία που έχει διαπράξει ο Markoff είναι εγκληματική. Αυτός θα έπρεπε να σαπίζει στη φυλακή, αντί για τον Kevin Mitnick. Ο Kevin δεν είναι hacker της σκοτεινής πλευράς. Δεν είναι μοχθηρός. Δεν είναι δαίμονας. Δεν καταχράστηκε πιστωτικές κάρτες, δεν μετέδωσε το software που βρήκε, ή δεν αρνήθηκε τη συντήρηση μιας μηχανής. Είναι τόσο δύσκολο να το καταλάβετε;».

Άλλο απόσπασμα από τις δηλώσεις των hackers αναφέρει: «Επειδή τα γράφουμε όλα κεφαλαία και χρησιμοποιούμε «elite» γλώσσα δεν σημαίνει ότι είμαστε παιδιά. Για όποιον μας φωνάζει ανώριμα παιδιά., δείχνει ότι ακόμα ένας άνθρωπος μας έχει υποτιμήσει. Και χειρότερα, τι σημαίνει αυτό για την ασφάλειά τους; Ότι τα «ανώριμα παιδιά» ήταν ικανά να ξεπεράσουν τα αξίας \$25.000 firewalls, να ξεπεράσουν την ασφάλεια που υπάρχει εκεί με xx χρόνια εμπειρίας ή xxx πτυχίο από κάποιο κολέγιο. Αηδία».

Εκτός από τη χρησιμοποίηση κεφαλαίων γραμμάτων, οι hackers αναφέρουν συχνά φράσεις από λογοτεχνικά κομμάτια, όπως του Βολταίρου.

### **Αξιολόγηση της επίθεσης**

Ο Eric Meyer, καθηγητής δημοσιογραφίας στο Πανεπιστήμιο του Illinois, είπε ότι η επίθεση στο Web site του οργανισμού των ειδήσεων είχε σκοπό τη δημοτικότητα των hackers και τόνισε ότι οι επιθέσεις αυτές θα αυξάνονται όσο περισσότερη προσοχή συγκεντρώνεται σε αυτούς.

Ο Meyer, σύμβουλος σε θέματα του Internet στη βιομηχανία εφημερίδων, παρομοίασε τις επιθέσεις αυτές με τις απειλές για τοποθέτηση βόμβας που ήταν σε έξαρση στο τέλος της δεκαετίας του '90.

### ΠΕΡΙΠΤΩΣΗ 39<sup>η</sup> (08/11/99)

#### Ρατσιστικά Ηλεκτρονικά Μηνύματα

68 ρατσιστικά ως προς τις μειονότητες μηνύματα e-mail δέχτηκαν οι ηλεκτρονικοί υπολογιστές του Πανεπιστημίου της Pennsylvania. Πιθανολογείται ότι τα μηνύματα στάλθηκαν από το εργαστήριο ηλεκτρονικών υπολογιστών του Πανεπιστημίου Temple. Τα μηνύματα τα οποία υπογράφονταν με το όνομα «Πατριώτης» στάλθηκαν μεταξύ 18:30μ.μ. και 19:15μ.μ. στις 2 Νοεμβρίου – ημέρα εκλογών.

Σύμφωνα με τις αρχές τα μηνύματα ήταν διαφορετικά αλλά όλα είχαν το ίδιο ρατσιστικό θέμα. Μερικά από αυτά: «Ο χρόνος σας είναι περιορισμένος», «Σας παρακολουθούμε», «Συνειδητοποιήστε το, τα χρόνια σας λιγοστεύουν και οι ημέρες σας είναι μετρημένες», «Να ζήσει η Αμερική».

#### **Η τεχνολογία, σύμμαχος του αποστολέα**

Δεν μπορεί να ειπωθεί με ακρίβεια από που στάλθηκαν τα ρατσιστικά ηλεκτρονικά μηνύματα. Δεν μπορεί να καθορισθεί αν κάποιος μπήκε στο εργαστήριο του Temple για να γράψει και να στείλει τα αποκρουστικά μηνύματα ή αν κάποιος παραβίασε το σύστημα των ηλεκτρονικών υπολογιστών του Πανεπιστημίου και προώθησε τα μηνύματα μέσω αυτού.

«Η τεχνολογία του Internet εξασφαλίζει ευκολία στην πρόσβαση που επιτρέπει στους χρήστες να στέλνουν μηνύματα ανώνυμα. Αυτή τη στιγμή, δεν μπορούμε να είμαστε σίγουροι ότι τα μηνύματα στην πραγματικότητα προέρχονται από ηλεκτρονικούς υπολογιστές του Temple» είπε η εκπρόσωπος του πανεπιστημίου Temple, η Harriet K. Goodheart.

Ο Bill Mahon, εκπρόσωπος της πολιτείας, είπε ότι μερικά από τα ρατσιστικά μηνύματα είχαν σταλεί από προσωπικές

ηλεκτρονικές διευθύνσεις, οι οποίες φαίνεται ότι ανήκουν σε Ισπανούς και Αφροαμερικανούς.

Ο Επιθεωρητής της αστυνομίας της Pennsylvania, Tom Sowerby, είπε ότι γύρω στις 09:00 π.μ. την περασμένη Τρίτη ένας μαθητής ο οποίος έλαβε ένα από τα μηνύματα κάλεσε την αστυνομία. Δήλωσε ακόμη ότι υπάρχει πολύς δρόμος για να βρουν τους ένοχους.

Εργαζόμενοι του πανεπιστημίου ζήτησαν από το FBI να συμμετέχει στην έρευνα. Επίσης ενημερώθηκε και ο τοπικός εισαγγελέας.

Αν κάποιος δεν έστειλε τα e-mails από το εργαστήριο ηλεκτρονικών υπολογιστών του Temple τότε θα χρειαστεί αρκετός χρόνος για τον εντοπισμό του.

Σε περίπτωση που βρεθεί, ο αποστολέας των e-mails, θα αντιμετωπίσει κατηγορίες για παρενόχληση, εγκλήματα μίσους και εθνικό εκφοβισμό.

### **Απειλές θανάτου**

Αυτή είναι τουλάχιστον η δεύτερη φορά που ένας μαθητής του πανεπιστημίου της Pennsylvania λαβαίνει ρατσιστικό ηλεκτρονικό μήνυμα από κάποιον που ισχυρίζεται ότι είναι «ο Πατριώτης».

Τον περασμένο Μάρτιο, κάποιος έστειλε ένα ρατσιστικό μήνυμα στην Laura Hennessey, αρθρογράφος της εφημερίδας «The Daily Collegion» που ανήκει στο πανεπιστήμιο.

Τον Ιούνιο, το πανεπιστήμιο Stanford ερεύνησε την πηγή ενός ρατσιστικού ηλεκτρονικού μηνύματος το οποίο στάλθηκε σε 25.000 φοιτητές, χρήστες ηλεκτρονικών υπολογιστών. Μία από τις παραγράφους του μηνύματος κατηγορούσε το πανεπιστήμιο ότι δείχνει προτίμηση στη στέγαση των μη λευκών φοιτητών.

Τον Ιανουάριο, ο Kingman Quon, ένας Αμερικάνος Κινέζικης καταγωγής, 22 ετών, από το Los Angeles, δήλωσε ένοχος για την αποστολή μηνυμάτων ρατσιστικού περιεχομένου

σε περισσότερους από 70 ανθρώπους ισπανικής καταγωγής, ανάμεσά τους και καθηγητές πανεπιστημίου.

Τα περισσότερα από αυτά τα μηνύματα σχετίζονται με τα πανεπιστήμια και το φαινόμενο εκτείνεται από την πολιτεία California ως την πολιτεία της Massachusetts. Τα μηνύματα λένε πράγματα όπως: «Μισώ τη φυλή σας» και «Θέλω όλους σας να πεθάνετε».

Παρόμοια μηνύματα είχαν σταλεί στις 7 Μαρτίου 1998 σε 42 Λατίνους καθηγητές του Ινστιτούτου Τεχνολογίας της Massachusetts, καθώς και στην εταιρεία Xerox, στην Ισπανική εφημερίδα της πολιτείας του Texas, στο πανεπιστήμιο της Indiana, στην Υπηρεσία Internal Revenue Service και στο ερευνητικό κέντρο της NASA.

Παρά την ανησυχία των αρχών για τις ρατσιστικές εκδηλώσεις στο Internet, οι συλλήψεις των δραστών είναι ελάχιστες. Εκτός από την σύλληψη του Quon ο οποίος ομολόγησε, ο ένοχος βρέθηκε και για το περιστατικό στο Los Angeles.

Ο ένοχος βρίσκεται στην φυλακή και θα εκτίσει ποινή 12 μηνών γιατί έστειλε απειλές θανάτου σε μαθητές του πανεπιστημίου της California, Los Angeles.

### ΠΕΡΙΠΤΩΣΗ 40<sup>η</sup> ( 09/11/99 )

#### Δικτυακός πόλεμος στην Γιουγκοσλαβία

Η εφημερίδα Washington Post δημοσίευσε άρθρο στο οποίο αναφέρεται ότι το Πεντάγωνο έχει την πρόθεση να παραβιάσει τα Σερβικά δίκτυα υπολογιστών για να συντρίψει τις στρατιωτικές επιχειρήσεις των Σέρβων καθώς και τις δημόσιες υπηρεσίες της χώρας. Εξαιτίας όμως της αβεβαιότητας αναφορικά με τις νομικές ισχύουσες διατάξεις, αποφασίστηκε ή μη παραβίαση των Σερβικών δικτύων.

Ο Henry H. Shelton, Πρόεδρος των Ηνωμένων Πολιτειών, χρησιμοποίησε μία μορφή ηλεκτρονικού πολέμου κατά τη διάρκεια του εναέριου πολέμου του NATO εναντίον της

Γιουγκοσλαβίας την προηγούμενη άνοιξη. Ο Shelton είπε ότι κατά τη διάρκεια της εκστρατείας στο Κόσοβο, απασχολήθηκαν κάποια συστήματα ηλεκτρονικών υπολογιστών, με αποτελέσματα επιβλαβή στο φυσικό περιβάλλον, αλλά πρόσθεσε ότι δεν μπορούσε να γίνει πιο συγκεκριμένος.

Οι νόμοι που ισχύουν σε εμπόλεμες παραδοσιακές καταστάσεις δεν είναι αρκετοί και ιδιαίτερα χρήσιμοι όσον αφορά των διαδικτυακό πόλεμο. Τι γίνεται με τις «λογικές βόμβες», όπως χαρακτηρίζονται οι ιοί, όταν χρησιμοποιούνται για να καταστρέψουν πληροφοριακά συστήματα της αντίπαλης χώρας σε περιόδους πολέμου; Αναφορά του Πενταγώνου υποστηρίζει ότι αφορά ανταλλαγές μετοχών, τραπεζικά συστήματα, πανεπιστήμια και παρόμοια συστήματα ηλεκτρονικών υπολογιστών δεν πρέπει να δέχονται επιθέσεις απλά επειδή μία από τις εμπόλεμες χώρες έχει την ικανότητα να το κάνει. «Μία επίθεση στο δίκτυο ηλεκτρονικών υπολογιστών είναι σαν να ανατινάξεις μία κατοικημένη περιοχή ή να εξωθείς ραδιενέργεια», λει σημείο της αναφοράς.

Σε ένα άλλο σημείο αναφέρεται «Είναι δυνατό να χρησιμοποιήσεις τεχνικές «μορφολογίας» του ηλεκτρονικού υπολογιστή για να τσαλακώσεις μία εικόνα π.χ. του Αρχηγού της πολιτείας του εχθρού, ενημερώνοντας τους στρατιώτες του για μια ψεύτικη ανακωχή ή για μία ανύπαρκτη υπογραφή μίας συμφωνίας παύσης των πυρών! Αν είναι λάθος κάτι τέτοιο, τότε αν γίνεται, πρέπει να θεωρείται έγκλημα πολέμου».

### ΠΕΡΙΠΤΩΣΗ 41<sup>η</sup> ( 12/11/99 )

#### Νέα Απειλή:

Ελεύθερα κυκλοφορεί στο Internet ένας νέος ιός ηλεκτρονικών υπολογιστών που ενεργοποιείται με το άνοιγμα του προγράμματος e-mail. Πριν από δύο μέρες ο ιός εντοπίστηκε από κάποιους ειδικούς σε προβλήματα ιών των ηλεκτρονικών υπολογιστών, οι οποίοι ενημέρωσαν τον κόσμο για την ύπαρξη του ιού και τον έθεσαν σε επιφυλακή. Τώρα ο ιός έχει τοποθετηθεί σε ένα Γιαπωνέζικο site στο Internet και είναι διαθέσιμο σε οποιονδήποτε κατεβάσει (download) το site.

Ο ιός έχει το όνομα Bubbleboy και είναι γνωστός ως «σκουλήκι». Δεν θεωρείται ιδιαίτερα επικίνδυνος από τους ειδικούς αφού το μόνο που κάνει είναι να αλλάζει τις πληροφορίες εγγραφής του ιδιοκτήτη του ηλεκτρονικού υπολογιστή. Ο ιδιοκτήτης καταχωρείται με το όνομα Bubbleboy και αν πρόκειται για εταιρεία μετονομάζεται σε Vandalay Inc. – ονόματα δανεισμένα από επεισόδια μιας αμερικάνικης τηλεοπτικής σειράς, της «Seinfeld». Ο ιός μεταδίδεται από μόνος του στέλνοντας καινούρια e-mail σε όποια διεύθυνση υπάρχει στο πρόγραμμα Microsoft Outlook Express του ηλεκτρονικού υπολογιστή.

Άλλοι ιοί που μεταδίδονται με παρόμοιο τρόπο μέσω e-mail και εμφανίζονται σαν μηνύματα ενεργοποιούνται όταν ο παραλήπτης ανοίξει το μήνυμα. Ο Bubbleboy διαφοροποιείται ως προς την ενεργοποίησή του. Ο χρήστης χρειάζεται μόνο να ανοίξει το πρόγραμμα e-mail για να ελευθερωθεί ο ιός το βλαβερό πρόγραμμά του.

Ο ίδιος ο ιός Bubbleboy, δεν είναι ιδιαίτερα ενοχλητικός, δίνει όμως την ευκαιρία σε οποιονδήποτε με πιο κακοήθη στόχους από τον δημιουργό του να απενεργοποιήσει τον κωδικό μιας εταιρείας και να μεταφέρει σ' αυτή πιο καταστρεπτικά προγράμματα.

Λέγεται ότι το site όπου έχει τοποθετηθεί ο ιός, μαζί με έναν αριθμό από άλλους ιούς, έχει δημιουργηθεί στην Argentina από κάποιον ονομαζόμενο «Zulu».

### **Τρύπα στην ασφάλεια του Outlook Express της Microsoft**

Ο Richard Jacobs, πρόεδρος των Αμερικανικών επιχειρήσεων Sophos Inc.<sup>29</sup>, είπε ότι ο δημιουργός του ιού εκμεταλλεύτηκε μία τρύπα στην ασφάλεια του προγράμματος Outlook Express της Microsoft, στα Windows 98 και 2000. Είπε ότι η εταιρεία Microsoft έχει επιδιορθώσει το software για να εμποδίσει τον ιό. Ο ιός δεν επηρεάζει τα Windows NT.

Δεν υπήρχαν άλλοι ιοί σε μορφή μηνυμάτων που να ενεργοποιούνται παρά μόνο όταν ο χρήστης του ηλεκτρονικού

<sup>29</sup> Εταιρεία που ασχολείται με την αντιμετώπιση ιών.



υπολογιστή διάβαζε τα μηνύματά του. Όμως ο Bubbleboy διαδόθηκε στα συστήματα Unix χωρίς να απαιτεί από τους χρήστες να διαβάσουν την αλληλογραφία τους. Αυτή η ιδιαιτερότητα του ιού Bubbleboy τον διαφοροποιεί από άλλους παρόμοιους ιούς.

Ο Doug Muth, ειδικός ασφαλείας ηλεκτρονικών υπολογιστών, είπε ότι ο ιός έχει σχεδιαστεί έτσι ώστε να ενεργοποιείται μόνο μέσω δύο προγραμμάτων e-mail της Microsoft. Πρόσθεσε ότι δεν επηρεάζει κανένα άλλο πρόγραμμα e-mail όπως το Eudora ή το Pegasus.

Σύμφωνα πάλι με τον Muth, αυτό που το κάνει πραγματικά διαφορετικό είναι ότι η γλώσσα στην οποία είναι γραμμένο, η «Visual Basic Script», το θέτει αυτόματα σε εφαρμογή από το πρόγραμμα Microsoft Outlook. Αφού ο χρήστης ανοίξει το μήνυμα e-mail, ο ιός αντιγράφει ένα πρόγραμμα από την «έναρξη» του ηλεκτρονικού υπολογιστή έτσι ώστε την επόμενη φορά που θα ανοίξει ο ηλεκτρονικός υπολογιστής, ο ιός θα σταλεί από μόνος του σε ένα «ξέσπασμα» από e-mail σε κάθε ηλεκτρονικό υπολογιστή που η διεύθυνσή του συμπεριλαμβάνεται στο πρόγραμμα με τις διευθύνσεις.

Το μήνυμα e-mail εμφανίζει στη διεύθυνση του αποστολέα κάποια γνωστή ως προς τον παραλήπτη διεύθυνση. Στη γραμμή του θέματος εμφανίζεται η φράση: «Ο Bubbleboy είναι πίσω.», ενώ το κείμενο του μηνύματος λει: «Το περιστατικό του Bubbleboy, φωτογραφίες και ήχοι <http://www.towns.com/dorms/tom/bblboy.htm> ».

Η διεύθυνση αυτή δεν λειτουργεί.

### **Φασαρία για το τίποτα;**

Ο Space Rogue, εκδότης της εφημερίδας «Hacker News Network», αναρωτιέται γιατί είναι η πρώτη φορά που αυτό το είδος του ιού έχει γίνει είδηση, αφού η θεωρία πίσω από αυτό υπάρχει εδώ και ένα χρόνο περίπου.

Υποστηρίζει ότι το μόνο ενδιαφέρον σχετικά με τον Bubbleboy, εκτός από ένα χαριτωμένο όνομα, είναι ο τρόπος που μεταδίδεται, το ότι μπορεί να μεταδοθεί μόνο με το να το λάβει

κάποιος. Πέρα από αυτό, ο Bubbleboy δεν είναι καταστροφικός και δεν κάνει τίποτα άλλο από το να μεταδίδεται.

Συμπερασματικά είπε: «Ακόμα δεν μπορώ να καταλάβω γιατί γίνεται όλη αυτή η φασαρία».

Άλλος πάλι, όπως ο Mikko Hyrponen, διευθυντής των Ερευνών Αντιβιοτικών στην εταιρεία Data Fellows Corp., πιστεύουν ότι η μοναδικότητα του ιού είναι ο τρόπος που διανέμεται. Πρόσθεσε ότι στο μέλλον θα πρέπει να αναμένουμε πολλούς νέους ιούς «σε έξαρση» να χρησιμοποιούν αυτή τη τεχνική μετάδοσης.

### **ΠΕΡΙΠΤΩΣΗ 42η (15-11-1999)**

#### **Υπόθεση μηχανογραφίας στο Internet**

Για πρώτη φορά μία νομική εταιρεία κατηγορείται για παραβίαση ηλεκτρονικών συστημάτων. Μία υπόθεση ασυνήθιστη ακόμα και για τα δεδομένα του Internet. Η ιδιωτική εταιρεία Dig Dirt Inc<sup>30</sup> έκανε μήνυση εναντίον της μεγάλης νομικής εταιρείας Steptoe & Johnson LLP<sup>31</sup>, με την κατηγορία ότι η τελευταία προσπάθησε να παραβιάσει τους ηλεκτρονικούς υπολογιστές της τουλάχιστον 750 φορές.

Η εταιρεία Moore Publishing Inc., η οποία διαχειρίζεται την υπηρεσία πληροφοριών Dig Dirt Inc., υποστηρίζει ότι 4 υπάλληλοι από της νομικής εταιρείας προσπάθησαν να παραβιάσουν τους υπολογιστές και το Web site της εταιρείας Dig Dirt Inc. Που παρέχεται από την CIBIR Corporation και ζητά αποζημίωση ύψους \$10εκ.

Στο Περιφερειακό Δικαστήριο της πολιτείας Columbia (Η.Π.Α.), η εκπρόσωπος της εταιρείας Moore Publishing κατέθεσε ότι η εταιρεία Steptoe & Johnson παραβίαζε συνεχώς κάποια συγκεκριμένα domain names και Internet sites. Ισχυρίστηκε ακόμη ότι ένας υπάλληλος της εταιρείας αυτής,

<sup>30</sup> Ασχολείται με εξεταστική και ερευνητική εργασία για νομικές εταιρείες, επιχειρήσεις και κρατικές υπηρεσίες.

<sup>31</sup> Steptoe & Johnson: Μεγάλη νομική εταιρεία, με γραφεία στην Washington, στο Phoenix, στο Los Angeles και στη Μόσχα, με πάνω από 290 δικηγόρους.

έκλεψε έναν κωδικό του Internet από κάποιο παλιό πελάτη με το όνομα Lois Gloor.

Η ακρόαση έχει προγραμματιστεί για τις 23 Νοεμβρίου. Δικαστής στην υπόθεση θα είναι ο Thomas Penfield, ο οποίος θα εκδικάσει και την υπόθεση anti-trust της Microsoft.

Οι υπάλληλοι της Steptoe & Johnson οι οποίοι κατηγορούνται είναι οι James Cramer, Thomas Felts, Myra Burch και Jane Doe, ενώ η μήνυση δε βαρύνει και τη διοίκηση της εταιρείας η οποία δηλώνει άγνοια και αρνείται τις κατηγορίες.

Ένα μήνα νωρίτερα, τον Οκτώβριο, η βουλή ενέκρινε ένα νόμο για το cybersquatting: Όποιος με κακή πίστη καταχωρεί «domain names» παρόμοιο ή ίδιο με κάποιο που ήδη υπάρχει, αντιμετωπίζει πρόστιμο \$100.000.

### **ΠΕΡΙΠΤΩΣΗ 43<sup>η</sup> ( 16/11/99 )**

#### **Τα \$11 δισ. το χρόνο αγγίζει η πειρατεία σε software**

Η εταιρεία Business Software Alliance (BSA) έκανε μήνυση για παραβίαση των πνευματικών της δικαιωμάτων εναντίον 25 ατόμων σε 6 πολιτείες της Αμερικής και του Καναδά. Η μήνυση κατατέθηκε στο US District Court στην πολιτεία California. Μήνυση για παραβίαση των πνευματικών τους δικαιωμάτων έχουν κάνει επίσης και πολλές άλλες εταιρείες software όπως οι εταιρείες Adobe Systems Inc., η Corel Corporation, η Microsoft Macromedia και η Symantec. «Πειρατικό» software των εταιρειών αυτών καθώς και προγράμματα όπως τα: Adobe Acrobat, Dreamweaver, Adobe Photoshop, Freehand, Microsoft Office 2000 και Norton Antivirus, διακινούνται παράνομα στο κανάλι επικοινωνίας του Internet warez4-cable.

Με την κατάθεση της μήνυσης στις 2 Νοεμβρίου άρχισαν να γίνονται απροειδοποίητες έρευνες στον εξοπλισμό των ηλεκτρονικών υπολογιστών σε σπίτια στις περιοχές Sacramento, Downey, California, Troy, West Bloomfield και Michigan.

Κατασχέθηκαν 5 ηλεκτρονικοί υπολογιστές και μεγάλος αριθμός CD-ROMS.

Η βιομηχανία των software εκτιμά ότι οι οικονομικές απώλειες από τη διεθνή πειρατεία ανέρχονται στα \$11 δισεκατομμύρια περίπου το χρόνο, από τα οποία τα \$2,8 δισεκατομμύρια αναλογούν στις Ηνωμένες Πολιτείες.

Ο Robert Kruger, αντιπρόεδρος της νομικής υπηρεσίας BSA, είπε ότι η διανομή πειρατικού software μέσω των chat rooms είναι ιδιαίτερα διαδεδομένη, εξαιτίας της αυξανόμενης πρόσβασης στις high-speed συνδέσεις, η διακίνηση παράνομου software στο Internet γίνεται γρήγορα και γι' αυτό είναι δημοφιλής.

Η BSA, χρησιμοποιώντας μία ειδική διαδικασία κλήσης που δημιουργήθηκε το 1998 από την εταιρεία Digital Millenium Copyright Act., κατάφερε να αναγνωρίσει κάποια από τα άτομα που διακινούσαν παράνομο software και να λάβει νομικά μέτρα.

Σύμφωνα με τον John Wolfe, διευθυντή της ομάδας των ερευνών, παλιότερα οι χρήστες έπρεπε να κατεβάσουν διάφορα κομμάτια από ένα πρόγραμμα και να το συναρμολογήσουν οι ίδιοι αργότερα, τώρα όμως, μπορούν να κατεβάσουν ολόκληρο το πρόγραμμα άθικτο. Το κανάλι του Internet όπου γίνεται η διακίνηση του πειρατικού software δεν είναι μυστικό, διαφημίζεται άφοβα και μπορεί οποιοσδήποτε να μπει.

Ο Peter Beruk, αντιπρόεδρος των Εταιρειών της Software & Information Industry Association, είπε ότι έχουν γίνει πολλές έρευνες και προειδοποιήσεις προς τους χρήστες αλλά είναι η πρώτη φορά που λαμβάνονται νομικά μέτρα.

#### **ΠΕΡΙΠΤΩΣΗ 44<sup>η</sup> (17/11/1999)**

##### **«Συνάντηση με τον Εχθρό»**

Οι hackers λένε ότι ο κόσμος τους έχει παρεξηγήσει αλλά αγαπούν την δημοσιότητα.

Λένε ότι δεν είναι επικίνδυνοι, αλλά προειδοποιούν τους χρήστες των Η/Υ να πάρουν πιο γερά μέτρα ασφαλείας για τους ηλεκτρονικούς υπολογιστές.

Λένε ότι δεν ενδιαφέρονται πάντα για εγκληματική δραστηριότητα όπως κλέψιμο, καταστροφή ή κατασκοπεία. Κάνουν hacking για πνευματική περιέργεια και για παρατήρηση.

Σε ένα ασυνήθιστο πάρε δώσε που έλαβε χώρα χθες βράδυ σε ξενοδοχείο στην πολιτεία της Washington, ένας αριθμός από αμετανόητους hackers εξήγησαν γιατί εισβάλουν στα συστήματα των ηλεκτρονικών υπολογιστών.

Είπαν ότι είναι για πλάκα και για την ικανοποίηση της περιέργειας τους. Και τα αναζητούν αυτά τόσο άπληστα που ρισκάρουν να τους επιβληθούν ποινές για αθέμιτες διεισδύσεις σε ηλεκτρονικούς υπολογιστές.

### **200 ειδικοί παρίστανται**

Αυτή την εβδομάδα το Ινστιτούτο Ασφαλείας Ηλεκτρονικών Υπολογιστών διοργάνωσε συνέδριο με θέμα την ασφάλεια των ηλεκτρονικών υπολογιστών, στο Ξενοδοχείο Marriott στην πολιτεία Washington. Οι hackers ξεπρόβαλαν στην αίθουσα χορού του ξενοδοχείου σε μία ακουστική διάσκεψη αντιμέτωποι με ένα κοινό περίπου 200 ατόμων. Το όνομα της σύσκεψης: «Γνώρισε τον εχθρό».

Ανάμεσα στο κοινό βρίσκονταν άνθρωποι που δουλεύουν για την κυβέρνηση, το στρατό, εργάζονται στη παρασκευή hardware και software, εργαζόμενοι σε εταιρείες που παρέχουν οικονομικές συναλλαγές και σε εμπορικά καταστήματα του διαδικτύου.

Το κοινό έκανε ερωτήσεις στους hackers, αναγνωρίζοντάς τους μόνο από τους «τίτλους» που είχαν στο Internet. Εξέφρασαν ακόμη και τη λύπη τους για τις ποινές που εφαρμόζονται από το νόμο στους hackers για τις παραβιάσεις που κάνουν. Οι οργανωτές της φιλικής αυτής συζήτησης είπαν ότι σκοπός τους ήταν να ανυψωθεί η δικτυακή διπλωματία.

Οι hackers μιλούσαν με αυτοπεποίθηση και κυνισμό, επιδείκνυαν μία συνεπή γραμμή «μαύρου» χιούμορ με αποτέλεσμα να κάνουν τους παρευρισκόμενους να γελούν όλο το βράδυ. Οι ειδικοί ασφαλείας των Η/Υ φάνηκαν να τρομάζουν από τους νεαρούς hackers.

### **Η αλλαγή ενός site είναι κατοπινή σκέψη**

Κάποιος ρώτησε πως δικαιολογούνται πολιτικά αλλαγές σε Web Sites όπως του FBI, του Κογκρέσου ή άλλων κυβερνητικών ιδρυμάτων, όπου εμφανίζονται παράξενα σλόγκαν και εικόνες.

Ένας hacker ονομαζόμενος Elias Levy είπε ότι οι αλλαγές είναι συχνά μία σκέψη μετά από μία επιτυχημένη διείσδυση που είχε ως σκοπό την δημοσιότητα.

Κάποιος άλλος hacker είπε ότι αυτό δίνει την δυνατότητα στα πολυμέσα να φτιάχνουν περισσότερες λέξεις που περιγράφουν τη δραστηριότητα των hackers.

Σχετικά με τον χαρακτηρισμό των hackers ως «διάβολοι των πολυμέσων», είπαν ότι τα ΜΜΕ θεωρούνται αναγκαία για τους hackers που θέλουν τα κατορθώματά τους στο δίκτυο να αναγνωρίζονται από το κοινό και από τις κρυφές οργανώσεις του Internet.

### **Που στοχεύουν οι hackers**

Ένας hacker με το όνομα Microft, απάντησε σε μια ερώτηση που αφορούσε την επιλογή του στόχου, λέγοντας ότι υπάρχουν διάφορες σκέψεις: «Κοιτάζουμε διάφορα πράγματα, όπως την προσπέλαση, τη σύνδεση ή τη δημοσιότητα». Οι αλλαγές τυπικά υπογράφονται από έναν αναγνωρίσιμο τίτλο.

Οι περισσότεροι από τους συμμετέχοντες hackers είχαν πάνω από μία δεκαετία εμπειρίας στα δίκτυα ηλεκτρονικών υπολογιστών, ενώ πολλοί παραδέχθηκαν ότι λίγο ή πολλοί μπήκαν στον ίδιο δρόμο και τώρα δουλεύουν ως σύμβουλοι ασφαλείας.

Ο Βρετανός hacker Maelstrom είπε: «Οι hackers πιάνονται, αποφασίζουν ότι δεν θέλουν να τους πιάσουν ή ωριμάζουν και

απλά αλλάζουν». «Πολλοί συλλαμβάνονται και πηγαίνουν φυλακή, τους παίρνουν τα υπάρχοντά τους και χρειάζεται να αρχίσουν πάλι από την αρχή», είπε ένας άλλος με το όνομα K0resh. «Είμαι 29 ετών και δεν θέλω να ξεκινήσω πάλι από την αρχή».

### **Μπαίνουν στον πειρασμό να ακολουθήσουν την σκοτεινή πλευρά**

Οι μετανοημένοι hackers μπαίνουν τακτικά στον πειρασμό να ακολουθήσουν την σκοτεινή πλευρά του Internet και ακόμα τριγυρνούν γύρω από αυτή.

Όλοι ισχυρίζονται ότι έχουν λάβει παρακλήσεις – συχνά προσωπικά – από ξένα μυαλά, ομοσπονδιακούς πράκτορες και ενεργά σωματεία που ψάχνουν πληροφορίες ανταγωνιστών, όπως πρωτότυπα σχέδια. Λένε ότι τους προσφέρουν χιλιάδες δολάρια για να κάνουν παράνομες διεισδύσεις.

«Λαμβάνω σε καθημερινή βάση προτάσεις για κάνω hacking για διάφορα πράγματα», είπε ο Maelstrom.

Όταν με πλησιάζουν, «Έχω μια μικρή διαίσθηση που μου λει ότι εδώ θα μπλέξω. Δεν το σκέφτομαι πολύ. Απλά τους λεω όχι, και συνεχίζω τον δρόμο μου» λει ο K0resh.

### **Μπορούν να μπουν σχεδόν οπουδήποτε**

Η κύρια παραδοχή από τους δικηγόρους και τους μυστικούς είναι ότι οι έμπειροι hackers μπορούν να εισβάλουν σχεδόν παντού. Και η παραδοχή τους είναι σωστή.

Ένας hacker είπε ότι κανένα σύστημα δεν είναι «αλεξίσφαιρο», αλλά όλα τα δίκτυα ηλεκτρονικών υπολογιστών μπορούν να ενισχυθούν με «πύρινους τοίχους» ή άλλα μέτρα.

Κάποιος ρώτησε: «Υπάρχει κάτι στο οποίο δεν μπορείτε να εισβάλετε;».

«Μπανάνες», αστειεύτηκε ο Microsoft. «Και τα kiwis (φρούτο Νέας Ζηλανδίας) δύσκολα ξεφλουδίζονται».

## Συντριβή των μύθων

Ο σύμβουλος ασφαλείας Ray Karlan είπε ότι η 10η επέτειος της διάσκεψης σχεδιάστηκε για να συντρίψει την μυθολογία που περιβάλλει τους hackers και που είναι πάντα συνδεδεμένη με εγκληματική δραστηριότητα.

«Κατά την άποψή μου, ο όρος «hacker» έχει κατά πολύ δυσφημιστεί, κακοποιηθεί, κακοχρησιμοποιηθεί ή δεν έχει γίνει κατανοητή» είπε στο ABPnews.com. Είπε ακόμη ότι στους hackers αρέσει να βοηθούν αυτό που ονομάζεται νόμιμη κοινωνία να καταβάλουν τα μυστικά που θα τους παρέχουν ασφάλεια.

## Ο φόβος για το 2000

Οι συμμετέχοντες στο συνέδριο επανειλημμένως ζητούσαν να ξέρουν αν υπάρχει κάποια αλήθεια όσον αφορά τις φήμες για τα προβλήματα που θα δημιουργηθούν από τον Y2K, τον 10ο της χιλιετίας, και αν θα αυξηθούν οι επιθέσεις, οι εισβολές και οι ληστείες στο δίκτυο. Ο hacker Maelstrom απάντησε «Η μεγαλύτερη τρωτότης είναι ότι οι άνθρωποι δίνουν πολύ μεγάλη προσοχή σε αυτήν την ερώτηση, και δεν ξοδεύουν αρκετά χρήματα για ασφάλεια».

«Οι περισσότεροι hackers θα είναι πολύ μεθυσμένοι την Πρωτοχρονιά, γι' αυτό όλοι θα είστε ασφαλείς».

## ΠΕΡΙΠΤΩΣΗ 45<sup>η</sup> ( 19/11/99 )

### «Πόλεμος» σε chat room

Ο Pro Tem Marcine Anderson, δικαστής στο King Country District Court, εμπόδισε έναν 47χρονο άντρα με το όνομα Scotto Abraham να συμμετέχει σε ένα newsgroup αφιερωμένο σε λάτρεις του ski. Η υπόθεση ξεκίνησε από μία διαμάχη για εισιτήρια του ski στο Internet usenet newsgroup: rec.skiing.alpine και εξελίχθηκε σε μια άγρια σειρά κατηγοριών και αντικατηγοριών μεταξύ αυτών που μετείχαν στο chat room του newsgroup. Ο Δικαστής εξέδωσε περιοριστική διαταγή όσον



αφορά τη συμμετοχή του Abraham στο συγκεκριμένο newsgroup, έπειτα από τις κατηγορίες ενός άλλου άντρα με το όνομα Hobbs για παρενόχληση. Ο Hobbs κατήγγειλε ότι ο Abraham τον είχε ενοχλήσει πολλές φορές από τον Μάρτιο του 1999 τρομοκρατώντας αυτόν και τους φίλους του.

Η διαμάχη μεταξύ τους άρχισε τον προηγούμενο Μάρτιο για το ποιος θα πάρει τα δωρεάν εισιτήρια ski. Ο Abraham είχε κερδίσει τα εισιτήρια και τα έδωσε στην Anthea Kerrison, η οποία όπως φαίνεται τα έδωσε στον Hobbs, τον οποίο δεν ενέκρινε ο Abraham. Ο Abraham τότε είχε μια συνομιλία με την Kerrison μέσω του chat room και η διαφωνία τους εξελίχθηκε σε δικτυακό πόλεμο με όλα τα μέλη.

Ο Jim Biesterfield, ιδιωτικός αστυνομικός στην πολιτεία του Los Angeles, φίλος του Hobb, ο οποίος ασχολήθηκε με την υπόθεση, έκρινε ότι ο Abraham ήταν επικίνδυνος και έκρινε απαραίτητο να προσφύγει στις αρχές. Βέβαια ο Abraham αρνείται ότι απείλησε ποτέ κανέναν και ισχυρίζεται ότι εκείνος ήταν που δεχόταν απειλές θανάτου και ενοχλήσεις.

Με την εξέλιξη που είχε λάβει η διαμάχη χρειάστηκε εκτός από την περιοριστική εντολή του δικαστή και το εξής μήνυμα, το οποίο τοποθετήθηκε στο newsgroup:

«Ζητάμε από όλους τους συμμετέχοντες του newsgroup να σταματήσουν τις συζητήσεις που δεν έχουν άμεση σχέση με το ski. Χρειάζεται μια ανακωχή. Αγνοήστε οτιδήποτε δεν είναι φιλικό και δεν σχετίζεται με το ski. Μην ανταποκρίνεστε σε οτιδήποτε έχει σχέση μ' αυτή την υπόθεση. Αν υπάρχουν ερωτήσεις μπορείτε να στείλετε e-mail. Ζητάμε από όλες τις πλευρές να σταματήσουν τον πόλεμο των λέξεων. Εκτιμούμε τη συνεργασία όλων των πλευρών που εμπλέκονται. Νομίζουμε ότι η ομάδα θα μπορέσει να ξαναβρεί τα ίχνη της».

## ΠΕΡΙΠΤΩΣΗ 46<sup>η</sup> ( 23/11/99 )

### Συλλαμβάνεται νεαρός hacker για επίθεση στο Web site του Λευκού Οίκου

Ο hacker Eric Burns, περιπλανήθηκε σε ιστοσελίδες στο Internet όπου λίγοι είχαν περιπλανηθεί πριν από αυτόν, κατάφερε ακόμα να εισβάλει παράνομα στους ηλεκτρονικούς υπολογιστές του Λευκού Οίκου την περασμένη άνοιξη.

Σήμερα, ο Eric Burns, γνωστός στο Internet με το όνομα «Zyklon» και μόλις 19 χρονών, βρίσκεται αντιμέτωπος με 15 μήνες φυλάκιση και πληρώσει πρόστιμο \$36.240 για την αποκατάσταση των θυμάτων του. Του απαγορεύτηκε ακόμη να αγγίξει ηλεκτρονικό υπολογιστή για τρία χρόνια μετά την αποφυλάκισή του.

«Ειλικρινά δεν πίστευα ότι θα γινότανε τόσο μεγάλο ζήτημα» είπε ο Burns, ο οποίος αποδέχτηκε την ευθύνη για τις εντυπωσιακές επιθέσεις σε σωματειακά και κυβερνητικά sites στο Internet κατά την διάρκεια της εκδίκασης της υπόθεσής του.

Ο Burns ομολόγησε την ενοχή του για μία μόνο από τις κατηγορίες που του απαγγέλθηκαν σχετικά με την σκόπιμη εισβολή σε έναν ηλεκτρονικό υπολογιστή. Επιπλέον παραδέχτηκε την ανάμειξή του και σε μία σειρά από άλλες ηλεκτρονικές επιθέσεις.

Ο Burns αρχικά παραπέμφθηκε για την 13η Μαΐου για κατηγορούμενος ότι εισέβαλε στους ηλεκτρονικούς υπολογιστές της Αμερικάνικης Υπηρεσίας Πληροφοριών και δύο επιχειρήσεων. Αυτό συνέβη 4 ημέρες μετά την επίθεση που δέχθηκε η σελίδα στο Internet του Λευκού Οίκου.

Αρχικά ο Burns είπε ότι δεν είχε άμεση σχέση με την επίθεση στον Λευκό Οίκο. Η επίθεση αυτή περιελάμβανε μία δήλωση και μία λίστα από 12 ονόματα μεταξύ των οποίων και το όνομα «Zyklon», οι οποίοι αναλάμβαναν την επίθεση.

Σύμφωνα με ομοσπονδιακούς εισαγγελείς που είχαν αναλάβει την υπόθεση, ο Burns υπερηφανευόταν για την δικτυακή εισβολή στο Λευκό Οίκο πριν ακόμα γίνει. Στη δίκη ο Burns παραδέχθηκε ότι αυτός μαζί με άλλους δύο άλλαξαν το

site έτσι ώστε να δείχνει μία μαύρη ιστοσελίδα με τα ονόματα ομάδων hacker και διάφορα μηνύματα.

Σε τηλεφωνική συνέντευξη που έδωσε ο Burns από το σπίτι του στην περιοχή Shoreline, είπε, ότι αρνήθηκε να μαρτυρήσει τους δύο συνεργάτες του στις Μυστικές Υπηρεσίες, κυρίως γιατί πιστεύει ότι οι ποινές που αποδίδονται στους hackers είναι πολύ αυστηρές.

«Προτιμώ αυτό που συνέβη σε μένα να μη συμβεί σε κανέναν άλλο. Δεν συμφωνώ με τις ποινές που υπάρχουν για το έγκλημα» είπε ο Burns.

Τη σοβαρότητα του προβλήματος δεν φαίνεται να καταλαβαίνει ο Burns ο οποίος θεωρούσε ασήμαντη την πράξη του ακόμα και όταν πράκτορες του FBI εισέβαλαν στο σπίτι του.

### **Μεγάλο το κόστος των εισβολών**

Σύμφωνα με τη δικηγόρο Helen Fahey, ο Burns εισέβαλε στο Internet ελέγχοντας τα Web sites του NATO, της Αμερικάνικης Πρεσβείας και διαφόρων προξενείων. Κατάφερε ακόμη μαζί με τους συνεργάτες του να κλείσει το USIA Web site για οκτώ ημέρες. Αυτές οι εισβολές κόστισαν στην κυβέρνηση και στις επιχειρήσεις περισσότερα από \$40.000.

### **Ελπίδες για μείωση της ποινής**

Ο Burns ελπίζει ότι στη φυλακή θα τον αφήσουν να περάσει τις γιορτές με την οικογένειά του. Ο δικηγόρος του είπε ότι αν επιδείξει καλή συμπεριφορά στη φυλακή είναι πιθανότατο να αποφυλακιστεί σε λιγότερο από 13 μήνες. Παρ' ότι η καταδίκη του δεν του επιτρέπει την χρησιμοποίηση ηλεκτρονικού υπολογιστή για τρία χρόνια μετά την αποφυλάκισή του, ο Burns σκοπεύει να ζητήσει να του επιτραπεί η χρήση του ηλεκτρονικού υπολογιστή για δουλειά υπό επιτήρηση.

«Ειλικρινά δεν γνωρίζω πως η σύλληψη και ο χρόνος που θα μείνω στη φυλακή θα με επηρεάσουν στο μέλλον. Ελπίζω ότι δεν θα το επηρεάσουν πάρα πολύ άσχημα» δήλωσε ο Burns.

## ΠΕΡΙΠΤΩΣΗ 47<sup>η</sup> ( 26/10/99 )

### Καταπολέμηση της παιδικής πορνογραφίας

Με σκοπό την καταπολέμηση της παιδικής πορνογραφίας, βρέθηκαν στο Texas, ο Γενικός Εισαγγελέας της πολιτείας του Texas και εκπρόσωποι των υπηρεσιών παροχής Internet. Μια ασυνήθιστη συνεργασία μεταξύ δημόσιου και ιδιωτικού τομέα θα υπάρχει από εδώ και στο εξής αφού οι εκπρόσωποι των υπηρεσιών του Internet συμφώνησαν να προμηθεύουν με σχετικές αναφορές από τα sites τους περιστατικά παιδικής πορνογραφίας, τον Γενικό Εισαγγελέα, John Cornyn.

Με αυτή τη συμφωνία οι παιδικοί πορνογράφοι θα δυσκολευτούν να βρουν ασφαλή χώρο στο διαδίκτυο για την έκθεση του υλικού τους και οι υπηρεσίες του Internet δε θα έχουν το φόβο να κατηγορηθούν για συνενοχή στην κατοχή του απαγορευμένου υλικού ενημερώνοντας τις αρχές.

«Έχουμε ένα κοινό στόχο: να βγάλουμε την παιδική πορνογραφία από το Internet. Αυτές οι κατευθυντήριες γραμμές εξυπηρετούν τα συμφέροντα της πολιτείας γιατί θα βγάλουν αυτούς τους εγκληματίες από το Internet. Και τα συμφέροντα των εταιρειών του Internet αφού θα κερδίσουν την εμπιστοσύνη του καταναλωτή. Πρόκειται για μια ισόπαλη συμφωνία και ελπίζω να ακολουθήσουν και άλλες εταιρείες.»

Σύμφωνα με τους όρους αυτής της συμφωνίας όταν ένας χρήστης καταγγείλει ότι συνάντησε παιδική πορνογραφία σε κάποιο site, η υπηρεσία του Internet θα πρέπει να εξακριβώσει αν πραγματικά στο συγκεκριμένο site υπάρχει τέτοιου είδους υλικό και να μεταφέρει την πληροφορία στον Γενικό Εισαγγελέα. Ο Γενικός Εισαγγελέας θα εξετάσει την καταγγελία και μέσα σε δύο εβδομάδες θα πρέπει να ενημερώσει τους ενδιαφερόμενους αν υπάρχει υπόθεση που να στηρίζεται στις καταγγελίες.

Η εκπρόσωπος του γραφείου του Γενικού Εισαγγελέα, είπε ότι αυτή η συμφωνία θα μπορούσε να αποτελέσει εθνικό μοντέλο για άλλες συμφωνίες.

Μία από τις υπηρεσίες παροχής υπηρεσιών του Internet που έλαβε μέρος στη συμφωνία είναι η America On Line (AOL), ο μεγαλύτερος προμηθευτής του Internet για τις ΗΠΑ. Ο Don Colcolough, Γενικός Διευθυντής του Δικτύου Ασφαλείας και Παρακολούθησης της AOL, είπε ότι η εταιρεία δεν έχει καμία ανοχή απέναντι στην παράνομη συμπεριφορά: «Η προστασία και ασφάλεια των μελών είναι η πρώτη προτεραιότητα της America Online. Συνεργαζόμαστε στενά με υπηρεσίες εκτέλεσης του νόμου έτσι ώστε να εξασφαλίζουμε στα μέλη ασφάλεια. Τα μέλη μας ενδιαφέρονται και για την ανάγκη καταπολέμησης της παιδικής πορνογραφίας στο Internet και για την ανάγκη προστασίας του ιδιωτικού απορρήτου. Αισθανόμαστε ότι οι κατευθυντήριες γραμμές της συμφωνίας σκιαγραφούν μία διαδικασία η οποία επισπεύδει την εκτέλεση του νόμου και διαβεβαιώνουν ότι τα προσωπικά στοιχεία των πελατών μας θα κρατηθούν μυστικά έως το βαθμό που ορίζει ο νόμος. Έτσι ενθαρρύνουμε όλες τις υπηρεσίες παροχής υπηρεσιών να υιοθετήσουν την ίδια διαδικασία αντιμετώπισης του προβλήματος».

Ο Ed Cavazos, Αντιπρόεδρος Νομικών και Επαγγελματικών Υποθέσεων, στο Internet, είπε: «Το Internet δε θα πρέπει να αποτελεί ένα ασφαλές καταφύγιο για τους παιδικούς πορνογράφους. Η συνεργασία με τις αρχές θα εξασφαλίσει να μη συμβεί αυτό».

### **ΠΕΡΙΠΤΩΣΗ 48<sup>η</sup> (01/12/99)**

#### **Κλεμμένα αντικείμενα δημοπρατούνται στο Διαδίκτυο**

Πρόκειται για αντικείμενα που είχε στην κατοχή του ο Morris Sochaccowski μέσα στο αυτοκίνητό του μέχρι την στιγμή που τον λήστεψαν. Τότε είχε καταγγείλει το συμβάν στην αστυνομία αλλά δεν έλπιζε να βρεθούν τα αντικείμενα τα οποία είχαν κυρίως συναισθηματική αξία αφού επρόκειται για αντικείμενα θρησκευτικής λατρείας. Ακολουθώντας τη συμβουλή ενός φίλου του αποφάσισε να κοιτάξει για τα κλεμμένα αντικείμενα στο διαδίκτυο και τα βρήκε στο site eBay. Συγκεκριμένα, βρήκε ένα εβραϊκό σετ προσευχής από μπλε βελούδο του οποίου η περιγραφή έμοιαζε πολύ με αυτό που του

είχε κλαπεί. Τότε επικοινωνήσε με τον αστυνομικό Ken Driscoll, ο οποίος χρησιμοποίησε τον προσωπικό του ηλεκτρονικό υπολογιστή για να μην κινήσει υποψίες και προσφέροντας αρχικά \$158 για το επίμαχο αντικείμενο και καταλήγοντας στην προσφορά των \$395 έκλεισε την συμφωνία. Μ' αυτό τον τρόπο βρέθηκε στο σπίτι της γυναίκας που πουλούσε τα αντικείμενα με την πρόφαση να τα αγοράσει. Τα αντικείμενα που είχε στην κατοχή της ήταν εκείνα που είχαν κλαπεί στις 23 Νοεμβρίου από το αυτοκίνητο του Sochacewski. Η γυναίκα ισχυρίστηκε ότι τα είχε αγοράσει σε ένα παζάρι.

Ο Kevin Pursglove, εκπρόσωπος του site eBay, είπε ότι τα συγκεκριμένα πράγματα δεν είναι παρά μόνο ένα μικρό τμήμα από τα 400.000 αντικείμενα που προσφέρονται για πώληση στο site καθημερινά των οποίων η προέλευση αμφισβητείται. Πρόσθεσε ότι συχνά στο site eBay υποβάλλονται παράξενες προσφορές, συμπεριλαμβανομένων και προσφορών ανθρώπινων οργάνων. Η εταιρεία ανησυχεί γι' αυτό και συνεργάζεται με τις αρχές όταν οι πωλητές παραβιάζουν τους κανόνες που έχει θέσει το site.

### ΠΕΡΙΠΤΩΣΗ 49η ( 02/12/99 )

#### Νόμος για τις πωλήσεις μέσω Internet

Όσον αφορά την πώληση αγαθών στο Internet για την πολιτεία της Βόρειας Carolina, ισχύει ένας νόμος ο οποίος απαιτεί άδεια από την πολιτεία για τις πωλήσεις. Οι αρχές τύπωσαν φυλλάδια με στόχο να ενημερώσουν τους πολίτες και το κοινό της Βόρειας Carolina για την ισχύ του νόμου, αφού πρόσφατη έρευνα έδειξε ότι κάθε χρόνο γίνονται 20.000 πωλήσεις στο site eBay που προέρχονται από την πολιτεία της Βόρειας Carolina. Ο νόμος ορίζει πρόστιμο \$175 για τους παραβάτες και από την 1<sup>η</sup> Ιανουαρίου 2000 το πρόστιμο θα αυξηθεί σε \$250 συν \$150 για ανανέωση συνδρομής και \$50 για το ταμείο διαχείρισης αποθεματικών κεφαλαίων.

Ο νόμος ισχύει για όσους αγοράζουν πράγματα και τα μεταπωλούν μέσω Internet και όχι για εκείνους που θέλουν να πουλήσουν κάτι που έχουν στην κατοχή τους και δεν το θέλουν πια, ή εκείνους που πουλούν πράγματα για χόμπι. Το πρόβλημα

έγκειται στο να γίνει διαχωρισμός αυτών των δύο κατηγοριών των πωλητών και γι' αυτό το λόγο οι αρχές ευελπιστούν στην εθελοντική συμμόρφωση με το νόμο.

Η ανάγκη ύπαρξης του παραπάνω νόμου προέρχεται από την ανησυχία και ανάγκη των χρηστών – αγοραστών να μην πέσουν θύματα απάτης.

### **ΠΕΡΙΠΤΩΣΗ 50<sup>η</sup> (03/12/99)**

#### **Ο ιός της Πρωτοχρονιάς**

Οι ειδικοί ηλεκτρονικών υπολογιστών προειδοποιούν για την ύπαρξη ενός νέου καταστροφικού ιού ο οποίος μεταδίδεται μέσω e-mail. Ο ιός έχει σχεδιαστεί για να σβήσει όλα τα αρχεία που βρίσκονται στο σκληρό δίσκο των ηλεκτρονικών υπολογιστών την Πρωτοχρονιά.

Ο ιός, που ανακαλύφθηκε την Πέμπτη, ονομάστηκε W32.Myrics.Worm. Επηρεάζει τα συστήματα Windows 95, Windows 98 και Windows NT. Το καταστροφικό του φορτίο είναι σχεδιασμένο να ενεργήσει τα μεσάνυχτα στις 31 Δεκεμβρίου.

Ο Simo Perry, διευθυντής της εταιρείας eTrust είπε ότι ο ιός έχει σχεδιαστεί για να προκαλέσει σημαντική ζημιά το έτος 2000. Και πρόσθεσε: «Όσο πλησιάζει το έτος 2000, αρχίζουμε να βλέπουμε μια αυξημένη συχνότητα εμφάνισης επικίνδυνων ιών».

Οι ειδικοί λένε ότι ο ιός εξαπλώνεται από μόνος του στέλνοντας ηλεκτρονικά μηνύματα μέσω του address book (διευθύνσεις) που υπάρχουν στο Outlook σε τουλάχιστον 50 άτομα. Η γραμμή του θέματος του μηνύματος παραμένει κενή ενώ στο κείμενό του υπάρχει η φράση: «Εδώ είναι μερικές φωτογραφίες για σένα». Περιέχει ακόμη ένα συνημμένο πρόγραμμα που ονομάζεται pics4you.exe (34.304 bytes). Προσπαθεί να ξεγελάσει τον χρήστη κάνοντάς τον να πιστέψει ότι το συνημμένο αρχείο περιέχει εικόνες. Όταν ο χρήστης το ανοίξει, το πρόγραμμα δεν εμφανίζει εικόνες και απλά φαίνεται ότι δεν λειτουργεί. Έτσι όμως ο ιός εγκαθίσταται στη μνήμη και στέλνεται σε 50 τουλάχιστον ακόμη άτομα. Η εγγραφή των

Windows τροποποιείται με αποτέλεσμα ο ιός να είναι πάντα παρών στον ηλεκτρονικό υπολογιστή. Ο ιός κουβαλά δύο φορτία που μοιάζουν με τον ιό Y2K (ο ιός του 2000). Ο ιός παρακολουθεί το σύστημα του ρολογιού και όταν ανιχνεύσει ότι το έτος είναι το 2000, τότε τροποποιεί το σύστημα BIOS. Όταν ο χρήστης θα ανοίξει τον ηλεκτρονικό υπολογιστή, θα εμφανιστεί στην οθόνη το μήνυμα «CMOS Checksum Invalid» και θα είναι αδύνατη η επανεκκίνηση του υπολογιστή. Δήθεν λύση στο πρόβλημα είναι η διόρθωση του BIOSsetup. Όταν όμως διορθωθούν οι εγκαταστάσεις BIOS, ο ιός θέτει σε εφαρμογή το δεύτερο φορτίο και μορφοποιεί το σκληρό δίσκο.

Οι ειδικοί ασφαλείας ηλεκτρονικών υπολογιστών έχουν χαρακτηρίσει τον ιό ως μέτριας επικινδυνότητας και έχουν τοποθετήσει σε ιστοσελίδες ειδικό software που θα βοηθήσει τους χρήστες να αποτρέψουν τη δράση του ιού.

Ο ιός βρίσκεται σε «έξαρση» από την άποψη ότι κάθε ανυποψίαστος χρήστης ηλεκτρονικού υπολογιστή μπορεί να το λάβει. Είναι σημαντικό οι χρήστες να λάβουν τα απαραίτητα μέτρα έτσι ώστε οι ηλεκτρονικοί υπολογιστές να είναι σε θέση να παραμείνουν ασφαλείς μετά από την επίθεση του ιού.

### **ΠΕΡΙΠΤΩΣΗ 51<sup>η</sup> ( 07/12/99 )**

#### **Νέος επικίνδυνος ιός**

Ερευνητές σε θέματα προστασίας ηλεκτρονικών υπολογιστών, ανακάλυψαν ένα νέο καταστροφικό ιό, ο οποίος είναι μια διόρθωση του ιού Y2K και είναι ικανός να σβήσει τον σκληρό δίσκο του ηλεκτρονικού υπολογιστή και να «ξαφρίσει» πληροφορίες για τις πιστωτικές κάρτες του χρήστη. Ο ιός μεταδίδεται μέσω του m/RC, ενός προγράμματος που χρησιμοποιείται για τη σύνδεση σε chat rooms στο Internet όπου ανταλλάσσονται δακτυλογραφημένα μηνύματα. Είναι σχεδιασμένος να λειτουργεί στο περιβάλλον των Windows 95, Windows 98 και NT και είναι ιδιαίτερα επικίνδυνος γιατί εξαπλώνεται γρήγορα και αυτοενεργοποιείται αμέσως μετά τη μόλυνση του υπολογιστή.



Μέσω του προγράμματος m/RC, ο ιός, αυτόματα μεταδίδεται σε όλους όσους βρίσκονται στο chat room. Με την ενεργοποίησή του, μολύνονται όλα τα προγράμματα και τα αρχεία και πολλά από αυτά καταστρέφονται. Έπειτα, κάθε φορά που ο χρήστης συνδέεται με το m/RC, ο ιός βρίσκει ένα Ιαπωνικό site στο οποίο ψάχνει για νέες καταστροφικές μορφές του ιού, γνωστές ως «plug-ins» και τα μεταφέρει στον μολυσμένο υπολογιστή. Μερικά από τα «plug-ins» μπορούν να αλλάξουν ή να διαγράψουν τον σκληρό δίσκο και να συγκεντρώσουν προσωπικές πληροφορίες για τις πιστωτικές κάρτες του χρήστη. Προς το παρόν υπάρχουν 4 plug-ins που ο ιός κατεβάζει από το site, αλλά οι ειδικοί προειδοποιούν ότι ο κατασκευαστής του ιού είναι σε θέση να τα αλλάζει συχνά.

Ο Simon Perry, στέλεχος της διοίκησης της εταιρείας ασφάλειας ηλεκτρονικών υπολογιστών Computer Associates International Inc. Security Solutions είπε: «Είναι ένας ιδιαίτερα επικίνδυνος ιός εξαιτίας της ικανότητας του δημιουργού του να αλλάζει τη μορφή του ιού και μετά την μόλυνση των ηλεκτρονικών υπολογιστών. Ως εταιρεία συνιστούμε στις επιχειρήσεις και όλους τους χρήστες να ενημερώσουν τα προγράμματα anti-virus αμέσως».

Ο ιός, για τον οποίο πιθανότατα είναι υπεύθυνη η αυτοαποκαλούμενη ομάδα 29<sup>A</sup>, θα προσπαθεί να τροποποιήσει το μολυσμένο σύστημα εκθέτοντας στην οθόνη τα εξής μηνύματα:

WAS/Babylonia by Venca ( c) 1999  
Greetz to Roadkil and Virus Buster  
Big thankz to sok4ever webmaster  
Abracos pra galera bruzuca!!!  
Eu boto fogo na Babilonia!

Οι δύο τελευταίες φράσεις είναι στα Πορτογαλικά και μεταφράζονται ως εξής:

«Αγκαλιές στους φίλους!!!»  
«Βάζω φωτιά στη Βαβυλωνία!».

Η σημασία τους είναι άγνωστη.

Ο ιός στέλνει e-mail μετά από κάθε επίθεση στην διεύθυνση [babylonia\\_counter@hotmail.com](mailto:babylonia_counter@hotmail.com). Οι ειδικοί πιστεύουν ότι μ'

αυτό το τρόπο ο δημιουργός του ιού μπορεί να εντοπίσει τους μολυσμένους ηλεκτρονικούς υπολογιστές.

### ΠΕΡΙΠΤΩΣΗ 52<sup>η</sup> ( 9/12/99 )

#### Ο δημιουργός του ιού "Melissa"

Ο 31χρονος David L. Smith, δήλωσε ένοχος στην κατηγορία της δημιουργίας του ιού "Melissa", ο οποίος προκάλεσε ζημιές εκατομμυρίων δολαρίων (υπολογίζονται περισσότερα από \$80 εκατομμύρια) σε συστήματα ηλεκτρονικών υπολογιστών σε όλο τον κόσμο.

Ο Smith με τη δήλωση ενοχής αντιμετωπίζει μέχρι 10 χρόνια φυλάκιση. Στις 18 Φεβρουαρίου 2000 το δικαστήριο θα ανακοινώσει την ποινή του. (βλ. ΠΕΡΙΠΤΩΣΗ 8η, 1 Απριλίου 1999, σελ. 42 και ΠΕΡΙΠΤΩΣΗ 9η, 2 Απριλίου 1999, σελ. 43).

### ΠΕΡΙΠΤΩΣΗ 53<sup>η</sup> ( 15/12/99 )

#### Απειλή φόνου μέσω Internet

Στην φυλακή κρατείται ο 32χρονος Paul Clark γιατί απειλούσε να σκοτώσει 2 άτομα. Ο Clark είχε τοποθετήσει στην προσωπική του ιστοσελίδα μια αγγελία «φόνου», σύμφωνα με την οποία ήταν διατεθειμένος να πληρώσει \$25.000 σε όποιον σκότωνε ένα ζευγάρι από το Texas, τον Rick και την Brandy Arnett από το El Paso, του Texas. Επιπλέον είχε τοποθετήσει και μία φωτογραφία του ζευγαριού, ενώ προκειμένου να δώσει τα χρήματα ζητούσε να του στείλουν φωτογραφίες που θα αποδείκνυαν το θάνατό τους.

Προφανώς ο Clark είχε κάποιο ερωτικό ενδιαφέρον για την 26χρονη Brandy Arnett, το οποίο αναπτύχθηκε κατά τη διάρκεια της ηλεκτρονικής αλληλογραφίας μεταξύ τους.

Ο Clark διαβεβαίωνε επίσης για την εγκυρότητα της προσφοράς εφ' όσον θα είχε στα χέρια του τις αποδείξεις που θα επαλήθευαν ότι το ζευγάρι ήταν νεκρό.

Η έρευνα άρχισε όταν η αστυνομία του El Paso ανέφερε την υπόθεση στην αστυνομία του Portsmouth και δύο μήνες αργότερα ο P. Clark συνελήφθη στο σπίτι του. Κατασχέθηκαν δισκέτες ηλεκτρονικού υπολογιστή και χιλιάδες έγγραφα. Ο Clark τώρα βρίσκεται στη φυλακή και θα δικαστεί μέσα στην επόμενη εβδομάδα.

Ο Derrek Stone, αστυνομικός στο Portsmouth, είπε ότι είναι η πρώτη υπόθεση αυτού του είδους στη Βρετανία. Παρά την σοβαρότητα της υπόθεσης το FBI δεν θα προβεί σε έκδοση του Clark αλλά θα τον αφήσει να δικαστεί στην Βρετανία.

### ΠΕΡΙΠΤΩΣΗ 54<sup>η</sup> ( 15/12/99 )

#### Παραβίαση κυβερνητικού site και τραπεζική απάτη

Τρεις άντρες κρατούνται στις φυλακές του Monmouth County, κατηγορούμενοι για κλοπή των κωδικών Κοινωνικής Ασφάλισης Αξιωματικών του στρατού και για τραπεζική απάτα, μέσω Internet.

Οι κλέφτες απέκτησαν τους κωδικούς μέσω ενός Web site, το οποίο περιέχει καταλόγους με τους κωδικούς κοινωνικής ασφάλισης για περισσότερους από 4.500 αξιωματικούς. Ανάμεσά τους ήταν ο πρώην πρόεδρος και συνταξιούχος Gen. John Shali Kashvili και ο διοικητής των Αμερικανικών Δυνάμεων στη Νότια Κορέα Gen. John Telilli. Οι τρεις κλέφτες πήραν τους κωδικούς παραβιάζοντας το site και δημιούργησαν 700 ψεύτικες πιστωτικές κάρτες. Σύμφωνα με τον Jan Gilhooly, ειδικός πράκτορας της Μυστικής Υπηρεσίας του Newark, οι ύποπτοι κατηγορούνται ότι έκλεψαν πάνω από \$37.000. Σύμφωνα με την πιστωτική αξία των καρτών, οι πιθανές απώλειες μπορούσαν να φτάσουν τα \$1,4 εκατομμύρια. Τα ονόματα των υπόπτων είναι: Lamar Christian, Nevison Stevens οι οποίοι συνελήφθησαν στο Trenton και ο Ida Johnson – Christian ο οποίος συνελήφθη στο Bristol της πολιτείας Pennsylvania.

## **Δημιουργία του site**

Το Web site με τους κωδικούς Κοινωνικής Ασφάλισης, δημιουργήθηκε το 1997 από τον δικηγόρο Glen Roberts. Ο Roberts τοποθέτησε στο site τους κωδικούς Κοινωνικής Ασφάλισης του προσωπικού του στρατού καθώς και άλλων επιφανών προσώπων όπως του Προέδρου της Microsoft Bill Gates, του εκδότη της εφημερίδας New York Times Arthur Sulzberger και του μεγιστάνα των media Ted Turner. Το site ανήκει στην κυβέρνηση και αποτελεί μέρος του αρχείου. Οι κωδικοί κοινωνικής ασφάλισης των αξιωματικών του στρατού στέλνονται μέσω Internet στο Κογκρέσο, το οποίο εκδίδει το Κοινοβουλευτικό Αρχείο, κάθε φορά που η Κυβερνητική Ομάδα ειδοποιείται για μια στρατιωτική προαγωγή.

Ο Roberts ενοχλήθηκε από το γεγονός ότι ορισμένοι αξιωματικοί έστρεψαν τα πυρά προς εκείνον, τον δημιουργό του site και είπε: «Στόχος θα πρέπει να είναι η έλλειψη των νόμων της ιδιωτικής ζωής και της προστασίας των προσωπικών πληροφοριών, όπως είναι οι κωδικοί Κοινωνικής Ασφάλισης. Ο κωδικός Κοινωνικής Ασφάλισης αποτελεί ένα πολύμορφο κλειδί στη ζωή μας, συγχρόνως όμως υποτίθεται ότι είναι ένας μυστικός κωδικός που κρατάει όλους τους υπόλοιπους έξω. Σε αυτό το σημείο, τοποθετούν όλο το θέμα του παγκόσμιου προβλήματος της ιδιωτικής ζωής στους ώμους μου».

## **ΠΕΡΙΠΤΩΣΗ 55<sup>η</sup> ( 15/12/99 )**

### **Επίθεση ακτιβιστών σε site εταιρείας**

Μία εβδομάδα πριν τα Χριστούγεννα, η μεγάλη εταιρεία πώλησης παιχνιδιών στο Internet, eToys.com, έγινε στόχος μια ομάδας ακτιβιστών οι οποίοι παρακινούσαν μέσω Internet τους hackers και τους καταναλωτές να σαμποτάρουν το ηλεκτρονικό εμπόριο του δημοφιλούς επιχειρηματικού site. Η έκκληση για ηλεκτρονική παραβίαση του site της παραπάνω εταιρείας έγινε από την ομάδα RTMark, η οποία στρέφεται κατά της ιδεολογίας που θέλει το Internet ως μέσο για εμπορικές συναλλαγές. Φιλοδοξία της ομάδας είναι να συντρίψει το Web site της εταιρείας eToys και να μειώσει την αξία των μετοχών της.

Η διαδικτυακή διαμάχη γεννήθηκε έπειτα από μια διαφωνία σχετικά με το όνομα domain etoy.com. Το 1995 Ευρωπαίοι καλλιτέχνες δημιούργησαν μία ομάδα με το όνομα αυτό με σκοπό να προβάλλουν τις απόψεις τους για την μη εμπορευματοποίηση του Internet. Δύο χρόνια αργότερα, το 1997, ιδρύθηκε η εταιρεία eToys, με έδρα στην πολιτεία Santa Monica. Τότε η εταιρεία έκανε μία προσφορά πάνω από \$500.000 μετρητά στην ομάδα των καλλιτεχνών για την απόκτηση των δικαιωμάτων του ονόματος, αλλά εκείνοι αρνήθηκαν.

Η εκπρόσωπος της ομάδας RTMark Ernest Lucha, είπε ότι με αφορμή τη διαμάχη του ονόματος και με στόχο το μπουκοτάζ της διαφημιστικής καμπάνιας της εταιρείας στο Internet έγινε έκκληση στους hackers να βρουν τρόπους να παραβιάσουν το site της εταιρείας. Κάτι τέτοιο απαιτεί εξειδικευμένη εργασία, αλλά όπως πρόσθεσε η Lucha, γνωρίζουν πολλούς που θα το έκαναν.

Η εταιρεία eToy εκμεταλλευόμενη το γεγονός ότι ο νόμος δεν προβλέπει την προστασία των ομάδων καλλιτεχνών ή ακτιβιστών και θέλοντας να κερδίσει την ιδιοκτησία του ονόματος, κατέθεσε μήνυση τον Σεπτέμβριο στο Ανώτατο Δικαστήριο της πολιτείας Los Angeles.

Ο Jonathan Cutler, εκπρόσωπος της εταιρείας eToys είπε ότι κάνουν τα πάντα για να εξασφαλίσουν ασφάλεια στις συναλλαγές τους με τους καταναλωτές, καθώς την εποχή αυτή η κίνηση στο site είναι τεράστια. Τέλος αρνήθηκε να δεχθεί οποιαδήποτε διαπραγμάτευση για το όνομα της εταιρείας.

Τέλος στη διαμάχη θα δώσει ο δικαστής John J. Shook στο Ανώτατο Δικαστήριο στην πολιτεία Los Angeles, στις 29 Νοεμβρίου 2000. Προσωρινά, αποφάσισε να κλείσει το site των καλλιτεχνών το οποίο δεν είναι πλέον προσιτό, δακτυλογραφώντας etoy.com, παρά μόνο με το Internet protocol: <http://146.228.204.72:8880/>. Αυτή η απόφαση πυροδότησε ακόμη περισσότερο την οργή εναντίον της εταιρείας.

## Γ. ΚΡΙΤΙΚΕΣ ΠΑΡΑΤΗΡΗΣΕΙΣ

«Βιώνουμε το ξεκίνημα μιας νέας εποχής. Στα επόμενα 25 χρόνια η ανθρωπότητα θα έχει τη μοναδική ευκαιρία να ζήσει μέσα σ' ένα περιβάλλον οικονομικής ευημερίας και απόλυτης ελευθερίας». Μ' αυτά τα λόγια εκθειάζει τη λειτουργία του Διαδικτύου το περιοδικό «Wired». Κανένας δεν αμφισβητεί το πολύτιμο έργο που επιτελεί το Internet σε όλους τους τομείς της ανθρώπινης δραστηριότητας, όπως επίσης κανένας δεν μπορεί να παραβλέψει και τη «σκοτεινή» πλευρά του. Μία ματιά στις περιπτώσεις παραβιάσεων στο Internet το 1999, και δεδομένου ότι αυξάνονται συνεχώς τα περιστατικά παραβατικής συμπεριφοράς, θα προκαλούσε φόβο σε ένα χρήστη ο οποίος θέλει απλά να περιπλανηθεί στις λεωφόρους του Διαδικτύου, πόσο μάλλον σε κάποιον που σκέφτεται να δραστηριοποιηθεί στο χώρο αυτό.

Ασφαλώς κίνδυνοι υπάρχουν παντού, όμως η γεωγραφία του κυβερνοχώρου μοιάζει να θέτει με διαφορετικό τρόπο τα σύνορα, η πιο σωστά καταργεί τα σύνορα. Ειδικοί απ' όλο τον κόσμο αντιπαραβάλλουν τα δεινά που υπάρχουν ή αναμένεται να υπάρξουν στο Διαδίκτυο και οι αρνητικές κριτικές πληθαίνουν.

Από τις παραπάνω περιπτώσεις, η παιδική πορνογραφία είναι μόνο η κορυφή του παγόβουνου για τα εγκλήματα που συντελούνται στο Διαδίκτυο. Πολλά περιστατικά αφορούν την παράνομη διακίνηση πληροφοριών που σχετίζεται με θέματα: εθνικής ασφάλειας, προστασίας της ανθρώπινης αξιοπρέπειας (υποκίνηση σε φυλετικό μίσος ή φυλετικές διακρίσεις), οικονομικής ασφάλειας (οικονομικές απάτες), ασφάλειας πληροφοριών (hacking), προστασίας της ιδιωτικής ζωής (παράνομη διακίνηση προσωπικών στοιχείων, ηλεκτρονική σεξουαλική παρενόχληση), προστασίας της φήμης (δυσφήμιση, παράνομη συγκριτική διαφήμιση), πνευματικής ιδιοκτησίας (παράνομη διακίνηση κατοχυρωμένων έργων), και τέλος προστασίας ανηλίκων (παραπλανητική διαφήμιση, πορνογραφία, απόπλάνηση, βία). Υπολογίζεται ότι στη Βόρεια Αμερική περισσότερα από 800 παιδιά το χρόνο πέφτουν θύματα κακοποίησης από άτομα που γνωρίζουν on line. Αναρίθμητα είναι τα άτομα και οι επιχειρήσεις που πέφτουν θύματα κάποιου

άλλου είδους παραβατικής συμπεριφοράς ή οικονομικής απάτης, ενώ τα νούμερα αυξάνονται συνεχώς.

Το θαύμα της τεχνολογίας είναι ένα εργαλείο στα χέρια κάθε φανατικού ή διεστραμμένου εγκληματία και κάθε απατεώνα, που τους δίνει τη δυνατότητα να κινούνται ελεύθερα, χωρίς να αφήνουν ίχνη και επιπλέον τους προσφέρει ανωνυμία.

Στοιχειώδεις ανθρώπινα δικαιώματα και αξίες καταπατούνται καθημερινά. Από τις παραπάνω περιπτώσεις βγαίνει το συμπέρασμα ότι πολύ λίγες υποθέσεις φτάνουν στις αίθουσες των δικαστηρίων λόγω της δυσκολίας που υπάρχει στον εντοπισμό των δραστών. Επιπλέον την απόδοση δικαιοσύνης δυσχεραίνει το γεγονός της έλλειψης ενός επαρκούς νομοθετικού πλαισίου, κοινού για όλο τον κόσμο όσον αφορά το Internet. Τέλος η ύπαρξη μεγάλου αριθμού ατόμων που πιστεύουν ότι στον κυβερνοχώρο η πληροφορία πρέπει να είναι ελεύθερη και προσβάσιμη σε όλους, χωρίς την ύπαρξη στεγανών και λογοκρισίας, περιπλέκει ακόμη περισσότερο την κατάσταση.

## ΕΠΙΛΟΓΟΣ

Πριν από μερικά χρόνια μόνο ένας σεναριογράφος επιστημονικής φαντασίας θα μπορούσε να συλλάβει τη δημιουργία και την εξέλιξη ενός χώρου όπως το Internet. Ενός κυβερνοχώρου που προσφέρει εκπληκτικές δυνατότητες επικοινωνίας σε εκατομμύρια ανθρώπους σε όλο τον κόσμο. Η εντυπωσιακή ταχύτητα με την οποία κινούνται οι πληροφορίες στις ηλεκτρονικές σελίδες των δικτύων και στις λεωφόρους των πληροφοριών είναι ένα από τα ποικίλα οφέλη του δικτύου. Τι είναι όμως τελικά το Internet, ο «παράδεισος της επικοινωνίας» ή ένα «ηλεκτρονικό τέρας»; Μήπως τελικά είναι ένα πολύτιμο εργαλείο στα χέρια των παρανόμων; Στον τεράστιο κυβερνοχώρο, ο δρόμος είναι ανοιχτός όχι μόνο γι' αυτούς που εργάζονται, δραστηριοποιούνται οικονομικά, επικοινωνούν, διασκεδάζουν, ανταλλάσσουν, αγαθά και πληροφορίες, αλλά και για τους απατεώνες και τους εγκληματίες. Οποιοσδήποτε θέλει μπορεί να συνδεθεί με το Internet και να μάθει ότι θέλει ή να δραστηριοποιηθεί μέσα σ' αυτό. Οι εγκληματίες και οι απατεώνες γίνονται «αόρατοι» στον κυβερνοχώρο, είναι όμως μία πραγματικότητα. Τα περιστατικά παραβάσεων αυξάνονται συνεχώς και κάνουν το Internet να φαντάζει επικίνδυνο πεδίο, όπου ο χρήστης κινδυνεύει ανά πάσα στιγμή.

Διεθνές δίκαιο για τη ρύθμιση των ποινικών κυρώσεων των αδικημάτων στο δίκτυο δεν υπάρχει. Σχετική ανακοίνωση της Επιτροπής της Ευρωπαϊκής Ένωσης λει τα εξής: «Όλες οι δραστηριότητες εμπίπτουν στη δικαιοδοσία του υπάρχοντος νομικού πλαισίου. Το Internet δεν λειτουργεί σ' ένα νομικό κενό, καθώς όλοι όσοι εμπλέκονται υπόκεινται στους νόμους των κρατών μελών». Αυτό όμως, αποτελεί την αφετηρία του προβλήματος της απόδοσης δικαιοσύνης, αφού ανάμεσα στα κράτη μέλη υπάρχει διαφορετική νομική αντιμετώπιση του ίδιου αδικήματος. Όσον αφορά τις Η.Π.Α., εκεί το πρόβλημα είναι οξύτερο αφού η απονομή δικαιοσύνης γίνεται με βάση τις αποφάσεις ήδη δεδικασμένων υποθέσεων και το παρελθόν του Internet σ' αυτόν το τομέα είναι σχεδόν ανύπαρκτο. Επιπλέον στις ηλεκτρονικές απάτες, θύτες και θύματα δεν γνωρίζονται.



Υπάρχει λύση; Προς το παρόν, οι απόπειρες ελέγχου, δημιουργίας ασφαλών συστημάτων και απονομής δικαιοσύνης δεν έχουν στεφθεί με ιδιαίτερη επιτυχία. Η ανάγκη για διακρατική συνεργασία και ανταλλαγή πληροφοριών στον τομέα αυτό, καθώς και η θέσπιση ενιαίων νομικών κριτηρίων για την αντιμετώπιση των παράνομων δραστηριοτήτων είναι επιτακτική.

Η πληροφορία πρέπει να διακινείται ελεύθερα και το Internet είναι ο θαυμαστός χώρος όπου αυτό γίνεται πραγματικότητα. Θεμελιώδες δικαίωμα αλλά και υποχρέωση του κάθε χρήστη είναι η κριτική στάση απέναντι στις πληροφορίες που υπάρχουν στο Internet. Απόλυτη ασφάλεια δεν υπάρχει ούτε και μαγικές συνταγές για κάποιον που κινείται στο Internet. Υπάρχει, όμως, το πλεονέκτημα της επιλογής που είναι ίσως ο αποτελεσματικότερος τρόπος για την αποφυγή των προβλημάτων.

## ΠΗΓΕΣ

### A. ΒΙΒΛΙΑ

#### A.1. ΕΛΛΗΝΙΚΑ

1. Τσουραμάνης Χρήστος (1996), Οικονομική Παραβατικότητα, Αθήνα, Εκδόσεις «ΕΛΛΗΝ».

#### A.2. ΞΕΝΑ

1. Noel Estabrook, (1997), Μάθετε το Internet σε 24 ώρες, μτφρ. κ. Συρράκος, Αθήνα, Εκδότης Μ. Γκιούρδας.

### B. ΑΡΘΡΑ

#### B.1. ΕΛΛΗΝΙΚΑ

1. «Ασυνήθεις Ύποπτοι», net/T9 Ιούνιος 1997.
2. Buerkle Tom, «Το παγκόσμιο δίκτυο των κυβερνοδιαρρηκτών», ΤΟ ΒΗΜΑ, 22 Μαρτίου 1998.
3. Γαλανόπουλος Κώστας, «Τέλος το απόρρητο», ΤΑ ΝΕΑ, 22 Αυγούστου 1996, σελ. 33.
4. Ε. Ελευθεριάδου, Λ. Σταμάτη, «Η σκοτεινή πλευρά του Internet», ΤΑ ΝΕΑ, 4-5 Μαρτίου 2000, σελ. 74.
5. Ελευθερίου Έλλη, «Α' Διεθνής Πειρατών Κομπιούτερ», ΤΑ ΝΕΑ, 16 Αυγούστου 1997, σελ. 9.
6. Ελευθερίου Έλλη, «Πληθαίνουν οι απατεώνες στο Internet», ΤΑ ΝΕΑ, 15 Σεπτεμβρίου 1997, σελ. 18.
7. Καλκαβούρος Αριστομένης, «Η ΓΗΡΑΙΑ ΗΠΕΙΡΟΣ ΠΑΡΑΜΕΝΕΙ ΕΛΕΥΘΕΡΗ», E-INFO.

8. Σ. Καλλίτση, «Hacks and Cracks», Ο Κόσμος του Internet, Τ19/Ιανουάριος 1997, σελ. 36-40.
9. Α. Κατσούλη, «Ο κυνηγός των χάκερ», ΕΘΝΟΣ ΤΗΣ ΚΥΡΙΑΚΗΣ, 16 Ιανουαρίου 2000, σελ. 63.
10. Α. Κατσούλη, «Το Διαδίκτυο σε ομηρία», ΕΘΝΟΣ ΤΗΣ ΚΥΡΙΑΚΗΣ, 20 Φεβρουαρίου 2000, σελ. 60.
11. Κουράκης Νέστορας, Το Οικονομικό Έγκλημα στην Ελλάδα σήμερα, Ποινική Δικαιοσύνη, Τεύχος 6/Έτος 2000.
12. Μάνδρου Ιωάννα, «Εγκλήματα στο Internet», ΤΟ ΒΗΜΑ, 12 Οκτωβρίου 1997, σελ. 66.
13. Μηλιαρέσης Γρηγόρης, «Πώς έκλεψα την εφορία», ΤΟ ΒΗΜΑ, 28 Μαρτίου 1999, σελ. 19.
14. Μουμούρης Νίκος, «Η σκοτεινή πλευρά του Δικτύου», net/Τ6, Φεβρουάριος 1997, σελ. 30-36.
15. Ντουδεσκέας Γιώργος, «Οι καουμπόη του κυβερνοδιαστήματος», Ταχυδρόμος, Νοέμβριος 2000, σελ. 39-43.
16. Παπαματθαίου Μάρνου, «ΗΙ ΤΕΧΗ ΕΓΚΛΗΜΑΤΑ», ΤΟ ΒΗΜΑ, 12 Δεκεμβρίου 1999, σελ. 20.
17. Α. Πισκιτζή, «Ηλεκτρονικό Έγκλημα», CD.SHOW, Οκτώβριος 1997, σελ. 16-19.
18. Τόμπρας Χ., «Το Αμφιλεγόμενο Internet», RAM, Τ/108, Νοέμβριος 1997, σελ. 73-75.
19. Φακατσέλης Αχιλλέας, «Το μανιφέστο των χάκερ», info-tech, 22 Φεβρουαρίου 2000, σελ. 6-11.
20. Ν. Φραντής, «Χρηματιστηριακές απάτες μέσω Internet», ΤΟ ΒΗΜΑ, 30 Μαΐου 1999, σελ. 18.

## **B.2. ΞΕΝΑ**

1. «CRIME WATCH», PC PRO, Μάιος 1997, σελ. 220-225.
2. «DRIVEN TO CRIME», PC PRO, Ιανουάριος 2000, σελ. 54.

## **Γ. ΙΣΤΟΣΕΛΙΔΕΣ (WEB SITES) ΤΟΥ INTERNET**

1. [www.apbnews.com](http://www.apbnews.com).
2. [www.hack.gr](http://www.hack.gr).

## ΠΑΡΑΡΤΗΜΑ

### Α. ΓΛΩΣΣΑΡΙΟ

**Anti-virus program** (πρόγραμμα anti-virus): Πρόγραμμα που τοποθετείται στον ηλεκτρονικό υπολογιστή για να εμποδίσει τους ιούς να εισέλθουν και να καταστρέψουν το software του ηλεκτρονικού υπολογιστή.

**Domain όνομα:** Το όνομα του δίνεται σε οποιονδήποτε υπολογιστή καταγράφεται ως επίσημος φορέας παροχής πληροφοριών και αρχείων στο World Wide Web. Τα ονόματα domain περιλαμβάνουν συνήθως δύο ή περισσότερα μέρη χωρισμένα μεταξύ τους με τελείες π.χ. τα www.msu.edu.

**E-mail address** (διεύθυνση ηλεκτρονικού ταχυδρομείου): Αποτελείται από ένα όνομα χρήστη ακολουθούμενο από σύμβολο @ και ένα domain όνομα.

**Chat rooms:** Δίκτυο από servers που επιτρέπουν στους χρήστες να επικοινωνούν μεταξύ τους σε πραγματικό χρόνο μέσω του πληκτρολογίου.

**Modem:** Μία συσκευή η οποία επιτρέπει στον υπολογιστή να συνδεθεί με το Internet, να συνομιλεί δηλαδή με άλλους υπολογιστές χρησιμοποιώντας μία τηλεφωνική γραμμή.

**Packet** (πακέτο): Μία ακολουθία ψηφιακών δεδομένων. Κάθε πακέτο δεδομένων το οποίο αποστέλλεται μέσω ενός δικτύου έχει ένα μοναδικό αναγνωριστικό.

**Search engine** (μηχανισμός διεξαγωγής αναζητήσεων): Ένας μηχανισμός διεξαγωγής αναζητήσεων, ένα πρόγραμμα το οποίο ταξινομεί τα στοιχεία μίας βάσης δεδομένων και δίνει στους χρήστες τη δυνατότητα να αναζητήσουν τις πληροφορίες που τους ενδιαφέρουν.

**Server**: Υπολογιστής που παραδίδει πληροφορίες και δεδομένα.

**Software**: Το λογισμικό, τα προγράμματα του υπολογιστή.

**UNIX**: Ένα πολύ ισχυρό λειτουργικό σύστημα, το οποίο αποτελεί τη βασική γλώσσα του Internet.

**Usenet**: Το όνομα της ομάδας χρηστών του UNIX, δηλαδή το δίκτυο χρηστών του UNIX.

**Virus** (ιός): Πρόγραμμα σχεδιασμένο να προκαλέσει βλάβες στο software του υπολογιστή.

**Web site** (ιστοσελίδα): Η αρχική σελίδα μίας συλλογής εγγραφών και άλλες σχετιζόμενες σελίδες, ένα «ηλεκτρονικό βιβλίο».