ΠΑΝΤΕΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΟΙΝΩΝΙΚΩΝ ΚΑΙ ΠΟΛΙΤΙΚΩΝ ΣΠΟΥΔΩΝ
ΤΜΗΜΑ ΚΟΙΝΩΝΙΟΛΟΓΙΑΣ

Ο ΡΟΛΟΣ ΤΗΣ ΤΕΧΝΟΛΟΓΙΑΣ ΣΤΟ ΟΡΓΑΝΩΜΕΝΟ ΟΙΚΟΝΟΜΙΚΟ ΕΓΚΛΗΜΑ ΠΟΥ ΔΙΑΠΡΑΤΤΕΤΑΙ ΣΤΗΝ ΕΥΡΩΠΗ

ΔΗΜΗΤΡΙΟΣ Θ. ΚΑΪΤΣΑΣ

ΔΙΔΑΚΤΟΡΙΚΟ
ΑΘΗΝΑ 2004

Το Βιβλίο αυτό το αφιερώνω στην
Τέση Χατζόγλου

ΕΥΧΑΡΙΣΤΙΕΣ

Θα ήθελα να εκφράσω θερμές ευχαριστίες στον καθηγητή και υπεύθυνο αυτής της διατριβής κ. Α. Μαγγανά για την καθοδήγηση και την διαρκή του υποστήριξη κατά την εκπόνηση της παρούσας διατριβής.

Θεωρώντας πολύ σημαντική την συνεισφορά του καθηγητή κ, Γρ. Λάζου, θα ήθελα ιδιαιτέρως να τον ευχαριστήσω για τις καίριες υποδείξεις και διορθώσεις.

Τέλος, θέλω να ευχαριστήσω την καθηγήτρια κ. Ζαραφωνίτου για την υποστηριξή της και το ενδιαφέρον της κατά την εκπόνηση της παρούσας διατριβής.

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

Περίληψη

Τα εγκλήματα στη σύγχρονη εποχή είναι αρκετά πιο προηγμένα[1] και θανατηφόρα από τις παραδοσιακές κλοπές και ληστείες. Πολλές οργανώσεις ακόμα και χώρες έχουν απειληθεί από αυτούς τους χωρίς προσανατολισμό εγκληματίες που δεν κάνουν τίποτα άλλο παρά να πληκτρολογούν και καταλήγουν να δημιουργούν οικονομική αναστάτωση στα θύματά τους. Οι υπολογιστές και το Διαδίκτυο δίνουν στην κοινωνία τα εργαλεία για να επικοινωνήσουν και να αλληλεπιδράσουν αποτελεσματικότερα και πιο αποδοτικά. Οι εγκληματίες μπορούν να εκμεταλλευτούν αυτά τα εργαλεία για προσωπικό κέρδος, τρομοκρατία, ή άλλη κακόβουλη πρόθεση, πράγμα που καθιστά τις έρευνες για αυτά τα εγκλήματα κρίσιμες.

Το έγκλημα στον υπολογιστή μπορεί να χωριστεί σε δύο κατηγορίες: η πρώτη κατηγορία περιλαμβάνει τα εγκλήματα που έχουν διεξαχθεί μέσω ενός υπολογιστή. Η δεύτερη κατηγορία εστιάζει στα εγκλήματα που ένα συγκεκριμένος υπολογιστής ή ένα σύστημα ηλεκτρονικών υπολογιστών είναι ο στόχος μιας επίθεσης.

Το έγκλημα που διεξάγεται από έναν υπολογιστή συμβαίνει όταν χρησιμοποιείται ο υπολογιστής ως εργαλείο ενίσχυσης της εγκληματικής δραστηριότητας . Αυτό μπορεί να περιλαμβάνει την αποθήκευση των αρχείων της απάτης, την παραγωγή ψεύτικης ταυτότητας, την αναπαραγωγή και τη διανομή του υλικού πνευματικών δικαιωμάτων, τη συλλογή και τη διανομή παιδικής πορνογραφίας, και πολλά άλλα εγκλήματα.

Τα εγκλήματα στα οποία οι υπολογιστές είναι οι στόχοι είναι αντίθετα από τους παραδοσιακούς τύπους εγκλημάτων. Η τεχνολογία έχει καταστήσει δυσκολότερη την απάντηση στο ερώτημα ποιοι, τι, πού, πότε και πώς. Επομένως, σε ένα ηλεκτρονικό ή ψηφιακό περιβάλλον τα στοιχεία συλλέγονται τώρα και αντιμετωπίζονται διαφορετικά από το παρελθόν.

Τα σύγχρονα εγκλήματα έχουν τα χαρακτηριστικά της επιτήδευσης καθώς επίσης και της προσέγγισης του πεδίου δράσης. Το Ομοσπονδιακό Γραφείο Έρευνας του Υπουργείου Δικαιοσύνης των Η.Π.Α έχει καθήκον να δυναμώνει τους ομοσπονδιακούς νόμους που μπορεί να πέσουν στο πεδίο δράσης ενός υπολογιστή ή μιας έρευνας κυβερνητικού εγκλήματος.

Η απάτη στην Ευρώπη έχει αυξηθεί σημαντικά κατά τη διάρκεια των τελευταίων 25 ετών, ειδικά με τη διεύρυνση της Ευρωπαϊκής Ένωσης. Το πραγματικό μέγεθος είναι άγνωστο, και είναι απίθανο να μαθευτεί. Επομένως, όποιες προσπάθειες γίνονται από τα κράτη μέλη για να προσδιορίσουν τα επίπεδα απάτης είναι παραπλανητικές. Η αύξηση της χρήσης των πιστωτικών καρτών έχει ασκήσει τεράστια επίδραση στις μεταβαλλόμενες συνήθειες αγοράς καθώς διευκολύνουν πολύ τους καταναλωτές να χρηματοδοτήσουν τις αγορές. Επίσης μειώνουν τα ποσοστά αποταμίευσης (επειδή οι καταναλωτές δεν χρειάζεται να κρατήσουν χρήματα για μεγαλύτερες αγορές). Οι επιχειρήσεις πετρελαίου, οι κατασκευαστές αυτοκινήτων, και οι λιανοπωλητές έχουν χρησιμοποιήσει επίσης τις κάρτες για να εμπορευτούν τα αγαθά και τις υπηρεσίες τους, χρησιμοποιώντας την πίστωση ως τρόπο ενθάρρυνσης των καταναλωτών για να αγοράσουν. Ανησυχία έχει εκφραστεί για τη διαδεδομένη διανομή των τραπεζικών πιστωτικών καρτών στους καταναλωτές που μπορεί να μην είναι σε θέση να πληρώσουν τους λογαριασμούς, τις δαπανηρές απώλειες και κλοπή των καρτών, τα ανακριβή (και καταστρεπτικά) πιστωτικά αρχεία, τα υψηλά επιτόκια στα απλήρωτα δάνεια και την υπερβολική

[1] Ν. Λίβος,στο βιβ. Ν. Κουράκης.,Το Οργανωμένο Έγκλημα: Φαινομενολογία του προβλήματος και δυνατότητες αντιμετώπισης του στην Ελλάδα. Ποιν.Δικ, 10/1999,σελ 1016.

ενθάρρυνση του καταναλωτικού χρέους η οποία έχει μειώσει την αποταμίευση στις Ηνωμένες Πολιτείες. Οι τεχνολογικές εξελίξεις έχουν διευκολύνει τη χρήση των πιστωτικών καρτών. Οι έμποροι συνδέονται τώρα με τις τράπεζες με το μόντεμ, και έτσι οι αγορές εγκρίνονται γρήγορα. Οι απευθείας αγορές μέσω διαδικτύου είναι δυνατές με την πληρωμή με πιστωτική κάρτα. Οι εταιρίες πιστωτικών καρτών πειραματίζονται επίσης με τις 'έξυπνες κάρτες' που θα ενεργήσουν όπως ένας μικρός υπολογιστής που αποθηκεύει τον λογαριασμό και άλλες πληροφορίες απαραίτητες για τη χρήση της. Όσο περισσότεροι άνθρωποι και ιδρύματα εξαρτώνται[2] από απλούστερα τεχνολογικά ευρήματα όπως οι πιστωτικές κάρτες, μηχανήματα αυτόματης συναλλαγής (ATM), οι μέσω δικτύου και οι σε απευθείας σύνδεση επιχειρησιακές συναλλαγές, τόσο κρισιμότερο γίνεται για την κυβέρνηση και τους προμηθευτές να εξασφαλίσουν ένα υπόβαθρο .

Όλες οι εξελίξεις εστιάζουν τώρα στις πιθανές απειλές που είναι συνημμένες με αυτές. Ένα παράδειγμα είναι το ίδιο το τμήμα του Ηλεκτρονικού εμπορίου. Εάν δεν υπήρχαν οι ανησυχίες για τα ζητήματα ασφάλειας και αποκλειστικότητας που καλύπτουν ολόκληρο το φαινόμενο, δεν θα υπήρχε κανένας λόγος να ακολουθούμε κάποια μορφή παραδοσιακών επιχειρησιακών τεχνικών για να ικανοποιήσουμε τις οικονομικές και συναλλακτικές απαιτήσεις μας. Η Ευρώπη, με πολλές άλλες χώρες, βρίσκεται αντιμέτωπη με ένα δίλημμα: να δημιουργήσουν μια ομάδα εργασίας ή ένα νομικό σύστημα που όχι μόνο καταργεί αυτά τα ζητήματα ασφάλειας αλλά και αποτρέπει κάθε ξένο στοιχείο από τη διατάραξη της αρμονίας που έχει δημιουργήσει στο σύστημά της. Η ολοκληρωτική απουσία 'χάκερ', κλοπής και απάτης είναι σχεδόν σαν όνειρο δεδομένου ότι είναι σαν να ζητάς ένα κόσμο χωρίς έγκλημα. Αλλά όσο δυσκολότερα είναι τα βήματα για τους εγκληματίες και σκληρότερες οι τιμωρίες για τέτοιες δραστηριότητες, τόσο πιο πολύ μειώνονται οι ευκαιρίες να διαπραχθούν τέτοια εγκλήματα.

[2] M.Wasic, Crime and the Computer, Oxford:Claredin Press,1991, σ.12.

ΚΕΦΑΛΑΙΟ 1

Εισαγωγή

1.1.- Δήλωση προβλήματος

Απο τότε που εμφανίστηκαν οι υπολογιστές, πολλοί λένε ότι η τεχνολογία έχει εισβάλει σε όλες τις πτυχές της ζωής μας κάνοντας μας σκλάβους στα τεχνάσματα και τις εντολές της. Αν και αυτή η κρίσιμη άποψη μπορεί να είναι αληθινή, χωρίς αμφιβολία η εύκολη διαβίωση που μας παρέχει η τεχνολογία δεν θα μπορούσε να είναι εφικτή χωρίς μερικές από τις σημαντικότερες εφευρέσεις της εποχής, όπως ο προσωπικός υπολογιστής και οι ασύρματες επικοινωνίες.

Η κατάσταση φαίνεται τέλεια όταν εξετάζεται, όπως παραπάνω, αλλά στην πραγματικότητα τα προβλήματα προκύπτουν, μόλις φανερώνονται η δωροδοκία και το κακό της κοινωνίας που εισβάλουν στην τεχνολογία και δημιουργούν έναν νέο τύπο εγκλήματος, τον κυβερνητικό τύπο. Σε πολλές πτυχές της ανθρώπινης ζωής, όπως στον οικονομικό τομέα που περιλαμβάνει τις πιστωτικές κάρτες, τα ATMs, τις τηλεφωνικές συνδιαλέξεις[3], τις συναλλαγές Διαδικτύου κ.λ.π., αυτός ο όλεθρος ξεσπά, όταν οι εγκληματίες της κυβερνητικής εποχής κινούνται ύπουλα ενάντια σε ολόκληρο το σύστημα και με έξυπνη πληκτρολόγηση ληστεύουν ένα πρόσωπο ή ακόμα και ένα ίδρυμα εκατομμυρίων ECU χωρίς οποιαδήποτε προσωπική επέμβαση αφήνοντας τα θύματα χωρίς ενδείξεις σχετικά με την προέλευση και τη μέθοδο επίθεσης.

Το πρόβλημα είναι ότι αυτοί οι εγκληματίες είναι πολύ προηγμένοι στις μεθόδους εγκλήματός τους, μερικές φορές περισσότερο απ' ό,τι τα θύματά τους, καθώς επίσης και τα αυξανόμενα ποσά που κάθε οργάνωση και χώρα δαπανούν, για να υπερασπίσουν την τεχνολογική υποδομή πράγμα που εκτοξεύει τα γενικά έξοδα στα ύψη. Πολλές χώρες έχουν συμπεριλάβει ακόμη και τις νομικές υπηρεσίες τους, για να κρατήσουν τις ειδικές μονάδες και τη στρατιωτική δύναμη, για να αντιμετωπίσουν αυτούς τους εγκληματίες, καθώς διαφέρουν από τους συνηθισμένους εγκληματίες και πρόκειται να εξεταστούν εντελώς διαφορετικά και από το δικό τους μήκος κύματος. Πολλοί νόμοι έχουν τροποποιηθεί τα τελευταία χρόνια, για να συσσωρεύσουν τους ορισμούς και να θέσουν τα όρια για τους ανθρώπους που διασχίζουν τη γραμμή μεταξύ της ελευθερίας των πληροφοριών και της παραβίασης της ιδιωτικής ζωής και της πειρατείας.

Αυτές οι εγκληματικές δραστηριότητες δεν είναι άγνωστες στην Ευρώπη που έχει υποστεί ισχυρά χτυπήματα τέτοιων ενεργειών. Όσο περισσότερα τεχνολογικά βήματα εγκρίνονται και υιοθετούνται από την κοινωνία, τόσοι περισσότεροι είναι οι κίνδυνοι διαρρήξεων και παραχαράξεων. Οι άνθρωποι οδηγούνται στο νέο πρότυπο αλλά όχι χωρίς τίμημα: το τίμημα μιας μόνιμης απειλής και ενός επισφαλούς μέλλοντος. Όσο περισσότερο εξαρτόμαστε από την τεχνολογία, τόσο δυσκολότερο είναι να δεχθούμε ένα χτύπημα από αυτήν. Αυτή η διατριβή θα αναλύσει όλες τις απειλές, τις πιθανές λύσεις, τα τρέχοντα σενάρια, τις πρόσφατες επιθέσεις και τις λεπτομερείς διαδικασίες τους, όπου αυτό είναι εφαρμόσιμο.

Ένα σημαντικό μέρος αυτών των εγκλημάτων είναι τα εγκλήματα υπολογιστών[4]. Στο Αμερικανικό σενάριο, η ομάδα που αναλαμβάνει αυτά τα εγκλήματα είναι το FBI. Έχει εφαρμόσει διάφορα τεχνικά

---

[3] P.W. Grabosky κ΄ R.G.Smith, Crime in the Digital Age, Annesdale:Transaction, 1998.

[4] ' σε κάθε δώδεκα περιπτώσεις οικονομικού εγκλήματος που χρησιμοποιείται η/υ αναλογεί μόλις μια περίπτωση των άλλων κατηγοριών ', Γρ.Λάζος, Μορφές εγκληματικότητας Ι: Πληροφορική κ΄ έγκλημα, Αθήνα: Πάντειο, 1997.

προγράμματα, για να εντοπίσει την αυξανόμενη πολυπλοκότητα των ερευνών στους υπολογιστές. Ο νομικός ακόλουθος του FBI που τοποθετείται σε 41 χώρες επιτρέπει στο FBI να χρησιμοποιεί περίπλοκες μεθόδους για να ερευνήσει και να συντονίσει τα γεγονότα σε όλο τον κόσμο. Στην Ουάσιγκτον, DC, το εθνικό κέντρο προστασίας υποδομής (NIPC) είναι μια ειδική μονάδα που συντονίζει τις έρευνες εγκλημάτων υπολογιστών στις Ηνωμένες Πολιτείες. Το FBI εκπαιδεύει και πιστοποιεί τους νόμιμους εξεταστές υπολογιστών για κάθε ένα από 56 τμήματα του FBI στις Ηνωμένες Πολιτείες για να ανακτήσει και να συντηρήσει τα ψηφιακά στοιχεία. Το FBI διατηρεί ένα νομικό εργαστήριο υπολογιστών στην Ουάσιγκτον, DC για την προηγμένη αποκατάσταση στοιχείων και για την έρευνα και την ανάπτυξη.

1.2.-Σκοπός της μελέτης

Ο σκοπός αυτής της μελέτης είναι αρκετά απλός. Η πρόσφατη ιστορία των απειλών και τα εγκλήματα που γίνονται μέσω των ηλεκτρονικών μέσων (ή με χρησιμοποίηση οποιασδήποτε μορφής τεχνολογίας για τη διάπραξη μιας απάτης ή ενός εγκλήματος στον οικονομικό τομέα) έχουν αυξηθεί ραγδαία με τον εκσυγχρονισμό των υπολογιστών και παρόμοιων μηχανημάτων. Καμία μορφή τεχνολογίας δεν είναι 100% ασφαλής από τα χέρια των εγκληματιών που έχουν διακριθεί στην υποκρισία ή στην ύπουλη χρήση αυτών των τεχνολογιών και φαίνονται να είναι ένα βήμα μπροστά από τους εφαρμοστές του ίδιου πράγματος. Αυτή η διατριβή θα αναλύσει αυτά τα εγκλήματα λεπτομερώς και θα εστιάσει σε αυτές τις δραστηριότητες στην Ευρώπη.

Τα εγκλήματα αυτού του είδους περιλαμβάνουν την απάτη μέσω πιστωτικών καρτών, τα εγκλήματα στο Διαδίκτυο, τα ATMs και την κακή χρήση τους, τις παραβάσεις πνευματικών δικαιωμάτων και την κλοπή των αριθμών πιστωτικών καρτών, τα εγκλήματα υπολογιστών, την κλοπή πακέτων λογισμικού και υλικού από την Ευρωπαϊκή Ένωση, την παράνομη διανομή πνευματικών δικαιωμάτων, τους 'χάκερ' και τις κοινωνίες τους καθώς επίσης και τον τρόπο που δικαιολογούν τη συμπεριφορά τους. Επιπλέον αυτή η διατριβή θα εξετάσει τις πρακτικές του ξεπλύματος χρημάτων, την κακή χρήση του Διαδικτύου, τις απειλές στο σε απευθείας σύνδεση τραπεζικό σύστημα και τους κινδύνους που δημιουργούνται από τους εγκληματίες στις μεταφορές τραπεζικού λογαριασμού. Επιπλέον, θα συζητήσει λεπτομερώς τις υιοθετημένες πρακτικές και τις τεχνολογίες για την προστασία και θα καταπολεμήσει αυτά τα εγκλήματα υψηλής τεχνολογίας (cyber) και τις προσπάθειες που καταβάλλονται από τα πολιτικά ιδρύματα σε όλο τον κόσμο, όπως η U.N, η Europol, G8 και η Interpol.

Ο σκοπός αυτής της διατριβής δεν είναι απλά να περιγράψει τον πραγματικό τρόπο με τον οποίο αυτά τα εγκλήματα εκδηλώνονται και τις διαδικασίες που τα καταστούν επιτυχή, αλλά να διευκρινίσει το σενάριο στο οποίο αυτά τα εγκλήματα κάνουν όλα τα έθνη θύματά τους. Ένα μέρος της έκθεσης θα ρίξει φως στις διαδικαστικές λεπτομέρειες μερικών δραστηριοτήτων, για να διευκρινίσει το λεπτομερή και μεθοδολογικό τρόπο με τον οποίο αυτά τα εγκλήματα δεν μπορούν να διαπραχθούν από οποιουσδήποτε μη ειδικούς.

Εκτός από όλους αυτούς τους παράγοντες και τις λύσεις τους, οι κίνδυνοι που ακολουθούν τέτοιες δραστηριότητες θα αποδοθούν οπουδήποτε είναι δυνατόν ακολουθούμενα από τα κοινωνιολογικά και εγκληματολογικά επιχειρήματα, όπου είναι εφαρμόσιμα. Δεδομένου ότι αυτά τα εγκλήματα είναι σχετικά νέα, οι νόμοι που δεσμεύουν αυτές τις πράξεις θα συζητηθούν περιληπτικά, για να καταδειχθούν οι νομοθετικές ενέργειες που έχουν ληφθεί, για να μειώσουν αυτές τις δραστηριότητες στο ελάχιστο.

1.3.-Σημασία της μελέτης

Αυτό η διατριβή διαφέρει από τις περισσότερες μορφές γενικής διατριβής, δεδομένου ότι δεν είναι μόνο μια λεπτομερής επισκόπηση των στοιχείων που συγκεντρώνονται, για να παρουσιάσουν μια τάση ή τη σύγκριση αυτής με οποιαδήποτε άλλη, αλλά ένα πραγματικό σενάριο ζωής στο οποίο αλλάζουν οι αριθμοί τόσο γρήγορα όσο αυτό το έγγραφο γράφεται. Αυτές οι εγκληματικές πρακτικές προγραμματίζονται και οργανώνονται από πολλούς εγκεφάλους αυτήν την στιγμή και συγχρόνως λαμβάνονται μέτρα που αυξάνουν την ασφάλεια, αναπτύσσουν τα καλύτερα και ασφαλέστερα προϊόντα και υπηρεσίες και δημιουργούν τις πιο προηγμένες τεχνολογίες για να προστατεύσουν τα τρέχοντα συστήματα και τα τεχνολογικά περιθώρια που έχουν οι δράστες.

Αυτή η διατριβή θα είναι ένα χρήσιμο εργαλείο σε οποιοδήποτε πρόσωπο, οργάνωση, οντότητα ή ακόμα και χώρα που ανησυχεί και προγραμματίζει να μειώσει τις ανησυχίες για την ασφάλεια που αντιμετωπίζει σε αυτούς τους σύγχρονους καιρούς. Τα μέτρα που θα συζητηθούν σε αυτό το έγγραφο είναι εκείνα που οι εμπειρογνώμονες σ' αυτούς τους τεχνολογικούς τομείς προτείνουν και πρέπει να εξεταστούν πριν από την εφαρμογή αυτών των τεχνολογιών ως εναλλαγή στις παραδοσιακές μεθόδους που χειρίζονται τις οικονομικές υποθέσεις.

Για την Ευρώπη, αυτό το έγγραφο θα χρησιμεύσει ως μια λεπτομερής επισκόπηση συνολικής περιγραφής των πρακτικών που παρενοχλούν την δομή της ηπείρου και απειλούν να την αποδυναμώσουν καθημερινά. Οι απώλειες που πολλές χώρες έχουν λόγω τέτοιων επιθέσεων έχουν αυξηθεί σε εκατομμύρια (μόνο για τους οικονομικούς όρους) και δεδομένου ότι όλο και περισσότερες εξαρτήσεις αναπτύσσονται προς αυτές τις τεχνολογίες, αυξάνεται και ο κίνδυνος σε αυτές τις δραστηριότητες.

Είναι πολύ σημαντικό, αυτή τη στιγμή, να υπάρξει μια παγιωμένη έκθεση, όπως αυτή για να λειτουργήσει ως συνταγμένο κέντρο πληροφόρησης που δίνει μια γρήγορη επισκόπηση και μια περιγραφή όλων αυτών των απειλών αλλά και των μέτρων ασφάλειας και των ενεργειών που γίνονται από τις κυβερνήσεις και τις ιδιωτικές οργανώσεις αυτή τη στιγμή καθώς επίσης και για να συνδέσει αυτές με τις πραγματικά απαραίτητες προσπάθειες που θα αναπτύσσονταν σε μια ασφαλή και απαλλαγμένη από εγκλήματα κοινωνία όπου κάθε πολίτης μπορεί να απολαύσει αυτές τις τεχνολογίες χωρίς δικαιολογημένη ανησυχία για τους κινδύνους που απειλούν τη σταθερότητα της οικονομικής του θέσης.

1.3.1-Το πεδίο της απειλής

"Η απάτη συνεχίζει να είναι σημαντικά ανεπτυγμένη στο Ηνωμένο Βασίλειο σήμερα και είναι ένα πρόβλημα που απαιτεί να εξεταστεί κατά τρόπο ρεαλιστικό και εποικοδομητικό. Με το άνοιγμα και τη χαλάρωση των Ευρωπαϊκών συνόρων και τη διαδεδομένη εισαγωγή της νέας τεχνολογίας, η απάτη έχει γίνει ένα καθολικό πρόβλημα και προσφέρει στον απατεώνα ένα ευρύ στάδιο στο οποίο εξασκείται και αναπτύσσει αυτό το επάγγελμα και τις τεχνικές[5]. Καθώς μπαίνουμε στη νέα χιλιετία, το διεθνές οικονομικό αδίκημα συνεχίζει να είναι μια αναπτυγμένη επιχείρηση που προβλέφθηκε από εμάς κατά τη διάρκεια των προηγούμενων δύο δεκαετιών. Με την εμφάνιση του υπολογιστή και της δυνατότητας πρόσβασής του σε όλους, επιχειρηματίες και μαθητές εξίσου, τα διεθνή σύνορα έχουν εξαφανιστεί. Το παγκόσμιο δίκτυο έχει καταστήσει την επικοινωνία στιγμιαία, χωρίς καλώδια, χωρίς έγγραφα και χωρίς ανθρώπινη παρουσία. Το

[5] Society for Risk Analysis-Europe, 1997 Annual Meeting.

Διαδίκτυο έχει γίνει έτσι το εργαλείο του απατεώνα, του ανθρώπου που ξεπλένει χρήματα και του εμπόρου ναρκωτικών. Κατά συνέπεια, εκείνοι που περιλαμβάνονται στο οργανωμένο οικονομικό έγκλημα έχουν γίνει μια μεγαλύτερη απειλή στην παγκόσμια οικονομική σταθερότητα από ποτέ.

1.3.2.-Παγκόσμια παραδείγματα απειλής

Α) Το πεδίο της απειλής είναι μνημειακό. Η πιο πρόσφατη κρίση, η έρευνα για την οποία βρίσκεται σε εξέλιξη, περιλαμβάνει τον ιό ''Love Bug'', ο οποίος φαίνεται να προήρθε από τις Φιλιππίνες και έχει επηρεάσει τους υπολογιστές σε περισσότερες από 20 χώρες. Οι ανταλλαγές αποθεμάτων, οι τράπεζες, οι στρατιωτικές και κυβερνητικές εγκαταστάσεις σε όλο τον κόσμο επηρεάστηκαν και εκατοντάδες εκατομμυρίων δολαρίων, ίσως και δισεκατομμυρίων χάθηκαν. Ο ιός είχε ένα κωδικό πρόσβασης κλοπής προγράμματος, ο σκοπός για τα οποία δεν είναι ακόμα γνωστός, αλλά η δυνατότητα για απάτη είναι προφανής. Ο διάσημος Νιγηριανός παίρνει πολλές γρήγορες επιστολές που ενώ συνήθιζαν να ταχυδρομούνται σε μεγάλες ποσότητες τώρα στέλνονται με φαξ και με το ηλεκτρονικό ταχυδρομείο σε όλο τον κόσμο.

Β) Η `μαύρη οικονομία` της Ρωσίας, αξίας κατ' εκτίμηση 400 δισεκατομμυρίων δολαρίων ετησίως, χρησιμοποιείται για να διαφθείρει ανώτερους υπαλλήλους και ιδρύματα σε όλο τον κόσμο. Τα κεφάλαια μεταφέρονται μέσω δικτύου και ξεπλένονται μέσω μιας μυριάδας αρμοδιοτήτων έως ότου νομιμοποιηθούν. Κατ' εκτίμηση 600 δισεκατομμύρια δολάρια από ναρκωτικά διακινούνται μέσω του διεθνούς οικονομικού συστήματος κάθε έτος και χρησιμοποιούνται για να εξαγοράσουν τις τράπεζες, να διαφθείρουν ανώτερους υπαλλήλους και ακόμη και για να εξαγοράσουν τις κυβερνήσεις. Η απειλή είναι πραγματική και συνεχώς αυξανόμενη . Οι κίνδυνοι για την παγκόσμια πολιτική και οικονομική σταθερότητα είναι μέγιστοι στους τομείς της πολιτικής δωροδοκίας και της δωροδοκίας των χρηματοδοτικών οργανισμών. [6]

1.3.3.-Πανευρωπαϊκή απειλή

Οι απάτες ενάντια στα οικονομικά συμφέροντα της Ευρωπαϊκής Ένωσης είναι μια παραδοσιακή πηγή παράνομων εισπράξεων από την εκμετάλλευση της νομοθεσίας ή από την έλλειψη εσωτερικών ελέγχων. Αυτές οι εγκληματικές δραστηριότητες όχι μόνο πραγματοποιούνται από τους επαγγελματίες στη νόμιμη βιομηχανία στο περιθώριο της επιχείρησής τους αλλά και από τα εκτενή οργανωμένα δίκτυα εγκλήματος, τα οποία, στο Βέλγιο, στις Κάτω Χώρες, Πορτογαλία και Ιταλία, έχουν μεταλλαχθεί σε καλά εδραιωμένες εγκληματικές κοινότητες. Πιστεύεται ότι η πλειοψηφία των παράνομων ενεργειών που δεσμεύονται μέσα στα όρια των συνόρων της ΕΕ στην πραγματικότητα υποκινούνται από τα διεθνή οργανωμένα συνδικάτα εγκλημάτων. Αυτές οι ίδιες ομάδες είναι πιθανώς υπεύθυνες για το πανευρωπαϊκό εμπόριο ναρκωτικών, το λαθρεμπόριο, την κλοπή και το ξέπλυμα χρημάτων.

Η Ελβετία, ένα αξιοσημείωτο παράδειγμα για την οικονομική αξιοπιστία, επικρίνεται σε μια έκθεση του Ευρωπαϊκού Κοινοβουλίου ως πέρασμα διαφθοράς στην ενιαία αγορά της Ευρωπαϊκής Ένωσης. Μέσα στην Ευρωπαϊκή Επιτροπή και την επιχείρηση ναύλωσης, οι ανώτεροι υπάλληλοι έχουν επιβεβαιώσει επίσης το βασικό ρόλο της Ελβετίας στο λαθρεμπόριο τσιγάρων, τα οποία κοστίζουν στις κυβερνήσεις της ΕΕ κατ' εκτίμηση 3.5 δισεκατομμύρια δολάρια ετησίως. Η Μεγάλη Βρετανία υπολογίζεται ότι χάνει 100 εκατομμύρια

---

[6]Saul M. Froomkinm, 2001 Organised Economic Crime: The Risk to World Economic Stability.

δολάρια ετησίως. "Σε 80% των περιπτώσεων απάτης εμπλέκονται Ελβετικές επιχειρήσεις," αναφέρεται από έναν ανώτερο υπάλληλο κατά της εγκληματικότητας της Επιτροπής. Λειτουργούν ως άξονες σε ολόκληρο το δίκτυο. Η Ελβετία είναι ένα πολύ σημαντικό κέντρο σε αυτήν την επιχείρηση. Για τους εγκληματίες είναι ένας ιδανικός κρίκος στην αλυσίδα της απάτης. Η απάτη περιλαμβάνει εμπορευματοκιβώτια αποστολής των τσιγάρων που φθάνουν στην Αμβέρσα από την Αμερική διαμέσου Ελβετίας. Εκεί το φορτίο αγοράζεται για επανεξαγωγή, φαινομενικά έξω από την ΕΕ. Εξαιτίας της ενιαίας αγοράς, τα τσιγάρα δεν υπόκεινται σε έλεγχο έως ότου φθάνουν στον επίσημο προορισμό τους. Το χαοτικό γραφειοκρατικό σύστημα που ρυθμίζει το εμπόριο είναι ανεπαρκές για την παρακολούθηση της μετακίνησης των εμπορευμάτων, ολοκληρώνει η έκθεση. Οι εμπειρογνώμονες στη βιομηχανία λένε ότι η χρήση των σφυρηλατημένων τελωνειακών σφραγίδων είναι διαδεδομένη[7]. Ανώτεροι υπάλληλοι που συμμετέχουν στη σύνταξη της έκθεσης θεωρούν ότι ο ελβετικός σύνδεσμος επιτρέπει στις μεγάλες επιχειρήσεις καπνών να διεισδύσουν στη μαύρη αγορά της Ευρώπης, ενώ παράλληλα παραμένουν σε απόσταση. Στη μέχρι τώρα σύντομη ύπαρξη της η ΕΕ , έχει ήδη αντιμετωπίσει προβλήματα εσωτερικής απάτης και η τεχνολογία βοηθά μόνο να πολλαπλασιαστεί πέρα από το σημείο που η ΕΕ θα ήθελε.

1.4.-Πεδίο της μελέτης

Αυτή η μελέτη εστιάζει στις τρέχουσες εγκληματικές δραστηριότητες καθώς επίσης και στα προηγούμενα γεγονότα που έχουν πραγματοποιηθεί στην Ευρώπη και παραθέτει μερικά παραδείγματα από τις Ηνωμένες Πολιτείες, για να ενδυναμώσουν εκείνα τα παραδείγματα. Το πεδίο δράσης αυτής της διατριβής δεν υπερβαίνει τα γεγονότα και τους αριθμούς που ανακοινώνονται στο κοινό καθώς πολλές οργανώσεις, άτομα και χώρες δεν δημοσιεύουν ή απαριθμούν τέτοιες πράξεις και τις εξετάζουν με μυστικότητα καθώς από τις λεπτομέρειές τους θα διέρρεαν μερικά από τα παραθυράκια της τεχνολογίας τους. Όσον αφορά το δημόσιο τομέα, τα στοιχεία έχουν συγκεντρωθεί από διαφορετικές πηγές και πολλές διαφορετικές απόψεις ενσωματώνονται συμπεριλαμβανομένων των προσωπικών απόψεων του συντάκτη. Έτσι είναι δυνατό ένα μέρος από τη χωρίς αναφορές εργασία να περιέχει κάποια ιδεολογία που είναι αντιφατική ως προς κάποια έγκυρη πεποίθηση ή πρακτική.

Όπως έχει ήδη αναφερθεί η διατριβή αυτή αναφέρεται σε μια ζωντανή εγκληματική δραστηριότητα που ρίχνει τα δίχτυα της στην κοινωνία μας σχεδόν κάθε ημέρα. Έτσι είναι προφανές ότι τα γεγονότα και οι αριθμοί δεν είναι σημερινοί αλλά περιέχουν κάποια στοιχεία που πλέον δεν ισχύουν δεδομένου ότι περιέχουν τις τιμές που δεν υπάρχουν πλέον (έχουν αυξηθεί ή έχουν μειωθεί), όπως το ποσοστό εγκλήματος σε μια πόλη ή μια χώρα ή ο πραγματικός αριθμός απατών που διαπράττονται σε έναν μήνα κ.λπ.... Αν και πολλές προσπάθειες έχουν καταβληθεί, ώστε να μην δοθούν οποιαδήποτε ξεπερασμένα στοιχεία που θα διακινδύνευαν την ακεραιότητα της έκθεσης, σε μερικά στοιχεία θα έπρεπε να αποδοθεί η επιρροή για το σκοπό των τελευταίων παραδειγμάτων.

Αν και οι ορισμοί που δίνονται παρακάτω διευκρινίζουν τους περισσότερους από τους όρους και τις βασικές λέξεις που χρησιμοποιούνται στη διατριβή, μερικές αναλογίες καθώς και επαγγελματική ορολογία ίσως ενσωματωθούν στην έκθεση πράγμα που είναι τεχνικά απαραίτητο, καθώς τα εγκλήματα τέτοιου είδους

---

[7] Financial Crimes: how they effect Europe, 2002 ,a web article at: http://web.ukonline.co.uk/p.mordecai/europe_financial.htm

σχετίζονται τόσο με απλές απάτες όσο και με αρκετά προηγμένα μηχανήματα και διαδικασίες. Μερικές υποθέσεις έχουν γίνει από το συντάκτη προκειμένου να δοθεί σε αυτήν την διατριβή μια επαγγελματική έκβαση δεδομένου ότι, αν στοιχεία μεταφράζονταν με απλούς όρους, θα ήταν απίθανο να σήμαιναν το ίδιο πράγμα μετά από τη μετατροπή.

Το πεδίο αυτής της έκθεσης καλύπτει μόνο την Ευρωπαϊκή ήπειρο και μερικά γεγονότα των ΗΠΑ . Τα ίδια στοιχεία μπορεί να είναι εντελώς διαφορετικά, όταν συγκεντρώνονται από τον υπόλοιπο κόσμο ή από οποιαδήποτε άλλη χώρα αλλά είναι βέβαιο ότι δεν θα έρχονταν σε αντίθεση με οποιαδήποτε άλλη επίσημη πηγή που δίνεται τον ίδιο χρόνο και σε συγκεκριμένη περιοχή. Πολλά εγκλήματα που πραγματοποιήθηκαν στη Μεγάλη Βρετανία, παραδείγματος χάριν, παρατίθενται με την αναφορά της δημοσίευσής τους αλλά περισσότερες πληροφορίες ή μια εν μέρει διαφορετική διατύπωση μπορεί να είναι διαθέσιμη από μια διαφορετική πηγή που δεν εμποδίζει τους στόχους ή την έκβαση αυτής της διατριβής.

1.5.-Αιτιολογία της μελέτης

Ο βρετανικός νόμος είναι ο πρώτος νόμος, εκτός από τις δυνάμεις έκτακτης ανάγκης, ο οποίος απαιτεί κάθε Βρετανός πολίτης (πράγματι οποιοσδήποτε κάτοικος) να αναφέρει στις αρχές όχι μόνο ότι ένα πρόσωπο είναι αναμειγμένο σε ένα έγκλημα αλλά και μια υποψία. Η μη αναφορά είναι ποινικό αδίκημα και το πρόσωπο που δεν το αναφέρει μπορεί, ανάλογα με τις ακριβείς περιστάσεις, να αντιμετωπίσει ποινή φυλάκισης 14 ετών.

Η βρετανική κυβέρνηση επιδεικνύει πόσο σοβαρό θεωρούν αυτό το ζήτημα από το γεγονός ότι οι ποινές δεν φέρνουν καμία απαλλαγή: ένα πρόσωπο που καταδικάζεται σε 14 έτη θα εκτίσει πραγματικά 14 έτη. Σε μερικές περιπτώσεις το να επικαλεστείς άγνοια δεν είναι δικαιολογία και επομένως, είναι σημαντικό οι οργανώσεις και οι υπάλληλοι που είναι σε κίνδυνο να γνωρίζουν τις υποχρεώσεις τους στο πλαίσιο της νομοθεσίας που είναι τώρα σε ισχύ. Αυτό δημιουργεί υποχρεώσεις στις επιχειρήσεις και το προσωπικό τους για να αναφέρουν οποιεσδήποτε υποψίες και όπως αναφέρεται ανωτέρω οι ποινικές ρήτρες μπορεί να είναι αυστηρές για την αθέτηση αυτών των υποχρεώσεων.

Ακριβώς όπως η κυβέρνηση είναι πρόθυμη να αποτρέψει όλα τα εγκλήματα, το ίδιο είναι και οι πολίτες και οι οργανώσεις που επιλέγονται για να είναι θύματα της πρόσφατα υιοθετημένης τεχνολογίας τους. Ο ελλοχεύων λόγος για αυτήν τη διατριβή είναι να παρέχει μια μελέτη που δίνει έμφαση στα εγκλήματα τα οποία μπορεί κάποιος να αναμένει και με τα οποία πρέπει να εξοικειωθεί πριν ασπαστεί μια τεχνολογία όπως η ανάμειξη στο ηλεκτρονικό εμπόριο ή η χρησιμοποίηση των καρτών των ΑΤΜ. Η αρχή που η παρούσα διατριβή ακολουθεί είναι η αρχή της ελευθερίας. Κάθε άτομο έχει ένα δικαίωμα στην ιδιοκτησία του και τα αγαθά του και η κλοπή δεν πρέπει να θεωρείται ως ασήμαντο πρόβλημα στην Ευρώπη. Όλες οι προσπάθειες της κυβέρνησης καθώς επίσης και των επιχειρήσεων ιδιωτικής ασφάλειας παρατίθενται εδώ (οι αναφορές μπορούν να χρησιμοποιηθούν για να έρθουν σε επαφή με τις αρχές) και σε πολλά μέρη της έκθεσης, δίνεται ένα προφητικό βλέμμα στο μέλλον της τεχνολογίας εάν οι όροι παραμένουν οι ίδιοι. Αν και η τεχνολογία λέγεται ότι είναι ο καλύτερος σύμμαχός μας στο σύγχρονο κόσμο, τα οικονομικά αδικήματα που καταστρέφουν αυτό το θαύμα είναι πολύ πιο προκλητικά και προκαλούν προβληματισμό περισσότερο από πότε .

1..6.-Καθορισμός των όρων

Πριν αρχίσει αυτή η διατριβή, όπως ρυθμίζεται από τις απαιτήσεις της διατριβής, μερικοί όροι και λέξεις κλειδιά περιγράφονται κατωτέρω για τη σαφέστερη κατανόηση των εννοιών που χρησιμοποιούνται στη συνέχεια. Μερικοί από αυτούς είναι λέξεις που ακούστηκαν ήδη από τους περισσότερους από μας, αλλά η έννοια μπορεί να φέρει έναν ελαφρώς διαφορετικό τόνο όταν αναφέρεται στο τρέχων θέμα. Αυτοί οι όροι καθορίζονται από τα ηλεκτρονικά λεξικά παγκοσμίως ως ακολούθως, αλλά η σημασία μπορεί να διαφέρει σε μερικές περιπτώσεις λόγω της αλλαγής της διατύπωσης ή της επικαιρότητας του ορισμού· η βασική έννοια όμως παραμένει ίδια.

Οργανωμένο Έγκλημα:

Από εγκληματολογικής απόψεως τέσσερα[8] στοιχεία συναπαρτίζουν την έννοια του οργανωμένου εγκλήματος.

i. η οργάνωση με διαρθρωμένη ιεραρχία, αυστηρή κατανομή καθηκόντων και εσωτερικό κανονισμό επιβολής εξοντωτικών κυρώσεων για όσους αθετούν τους βασικούς κανόνες της οργάνωσης, ii. ο ορθολογικός σχεδιασμός και η σταθερή (ή και αποκλειστική) επιδίωξη μιας αθέμιτης δραστηριότητας που στοχεύει σε μαζική διάπραξη παρανομιών και σε μεγάλα οικονομικά ή άλλα οφέλη, iii. η χρησιμοποίηση βίας ή απειλών για άσκηση βίας προς επίτευξη των σκοπών της οργάνωσης και iv . η ύπαρξη άφθονων οικονομικών μέσων, πολιτικής επιρροής, σύγχρονης τεχνολογίας και νομικού επιτελείου, μέσω των οποίων επιδιώκεται η επίτευξη των αθέμιτων σκοπών.

Ο Ν. Λίβος εύστοχα προσθέτει ό,τι πρόκειται για ποιοτική μεταβολή έναντι της παραδοσιακής εγκληματικότητας, η οποία ανιχνεύεται στην ορθολογική οργάνωση της οικονομικής εκμετάλλευσης παράνομων αγαθών ή υπηρεσιών σύμφωνα με τους κανόνες των σύγχρονων logistics, με επαγγελματισμό, έλλειψη ηθικών αναστολών, χρησιμοποίηση σύγχρονων τεχνολογικά μέσων[9] και διεθνών διασυνδέσεων και κυρίως διά της εξαγοράς συνειδήσεων στον κρατικό μηχανισμό, την τοπική αυτοδιοίκηση και στους διάφορους κοινωνικούς φορείς.

Οικονομική Εγκληματικότητα:

Οικονομική Εγκληματικότητα είναι το σύνολο της αθέμιτης εκείνης δραστηριότητας, η οποία τελείται μέσω των επιχειρήσεων και η οποία έχει ως αποτέλεσμα την προσβολή της καλής λειτουργίας της οικονομίας ή σημαντικών κλάδων και θεσμών της όπως το δημόσιο, τράπεζες και επιχειρήσεις ή πιστωτές ή το καταναλωτικό κοινό[10]. Η οικονομική εγκληματικότητα διακρίνεται απο την οργανωμένη. Αφορά εγκληματικές πράξεις, που τελούνται με την ευκαιρία άσκησης μιας επαγγελματικής δραστηριότητας απ'όπου οι δράστες δεν αποζητούν κατά κύριο λόγο απάτες, και υπεξαιρέσεις αλλά και παραβιάσεις των κανόνων ελεύθερου ανταγωνισμού, οικονομικών κανονισμών, κοινωνικών ρυθμίσεων, και φορολογικών κανόνων[11]. Μεταξύ όμως της οικονομικής εγκληματικότητας και του οργανωμένου εγκλήματος υπάρχει διαπλοκή, αφού είναι δυνατό η

---

[8] Ν. Κουράκης,Το Οργανωμένο Έγκλημα: Φαινομενολογία του προβλήματος και δυνατότητες αντιμετώπισης του στην Ελλάδα. Ποιν.Δικ, 10/1999,σελ 1016.

[9] A.K Cohen 2/1997, n 17 σ. 97 επ.

[10] Ν.Κουράκης, Τα οικονομικά εγκλήματα, Εκδ.Σακκούλα,1998, σ.32-33., κ΄ Ι Μανωλεδάκη, Η τυποποίηση οικονομικών εγκλημάτων σε ειδικούς ποινικούς νόμους και η συρροή τους με αντίστοιχα εγκλήματα,τυποποιημένα στον ποινικό κώδικα (Πανηγυρικός Τόμος Α για τα εικοσάχρονα του Ελληνικού Τμήματος της Διεθνούς Εταιρίας Κοινωνικής Αμύνης, Θεσσαλονίκη,1992,σ.265.

[11] Ι. Φαρσεδάκης, Στοιχεία Εγκληματολογίας, Νομική Βιβλιοθήκη 1996,σ. 43.

πρώτη να εξελιχθεί σε μια εγκληματική επιχείρηση με εφαρμογή σύγχρονων τεχνολογιών, ιδιαίτερα στο πεδίο της πληροφορικής και στις τηλεπικοινωνίες[12].

Ηλεκτρονικό εμπόριο:

Αναφέρεται στη διεύθυνση της επιχείρησης on-line. Αυτό περιλαμβάνει, παραδείγματος χάριν, την αγορά και πώληση προϊόντων με ψηφιακά μετρητά και μέσω της ηλεκτρονικής ανταλλαγής δεδομένων (EDI).

Κρυπτογράφηση:

Η μετάφραση στοιχείων σε έναν μυστικό κώδικα αναφέρεται ως Κρυπτογράφηση. Η Κρυπτογράφηση είναι ο αποτελεσματικότερος τρόπος να επιτευχθεί η ασφάλεια στοιχείων. Για να διαβάσετε ένα κρυπτογραφημένο αρχείο, πρέπει να έχετε πρόσβαση σε ένα μυστικό κλειδί ή έναν κωδικό πρόσβασης που επιτρέπουν σε σας την αποκρυπτογράφηση. Τα μη αποκρυπτογραφημένα κείμενα μπορούν να αναφερθούν ως σαφές κείμενο. Το κρυπτογραφημένο κείμενο αναφέρεται ως κρυπτογραφικό κείμενο. Υπάρχουν δύο κύριοι τύποι κρυπτογραφήσεων: ασύμμετρη κρυπτογράφηση ή κρυπτογράφηση με λέξεις-κλειδιά και η συμμετρική κρυπτογράφηση.

Κωδικός ασφάλειας καρτών:

Τα τελευταία τρία ή τέσσερα ψηφία ενός αριθμού που τυπώνεται επάνω ή ακριβώς κάτω από το πλαίσιο υπογραφής στις κάρτες πληρωμής.

CVM (μέθοδος επαλήθευσης κατόχων κάρτας):

Τα μέσα με τα οποία ο κάτοχος της κάρτας μπορεί να προσδιοριστεί ως γνήσιος, παραδείγματος χάριν μια υπογραφή ή ένας κωδικός (PIN).

Κάρτα 'τσιπ' :

Μια πλαστική κάρτα που περιέχει ένα μικροτσίπ που έχει τις υψηλής ασφάλειας ικανότητες μνήμης και επεξεργασίας, οι οποίες μπορούν να αναγνωριστούν από το χρυσό χρωματισμένο πιάτο επαφών στη πρόσοψη της κάρτας. Οι κάρτες τσιπ είναι επίσης γνωστές ως κάρτες ολοκληρωμένων κυκλωμάτων (ICCs) ή έξυπνες κάρτες.

CIFAS (το Βρετανικό σύστημα αποφυγής απάτης):

'CIFAS' είναι μια ανταλλαγή πληροφοριών που βοηθά το ευρύ φάσμα των μελών οργανώσεων του να προσδιορίζει τους διαφορετικούς τύπους απάτης, συμπεριλαμβανομένης αυτής στις πλαστικές κάρτες.

Πλαστή κάρτα:

Μια κάρτα που έχει τυπωθεί με ανάγλυφα ή με κωδικό, ώστε να θεωρείται νόμιμη κάρτα ή μια κάρτα που έχει εκδοθεί εγκύρως αλλά στη συνέχεια άλλαξε ή επανακωδικοποιήθηκε .

Διασυνοριακή απάτη:

Απάτη που διαπράττεται σε μια πλαστική κάρτα ή με χρησιμοποίηση ενός αριθμού κάρτας σε μια χώρα εκτός από τη χώρα έκδοσης της.

CVC/$l*CVV- κώδικας επαλήθευσης καρτών (MasterCard)/κάρτα επαλήθευσης της αξίας (Visa).

Κρυπτογραφημένη αριθμητική αξία που περιλαμβάνεται στα δεδομένα της μαγνητικής λωρίδας που μπορεί να ελεγχθεί, για να επιβεβαιώσει ότι οι πληροφορίες δεν έχουν αλλάξει από καμιά άποψη[13].

---

[12] Β.Ζησιάδη, Η Οικονομική Εγκληματικότητα: Το Ουσιαστικό και Δικονομικό Οικονομικό Ποινικό Δίκαιο,Εκδ.Σακκούλα, Αθήνα 2001, σ.51.

Πιστωτικές κάρτες:

Μια συσκευή που χρησιμοποιείται, για να εξασφαλίσει την καταναλωτική πίστη κατά την διάρκεια της εξαγοράς ενός αντικειμένου ή μιας υπηρεσίας. Οι πιστωτικές κάρτες μπορούν να εκδοθούν από μια επιχείρηση, όπως ένα πολυκατάστημα ή μια επιχείρηση πετρελαίου, για να διευκολύνουν τους καταναλωτές να αγοράσουν τα προϊόντα τους. Οι πιστωτικές κάρτες επίσης μπορούν να εκδοθούν από τρίτους, όπως μια τράπεζα ή μια οικονομική επιχείρηση , και να χρησιμοποιηθούν από τους καταναλωτές για να αγοράσουν τα αγαθά και τις υπηρεσίες από άλλες επιχειρήσεις. Υπάρχουν δύο τύποι πιστωτικών καρτών: α) οι πιστωτικές κάρτες και β) οι κάρτες χρέωσης.

Α. Οι πιστωτικές κάρτες όπως η Visa και MasterCard επιτρέπουν στον καταναλωτή να πληρώσει ένα μηνιαίο ελάχιστο στις αγορές τους με μια επιβάρυνση στο απλήρωτο ποσό. Οι κάρτες χρέωσης , όπως η American Express, απαιτούν από τον καταναλωτή να πληρώσει για όλες τις αγορές στο τέλος της περιόδου χρέωσης. Οι καταναλωτές μπορούν επίσης να χρησιμοποιήσουν τις τραπεζικές κάρτες για να λάβουν βραχυπρόθεσμα προσωπικά δάνεια συμπεριλαμβανομένων των "προκαταβολών μετρητών" μέσω των αυτοματοποιημένων μηχανών . Οι εκδότες πιστωτικών καρτών λαμβάνουν το εισόδημα από τις αμοιβές που πληρώνονται από τα καταστήματα που δέχονται τις κάρτες τους, από τους καταναλωτές που χρησιμοποιούν τις κάρτες και από τόκους που χρεώνονται στους καταναλωτές .

Η Diners Club , η πρώτη επιχείρηση πιστωτικών καρτών που ιδρύθηκε το 1950, όταν εξέδωσε μια κάρτα επέτρεπε στα μέλη να χρεώσουν τα γεύματα σε 27 εστιατόρια της Νέας Υόρκης. Το 1958, η τράπεζα της Αμερικής εξέδωσε το BankAmericard (τώρα Visa), η πρώτη πιστωτική κάρτα τραπεζών. Το 1965, μόνο 5 εκατομμύρια κάρτες ήταν στην κυκλοφορία. Μέχρι το 1996, οι Αμερικανοί καταναλωτές είχαν σχεδόν 1,4 δισεκατομμύρια κάρτες, τις οποίες χρησιμοποίησαν, για να καταναλώσουν 991 δισεκατομμύρια δολάρια σε αγαθά ετησίως.

Β. Μια εναλλακτική λύση των πιστωτικών καρτών είναι η χρεωστική κάρτα, η οποία χρησιμοποιείται για να αφαιρέσει την τιμή των αγαθών και την υπηρεσία άμεσα από τον τραπεζικό λογαριασμό των πελατών.

Ξάφρισμα:

Η επικρατέστερη μορφή πλαστής απάτης κατά την οποία οι μαγνητικές λεπτομέρειες λωρίδων μιας κάρτας αντιγράφονται ηλεκτρονικά και τίθενται επάνω σε μια άλλη κάρτα.

Τύπος LUHN:

Με βάση το Ansi X4.13, ο τύπος LUHN (επίσης γνωστός ως συντελεστής 10 αλγόριθμος) χρησιμοποιείται για να παράγει να επικυρώσει και να ελέγξει την ακρίβεια των αριθμών πίστωσης καρτών. Οι περισσότερες πιστωτικές κάρτες περιέχουν ένα ψηφίο ελέγχου, το οποίο είναι το ψηφίο στο τέλος του αριθμού πιστωτικών καρτών. Το πρώτο μέρος του αριθμού πίστωσης καρτών προσδιορίζει τον τύπο πιστωτικής κάρτας (Visa, MasterCard, American Express, κ.λπ.), και τα μεσαία ψηφία προσδιορίζουν την τράπεζα και τον πελάτη. Για να παραγάγει το ψηφίο ελέγχου, ο τύπος LUHN εγκαθίσταται στον αριθμό. Για να επικυρώσει τον αριθμό πίστωσης καρτών, το ψηφίο ελέγχου εμφανίζεται στον τύπο.

Ο αλγόριθμος λειτουργεί σε τρία στάδια για την επαλήθευση των πιστωτικών καρτών:

---

[13] APACS Card watch definitions, Prev 4, web article, April 2002 at: http://www.cardwatch.org.uk/html/definitions.html

1) Αρχίζοντας από το δεύτερο προς το τελευταίο ψηφίο και με κίνηση προς αριστερά, αυτό διπλασιάζει την αξία όλων των εναλλασσόμενων ψηφίων.
2) Αρχίζοντας από αριστερά, παίρνουμε όλα τα απρόσβλητα ψηφία και τα προσθέτουμε στα αποτελέσματα όλων των μεμονωμένων ψηφίων από το βήμα 1. Εάν τα αποτελέσματα από τους αριθμούς από το βήμα 1 είναι διψήφιος αριθμός, προσθέτουμε τους δύο αριθμούς πρώτα (δηλ. 18 θα παρήγαγε 1+8). Η εξίσωση θα μοιάσει με ένα κανονικό πρόβλημα πρόσθεσης που προσθέτει κάθε ενιαίο ψηφίο.
3) Το σύνολο από το βήμα 2 πρέπει να τελειώνει σε μηδέν για να ισχύει ο αριθμός της πιστωτικής κάρτας.

Ο τύπος LUHN δημιουργήθηκε προς το τέλος της δεκαετίας του '60 από μια ομάδα μαθηματικών. Σύντομα έκτοτε, οι επιχειρήσεις πιστωτικών καρτών τον υιοθέτησαν. Επειδή ο αλγόριθμος είναι στο δημόσιο τομέα, μπορεί να χρησιμοποιηθεί από καθέναν. Ο τύπος LUHN χρησιμοποιείται επίσης για να ελέγξει την καναδική ισχύ αριθμών κοινωνικής ασφάλειας (SIN). Στην πραγματικότητα, ο τύπος LUHN χρησιμοποιείται ευρέως για να παραγάγει τα ψηφία ελέγχου πολλών διαφορετικών αρχικών αριθμών απολογισμού. Σχεδόν όλα τα ιδρύματα που δημιουργούν και απαιτούν τους μοναδικούς αριθμούς απολογισμού ή αναγνώρισης χρησιμοποιούν το mod 10 αλγόριθμο[14].

Κωδικός πρόσβασης:

Αναφέρεται σε μια μυστική σειρά χαρακτήρων που επιτρέπει σε έναν χρήστη να έχει πρόσβαση σε ένα αρχείο, υπολογιστή, ή ένα πρόγραμμα. Στα πολλών χρηστών συστήματα, κάθε χρήστης πρέπει να πληκτρολογήσει τον προσωπικό κωδικό του/της προτού να αποκριθεί ο υπολογιστής στις εντολές. Ο κωδικός πρόσβασης εξασφαλίζει ότι οι αναρμόδιοι χρήστες δεν έχουν πρόσβαση στον υπολογιστή. Επιπλέον, τα αρχεία στοιχείων και τα προγράμματα μπορούν να απαιτήσουν έναν κωδικό πρόσβασης. Ιδανικά, ο κωδικός πρόσβασης πρέπει να είναι κάτι που κανένας δεν θα μπορούσε να υποθέσει. Στην πράξη, οι περισσότεροι άνθρωποι επιλέγουν έναν κωδικό πρόσβασης που είναι εύκολο να θυμηθούν, όπως το όνομά τους ή τα αρχικά τους. Αυτός είναι ένας λόγος που είναι σχετικά εύκολο να σπάσει στα περισσότερα συστήματα ηλεκτρονικών υπολογιστών[15].

Χάκερ>:

Ένας όρος λαϊκού ιδιώματος για έναν ενθουσιώδη χρήστη υπολογιστών, δηλ., ένα πρόσωπο που απολαμβάνει να μαθαίνει τις γλώσσες προγραμματισμού και τα συστήματα ηλεκτρονικών υπολογιστών και μπορεί συχνά να θεωρηθεί εμπειρογνώμονας στο θέμα. Μεταξύ των επαγγελματιών προγραμματιστών, ανάλογα με το πώς χρησιμοποιείται, ο όρος μπορεί να είναι είτε φιλοφρονητικός είτε μειωτικός, αν και αναπτύσσει μια όλο και περισσότερο μειωτική υποδήλωση. Η μειωτική αίσθηση του <χάκερ> γίνεται πιο εξέχουσα κατά ένα μεγάλο μέρος επειδή ο Τύπος έχει προσδεχτεί τον όρο για να αναφερθεί στα άτομα που κερδίζουν την αναρμόδια πρόσβαση στα συστήματα ηλεκτρονικών υπολογιστών με σκοπό την κλοπή και την αλλοίωση των στοιχείων. Οι <χάκερ>, οι ίδιοι, υποστηρίζουν ότι ο κατάλληλος όρος για τέτοια άτομα είναι <κράκερ>[16].

[14] Tech Glossary 1, at Lycos website at webopedia.lycos.com
[15] Tech Glossary 1 at Lycos website at webopedia.lycos.com
[16] Tech Glossary 1, at Lycos website at webopedia.lycos.com

Πνευματικά δικαιώματα:

Τα πνευματικά δικαιώματα είναι μια μορφή προστασίας που παρέχεται από τους νόμους των Ηνωμένων Πολιτειών[17] στους συντάκτες του "αρχική εργασία του συγγραφικού επαγγέλματος," συμπεριλαμβανομένου λογοτεχνικών, θεατρικών, μουσικών, καλλιτεχνικών, και ορισμένων άλλων διανοητικών εργασιών. Αυτή η προστασία είναι διαθέσιμη και στις δημοσιευμένες και αδημοσίευτες εργασίες. Ο δημιουργός πνευματικών έργων είναι και ιδιοκτήτης των πνευματικών του δικαιωμάτων και του παρέχεται το αποκλειστικό δικαίωμα[18] να επιτρέπει σε άλλους να αναπαράγουν την εργασία σε αντίγραφα, να προετοιμάζουν παράγωγες εργασίες που βασίζονται στην εργασία, να διανέμουν τα αντίγραφα της εργασίας στο κοινό μέσω πώλησης ή άλλης μεταφοράς της ιδιοκτησίας, μέσω ενοικίασης, μίσθωσης ή δανεισμού, να παρουσιάσουν την εργασία δημόσια, στην περίπτωση των λογοτεχνικών, μουσικών, δραματικών και χορογραφικών έργων σε παντομίμες, ταινίες και άλλες οπτικοακουστικές εργασίες ακόμη και εικονογραφημένες, γραφικές ή γλυπτές εργασίες, συμπεριλαμβανομένων των μεμονωμένων εικόνων μιας ταινίας ή άλλης οπτικοακουστικής εργασίας και στην περίπτωση των υγιών καταγραφών, για να εκτελέσει την εργασία δημόσια με τη βοήθεια μιας ψηφιακής ακουστικής μετάδοσης.

Είναι παράνομο για τον καθέναν να παραβιάσει οποιαδήποτε από τα δικαιώματα που παρέχονται από το νόμο πνευματικών δικαιωμάτων στον ιδιοκτήτη των πνευματικών δικαιωμάτων. Αυτά τα δικαιώματα, εντούτοις, δεν είναι απεριόριστα στο πεδίο. Νομικοί περιορισμοί[19] έχουν καθιερωθεί σε αυτά τα δικαιώματα. Σε μερικές περιπτώσεις, αυτοί οι περιορισμοί είναι διευκρινισμένες απαλλαγές από την ευθύνη πνευματικών δικαιωμάτων. Ένας σημαντικός περιορισμός είναι το δόγμα της "δίκαιης χρήσης,"[20] στο οποίο δίνεται μια νομική βάση στην παράγραφο 107 του νόμου πνευματικών δικαιωμάτων του 1976. Σε άλλες περιπτώσεις, ο περιορισμός λαμβάνει τη μορφή μιας "υποχρεωτικής άδειας" κάτω από την οποία ορισμένες περιορισμένες χρήσεις στην εργασία επιτρέπονται με την πληρωμή των διευκρινισμένων δικαιωμάτων και της συμμόρφωσης με τους νομικούς όρους. Για περισσότερες πληροφορίες σχετικά με τους περιορισμούς σ'αυτά τα δικαιώματα, συμβουλευτείτε το νόμο πνευματικών δικαιωμάτων ή γράψτε στο γραφείο πνευματικών δικαιωμάτων.

Ο νόμος πνευματικών δικαιωμάτων και τα πνευματικά δικαιώματα δημιουργήθηκαν στο Ηνωμένο Βασίλειο ως ένας κοινός νόμος, το καταστατικό της Anne 1709. Έγινε καταστατικό με το πέρασμα της κίνησης πνευματικών δικαιωμάτων το 1911. Ο νόμος πνευματικών δικαιωμάτων δίνει τους δημιουργούς των λογοτεχνικών, δραματικών, μουσικών, καλλιτεχνικών έργων, ηχογραφήσεων, ραδιοφωνικών μεταδόσεων, ταινιών και τυπογραφικής ρύθμισης των δημοσιευμένων δικαιωμάτων εκδόσεων να ελεγχθούν οι τρόποι με τους οποίους το υλικό τους μπορεί να χρησιμοποιηθεί. Τα δικαιώματα καλύπτουν: ραδιοφωνική μετάδοση και δημόσια παρουσίαση, αντιγραφή, προσαρμογή, έκδοση, ενοικίαση και δανεισμό στο κοινό. Σε πολλές περιπτώσεις, ο δημιουργός θα έχει επίσης το δικαίωμα να προσδιοριστεί ως συντάκτης και να αντιτεθεί στις διαστρεβλώσεις και τους ακρωτηριασμούς της εργασίας του. Οι διεθνείς συμβάσεις δίνουν την προστασία βρετανικών πνευματικών δικαιωμάτων στις περισσότερες χώρες, υπό τον όρο να υπόκεινται στην εθνική νομοθεσία. Οι τύποι εργασιών για τους οποίους τα πνευματικά δικαιώματα ισχύουν, περιλαμβάνουν τα

---

[17] Άρθρο 17 Αμερικάνικου Κώδικα.
[18] Παρ. 106 Νόμου Πνευματικών Δικαιωμάτων SELF, 1976.
[19] Παρ. 107-121 Νόμου Πνευματικών Δικαιωμάτων SELF, 1976.
[20] CSU-SUNNY-CUNNYJOINT COMMITTEE, Fair Use of Copyrighted Works, 1995, http:// www.fairindex.html.

λογοτεχνικά, τους στίχους τραγουδιών, χειρόγραφα, εγχειρίδια, προγράμματα υπολογιστών, εμπορικά έγγραφα, φυλλάδια, ενημερωτικά δελτία και άρθρα. Οι κανονισμοί προγραμμάτων υπολογιστών το 1992 επέκτειναν τα πνευματικά δικαιώματα των λογοτεχνικών έργων για να περιλάβουν τα προγράμματα υπολογιστών[21].

Μηχάνημα Αυτόματων Συναλλαγών (ΑΤΜ):

Μια συσκευή που χρησιμοποιείται από τους πελάτες τραπεζών για να επεξεργαστούν τις συναλλαγές λογαριασμού. Χαρακτηριστικά, ένας χρήστης παρεμβάλλει στο ΑΤΜ μια ειδική πλαστική κάρτα που κωδικοποιεί τις πληροφορίες μέσω μιας μαγνητικής λωρίδας. Η λουρίδα περιέχει έναν κώδικα προσδιορισμού που διαβιβάζεται στον κεντρικό υπολογιστή της τράπεζας με το διαποδιαμορφωτή. Για να αποτρέψει τις αναρμόδιες συναλλαγές, ένας προσωπικός αριθμός αναγνώρισης (PIN) πρέπει επίσης να εισαχθεί από το χρήστη χρησιμοποιώντας ένα πληκτρολόγιο. Ο υπολογιστής επιτρέπει έπειτα στο ΑΤΜ να ολοκληρώσει τη συναλλαγή. Οι περισσότερες μηχανές μπορούν να διανείμουν τα μετρητά, να δεχτούν τις καταθέσεις, να μεταφέρουν τα κεφάλαια και να παρέχουν τις πληροφορίες για τις κινήσεις λογαριασμού. Οι τράπεζες έχουν διαμορφώσει τα συνεταιριστικά, σε εθνικό επίπεδο δίκτυα έτσι ώστε ένας πελάτης μιας τράπεζας μπορεί να χρησιμοποιήσει το ΑΤΜ άλλης τράπεζας για την απόκτηση μετρητών. Μέχρι το 1997 υπήρξαν περισσότερα από 160.000 ATMs στις Ηνωμένες Πολιτείες. Κάποια ATMs δέχονται επίσης τις πιστωτικές κάρτες για την προώθηση μετρητών. Το πρώτο ΑΤΜ εγκαταστάθηκε το 1969 από τη Χημική τράπεζα στο υποκατάστημα της στο κέντρο του Ρόκβιλ, στη Νέα Υόρκη. Σε ένα πελάτη που χρησιμοποιεί μια κωδικοποιημένκη κάρτα του δίνεται μια συσκευασία που περιέχει ένα καθορισμένο ποσό χρημάτων.

1.7.-Επισκόπηση της μελέτης:

1.7.1.- Πολιτική ανοχή απέναντι στο οργανωμένο έγκλημα.

Το οργανωμένο έγκλημα και η δωροδοκία λέγεται ότι είναι ένας από τους 4 βασικούς τομείς ανησυχίας στην Ευρώπη σήμερα. Υπάρχει διαδεδομένη ανοχή στην περιοχή του οργανωμένου εγκλήματος και της δωροδοκίας. Οι οργανωμένες εγκληματικές επιχειρήσεις συνιστούν την απεικόνιση μιας εγκληματικότητας μεγάλης εμβέλειας, έχουν σχηματιστεί παράλληλα με την κοινωνία, χρησιμοποιώντας σχεδόν τον ίδιο τρόπο λειτουργίας με τους επίσημους θεσμούς του κράτους[22]. Αυτό απεικονίζει και ένα συναίσθημα ανικανότητας μεταξύ των πολιτών, την έλλειψη πολιτικής θέλησης, την πολιτική συνενοχή και την έλλειψη πείρας και μηχανισμών περιφερειακής συνεργασίας για να καταπολεμήσει το οργανωμένο έγκλημα και τη δωροδοκία. Οι εγκληματικές οργανώσεις και οι διεφθαρμένοι ανώτεροι υπάλληλοι θεωρούνται υπεράνω του νόμου. Το χαμηλό ποσοστό δίωξης της δωροδοκίας και των οργανωμένων περιπτώσεων εγκλήματος χρησιμεύει για να ενισχύσει αυτήν την αίσθηση της ανικανότητας. Το οργανωμένο έγκλημα αποτελεί και φυσική και οικονομική απειλή για τους πολίτες. Οι απώλειες στην κανονική οικονομία αυξήθηκαν μέσω του οργανωμένου οικονομικού εγκλήματος στην περιοχή και είναι ουσιαστικές.

Η αστυνομία και οι δυνάμεις δίωξης που δεν είναι οι ίδιοι συνένοχοι συχνά δεν έχουν τους απαραίτητους πόρους[23] για την πάλη ενάντια στο οργανωμένο έγκλημα και τη δωροδοκία. Εκείνοι που

---

[21] Copyright Law: Fact sheet No. P-01 Issue: April 2000 Amended July 2001

[22] Ε.Λαμπροπούλου, Οργανωμένη Εγκληματικότητα κ΄ εσωτερική (αν-) ασφάλεια, Ποιν.Δικ., 8-9/2000,σ. 881.

[23] Ν.Κουράκης, Τα οικονομικά εγκλήματα,Εκδ.Σακκούλα,1998,σ.88-89.

περιλαμβάνονται στο οργανωμένο έγκλημα ωφελούνται από τους πόρους και από ένα δίκτυο διασυνοριακών συνδέσεων, ενώ εκείνοι που χρεώνονται την επιβολή του νόμου, όχι. Τα περιφερειακά δίκτυα για να καταπολεμήσουν το διασυνοριακό οργανωμένο έγκλημα και τη δωροδοκία είναι αδύνατα ή απόντα. Το πεδίο των αρμοδιοτήτων των διεθνών αντιπροσωπειών επιβολής του νόμου και των τελωνίων είναι περιορισμένο.

1.7.2.- Μέθοδοι αντιμετώπισης της ανοχής

Αυτή η διατριβή συστήνει ποικίλες μεθόδους που πρέπει να χρησιμοποιηθούν για να ενισχύσουν τη διαφάνεια και την εγκυρότητα. Ένας τρόπος θα ήταν να εκπαιδευθούν οι δημοσιογράφοι για να ερευνήσουν καλύτερα τις ιστορίες του οργανωμένου εγκλήματος και της δωροδοκίας και των πηγών τους. Άλλος τρόπος είναι να συλλεχθούν και να δημοσιευθούν οι πληροφορίες για να καταστούν οι πολίτες πιο ενήμεροι για τις οικονομικές και κοινωνικές απώλειες λόγω του οργανωμένου εγκλήματος καθώς διατριβές όπως αυτή δημοσιοποιούνται και η δημόσια ευαισθητοποίηση αυξάνεται. Περιφερειακοί οργανισμοί πρέπει να δημιουργηθούν για να πολεμήσουν τη δωροδοκία και το οργανωμένο έγκλημα με τις συνδέσεις με τους οργανισμούς στην Ευρωπαϊκή Ένωση. Σε αυτούς τους οργανισμούς πρέπει να δοθούν ισχυρές δυνάμεις για να ενεργήσουν ενάντια στους εγκληματίες.

Επιθυμία του συντάκτη είναι να δοθεί έμφαση στα συγκεκριμένα εγκλήματα που αντιμετωπίζουμε και μας ληστεύουν τα εισοδήματά μας, να συζητηθούν λεπτομερώς οι διαδικασίες τους, τα βιογραφικά στοιχεία του εγκληματία και οποιαδήποτε άλλη σχετική με εκείνα τα εγκλήματα θεωρία.

Αυτή η διατριβή θα διευκρινίσει επίσης πολλά εγκλήματα που θεωρούνται πολύ υψηλού κινδύνου αλλά και σπάνιες περιπτ΄σεις και θα συζητήσει εάν οι προηγούμενες κυβερνητικές προσπάθειες στην Ευρωπαϊκή περιοχή έχουν διαδραματίσει έναν σημαντικό ρόλο στην πρόληψη ή στην επιβράδυνση του ρυθμού αυτών των εγκληματικών δραστηριοτήτων.

Κεφάλαιο ΙΙ

2.1.- Βιβλιογραφική επισκόπηση

Η διατριβή άρχισε με μια σαφή εννοιολογική άποψη της συγκέντρωσης των στοιχείων από τις πηγές που δεν έχουν χρησιμοποιήσει τα στοιχεία για οποιαδήποτε δημιουργία μελέτης μέχρι τώρα, αλλά έχουν γίνει ήδη μερικές έρευνες στις μικρό-περιοχές, σχετικές με αυτήν την έκθεση, που αξίζουν. Εκτός από εκείνες τις εργασίες, τα δελτία ειδήσεων και τα αρχεία των νομικών εγγράφων παρουσιάζουν μια σειρά παρόμοιων ερευνών και μελετών που εστιάζουν είτε στη γενικευμένη είτε στη συγκεκριμένη μορφή αυτών των εγκλημάτων.

Οι εγκληματικές δραστηριότητες που περιγράφηκαν από πολλές εγκυκλοπαίδειες σε απευθείας σύνδεση ή ενημερωτικά λήφθηκαν ως κύριος ορισμός και οι διαδικασίες τους που περιγράφηκαν από τις πηγές που ήταν όχι μόνο γνήσιες και αρχικές αλλά και δεν έρχονταν σε αντίθεση με παρόμοιες εργασίες έγιναν αποδεκτές. Αυτό το κεφάλαιο χωρίζεται σε πολλές υποενότητες, που εστιάζουν σε ένα διαφορετικό κάθε φορά οικονομικό αδίκημα και τις προσπάθειες λύσης του. Η συνοδευτική βιβλιογραφική αναθεώρηση του ίδιου πράγματος ακολουθεί κάθε τμήμα και αποδεικνύεται επίσης πρωτότυπη ή όχι.

2.2.- Συνεισφορά άλλων επιστημών στην εγκληματολογία

Η εγκληματολογία αφορά παραδοσιακά τα εγκλήματα ενάντια στην ιδιοκτησία και το πρόσωπο, την παρεκκλίνουσα συμπεριφορά, και τη μεταχείριση των παραβατών. Οι κύριοι τομείς της έρευνας είναι το ποινικό δίκαιο, η ψυχιατρική, η ψυχολογία και η κοινωνιολογία. Εντούτοις, οι πρόσφατες εξελίξεις στα επιχειρησιακά εγκλήματα, όπως τα περιβαλλοντικά εγκλήματα, η φορολογική διαφυγή, και το έγκλημα σχετικά με τις νέες τεχνολογίες πληροφοριών απαιτούν τη συνεισφορά από άλλες επιστήμες. Οι προφανείς επιστήμες είναι η επιχειρησιακή διοίκηση, τα οικονομικά και η τεχνολογία πληροφοριών. Επιπλέον, η παγκοσμιοποίηση της επιχείρησης και των σχετικών εγκλημάτων μειώνει τη δύναμη ελέγχου και φορολογίας από το εθνικό κράτος. Πράγματι, η κυκλοφορία των ατόμων και του κεφαλαίου σε συνδυασμό με τα νέα εγκλήματα στην παγκόσμια επιχειρησιακή κοινότητα μπορούν, στο τέλος, να απειλήσουν το σύγχρονο κράτος κοινωνικής πρόνοιας που στηρίζεται στη φορολογία. Η έρευνα στην ηθική, το νόμο, την ιστορία και την πολιτική επιστήμη, παραδείγματος χάριν, πρέπει επίσης να συνεισφέρει σημαντικά[24].

2.3.- Τάσεις εγκληματικής δραστηριότητας

Το έγκλημα είναι ένα μεταβαλλόμενο φαινόμενο. Μερικές δραστηριότητες που στο παρελθόν θεωρούνταν σοβαρά απειλητικές στο κοινωνικό χώρο είναι τώρα περιέργως αρχαΐζουσες. Η ληστεία στις εθνικές οδούς είναι στο προσκήνιο. Άλλες δραστηριότητες, όπως η εγκληματική εκμετάλλευση του σε απευθείας σύνδεση εμπορίου, που ήταν ασύλληπτες μια δεκαετία πριν, θέτουν τώρα σημαντικούς κινδύνους για την οικονομία και την κοινωνία της Αυστραλίας. Η απάτη είναι ένας γενικός τύπος εγκλήματος που, αν και είναι τόσο παλιό όσο το εμπόριο, μπορεί να λάβει νέες μορφές στο 21ο αιώνα. Σε μερικές περιπτώσεις, αυτές οι μορφές έχουν αρχίσει ήδη να προκύπτουν.

Οι Τάσεις και τα Ζητήματα περιγράφουν διάφορες κοινωνικές, δημογραφικές και οικονομικές εξελίξεις που μπορούν να αναμένονται για να επηρεάσουν τη μορφή της απάτης στα επόμενα έτη. Κάποιος

---

[24] Call for Papers: Research into Economic Crime, 2001

γρήγορα σημειώνει ότι αυτές οι τάσεις, και η ποικιλία της απάτης που μπορούν να αναμένονται για να τους συνοδεύουν, είναι πέρα από την ικανότητα ελέγχου των αντιπροσωπειών επιβολής νόμου .Ένα μεταγενέστερο έγγραφο Τάσεων και Ζητημάτων θα συζητήσει τα μέσα με τα οποία τα ιδρύματα και οι πηγές έξω από το ποινικό δικαστικό σύστημα μπορούν να χρησιμοποιηθούν για την επιβολή του νόμου. Η παγκοσμιοποίηση ενισχύεται από την τεχνολογία, η οποία στη συνέχεια διευκολύνει τόσες πολλές άλλες πτυχές της σύγχρονης ζωής. Οι δραματικές αλλαγές στην ικανότητα και τη δυνατότητα πρόσβασης των νέων τεχνολογιών έχουν αλλάξει τον τρόπο που γεννιόμαστε, τον τρόπο που ζούμε, και τον τρόπο που πεθαίνουμε. Ο συναρπαστικός ρυθμός των τεχνολογικών αλλαγών, ίσως εμφανέστερος στη σύγκλιση των υπολογιστών και των επικοινωνιών, μας έχει οδηγήσει στην αυγή μιας νέας εποχής. Στη βασίλειο της απάτης, η επέκταση της "βασικής εκπαίδευσης υπολογιστών" θα αυξήσει τον αριθμό ενδεχόμενων παραβατών, ενώ οι νέες τεχνολογίες επιτρέπουν την ευκολότερη και φτηνότερη πρόσβαση σε μια πολύ μεγαλύτερη ομάδα ενδεχόμενων θυμάτων.

Ο αριθμός ανθρώπων που πλήρωσαν για τα αγαθά και τις υπηρεσίες δίνοντας στοιχεία πιστωτικών καρτών μέσω δικτύου, εντούτοις, ελαττώθηκε από 80,5% (279.000 αγοραστές Διαδικτύου) τους δώδεκα μήνες μέχρι τον Νοέμβριο του 1998 σε 77% (502.810 αγοραστές Διαδικτύου) τους δώδεκα μήνες μέχρι τον Νοέμβριο του 1999. Τους δώδεκα μήνες μέχρι τον Φεβρουάριο του 2000 ,74% (547.600 αγοραστές Διαδικτύου) που πλήρωσαν για το σύνολο ή μέρος της αγοράς τους δίνοντας στοιχεία των πιστωτικών καρτών τους μέσω δικτύου . Αυτή η μείωση είναι ίσως ενδεικτική της ανησυχίας που υπάρχει στην κοινότητα σχετικά με την ασφάλεια των σε απευθείας σύνδεση μηχανισμών πληρωμής. Αν και μερικοί καταναλωτές μπορεί να είναι απρόθυμοι να χρησιμοποιήσουν τις νέες τεχνολογίες από φόβο να γίνουν θύματα, η επέκταση του ηλεκτρονικού και κινητού εμπορίου δεν μπορεί να διακοπεί, ιδιαίτερα για τις δραστηριότητες επιχειρήσεων και κυβέρνησης. Η έρευνα «Forrester», παραδείγματος χάριν, έχει υπολογίσει ότι το παγκόσμιο ενδοεπιχειρησιακό ηλεκτρονικό εμπόριο θα αξίζει 2,7 τρισεκατομμύρια δολάρια μέχρι το 2004 ενώ η ομάδα «Gartner» ισχυρίζεται ότι θα αξίζει περίπου 7 τρισεκατομμύρια δολάρια[25].

2.4.-Νέος εγκληματολογικός κώδικας

Για πρώτη φορά ο St Lucia θα εισαγάγει τη νέα νομοθεσία επιτρέποντας τη δίωξη των εγκλημάτων που περιλαμβάνουν τον κακό χειρισμό των ηλεκτρονικών στοιχείων όπως η απάτη μέσω πιστωτικών καρτών. Ο νέος εγκληματικός κώδικας θα θεσπίζεται μέχρι το Μάρτιο του 2004.

Ο νέος εγκληματικός κώδικας που συντάσσεται από το Γραφείο του Γενικού Εισαγγελέα ακολουθεί εκτενείς διαβουλεύσεις με τους βασικούς συμμέτοχους μέσα στο ποινικό δικαστικό σύστημα της St Lucia. Οι αντιπρόσωποι από τα γραφεία του Διευθυντή Δημόσιων Διώξεων, του Αρχηγού της αστυνομίας, των Δικαστών και της ένωσης Δικηγόρων ήταν μεταξύ εκείνων που συμμετέχουν στη συμβουλευτική διαδικασία.

Ο διευθυντής Δημοσίων Διώξεων, Norton Jack λέει ότι ο προτεινόμενος εγκληματικός κώδικας επαρκέστερα και πιο ρεαλιστικά θα προσδιορίσει, θα διώξει ποινικώς και θα τιμωρήσει τα εγκλήματα στη σύγχρονη κοινωνία μας. Ο κ. Jack προσθέτει, ο γρήγορος ρυθμός με τον οποίο οι εγκληματίες αλλάζουν τις μεθόδους που διαπράττουν εγκλήματα απαιτεί επαγρύπνηση και αναθεώρηση του εγκληματικού κώδικα. Ο

---

[25] O'Brien, Chris 2000, 'The Next Revolution?' The Age (Melbourne), I.T. (2), 27 June 2000.

νέος εγκληματικός κώδικας θα εξετάσει επίσης τις ανωμαλίες σχετικά με την καταδίκη των προσώπων που καταδικάζονται για σεξουαλική παρενόχληση, και θα διευκρινίσει τις εγκληματικές διαδικασίες όπου ο παλαιός εγκληματικός κώδικας ήταν σιωπηλός ή ασαφής[26].

2.5.-Ηλεκτρονικό Εμπόριο

Αυτή τη στιγμή, τα βιβλία, τα περιοδικά και ο εξοπλισμός λογισμικού υπολογιστών είναι οι πιο κοινοί τύποι προϊόντων που αγοράζονται από το Διαδίκτυο. Η πιθανότητα υπάρχει, εντούτοις, για ο,τιδήποτε αγοράζεται ηλεκτρονικά και πρόσφατα διάφορες υψηλής αξίας συναλλαγών έχουν διεξαχθεί ηλεκτρονικά από αγοραστές που αγοράζουν πακέτα διακοπών, αυτοκίνητα ακόμη και σπίτια μέσω δικτύου. Έχουμε δει επίσης την καθιέρωση διάφορων σε απευθείας σύνδεση δημοπρασιών σπιτιών και τη χρήση του Διαδικτύου για την σε απευθείας σύνδεση πώληση μετοχών και για τζόγο, κάθε ένα από τα οποία συνεπάγεται μεγάλα χρηματικά ποσά. Οι πιθανές απώλειες λόγω της σε απευθείας σύνδεση απάτης θα μπορούσαν, επομένως, να είναι σημαντικές[27].

Δεδομένου ότι το ηλεκτρονικό εμπόριο συνεχίζει να επεκτείνεται από την άποψη της ποικιλίας των προϊόντων και των υπηρεσιών που προσφέρει για πώληση σε απευθείας σύνδεση, και καθώς ο αριθμός χρηστών συνεχίζει να αυξάνεται, οι ευκαιρίες για την απιστία και την απάτη έχουν αυξηθεί. Μια παγκόσμια λειτουργία καθαρισμού, που περιλαμβάνει το Γραφείο Δίκαιων Εμπορικών Συναλλαγών στη Μεγάλη Βρετανία και τα παραρτήματά της σε είκοσι δύο άλλες χώρες, προσδιόρισε 1.159, "Γίνε γρήγορα πλούσιος'', σχέδια που διαφημίζονται στους χώρους του Διαδικτύου[28].Στις Ηνωμένες Πολιτείες, πάνω από 18.600 καταγγελίες καταχωρήθηκαν στην βάση δεδομένων της ομοσπονδιακής Επιτροπής απάτης του Εμπορίου το 1999, ο διπλάσιος αριθμός το 1998 —ενώ καταχωρήθηκαν 8.000[29]. Σε μια τηλεφωνική έρευνα για 1.006 σε απευθείας σύνδεση καταναλωτές που πραγματοποιήθηκε για εθνική καταναλωτική ένωση στις Ηνωμένες Πολιτείες μεταξύ του Απριλίου και του Μαΐου του 1999, 24% είπαν ότι είχαν αγοράσει τα αγαθά και τις υπηρεσίες σε απευθείας σύνδεση. Επτά τοις εκατό, που αντιπροσωπεύει έξι εκατομμύρια ανθρώπους, εντούτοις, είπαν ότι είχαν δοκιμάσει την απάτη ή την αναρμόδια χρήση της πιστωτικής κάρτας ή των προσωπικών πληροφοριών σε απευθείας σύνδεση[30]. Ένας άλλος σχολιαστής έχει υπολογίσει ότι τουλάχιστον δέκα τοις εκατό του σε απευθείας σύνδεση εμπορίου μπορούν να περιλαμβάνουν την καταναλωτική απάτη[31]. Το 1999, μια έρευνα πραγματοποιήθηκε στο πανεπιστήμιο του Utah του τμήματος Εμπορικών Συναλλαγών Διαδικτύου που συντονίστηκε από τη διεθνή ένωση καταναλωτών και χρηματοδοτήθηκε από την Ευρωπαϊκή Ένωση. Οι εκπρόσωποι εκείνων των ομάδων αγόρασαν περισσότερα από 150 προϊόντα από τους ιστοχώρους που βρίσκονται σε δεκαεπτά χώρες, και προσπάθησαν έπειτα να τα επιστρέψουν. Διαπιστώθηκε ότι οκτώ τοις εκατό των στοιχείων που παρήγγειλαν δεν έφθασαν ποτέ, πολλοί ιστοχώροι δεν έδωσαν σαφείς πληροφορίες

---

[26] St. Lucia fraud detection, 2002, on the web at:
http://www.stlucia.gov.lc/pr2002/new_legislation_to_address_electronic_fraud.htm

[27] Confronting Fraud in the Digital Age, Dr Russell G. Smith Australian Institute of Criminology, August 2000.

[28] Office of Fair Trading, 1998.

[29] United States, Department of Justice 2000, *Internet Fraud: Appendix B*, Report of the Criminal Division's Computer Crime and Intellectual Property Section, on the web at:
http://www.cybercrime.gov/append.htm (visited 5 July 2000).

[30] Louis Harris & Associates Inc. 1999, Consumers and the 21st Century: A Survey Conducted for the National Consumers League, Louis Harris & Associates Inc, New York.

[31] Rothchild 1999, σ. 897, ν. 11.

για τις δαπάνες παράδοσης, ένα μικρό ποσοστό αμφισβήτησε εάν οι νόμοι της χώρας του πωλητή ή της χώρας του αγοραστή θα ίσχυαν σε περίπτωση διαφωνίας και μόνο πενήντα τρία τοις εκατό είχαν μια επιστροφή. Επιπλέον, μόνο περίπου δεκατρία τοις εκατό των περιοχών υποσχέθηκαν να μην αποκαλύψουν τα προσωπικά στοιχεία των πελατών σε έναν τρίτο και μόνο τριάντα δύο τοις εκατό παρείχαν τις πληροφορίες για το πώς να παραπονεθούν, εάν υπάρξει ένα πρόβλημα με μια συναλλαγή[32].

2.6.- Οι μηχανικοί της ηλεκτρονικής απάτης

Οι εμπορικές συναλλαγές μπορούν να πραγματοποιηθούν με μια ευρεία ποικιλία ηλεκτρονικών τρόπων και κάθε ένα από τα διάφορα συστήματα πληρωμής έχει γίνει στόχος των απατεώνων. Επιπλέον, η παραποίηση ταυτότητας κάποιου αποτελεί συχνά τον πυρήνα της ηλεκτρονικής απάτης.

2.6.1.-Απάτη μέσω έγγραφων συστημάτων πληρωμής

Όπου τα αγαθά και οι υπηρεσίες αποκτούνται σε ανοικτή γραμμή και πληρώνονται με χρήματα ή επιταγές, η απάτη μπορεί να διαπραχθεί με τους ίδιους τρόπους όπως εκείνοι που έχουν λειτουργήσει στο παρελθόν όπου αυτά τα συστήματα πληρωμής έχουν χρησιμοποιηθεί. Τα τρωτά σημεία αφορούν κυρίως τα άτομα που χρησιμοποιούν τους λογαριασμούς που έχουν ανοίξει μέσω της χρήσης των ψεύτικων στοιχείων ταυτότητας, υπερβαίνουν την πιστωτική ισορροπία που κρατιέται στους λογαριασμούς επιταγών, ή πλαστογραφούν ή αλλάζουν τα όργανα οι ίδιοι. Επειδή υπάρχει πίεση οι ηλεκτρονικές συναλλαγές να πραγματοποιούνται γρήγορα, οι έμποροι μπορούν να είναι λιγότερο πρόθυμοι να περιμένουν τις επιταγές που εξαργυρώνονται ή τους ελέγχους επικύρωσης που πραγματοποιούνται πριν από την έγκριση της αποστολής των αγαθών ή της παροχής υπηρεσιών, αφήνοντας τους κατά συνέπεια ανοικτούς στην απάτη. Ομοίως, οι καταναλωτές μπορούν να στείλουν μια επιταγή σε έναν έμπορο που δεν έχουν καμία πληροφορία αν μπορεί να βρεθεί σε μια ξένη χώρα, να λάβει την πληρωμή, και να προκαθορίσει τη συμφωνία.

2.6.2.-Απάτη που περιλαμβάνει άμεσα συστήματα χρεώσεων

Εκτός από τις συναλλαγές σε χαρτί, οι σε απευθείας σύνδεση πληρωμές θα μπορούσαν να γίνουν μέσω της άμεσης χρέωσης, στην οποία η αξία μεταφέρεται άμεσα από τον λογαριασμό του πληρωτή στην τράπεζα του παραλήπτη, ή μέσω της λογιστικής μεταφοράς στην οποία ένας πληρωτής συμβουλεύει την τράπεζά του/της για να χρεώσει τον λογαριασμό του/της με ένα ποσό που πιστώνεται ηλεκτρονικά σε έναν άλλο λογαριασμό. Αυτές είναι ουσιαστικά 'συναλλαγές χωρίς την παρουσία καρτών' που λειτουργούν με τον ίδιο τρόπο με οποιαδήποτε τηλεφωνική συναλλαγή ή μέσω ταχυδρομείου βασισμένες σε έναν λογαριασμό πιστωτικής κάρτας.

Για να πραγματοποιηθούν τέτοιες μεταφορές, πρέπει να ληφθούν τα προκαταρκτικά μέτρα από τα ενδιαφερόμενα μέρη που περιλαμβάνουν την ανταλλαγή στοιχείων λογαριασμού και τη διεξαγωγή διάφορων ελέγχων ταυτότητας. Από την άποψη του αγοραστή, ένα στοιχείο του κινδύνου προκύπτει εάν τα κεφάλαια μεταφέρονται προτού να φθάσουν τα αγαθά ή παρέχεται η υπηρεσία. Από την άποψη του εμπόρου, είναι

---

[32] Clausing, J. 1999, 'FTC Holds Meeting on International E-Commerce', *New York Times*, June 8.

απαραίτητο τα κεφάλαια να φθάσουν προτού να αποσταλούν τα αγαθά ή η παρεχόμενη υπηρεσία . Η κύρια προστασία ενάντια σε τέτοια απάτη περιλαμβάνει τη λήψη επαρκών μέτρων από τους εμπόρους για να επικυρώσουν τις λεπτομέρειες λογαριασμού που παρέχονται από τον αγοραστή και για να εξασφαλίσουν ότι τα επαρκή κεφάλαια υπάρχουν στον λογαριασμό για να καλύψουν την αγορά. Η λήψη της έγκρισης από έναν χρηματοδοτικό οργανισμό είναι το πρώτο βήμα στην πρόληψη απάτης και μερικές τράπεζες τώρα προσφέρουν χρονική έγκριση για τις συναλλαγές πέρα από τα διευκρινισμένα όρια .

2.6.3. Απάτη που περιλαμβάνει τα Ηλεκτρονικά Συστήματα Μεταφοράς Κεφαλαίων

Διάφορα συστήματα αναπτύσσονται για να επιτρέψουν στους πελάτες, τις τράπεζες, και τους εμπόρους για να επικοινωνήσουν ασφαλώς ο ένας με τον άλλον. Διάφορα ηλεκτρονικά συστήματα μεταφοράς κεφαλαίων λειτουργούν ήδη σε όλο τον κόσμο ως υποκατάστατα των σε χαρτί συναλλαγών με επιταγές και αυτά θα μπορούσαν καλά να προσαρμοστούν για τη χρήση Διαδικτύου. Το σύστημα 'Giro'του Ηνωμένου Βασιλείου, παραδείγματος χάριν, έχει ωφελήσει στην παρεμπόδιση της απάτης μέσω επιταγών επειδή η διαταγή πληρωμής κατευθύνεται στον τραπεζίτη άμεσα παρά μέσω του δικαιούχου πληρωμής. Στο 'GIRO' σύστημα, το πρόσωπο επιθυμεί να κάνει μια πληρωμή, ο πληρωτής, καθοδηγεί την τράπεζά του /της σχετικά με τις λεπτομέρειες της πληρωμής και τα κεφάλαια μεταφέρονται ηλεκτρονικά από τον λογαριασμό του πληρωτή στον λογαριασμό του δικαιούχου πληρωμής. Αυτά τα συστήματα δημιουργούν έναν κίνδυνο ασφάλειας εάν οι διαδικασίες δεν είναι σε θέση να ελέγξουν τη διαθεσιμότητα των κεφαλαίων που πρόκειται να μεταφερθούν ή εάν οι έλεγχοι πρόσβασης λογαριασμού δεν είναι σε ισχύ. Υπάρχει επίσης η δυνατότητα χειρισμού των πληροφοριών καθώς περνούν πέρα από το δίκτυο σε μη κρυπτογραφημένη μορφή. Προκειμένου να εξασφαλιστούν οι ηλεκτρονικές μεταφορές κεφαλαίων, τα στοιχεία κρυπτογραφούνται γενικά χρησιμοποιώντας τους αλγορίθμους που κωδικοποιούν τα μηνύματα. Αυτοί αποκωδικοποιούνται έπειτα χρησιμοποιώντας τα ηλεκτρονικά κλειδιά που είναι γνωστά στον αποστολέα και τον παραλήπτη. Ο σημαντικότερος κίνδυνος ασφάλειας που συνδέεται με ένα τέτοιο σύστημα βρίσκεται στη δυνατότητα των κλειδιών κρυπτογράφησης να εξακριβώσουν, σε ποια περίπτωση τα στοιχεία μέσα στο σύστημα θα μπορούσαν να αποκαλυφθούν ή να χειριστούν. Οι περισσότερες από τις ηλεκτρονικές απάτες μεταφοράς κεφαλαίων μεγάλης κλίμακας που έχουν διαπραχθεί στο παρελθόν έχουν περιλάβει την παρεμπόδιση ή την αλλαγή των μηνυμάτων ηλεκτρονικών στοιχείων που διαβιβάζονται από τους υπολογιστές των χρηματοδοτικών οργανισμών[33]. Σε πολλές περιπτώσεις οι παραβάτες έχουν εργαστεί μέσα στους χρηματοδοτικούς οργανισμούς οι ίδιοι και είναι μυημένοι στη λειτουργία των εν λόγω συστημάτων ασφάλειας .

Προκειμένου να ενισχυθεί η ασφάλεια των συναλλαγών πιστωτικών καρτών στο διαδίκτυο, διάφορες επιχειρήσεις έχουν σχεδιάσει τα συστήματα για να εξασφαλίσουν ότι η ταυτότητα των συμβαλλόμενων μερών είναι σε θέση να επικυρωθεί και ότι οι έμποροι είναι σε θέση να εξακριβώσουν εάν ο πελάτης έχει τα επαρκή κεφάλαια με τα οποία να πραγματοποιήσει τη συναλλαγή. Η Microsoft και η Visa, παραδείγματος χάριν, αναπτύσσουν ένα πρωτόκολλο πληρωμής αποκαλούμενο "SET" (Ασφαλείς Ηλεκτρονικές Συναλλαγές) που χρησιμοποιεί τη δημόσια βασική κρυπτογράφηση για να προστατεύσει τα στοιχεία από το συμβιβασμό. Οι

---

[33] . Meijboom, A.P. 1988, 'Problems related to the use of EFT and teleshopping systems by the consumer', in *Telebanking, Teleshopping and the Law*. eds. Y.Poullet & G.P.V. Vandenberghe, Kluwer, Deventer, σσ.23–32.

ψηφιακές υπογραφές χρησιμοποιούνται επίσης για να επικυρώσουν καθένα από τα ενδιαφερόμενα μέρη. Οι πληροφορίες λογαριασμού κρυπτογραφούνται πριν από τη μετάδοση με τα κλειδιά αποκρυπτογράφησης να προστατεύονται χωριστά. Οι έμποροι λαμβάνουν την πληρωμή μέσω διαβίβασης στην τράπεζά τους ενός κρυπτογραφημένου μηνύματος που δημιουργείται με τον πελάτη που επιτρέπει στα κεφάλαια να μεταφερθούν από τον λογαριασμό του πελάτη στον λογαριασμό του εμπόρου[34].

Οι κύριοι κίνδυνοι ασφάλειας που συνδέονται με αυτά τα συστήματα αφορούν στο ότι υπάρχει η δυνατότητα κλοπής των ιδιωτικών κλειδιών κρυπτογράφησης ή να χρησιμοποίησής τους χωρίς έγκριση από τους ανθρώπους που τα έχουν λάβει παράνομα. Ο ευκολότερος τρόπος να γίνει αυτό θα ήταν να υποβληθούν τα ψεύτικα στοιχεία ταυτότητας στις Αρχές Ελέγχου κατά τη λήψη ενός δημόσιου - ιδιωτικού ζευγαριού κλειδιών. Εναλλακτικά, εάν ένα ιδιωτικό κλειδί κρατήθηκε σε μια έξυπνη κάρτα, θα μπορούσε να γίνει η πρόσβαση στο κλειδί απλά με το σπάσιμο της συσκευής ελέγχου πρόσβασης στην κάρτα που θα μπορούσε απλά να είναι ένας κωδικός πρόσβασης. Κατά συνέπεια θα μπορούσε να είναι δυνατό για κάποιον να χρησιμοποιήσει το ιδιωτικό κλειδί ενός άλλου προσώπου, για να παραγγείλει τα αγαθά ή τις υπηρεσίες από το Διαδίκτυο και να είναι αδύνατον να ανιχνευθεί.

2.6.4.-Απάτη που περιλαμβάνει τα σε κάρτα-βασισμένα συστήματα

Σαφώς, θα διευκόλυνε πολύ το ηλεκτρονικό εμπόριο, εάν ένας χρήστης ήταν σε θέση να παρεμβάλει μια πλαστική κάρτα σε ένα τερματικό EFTPOS που συνδέθηκε με έναν προσωπικό υπολογιστή και διεξάγει συναλλαγές άμεσα μεταξύ ενός εμπόρου και ενός χρηματοδοτικού οργανισμού. Αυτό, εντούτοις, θα σήμαινε ότι κάθε προσωπικός υπολογιστής περιλαμβάνεται στο δίκτυο υπολογιστών που συνδέει όλους τους χρηματοδοτικούς οργανισμούς παγκοσμίως.

Ακόμα κι αν αυτό ήταν οικονομικά δυνατό, τα συστήματα πληρωμής με πλαστικές κάρτες είναι ευπρόσβλητα στην απάτη μέσω της πλαστογράφησης, της αλλαγής και της κλοπής των καρτών[35], για να μην αναφέρουμε τα λογιστικά και τα προβλήματα ασφάλειας που συνδέονται με την παροχή ασφαλούς δικτύου κάθε χρηματοδοτικού οργανισμού σε κάθε χρήστη του Διαδικτύου. Άλλοι εξετάζουν τη χρήση των έξυπνων καρτών με την ικανότητα να αποθηκευτεί η αξία και να μεταφερθεί αυτό στους εμπόρους μέσω του Διαδικτύου. Τα συστήματα πληρωμών με έξυπνες κάρτες μπορούν να λάβουν ποικίλες μορφές. Το σύστημα που μοιάζει περισσότερο με τις πρόωρες μορφές αποθηκευμένων καρτών αξίας περιλαμβάνει έναν χειριστή σχεδίου που διαχειρίζεται μια κεντρική ομάδα των κεφαλαίων. Όταν ένας κάτοχος καρτών μεταφέρει την αξία στην κάρτα, τα κεφάλαια μεταφέρονται πραγματικά σε μια ομάδα που ελέγχεται από το χειριστή σχεδίου. Ένας έμπορος που πληρώνεται από την κάρτα παίρνει τα στοιχεία της απόδειξης του χειριστή σχεδίου, η οποία καταβάλλει το σχετικό ποσό από το κεφάλαιο. Άλλες προτάσεις, όπως εκείνες που χρησιμοποιούνται από τη MasterCard και τη Visa International, προβλέπουν διάφορα εμπορικά σήματα καρτών που δέχονται. Σε τέτοια σχέδια δεν υπάρχει καμία κεντρική ομάδα των κεφαλαίων, αλλά μάλλον κάθε εκδότης καρτών είναι αρμόδιος για την αποζημίωση των εμπόρων που δέχονται τις κάρτες τους. Στο Ηνωμένο Βασίλειο, στο σύστημα Mondex που αναπτύχθηκε από την Εθνική τράπεζα του Westminster και του Midland δεν αναμιγνύονται χειριστές

---

[34] Visa International 1997, 'SET Draft Reference Implementation', http://www.visa.com/ (visited 2 May 2000).

[35] Smith, R. G. 1997, 'Plastic Card Fraud', in *Trends and Issues in Crime and Criminal Justice*, No.71, Australian Institute of Criminology, Canberra.

σχεδίου. Τα Κεφάλαια χρεώνονται στην κάρτα που μπορεί έπειτα να χρησιμοποιηθεί χωρίς αναφορά σε οποιοδήποτε πρόσωπο. Τα Κεφάλαια μεταφέρονται από τη μια κάρτα στην άλλη καθώς επίσης και στους εμπόρους αλλά επειδή τα κεφάλαια που υπάρχουν στην κάρτα δεν υπάρχουν οπουδήποτε εκτός από την κάρτα, δεν υπάρχει κανένας λογιστικός έλεγχος των συναλλαγών ή του συμβιβασμού των πληρωμών. Αυτό σημαίνει ότι η παραποίηση θα μπορούσε να εμφανιστεί χωρίς ίχνος και το σχέδιο θα μπορούσε να χρησιμοποιηθεί για το ξέπλυμα χρημάτων ή τη διασκόρπιση των εισπράξεων εγκληματικών δραστηριοτήτων. Η κάρτα Mondex μπορεί να επαναφορτιστεί από μια σύνδεση κινητών τηλεφώνων και μπορεί να χρησιμοποιηθεί στα τερματικά EFTPOS. Στις Ηνωμένες Πολιτείες μια τροποποιημένη έκδοση του συστήματος Mondex είναι που θα επιτρέψει στις τράπεζες να επισημάνουν τη χρήση καρτών. Επίσης θα είναι δυνατό τα χρήματα που κρατιούνται στις κάρτες να εισχωρηθούν στους υπολογιστές, επιτρέποντας κατά συνέπεια στις αγορές Διαδικτύου να πληρωθούν ηλεκτρονικά από την κάρτα[36].

Ο κύριος κίνδυνος ασφάλειας που συνδέεται με τις έξυπνες κάρτες βρίσκεται στον τρόπο με τον οποίο τα στοιχεία κρυπτογραφούνται. Η κρυπτογράφηση που χρησιμοποιείται στις έξυπνες κάρτες μπορεί να σπαστεί εάν μπορούν να δημιουργηθούν στην κάρτα ορισμένοι τύποι λαθών, για παράδειγμα μέσω της χρήσης του ιονισμού ή της ακτινοβολίας μικροκυμάτων. Η 'Bellcore', μια επιχείρηση ασφάλειας των υπολογιστών και των επικοινωνιών, αλλά και άλλες έχουν προσδιορίσει διάφορα λάθη σχεδίου στις κάρτες 'chip' των υπολογιστών που μπορούν να επιτρέψουν τη διαρροή των στοιχείων ή το πείραγμα των πληροφοριών που περιλαμβάνονται στην κάρτα [37].

2.6.5.-Απάτη που περιλαμβάνει τα ηλεκτρονικά μετρητά - 'Digicash'

Αναπτύσσονται επίσης διάφορα συστήματα που θα επιτρέψουν στις συναλλαγές να πραγματοποιηθούν ασφαλώς στο διαδίκτυο μέσω της χρήσης των ηλεκτρονικών μετρητών ή της συμβολικής αξίας που καταγράφονται ψηφιακά στους υπολογιστές.

Το σύστημα Digicash, παραδείγματος χάριν, που εδρεύει στις Κάτω Χώρες, χρησιμοποιεί μια μορφή ηλεκτρονικών χρημάτων γνωστή ως 'e-cash'[38]. Προτού να μπορέσουν να γίνουν οι αγορές, και ο έμπορος και ο καταναλωτής έχουν την ανάγκη να καθιερώσουν τραπεζικές ρυθμίσεις και συνδέσεις Διαδικτύου με την τράπεζα που εκδίδει το 'e-cash'. Ο πελάτης ζητά αρχικά μια μεταφορά των κεφαλαίων από τον τραπεζικό λογαριασμό του /της στο σύστημα Ecash. Αυτό είναι παρόμοιο με την ανάληψη μετρητών από το ATM. Το e-cash σύστημα παράγει έπειτα και επικυρώνει e-cash νομίσματα που ο πελάτης είναι σε θέση να χρησιμοποιήσει στο Διαδίκτυο. Τα νομίσματα είναι εισροές στοιχείων που υπογράφονται ψηφιακά από την εκδότρια τράπεζα που χρησιμοποιεί το ιδιωτικό κλειδί του. Ο πελάτης είναι έπειτα ικανός να στείλει e-cash σε οποιοδήποτε έμπορο που θα δεχτεί αυτήν την μορφή πληρωμής χρησιμοποιώντας το λογισμικό που παρέχεται από τον e-cash φορέα παροχής υπηρεσιών. Ο πελάτης κρυπτογραφεί το μήνυμα και επικυρώνει τα νομίσματα χρησιμοποιώντας το δημόσιο κλειδί του εμπόρου. Ο έμπορος αποκρυπτογραφεί έπειτα το μήνυμα με το ιδιωτικό του κλειδί και ελέγχει την ισχύ του νομίσματος χρησιμοποιώντας το κλειδί της τράπεζας έκδοσης. Ο έμπορος είναι έπειτα ικανός να μετατρέψει το e-cash σε πραγματικά κεφάλαια με την παρουσίαση e-cash στην

---

[36] Hansell 1996

[37] Spinks, P. 1996, 'Tests Show Up Smart Card Flaws', *The Age (Melbourne)*, 6 December,
Denning, D. E. 1999, *Information Warfare and Security*, ACM Press, Reading, Massachusetts.

[38] E-cash 2000, on the web.

εκδότρια τράπεζα και με αίτημα ένα ισοδύναμο ποσό πραγματικών κεφαλαίων που πιστώνονται στον τραπεζικό λογαριασμό του εμπόρου.

2.6.6.-Παραποίηση ταυτότητας

Η εμφάνιση του σε απευθείας σύνδεση εμπορίου έχει δημιουργήσει επίσης νέες μορφές παρανομίας που είναι λιγότερο πιθανό να εμφανιστούν στις παραδοσιακές αγορές. Πολλοί καταναλωτές, παραδείγματος χάριν, έχουν τώρα μεγάλη δυσκολία στον προσδιορισμό εκείνων με τους οποίους κάνουν επιχειρήσεις. Μερικοί έμποροι μπορούν σκόπιμα να αλλοιώσουν την ταυτότητά τους μέσω της χρήσης ηλεκτρονικού ταχυδρομείου, για να παραπλανήσουν τους πελάτες και να αποφύγουν την ανίχνευση[39]. Άλλοι μπορούν απλά να είναι αμελείς στην παροχή των εξακριβωμένων και επαληθεύσιμων πληροφοριών. Η τεχνολογία του Διαδικτύου καθιστά σχετικά απλό για τους χρήστες να παραποιήσουν τις ταυτότητές τους. Οι διευθύνσεις ηλεκτρονικού ταχυδρομείου και Διαδικτύου μπορούν να χειριστούν συμπεριλαμβάνοντας είτε λεπτομέρειες που είναι παραπλανητικές ή την πηγή ενός μηνύματος που μπορεί να γίνει ανώνυμη ή να αλλάξει έτσι ώστε να εμφανίζεται από έναν άλλο χρήστη. Ομοίως, δεν υπάρχει κανένας τρόπος να γνωρίζουν τους εμπορικούς συνεργάτες εκείνων στο Διαδίκτυο. Οι διαιτητές για τις επιχειρήσεις ή τα προϊόντα, στην πραγματικότητα, είναι άτομα που απασχολήθηκαν συγκεκριμένα για να δείξουν την έγκρισή τους για την επιχείρηση ή το εν λόγω προϊόν. Οι επιχειρήσεις επίσης μπορούν να επιλέξουν τα νόμιμα ονόματα προκειμένου να βελτιωθεί η αξιοπιστία τους ή να περιληφθούν τα ονόματα δικτυακών τόπων που είναι παραπλανητικά. Έχει αναπτυχθεί πρόσφατα στις Ηνωμένες Πολιτείες και τον Καναδά μια πρακτική μερικών επιχειρήσεων που υιοθετεί τα ονόματα περιοχών που περιέχουν τα ονόματα αυστραλιανών πόλεων προκειμένου να βελτιωθεί η εμπορευσιμότητα και η αξιοπιστία τους, παρά το γεγονός ότι δεν έχουν καμία σχέση με την Αυστραλία.

Σε μια περίπτωση που ερευνήθηκε από το ACCC (1997b), ένας έμπορος Διαδικτύου χρησιμοποίησε το ίδιο όνομα δικτυακού τόπου με έναν άλλο έμπορο (ο αρχικός φορέας του ονόματος), αλλά με ένα <com> επίθημα, σε αντιδιαστολή με το <net> επίθημα του αρχικού τόπου. Η σύγχυση που δημιουργήθηκε ως προς την ταυτότητα του πραγματικού ιδιοκτήτη της περιοχής οδήγησε τους καταναλωτές στο να παραπλανηθούν ή να εξαπατηθούν. Ο τόπος με το επίθημα <com>, εντούτοις, περιελάμβανε μια δυσδιάκριτη ειδοποίηση δηλώνοντας ότι δεν πρέπει να συγχέεται με τον αντίστοιχο δικτυακό τόπο με επίθημα <net>, αν και αυτό θα μπορούσε εύκολα να έχει αγνοηθεί από εκείνους που επισκέπτονται τον δικτυακό τόπο.

2.7.- Απάτη πιστωτικών καρτών

Σύμφωνα με ένα δελτίο ειδήσεων Βρετανικού ραδιοφωνικού σταθμού, η απάτη πιστωτικών καρτών στην Ευρωπαϊκή Ένωση αυξήθηκε κατά 50% πέρυσι και ένα μεγάλο μέρος της αύξησης περιλαμβάνει τις πληρωμές που γίνονται μέσω του Διαδικτύου ή του τηλεφώνου και θα μπορούσε να πλήξει την καταναλωτική εμπιστοσύνη στο ηλεκτρονικό εμπόριο.

Η Ευρωπαϊκή Επιτροπή λέει ότι είναι αναγκαίο να καταπατηθεί η απάτη στις παράνομες συναλλαγές, η οποία υπολογίζεται στα 600 εκατομμύρια ευρώ ($553m) στην Ευρώπη τον περασμένο χρόνο. Ένας εκπρόσωπος της ΕΕ είπε ότι ενώ οι πωλήσεις ηλεκτρονικού εμπορίου ήταν σε άνοδο, το δυναμικό τους "εμποδίστηκε από την έλλειψη εμπιστοσύνης, την εχεμύθεια και την ασφάλεια των συναλλαγών πληρωμής

---

[39] Rothchild 1999, σ. 927

που εκτελέσθηκαν μέσω του Διαδικτύου". Πρόσφατα στοιχεία έχουν δείξει ότι οι συναλλαγές Διαδικτύου αντιπροσωπεύουν μόνο 2% όλης της χρήσης πιστωτικών καρτών, αλλά αποτελούν τις μισές από τις καταγγελίες πελατών. Η ανωνυμία του Διαδικτύου επιτρέπει στους εγκληματίες να κάνουν τις διασυνοριακές αγορές με τα κλεμμένα στοιχεία πιστωτικών καρτών με σχετικά μικρό κίνδυνο σύλληψης. Νέα τεχνικά μέτρα αναπτύσσονται επίσης για να αποτρέψουν την απάτη, όπως τα ηλεκτρονικά 'τσιπ' στις πιστωτικές κάρτες. Σημαντικές εταιρίες όπως η Visa, η American Express και η MasterCard έχουν αρχίσει ήδη να συνεργάζονται για να βελτιώσουν μαζί τα πρότυπα ασφάλειας στο Διαδίκτυο. Οι "πιστωτικές κάρτες δεν έγιναν για να λειτουργούν στο Διαδίκτυο," είπε μια πηγή της Επιτροπής. "Υπάρχει πραγματική ανάγκη ασφαλέστερων συστημάτων πληρωμής και ελπίζουμε ότι η βιομηχανία θα τα διαμορφώσει." Όπως αυτό το άρθρο προτείνει, το συνηθέστερα χρησιμοποιημένο εργαλείο για το ηλεκτρονικό εμπόριο στο Διαδίκτυο έχει επίσης χαρακτηριστεί ως η πιο επισφαλής μέθοδος. Οι πιστωτικές κάρτες μπορούν να είναι μια ανάγκη για τους περισσότερους από μας αλλά η χρήση της στο διαδίκτυο δεν έρχεται χωρίς ένα τίμημα. Εννέα από τις δέκα σε απευθείας σύνδεση απάτες πιστωτικών καρτών στο Ηνωμένο Βασίλειο καταλήγουν ατιμώρητες, δεδομένου ότι πολλοί λιανοπωλητές Διαδικτύου δεν αναφέρουν τις περιπτώσεις και η αστυνομία σπάνια καταδιώκει τις καταγγελίες. Σύμφωνα με μια έρευνα της αντιπροσωπείας πίστωσης, Experian, πολλοί σε απευθείας σύνδεση λιανοπωλητές αποτυγχάνουν να κάνουν τους βασικούς ελέγχους στους αγοραστές, όπως την εξέταση, εάν η διεύθυνση του κατόχου πιστωτικών καρτών και η διεύθυνση παράδοσης είναι οι ίδιες[40].

Ένα πέμπτο όλων των σε απευθείας σύνδεση λιανοπωλητών δοκιμάζει την απάτη που ανέρχεται σε περισσότερο από 1% των πωλήσεων και μερικές εταιρίες ακόμη διαπιστώνουν ότι μέχρι 10% των πωλήσεών τους πραγματοποιούνται με απατεώνες. Οι επιχειρήσεις που προσφέρουν τις σε απευθείας σύνδεση υπηρεσίες ή το λογισμικό για μεταφόρτωση είναι ιδιαίτερα τρωτές, δεδομένου ότι οι απατεώνες έχουν μικρή δυσκολία στην κάλυψη των ιχνών τους. Αλλά η αγορά φυσικών αγαθών δεν αποτελεί πρόβλημα . Μετά από τη κλοπή στοιχείων πιστωτικών καρτών κάποιου άλλου, οι απατεώνες απλά ζητούν από τους λιανοπωλητές να στείλουν τα αγαθά σε μια διεύθυνση απ` όπου συλλέγουν τα αγαθά και εξαφανίζονται. Σύμφωνα με την Experian, σχεδόν οι μισές εταιρίες αποτυγχάνουν να χρησιμοποιήσουν τα εξωτερικά στοιχεία για να επιβεβαιώσουν ότι ο αγοραστής είναι πραγματικά ο κάτοχος της πιστωτικής κάρτας, κάνοντας κατά συνέπεια εύκολη την πρόσβαση στους εγκληματίες και μόνο 15% των λιανοπωλητών χρησιμοποίησε τα αυτοματοποιημένα συστήματα για να κάνει τους ελέγχους ταυτότητας.

2.7.1.- Στρατηγικές αποτροπής απάτης πιστωτικών καρτών

2 .7.1.1.- Εκδότες καρτών-Χρηματοδοτικοί οργανισμοί-Τράπεζες

Υπάρχουν τέσσερις αρχικές στρατηγικές που μπορούν να χρησιμοποιηθούν για να αποτρέψουν την απάτη πλαστικών καρτών. Πρώτα είναι οι ενέργειες που πρέπει να ληφθούν από τους εκδότες καρτών ή τους χρηματοδοτικούς οργανισμούς. Οι εκδότες καρτών είναι σε θέση να υιοθετήσουν μια ευρεία ποικιλία των στρατηγικών που μπορεί να μειώσει τον κίνδυνο απάτης πλαστικών καρτών. Η πιο επείγουσα ανάγκη είναι οι χρηματοδοτικοί οργανισμοί να μην διανέμουν κάρτες στα άτομα εκτός αν είναι σίγουροι για την ταυτότητά τους. Αν και το σύστημα 100 βαθμών για τους ανοιχτούς λογαριασμούς είναι μια αφετηρία, αυτό πρέπει να γίνει σωστά με τα κατάλληλα αρχικά έγγραφα όπως τα πιστοποιητικά γέννησης που ελέγχονται λεπτομερώς

---

[40] BBC Business News, Credit card fraud rise, web article, 20 February, 2001 at: http://news.bbc.co.uk/hi/english/business/newsid_1179000/1179590.stm

και επικυρώνονται. Τα αρχικά έγγραφα ταυτότητας πρέπει να παραχθούν με τέτοιο τρόπο ώστε να μειωθούν οι δυνατότητες πλαστογράφησης. Διάφορες διαδικασίες μπορούν επίσης να υιοθετηθούν για να εξασφαλίσουν ότι οι πλαστικές κάρτες δεν κλέβονται και ότι οι κάρτες και τα PIN κοινοποιούνται ασφαλώς στους πελάτες. Οι τράπεζες είναι επίσης ικανές να βοηθήσουν τους εμπόρους ενημερώνοντας τους αμέσως για τις κλεμμένες κάρτες και PIN. Οι τράπεζες, παραδείγματος χάριν, στην Αυστραλία έχουν τώρα μια κεντρική αντιπροσωπεία υποβολής εκθέσεων και έρευνας απάτης για τις πλαστικές κάρτες, την Cardlink Services Limited, η οποία διατηρεί στενό σύνδεσμο με την αστυνομία. Η Cardlink ερευνά περιπτώσεις δόλιας χρήσης καρτών σε κάθε πολιτεία και περιοχή της Αυστραλίας και συγκεντρώνει στοιχεία που έπειτα παραδίδονται στην αστυνομία[41]. Θα μπορούσε επίσης να ζητηθεί να επιδεικνύουν οι κάρτες τη φωτογραφία του κατόχου, ενώ οι διαδικασίες ασφάλειας μπορούν να ενισχυθούν για εκείνους που αναλαμβάνουν τη νόμιμη κατασκευή των καρτών για να εξασφαλίσουν ότι τα φύλλα, οι χρωστικές ουσίες, οι εκτυπωτές και οι κωδικοποιητές PVC δεν κλέβονται και χρησιμοποιούνται για πλαστογράφηση[42]. Μια από τις κύριες στρατηγικές που χρησιμοποιείται για να αποτρέψουν την απάτη EFTPOS είναι απλώς η μείωση σε χαμηλότερα επίπεδα (η αξία συναλλαγής στην οποία η έγκριση απαιτείται από τις τράπεζες προτού να γίνει αποδεκτή η κάρτα). Τέλος, διάφορες στρατηγικές ελέγχου έχουν προταθεί για να ελαχιστοποιήσουν τις απώλειες μέσω πλαστογράφησης έξυπνων καρτών προσδιορίζοντας γρήγορα τις ψευδείς συναλλαγές και περιορίζοντας την μέγιστη αξία των συναλλαγών.

2.7.1.2.- Έμποροι

Μια άλλη στρατηγική είναι τα προληπτικά μέτρα που πρέπει να υιοθετηθούν από τους εμπόρους που δέχονται εκείνες τις κάρτες. Οι απάτες στις οποίες αναμειγνύονται έμποροι αποτελούν ένα μεγάλο πρόβλημα για τους χρηματοδοτικούς οργανισμούς καθώς οι έμποροι ή οι υπάλληλοί τους τοποθετούνται ιδανικά για να επιτρέψουν την πρόσβαση στα δίκτυα υπολογιστών και για να αλλάξουν τα στοιχεία της συναλλαγής. Ο Bonney[43] συζητά διάφορους τρόπους για να αποτραπεί η απάτη πιστωτικών καρτών συμπεριλαμβάνοντας τυχαίους ελέγχους έγκρισης των αρχείων τραπεζικού λογαριασμού των εμπόρων και αποδείξεων πωλήσεων. Οι έμποροι διαφημίζουν το γεγονός ότι λαμβάνονται μέτρα για να αποτρέψουν την απάτη πιστωτικών καρτών στις εγκαταστάσεις τους, και ότι γίνεται πιο προσεκτική εξέταση των χαρακτηριστικών γνωρισμάτων ασφάλειας των καρτών από το προσωπικό πωλήσεων όταν διεξάγονται οι συναλλαγές. Οι έμποροι πρέπει επίσης να κρατούν μια διεύθυνση παράδοσης και έναν αριθμό τηλεφώνου όταν εκτελούνται οι διαταγές τηλεφωνικώς και να καλούν έπειτα τον αριθμό για να επαληθεύσουν τις παρεχόμενες πληροφορίες. Να ζητούν από τα άτομα που παίρνουν τα αγαθά που αγοράζονται με πιστωτική κάρτα να τους επιδεικνύουν την ταυτότητά τους και να επιθεωρούν την πιστωτική κάρτα που χρησιμοποιείται εξασφαλίζοντας ότι οι παραδόσεις των αγαθών γίνονται στο πρόσωπο που έδωσε την παραγγελία[44]. Τέλος, οι έμποροι πρέπει να εξετάσουν οποιαδήποτε ύποπτη συμπεριφορά και εμφάνιση των πελατών όπως όταν οι πελάτες επιλέγουν τις αγορές, όταν ντύνονται αντιφατικά σε σχέση με τη φύση των αγορών που επιλέγονται, πελάτες που αναιρούν τις αγορές μέσα από διάφορα λάθη σε μία προσπάθεια να ματαιωθούν οι κλήσεις έγκρισης στους εκδότες, πελάτες που επιδιώκουν να βιάσουν μια συναλλαγή, πελάτες που κάνουν μια αγορά και έπειτα μια επιστροφή,

---

[41] Van – Rhoda 1991, σ.1991.

[42] Duncan, M. D. G. 1995, The future threat of credit card crime, RCMP Gazette, vol. 57, no. 10, σ. 25-6.

[43] Bonney, R. 1992, Preventing Credit Card Fraud, New South Wales Bureau of Crime Statistics and Research Crime and Justice Bulletin No. 17, NSW Bureau of Crime Statistics and Research, Sydney,σσ. 6-8.

[44] Van Leeuwen, H. 1996, A surge in credit card fraud, Financial Review, 24 September, σ. 49.

πελάτες που κάνουν πολλαπλές αγορές όλες κάτω από το όριο και πελάτες που αγοράζουν πολλά από τα ίδια εμπορεύματα αλλά σε διαφορετικά χρώματα και μεγέθη[45]. Δυστυχώς, δεν είναι συχνά δυνατό για τους εμπόρους να χρησιμοποιήσουν όλες αυτές τις τεχνικές εξαιτίας του φόβου ότι θα αποθαρρύνουν πιθανούς πελάτες.

2.7.1.3.- Καταναλωτές

Ο κάτοχος κάρτας πρέπει να λάβει υπόψη τα εξής: Η προστασία της κάρτας, του Pin ή του κωδικού πρόσβασης κάποιου είναι η αρχική στρατηγική πρόληψης εγκλήματος που οι κάτοχοι πρέπει να πάρει. Αν και οι καταναλωτές ενθαρρύνονται για να μην αποκαλύψουν το Pin τους, να μην το κρατήσουν μαζί με την κάρτα τους, ή το γράψουν πάνω στην κάρτα, οι μελέτες έχουν αποκαλύψει ότι από 20 έως 70 τοις εκατό των ανθρώπων αποτυγχάνουν στο να ακολουθούν τέτοιες συμβουλές[46].

2.7.1.4.- Αποτέλεσμα

Όπου αυτές οι στρατηγικές έχουν εφαρμοστεί με συνέπεια, μπορούν να εμφανιστούν ουσιαστικές μειώσεις της απάτης. Στη Μεγάλη Βρετανία, παραδείγματος χάριν, η χρήση ποικίλων στρατηγικών με σκοπό να αποτρέψουν την πλαστική απάτη καρτών οδήγησε σε μια μείωση τέτοιου είδους απάτης της τάξης του 41% συνολικά μεταξύ 1991 και 1994, ενώ οι απώλειες που εμφανίζονται στις λιανικές θέσεις πώλησης μειώθηκαν κατά 49% κατά τη διάρκεια της ίδιας περιόδου. Οι απώλειες από τις κάρτες που χάθηκαν ή που κλάπηκαν μειώθηκαν κατά 62 %μεταξύ 1991 και 1994[47].

2.7.2.- Μέθοδοι απάτης και σχόλια ειδικών

Σήμερα, ένας αριθμός πιστωτικής κάρτας είναι πολύτιμο αγαθό για τους κλέφτες. "Δεν χρειάζεστε το πλαστικό για να χρησιμοποιήσετε τον αριθμό πιστωτικής κάρτας κάποιου," ιδιαίτερα σε αυτήν την εποχή Διαδικτύου και του καταλόγου αγορών, λέει ο Beth Givens, διευθυντής του γραφείου δικαιωμάτων ιδιοκτησίας στο Σαν Ντιέγκο. Το ίδιο πράγμα ισχύει και για τις χρεωστικές κάρτες. Ένας κλέφτης που κατέχει έναν αριθμό χρεωστικής κάρτας μπορεί να κάνει ένα όργιο αγορών, που χρηματοδοτείται από τον λογαριασμό σας.

Οι εγκληματίες είναι γνώστες της τεχνολογίας και επινοούν νέους τρόπους για να πάρουν στα χέρια τους πληροφορίες καρτών. Αυτοί διαπίστωσαν ότι η απάτη στις κάρτες υπερτερεί της ληστείας με όπλα. Αντ' αυτού, στις βάσεις δεδομένων Διαδικτύου που είναι γεμάτες με στοιχεία καρτών πελατών χαράσσουν και αντιγράφουν στοιχεία λογαριασμού που κωδικοποιούνται στη μαγνητική λωρίδα μιας κάρτας. "Η απάτη πιστωτικών καρτών είναι η ληστεία τραπεζών του μέλλοντος," λέει ο Gregory Regan, ειδικός πράκτορας υπεύθυνος για το οικονομικό τμήμα εγκλημάτων της Αμερικάνικης μυστικής υπηρεσίας. "Οι εγκληματίες έχουν συνειδητοποιήσει ότι οι πιστωτικές κάρτες και το τραπεζικό σύστημα είναι εύκολος στόχος."

Όπως ήταν αναμενόμενο, το Διαδίκτυο τροφοδοτεί τέτοια απάτη. Όχι μόνο βοηθά τους εγκληματίες να ανακτήσουν τα στοιχεία λογαριασμού γρήγορα και αποτελεσματικά, αλλά επίσης επιτρέπει να διαπράξουν παραβάσεις από οπουδήποτε στον κόσμο. Οι κλέφτες μπορούν να στείλουν με μήνυμα μέσω του ηλεκτρονικού

---

[45] Grau, J. J. (ed.) 1992, Criminal and Civil Investigation Handbook, 2nd ed., McGraw-Hill Inc., New York, σ.39.

[46] Sullivan, C. 1987, Unauthorised automatic teller machine transactions: Consequences for customers of financial institutions, Australian Business Law Review, vol. 15, no. 3, σ. 189.

[47] Webb, B. 1996, "Preventing plastic card fraud in the UK", Security Journal, vol. 7, σσ. 24-25

ταχυδρομείου τις πληροφορίες λογαριασμού στο εξωτερικό στις ομάδες, οι οποίες παράγουν έπειτα τις πλαστές κάρτες. Τα εμπορεύματα μπορούν επίσης να αγοραστούν από έναν έμπορο Διαδικτύου, επιτρέποντας στον απατεώνα να αποκρύψει την ταυτότητα του και να αφήσει λίγες ενδείξεις για να τον ανακαλύψουν. Όταν η συναλλαγή δεν γίνεται απευθείας , τότε η απάτη καθίσταται ευκολότερη."

Η εκπληκτική αύξηση των περιοχών ηλεκτρονικού-εμπορίου παρέχει στους εγκληματίες έναν κόσμο εμπόρων που υποστηρίζουν προϊόντα που είναι εύκολα προστατευμένα. Ανεξάρτητα από το πόσο κάποιος μπορεί να πάρει μια λαβή των οικονομικών πληροφοριών ενός καταναλωτή, η δυνατότητα να παραβιαστούν στο διαδίκτυο είναι τεράστια ".

Σύμφωνα με την Αμερικάνικη μυστική υπηρεσία, το ταχύτατης ανάπτυξης τέχνασμα που χρησιμοποιείται ιδιαίτερα από τις οργανωμένες ομάδες εγκληματιών στο εξωτερικό είναι η κλοπή στοιχείων καρτών με "το ξάφρισμα" τους από μια γνήσια κάρτα. Η μαγνητική λωρίδα στην πλάτη της κάρτας κωδικοποιείται με το όνομα ενός κατόχου κάρτας, τον αριθμό λογαριασμού, την ημερομηνία λήξης –και έναν κώδικα μοναδικό σε κάθε κάρτα. Χωρίς τον τελευταίο αριθμό, η κάρτα δεν μπορεί να πλαστογραφηθεί. Αλλά οι κλέφτες αγοράζουν τους μαγνητικούς αναγνώστες λωρίδων –διαθέσιμους για περίπου $400 στο Διαδίκτυο – και τους αλλάζουν για να καταγράψουν όλα τα στοιχεία σε μια μαγνητική λωρίδα με μια απλή κλοπή της κάρτας.

Στις ειδήσεις του περασμένου Νοεμβρίου (U.S ιστοσελίδα ειδήσεων), παραδείγματος χάριν, ένας Bloomingdale αγοραστής στη Νέα Υόρκη που πληρώνει για τα γυαλιά ηλίου με πιστωτική κάρτα παρατήρησε κάτι ύποπτο. Η κάρτα ήταν δύο φορές κλεμμένη, μια φορά μέσω της συσκευής πιστωτικών καρτών του καταστήματος και μια μέσω του προμηθευτή ενός καταστήματος Palm, ο οποίος συνδέθηκε με μια συσκευή κλοπής. Οι αρχές επιβολής νόμου βλέπουν συχνά αυτό το τέχνασμα στα εστιατόρια, όπου ένας ανέντιμος σερβιτόρος ή μια σερβιτόρα θα τραβήξει διακριτικά τη μικρή συσκευή από την τσέπη του /της, θα παραποιήσει την κάρτα και θα την κρύψει, πριν γίνει αντιληπτό.

Μερικοί εγκληματίες έχουν υψηλές βλέψεις. Πρόσφατα, ένας χάκερ υπολογιστών πήρε χιλιάδες αριθμούς πιστωτικών καρτών πελατών του CD Universe Website και τους δημοσίευσε στο Διαδίκτυο αφότου η επιχείρηση αρνήθηκε να πληρώσει τα λύτρα. Ο "κόσμος του CD άφησε βασικά τη πρόσβαση ανοικτή," λέει ο Raf Sorrentino, αντιπρόεδρος της διαχείρισης απάτης και κινδύνου στην εταιρία 'First Data', έναν ηλεκτρονικό επεξεργαστή πληρωμής στην Ατλάντα. Η επιχείρηση λέει ότι η ασφάλεια είναι σημαντική, και "προφανώς θα είναι ακόμα πιο κυρίαρχη τώρα," λέει ο Brett Brewer, αντιπρόεδρος του ηλεκτρονικού εμπορίου για το παγκόσμιο εμπόριο, το οποίο διοικεί το CD Universe. Ωστόσο οι εμπειρογνώμονες υποστηρίζουν ότι οι εταιρίες πρέπει εν μέρει να κατηγορηθούν. "Έχουμε τις επιχειρήσεις που βιάζονται να επωφεληθούν από αυτήν την τρέλα του ηλεκτρονικού εμπορίου και δεν δίνουν αρκετή προσοχή στην ασφάλεια," λέει ο Elias Levy, ανώτερος υπάλληλος τεχνολογίας της εταιρίας Security Focus., μιας εταιρίας ασφάλειας πληροφοριών Δικτύου στο SAN Mateo,στην Καλιφόρνια.

Μια λιγότερο περίπλοκη μέθοδος κλοπής αριθμών καρτών είναι τα πολλά προγράμματα λογισμικού, που βρίσκονται ελεύθερα στο Δίκτυο, τα οποία παράγουν τους αριθμούς χρησιμοποιώντας τους ίδιους αλγορίθμους με εκείνους που χρησιμοποιούνται από τις τράπεζες. Καθένας με μέτριες δεξιότητες υπολογιστών μπορεί να παραγάγει μέχρι 999 αριθμούς καρτών από μια κάρτα, λέει ο Mark Batts, ειδικός πράκτορας της μονάδας καταπολέμησης της απάτης χρηματοδοτικών οργανισμών του FBI. Νωρίς πέρυσι, η ομοσπονδιακή εμπορική Επιτροπή χρέωσε διάφορα άτομα και επιχειρήσεις με τους παράλογους λογαριασμούς 783.947 και

χρέωσε λογαριασμούς καρτών παράνομα για υπηρεσίες Διαδικτύου. Πώς οι επιχειρήσεις πήραν τις πληροφορίες; Από μια τράπεζα που τους πώλησε τους αριθμούς.

Φυσικά, οι κλέφτες αποκτούν ακόμα τους αριθμούς πιστωτικών καρτών με παραδοσιακούς τρόπους, όπως η παράνομη διείσδυση και κλοπή του ηλεκτρονικού ταχυδρομείου. Ο ομοσπονδιακός νόμος ορίζει το παθητικό από πιστωτικές κάρτες σε $50 από ψευδείς δαπάνες. Με μια πιστωτική κάρτα, δεν είναι τα χρήματά σας σε κίνδυνο. Αλλά εάν κάποιος χρησιμοποιεί τον αριθμό χρεωστικών καρτών σας, τα κεφάλαια λογαριασμού σας, οι αποταμιεύσεις ή ο λογαριασμός μεσιτειών –οπουδήποτε κι αν είναι ο αριθμός –μπορεί να αποσυρθεί. Και η γραμμή πίστωσής σας είναι επάνω για κλοπή επίσης. Εν τω μεταξύ, οι επιταγές δε γίνονται δεκτές ανεπαρκείς λογαριασμοί συσσωρεύονται και αφήνεστε να περιορίσετε τη ζημία.

Μια τέτοια δυσάρεστη κατάσταση μπορεί να δημιουργήσει συναισθηματικές απώλειες. Η τράπεζα της Foote Leitha δεν έφερε αντιρρήσεις, όταν απέσυρε κάποιος $192 τον περασμένο μήνα από τον λογαριασμό ελέγχου της γυναίκας του Ντάλας χρησιμοποιώντας τον αριθμό χρεωστικών καρτών της. Επέστρεψε τα χρήματα αμέσως σε αναμονή μιας έρευνας, ακύρωσε την κάρτα. "Δεν έχω ιδέα πώς οποιοσδήποτε μπορεί να πάρει αλλιώς τον αριθμό καρτών, "λέει η Foote. "Αισθάνομαι πολύ παραβιασμένη." Συνεπώς, η Foote εξετάζει τώρα τη φρόνηση μιας χρεωστικής κάρτας, την οποία επιθυμούσε για να πληρώνει τους μηνιαίους λογαριασμούς. "Αυτό με έχει κάνει πραγματικά να ξανασκέφτομαι, εάν πρόκειται να συνεχίσω εκείνο τον άνετο τρόπο ζωής," λέει η Foote.

Η παρεμπόδιση των ανιχνευτών από το να ρίξει τα δίχτυα του στον αριθμό καρτών σας είναι πολύ πιο δύσκολη από τη προστασία του πλαστικού. "Δεν υπάρχουν πολλά που ο καταναλωτής μπορεί να κάνει," λέει η Wesley Wilhelm, μια διευθύνων σύμβουλος του eHNC, ενός υποκαταστήματος λογισμικού HNC, βοηθού έρευνας και παρεμπόδισης της απάτης στο Σαν Ντιέγκο. Ακόμα, οι καταναλωτές πρέπει να είναι προσεκτικοί στην αποκάλυψη του αριθμού καρτών τους –να μη τη δίνουν ποτέ σε κάποιον που υποστηρίζει ότι είναι, για παράδειγμα, ο τραπεζίτης σας, ή σε ένα δίκτυο που εμφανίζεται ανεπαρκές στην ασφάλειά του[48].

2.8.- Μηχανές Αυτόματων Συναλλαγών (ATM)

Τα ATMs διατρέχουν τον ίδιο κίνδυνο με τον πελάτη που φέρνει τις κάρτες του στις μηχανές, μερικές φορές, σε επικίνδυνες θέσεις όπου με πολλά τεχνάσματα και μηχανές αποσπούν την κάρτα του προσώπου ενώ ο δράστης προσπαθεί να ανακαλύψει το PIN τους (προσωπικός αριθμός αναγνώρισης). Ένα πρόγραμμα έχει αναπτυχθεί για να προστατεύσει τους πολίτες και για να τους ενημερώσει για τη σωστή χρησιμοποίηση των ATM. Ο αρχικός στόχος του προγράμματος πρόληψης εγκλήματος στα ATM είναι η ασφάλεια των χρηστών. Λόγω των έντονων προσπαθειών συνειδητοποίησης και πρόληψης των χρηστών, μια πρόσφατη έρευνα έδειξε ότι τα περιστατικά εγκλήματος στα ATM παρουσιάζουν μια πτωτική τάση. Εξαιτίας της ποικιλίας ATMs, των μοναδικών χαρακτηριστικών κάθε εγκατάστασης, και των εκτιμήσεων εγκλήματος σε κάθε θέση, ούτε ένας τύπος δεν μπορεί να εγγυηθεί την ασφάλεια των πελατών του ATM. Επομένως, είναι απαραίτητο για τους πελάτες του ATM να εξετάζουν τον περιβάλλοντα χώρο γύρω από κάθε ATM και τις διάφορες διαδικασίες για ασφάλεια κατά τη χρησιμοποίησή του ATM .

---

[48]Margaret Mannix, High-tech card fraud goes on right behind your back, 2002, on the web at: http://www.usnews.com/usnews/nycu/money/articles/000214/nycu/credit.htm

Οι εγκληματίες επιλέγουν τα θύματα και τους στόχους τους, εστιάζοντας στους απληροφόρητους ή απροετοίμαστους. Οι εγκληματίες έλκονται επίσης από τις περιβαλλοντικές συνθήκες που ενισχύουν την ευκαιρία να ολοκληρωθεί επιτυχώς το έγκλημά τους. Η στάση και η συμπεριφορά που εκφράζεται μπορούν να έχουν μια τεράστια επίδραση στους πιθανούς δράστες. Υπάρχουν διάφορα πράγματα που μπορείτε να κάνετε για να αυξήσετε την προσωπική ασφάλειά σας και να μειώσετε τον κίνδυνο να πέσετε θύμα εγκλήματος σε ATM[49].

Περιληπτικά μερικές οδηγίες για την περίπτωση συναλλαγής μέσω ATM είναι, αρχικά να απομνημονευθεί ο προσωπικός αριθμός αναγνώρισής σας (PIN). Μην τον γράψτε ή μην τον κρατήστε στο πορτοφόλι ή στη τσάντα σας. Μην πείτε σε οποιονδήποτε άλλο το PIN συμπεριλαμβανομένων των υπαλλήλων τραπεζών, της αστυνομίας κ.λπ. .Να προστατεύετε το αριθμητικό πληκτρολόγιο του ATM από καθένα που μπορεί να στέκεται κοντά ή που σας πλησιάζει σε μία προσπάθεια να δει το PIN ή /και τη συναλλαγή σας. Χρησιμοποιήστε το σώμα σας ως ασπίδα εάν είναι απαραίτητο ενώ πληκτρολογείτε τον κωδικό πρόσβασής σας και σιγουρευτείτε ότι κρατάτε την απόδειξη της συναλλαγής σας . Μην πετάξτε την απόδειξη κοντά στον τόπο του ATM. Αυτό το λεπτομερές άρθρο γνωστοποιεί τους κανονισμούς για την ασφάλεια που πρέπει να ακολουθηθούν ανεξάρτητα από το πόσο ασφαλές εσείς θεωρείτε το ATM, επειδή μετά από την προσωπική ασφάλειά σας, η οικονομική ασφάλειά σας είναι επίσης σημαντική[50].

Εκτός από τη χρήση και σκληρών και μαλακών-ρυθμιστικών προσεγγίσεων, πολλά μπορούν να επιτευχθούν μέσω των στρατηγικών αυτοβοήθειας που στοχεύουν να προειδοποιήσουν τους χρήστες στην παρουσία παραπλανητικών πρακτικών για να μπορούν να αποφύγουν τη δίωξη. Τέτοια προληπτική δράση μπορεί να λάβει τη μορφή κανονικής επιτήρησης του Διαδικτύου προκειμένου να βρεθούν οι απαράδεκτες και παράνομες πρακτικές, παρέχοντας εκπαιδευτικό υλικό που προειδοποιεί τους χρήστες για τα επικίνδυνα σχέδια και χρησιμοποιεί την τεχνολογία επικύρωσης για να επιτρέψει στα άτομα να γνωρίζουν με βεβαιότητα με ποιόν σχετίζονται μέσω Διαδικτύου.

2.9.- Ξέπλυμα χρημάτων

Εξ ορισμού, περιγράφεται ως "συμπεριφορά ή ενέργεια σχεδιασμένη γενικά ή εν μέρει για να κρύψει ή να μεταμφιέσει τη φύση, τη θέση, την πηγή, την ιδιοκτησία ή τον έλεγχο των χρημάτων (μπορεί να είναι νόμισμα ή ισοδύναμα, π.χ. επιταγές, ηλεκτρονικές συναλλαγές, κ.τ.λ.) για να αποφύγει μια απαίτηση για την υποβολή εκθέσεων συναλλαγής από το κράτος ή τον ομοσπονδιακό νόμο ή για να παραποιήσει το γεγονός ότι τα χρήματα αποκτήθηκαν με παράνομα μέσα"[51]. Το ξέπλυμα χρημάτων περιλαμβάνει το κρύψιμο, τη διακίνηση, και την επένδυση των εισπράξεων της εγκληματικής συμπεριφοράς. Ακόμη και τα νόμιμα χρήματα μπορούν να γίνουν παράνομα, παραδείγματος χάριν, εάν διακινούμενα παραβιάζουν τους ελέγχους ξένου-συναλλάγματος μιας χώρας ή άλλους οικονομικούς κανονισμούς. Παραδείγματος χάριν, όλες οι συναλλαγές ξένου συναλλάγματος από τη Μαλαισία πρέπει να αναφερθούν στην τράπεζα Negara Μαλαισία, την κεντρική

---

[49] The National Fraud Information Center, ATM Safety & Security Tips, web article, 2001 at: ttp://www.lapdonline.org/bldg_safer_comms/prevention/personal_safety/ATM.htm.

[50] The National Fraud Information Center, ATM Safety & Security Tips, web article, 2001 at: ttp://www.lapdonline.org/bldg_safer_comms/prevention/personal_safety/ATM.htm.

[51] The Lectric Law Library's Lexicon on Money Laundering. Web dictionary, April 2002 at: http://www.lectlaw.com/def2/m038.htm.

τράπεζα. Αλλίώς, καθίσταται το εξαγόμενο ποσό παράνομο. Τα καθαρά χρήματα μπορούν επίσης να παράγουν τα βρώμικα χρήματα μέσω της φορολογικής διαφυγής. Η έκθεση της υποεπιτροπής της Αμερικάνικης Συγκλήτου με τίτλο 'ανταποκρίτρια τράπεζα: μια πύλη για το ξέπλυμα χρημάτων', δημοσιευμένη το Φεβρουάριο 2001, ανέφερε τα παραδείγματα των ανθρώπων που τοποθέτησαν ποσά μεγαλύτερα από $100.000 σε μια τράπεζα των Νήσων Καίημαν χωρίς πληρωμή του φόρου για εκείνα τα χρήματα.

2.9.1.- Επιπτώσεις στην οικονομία

Οι δραστηριότητες αυτές αποτελούν μια άνευ προηγουμένου επίθεση κατά της διεθνούς κοινωνικής τάξης και εν δυνάμει του οικονομικού και χρηματοπιστωτικού συστήματος του δημοκρατικού κόσμου[52]. Ακόμα κι αν τα ίδια τα χρήματα κερδήθηκαν σύμφωνα με το νόμο, τα ποσά που έπρεπε να έχουν καταβληθεί στους φόρους θεωρούνται παράνομα. Κατά γενικό κανόνα, το ξέπλυμα χρημάτων βλάπτει την κοινωνία τροφοδοτώντας το οικονομικό έγκλημα, και το οικονομικό έγκλημα έχει επιπτώσεις σε όλους. Ως αποτέλεσμα της ασφαλιστικής απάτης, όλοι πληρώνουμε περισσότερα για την ασφάλεια. Ως αποτέλεσμα των ληστειών και της απάτης, όλοι λαμβάνουμε λιγότερο τόκο στις καταθέσεις τραπεζών και πληρώνουμε περισσότερο τόκο στα δάνεια. Λόγω της απάτης στην κοινωνική ασφάλιση, άλλα οφέλη, και στις κυβερνητικές επιχορηγήσεις για την ευημερία και την εκπαίδευση, πληρώνουμε περισσότερους φόρους. Πληρώνουμε επίσης περισσότερους φόρους για τις δαπάνες δημόσιων έργων που διογκώνονται από τη διαφθορά. Όσοι από μας πληρώνουν τους φόρους, πληρώνουν περισσότερα από εκείνους που αποφεύγουν τους φόρους. Έτσι όλοι δοκιμάζουμε υψηλότερο κόστος ζωής από ό,τι εάν το οικονομικό έγκλημα, συμπεριλαμβανομένου του ξεπλύματος χρημάτων, είχε αποτραπεί.

2.9.2.- Ξέπλυμα χρημάτων στο Διαδίκτυο

Η κοινή παρατήρηση ότι το Διαδίκτυο παρέχει νέες και μη ανιχνεύσιμες μεθόδους ξεπλύματος χρημάτων δεν έχει καμία θέση στη σοβαρή εκτίμηση κοινών σημείων μεταξύ του ξεπλύματος χρημάτων και της τεχνολογίας. Εξάλλου, δεν υπάρχει άμεση αντιστοιχία ή ευθεία σχέση αιτίου (τεχνολογία) – αποτελέσματος (έγκλημα) μεταξύ τους[53]. Στην ουσία, το Διαδίκτυο δεν είναι τίποτα περισσότερο από ένα σύστημα μηνυμάτων. Για να διακινήσουν τα χρήματα, οι τράπεζες διακινούν τις πληροφορίες μέσω οποιουδήποτε διαθέσιμου συστήματος μηνυμάτων κινώντας πλάκες χρυσού από μια θέση σε άλλη κατά τη διεξαγωγή ελέγχων. Σε αυτό το πλαίσιο, το Διαδίκτυο είναι απλά ένα ενημερωμένο σύστημα ελέγχου ή ένας αποδοτικότερος, φτηνότερος, και ασφαλέστερος τρόπος διακίνησης οικονομικών πληροφοριών. Ο προσδιορισμός των πελατών είναι το αρχικό πρόβλημα που προκύπτει από τη χρήση Διαδικτύου, και εκείνο το πρόβλημα είναι ακριβώς το ίδιο με οποιαδήποτε σχέση που διεξάγεται από απόσταση. Εντούτοις, μερικοί χρησιμοποιούν το ξέπλυμα χρημάτων μέσω Διαδικτύου ως δικαιολογία για να κινηθούν προς πιο εκτενείς ρυθμίσεις του Διαδικτύου. Ακόμα κι αν ήταν δυνατό να δημιουργηθεί ο αποτελεσματικός κανονισμός του Διαδικτύου, μια τέτοια επιχείρηση θα μεγάλωνε τα εμπόδια για την είσοδο των φτωχών εθνών. Το Διαδίκτυο μπορεί να ωφελήσει μεγάλα μέρη του κόσμου με χαμηλότερο κόστος με τη μείωση της απομόνωσης και παρέχοντας στις μακρινές κοινότητες τη δυνατότητα να παρέχουν υπηρεσίες και να δημοσιεύουν καταλόγους

---

[52] Ι.Φαρσεδάκης, Ναρκωτικά, Νομική κ΄ Εγκληματολογική διάσταση στην Ελλάδα και στην Ευρωπαϊκή Ένωση.,Νομική Βιβλιοθήκη, Αθήνα 1996, σ. 540.
[53] Γ.Λάζος., Πληροφορική και Έγκλημα, Νομική Βιβλιοθήκη, 2001, σ.31.

τοπικών αγαθών. Αυστηρότερος κανονισμός θα επιδείνωνε μόνο τη "ψηφιακή διαίρεση" μεταξύ των πλούσιων και αναπτυσσόμενων οικονομιών[54].

Στο ανωτέρω απόσπασμα ο Nigel Morris-Cotterill, είναι πολύ δύσπιστος στην ιδέα της χρήσης της τεχνολογίας για να ξεπλύνει τα χρήματα δεδομένου ότι η πρωταρχική περίπτωση στα μάτια του περιλαμβάνει εξ ορισμού τη φυσική ύπαρξη μιας τράπεζας. Αυτό ισχύει κατά γενικό κανόνα, δεδομένου ότι οι τράπεζες αποτελούν την πρωταρχική ανησυχία όσον αφορά αυτή την εγκληματική δραστηριότητα αλλά εξαιτίας του ότι όλο και περισσότερες τράπεζες και χρηματοδοτικοί οργανισμοί προσφέρουν τις υπηρεσίες τους στο Διαδίκτυο ή μέσω κάποιας μορφής ηλεκτρονικού μέσου, η τεχνολογία που χρησιμοποιείται για να προσδιορίσει και να επικυρώσει τους πελάτες μπορεί να παραβιαστεί ακριβώς όπως οποιαδήποτε βασισμένη στο Διαδίκτυο ασφάλεια. Αν και οι απόψεις του για την κατάσταση είναι πρωταρχικής ανησυχίας στις οργανώσεις που προσπαθούν να αποτρέψουν αυτό το σενάριο, όταν δηλώνει: "Ο προσδιορισμός των πελατών είναι το αρχικό πρόβλημα που προκύπτει από τη χρήση Διαδικτύου, και εκείνο το πρόβλημα είναι ακριβώς το ίδιο με οποιαδήποτε σχέση που διεξάγεται από μια απόσταση", οι απάτες ταυτότητας είναι ένας κάπως ξεχωριστός τομέας . Το ξέπλυμα χρημάτων στο Διαδίκτυο περιλαμβάνει τη φυσική ύπαρξη των χρυσών ράβδων ή των μετρητών λόγω της εμφάνισης e-Cash (επίσης καλούμενο cyber - μετρητά). Στον εικονικό κόσμο του κυβερνοχώρου η απαίτηση για τις αποδοτικές καταναλωτικές συναλλαγές έχει το προβάδισμα στην καθιέρωση των ηλεκτρονικών μετρητών. Τα ηλεκτρονικά μετρητά ή τα ψηφιακά χρήματα, είναι μια ηλεκτρονική αντικατάσταση για τα μετρητά. Τα ψηφιακά μετρητά έχουν οριστεί ως μια σειρά αριθμών που έχουν μια εγγενή αξία με κάποια μορφή νομίσματος. Χρησιμοποιώντας τα ψηφιακά μετρητά, τα πραγματικά προτερήματα μεταφέρονται μέσω των ψηφιακών επικοινωνιών υπό μορφή χωριστά προσδιορισμένων αντιπροσωπειών των λογαριασμών και των νομισμάτων, παρόμοιων με τους αύξοντες αριθμούς στο μεταλλικό νόμισμα. Ενώ ο τελευταίος στόχος κάθε προμηθευτή είναι να διευκολύνει την απόδοση των συναλλαγών , να υποστηρίξει την αγοραστική δύναμη στο Διαδίκτυο, και φυσικά να κερδίσει το ουσιαστικό κέρδος σε έναν νέο τομέα του εμπορίου, κάθε προμηθευτής παίζει με ελαφρώς διαφορετικούς κανόνες. Αν και οι διαπλοκές των μεμονωμένων προμηθευτών είναι αρκετά συναρπαστικές, με σκοπό αυτό το άρθρο, είναι δίκαιο να ειπωθεί ότι όλοι οι προμηθευτές έχουν ένα κοινό γνώρισμα ,την έλλειψη ανωνυμίας.

2.9.3.- Μεταφορές καλωδίων

Δεδομένου ότι ο φυσικός κόσμος του ξεπλύματος χρημάτων άρχισε να διαβρώνεται, η τάση να χρησιμοποιηθούν οι ηλεκτρονικές μεταφορές για να αποφευχθεί η ανίχνευση κέρδισε πιστούς οπαδούς. Οι ηλεκτρονικές μεταφορές των κεφαλαίων είναι γνωστές ως μεταφορές καλωδίων. Τα συστήματα μεταφοράς καλωδίων επιτρέπουν στις εγκληματικές οργανώσεις καθώς επίσης και στις νόμιμες επιχειρήσεις και τους μεμονωμένους τραπεζικούς πελάτες, να απολαύσουν έναν άμεσο και σχεδόν ακίνδυνο αγωγό για την διακίνηση των χρημάτων μεταξύ των χωρών. Θεωρώντας ότι κατ' εκτίμηση 700.000 μεταφορές εμφανίζονται καθημερινά στις Ηνωμένες Πολιτείες, που διακινούν καλά πάνω από $2 τρισεκατομμύρια, οι παράνομες μεταφορές είναι εύκολα κρυμμένες. Οι ομοσπονδιακές αντιπροσωπείες υπολογίζουν ότι τουλάχιστον $300 δισεκατομμύρια ξεπλένονται ετησίως, παγκοσμίως. Καθώς ο όγκος των αποθηκευμένων αυτοματοποιημένων

[54] Nigel Morris-Cotterill, How Not to Be a Money Launderer, 2nd edition (Brentwood: Silkscreen Publications, 1999).

πληροφοριών σχετικά με αυτές τις μεταφορές φθάνει στα ύψη, η δυνατότητα επιτυχούς ξεπλύματος αυξάνεται καθώς επίσης και ο φόρτος εργασίας των ανακριτών. Αν και οι μεταφορές παρέχουν αυτήν την περίοδο μόνο περιορισμένες πληροφορίες σχετικά με τα ενδιαφερόμενα μέρη, η αυξανόμενη τάση είναι να καταγράφονται περισσότερες λεπτομέρειες. Εάν η μυστικότητα των μεταφορών καλωδίων συμβιβάζεται, λόγω των καταπιεστικών και λεπτομερών κανονισμών τήρησης αρχείων, της ηλεκτρονικής επιτήρησης των μεταφορών ή άλλης ενδεχομένως τακτικής εισβολής, κατόπιν το πέρασμα από το φυσικό στον εικονικό κόσμο θα είναι σχεδόν πλήρες. Εάν το ξέπλυμα πρόκειται να επιζήσει, πρέπει να επεκτείνει το στόχο του και να εισχωρήσει στον κόσμο του κυβερνοχώρου.

2.9.3.1.- Συστήματα ηλεκτρονικής μεταφοράς κεφαλαίων

Τα διάφορα συστήματα αναπτύσσονται, για να επιτρέψουν στους πελάτες, τις τράπεζες, και τους εμπόρους να επικοινωνήσουν ασφαλώς ο ένας με τον άλλον. Διάφορα ηλεκτρονικά συστήματα μεταφοράς κεφαλαίων λειτουργούν ήδη σε όλο τον κόσμο ως υποκατάστατα των σε χαρτί συναλλαγών επιταγών και αυτά θα μπορούσαν καλά να προσαρμοστούν στη χρήση Διαδικτύου.

i. GIRO SYSTEM. Το GIRO σύστημα του Ηνωμένου Βασιλείου, παραδείγματος χάριν, ωφελείται από την παρεμπόδιση της απάτης επιταγών, επειδή η διαταγή πληρωμής κατευθύνεται στον τραπεζίτη άμεσα παρά μέσω του δικαιούχου πληρωμής. Στο GIRO σύστημα, το πρόσωπο που επιθυμεί να κάνει μια πληρωμή, ο πληρωτής, καθοδηγεί την τράπεζά του /της σχετικά με τις λεπτομέρειες της πληρωμής και τα κεφάλαια μεταφέρονται ηλεκτρονικά από τον λογαριασμό του πληρωτή στον λογαριασμό του δικαιούχου πληρωμής. Αυτά τα συστήματα δημιουργούν έναν κίνδυνο ασφάλειας, εάν οι διαδικασίες δεν είναι σε θέση να ελέγξουν τη διαθεσιμότητα των κεφαλαίων που πρόκειται να μεταφερθούν ή εάν οι έλεγχοι πρόσβασης λογαριασμού δεν είναι σε ισχύ. Υπάρχει επίσης η δυνατότητα κακού χειρισμού των πληροφοριών καθώς περνούν μέσα από το δίκτυο σε κρυπτογραφημένη μορφή.

ii. ΗΛΕΚΤΡΟΝΙΚΑ ΔΙΚΤΥΑ ΜΕΤΑΦΟΡΑΣ ΚΕΦΑΛΑΙΩΝ (EFT). $2 τρισεκατομμύρια έως $3 τρισεκατομμύρια ημερησίως διακινούνται σε όλη την υδρόγειο μέσα από τα ηλεκτρονικά δίκτυα μεταφοράς κεφαλαίων (EFT)[55], ένα μεγάλο μέρος του οποίου γίνεται μέσω των διαποδιαμορφωτών και μέσα από τις τηλεφωνικές γραμμές. Υπάρχουν δύο είδη δικτύων EFT που απαιτούν κάπως διαφορετικές διαδικασίες ασφάλειας: Δίκτυα μεταφοράς καλωδίων σε πραγματικό χρόνο, όπου οι συναλλαγές είναι οριστικές τη στιγμή που απελευθερώνονται και επεξεργάζονται σε ποσότητα και αυτοματοποιημένες πληρωμές της επόμενης μέρας γραφείων συμψηφισμού (ACH), όπου οι ψευδείς συναλλαγές μπορούν να αντιστραφούν, εάν γίνουν αντιληπτές εντός ενός περιορισμένου χρονικού διαστήματος. Επειδή τα καλώδια είναι ο παραδοσιακός φορέας EFT της επιλογής για τις συναλλαγές πολλών δολαρίων που απαιτούν την επικαιρότητα και τη βεβαιότητα της πληρωμής, και επειδή είναι αμετάκλητα, η ασφάλεια συνήθως θα είναι ιδιαίτερα σφιχτή γύρω από τα τερματικά και τις διαδικασίες έναρξης καλωδίων. Οι περισσότερες επιχειρήσεις υποστηρίζουν ότι δεν είχαν καμία απώλεια λόγω απάτης ή λάθους του EFT. Αλλά οι ειδικοί υποπτεύονται ότι δεν λένε όλοι την αλήθεια. "Σκεφτόμαστε ότι τα δίκτυα EFT είναι πολύ ασφαλή, αλλά δεν είμαστε βέβαιοι πόσο ασφαλή," σημειώνει ο Ντάγκλας Graham, συνεργάτης στην εξάσκηση ηλεκτρονικού εμπορίου KPMG της Peat Marwick στη Νέα Υόρκη. "Η υποψία είναι ότι υπάρχουν περισσότερες απώλειες από αυτές που αναφέρονται. Οι επιχειρήσεις δεν

---

[55] Γ.Λάζος., Πληροφορική και Έγκλημα, Νομική Βιβλιοθήκη, 2001, σ.124.

θέλουν κακές ειδήσεις να υπονομεύουν την εμπιστοσύνη και ίσως να τους αναγκάσουν να χάνουν τους πελάτες και έτσι δέχονται την απώλεια και δεν λένε ποτέ τίποτα για αυτήν[56]."

Ενώ σχεδόν όλες οι εταιρίες ασφαλίζονται ενάντια στις απώλειες απάτης, πολλές εταιρίες δεν θα αναφέρουν τις λιγότερο καταστροφικές απώλειες, επειδή δεν θέλουν οι ασφαλιστικές εταιρείες τους να ξέρουν για τις διαρροές στην εσωτερική ασφάλεια, εν μέρει επειδή ο ασφαλιστής ίσως χρησιμοποιήσει τις πληροφορίες, για να αρνηθεί την κάλυψη ή να αυξήσει τα ασφάλιστρα, εξηγεί.

Αυτή η εντυπωσιακή ανασκόπηση παρουσιάζει διάφορες πρόσφατες θέσεις που διαχειρίζονται ευαίσθητες διαδικασίες EFT που μπορεί να ανήκουν σε έναν υποσχόμενο υπάλληλο ή σε κάποιον που έχει απολυθεί ήσυχα επειδή είχε εξαπατήσει προηγούμενους εργοδότες. Μόλις το EFT ασφαλώς ενεργοποιηθεί από το εξουσιοδοτημένο προσωπικό, πρέπει να διασχίσει μια τηλεφωνική γραμμή και τους διαποδιαμορφωτές σε κάθε άκρη. Έτσι η ίδια η διαδικασία μετάδοσης πρέπει να εξασφαλιστεί, από την κρυπτογράφηση, η οποία μεταφράζει το μήνυμα έναρξης EFT στο δυσανάγνωστο κώδικα για να αποτρέψει οποιοδήποτε μέρος από την παρεμπόδιση και την ανάγνωση του κατά τη διάρκεια της διαδικασίας. Μόλις φθάσει ακίνδυνα στην τράπεζα, αποκρυπτογραφείται και ενεργοποιείται . Η διαδικασία κρυπτογράφησης / αποκρυπτογράφησης εκτελείται από τις μηχανές και έτσι ούτε ο τραπεζίτης ούτε ο διευθυντής χρηματοδότησης της επιχείρησης δεν γνωρίζει πώς να τη χρησιμοποιήσει, μόνο αν είναι αρμόδιο να δει ότι είναι σε ισχύ.

Η κρυπτογράφηση βεβαιώνει ότι το περιεχόμενο του μηνύματος πληρωμής θα παραμείνει εμπιστευτικό. Μια συμπληρωματική διαδικασία γνωστή ως επικύρωση βεβαιώνει την τράπεζα ότι το μήνυμα προήλθε από το νόμιμο ιδιοκτήτη του λογαριασμού από τον οποίο θα καταβληθούν τα κεφάλαια και ότι το μήνυμα δεν έχει πειραχτεί κατά τη διάρκεια της διαδικασίας μετάδοσης. Τα μέτρα ασφάλειας είναι σημαντικά και για την προστασία του EFT και για να καθορίσουν ποιος είναι εκτεθειμένος εάν κάτι πάει στραβά. Σύμφωνα με τον Ενιαίου Εμπορικού Κώδικα[57] (UCC), οι τράπεζες μπορούν τώρα να απαλλαχθούν της νομικής ευθύνης για τα σφάλματα του EFT εάν παρέχει την "εμπορικά λογική ασφάλεια," που αφήνεται εσκεμμένα ασαφής, ώστε ο καθορισμός να μπορεί να καλύψει πολλές περιστάσεις. Αλλά το UCC ρητά δηλώνει ότι απλά η απαίτηση για κωδικούς πρόσβασης δεν μπορεί να αποτελέσει την εμπορικά λογική ασφάλεια. Οι τράπεζες πρέπει να προσφέρουν σωστά μέτρα ασφάλειας, διαφορετικά θα θεωρηθούν υπεύθυνες για τις συνέπειες της ανεπαρκούς ασφάλειας. Οι επιχειρήσεις δεν απαιτούνται να τους δεχτούν, αλλά αν παραμερίσουν τα διαθέσιμα μέτρα ασφάλειας μιας τράπεζας σημαίνει ότι αναλαμβάνουν την ευθύνη για τα πράγματα που πηγαίνουν στραβά.

2.10.- Πειρατεία λογισμικού

Η προστασία πνευματικών δικαιωμάτων δεν περιορίζεται μόνο στα βιβλία, τα τραγούδια και τις κινηματογραφικές ταινίες. Περιλαμβάνει πολλούς τύπους δημιουργικών εργασιών, συμπεριλαμβανομένου του λογισμικού υπολογιστών. Αυτό σημαίνει ότι ο ιδιοκτήτης των πνευματικών δικαιωμάτων έχει δικαίωμα να πει πώς και κάτω από ποιες περιστάσεις το λογισμικό μπορεί να αναπαραχθεί, διανεμηθεί και εγκατασταθεί. Ο "ιδιοκτήτης" των πνευματικών δικαιωμάτων είναι συνήθως ο εκδότης λογισμικού. Δεν γίνεσαι ο ιδιοκτήτης πνευματικών δικαιωμάτων με την αγορά ενός αντιγράφου ενός πακέτου λογισμικού. Αντ' αυτού, όταν αγοράζετε το λογισμικό, αγοράζετε το δικαίωμα να το χρησιμοποιήσετε, κάτω από ορισμένους περιορισμούς

---

[56] Richard H. Gamble, Short Circuiting Wire Transfer Fraud, 2001.
[57] άρθρο 4^A του Ενιαίου Εμπορικού Κώδικα (UCC4A).

που επιβάλλονται από τον ιδιοκτήτη πνευματικών δικαιωμάτων. Γενικά, τα ακριβή δικαιώματα που αγοράζετε περιγράφονται στην άδεια ή άλλη τεκμηρίωση που συνοδεύει το λογισμικό. Εάν αντιγράφετε, διανείμετε ή εγκαταστήσετε το λογισμικό με τρόπο που η άδεια δεν επιτρέπει, παραβιάζετε τον ομοσπονδιακό νόμο πνευματικών δικαιωμάτων. Παραδείγματος χάριν, εάν η άδεια λέει ότι δεν μπορείτε να κάνετε περισσότερο από ορισμένα αντίγραφα, η παραγωγή περισσοτέρων από εκείνο τον αριθμό αντιγράφων είναι μια παραβίαση του νόμου. Ανεξάρτητα από οποιοδήποτε άλλο περιορισμό αντιγραφής, εντούτοις, ο νόμος επιτρέπει σε σας να κάνετε ένα επιπλέον αντίγραφο.

Η παραγωγή αντιγράφων του λογισμικού χωρίς έγκριση είναι μια παραβίαση του νόμου, ανεξάρτητα από το πόσα αντίγραφα κάνετε. Παραδείγματος χάριν, είτε κάνετε μερικά αντίγραφα για τους φίλους ή είστε μια επιχείρηση που αγοράζει ένα αντίγραφο ενός προγράμματος, αλλά το εγκαθιστά σε 100 υπολογιστές, παραβιάζετε ακόμα τον ομοσπονδιακό νόμο εάν δεν έχετε έγγραφη την άδεια να κάνετε εκείνα τα αντίγραφα. Εκτίθεστε στις πιθανές αστικές και εγκληματικές ποινικές ρήτρες. Με άλλα λόγια, μπορείτε να μηνυθείτε από τον ιδιοκτήτη πνευματικών δικαιωμάτων και να θεωρηθείτε υπεύθυνοι για ζημίες χρημάτων ή η κυβέρνηση θα μπορούσε να σας χρεώσει με ένα ποινικό αδίκημα.

Παρά τους ισχυρότερους νόμους και την επιβολή τους, η πλαστογράφηση λογισμικού επιδεινώνεται από την Ασία, στη Νότια Αμερική και στην Ανατολική Ευρώπη. Η αστραπιαία αύξηση της οικονομίας υψηλής τεχνολογίας έχει οδηγήσει σε μια έντονη σφαιρική απαίτηση για το λογισμικό επιχειρήσεων και καταναλωτών, είτε γνήσιο είτε πλαστό. Και η πλαστογράφηση λογισμικού — που τροφοδοτείται από το Διαδίκτυο, το οργανωμένο έγκλημα και τη διαφθορά στον Τρίτο Κόσμο — έχει γίνει βιομηχανία πολλών δισεκατομμυρίων δολαρίων.

Οι επιχειρήσεις λογισμικού εκτιμούν ότι έχασαν 12 δισεκατομμύρια δολάρια στις εισπράξεις τους πέρυσι λόγω της πλαστογράφησης. Αυτό αντιστοιχεί σε 15% των 80 δισεκατομμυρίων δολαρίων παγκόσμιων πωλήσεων. Οι απώλειες θα αυξηθούν, προειδοποιούν, καθώς οι οικονομίες Τρίτων Χωρών ορμούν στην εποχή υψηλής τεχνολογίας,. Το ζήτημα έχει γίνει ένα τεράστιο σημείο διαπραγμάτευσης[58] στις εμπορικές συνθήκες με τις χώρες από το Βιετνάμ ως την Ιορδανία. Οι εμπειρογνώμονες επιβολής υψηλής τεχνολογίας και νόμου προειδοποιούν ότι εάν το πρόβλημα επεκταθεί, θα περιορίσει την ανάπτυξη της κυρίαρχης βιομηχανίας λογισμικού των ΗΠΑ.

2.10.1.- Πειρατεία στα παιχνίδια

Μια πειρατική οργάνωση είναι η οργάνωση που κλέβει κατοχυρωμένα υλικά και αναπαράγει αυτά τα υλικά έτσι ώστε να μπορούν να πωληθούν και να αποφέρουν κέρδος. Στη σφαίρα του NES, ο όρος "πειρατής" χρησιμοποιείται συνήθως σχετικά με το λογισμικό που κλέβεται από μια άλλη επιχείρηση, ελαφρώς διασκευασμένο και σε κυκλοφορία με άλλη μορφή. Εντούτοις, οι επιχειρήσεις πειρατών παράγουν επίσης το μηχανικό μέρος υπολογιστικού συστήματος που κλέβει πληροφορίες σχεδίου υπό μορφή συστημάτων "κλώνων", όπως είναι γενικά γνωστά. Τα πειρατικά υλικά είναι παράνομο να κατέχονται επειδή περιέχουν παράνομα αντιγραμμένες πληροφορίες.

---

[58] D.Halber, Computer Technology and Legal Discourse, 1994, at: ftp/pub/subj/law/jnl/elaw/comment/halbert.txt.

Το πειρατικό λογισμικό περιλαμβάνει και τις κασέτες ενιαίου-τίτλου και τις κασέτες πολλαπλών-τίτλων, που αναφέρονται συνήθως ως "multicarts. "Πολλά multicarts καυχώνται τα γελοία ποσά παιχνιδιών, όπως" 1.000.000 στο 1 "και υψηλότερα, αλλά στην πραγματικότητα περιέχουν μόνο 5 ή 6 τίτλους και τις πολυάριθμες αμυχές αυτών των ίδιων παιχνιδιών. Υπάρχουν μερικά multicarts (με τους σημαντικά χαμηλότερους αριθμούς κλεμμένους τίτλους) που έχουν πιο προηγμένα παιχνίδια και πραγματικά σας δίνουν ότι λένε, αλλά η πλειοψηφία των multicarts αποτελείται από διάφορα απλά παιχνίδια και πολλαπλάσιες παρτίδες εκείνων των παιχνιδιών. Ένας άλλος τύπος πειρατικής άμαξας είναι το αρχικό "cart" πειρατών, επίσης γνωστό ως 'άμαξα του Χονγκ-Κονγκ' λόγω της μεγάλης αγοράς πειρατών στην Ασία. Αυτές οι κασέτες περιέχουν τα παιχνίδια που είτε δεν εκδόθηκαν ποτέ για τα NES ή που είναι δημιουργίες της συγκεκριμένης οργάνωσης πειρατών. Αυτά τα παιχνίδια εξετάζονται ακόμα ως πειρατικά, επειδή περιέχουν πληροφορίες που είναι από κάποιο άλλο. Τα παραδείγματα των αρχικών παιχνιδιών του Χονγκ-Κονγκ είναι: Somari, Sonic ο πειρατής των σκαντζόχοιρων με τα ξωτικά του 'Mario' αντί του Sonic, ο Μαχητής Kart, ένας κακός κλώνος του μαχητή II με χαρακτήρες της σειράς του Mario, Mortal Kombat VI-30 Peoples, ένας κλώνος των παιχνιδιών Mortal Combat.

Τα πειρατικά συστήματα "κλώνων" έχουν γίνει πιο παραγωγικά από το τέλος της ενεργού διάρκειας ζωής του NES, με πολλές οργανώσεις στις αγορές πειρατών τώρα που κατασκευάζουν τα δικά τους συστήματα κλώνων. Οι κλώνοι έρχονται σε όλα τις μορφές, τα μεγέθη και τα χρώματα και είναι (γενικά) αρκετά φτωχά κατασκευασμένοι. Μερικά συστήματα κλώνων έρχονται με τα παιχνίδια που ενσωματώνονται ήδη, ενώ μερικά συστήματα σας άφησαν να παρεμβάλετε τα 'cart' όπως σε ένα κανονικό σύστημα. Πολλοί κλώνοι που έρχονται με έναν σταθερό αριθμό παιχνιδιών σχεδιάζονται για να μοιάσουν με τους ελεγκτές των πιο σύγχρονων συστημάτων.

2.10.1.1.- Τρόποι εξακρίβωσης πειρατικών κασετών

Οι πειρατικές οργανώσεις λογισμικού επιλέγουν μερικές φορές να κρατήσουν τις ταυτότητές τους απολύτως άγνωστες έτσι ώστε να είναι δυσκολότερο να ανακαλυφθούν και να επισημανθούν οι παράνομες δραστηριότητές τους, αλλά μερικές ομάδες πειρατών είναι οργανωμένες και έχουν πραγματικά δικές τους ταυτότητες και σχέδια κασετών .Παραδείγματα τέτοιων οργανώσεων περιλαμβάνουν τις : Spica, Supervision, και Whirlwind Manu, οι οποίες τοποθετούν το όνομα της "επιχείρησής τους" στις ετικέτες των κασετών τους. Εντούτοις, ακριβώς επειδή μια ομάδα πειρατών δεν βάζει το όνομά τους στην κασέτα, είναι ακόμα συνήθως εύκολο να επισημανθεί ένα παιχνίδι πειρατών εάν ξέρετε τι να ψάχνετε. Εάν υπάρχουν εικόνες των πραγμάτων από τα πολλά παιχνίδια (όπως ένας στρατιώτης, ένα μπαλόνι, ένα ξένο διαστημικό σκάφος, ένα περιστέρι, και ένα σχολικό λεωφορείο) όλα στην ίδια ετικέτα, αυτό συνήθως δηλώνει ότι η κασέτα είναι πειρατική, θα μπορούσε ακριβώς να είναι ένα εξαιρετικά παρεκκλιμένο παιχνίδι. Εάν η ετικέτα είναι παραποιημένη και μοιάζει σαν να μεγεθύνθηκε ή αντιγράφηκε από μια άλλη εικόνα, ή εάν δεν υπάρχει κανένα λογότυπο επιχείρησης, κώδικας προσδιορισμού, ή υλικό πνευματικών δικαιωμάτων στην ετικέτα, αυτό επίσης δηλώνει ότι είναι πειρατική κασέτα. Άλλοι τρόποι να καθοριστεί, εάν μια κασέτα είναι πειρατική, είναι να φανεί, εάν η κασέτα χρησιμοποιεί έναν αριθμό ταυτότητας που είναι διαφορετικός από τα κανονικά πρότυπα, να δει εάν οι πληροφορίες πνευματικών δικαιωμάτων στην ετικέτα ισχύουν (όπου εφαρμόσιμες), και να επαληθεύσει με μια γνωστή πηγή, για να καθορίσει, εάν μια εξουσιοδοτημένη έκδοση με αυτόν τον τίτλο έγινε ποτέ. Ακόμα κι αν κάποιο πειρατικό υλικό είναι ενδιαφέρον και με πλοκή ή είναι γελοίο ως χιουμοριστικό, το γεγονός παραμένει

ότι τα πειρατικά υλικά είναι παράνομα και μπορούν να είναι οικονομικά καταστρεπτικά για τους δικαίως εξουσιοδοτημένους παραγωγούς παιχνιδιών και εξοπλισμού[59].

2.11.-Πειρατεία Διαδικτύου

Οι νόμοι πνευματικών δικαιωμάτων παρέχουν μια περιορισμένη μορφή προστασίας για τα λογοτεχνικά, δραματικά και μουσικά έργα παρέχοντας στους δημιουργούς τον αποκλειστικό έλεγχο των διάφορων πράξεων που πραγματοποιούνται σε σχέση με τις εργασίες τους. Αυτά περιλαμβάνουν την αναπαραγωγή, τη δημοσίευση, την απόδοση στο κοινό, τη ραδιοφωνική μετάδοση, την προσαρμογή και τη μετάδοση του υλικού. Οι δημιουργοί των καλλιτεχνικών εργασιών έχουν άλλα δικαιώματα σε σχέση με τις εργασίες τους. Μόνο εκείνες οι διανοητικές παραγωγές που είναι πρωτότυπες προστατεύονται και η προστασία επεκτείνεται μόνο στη μορφή με την οποία μια ιδέα εκφράζεται παρά η ίδια η ιδέα.

Εντούτοις δεν προστατεύονται όλες οι εργασίες , δεδομένου ότι το δόγμα της δίκαιης συναλλαγής επιτρέπει στις εργασίες να χρησιμοποιηθούν υπό ορισμένους όρους σχετικά με το περιεχόμενο και τη διάδοση ενώ δημοσιευμένες εργασίες που δημιουργούνται από συγγραφείς που πέθαναν πενήντα έτη πριν ή περισσότερο επίσης δεν προστατεύονται[60]. Ο τρόπος με τον οποίο τα πνευματικά δικαιώματα δημιουργούνται και παραβιάζονται στο Διαδίκτυο έχει αποτελέσει το αντικείμενο ιδιαίτερης συζήτησης τα τελευταία χρόνια. Ακόμη και ο προσδιορισμός των δημιουργών των εργασιών δημιουργεί προβλήματα δεδομένου ότι οι νέες εργασίες στο Διαδίκτυο μπορούν να δημιουργηθούν ή/και να προσαρμοστούν σε μια πολλαπλότητα των συνεισφερόντων ανίκανων για διαφοροποίηση. Ομοίως, οι παραδοσιακές κατηγορίες εργασιών που αποτελούν το αντικείμενο της προστασίας πνευματικών δικαιωμάτων (λογοτεχνία, δράμα, μουσική, καλλιτεχνικά, ηχογραφήσεις ταινίες και ήχος και ραδιοτηλεοπτικές μεταδόσεις) έχουν καταρρεύσει κατά τη διαδικασία της ψηφιακής αναλογικής μεταλλαγής έτσι ώστε όλες οι μεταλλαγμένες εργασίες που υπάρχουν στον ίδιο τύπο σχήματος να είναι ικανές για ηλεκτρονική μετάδοση. Υπάρχουν λίγες εκτιμήσεις του βαθμού στον οποίο τα πνευματικά δικαιώματα παραβιάζονται από τους χρήστες Διαδικτύου και εκείνοι που υπάρχουν υποφέρουν από τα προβλήματα της παρέκτασης των στοιχείων και της ψευδούς δήλωσης. Το πρόβλημα είναι, εντούτοις, πιθανώς διαδεδομένο. Υπάρχουν κάποια στοιχεία ότι οι παραβάσεις πνευματικής ιδιοκτησίας γενικά αναφέρονται συχνότερα απ' ό,τι στο παρελθόν.

2.11.1.- Προτεινόμενες τεχνολογικά λύσεις

Ένα ευρύ φάσμα των τεχνολογικών λύσεων έχει προταθεί, για να εξετάσει την παράβαση πνευματικών δικαιωμάτων στο Διαδίκτυο. Αυτές περιλαμβάνουν τον περιορισμό της πρόσβασης στους χώρους διαδικτύου ή τις συγκεκριμένες εργασίες, τον περιορισμό της χρήσης των εργασιών για το Διαδίκτυο και την εισαγωγή κάποιας μορφής ηλεκτρονικής επιτήρησης των δραστηριοτήτων. Τέτοιες προσεγγίσεις υποφέρουν από τα προβλήματα περιορισμού της ελευθερίας της χρήσης του Διαδικτύου και μπορούν επίσης να περιλάβουν την πιθανή παράβαση της μυστικότητας. Εντούτοις, διευκολύνουν τη διαχείριση των σχεδίων χορήγησης αδειών και συλλογής πνευματικών δικαιωμάτων. Ο περιορισμός της πρόσβασης στις πνευματικά κατοχυρωμένες εργασίες μπορεί να επιτευχθεί μέσω ποικίλων συσκευών, όπως ο έλεγχος κεντρικών

---

[59] NES Database, 2002 on the web at:
http://www.oldburetto.com/pirates

[60] Russell G. Smith trends & issues in crime and criminal justice No. 65 Internet Piracy, 1997.

υπολογιστών, η κρυπτογράφηση, οι ψηφιακές υπογραφές και η στεγανοποίηση που επιτρέπει μόνο στα εξουσιοδοτημένα άτομα να έχουν πρόσβαση σε συγκεκριμένες εργασίες. Το πρόβλημα με τέτοιες προσεγγίσεις είναι ότι τα κλειδιά πρόσβασης, ανεξάρτητα από το πόσο περίπλοκο είναι αυτό, μπορούν να παρακαμφθούν τεχνολογικά. Οι ομάδες εξετάζουν τη χρήση του ψηφιακού μαρκαρίσματος των εργασιών που θα τις προσδιορίσει δεδομένου ότι διαβιβάζονται στο Διαδίκτυο. Το λογισμικό είναι έπειτα ικανό να χρησιμοποιηθεί για να προσδιορίσει ψηφιακά - επονομαζόμενες εργασίες και για να αποτρέψει τα αναρμόδια άτομα από να αποκτήσουν πρόσβαση σε αυτές ή να παράγουν αντίγραφα χωρίς άδεια[61].

Διάφορες τεχνολογικές συσκευές έχουν σχεδιαστεί για να περιορίσουν τη χρήση στην οποία οι εργασίες πνευματικών δικαιωμάτων μπορούν να τεθούν. Παραδείγματος χάριν, το λογισμικό είναι σε θέση να περιορίσει περαιτέρω αντιγραφή, να περιορίσει την οπτική επαφή ή το άκουσμα και να περιορίσει τον αριθμό αντιγράφων που μια εργασία μπορεί να παραχθεί, να ανοιχθεί , να αναπαραχθεί ή να τυπωθεί[62]. Τέλος, συσκευές επίσης μπορούν να χρησιμοποιηθούν που επιτρέπουν την ηλεκτρονική επιτήρηση των δικτύων ή ακόμα και των ιδιωτικών εσωτερικών οπτικοακουστικών συστημάτων υπολογιστών προκειμένου να προσδιοριστούν οι χρήστες που έχουν πρόσβαση ή χρησιμοποιούν τις εργασίες πνευματικών δικαιωμάτων παραβιάζοντας τα δικαιωμάτων των ιδιοκτητών. Μια τέτοια προσέγγιση προκαλεί προφανώς σημαντικές ανησυχίες για την τήρηση της μυστικότητας[63].

Εάν υιοθετούνται τέτοιες τεχνολογικές λύσεις στην πειρατεία πνευματικών δικαιωμάτων, θα πρέπει να ληφθούν μέτρα, για να εξασφαλίσουν ότι η αποτελεσματικότητά τους δεν νικιέται μέσω της χρήσης των τεχνολογικών μέσων. Μπορούν, παραδείγματος χάριν, να ψηφισθούν νόμοι, οι οποίοι να εξασφαλίζουν ότι οι συσκευές, όπως οι συσκευές αποκωδικοποίησης κρυπτογράφησης ή οι συσκευές καταπολέμησης αντιγραφής, δεν υιοθετούνται για να υπονομεύσουν την αποτελεσματικότητα των τεχνολογικών στρατηγικών με σκοπό την προστασία των πνευματικών δικαιωμάτων.

2.12.- Ζητήματα ασφάλειας στο Διαδίκτυο

Πολλές οργανώσεις έχουν να αντιμετωπίσουν σοβαρά ζητήματα Διαδικτύου[64]. Μερικά από τα σημαντικότερα ζητήματα περιλαμβάνουν:

2.12.1.- Καταχώρηση των χώρων Διαδικτύου στους οργανισμούς σας

Πολλές οργανώσεις δεν γνωρίζουν την πλήρη παρουσία του Διαδικτύου τους. Γνωρίζουν συχνά τον κύριο ιστοχώρο τους, και μερικές φορές ακόμη και να γνωρίζουν την πλήρη έκθεση στο Υπερδίκτυο. Εντούτοις, πολλοί από αυτούς έχουν 'παράνομες' συνδέσεις με το Διαδίκτυο που οργανώνονται από τις μικρές ομάδες ή τα μεγάλα τμήματα μέσα στην επιχείρηση. Σε αρκετούς από τους πρόσφατους λογιστικούς ελέγχους διείσδυσης Διαδικτύου, οι μηχανικοί διαπέρασαν το δίκτυο του πελάτη προσδιορίζοντας και εκμεταλλευόμενοι

---

[61] Fox, B. 1995, Speedy net threatens movie moguls, New Scientist, 16 December, σ. 22.
[62] Copyright Law Review Committee 1996, Copyright Reform: A Consideration of Rationales, Interests and Objectives, AGPS, Canberra, σσ.15-16.
[63] Copyright Law Review Committee 1996, Copyright Reform: A Consideration of Rationales, Interests and Objectives, AGPS, Canberra, σσ.15-16.
[64] Securing the Internet for 2002, Gordon Smith, President, Canaudit Inc, 2002 on the web at: http://www.canaudit.com/Articles_Pubs/past_articles/sept01_perspective.htm

μια κακώς ελεγχόμενη περιοχή απατεώνων που συνδέεται με το εσωτερικό δίκτυο. Αυτές οι περιοχές παρακάμπτουν τις κανονικές διαδικασίες ανάπτυξης, διαχείρισης και ασφάλειας του ΗΥ. Κατά συνέπεια, οι απαραίτητοι έλεγχοι δεν είναι σε ισχύ και οι χάκερς μπορούν απλά να γλιστρήσουν στο δίκτυο.

Μόλις διαπεράσουν ένα δίκτυο χρησιμοποιώντας ένα πλαστό δίκτυο, η διαχείριση του Η/Υ είναι συχνά δύσκολη, επειδή δεν ξέρουν ότι το δίκτυο υπήρξε. Ακόμα η διαχείριση τους θεωρεί αρμόδιους για την ασφάλεια του Διαδικτύου. Γι` αυτό είναι τόσο σημαντικό η παρουσία μιας επιχείρησης στο Διαδίκτυο να χαρτογραφείται και να καταχωρείται. Αυτό μπορεί να γίνει από την ομάδα ασφάλειας Η/Υ ή από μια εξωτερική πηγή. Στην πραγματικότητα, η καταχώρηση της πλήρους παρουσίας του πελάτη στο Διαδίκτυο είναι το πρώτο πράγμα που πρέπει να γίνεται κατά την έναρξη ενός λογιστικού ελέγχου Διαδικτύου ή διείσδυσης Διαδικτύου.

2.12.2.- Σχέδιο και διαμόρφωση

Σε πολλές οργανώσεις, η παρουσία Διαδικτύου άρχισε σαν την αναζήτηση χρυσού της Καλιφόρνιας. Όλοι παρατάσσονται. Κάποιος μετρούσε ως το τρία και, το ιόν, η επιχείρησή σας ήταν στο διαδίκτυο. "Απλά ενεργοποιήστε, θα το ελέγξουμε αργότερα." "Πρέπει να είμαστε στο 'δίκτυο' επειδή οι ανταγωνιστές μας είναι ήδη εκεί." "Έχουμε μια αντιπυρική ζώνη." Αυτές και παρόμοιες φάσεις είναι πολύ κοινές και οι περισσότεροι από μας τις έχουν ακούσει πολλές φορές. Παρά τις καλύτερες προθέσεις, μερικές οργανώσεις δεν επιδιώκουν ποτέ ξανά το σχέδιο και τη διαμόρφωση του Διαδικτύου τους. Αυτό οδηγεί όχι μόνο σε φτωχούς ελέγχους της παρουσίας Διαδικτύου, αλλά μπορεί επίσης να οδηγήσει σε δικτυακούς τόπους που δεν έχουν την απαραίτητη λειτουργία για να προσελκύσουν και να διατηρήσουν τη βάση πελατών σας.

Πολλές από τις περιοχές που αναθεωρούνται είναι πρώτιστα περιοχές "φυλλαδίων". Αυτές οι περιοχές παρέχουν τις πληροφορίες για τα προϊόντα και τις υπηρεσίες. Αυτό είναι επίτευγμα για τους πελάτες που θέλουν απλά να κοιτάξουν βιαστικά έναν ηλεκτρονικό κατάλογο. Δυστυχώς, δεν προσεγγίζει πληροφορίες μάρκετινγκ για τους επισκέπτες του δικτυακού σας τόπου. Ούτε επιτρέπει στην επιχείρηση να έρθει σε επαφή με τους πελάτες, να επιτρέψει στους πελάτες να παραγγείλουν το προϊόν , ή να επιτρέψει στην επιχείρησή σας να ωθήσει τις κρίσιμες πληροφορίες όπως οι μεταβολές των τιμών και άλλα στοιχεία πωλήσεων σε αυτούς.

Από τη σκοπιά της ασφάλειας, το φτωχό σχέδιο και η διαμόρφωση οδηγούν στην πολύ φτωχή ασφάλεια. Στις περισσότερες περιπτώσεις, η ασφάλεια αποτελείται από μια αντιπυρική ζώνη. Δυστυχώς, οι αντιπυρικές ζώνες μπορούν να παρακαμφθούν μέσα από τις προαναφερθείσες πλαστές συνδέσεις ή από τους κακώς διαμορφωμένους δρομολογητές, τους κεντρικούς υπολογιστές και τις συνδέσεις εμπορικών εταίρων. Το σχέδιο και η διαμόρφωση Διαδικτύου πρέπει να περιλάβουν το αρχικό σχέδιο των δικτυακών τόπων και των ελέγχων που απαιτούνται για να ελέγξουν εκείνες τις περιοχές. Οι πραγματικοί έλεγχοι εφαρμόζονται είτε μέσω των ελέγχων αντιπυρικών ζωνών, κεντρικών υπολογιστών και εφαρμογής ή/ και της εγκατάστασης του λογισμικού ασφάλειας.

Το σχέδιο και η διαμόρφωση Διαδικτύου δεν είναι κάτι που αναθεωρείται μόνο μία φορά. Είναι ένας τρέχων στόχος που πρέπει να εκτελείται ανά εξάμηνο. Αυτό θα εξασφαλίσει ότι οι συνδέσεις με το Διαδίκτυο συνεχίζουν να ικανοποιούν τις ανάγκες της εταιρίας σας και των πελατών σας.

2.12.3.- Το Υπερδίκτυο

Πολλές οργανώσεις οδηγούν τις εφαρμογές στο Υπερδίκτυο. Κατά συνέπεια, τα κρίσιμα σημεία ελέγχου πρέπει επίσης να μεταφερθούν στο Υπερδίκτυο. Οι λογιστικοί έλεγχοι έχουν προσδιορίσει ότι πολλές οργανώσεις έχουν ένα κακώς ελεγχόμενο περιβάλλον Υπερδικτύου. Οι κρίσιμες πληροφορίες πελατών, καθώς επίσης και οι επιχειρησιακές συναλλαγές, μπορούν να αντιγραφούν ή ακόμα και να αλλάξουν από τους χάκερς και τους ηλεκτρονικούς συμβούλους κατασκοπείας. Αυτοί οι "σύμβουλοι" εκμεταλλεύονται το Διαδίκτυο για τις πληροφορίες που μπορούν να πωληθούν στους εγκληματίες και τους ανταγωνιστές. Η αποτελεσματική ασφάλεια του Υπερδικτύου καλύπτει το Διαδίκτυο, τον κεντρικό υπολογιστή, το δίκτυο, τη βάση δεδομένων και την ασφάλεια εφαρμογής. Το Υπερδίκτυο δεν έχει υποβληθεί σε μια πλήρη αναθεώρηση ή έναν λογιστικό έλεγχο ασφάλειας. Μια από τις προτεραιότητες για τις οργανώσεις πρέπει να είναι να ολοκληρώσει αυτές τις αναθεωρήσεις έτσι ώστε οι έλεγχοι να μπορούν να ενισχυθούν και η χρηματοδότηση να διατεθεί για την τρέχουσα ασφάλεια του Υπερδικτύου το 2002.

Πολλές οργανώσεις έχουν μεταφέρει extranet τους isp ή ASP. Αυτό δεν σημαίνει ότι η ασφάλεια και ο έλεγχος θα είναι καθόλου καλύτεροι, ούτε μεταφέροντας extranet ανακουφίζεται η οργάνωσή σας από την ευθύνη να προστατευθούν τα στοιχεία του πελάτη σας. Μια πρωταρχική τρέχουσα ανησυχία είναι ότι αρκετά από τα σημαντικότερα ISPs μπορούν να έχουν τα σοβαρά ζητήματα ταμειακών ροών, δεδομένου ότι σημεία <com> τρέπονται στο σημείο <busts>. Εάν το isp σας αποτυγχάνει, τι συμβαίνει στο extranet σας και τη δυνατότητά σας να επεξεργαστείτε τις συναλλαγές Διαδικτύου;

2.12.4.- Αντιπυρικές ζώνες

Οι "αντιπυρικές" ζώνες είναι ένας μεγάλος έλεγχος. Εντούτοις, έρευνα έδειξε ότι οι αντιπυρικές ζώνες μπορούν να παρακαμφθούν. Επίσης, εάν η οργάνωσή σας αποτύχει να εγκαταστήσει τις απαραίτητες αναβαθμίσεις και τις διορθώσεις, τότε οι έλεγχοι αντιπυρικών ζωνών μπορούν να παραβιαστούν. Ένα άλλο ζήτημα είναι η ανίχνευση και η ανταπόκριση στους εισβολείς. Έχει παρατηρηθεί ότι πολλές οργανώσεις αφήνουν την αντιπυρική ζώνη να παρεμποδίσει τις προσπάθειες. Σε πολλές περιπτώσεις, τα υλικά αντιπυρικών ζωνών δεν αναθεωρούνται. Οι χάκερς μπορούν να εξετάσουν ήσυχα το δίκτυο, τα τρωτά σημεία των εγγράφων και, ενδεχομένως επιτυχώς (από τη σκοπιά τους), εκτελούν και εκμεταλλεύονται το δίκτυο. Εάν η αντιπυρική ζώνη εμποδίσει την Ηλεκτρονική τους διεύθυνση, ένας χάκερ θα χρησιμοποιήσει ακριβώς έναν άλλο λογαριασμό για να συνεχίσει την επίθεσή του. Μόνο μια αυτοματοποιημένη επιφυλακή, που συνδυάζεται με τις τυποποιημένες διαδικασίες ανίχνευσης και δράσης, μπορεί να εξασφαλίσει ότι μια συνεχής επίθεση ανιχνεύεται και ερευνάται κατάλληλα.

2.12.5.- Ιδεατά ιδιωτικά δίκτυα

Τα ιδεατά ιδιωτικά δίκτυα πωλούνται συχνά ως ασφαλής εναλλακτική λύση άλλων τεχνολογιών σύνδεσης. Ενώ αυτό μπορεί να ισχύει εάν είναι κατάλληλα εγκατεστημένα και εξασφαλισμένα, μερικά VPNs έχουν χρησιμοποιηθεί από τους χάκερς, για να διαπεράσουν τα εταιρικά δίκτυα. Το Φεβρουάριο του 2001, πολλές οργανώσεις διείσδυσαν επιτυχώς στην Ανατολική Ευρώπη χρησιμοποιώντας τις συνδέσεις VPN τους. Όχι μόνο οι έλεγχοί τους νικήθηκαν, αλλά αυτές οι επιχειρήσεις έπρεπε να πληρώσουν το λογαριασμό. Μερικές από αυτές τις επιχειρήσεις ανακάλυψαν ότι υπάρχουν μόνο μόλις είδαν το τιμολόγιο προμηθευτών VPN. Αυτό θα μπορούσε να έχει ανακαλυφθεί νωρίτερα αν αμφισβητούσαν τα στοιχεία του VPN. Ένας αποτελεσματικός

τρόπος εντοπισμού των συνδέσεων VPN θα ήταν να εφοδιαστεί ο προμηθευτής με ένα αρχείο σε καθημερινή ή εβδομαδιαία βάση με τις πληροφορίες για τις εργασίες των χρηστών. Αυτό περιλαμβάνει τον αριθμό λογαριασμού, το σημείο αρχικής σύνταξης, την ημερομηνία και χρόνος της σύνδεσης, την ημερομηνία και το χρόνο της αποσύνδεσης, τα πακέτα διάρκειας συνδέσεων διαβίβασης και λήψης. Βάλτε αυτό το στοιχείο σε μια βάση δεδομένων ή έναν υπολογισμό με λογιστικό φύλλο (spreadsheet) και ταξινομήστε το ερευνώντας πολύ μακροχρόνιες συνδέσεις και αδύνατους συνδυασμούς (αναγραφή μέσα από το Σιάτλ στις 1 μ.μ., έπειτα Νέα Υόρκη στις 1:05 μ.μ.). Επίσης ψάξτε ταυτόχρονες διαβιβάσεις (δύο ή περισσότερες διαβιβάσεις για τον ίδιο λογαριασμό συγχρόνως). Αυτό θα σας επιτρέψει να ανακαλύψετε τους απλούς ή κοινούς λογαριασμούς. Η τελευταία απλή δοκιμή είναι να ψαχτούν οι μεγάλες αποθηκευτικές ενότητες στοιχείων από έναν συγκεκριμένο λογαριασμό. Αυτό μπορεί να είναι ένας χάκερ που μεταφορτώνει τα στοιχεία σας ή φορτώνει τα στοιχεία του /της στους κεντρικούς υπολογιστές σας.

2.12.6.- Ικανοποιητική διαχείριση και ασφάλεια

Πολλές οργανώσεις στερούνται στους ελέγχους περιεχομένου των ιστοχώρων. Δίκτυο που οι χάκερ έχουν αλλάξει συνήθως βρίσκεται. Δεδομένου ότι κανένας δεν αναθεωρεί το δίκτυο σε κανονική βάση, αυτές οι αλλαγμένες σελίδες θα παρατηρηθούν μόνο από τους πελάτες σας. Μερικές αλλαγές γίνονται λόγω του κακώς ελεγχόμενου κώδικα της CGI. Άλλες αλλαγές γίνονται με την εκμετάλλευση του λογισμικού δικτύου. Ο κεντρικός υπολογιστής πληροφοριών Διαδικτύου (IIS) είναι ιδιαίτερα τρωτός. Κάθε οργάνωση πρέπει να έχει μια επίσημη διαδικασία αναθεώρησης προτού να τοποθετήσει το περιεχόμενο στον Ιστό, κανονικές αναθεωρήσεις για να εξασφαλίσει ότι το περιεχόμενο δεν έχει αλλάξει, και αποτελεσματική ασφάλεια, για να προστατεύσει το δίκτυο και το περιεχόμενο του δικτύου σας.

2.12.7.- Διοικητικός έλεγχος και εποπτεία

Έχει διαπιστωθεί ότι η διοίκηση συχνά εξουσιοδοτεί το δίκτυο, τη διαχείριση και την εποπτεία στο κατώτερο προσωπικό. Αυτό όχι μόνο καταδεικνύει ότι η διαχείριση δεν ενδιαφέρεται για την παρουσία Διαδικτύου, αλλά ότι ένα σημαντικό μέρος της επαφής πελατών μιας οργάνωσης και του Δικτύου εφαρμόζεται από τους υπεύθυνους προγράμματος και τους αναλυτές, όχι από τους υπαλλήλους προώθησης. Η διοίκηση πρέπει να έχει έναν ενεργό ρόλο στη διαχείριση των ιστοχώρων και του περιεχομένου. Πρέπει να καθορίσουν ποιες πληροφορίες είναι δημόσιες και εξασφαλίζουν ότι οι πληροφορίες είναι δημόσιες και να εξασφαλίσει ότι παρουσιάζονται με ένα αποδεκτό σχήμα που δεν θα εκθέσει την επιχείρηση στα νομικά ζητήματα. Επιπλέον, το μη-δημόσιο περιεχόμενο και τα στοιχεία των πελατών πρέπει να προστατευθούν. Η διοίκηση πρέπει επίσης να εξασφαλίσει ότι η παρουσία Διαδικτύου εξασφαλίζεται και ότι η ανίχνευση καταπάτησης είναι σε ισχύ. Ένα ανώτερο στέλεχος πρέπει να διευθύνει τη συναφή ομάδα απάντησης υπολογιστών για να εξασφαλίσει ότι τα γεγονότα αναφέρονται κατάλληλα στην εκτελεστική διαχείριση και ότι δεν υπάρχει καμία επικάλυψη.

Κεφάλαιο ΙΙΙ

Μεθοδολογία

3.1.- Περιγράψτε την προσέγγιση

Η μέθοδος που υιοθετείται στο σχηματισμό αυτής της διατριβής είναι καθαρά η έρευνα και η στήριξη στα γεγονότα. Όλα τα στοιχεία έχουν συγκεντρωθεί από πραγματικές πηγές που είναι είτε οι συντάκτες των βιβλίων που θεωρούνται αληθινά καθώς παραμένουν δημοσιευμένα χωρίς να διαψεύδονται ή πληροφορίες ειδήσεων Δικτύου που λαμβάνονται μόνο από τις επίσημες συχνότητες διάσημων Δικτύων, όπως η Βρετανική Ραδιοφωνική Εταιρία (BBC) ή το καλωδιακό δίκτυο ειδήσεων (CNN). Το Διαδίκτυο έχει χρησιμοποιηθεί ευρέως στην έρευνα αυτού του θέματος, καθώς το θέμα αυτής της διατριβής περιστρέφεται γύρω από την τεχνολογία και κατά την άποψη του συντάκτη δεν υπάρχει καμία καλύτερη πηγή από το επίκεντρο της τεχνολογίας, για να τροφοδοτήσει τις απαιτήσεις των διατριβών με αυτά τα θέματα. Τα Δίκτυα ελέγχονται διπλά για οποιαδήποτε αντιφατική δήλωση με τις εργασίες άλλων συντακτών σε διαφορετικές ιστοσελίδες και ταχυδρομούνται έπειτα με παραπομπή σε κείμενα με πλήρη στοιχεία.

Επιπλέον, η προσέγγιση περιστρέφεται γύρω από τα προηγούμενα στοιχεία που συγκεντρώνονται από τις μελέτες ή τις έρευνες που έγιναν ήδη στον ίδιο τομέα και καμία νέα μελέτη ή έρευνα δεν έχει γίνει. Έτσι όλες οι πληροφορίες έχουν επαληθευθεί τουλάχιστον από την προηγούμενη έρευνα (που απαριθμείται στις παραπομπές). Η παράβαση πνευματικών δικαιωμάτων έχει ληφθεί υπόψη και το ίδιο συμβαίνει και με τη λογοκλοπή. Έτσι κάθε άρθρο που λαμβάνεται έχει ελεγχθεί ως προς τα πνευματικά δικαιώματα στον ιστοχώρο, εάν πρόκειται για το Διαδίκτυο, ή στο ίδιο το περιοδικό, και εάν η περίπτωση περιγράφει έτσι τέτοια πνευματικά δικαιώματα, η πλήρης πίστωση δίνεται στους κατόχους.

3.2.- Προσδιορίστε τη μέθοδο συλλογής στοιχείων

Τα στοιχεία σε αυτήν την έρευνα έχουν συγκεντρωθεί από δύο αρχικές πηγές: τα ερευνητικά περιοδικά που έχουν κάνει την εργασία για τα ζητήματα των εγκλημάτων cyber και των απειλών που τίθενται στην Ευρωπαϊκή Ένωση ή ολόκληρη την ήπειρο (συμπεριλαμβανομένων των ατόμων) και αφετέρου πηγές Διαδικτύου συμπεριλαμβανομένων των ιστοχώρων, ιστοσελίδων, των εγγράφων και των φύλλων έρευνας στοιχείων. Η μέθοδος που ακολουθείται είναι απόσπασμα με σημαντική εστίαση στη σχετικότητα και την ακρίβεια καθώς επίσης και στην προσθήκη των αναθεωρήσεων και του συσχετισμού των στοιχείων μιας πηγής με άλλες. Η αρχική έρευνα έχει γίνει από τον συντάκτη και περιλαμβάνει την έκδοση της παραπεμφθείσας εργασίας οπουδήποτε είναι απολύτως απαραίτητο, για να δημιουργήσει μια σχετική εικόνα. Η έκδοση δεν έχει γίνει, για να αφαιρέσει την ουσία ή τα βασικά σημεία της έρευνας, αλλά για να κάνει στιγμιαίες αλλαγές προκειμένου να διευκρινιστούν τα αποτελέσματα. Τα στοιχεία για τον Ευρωπαϊκό τομέα έχουν συγκεντρωθεί λαμβάνοντας υπόψη το χρονικό πλαίσιο τεσσάρων ετών, δηλ. κανένα στοιχείο πριν από εκείνη την ημερομηνία δεν έχει επιλεχτεί λόγω του παράγοντα χρόνου και της αχρηστίας εκείνων των στοιχείων. Οποιοδήποτε στοιχείο σχετικό με τη διαδικασία των εγκλημάτων ή του αντίκτυπού τους έχει συγκεντρωθεί κρατώντας το χρονικό όριο ως προς τα 2 έτη δεδομένου ότι οι μέθοδοι και οι διαδικασίες αλλάζουν αρκετά συχνά και έγιναν προσπάθειες να δοθεί απολύτως επίκαιρη ή τουλάχιστον πολύ πρόσφατη εικόνα των διαδικασιών.

3.3.- Βάση δεδομένων της μελέτης

Η πραγματική βάση δεδομένων όλων των στοιχείων που συγκεντρώνονται τίθεται στο τμήμα ανάλυσης στοιχείων και αναθεωρείται επίσης ακολουθώντας το. Δεν υπάρχει καμία πηγή στοιχείων, έτσι τα διάφορα πρότυπα καθώς επίσης και οι παραλλαγές αποτελεσμάτων υπάρχουν, αλλά έχουν ομαλοποιηθεί για αυτήν την αναφορά. Η βάση δεδομένων αποτελείται από τους πίνακες και τη γραφική παράσταση που διαμορφώνει το υλικό, το οποίο μπορεί να χρησιμοποιηθεί εύκολα, για να διαμορφώσει τις γραφικές παραστάσεις και τις τάσεις για οποιοδήποτε ιδιαίτερο γεγονός παρουσιάζεται στη βάση δεδομένων κατά τη διάρκεια μιας μεγάλης χρονικής περιόδου. Οι τάσεις ή η αύξηση στα ποσοστά εγκλήματος θα μπορούσαν να έχουν παρουσιαστεί γραφικά, αλλά αυτό δεν ήταν στο πλαίσιο αυτής της έκθεσης.

3.4.- Τύπο Ηλεκτρονικής Απάτης

Υπάρχουν τρεις κύριοι τύποι επιχειρησιακής και καταναλωτικής απάτης που μπορούν να πραγματοποιηθούν ηλεκτρονικά που αντιστοιχούν με την παραδοσιακή παραπλάνηση και τις παραπλανητικές επιχειρησιακές πρακτικές: προσποίηση ότι πωλείται κάτι που δεν έχετε ταυτόχρονα παίρνοντας τα χρήματα εκ των προτέρων (σχέδια προπληρωμών), παροχή αγαθών ή υπηρεσιών που είναι χαμηλότερης ποιότητας από τα αγαθά ή τις υπηρεσίες που πληρώνονται, ή αποτυχία να παραδοθούν τα αγαθά και οι υπηρεσίες (μη παράδοση και ελαττωματικά προϊόντα και υπηρεσίες). Πείθουν τους πελάτες, για να αγοράσουν κάτι που δεν θέλουν πραγματικά μέσω των καταπιεστικών τεχνικών μάρκετινγκ (ακούσια και ανεπιθύμητα αγαθά και υπηρεσίες).

3.4.1.- Σχέδια Προπληρωμής

Η ουσία των αποκαλούμενων 'σχεδίων προπληρωμής' είναι να εξαπατήσει τα ενδεχόμενα θύματα στο χωρισμό των κεφαλαίων και να τους πείσει ότι θα λάβουν έναν ουσιαστικό όφελος σε αντάλλαγμα αν δώσουν κάποια μέτρια πληρωμή εκ των προτέρων. Τα χαρακτηριστικά αυτού του τύπου σχεδίου απάτης συνεπάγονται συνήθως τις υπηρεσίες του ενδεχόμενου θύματος, για να βοηθήσουν σε μια δραστηριότητα αμφισβητήσιμης νομιμότητας, παρέχοντας ωστόσο κάποια διαβεβαίωση ότι το θύμα θα ήταν απίθανο να αναφέρει το θέμα στην αστυνομία, μόλις εξαπατηθεί. Κατά συνέπεια, ο παραβάτης είναι σε θέση να πραγματοποιήσει το σχέδιο επανειλημμένα, μερικές φορές στο ίδιο θύμα, ενώ η αστυνομία βρίσκεται αντιμέτωπη με τις δυσκολίες στην εύρεση μαρτύρων και εξασφάλιση των στοιχείων. Τα παραδείγματα των σε απευθείας σύνδεση σχεδίων προπληρωμής περιλαμβάνουν τα σχέδια πυραμίδων[65] που έχουν τον αρχικό σκοπό να κερδίσουν τα άτομα χρήματα μέσω της στρατολόγησης άλλων προσώπων, όπως μέσω της χρήσης του ηλεκτρονικού ταχυδρομείου και των ηλεκτρονικών καταλόγων διευθύνσεων. Ένα πρόσφατο παράδειγμα που ερευνήθηκε από το ACCC περιέλαβε την Καναδική Σφαιρική Διαλογική Λέσχη Επενδύσεων που διαφήμισε το γεγονός ότι οι παράκτιες τράπεζες θα εξέδιδαν κάρτες Visa με χαμηλό επιτόκιο μέσω του Διαδικτύου με την υπόσχεση να μην υπάρχει πιστωτικός έλεγχος ή εισοδηματική επαλήθευση. Το σχέδιο ήταν πραγματικά ένα διεθνές σχέδιο πυραμίδας, στο οποίο οι υποψήφιοι ενθαρρύνθηκαν, για να στρατολογήσουν άλλους με αντάλλαγμα $25 για κάθε ένα[66].

---

[65] Β.Ζησιάδη, Η Οικονομική Εγκληματικότητα: Το Ουσιαστικό και Δικονομικό Οικονομικό Ποινικό Δίκαιο, Εκδόσεις Σακκούλα, 2001. σ.72.

[66] Australian Competition and Consumer Commission 1997b, on the web at: http://www.accc.gov.au

Το Διαδίκτυο χρησιμοποιείται επίσης ως μέσο για τα σχέδια επένδυσης Ponzi[67] και ποικίλα ψευδή σχέδια επιχειρησιακής ευκαιρίας καθώς επίσης και σχέδια που χρησιμοποιούν τις σε απευθείας σύνδεση δημοπρασίες. Ένας από τους πιο πρόσφατους τομείς ανησυχίας αφορά την σε απευθείας σύνδεση απάτη . Διάφορα προβλήματα έχουν προκύψει ήδη με τις παραπλανητικές πληροφορίες που δίνονται στους επενδυτές και τις αγορές μετοχών τις οποίες χειρίζεται κανείς μέσω του ηλεκτρονικού ταχυδρομείου και του Διαδικτύου.

3.4.2.- Μη παράδοση και ελαττωματικά προϊόντα και υπηρεσίες

Η απάτη στο δίκτυο επίσης περιλαμβάνει τον έμπορο που αποτυγχάνει να παραδώσει τα αγαθά όταν και όπου ζητείται. Αυτό το πρόβλημα επιδεινώνεται στις παγκόσμιες εμπορικές συναλλαγές όπου περιλαμβάνεται η παράδοση των αγαθών σε μεγάλη απόσταση, μερικές φορές συμπεριλαμβάνεται ο εκτελωνισμός και η πληρωμή των φόρων εισαγωγής. Εναλλακτικά, τα ελαττωματικά αγαθά μπορεί να παραδοθούν ή να είναι ελαττωματικά, οπότε σ' αυτή την περίπτωση οι καταναλωτές πρέπει να τακτοποιήσουν την επιστροφή και την επιστροφή της τιμής που καταβλήθηκε και οποιωνδήποτε σχετικών δαπανών. Πολλά από αυτά τα προβλήματα προκύπτουν από το γεγονός ότι τα αγαθά είναι αδύνατον να εξετασθούν αρχικά στην σε απευθείας σύνδεση αγορά.

Τα προβλήματα δημιουργούνται επίσης λόγω της αμεσότητας μερικών συναλλαγών στις οποίες τα αγαθά ή οι υπηρεσίες λαμβάνονται ακριβώς την ίδια στιγμή που εξουσιοδοτείται η πληρωμή (π.χ. η αγορά του λογισμικού χρεώνεται, αμέσως μόλις δοθεί ένας αριθμός πιστωτικής κάρτας). Σε τέτοιες περιπτώσεις, οι παραδοσιακές μέθοδοι διακοπής της πληρωμής με επιταγή ή η απόσυρση της έγκρισης για μια αγορά με πιστωτική κάρτα δεν είναι διαθέσιμες. Όσο οι καταναλωτές συνεχίζουν να αυξάνουν τη χρήση του Διαδικτύου τόσο αυξάνεται και ο αριθμός καταγγελιών για τους φορείς παροχής υπηρεσιών στο Διαδίκτυο. Το ACCC, παραδείγματος χάριν, έχει ερευνήσει τους ισχυρισμούς υπερτιμολόγησης, την ανεπαρκή λεπτομέρεια κατά την τιμολόγηση, την αποτυχία να παρασχεθεί η τεχνική υποστήριξη και άλλες υπηρεσίες που παρουσιάζονται, την αποτυχία να συνδεθούν οι καταναλωτές με το Διαδίκτυο όπως έχει συμφωνηθεί, την απόρριψη αιτημάτων για αποσύνδεση, την ανάγκη ύπαρξης πιστωτικής κάρτας για να λάβει τις υπηρεσίες, προσπάθειες να αγνοηθούν τα νόμιμα δικαιώματα των καταναλωτών, και τις διαστρεβλώσεις για την ταχύτητα πρόσβασης στο Διαδίκτυο και την εμπειρία του φορέα παροχής υπηρεσιών[68].

Το Διαδίκτυο χρησιμοποιείται τώρα για να διαφημίσει[69] τις εξαρτήσεις αποκρυπτογράφησης καλωδιακών τηλεοράσεων που επιτρέπουν στους καταναλωτές να λάβουν την καλωδιακή τηλεόραση χωρίς καταβολή των αμοιβών συμβάσεων. τέτοιες εξαρτήσεις όχι μόνο σπάνια λειτουργούν, αλλά απαιτούν επίσης από τους καταναλωτές να παραβούν το νόμο με την κλοπή των καλωδιακών υπηρεσιών .

Στην ψηφιακή εποχή, είναι επίσης δυνατό να αγοραστούν ποικίλα μεταλλαγμένα προϊόντα με ηλεκτρονική χρέωση. Το Διαδίκτυο παρέχει ένα περιεκτικό μέσο διαφήμισης για αυτά τα προϊόντα, συχνά

---

[67] Charles Ponzi,1919 του οποίου το όνομα έχει γίνει συνώνυμο με ένα συγκεκριμένο τύπο απάτης- επενδυτικής πρακτικής , που βασίζεται στις οικονομικές διαφορές συναλάγματος που προκύπτουν μεταξύ διάφορων κρατών.

[68] Australian Competition and Consumer Commission 1999, on the web at: http://www.accc.gov.au

[69] Κατά την Οδηγία υπ' αριθμ. 84-4.50 της Επιτροπής της Κοινότητας της 10 ης Σεπτεμβρίου 1984, ως διαφήμιση μπορεί να οριστεί κάθε μορφή επικοινωνίας στα πλαίσια μιας εμπορικής, βιομηχανικής ή άλλης ελεύθερης δραστηριότητας, προκειμένου να προωθηθεί η προμήθεια αγαθών και η παροχή υπηρεσιών

παρέχοντας δωρεάν δείγματα σε απευθείας σύνδεση. Μόλις διαβιβαστεί η πληρωμή στον έμπορο, ο αγοραστής είναι σε θέση να αποκτήσει το πλήρες προϊόν μαζί με τις κατάλληλες άδειες για τη χρήση του. Εάν, εντούτοις, το λογισμικό έχει αντιγραφεί παράνομα, ή εάν είναι ελαττωματικό με κάποιο τρόπο, ο καταναλωτής συχνά απογοητεύεται επειδή έχει πληρώσει για ένα προϊόν που δεν μπορεί νόμιμα να χρησιμοποιήσει.

Ένας τομέας του σε απευθείας σύνδεση εμπορίου που έχει αναπτυχθεί παραγωγικά είναι αυτός που αφορά την παροχή πορνογραφικών εικόνων και τις σεξουαλικές υπηρεσίες. Μερικοί από αυτούς περιλαμβάνουν την παραπλανητική και ψεύτικη συμπεριφορά. Ένα παράδειγμα περιλαμβάνει μια επιχείρηση που διαφήμιζε τις 'ελεύθερες' ερωτικές φωτογραφίες στο διαδίκτυο. Προκειμένου να φανούν οι εικόνες, ο χρήστης πρέπει να εγκαταστήσει το λογισμικό που, μόλις εγκατασταθεί, παίρνει τον έλεγχο του διαποδιαμορφωτή του χρήστη, διακόπτει τον τοπικό φορέα παροχής υπηρεσιών Διαδικτύου, και σχηματίζει έναν αριθμό στην πρώην Σοβιετική Δημοκρατία της Μολδαβίας στην Ανατολική Ευρώπη. Η γραμμή παρέμεινε ανοικτή έως ότου κλείσει ο υπολογιστής με συνέπεια ο χρήστης να χρεώνεται μεγάλες διεθνείς τηλεφωνικές δαπάνες που μοιράζονται μεταξύ του απατεώνα και της επιχείρησης τηλεπικοινωνιών της Μολδαβίας . Η απάτη ανιχνεύθηκε μέσω της κανονικής επιτήρησης των τηλεφωνικών λογαριασμών των πελατών και το FTC ήταν σε θέση να λάβει μια διαταγή που απαιτεί από τους κατηγορουμένους να τοποθετήσουν ένα εκατομμύριο δολάρια σε έναν λογαριασμό μεταβιβάσεων εν αναμονή του ψηφίσματος της περίπτωσης[70]. Άλλες σε απευθείας σύνδεση παράνομες πρακτικές έχουν περιλάβει τη διαφήμιση και την πώληση των σχεδίων δανείου, των εξαρτήσεων πιστωτικής επισκευής, της υγείας και των ιατρικών προϊόντων όπως οι θεραπείες για τον καρκίνο και το HIV, και των εκπαιδευτικών προσόντων από τα ανοιχτά πανεπιστήμια, μερικά από τα οποία αποτυγχάνουν να παρέχουν αναγνωρισμένα, ή πράγματι, οποιαδήποτε έγκυρα προσόντα, ή αποτυγχάνουν περιστασιακά να παραδώσουν οποιαδήποτε εκπαιδευτικά προγράμματα .

3.4.3.- Ακούσιες και ανεπιθύμητες υπηρεσίες και αγαθά

Παραδοσιακά, υπήρξαν λίγοι έλεγχοι στη διαφήμιση που διεξάγεται ταχυδρομικώς και οι άμεσοι έμποροι επέβαλαν ένα φράγμα της διαφήμισης του υλικού στους ανυποψίαστους, και συχνά απρόθυμους, παραλήπτες. Το ηλεκτρονικό αντίτιμο, γνωστό ως "spam", συνεπάγεται την ίδια ιδέα που πραγματοποιείται μέσω της χρήσης του ηλεκτρονικού ταχυδρομείου. Τα μελλοντικά αντίτιμά του μπορούν να είναι ακόμα πιο απειλητικά με τις αυτόνομες συνδέσεις που θα μπορούσαν να φέρουν τους ιούς στο σκληρό δίσκο των υπολογιστών του παραλήπτη προκαλώντας ζημία και απώλεια.

Το δόλωμα που διαφημίζεται περιλαμβάνει την προσφορά ενός προϊόντος ή μιας υπηρεσίας για πώληση σε μια δελεαστικά χαμηλή τιμή[71] προκειμένου να πωληθούν κάποια άλλα ακριβότερα προϊόντα ή υπηρεσίες, ή τη διαφήμιση μιας συμφωνίας που δεν υπάρχει προκειμένου να προσελκυστούν οι πελάτες για να κάνει επιχειρήσεις με τον έμπορο και είναι δυνατόν να διευθυνθεί ηλεκτρονικά, αδρανείς πωλήσεις ή και αποστολή αγαθών στους καταναλωτές που δεν τα έχουν παραγγείλει τιμολογώντας τα με την ελπίδα ότι θα δεχτούν τα αγαθά και θα πληρώσουν το λογαριασμό ασυζητητί. Τα διάφορα καταστατικά καθιστούν τώρα τέτοιες πρακτικές παράνομες που, αμφισβητήσιμα, θα εφαρμόζονταν, όπου τα ηλεκτρονικά αγαθά ή οι

---

[70] Federal Trade Commission v Audiotex Connection Inc E.D.N.Y. Filed 13 February 1997.

[71] ' οι ενέργειες των επαγγελματιών, οι οποίοι προκειμένου να προωθήσουν προϊόντα τους, εξαπατούν τους καταναλωτές αφορούν γενικότερα την τιμή του προϊόντος '. .Ζησιάση, Οικονομική Εγκληματικότητα: Το Ουσιαστικό και Δικονομικό Οικονομικό Ποινικό Δίκαιο,Εκδ. Σακκούλα, Αθήνα 2001. σ.71.

υπηρεσίες παρέχονται στους σε απευθείας σύνδεση καταναλωτές χωρίς αίτημά τους. Κάποιος θα μπορούσε να φανταστεί το λογισμικό που παρέχεται σε αυτόνομη σύνδεση σε ένα μήνυμα ηλεκτρονικού ταχυδρομείου ότι θα τιμολογούταν έπειτα. Ομοίως, απαιτώντας την πληρωμή για την πρόσβαση σε χώρους Διαδικτύου θα μπορούσαν να ανέλθουν σε μορφή ανενεργής πώλησης της εν λόγω υπηρεσίας.

3.5.- Περίληψη της μεθοδολογίας

Τα στοιχεία που αποκτήθηκαν και η έρευνα που γίνεται σε αυτήν την έκθεση συγκεντρώνονται άμεσα από είτε από το Διαδίκτυο είτε από τα ερευνητικά περιοδικά όπως αναφέρεται στις αντίστοιχες αναφορές. Όλα τα στοιχεία στη φάση της ανάλυσης έχουν ελεγχθεί από το συντάκτη καθώς επίσης από το Δίκτυο για τις ενδεχόμενες τρέχουσες αλλαγές και οι τροποποιήσεις έγιναν από τους αρχικούς εκδότες. Η μεθοδολογία της έκθεσης αποτελείται από την καθαρή έρευνα των ήδη διαθέσιμων στοιχείων και τη συγκέντρωση εκείνων των στοιχείων σε σχετική μορφή και θέση που είναι κατάλληλη για όποιες πληροφορίες υποστηρίζουν την απόφαση. Όλα τα συνοπτικά στοιχεία μορφής ίσως να μην είναι τέλεια συντονισμένα με την υπόλοιπη έκθεση, αλλά αυτό οφείλεται στο χώρο του εγγράφου και στη μη επιτρεπόμενη (υποτιθέμενη) χρήση των εικόνων στην έκθεση.

Κεφάλαιο IV

4.1.- Ανάλυση στοιχείων

Αρχίζοντας την ανάλυση στοιχείων και τις επιπτώσεις της, εξετάζουμε τα προηγούμενα ποσοστά απατών στην Ευρώπη συνολικά. Οι διαφορές στους μηχανισμούς ασφάλειας παίζουν επίσης έναν ρόλο στα ποσοστά της απάτης, και έτσι η ανάλυσή μας θα εστιάσει όχι μόνο στην άνοδο και την πτώση εκείνων των ποσοστών αλλά και στους λόγους.

4.2.-Πιστωτικές κάρτες

Αν και δεν είναι το διασημότερο είδος του σε απευθείας σύνδεσης ή ηλεκτρονικού τεχνολογικού εγκλήματος, η απάτη μέσω πιστωτικών καρτών είναι μια από τις πιο διαδεδομένες πράξεις δεδομένου ότι περιλαμβάνει τα μικρότερα ζητήματα ασφάλειας και επιμέρους μάλλον παρά οργανωτικά επίπεδα παραβίασης. Για να εξετάσουμε τα ποσοστά αυτών των εγκλημάτων σε διαφορετικές εποχές, εξετάζουμε μια ερευνητική έκθεση των εκδόσεων 'Lafferty' που συνοψίζεται κατωτέρω στον πίνακα που παρουσιάζει όλες τις σημαντικές κάρτες με τα ποσοστά απατών τους στο έτος 2000 καθώς επίσης και το μηχανισμό ασφάλειας που κάθε ένας ακολουθεί.

Τύπος καρτών	**Ποσοστό**	**Μηχανισμός ασφάλειας**
Belgian Debit	0,02%	Smart Card & PIN
CB (Γαλλία)	0.04%	Smart card & PIN
Maestro (Europay)	0.06%	Mag-stripe & PIN
UK Debit	0.14%	Mag-stripe & PIN
Visa EU Credit	0.04%	Mag-stripe & signature
Visa USA Credit	0.06%	Mag-stripe & signature
Europay Credit	0.1%	Mag-stripe & signature
Canada Credit	0.15%	Mag-stripe & signature
UK Credit	0.16%	Mag-stripe & signature
Cartes Bancaires Abroad	0.47%	Mag-stripe & signature

Αν και τα στοιχεία δείχνουν ότι τα ποσοστά ποικίλουν ομοιόμορφα και με τις χρεωστικές και με τις πιστωτικές κάρτες, το ίδρυμα του οποίου είναι η κάρτα κάνει επίσης μια διαφορά όχι μόνο λόγω της τεχνολογίας ασφάλειας που υπάρχει αλλά και λόγω είτε της θεωρούμενης ευκολίας της απάτης είτε του αριθμού διαθέσιμων καρτών στην αγορά και οι έλεγχοι ισχύουν κατά τη χρησιμοποίηση εκείνων των καρτών από τους λιανοπωλητές ή τους εμπόρους.

Απάτη πληρωμών στη Γαλλία, 1998 - 2000

Κατηγορία	2000	1999	1998
Απάτη, παραποίηση & πλαστογράφηση	317,044	258,306	246,991
Παραποίηση / χρήση των κλεμμένων πιστωτικών καρτών	48,997	39,126	30,459
Παραποίηση / χρήση των κλεμμένων επιταγών	114,346	108,580	119,470
Έλεγχος σχετικά με άλλα εγκλήματα	16,619	15,476	16,813

Ποσοστά απάτης καρτών στα σημεία βάσης

Μηχανισμός ασφάλειας	Τύπος καρτών	Σημεία βάσης
MAG-LWRJ'DA & υπογραφή	UK Credit Cards	15
Mag-Stripe & Online Authorization	Visa US Credit Cards	6
Mag-Stripe with PIN	Europay Maestro Cards	3
Smart Card with PIN	Belgian Debit Cards	1

Η απάτη πιστωτικών καρτών στην Ευρωπαϊκή Ένωση αυξήθηκε κατά 50% πέρυσι, με τις παράνομες συναλλαγές που φθάνουν σε κατ' εκτίμηση $553 εκατομμύρια, λέει τη Δευτέρα η Επιτροπή. Ένα μεγάλο ποσοστό της αύξησης περιλαμβάνει τις πληρωμές που γίνονται τηλεφωνικώς ή μέσω του Διαδικτύου -- που προκαλεί την καταναλωτική εμπιστοσύνη στις συναλλαγές μέσω δικτύου και που αποθαρρύνει τη δυνατότητα για επέκταση του ηλεκτρονικού εμπορίου.

"Η απάτη αυξάνεται πιο πολύ σε σχέση με τις μακρινές συναλλαγές πληρωμής, ειδικά στο Διαδίκτυο," είπε το εκτελεστικό μέρος της ΕΕ σε ένα έγγραφο που εκδόθηκε τη 'Δευτέρα'. Για να ανταποκριθεί στην άνοδο στον αριθμό παράνομων συναλλαγών, η Επιτροπή προώθησε τη Δευτέρα ένα φιλόδοξο τρίχρονο σχέδιο που στόχευε στην αντιμετώπιση της απάτης σε ολόκληρη την Ευρώπη. Το σχέδιο θα αυξήσει το συντονισμό με τη βιομηχανία, με στόχο "το πιο υψηλό οικονομικά βιώσιμο επίπεδο ασφάλειας" των μακρινών συναλλαγών από τα μέσα του 2002. Νέα τεχνικά μέτρα για να αποτραπεί η απάτη, όπως η εισαγωγή ενός ηλεκτρονικού τσιπ στις πιστωτικές κάρτες, αναπτύσσονται και εφαρμόζονται, ακόμα κι αν οι δαπάνες παραμένουν υψηλές. Άλλα μέτρα, όπως η εισαγωγή ενός ενιαίου αριθμού γραμμών βοήθειας της ΕΕ για να δηλώσουν μια απώλεια πιστωτικών καρτών ή μια κλοπή, συμπεριλαμβάνονται επίσης στο πρόγραμμα δράσης. Σημαντικές οργανώσεις πληρωμής όπως η Visa,American Express, και MasterCard έχουν αρχίσει ήδη να εργάζονται για να βελτιώσουν μαζί τα πρότυπα ασφάλειας στο διαδίκτυο.

Η Ένωση Υπηρεσιών Συμψηφισμού Πληρωμών (APACS) είναι το βιομηχανικό τμήμα για τις Βρετανικές τράπεζες και τις οικοδομικές κοινότητες. Επιτηρεί τη μεταφορά χρημάτων και έχει ευθύνη για τις συνεταιριστικές πτυχές των πληρωμών συμπεριλαμβανομένων των πλαστικών καρτών. Ιδρύθηκε το 1985 σαν μια μη νόμιμη ένωση σημαντικών τραπεζών και οικοδομικών εταιρειών. Η APACS δημιουργεί τις προϋποθέσεις για να συζητήσουν μη ανταγωνιστικά ζητήματα σχετικά με τη μεταφορά χρημάτων. Ένα σημαντικό μέρος της εργασίας της APACS στον τομέα πλαστικών καρτών είναι η πρόληψη απάτης, και η APACS είναι επίσης ένα τμήμα της Ένωσης της Πρωτοβουλίας Πρόληψης Απάτης των Βρετανών Ασφαλιστών παράλληλα με άλλους τομείς των οργανώσεων και της βιομηχανίας.

Το Ηνωμένο Βασίλειο έχει δει την σταθερή άνοδο απωλειών από απάτες καρτών τα τελευταία χρόνια, όπως έχουν οι περισσότερες χώρες σε όλο τον κόσμο. Το 2000, η απάτη καρτών κόστισε στο Ηνωμένο Βασίλειο £292.6 εκατομμύρια. Για να τεθούν οι αυξήσεις απάτης σε πλαίσιο, πρέπει να αναφερθεί ότι η χρήση καρτών και οι αριθμοί καρτών που εκδίδονται συνεχίζουν να υπάρχουν στο Ηνωμένο Βασίλειο. Κατά συνέπεια, οι απώλειες απάτης ενάντια στο κέρδος εργασιών είναι ακόμα λιγότερο από το μισό μέγιστο επίπεδο του 1991 που ήταν 0,33%.

Ηνωμένο Βασίλειο: Απώλειες από απάτη σε κάρτες, 2000 - 2001 (εκατομμύρια)

Κατηγορία	**1999**	**2000**	**% Διαφορά**
Πλαστογραφία	50.3	102.8	+104
Απουσία κάρτας	29.3	56.8	+94
Απώλεια / κλοπή κάρτας	79.7	98.9	+24
Υποκλοπή ταχυδρομείου	14.6	17.3	+19
Ψευδή αίτηση	11.4	10.2	-11
Άλλα	3.0	6.5	+116
Σύνολο	188.4	292.6	+55
Ποσοστό %του συνόλου	0.117	0.145	+24

Οι εγκληματίες χρησιμοποιούν διάφορες μεθόδους απάτης καρτών. Τα δύο τρίτα της απάτης στις βρετανικές κάρτες συμβαίνουν στο Ηνωμένο Βασίλειο και το υπόλοιπο εμφανίζεται στο εξωτερικό. Το μεγαλύτερο μέρος της απάτης που πραγματοποιείται στο εξωτερικό είναι στις Ηνωμένες Πολιτείες (22 τοις εκατό απώλεια στις βρετανικές κάρτες χρησιμοποιούμενες στο εξωτερικό), στην Ισπανία (16 τοις εκατό) και

στη Γαλλία (15 %). Απάτη που διαπράττεται στο εξωτερικό στις βρετανικές κάρτες αυξάνονται κατά 79 τοις εκατό το 2000 επί του αριθμού του προηγούμενου έτους, κοστίζοντας £97.2 εκατομμύρια[72].

Δύο σημαντικοί παράγοντες βρίσκονται πίσω από την αύξηση. Οι Βρετανικές πρωτοβουλίες πρόληψης της απάτης έχουν οδηγήσει τους εγκληματίες στο εξωτερικό και οι εγκληματίες κινούνται όλο και πιο γρήγορα και εύκολα από χώρα σε χώρα. Η APACS και τα μέλη της, τράπεζες, οικοδομικές εταιρίες συνεχίζουν να συνεργάζονται στενά με τη Visa και τη Europay/MasterCard στις διασυνοριακές πρωτοβουλίες κατά της απάτης.

4.3.-Τύποι απάτης

Οι τύποι απάτης που χρησιμοποιούνται από τους εγκληματίες καρτών παρατίθενται κατωτέρω:

4.3.1.- Πλαστογραφία

Η πλαστογραφία στις κάρτες κόστισε σχεδόν £102.8 εκατομμύρια το 2000, μια αύξηση 104 τοις εκατό στις απώλειες των £50.3 εκατομμυρίων το 1999. Μια πλαστή κάρτα είναι είτε μια κάρτα που έχει τυπωθεί, έχουν αποτυπωθεί σε ανάγλυφο ή έχουν κωδικοποιηθεί χωρίς άδεια από τον εκδότη, είτε μια που έχει εκδοθεί εγκύρως έπειτα άλλαξε ή κωδικοποιήθηκε εκ νέου. Οι περισσότερες περιπτώσεις πλαστογραφίας περιλαμβάνουν "το ξάφρισμα", μια διαδικασία όπου το γνήσιο στοιχείο στη μαγνητική λωρίδα μιας κάρτας αντιγράφεται ηλεκτρονικά επάνω σε άλλη χωρίς την έγκριση του πρώτου κατόχου της κάρτας. Το 1996 το 'ξάφρισμα' αποτέλεσε 20 τοις εκατό της πλαστής απάτης για να ανέλθει σε σχεδόν £3 εκατομμύρια σε απώλειες. Το 2000 οι εγκληματίες καρτών οργανώνονται όλο και περισσότερο και κατά συνέπεια η αναλογία έχει αυξηθεί σε πάνω από 72 τοις εκατό στο κόστος £74 εκατομμυρίων. Το 'ξάφρισμα' εμφανίζεται κανονικά στις λιανικές πωλήσεις, ιδιαίτερα εστιατόρια και σταθμούς βενζίνης, όπου ένας διεφθαρμένος υπάλληλος αντιγράφει τα στοιχεία της κάρτας ενός πελάτη πριν τη δώσει πίσω και πωλεί έπειτα τις πληροφορίες στους ανώτερους εγκληματίες όπου φτιάχνονται τα πλαστά αντίγραφα . Συχνά ο κάτοχος κάρτας είναι απληροφόρητος για την απάτη έως ότου φθάνει μια δήλωση που παρουσιάζει αγορές που δεν έκαναν. Είναι ζωτικής σημασίας οι κάτοχοι κάρτας να ελέγχουν τις δηλώσεις τους για οποιεσδήποτε άγνωστες συναλλαγές.

4.3.2.-. Απάτη σε τηλεφωνική παραγγελία, ταχυδρομική ή συναλλαγή μέσω Διαδικτύου

Η απάτη χωρίς τη παρουσία κάρτας εμφανίζεται όταν ούτε η κάρτα ούτε ο κάτοχός της είναι παρόντες στο σημείο πώλησης, όπως συμβαίνει στο τηλέφωνο, το fax, και τις συναλλαγές ταχυδρομικών παραγγελιών ή Διαδικτύου. Το μεγαλύτερο μέρος αυτής της απάτης εμφανίζεται μέσω της τηλεφωνικής ή ταχυδρομικής παραγγελίας και λιγότερο συχνά μέσω του Διαδικτύου (βλ. τις αγορές στο τμήμα Διαδικτύου). Αυτό το έγκλημα περιλαμβάνει τη χρησιμοποίηση των παράνομα αποκτηθέντων στοιχείων καρτών για να γίνει μια αγορά. Συνήθως τα στοιχεία αντιγράφονται χωρίς τη γνώση του κατόχου της κάρτας ή λαμβάνονται από τις απορριμμένες αποδείξεις. Λιγότερο συχνά τα στοιχεία καρτών έχουν προέλθει από τα προγράμματα που παράγουν τους αριθμούς λογαριασμού που έχουν οργανωθεί στους υπερπόντιους χώρους διαδικτύου για μικρές χρονικές περιόδους. Όπως με την πλαστή απάτη, ο νόμιμος κάτοχος κάρτας μπορεί να μην γνωρίζει την απάτη, έως ότου παραλάβει μια δήλωση.

---

[72] Card Facts: Card fraud; the facts web article, April 2002, web at:
http://www.cardwatch.org.uk/html/card_fraud_facts.html

Ένα νέο σύστημα ελέγχου κωδικών ασφάλειας διευθύνσεων και καρτών για την καταπολέμηση της απάτης χωρίς την παρουσία κάρτας αναπτύσσεται στο Ηνωμένο Βασίλειο από τον Απρίλιο του 2001 ,τό οποίο δεν απορρίπτει τις αποδείξεις και ελέγχει τις δηλώσεις για οποιεσδήποτε άγνωστες συναλλαγές.

4.3.3.- Χαμένες ή κλεμμένες κάρτες

Απάτη σε χαμένες ή κλεμμένες κάρτες κόστισε £98.9 εκατομμύρια το 2000, μια αύξηση 24% στις απώλειες των £79.7 εκατομμυρίων του 1999. Η μεγαλύτερη απάτη στις χαμένες ή κλεμμένες κάρτες πραγματοποιείται στα πρατήρια λιανικής πώλησης προτού να αναφέρει ο κάτοχος κάρτας την απώλεια. Οι εκδότες καρτών συνεχίζουν να το εξετάζουν με τη χρησιμοποίηση των ευφυών συστημάτων ανίχνευσης απάτης. Ένα σύστημα "καυτών αρχείων καρτών" χρησιμοποιείται για να διανείμει τα στοιχεία για χαμένες ή οι κλεμμένες κάρτες σε 80.000 λιανοπωλητές στο UK και να τους προειδοποιήσει ώστε να αναφέρουν τις απώλειες καρτών . Είναι ζωτικής σημασίας οι κάτοχοι κάρτας αναφέρουν τις χαμένες κάρτες στην εκδότρια τράπεζά τους αμέσως ώστε να ακυρωθεί η κάρτα.

4.3.4.- Απάτη μέσω ταχυδρομείου χωρίς απόδειξη

Ο αριθμός πλαστικών καρτών που κλάπηκαν στο ταχυδρομείο κορυφώθηκε το 1991 όταν κόστισε στη βιομηχανία £33 εκατομμύρια και παρουσίασε ακριβώς λιγότερο από 20 τοις εκατό των συνολικών απωλειών απάτης. Σε αυτό το σημείο η τραπεζική βιομηχανία διαμόρφωσε μια τρέχουσα συνεργασία με το Βασιλικό ταχυδρομείο για να επιτηρήσει και να ελέγξει τη διανομή καρτών και αυτό οδήγησε το κόστος της απάτης μέσω ταχυδρομείου κάτω των £17.3 εκατομμυρίων το 2000.

4.3.5.- Απάτη στις αιτήσεις

Η χρησιμοποίηση κλεμμένης ή πλαστής ταυτότητας ή άλλων λεπτομερειών για να ανοίξει ένας λογαριασμός καρτών μειώθηκε κατά 11 τοις εκατό από το 1999 ως το 2000, όταν κόστισε £10.2 εκατομμύρια. Η επιτυχία στη μείωση αυτού του τύπου απάτης οφείλεται στη χρήση του CIFAS : το Σύστημα Αποφυγής Απάτης στη Βρετανία και άλλα συστήματα ανίχνευσης που βοηθούν στην ανίχνευση ψευδών εφαρμογών.

4.3.6.- Απάτη στα ATM

Η πλειοψηφία των περιπτώσεων της απάτης των ATM εμφανίζεται, όταν ο νόμιμος κάτοχος της κάρτας γράψει το PIN και το κρατήσει μαζί με την κάρτα του σε ένα πορτοφόλι ή μια τσάντα που κλέβονται. Μερικές περιπτώσεις επίσης συμβαίνουν μέσω "ανίχνευσης" όπου οι εγκληματίες κοιτάζουν πίσω από τον ώμο ενός χρήστη μηχανήματος συναλλαγών για να δουν τον αριθμό της κάρτας, κατόπιν κλέβουν την κάρτα χρησιμοποιώντας τις τεχνικές απόσπασης της προσοχής ή κλοπής πορτοφολιών. Η απάτη του ATM κόστισε στη βιομηχανία £17.9 εκατομμύριο το 2000, 6 % των συνολικών απωλειών απάτης[73].

Οι πιστωτικές κάρτες εκδόθηκαν αρχικά στο Ηνωμένο Βασίλειο το 1966 και οι χρεωστικές κάρτες το 1987. Από τότε, η χρήση καρτών αυξάνεται κάθε χρόνο: στα προηγούμενα πέντε έτη ο αριθμός καρτών που εκδόθηκαν έχει αυξηθεί κατά 32 τοις εκατό. Σήμερα υπάρχουν περισσότεροι από 42 εκατομμύρια κάτοχοι

---

[73] Card Facts: Card fraud; the facts web article, April 2002, web at:
http://www.cardwatch.org.uk/html/card_fraud_facts.html

καρτών στη Μεγάλη Βρετανία και σχεδόν 127 εκατομμύρια πλαστικές κάρτες συμπεριλαμβανομένης της πιστωτικής, της χρεωστικής, των μετρητών (ATM μόνο) και των καρτών εγγύησης επιταγών.

4.3.7.- Μερικά στοιχεία για τις πιστωτικές κάρτες και τη χρήση ATMs στην Ευρώπη

89 τοις εκατό των ενηλίκων κατέχουν μια ή περισσότερες πλαστικές κάρτες, 56 τοις εκατό των ενηλίκων έχουν μια κάρτα πίστωσης/ δαπανών, 84 τοις εκατό των ενηλίκων έχουν μια χρεωστική κάρτα. Τα ποσοστά αγορών πίστωσης και χρεωστικών καρτών αναμένονται να διπλασιαστούν περισσότερο στα επόμενα δέκα έτη. Τα πρώτα ATMs εισήχθησαν το 1967. Οι πρώτες μηχανές είχαν περιορισμένες λειτουργίες, διαθέτοντας καθορισμένα ποσά μετρητών σε αντάλλαγμα των χρεών. Ήταν μόνο στη μέση της δεκαετίας του '70 όταν οι μαγνητικές λωρίδες καρτών χρησιμοποιήθηκαν, για να αποσύρουν τα μετρητά. Υπάρχουν 31.000 ATMs στο UK. Μια συνηθισμένη ημέρα υπάρχουν περίπου 5,5 εκατομμύρια αποσύρσεις μετρητών από ATMs, η μέση απόσυρση από ATM είναι £56, ένας κοινός χρήστης ATM το χρησιμοποιεί μία φορά την εβδομάδα, ο μέσος όρος εξόδων ανά πιστωτική κάρτα είναι περίπου £1,500, η μέση αγορά με μια πιστωτική κάρτα σε ένα πρατήριο λιανικής πώλησης είναι γύρω στα £52. Σχεδόν έξι δισεκατομμύρια συναλλαγές έγιναν με κάρτες το 2000.

Περίπου £160 δισεκατομμύρια ξοδεύτηκαν από τους Βρετανούς κατόχους κάρτας στις συναλλαγές λιανικής πώλησης με κάρτα το 2000, η μέση συνολική απώλεια ανά χαμένη ή κλεμμένη πιστωτική ή χρεωστική κάρτα που χρησιμοποιήθηκε παράνομα ήταν £435, £292.6 εκατομμύρια χάθηκαν από απάτη καρτών πέρυσι, σχεδόν 67 τοις εκατό όλης της παράνομης χρήσης καρτών στο UK πραγματοποιείται στα σημεία λιανικής πώλησης .

4.4.-Απάτες Διαδικτύου

Η διαδεδομένη υιοθέτηση των νέων τεχνολογιών έχει δημιουργήσει νέες ευκαιρίες για απάτη στις οποίες οποιοσδήποτε χρήστης Διαδικτύου είναι ευαίσθητος, μια κατάσταση που γίνεται χειρότερη από την άγνοια για το ζήτημα, σύμφωνα με μια μελέτη που έγινε το 2001. Η κύρια καταγγελία που αναφέρθηκε ήταν για απάτη σε δημοπρασία μέσω Διαδικτύου, με σχεδόν 66 % των καταγγελιών να προέρχονται από εκείνη την κατηγορία. Ακολουθεί η απάτη στα μη παραδοθέντα εμπορεύματα ή η πληρωμή με ποσοστό 22 τοις εκατό και η απάτη πιστωτικών ή χρεωστικών καρτών με σχεδόν 5 %

Οι αριθμοί προέρχονται από την πρώτη έκθεση σχετικά με την απάτη μέσω Διαδικτύου που δημοσιεύτηκε από το Κέντρο Καταγγελίας Απάτης Διαδικτύου (IFCC), μια συνεργασία μεταξύ του FBI και του Εθνικού Κέντρου Εγκλήματος. Η έκθεση καλύπτει το εξάμηνο από τις 8 Μαΐου έως τις 8 Νοεμβρίου του 2000. Αυτές οι απάτες οδήγησαν σε πάνω από $4,6 εκατομμύρια συνολικές απώλειες, με τη μέση απώλεια να είναι $894. Παρά το τόσο υψηλό μέσο ποσό, μόνο 17% των απωλειών ήταν πάνω από $1.000. Η πλειοψηφία των απωλειών κατέληξε σε σύνολο λιγότερο από $500. Οι απάτες στις επενδύσεις οδήγησε σε μεγαλύτερες απώλειες. Η απάτη στις δημοπρασίες, αν και είναι ο μεγαλύτερος ένοχος, οδήγησε στις χαμηλότερες μέσες απώλειες.

Οι δράστες της απάτης τείνουν να είναι άρρενες, σύμφωνα με την έκθεση, και η συντριπτική πλειοψηφία είναι Αμερικανοί πολίτες (92%) που ζουν σε μεγάλες πολιτείες. Οι περισσότεροι δράστες (17 %) ζουν στη

Καλιφόρνια. Το μέσο θύμα της σε απευθείας σύνδεσης απάτης ζει επίσης σε μεγάλες και πυκνοκατοικημένες πόλεις και είναι άρρενες μεταξύ των ηλικιών 30 και 50. Η έκθεση σημειώνει εντούτοις ότι και γυναίκες έχουν πέσει επίσης θύματα της σε απευθείας σύνδεσης απάτης. Οι ηλικίες των θυμάτων κυμαίνονται από 10 έως 100. Πάνω από 50% των θυμάτων αρχικά έρχονται σε επαφή μέσω του ηλεκτρονικού ταχυδρομείου, με 38 τοις εκατό των συμβολαίων να προέρχονται μέσω ιστοσελίδας, όπως αναφέρει η έκθεση . Οι κύριες μέθοδοι πληρωμής σε περιπτώσεις απάτης είναι επιταγές χρημάτων και πιστωτικές κάρτες. Η έκθεση περιλαμβάνει στοιχεία που λαμβάνονται από πάνω από 20.000 καταγγελίες που αρχειοθετούνται στον ιστοχώρο IFCC. Η έκθεση[74] είναι βασισμένη στις σχεδόν 6.100 καταγγελίες που αναφέρονται στην επιβολή νόμου μέχρι τις 8 Νοεμβρίου, με την πλειοψηφία των καταγγελιών να περιλαμβάνουν το Διαδίκτυο. Όμως δεν αναμειγνύουν όλες οι καταγγελίες IFCC το Διαδίκτυο.

Οι καταναλωτές έχασαν πάνω από $3,2 εκατομμύρια από απάτες μέσω Διαδικτύου πέρυσι σύμφωνα με τις συναφείς εκθέσεις της Εθνικής Καταναλωτικής Ένωσης Παρακολούθησης της Απάτης στο Διαδίκτυο. Μια αύξηση 38 τοις εκατό στις καταγγελίες απάτης μέσω Διαδικτύου το 1999 συνδυασμένη με μια μέση καταναλωτική απώλεια τουλάχιστον $580 δείχνει μια επείγουσα ανάγκη για καταναλωτική εκπαίδευση με θέμα πως να ψωνίζουμε απ' ευθείας. Οι σε απευθείας σύνδεση συναλλαγές δημοπρασίας, αν και υπάρχει πληθώρα καταγγελιών απάτης μέσω Διαδικτύου, μειώνονται. Αλλά, άλλες κατηγορίες απάτης Διαδικτύου, όπως τα σχέδια εργασίας στο σπίτι, αυξάνονται. Όπως με την απάτη τηλεαγοράς, οι Νιγηριανές προσφορές χρημάτων έχουν διαμορφώσει την στήλη των δέκα πρώτων. Οι ταξινομήσεις και τα ποσοστά των συνολικών καταγγελιών παρουσιάζονται κατωτέρω:

1999 Top 10 ΑΠΑΤΕΣ	%	Ιαν.-Σεπτ. 2000 Top 10 ΑΠΑΤΕΣ	%
Δημοπρασίες σε απ' ευθείας σύνδεση	87%	Δημοπρασίες σε απ' ευθείας σύνδεση	79%
Γενικές Πωλήσεις Εμπορευμάτων	7%	Γενικές Πωλήσεις Εμπορευμάτων	9%
Υπηρεσίες Πρόσβασης στο Διαδίκτυο	2%	Δουλειά στο Σπίτι	2%
Εξοπλισμός Υπολογιστών/ Λογισμικό	1%	Υπηρεσίες πρόσβασης στο Διαδίκτυο.	2%
Δουλειά στο Σπίτι	1%	Προπληρωμένα Δάνεια	2%
Προπληρωμένα Δάνεια	.2%	Εξοπλισμοί Υπολογιστών /Λογισμικό	1%
Πωλήσεις Περιοδικών	.2%	Νιγηριανές προσφορές χρημάτων	.7%
Υπηρεσίες πληροφόρησης Ενηλίκων	.2%	Υπηρεσίες πληροφόρησης Ενηλίκων	.6%
Ταξίδια / Διακοπές	.1%	Προσφορές Πιστωτικών Καρτών	.3%
Αγορές / Πυραμίδες Πολλών Επιπέδων	.1%	Ταξίδια/ Διακοπές	.3%

[74] Internet Fraud Complaint Center 2001b, Internet Auction Fraud, May. At, http://www1.ifccfbi.gov/strategy/AuctionFraudReport.pdf

4.5.-Παγκόσμιος κώδικας για το κυβερνο-έγκλημα

Το σχεδιάγραμμα για έναν παγκόσμιο κώδικα για το κυβερνο-έγκλημα συμφωνήθηκε στο Στρασβούργο στη Γαλλία προετοιμάζοντας το έδαφος για τους διεθνείς κανόνες που κυβερνούν την σε απευθείας σύνδεση παράβαση πνευματικών δικαιωμάτων, την σε απευθείας σύνδεση απάτη, την παιδική πορνογραφία και την κλοπή προγραμμάτων (hacking). Τα 41 μέλη του Συμβουλίου της Ευρώπης (COE) συν τις ΗΠΑ, Καναδά και Ιαπωνία υπέγραψαν ένα σχέδιο σύμβασης σχετικά με το κυβερνο-έγκλημα η επικύρωση του οποίου σε υπουργικό επίπεδο τίθεται ως στόχος το Σεπτέμβριο. Η Συνθήκη περιέχει μια σειρά διαδικαστικών δυνάμεων, συμπεριλαμβανομένης της αναζήτησης των συγκροτημάτων ηλεκτρονικών υπολογιστών και της υποκλοπής. Ο κύριος στόχος του είναι να ακολουθήσει "μια κοινή εγκληματική πολιτική που στοχεύει στην προστασία της κοινωνίας ενάντια στο κυβερνο-έγκλημα με την υιοθέτηση της κατάλληλης νομοθεσίας και την ενθάρρυνση μιας διεθνούς συνεργασίας", ισχυρίζεται το Συμβούλιο της Ευρώπης.

Τα Βασικά Κίνητρα για την Κλοπή Ταυτοτήτων

Σκοπός	**Ποσοστό**
Να ελέγχει ένα λογαριασμό πιστωτικής κάρτας	53%
Να αποκτήσει τηλεπικοινωνιακές υπηρεσίες	27%
Να ελέγχει ένα λογαριασμό επιταγών	17%
Να πάρει ένα δάνειο	11%

4.5.1.-Νομολογία

Οι νόμοι που υπάρχουν μπορούν να προσαρμοστούν στις σημερινές νέες τεχνολογίες. Παραδείγματος χάριν, ο Αμερικάνικος νόμος πνευματικών δικαιωμάτων, που δεν έχει ανανεωθεί κατά ένα μεγάλο μέρος εδώ και ένα τέταρτο του αιώνα, λειτουργεί εντυπωσιακά καλά σήμερα, λαμβάνοντας υπόψη τέτοια απρόβλεπτα ζητήματα όπως πώς να προστατεύσει το λογισμικό, τα βιβλία υπολογιστών και τα MP3 αρχεία.

Εντούτοις, όσον αφορά το έγκλημα, οι υπαρκτοί νόμοι είναι συχνά ανεπαρκείς για την εξέταση των νέων απειλών οικονομίας όπως η χάραξη και η διάδοση ιών. Οι ποινικοί νόμοι είχαν ως σκοπό να τιμωρήσουν τους ληστές τραπεζών και τους δολοφόνους, όχι εκείνους που παραμορφώνουν τους ιστοχώρους ή καταστρέφουν το εσωτερικό σύστημα ηλεκτρονικού ταχυδρομείου μιας επιχείρησης. Αλλά αυτά τα τεχνολογικά εγκλήματα, αν και δεν είναι απαραιτήτως θανατηφόρα, σίγουρα αξίζουν τιμωρία όπως τα παραδοσιακά εγκλήματα, και η ζημία που προκαλούν είναι συχνά περισσότερο διαδεδομένη. Ο Γερουσιαστής Patrick Leahy (D. VT.) πέρυσι εισήγαγε το νόμο Ασφάλειας Διαδικτύου του 2000, έναν νόμο που θα είχε τροποποιήσει τον προ πολλού υπαρκτό νόμο απάτης και κατάχρησης υπολογιστών, έναν από τους λίγους ομοσπονδιακούς νόμους που μπορούν να χρησιμοποιηθούν ενάντια στους εγκληματίες υψηλής τεχνολογίας. Ο Leahy, ένας από τους νομοθέτες διάσωσης του Διαδικτύου, πρέπει να επαινεθεί για τις προσπάθειές του, αν και οι άνθρωποι έχουν

ακόμα ερωτηματικά για το αν οι υπαρκτοί νόμοι καιρικής τροποποίησης θα ήταν η καλύτερη λύση ή η εισαγωγή απολύτως νέων νόμων είναι μια ανάγκη της εποχής.

4.6.-Μέθοδοι επαφής

Οι ιστοχώροι είναι η πιο κοινή μέθοδος στην οποία οι καταναλωτές καταφεύγουν για παράνομες προσφορές Διαδικτύου, αλλά οι στατιστικές αποκαλύπτουν μια αύξηση στον αριθμό αρχικών επαφών που γίνονται από τους καλλιτέχνες στις ομάδες πληροφόρησης:

1999 Μέθοδοι Πρόσκλησης	**%**	**Ιαν.-Σεπτ. 2000 Μέθοδοι Πρόσκλησης**	**%**
Ιστοχώροι	90%	Ιστοχώροι	84%
Ηλεκτρονικό Ταχυδρομείο	9%	Ηλεκτρονικό Ταχυδρομείο	10%
Ομάδες Πληροφόρησης	.5%	Ομάδες Πληροφόρησης	4%

4.7.-Ηλικίες των καταναλωτών

Τα θύματα της απάτης Διαδικτύου είναι νεώτερα από εκείνα της απάτης μέσω της τηλεαγοράς, αλλά ο αριθμός παλαιότερων θυμάτων Διαδικτύου αυξάνεται, από 5 τοις εκατό στην ηλικία των 60 και μεγαλύτερων το 1999, σε 6% τους πρώτους εννέα μήνες του 2000. Το ποσό των χρημάτων που οι καταναλωτές χάνουν από την απάτη Διαδικτύου, όπως την απάτη τηλεαγοράς, αυξάνεται. Η μέση απώλεια ανά άτομο ανήλθε από $310 το 1999 σε $412 στους πρώτους εννέα μήνες του 2000. Τα περισσότερα θύματα της απάτης μέσω Διαδικτύου πληρώνουν ακόμα εκτός δικτύου, με επιταγή ή διαταγή χρημάτων. Αλλά ο αριθμός πληρωμών με πιστωτική κάρτα αυξάνεται, ειδικά δεδομένου ότι οι σε απευθείας σύνδεση δημοπρασίες διευκολύνουν τους αγοραστές να πληρώσουν τους πωλητές που προσφέρουν τα αγαθά και τις υπηρεσίες μέσω των δικτύων πρόσβασης με πιστωτική κάρτα. Όπως με την τηλεαγορά, είναι ασφαλέστερο για τους καταναλωτές να πληρώνουν με τις πιστωτικές κάρτες απ' ό,τι με επιταγές ή διαταγές χρημάτων λόγω των νόμιμων δικαιωμάτων τους να αμφισβητήσουν δαπάνες σε περιπτώσεις απάτης. Εντούτοις, οι χρηματοδοτικοί οργανισμοί μπορεί να ενοχληθούν εάν οι απώλειές τους αυξάνονται λόγω των αμφισβητούμενων δαπανών:

1999		**Ιαν.-Σεπτ.2000**	
5 Κορυφαίοι τρόποι πληρωμών		**5 Κορυφαίοι τρόποι πληρωμών**	
Διαταγή χρημάτων	46%	Διαταγή χρημάτων	44%
Επιταγές	39%	Επιταγές	31%
Πιστωτική κάρτα	5%	Πιστωτική κάρτα	14%
Έλεγχος ταμία	5%	Έλεγχος ταμία	6%
Μετρητά	1%	Μετρητά	2%

Υπάρχουν δραματικές διαφορές στις μεθόδους πληρωμής για κάθε μια από τις κορυφαίες κατηγορίες απάτης Διαδικτύου. Πάλι, οι Νιγηριανές προσφορές χρημάτων δεν συμπεριλαμβάνονται επειδή δεν έχει γίνει καμία πραγματική πληρωμή.

Απάτη Διαδικτύου	**Μέθοδος πληρωμής**	
Σε απευθείας σύνδεση δημοπρασίες:	Διαταγή χρημάτων	49%
	Επιταγή	32%
	Έλεγχος ταμία	7%
	Πιστωτική κάρτα	7%
	Μετρητά	2%
Γενικές πωλήσεις εμπορευμάτων:	Πιστωτική κάρτα	27%
	Επιταγή	25%
	Διαταγή χρημάτων	25%
	Έλεγχος ταμία	6%
	Εμπόριο	5%
Εργασία στο σπίτι:	Επιταγή	38%
	Διαταγή χρημάτων	25%
	Πιστωτική κάρτα	14%
	Χρέωση τραπεζικού λογαριασμού	9%
	Χρεωστική κάρτα	3%
Υπηρεσίες πρόσβασης Διαδικτύου:	Πιστωτική κάρτα	37%
	Χρέωση τραπεζικού λογαριασμού	13%
	Επιταγή	13%
	Τηλεφωνικός Λογαριασμός	3%
	Χρεωστική κάρτα	1%
Προπληρωμένα Δάνεια:	Διαταγή χρημάτων	40%
	Μετρητά	22%
	Τηλεφωνικά	21%
	Έλεγχος ταμία	7%
	Επιταγή	4%
Εξοπλισμός υπολογιστών Λογισμικό:	Διαταγή χρημάτων	26%
	Πιστωτική κάρτα	24%
	Επιταγή	23%
	Τηλεφωνικά	14%
	Έλεγχος ταμία	8%

Πληροφορίες / υπηρεσίες ενηλίκων:	Πιστωτική κάρτα	46%
	Τηλεφωνικός λογαριασμός	24%
	Χρέωση τραπεζικού λογαριασμού	16%
	Επιταγή	5%
	Χρεωστική κάρτα	5%
Προσφορές πιστωτικών καρτών:	Χρέωση τραπεζικού λογαριασμού	64%
	Διαταγή χρημάτων	12%
	Πιστωτική κάρτα	12%
	Έλεγχος ταμία	6%
	Χρεωστική κάρτα	6%
Ταξίδι / διακοπές:	Πιστωτική κάρτα	47%
	Χρέωση τραπεζικού λογαριασμού	26%
	Επιταγή	21%
	Μετρητά	5%

Οι αναλήψεις από τους καταναλωτικούς τραπεζικούς λογαριασμούς είναι κατά πολύ οι πιο κοινές μέθοδοι πληρωμής και στην παραπλανητική τηλεαγορά και στις σε απευθείας σύνδεση προσφορές για τις πιστωτικές κάρτες. Είναι λογικό οι πιστωτικές κάρτες να μη ταξινομούνται υψηλά σε αυτήν την κατηγορία, δεδομένου ότι οι περισσότερες ψευδείς προσφορές πιστωτικών καρτών στοχεύουν στους καταναλωτές με κακή πίστωση που δεν είναι σε θέση να λάβουν τις πιστωτικές κάρτες μέσω των νόμιμων εκδοτών. Σε άλλες κατηγορίες που εμφανίζονται και στις κορυφαίες απάτες τηλεαγοράς και Διαδικτύου, τα σχέδια εργασίας στο σπίτι και τα προπληρωμένα δάνεια , οι μέθοδοι πληρωμής είναι αρκετά παρόμοιες, αλλά ένα καταπληκτικό 22 τοις εκατό των σε απευθείας σύνδεση προσφορών προπληρωμένου δανείου περιλαμβάνουν την πληρωμή με μετρητά.

4.8.-Θέση των επιχειρήσεων

Αφού το Διαδίκτυο δεν έχει κανένα γεωγραφικό όριο, η διασυνοριακή απάτη έχει τη δυνατότητα να εκραγεί, ειδικά αν οι καταναλωτές πληρώνουν απευθείας παρά στέλνοντας επιταγές ή διαταγές χρημάτων. Ενώ ο αριθμός καταγγελιών απάτης μέσω Διαδικτύου ενάντια στις Καναδικές επιχειρήσεις έχει κρατηθεί σταθερά στο 3 τοις εκατό το 1999 και τους πρώτους εννέα μήνες του 2000, οι καταγγελίες ενάντια στις επιχειρήσεις σε άλλες ξένες χώρες έχουν ανέλθει από 1% μέχρι τώρα το 2000.

Τα ίδια στοιχεία συσχετίζονται με του 2001:

2001 Στατιστικές Απάτης Διαδικτύου

2000 10 Κορυφαίες Απάτες	**%**	**Ιαν.-Οκτ. 2001 10 Κορυφαίες Απάτες**	**%**
Σε απευθείας σύνδεση δημοπρασίες	78%	Σε απευθείας σύνδεση δημοπρασίες	63%
Γενικές πωλήσεις εμπορευμάτων	10%	Γενικές πωλήσεις εμπορευμάτων	11%
Υπηρεσίες πρόσβασης Διαδικτύου	3%	Νιγηριανές προσφορές χρημάτων	9%
Εργασία στο σπίτι	3%	Υπηρεσίες πρόσβασης Διαδικτύου	3%
Δάνεια αμοιβών προόδου	2%	Υπηρεσίες πληροφοριών ενηλίκων	3%
Εξοπλισμός υπολογιστών /Λογισμικό	1%	Εξοπλισμός υπολογιστών /Λογισμικό	2%
Νιγηριανές προσφορές χρημάτων	1%	Εργασία στο σπίτι	2%
Υπηρεσίες πληροφοριών ενηλίκων	1%	Δάνεια αμοιβών προόδου	1%
Έκδοση πιστωτικών καρτών	5%	Έκδοση πιστωτικών καρτών	6%
Ταξίδι /διακοπές	5%	Επιχειρησιακές ευκαιρίες / ποσοστά	4%

4.9.-Μέθοδοι επαφής

Οι ιστοχώροι είναι ακόμα η πιο κοινή μέθοδος στην οποία καταφεύγουν οι καταναλωτές για τις ψευδείς προσφορές Διαδικτύου, αλλά οι στατιστικές αποκαλύπτουν μια αύξηση σε αριθμό αρχικών επαφών που γίνονται από τους καλλιτέχνες con στα ηλεκτρονικά ταχυδρομεία.

2000 μέθοδος πρόσκλησης		**2001 μέθοδος πρόσκλησης**	
Ιστοχώροι	82%	Ιστοχώροι	78%
Ηλεκτρονικό ταχυδρομείο	12%	Ηλεκτρονικό ταχυδρομείο	18%
Ομάδες πληροφόρησης	4%	Ομάδες πληροφόρησης	2%

4.10.-Χρήματα που χάνονται

Το ποσό των χρημάτων που οι καταναλωτές χάνουν στην απάτη Διαδικτύου αυξάνεται. Οι απώλειες είναι συνολικά $4.371.724, επάνω από τις $3.387.530 το 2000. Η μέση απώλεια ανά άτομο ανήλθε από $427 το 2000 σε $636 το 2001. Υπάρχουν σημαντικές διαφορές ανά μέσους όρους προσώπων για κάθε κατηγορία.

Κορυφαία σχέδια	**Ποσοστό απώλειας ανά άτομο**
Απευθείας Δημοπρασία	$478
Γενικές εμπορικές πωλήσεις	$845
Νιγηριανές προσφορές χρημάτων	$6,542
Υπηρεσίες πρόσβασης στο Διαδίκτυο	$568
Υπηρεσίες πληροφόρησης ενηλίκων	$234
Εξοπλισμός υπολογιστών /Λογισμικό	$1,102
Εργασία στο σπίτι	$120

4.11.-Μέθοδοι πληρωμής

Αν και οι καταναλωτές χρησιμοποιούν τις πιστωτικές κάρτες τους περισσότερο σε απευθείας σύνδεση, οι διαταγές χρημάτων είναι ακόμα ο πιο κοινός τρόπος με τον οποίο τα θύματα απάτης στο διαδίκτυο πληρώνουν για τα προϊόντα ή τις υπηρεσίες τους. Μερικές κατηγορίες παρουσίασαν μεγάλη αύξηση στις πιστωτικές κάρτες για τις πληρωμές, ενώ άλλοι όπως οι Νιγηριανές προσφορές χρημάτων συνέχισαν να παρουσιάζουν τις χρεώσεις τραπεζικού λογαριασμού και τις τηλεγραφικές υπηρεσίες ως το πιο κοινό τρόπο για να πληρώσουν.

2000. 5 κορυφαίοι τρόποι πληρωμών		**2001. 5 κορυφαίοι τρόποι πληρωμών**	
Διαταγή χρημάτων	43%	Διαταγή χρημάτων	29%
Επιταγή	30%	Πιστωτική κάρτα	28%
Πιστωτική κάρτα	11%	Επιταγή	18%
Έλεγχος ταμία	6%	Χρέωση τραπεζικού λογαριασμού	6%
Μετρητά	3%	Χρεωστική κάρτα	5%

2000 απάτη Διαδικτύου			**Ιαν.- Οκτ. 2001 απάτη Διαδικτύου**		
	Μέθοδος πληρωμής			**Μέθοδος πληρωμής**	
Σε απευθείας σύνδεση δημοπρασίες:	Διαταγή χρημάτων	48%	**Σε απευθείας σύνδεση δημοπρασίες:**	Διαταγή χρημάτων	48%
	Πιστωτική κάρτα	32%		Έλεγχος	32%
	Έλεγχος	7%		Έλεγχος ταμία	7%
	Χρέωση τραπεζικού λογαριασμού	6%		Πιστωτική κάρτα	6%
	Χρεωστική κάρτα	3%		Μετρητά	3%
Γενικά πωλήσεις εμπορευμάτων:	Πιστωτική κάρτα	28%	**Γενικές πωλήσεις εμπορευμάτων:**	Πιστωτική κάρτα	41%
	Διαταγή χρημάτων	25%		Διαταγή χρημάτων	21%
	Επιταγή	24%		Επιταγή	16%
	Έλεγχος ταμία	5%		Χρεωστική κάρτα	6%
	Χρεωστική κάρτα	5%		τηλεφωνικά	4%
Υπηρεσίες πρόσβασης Διαδικτύου:	Πιστωτική κάρτα	37%	**Υπηρεσίες πρόσβασης Διαδικτύου:**	Πιστωτική κάρτα	54%
	Τηλεφωνικός λογαριασμός	15%		Χρέωση τραπεζικού λογαριασμού	21%
	Επιταγή	14%		Επιταγή	8%
	Χρέωση τραπεζικού λογαριασμού	13%		Χρεωστική κάρτα	6%
	Χρεωστική κάρτα	9%		Διαταγή χρημάτων	4%

Εργασία στο σπίτι:	Διαταγή χρημάτων	23%	**Εργασία στο σπίτι:**	Διαταγή χρημάτων	29%
	Πιστωτική κάρτα	19%		Πιστωτική κάρτα	20%
	Χρέωση τραπεζικού λογαριασμού	9%		Χρέωση τραπεζικού λογαριασμού	12%
	Μετρητά	3%		Χρεωστική κάρτα	5%
	Επιταγή	40%		Επιταγή	29%
Λογισμικό εξοπλισμού υπολογιστών:	Πιστωτική κάρτα	24%	**Λογισμικό εξοπλισμού υπολογιστών:**	Διαταγή χρημάτων	15%
	Επιταγή	22%		Χρεωστική κάρτα	12%
	Τηλεφωνικά	13%		Επιταγή	11%
	Έλεγχος ταμία	8%		Πιστωτική κάρτα	36%
	Διαταγή χρημάτων	27%			

4.12.-Πειρατεία λογισμικού

Το παγκόσμιο ποσοστό πειρατείας λογισμικού ανήλθε πέρυσι σε 37% από 36% το 1999, εκθέτει η Συμμαχία Επιχειρησιακού Λογισμικού, μια ομάδα βιομηχανίας στην Ουάσιγκτον. Αυτό σημαίνει ότι 37% του λογισμικού που πωλείται παγκοσμίως υπολογίζεται ότι είναι πλαστό. Οι ανώτεροι υπάλληλοι τεχνολογίας ανησυχούν για την αναστάτωση η οποία έρχεται αφότου η επιθετική επιβολή μειώνει το πλαστό ποσοστό από 45% το 1995. Σε μία σειρά επιδρομών πέρυσι, οι αρχές κατάσχεσαν $2 δισεκατομμύρια στο πλαστό λογισμικό της Microsoft — ένα μέρος του ψευδούς λογισμικού που βρέθηκε στη μαύρη αγορά. Εν τω μεταξύ, η Autodesk υπολογίζει ότι 5 παράνομα αντίγραφα του λογισμικού της υπάρχουν για κάθε νόμιμο αντίγραφο, λέει ο διευθυντής κατά της πειρατείας Sandy Boulton. Στις ΗΠΑ, το ποσοστό πειρατείας κατατάσσεται ως το χαμηλότερο στο κόσμο . Ακόμα, το ένα στα τέσσερα προγράμματα λογισμικού που χρησιμοποιούνται στις ΗΠΑ θεωρείται πλαστό. Πριν την εμφάνιση του Διαδικτύου, οι παραχαράκτες πωλούσαν το ψευδές λογισμικό στις αγορές οδών και άλλων τόπων συναντήσεως. Σήμερα, πουλούν λιανικώς όλο και περισσότερο τα εμπορεύματά τους στον Δίκτυο . "Το Διαδίκτυο δεν έχει κανένα όριο, και οι εγκληματίες το ξέρουν," λέει η Cynthia Navarro, διευθύντρια κατά της πειρατείας στην κατασκευάστρια εταιρία λογισμικού Adobe Systems.

Η Microsoft έχει μια μηχανή αναζήτησης που αναζητά το Διαδίκτυο, που επιδιώκει το κλεμμένο λογισμικό. Η επιχείρηση έχει λάβει νομικά μέτρα ενάντια στους χιλιάδες ιστοχώρους που πρόσφεραν σύμφωνα με τους ισχυρισμούς τα παράνομα αγαθά. Αλλά οι κυβερνό-απατεώνες αποφεύγουν συχνά τη σύλληψη. Πλαστογραφούν τις επιγραφές ηλεκτρονικού ταχυδρομείου και χρησιμοποιούν ανώνυμα κιβώτια ταχυδρομείων. Κινούνται συχνά, μεταβάλλοντας τις διευθύνσεις και τους τηλεφωνικούς αριθμούς τους.

4.13.-Ξέπλυμα χρημάτων

Η οδηγία ξεπλύματος χρημάτων (91/308/ΕΟΚ) παρέχει τη βάση για τις προσπάθειες των κρατών μελών να αποτρέψουν τα παράνομα χρήματα να εισβάλουν στο οικονομικό σύστημα, το οποίο είναι ένα κρίσιμο

μέρος της εκστρατείας ενάντια στο εμπορίο ναρκωτικών και το οργανωμένο έγκλημα γενικά. Πράγματι, η οδηγία χρησιμεύει ως μια αναφορά στο παγκόσμιο επίπεδο για τα μέτρα άλλων χωρών για να αντιμετωπίσουν το ξέπλυμα χρημάτων. Ο ακρογωνιαίος λίθος της οδηγίας είναι η υποχρέωση στην πίστωση και τους χρηματοδοτικούς οργανισμούς να απαιτηθεί ο προσδιορισμός όλων των πελατών τους κατά την αρχή μιας επιχειρησιακής σχέσης (ιδιαίτερα το άνοιγμα ενός λογαριασμού ή την προσφορά ασφαλούς κατάθεσης), όταν μια απλή συναλλαγή ή σύνολο συναλλαγών υπερβαίνουν τα 15.000 ECU ή όταν υποψιάζονται ξέπλυμα χρημάτων (ακόμη και όταν η συναλλαγή είναι κάτω από την τιμή εισόδου στη χώρα προ δασμών[75].)

Αριθμός ύποπτων εκθέσεων συναλλαγής:

	1998	**1999**	**2000**	**2001**
Βέλγιο (1)	2183	3926	5771	7747
Δανία	200	174	254	
Γερμανία	3282	2935	3289	
Ελλάδα				38
Ισπανία		163	670	
Γαλλία	684	866	902	1213
Ιρλανδία		199	378	
Ιταλία	1034	2961	3218	
Λουξεμβούργο (2)		75	77	
Κάτω Χώρες **(ασυνήθιστος)** **(ύποπτος)**	14753 3546	15007 2994	16087 2572	17000
Αυστρία	346	310	301	
Πορτογαλία	17	85	115	129
Φινλανδία	223	190	232	206
Σουηδία	429	391	502	909
Ηνωμένο Βασίλειο	15007	13170	16125	14148

Μια περιπτωσιολογική μελέτη έγινε στην Εσθονία, η οποία περιέλαβε αυτά τα σχόλια που θα συζητηθούν αργότερα για να εξηγήσουν το τρέχον σενάριο των οργανωμένων εγκλημάτων και την οικονομική σημασία τους σε μερικές μικρές ευρωπαϊκές χώρες.

Όπως συχνά συμβαίνει σε πολλές άλλες χώρες στην Ευρώπη, έτσι και στην Εσθονία η δωροδοκία και το οργανωμένο έγκλημα έχουν εμφανιστεί με δύο σημαντικές μορφές: "παραδοσιακό" οργανωμένο έγκλημα

[75] Money laundering: EU Directive to be extended, web article, 13 July 1998 at: http://europa.eu.int/comm/internal_market/en/finances/general/launden.htm

(που συμμετέχουν, παραδείγματος χάριν, εμπόριο ναρκωτικών και εκβιασμός), και οργανωμένο οικονομικό έγκλημα (όπου η παράνομη δραστηριότητα περιπλέκεται με τη νομική επιχείρηση, όπως η εξαγωγή και η εισαγωγή).

Μια γενική αξιολόγηση θα ήταν ότι ποσό παραδοσιακού οργανωμένου εγκλήματος (με εξαίρεση το εμπόριο ναρκωτικών, το οποίο συνεχίζει να επεκτείνεται) έχει σταθεροποιηθεί, ενώ το ποσό οργανωμένου οικονομικού εγκλήματος αυξάνεται μαζί με τις αυξανόμενες ευκαιρίες (πρόσφατα, παραδείγματος χάριν, όπως αποδεικνύεται στην αυξανόμενη μαύρη αγορά για τα κινητά τηλέφωνα)[76].

Υπάρχουν αυτήν την περίοδο περίπου δέκα ως είκοσι "παραδοσιακές" οργανωμένες ομάδες εγκλήματος στην Εσθονία. Μεταξύ των σημαντικών ομάδων είναι οι ομάδες 'Kemerova', 'Novosibirski' και 'Permi'. Διάφορες ομάδες έχουν επαφές με Ρωσικές ομάδες, ειδικότερα στην περιοχή της Αγίας Πετρούπολης. Μερικά μέλη των ομάδων έχουν προέλθει από άλλα μέρη της πρώην ΕΣΣΔ, συμπεριλαμβανομένου του Αζερμπαϊτζάν, της Τσετσενίας και του Καζακστάν. Σχετικά με την εμπορία ναρκωτικών, οι επαφές περιλαμβάνουν ομάδες και σε Δυτική και Ανατολική Ευρώπη, καθώς επίσης και στις Ηνωμένες Πολιτείες. Μέχρι το σημείο που το οργανωμένο έγκλημα είναι αναμεμειγμένο στον εκβιασμό των "χρημάτων προστασίας", κάποια δωροδοκία έχει βρεθεί. Η δωροδοκία αναφέρεται επίσης για να χρησιμοποιηθεί περιστασιακά από το οργανωμένο έγκλημα στην εμπορία ναρκωτικών, το λαθραίο εμπόριο κλεμμένων οχημάτων, το τζόγο και το λαθραίο πέρασμα των μεταναστών και λιγότερο συνήθως σε σχέση με άλλες παραβάσεις[77].

4.14.-Απειλές σχετικές με το Δίκτυο

Τα πρώτα δίκτυα υπολογιστών που καθιερώθηκαν κατά τη διάρκεια της πρόσφατης δεκαετίας του '60 αναπτύχθηκαν προκειμένου να διευκολυνθεί η επικοινωνία μέσα σε μια σχετικά μικρή ομάδα επιστημόνων που ήξεραν γενικά και εμπιστεύθηκαν ο ένας τον άλλο. Επιπλέον και για στρατιωτικούς λόγους, τα πρωτόκολλα δικτύων που καθιστούν τη μεταφορά και τη μετάδοση στοιχείων πιθανές σχεδιάστηκαν αρχικά για την ευθύτητα και την ευελιξία, όχι για την ασφάλεια.

Κατά τη διάρκεια της εποχής πληροφοριών, τα συστήματα επικοινωνιών και τα δίκτυα υπολογιστών των εμπορικών, εκπαιδευτικών και κυβερνητικών τομέων περιπλέκονται όλο και περισσότερο. Ακριβώς όπως οποιοδήποτε τηλέφωνο στον κόσμο μπορεί να έχει πρόσβαση σε οποιοδήποτε άλλο, οποιοδήποτε συγκρότημα ηλεκτρονικών υπολογιστών μπορεί ενδεχομένως να συνδεθεί και να μοιραστεί τις πληροφορίες με οποιοδήποτε άλλο δικτυωμένο συγκρότημα ηλεκτρονικών υπολογιστών. Δεδομένου ότι δεν υπάρχει κανένας ελλοχεύων έλεγχος πρόσβασης μέσα στα δίκτυα όπως το Διαδίκτυο, κάθε μεμονωμένο συγκρότημα ηλεκτρονικών υπολογιστών και δίκτυο πρέπει να διατηρήσει τον έλεγχο πρόσβασής του[78].

Η τεχνολογία υπολογιστών, αν και χρήσιμη ακόμα και αναπόφευκτη σε πολλούς τομείς της ανθρώπινης δραστηριότητας, είναι επίσης τρωτή στους διάφορους κινδύνους. Αυτοί οι κίνδυνοι αυξάνονται καθώς η κοινωνία γίνεται πιο εξαρτημένη από την επεξεργασία και τη μεταβίβαση πληροφοριών. Για αυτόν τον λόγο, οι

---

[76] Paper 1: Organized Crime in Estonia. Paper presented to the Pre-Congress on Organized Crimes in the Baltic Sea Area, June 6-8 1997, Saltsjöbaden, Sweden, σσ. 4-5.

[77] Paper 2: Situation in Estonia Regarding Organized Crime. Paper presented to the Pre-Congress on Organized Crimes in the Baltic Sea Area, June 6-8 1997, σσ. 3-6.

[78] Anderson, K. (1997), Criminal Threats to Business on the Internet.

κυβερνήσεις των κοινωνιών που εξαρτώνται από την τεχνολογία πληροφοριών (IT) είναι πιο ανήσυχοι για τη δυνατότητα σημαντικής απώλειας εάν τα συστήματά τους διασπαστούν.

Στον τομέα τεχνολογίας υπολογιστών, το παρελθόν δεν είναι καλός προάγγελος του μέλλοντος. Ακόμα κι έτσι, εάν εξετάσουμε τα ανωτέρω συμπεράσματα όπως συμπτωματικά του πιο ανεπιθύμητου σεναρίου της ανάπτυξης IT για την επιχειρησιακή κοινότητα, η πρόβλεψη είναι απλή: θα υπάρξει μια αυξανόμενη απειλή των επιθέσεων στα συγκροτήματα ηλεκτρονικών υπολογιστών μέσω των δικτύων τηλεπικοινωνιών, κλοπή των τηλεπικοινωνιακών υπηρεσιών και της χρήσης των υπολογιστών για να διαπράξουν την απάτη και τα εγκλήματα του χειρισμού στοιχείων. Εντούτοις, εάν κάποιος θέσει μια άλλη ερώτηση, εάν δηλαδή οι σύγχρονες τάσεις στο έγκλημα υπολογιστών δικαιολογούν ή όχι τέτοιες προβλέψεις, η απάντηση είναι λιγότερο καθορισμένη. Αν και μερικά επιχειρήματα κοινής λογικής και διάφορες έρευνες υποστηρίζουν την άποψη ότι το κυβερνό-έγκλημα εισβάλει και θέτει μια σοβαρή διεθνή απειλή , υπάρχουν επίσης και στοιχεία που προτείνουν ότι το Διαδίκτυο είναι μια αρκετά ασφαλής θέση και ότι δεν υπάρχει κανένας λόγος για το συναγερμό.

Η εχεμύθεια και η ακεραιότητα αναφέρονται συγκεκριμένα στην πρόληψη της κοινοποίησης, την αλλαγή ή τη διαγραφή των πληροφοριών που περιλαμβάνονται στα αρχεία υπολογιστών. Η ακεραιότητα είναι ιδιαίτερα σημαντική για την κρίσιμη ασφάλεια (π.χ., έλεγχος εναέριας κυκλοφορίας), και τα οικονομικά στοιχεία που χρησιμοποιούνται για τις δραστηριότητες όπως οι ηλεκτρονικές μεταφορές κεφαλαίων και η οικονομική λογιστική. Η εχεμύθεια, στη συνέχεια, συνεισφέρει σημαντικά στα ιατρικά και ασφαλιστικά αρχεία, τα ερευνητικά στοιχεία, τις προδιαγραφές νέων προϊόντων και τις εταιρικές στρατηγικές επένδυσης. Η αναρμόδια πρόσβαση, εντούτοις, είναι κρίσιμη για όλες τις πτυχές του υπολογιστή και της ασφάλειας πληροφοριών. Μόλις εκτεθεί , το σύστημα χρησιμοποιείται έπειτα για τέτοιες παραβάσεις της εχεμύθειας και της ακεραιότητας όπως για την άνευ αδείας ανάγνωση ή την αντιγραφή των στοιχείων, την εισαγωγή των ανακριβών στοιχείων, την αλλαγή, τις προσθήκες του, κ.λ.π.

Αυτές οι παραβάσεις μπορούν στη συνέχεια να αποτελέσουν αδικήματα και να οδηγήσουν στην απόδοση εγκληματικής ευθύνης στους δράστες τους .

Εν τούτοις, οι κίνδυνοι ασφάλειας Διαδικτύου για τους καταναλωτές φαίνονται να είναι εξαπλωμένοι. Σύμφωνα με τις εκθέσεις του 'Business Week', η σε απευθείας σύνδεση απάτη είναι ασήμαντη έναντι της συνηθισμένης απάτης επιταγών. Η Αμερικανική Ένωση Τραπεζιτών υπολογίζει ότι η απάτη επιταγών κοστίζει στις τράπεζες $10 δισεκατομμύρια ετησίως, ενώ η σε απευθείας σύνδεση απάτη στοιχίζει μόνο περίπου 0,05% αυτής ($5 εκατομμύρια ετησίως)[79].

4.15.-Ασύρματες τεχνολογίες και χάραξη

Η ασύρματη δικτύωση και η ασφάλεια δικτύων μοιάζουν όπως το λάδι με το νερό. Πολλές επιχειρήσεις έχουν αρχίσει την εφαρμογή ή την εξέταση της εφαρμογής του ασύρματου LAN λόγω της ευκολίας της χρήσης, του σχετικά χαμηλότερου κόστους, και της μεταβλητότητας, αδιαφορώντας για την ασφάλεια. Εάν η επιχείρησή σας είναι μεταξύ εκείνων που επιδιώκουν τις λύσεις ασύρματης-δικτύωσης,

---

[79] Busch, M. (1997), Worried About Credit Card Fraud?
Web article, at: http:// www.av.com/fraud

υπάρχουν μερικές εκτιμήσεις που πρέπει να γίνουν. "Κίνηση υπό παρανομία" ή ' πολεμική οδήγηση' είναι μια τάση στη κοινότητα παρανομίας. Όλα όσα απαιτούνται για να αρχίσουν είναι ένας φορητός υπολογιστής, ένα αυτοκίνητο και μια κάρτα του τοπικού ασύρματου LAN. Έχει πραγματοποιηθεί μελέτη ασύρματων δικτύων στην περιοχή της Νότιας Καλιφόρνιας και σε εκείνες τις περιοχές στις οποίες ταξιδεύει κανεις για δουλειά σε μία προσπάθεια να φανεί γιατί έγινε η διαφημιστική εκστρατεία (πρέπει να πω ότι έχω εθιστεί στην αναγνώριση του ραδιοφώνου). Εγκαταστάθηκε ένα φορητός υπολογιστής με μια ασύρματη κάρτα και μια κεραία και η πορεία γύρω από την περιοχή με μια κανονική ταχύτητα, οδήγησε στην ανακαλύψη 459 ασύρματων δικτύων. Από τα δίκτυα που προσδιορίστηκαν, μόνο 24% χρησιμοποιούσαν τη συνδεδεμένη με καλώδιο ισοδύναμη μυστικότητα (WEP) που έρχεται με το περισσότερο, εάν όχι όλο, το ασύρματο υλικό. Το 'WEP' είναι μια μορφή κρυπτογράφησης που χρησιμοποιεί τον RC4 αλγόριθμο. Οι ασύρματες συσκευές δικτύωσης μπορούν να χρησιμοποιήσουν 'WEP' για να βοηθήσουν να προστατευτούν οι πληροφορίες που διαβιβάζονται.

Δυστυχώς, η έλλειψη εγκατάστασης για τις περισσότερες ασύρματες συσκευές δικτύων είναι "NO WEP." Εάν η επιχείρησή σας δεν χρησιμοποιεί 'WEP' τότε καθένας μπορεί να καθίσει στους χώρους στάθμευσης του κτηρίου σας, να εισβάλει στο δίκτυό σας και να αρχίσει να ερευνά το εσωτερικό δίκτυο σαν να καθόταν δίπλα σας με ένα καλώδιο του τοπικού LAN που συνδέθηκε με το δίκτυό σας. Το πραγματικά τρομακτικό μέρος για αυτό είναι ότι δεν είναι απαραίτητο να είστε μάγος τεχνικός για να το κάνετε αυτό. Υπάρχουν ακόμη και ιστοχώροι που απαριθμούν τα ασύρματα δίκτυα που οι άνθρωποι έχουν ανακαλύψει – η επιχείρησή σας θα μπορούσε να είναι ένας από αυτά.

Η επιχείρησή σας μπορεί να είναι τρωτή σε μια ασύρματη επίθεση ακόμα κι αν ο ασύρματος δεν έχει εφαρμοστεί στο δίκτυο. Τα σημεία πρόσβασης είναι φτηνά και μικρά και μπορούν να συνδεθούν εύκολα με το δίκτυο κάτω από καταστάσεις δοκιμής. Ένα τμήμα ή ακόμα και ένα κτήριο επιχείρησης μπορεί να έχει ένα σημείο πρόσβασης για την περιοχή τους χωρίς να συνειδητοποιούν τι κινδύνους έχουν δημιουργήσει. Υπάρχουν εργαλεία που μπορούν να χρησιμοποιηθούν για να εντοπίσουν τα σημεία πρόσβασης απατεώνων και να προσδιορίσουν το SSID, τη διεύθυνση MAC της συσκευής, το κανάλι που χρησιμοποιείται, το όνομα προμηθευτών, και ακόμα κι αν χρησιμοποιείται το WEP.

Έτσι η λύση φαίνεται αρκετά εύκολη, σωστά; Ακριβώς, ανοίξτε το WEP και όλα είναι ασφαλή πάλι. Όχι τόσο γρήγορα! Υπάρχουν πολλοί κατάλογοι κοινού που προκαθορίζουν τα κλειδιά κρυπτογράφησης WEP που ταχυδρομούνται στο διαδίκτυο και ανανεώνονται συνεχώς. Εάν η επιχείρησή σας χρησιμοποιεί την ασύρματη δικτύωση, πρέπει να σιγουρευτείτε ότι δεν χρησιμοποιούν το βασικό πρόγραμμα παραγωγής ενός προμηθευτή με κωδικό πρόσβασης εύκολο να ανακαλυφθεί. Παραδείγματος χάριν: το όνομα της επιχείρησής σας, το όνομα του προμηθευτή ασυρμάτων σας ή τη λέξη "ασύρματος," για να ονομάσουμε μερικούς.

Οι κροτίδες WEP και 802.11 sniffers έχουν αναπτυχθεί επίσης και στα Windows και στο Unix. Τι σημαίνει αυτό για σας; Ακόμα κι αν χρησιμοποιείτε WEP, οι πιθανότητες παραβίασης είναι ακόμα αρκετά υψηλές. Το AirSnort είναι μια βασισμένη στο Linux κροτίδα WEP που αρπάζει παθητικά τα πακέτα στα μέσα της πτήσης και μόλις έχει αρκετά πακέτα (100 MB-1 GB), θα ραγίσει το κλειδί ασύρματης κρυπτογράφησης χρήσιμων πακέτων μέσα σε λίγα δευτερόλεπτα. Η διαδικασία συγκέντρωσης του απαιτούμενου ποσού χρήσιμων πακέτων περίπου 1 GB αξίας, μπορεί να πάρει κάποιο χρόνο σε ένα ασύρματο δίκτυο που δεν έχει πολλή κυκλοφορία. Θυμηθείτε εν τούτοις, ο επιτιθέμενος αρκεί μόνο να αφήσει έναν υπολογιστή μέσα στη σειρά του ασύρματου δικτύου σας, αφύλακτο εάν επιθυμεί, έως ότου πάρει αρκετά πακέτα. Βεβαιώνεται ότι

αυτά τα προγράμματα θα γίνουν μόνο αποδοτικότερα και γρηγορότερα καθώς ο χρόνος περνά, αυξάνοντας πολύ τον κίνδυνο.

Εξετάστε τους έμφυτους κινδύνους ασφάλειας πριν εγκαταστήσετε τον ασύρματο. Είστε και εσείς και η επιχείρηση σας πρόθυμοι να επιτρέψετε σε έναν ξένο να συνδεθεί με το δίκτυο και να έχει πρόσβαση στα εμπιστευτικά αρχεία της επιχείρησής σας στο όνομα της μείωσης κόστους και της ευκολίας της χρήσης;. Τα οφέλη ξεπερνούν τους σημαντικότερους κινδύνους ασφάλειας; Μπορείτε να εξασφαλίσετε αποτελεσματικά ένα ασύρματο δίκτυο χρησιμοποιώντας τις μεθόδους εκτός από το WEP όπως συζητήθηκε νωρίτερα; Αυτές είναι μερικές ερωτήσεις που πρέπει να απαντηθούν προτού να εφαρμόσετε εσείς και η επιχείρηση σας την ασύρματη δικτύωση.

Εάν μια επιχείρηση έχει αρχίσει ήδη την ασύρματη δικτύωση, τότε πρέπει να σιγουρευτεί ότι, τουλάχιστον το WEP χρησιμοποιείται και ότι κανένα αναρμόδιο AP δεν υπάρχει στο δίκτυο. Μια δευτεροβάθμια μορφή "δίπλα δίπλα " κρυπτογράφησης πρέπει να ερευνηθεί και να εφαρμοστεί αμέσως. Οι στρατηγικές και οι διαδικασίες που περιλαμβάνουν την ασύρματη δικτύωση πρέπει να αναπτυχθούν και οι υπάλληλοι πρέπει να ενημερωθούν για αυτές. Η εξασφάλιση του τρέχοντος ασύρματου δικτύου σας πρέπει να γίνει μια προτεραιότητα. Εάν ένας χάκερ δεν έχει βρει το δίκτυό σας ακόμα, ένας άλλος σίγουρα θα το βρει σύντομα[80].

4.16.-Εξεταση της Ηλεκτρονικής Απάτης

Υπάρχουν τρεις γενικά-αναγνωρισμένοι τρόποι αντιμετώπισης της ηλεκτρονικής απάτης : ο σκληρός κανονισμός που περιλαμβάνει τη χρήση του νόμου, ο ήπιος κανονισμός που χρησιμοποιεί τους κώδικες συμπεριφοράς και οι στρατηγικές βασισμένες στην πρόληψη απάτης.

4.16.1.-Σκληρός κανονισμός

Ο κανονισμός της διαφήμισης και του μάρκετινγκ είναι ένα σχετικά νέο φαινόμενο που εισήχθη βαθμιαία καθώς ο εικοστός αιώνας προχώρησε. Οι ομάδες καταναλωτικής υπεράσπισης, που προέκυψαν στη δεκαετία του '70, έτειναν να απαιτήσουν την ακριβή νομική απαγόρευση των ανήθικων πρακτικών (η αποκαλούμενη σκληρή προσέγγιση κανονισμού) ενώ εκείνοι εντός της επιχειρησιακής κοινότητας θεώρησαν ότι ο μόνος κανονισμός μέσω της χρήσης των κωδίκων συμπεριφοράς ήταν εξίσου αποτελεσματικός (ηπιός κανονισμός). Με την εισαγωγή των νέων μέσων επικοινωνίας, που περιέλαβαν το τηλέφωνο, το ραδιόφωνο, την τηλεόραση και αργότερα το Διαδίκτυο, η συζήτηση ως προς την κατάλληλη μορφή που ο κανονισμός πρέπει να λάβει συνεχίζεται αμείωτη.

4.16.1.1.-Αστική δράση

Το μεγαλύτερο μέρος του περιεχομένου της διαφήμισης που εμφανίζεται στο Διαδίκτυο είναι νομίμως είτε μια πρόσκληση προς τον χρήστη να χρησιμοποιήσει το προϊόν, ή μια απλή έκθεση. Μόνο εάν οι ενδιαφερόμενοι καταναλωτές αποκρίνονται με την αποκάλυψη των προσωπικών στοιχείων τους, τα οποία μπορεί να περιλάμβάνουν τους αριθμούς λογαριασμού ενός ονόματος πιστωτικών καρτών, όνομα, διεύθυνση,

---

[80] Wireless lan: the hacker's best friend, Chad Parks, Canaudit Inc. November 2002.

τότε διαβιβάζεται μια επίσημη προσφορά αγοράς που, εάν γίνει αποδεκτή και υποστηριχθεί, θα προκαλέσει μια δεσμευτική νομικά συμφωνία.

Εκείνοι που επιδεικνύουν τις απατηλές ή παραπλανητικές διαφημίσεις στο Διαδίκτυο γενικά μόνο θα παραμείνουν εκτεθειμένοι εάν το απαράδεκτο περιεχόμενο αντιταχθεί στους όρους της συμφωνίας. Αυτό μπορεί έπειτα να προκαλέσει το δικαίωμα να ακυρωθεί η σύμβαση ή να γίνει μήνυση για τις ζημίες. Από αυτή την άποψη, η χρήση του Διαδικτύου θέτει νομικά ζητήματα που είναι ουσιαστικά τα ίδια με εκείνα που προκύπτουν από εκείνα που είναι βασισμένα στα έγγραφα διαφημίσεων και συμβάσεων. Υπάρχουν, εντούτοις, ιδιαίτερα εμφανείς και δικανικές δυσκολίες που συνδέονται με την πιστοποίηση του τι συναλλάσσεται μεταξύ των συμβαλλόμενων μερών σε μια ηλεκτρονική συναλλαγή.

4.16.1.2-Προστασία καταναλωτών

Στην Αυστραλία, ένα από τα πρώτα καταστατικά προστασίας καταναλωτών που θεσπίζονται ήταν ο Νόμος Προστασίας Αγοραστών Βιβλίων του 1899 (NSW) που επιδίωξε να ρυθμίσει τη συμπεριφορά των πλανόδιων εμπόρων που συμμετείχαν στις από σπίτι σε σπίτι πωλήσεις. Από τότε, τα πιο περιοριστικά νομοθετικά καθεστώτα έχουν επινοηθεί για να ελέγξουν τις πρακτικές μάρκετινγκ και διαφήμισης. Αυτοί οι νόμοι βοηθούν τώρα να εξασφαλίσθεί ότι οι καταναλωτές δεν εξαναγκάζονται στην αγορά των προϊόντων που δεν θέλουν και δεν εξαπατώνται από τους πωλητές. πιο χαλαρές Νομικά περίοδοι, παραδείγματος χάριν, είναι ένα παράδειγμα νομοθετικών μέσων προς τους καταναλωτές που υποβάλλονται σε τεχνική υψηλών πωλήσεων στα σπίτια τους[81]. Τόσο και οι ομοσπονδιακοί όσο και οι κρατικοί νόμοι προστασίας καταναλωτών ισχύουν για τις συναλλαγές στις οποίες περιλαμβάνονται οι Αυστραλιανοί πολίτες ή οι εταιρίες. Η Κίνηση Εμπορικών Πρακτικών του 1974 έχει τις παροχές σχετικά με την προστασία καταναλωτών στο μέρος Β που προγράφουν τις διάφορες αθέμιτες πρακτικές και διευκρινίζουν τα πρότυπα ασφάλειας προϊόντων και τη λειτουργία των όρων και των εξουσιοδοτήσεων στις συμβάσεις.

Η Κίνηση Εμπορικών Πρακτικών του 1974 είναι, εντούτοις, γενικά σιωπηλή ως προς το εάν οι παροχές της ισχύουν για τη συμπεριφορά που πραγματοποιείται ηλεκτρονικά, αν και το εύρος των ελέγχων του, μάλλον δεν θα ίσχυε για όλες τις σε απευθείας σύνδεση δραστηριότητες που πραγματοποιούνται μεταξύ των εταιριών και των καταναλωτών. Οι περισσότερες από τις διατάξεις του νόμου για την προστασίας καταναλωτών ισχύουν συγκεκριμένα για να ορίσουν τι περιλαμβάνει η χρήση των ταχυδρομικών, τηλεγραφικών ή τηλεφωνικών υπηρεσιών[82] που φαίνεται να αποκλείει το Διαδίκτυο και το ηλεκτρονικό ταχυδρομείο (που δεν είναι συγκεκριμένα τηλεφωνικά). Αυτή η ερώτηση πρέπει να καθοριστεί δικαστικώς ακόμα στην Αυστραλία, αν και το ACCC συμφωνεί ότι η διαφήμιση στο Διαδίκτυο υπάρχει στις διατάξεις του νόμου εμπορικών πρακτικών του 1974 (Cth)[83] (ACCC 1997a). Αν και οι νόμοι προστασίας καταναλωτών της Αυστραλίας ίσχυαν για τις συμβάσεις για την αγορά των αγαθών και των υπηρεσιών που εισάγονται με τους εμπόρους που έχουν διαφημίσεις στο Διαδίκτυο, η επιβολή της ευθύνης μπορεί να είναι δύσκολη και δαπανηρή όπου περιλαμβάνονται οι υπερπόντιες εταιρίες. Οι περισσότεροι νόμοι ισχύουν μόνο για τις συναλλαγές που

---

[81] Goldring, Maher, McKeough, and Pearson, G. 1998, σσ. 270-306
[82] The Trade Practices Act 1974, σ. 6 (3)
[83] Australian Competition and Consumer Commission 1997a
http://www.accc.gov.au

πραγματοποιούνται μεταξύ των Αυστραλιανών πολιτών και των εταιριών μέσα στην Αυστραλία. Το κόστος, η δυσχέρεια, και οι διοικητικές μέριμνες των διασυνοριακών νομικών διαδικασιών κάνουν την επιβολή της ευθύνης στους κατασκευαστές, τους διανομείς, και τους εμπόρους έξω από την Αυστραλία μη εφαρμόσιμη για τους περισσότερους καταναλωτές.

4.16.1.3.-Εγκληματική δράση

Όπου η ιδιοκτησία έχει ληφθεί από εξαπάτηση ή όπου ψεύτικα έγγραφα έχουν χρησιμοποιηθεί, για να διαπράξουν μια απάτη, ίσως είναι δυνατό να γίνει εγκληματική πράξη. Η δίωξη εγκλημάτων και η τιμωρία στοχεύουν να αποτρέψουν εκείνους που διαπράττουν τις παραβάσεις από την επανάληψη αδικήματος και επίσης να αποτρέψουν άλλους στην κοινότητα από να ενεργήσουν παράνομα. Είναι δύσκολο να μετρηθεί ο ακριβής βαθμός στον οποίο ο νόμος αποτρέπει το έγκλημα, αν και οι καλά-κοινοποιημένες αυστηρές προτάσεις ενεργούν σαφώς ως αποτρεπτικός παράγοντας ως ένα ορισμένο βαθμό.

Εκτός από τις συμβατικές δικαστικές τιμωρίες όπως τα πρόστιμα και η φυλάκιση, υπάρχουν ποικίλες άλλες συνέπειες που μπορούν να ακολουθήσουν την ανίχνευση της παράνομης σε απευθείας σύνδεση ενέργειας. Αυτές περιλαμβάνουν τη δυσμενή δημοσιότητα, τις επαγγελματικές πειθαρχικές κυρώσεις, την αστική δράση, τις διατακτικές διαταγές και, πρόσφατα, τις διάφορες μορφές κοινοτικής σύσκεψης. Η κατάσχεση της περιουσίας ενός παραβάτη αντιπροσωπεύει επίσης τα αποτελεσματικά μέσα αποτροπής της παράβασης.

Υπάρχουν, εντούτοις, διάφορα νομικά προβλήματα που συνδέονται με την εξαπάτηση παρουσιάσεων αποδείξεων που πραγματοποιείται ηλεκτρονικά. Αυτά εξετάζονται βαθμιαία από οργανισμούς όπως η Πρότυπη Εγκληματικός Κώδικας Επιτροπής Ανώτερων Υπαλλήλων (2000) που στο πιο πρόσφατο έγγραφο συζήτησής της για τα εγκλήματα υπολογιστών και τις αρμοδιότητες έχει εξετάσει πολλά από τα προβλήματα που προκύπτουν στη δίωξη των εγκλημάτων της απιστίας που διαπράττονται ηλεκτρονικά. Παραμένουν, εντούτοις, οι διάφορες δικανικές δυσκολίες που συνδέονται με τη συγκέντρωση των στοιχείων από τους υπολογιστές σε διάφορες διαφορετικές αρμοδιότητες που καθιστούν συχνά τα πρακτικά και δύσκολα και δαπανηρά.

4.16.2.-Ήπιος κανονισμός

Λαμβάνοντας υπόψη τις πρακτικές δυσκολίες που συνδέονται με τη στήριξη επάνω στις νομοθετικές ρυθμιστικές προσεγγίσεις για να ελέγχουν παραπλανητική και απατηλή σε απευθείας σύνδεση συμπεριφορά, διάφορες ομάδες βιομηχανίας έχουν δημιουργήσει τις αυτορυθμιστικές ομάδες που έχουν επινοήσει τα πρότυπα και τους κώδικες συμπεριφοράς τους. Αυτοί δημιουργήθηκαν αρχικά για να εξετάσουν τις μη-ηλεκτρονικές μορφές διαφήμισης και μάρκετινγκ, αλλά επεκτείνονται τώρα για να εξετάσουν τη συμπεριφορά στον ψηφιακό κόσμο.

4.16.2.1.-Ικανοποιητικός κανονισμός

Μια από τις αρχικές στρατηγικές που επιδιώκει να αποτρέψει το απατηλό και παραπλανητικό υλικό από το να διαδοθούν ηλεκτρονικά έχει σχέση με τον κανονισμό του σε απευθείας σύνδεση περιεχομένου. Αυτό μπορεί να γίνει μέσω της χρήσης του λογισμικού διαλογής ή μέσω των μέτρων που απαιτούν οι φορείς παροχής

υπηρεσιών Διαδικτύου να ελέγξουν το υλικό που κοινοποιείται στα δίκτυά τους. Οι πρόσφατες προτάσεις συνεπάγονται επίσης ένα στοιχείο του σκληρού κανονισμού μέσω της ποινικοποίησης του περιεχομένου που κρίνεται να είναι ακατάλληλο και που έχει διαδοθεί δημόσια. Αν και η χρήση του λογισμικού διαλογής έχει υποστηριχτεί ευρέως για να ελέγξει την πρόσβαση στα άσεμνα και απαράδεκτα υλικά, η χρήση της στον έλεγχο της απατηλής και της παραπλανητικής διαφήμισης μπορεί να είναι δυσκολότερη. Συχνά η εξαπάτηση δεν είναι ευδιάκριτη από μια εικόνα ή μια περιγραφή του εν λόγω προϊόντος και είναι αδύνατο να γίνει διαφοροποίηση μεταξύ μιας νόμιμης διαφήμισης και μιας διαφήμησης που περιέχει κάποιο παραπλανητικό περιεχόμενο μόνο βάσει των λέξεων ή των εικόνων που χρησιμοποιούνται. Αντ' αυτού, οι διάφορες ομάδες βιομηχανίας έχουν αναπτύξει τις οδηγίες για τους φορείς παροχής υπηρεσιών Διαδικτύου για να ακολουθήσουν κατά ρύθμιση του περιεχομένου του υλικού που εμφανίζεται στα δίκτυά τους. Η ένωση βιομηχανίας Διαδικτύου, παραδείγματος χάριν, αναγνωρίζει ότι το Διαδίκτυο πρέπει να παρέχει όλα τα μέσα που χρειάζονται για να επιτραπεί ο έλεγχος της πρόσβασης στο περιεχόμενο αναγνωρίζοντας ότι δεν είναι πρακτικό να φιλτράρουν όλο το περιεχόμενο του Διαδικτύου. Συνεπώς, η Ένωση επικυρώνει τις μεθόδους με τις οποίες το περιεχόμενο μπορεί να αναγνωριστεί και να αποκλειστεί ενδεχομένως από τις ικανοποιητικές τεχνολογίες φιλτραρίσματος του περιεχομένου ως τα πρακτικότερα μέσα ενδυνάμωσης των αρμόδιων ενηλίκων για να ελεγθεί η πρόσβαση στο Διαδίκτυο και να καθορισθούν οι κατάλληλοι έλεγχει στο περιεχόμενο. Όπως με τον κανονισμό σεξουαλικά ρητού, ρατσιστικού, ή άλλου παράνομου περιεχόμενου, τα θέματα της ελευθερίας της ομιλίας και της πρακτικότητας της ρύθμισης του περιεχομένου είναι οι σημαντικότεροι τομείς ανησυχίας στην υιοθέτηση των ικανοποιητικών ρυθμιστικών προσεγγίσεων.

4.17.-Υπηρεσίες πιστοποίησης και επικύρωσης

Σαν εναλλακτική λύση της χρήσης των απαγορευτικών σχεδίων που επιδιώκουν να προσδιορίσουν το μη αποδεκτό περιεχόμενο και να αποτρέψουν τους χρήστες από το να αποκτήσουν πρόσβαση σε αυτό, διάφορες υπηρεσίες πιστοποίησης και επικύρωσης έχουν καθιερωθεί και παρέχουν στους χρήστες τις πληροφορίες ως προς την αξιοπιστία και την αποδοχή του σε απευθείας σύνδεση υλικού. Οι χρήστες είναι έπειτα ελεύθεροι να αποφασίσουν, εάν επιθυμούν ή όχι να χρησιμοποιήσουν το εν λόγω υλικό.

Το Πρόγραμμα για την Επιλογή Περιεχομένου Διαδικτύου (2000), παραδείγματος χάριν, είναι ένα εθελοντικό σύστημα εκτίμησης περιεχομένου που βοηθά τους χρήστες να προσδιορίσουν το υλικό που συμμορφώνεται με τα διευκρινισμένα πρότυπα. Αν και αυτό έχει χρησιμοποιηθεί πρώτιστα, για να εξετάσει το άσεμνο και απαράδεκτο περιεχόμενο, θα μπορούσε να προσαρμοστεί, για να εξετάσει το απατηλό και παραπλανητικό περιεχόμενο επίσης. Στις Ηνωμένες Πολιτείες, το Συμβούλιο των Καλύτερων Επιχειρησιακών Γραφείων δημιουργεί μια υπηρεσία πιστοποίησης, η οποία εγκρίνει τις επιχειρησιακές περιοχές Διαδικτύου. Οι περιοχές που επιδεικνύουν την εξουσιοδοτημένη και κρυπτογραφημένη σφραγίδα της έγκρισης συμφωνούν να τηρήσουν τα πρότυπα πραγματικής διαφήμισης του Συμβουλίου και να υιοθετήσουν τις διαδικασίες σχεδίου διαφωνίας. Τα μέλη των εγκεκριμένων Ενώσεων Διαδικτύου είναι σε θέση να επιδείξουν το γεγονός της ιδιότητας μέλους τους και οι καταναλωτές είναι σε θέση να ελέγξουν για να δουν εάν οι οργανώσεις, στην πραγματικότητα, έχουν την ιδιότητα μέλους. Το πρόγραμμα WebTrust, που αναπτύχθηκε από το Αμερικανικό Ίδρυμα Επικυρωμένων Επαγγελματικών Λογιστών (2000), πιστοποιεί τους χώρους Διαδικτύου που παρουσιάζουν υγιείς σε απευθείας σύνδεση επιχειρησιακές πρακτικές, αφού τις υποβάλει σε μια εκτενή

διαδικασία ελέγχου. Ο λογιστικός έλεγχος[84], που ποικίλλει στο κόστος ανάλογα με την πολυπλοκότητα της επιχείρησης και της περιοχής, περιλαμβάνει τον έλεγχο των μέτρων ασφάλειας της περιοχής, πρακτικές μυστικότητας καθώς και τα συστήματα συναλλαγής-επεξεργασίας. Η υπηρεσία είναι διαθέσιμη από οποιαδήποτε WebTrust-με άδεια CPA ή λογιστική επιχείρηση. Δεδομένου ότι το AICPA[85] άρχισε το πρόγραμμα WebTrust, περίπου 1.500 CPAs και εβδομήντα πέντε λογιστικές επιχειρήσεις είχαν τα προσόντα να παρουσιάσουν το λογιστικό έλεγχο WebTrust[86]. Μέχρι σήμερα, μόνο ένας μικρός αριθμός περιοχών έχει υποβληθεί επιτυχώς στη διαδικασία λογιστικού ελέγχου, που επιτρέπει σε αυτούς να επιδείξουν τη σφραγίδα WebTrust στο δίκτυο τους. Όπως άλλα προγράμματα πιστοποίησης τρίτων, το WebTrust εξαρτάται για την επιτυχία του από τη διαδεδομένη αποδοχή από τους σε απευθείας σύνδεση εμπόρους και τους χρήστες, η οποία, ενδεχομένως, θα επιτευχθεί εγκαίρως.

Οι υπηρεσίες πιστοποίησης και επικύρωσης έχουν δύο αρχικά οφέλη. Κατ' αρχάς, οι καταναλωτές είναι σε θέση να στηριχθούν επάνω στο γεγονός πιστοποίησης του εμπόρου προκειμένου να έχουν κάποιο μέτρο εμπιστοσύνης στην αξιοπιστία εκείνου του εμπόρου και στη διαθεσιμότητα των μηχανισμών επανόρθωσης, εάν προκύψουν προβλήματα. Αφετέρου, οι χρηματοδοτικοί οργανισμοί που συμμετέχουν στην παροχή των ευκολιών πληρωμής θα μπορούσαν να ενθαρρυνθούν, για να ασχοληθούν μόνο με τους εγκεκριμένους εμπόρους που έχουν συμφωνήσει να συμμορφωθούν με έναν κώδικα δεοντολογίας που ανταποκρίνεται σε ορισμένες βασικές αρχές. Αυτό θα παρείχε μια ισχυρή βιομηχανία-βασισμένη στην παρότρυνση των εμπόρων να υποβληθούν στην πιστοποίηση και να ενεργήσουν υπεύθυνα και σύμφωνα με τους καθιερωμένους κώδικες συμπεριφοράς. Ένα από τα κύρια προβλήματα για την επικύρωση και την πιστοποίηση είναι ο πολλαπλασιασμός των υπηρεσιών και ο προσδιορισμός των κατάλληλων προτύπων. Ήδη, περίπου είκοσι αποκαλούμενα 'Webseals' είναι στην κυκλοφορία στην Αυστραλία με την κυβέρνηση να παρέχει έναν συγκριτικό πίνακα που καθορίζει τις διάφορες ιδιότητές τους[87] (τμήμα επικοινωνιών, τεχνολογίας πληροφοριών και τεχνών) . Ο καθορισμός αποδεκτών προτύπων και η κοινοποίηση αυτών αντιπροσωπεύει μια σημαντική πρόκληση για το μέλλον.

4.18.-Στρατηγικές Πρόληψης

Εκτός από τη χρήση και των σκληρών και μαλακών-ρυθμιστικών προσεγγίσεων, πολλά μπορούν να επιτευχθούν μέσω των στρατηγικών πρόληψης απάτης. Αυτά μπορούν να επεκταθούν από τη δημιουργία των οδηγιών και των πολιτικών για τον έλεγχο απάτης, στη χρήση των βασισμένων σε υπολογιστή τεχνικών ασφάλειας.

4.18.1.-Διαχείριση του ελέγχου απάτης

Η υιοθέτηση των πολιτικών ελέγχου απάτης μέσα στις οργανώσεις είναι ένας από τους κύριους τρόπους καταπολέμησης της απάτης στα ηλεκτρονικά καθώς επίσης και στα μη-ηλεκτρονικά περιβάλλοντα. Η

---

[84] J.J. Bloombecker, Computer Crime and Abuse, The EDD Auditor Journal, 1990.ii. σσ. 34-41.
[85] American Institute of Certified Professional Accountants (2000).
[86] Tweney, D. 1998, 'Sex scam points out lack of safeguards in online business', 3 August, at: http://www.tweney.com/prophet/980803prophet.htm
[87] Department of Communications, Information Technology and the Arts 2000b 'Shopping on the Internet: Facts for Consumers',
http://www.dcita.gov.au/shoponline

καθιέρωση των αρχών[88], παραδείγματος χάριν, στην ηθική χρήση των τεχνολογιών πληροφοριών και πώς μπορεί να αποκριθεί στις περιπτώσεις απάτης είναι ουσιαστική στη διεύθυνση μιας επιχείρησης οποιουδήποτε είδους είτε χρησιμοποιεί το ηλεκτρονικό εμπόριο είτε όχι.

Ιδιαίτερης σπουδαιότητας είναι η ανάγκη να αναπτυχθούν οι συγκεκριμένες πολιτικές για την ασφάλεια υπολογιστών μαζί με τις κατάλληλες οδηγίες για την υποβολή εκθέσεων κακής χρήσης και κατάχρησης υπολογιστών. Οι πολιτικές έχουν να αντιμετωπίσουν συγκεκριμένη σε απευθείας σύνδεση συμπεριφορά των υπαλλήλων, όπως η ασφάλεια των συστημάτων επικύρωσης χρηστών (π.χ. κωδικοί πρόσβασης), της πρόσβασης και της χρήσης των υπολογιστών για ιδιωτικούς λόγους, η προσωπική χρήση του ηλεκτρονικού ταχυδρομείου, η μεταφόρτωση του λογισμικού, και η χρήση του υλικού πνευματικών δικαιωμάτων. Οι αρχές πρέπει επίσης να καθιερωθούν για να εξασφαλίσουν ότι εκείνοι που καταδεικνύουν την παράνομη συμπεριφορά δεν αδικούνται από τη συμπεριφορά τους.

4.18.2.-Έλεγχος Προσωπικού

Μια από τις σημαντικότερες περιοχές στις οποίες η βασισμένη στην τεχνολογία απάτη μπορεί να περιοριστεί βρίσκεται στην εξασφάλιση ότι αξιόπιστο και υπεύθυνο προσωπικό[89] απασχολείται, ιδιαίτερα στις ανώτερες και υπεύθυνες θέσεις. Η διοίκηση των σύγχρονων τεχνολογικά-βασισμένων συστημάτων ασφάλειας περιλαμβάνει ένα ευρύ φάσμα προσωπικού από εκείνους που συμμετέχουν στην κατασκευή των συσκευών ασφάλειας μέχρι εκείνους που διατηρούν τις ευαίσθητες πληροφορίες σχετικά με τους κωδικούς πρόσβασης και τα αρχεία λογαριασμών. Κάθε ένας έχει τη δυνατότητα να χρησιμοποιήσει τις εμπιστευτικές πληροφορίες ή τις εγκαταστάσεις για να διαπράξει απάτη ή, πράγμα που είναι πιθανότερο να εμφανιστεί, να συνεργήσει με ανθρώπους έξω από τον οργανισμό και να διαπράξει μια παράβαση.

Η παρεμπόδιση τέτοιων δραστηριοτήτων απαιτεί μια εφαρμογή αποτελεσματικών διοικητικών διαδικασιών κινδύνου που επεκτείνονται από τη διαλογή προϋπηρεσίας του προσωπικού στον κανονικό έλεγχο του εργασιακού χώρου. Οι υπάλληλοι που εργάζονται για πολλά χρόνια και έχουν αποκτήσει την ιδιαίτερη γνώση διαδικασιών ασφάλειας μιας οργάνωσης πρέπει να ελεγχθούν ιδιαίτερα, δεδομένου ότι είναι αυτοί που γνωρίζουν τις ευκαιρίες απάτης και είναι επιρρεπείς στο να τη διαπράξουν.

4.18.3.-Έλεγχος χρήσης υπολογιστών

Η χρήση των υπολογιστών από τους υπαλλήλους και των σε απευθείας σύνδεση δραστηριοτήτων τους μπορεί να ελεγχθεί μέσω της χρήσης του λογισμικού που καταγράφει τη χρήση και επιτρέπει στους διευθυντές να ξέρουν, παραδείγματος χάριν, εάν το προσωπικό έχει χρησιμοποιήσει το Διαδίκτυο για μη σχετικές με τη δουλειά δραστηριότητες. Ιδανικά, πρέπει να θεσπιστούν συμφωνηθέντες διαδικασίες και κανόνες που να επιτρέπουν στο προσωπικό να ξέρει ακριβώς το βαθμό στον οποίο οι υπολογιστές είναι σε θέση να χρησιμοποιηθούν για τις ιδιωτικές δραστηριότητες, εάν όχι καθόλου. Εάν το προσωπικό επιτρέπεται να χρησιμοποιήσει τους υπολογιστές για ιδιωτικούς λόγους, οι διαδικασίες πρέπει να είναι σε ισχύ, για να προστατεύσουν τη μυστικότητα και την ασφάλεια των επικοινωνιών, υποβάλλοντας, φυσικά, στους

---

[88] Ε.Λαμπροπούλου, Κοινωνιολογία του Ποινικού Δικαίου και Θεσμών της Ποινικής Δικαιοσύνης, Αθήνα Ελληνικά Γράμματα, 1999. σσ. 54.55

[89] K.Titdemann, Η Εγκληματικότητα στον Χώρο των Ηλεκτρονικών Υπολογιστών και η Γερμανική Μεταρρύθμιση του Ποινικού Δικαίου,1996.(Μετάφραση Μπιτζελέκη, σ.13. Δημοσιεύματα του Ελληνικού Τμήματος της Διεθνούς Εταιρείας Κοινωνικής Αμύνης, Τευχ.-4/1999.

υπαλλήλους να υπακούνε το νόμο. Όπου ορισμένες σε απευθείας σύνδεση δραστηριότητες έχουν απαγορευθεί, είναι δυνατό να ελεγχθούν οι δραστηριότητες του προσωπικού, μερικές φορές συγκεκαλυμμένα όπως μέσω της τηλεοπτικής επιτήρησης ή τον έλεγχο του ηλεκτρονικού ταχυδρομείου και των αρχείων που διαβιβάζονται μέσω των κεντρικών υπολογιστών. Το φιλτράρισμα του λογισμικού μπορεί επίσης να χρησιμοποιηθεί για να αποτρέψει το προσωπικό από τη συμμετοχή σε ορισμένες δραστηριότητες.

Το 'Surfwatch' , παραδείγματος χάριν, μπορεί να προσαρμοστεί για να αρνηθεί την πρόσβαση υπαλλήλων στο διευκρινισμένο περιεχόμενο. Όταν ο υπάλληλος ζητά μια περιοχή, το λογισμικό ελέγχει την ταυτότητα του χρήστη ως προς το επιτρεπόμενο περιεχόμενο για την συγκεκριμένη κατηγορία και κατόπιν είτε δίνει τη ζητούμενη σελίδα είτε πληροφορεί το χρήστη ότι το αίτημα έχει απορριφθεί. Το λογισμικό καταγράφει επίσης τα απορριφθέντα αιτήματα για την επόμενη επιθεώρηση από τη διοίκηση.

4.19.-Μέσα ανίχνευσης απάτης

Η χρήση του λογισμικού υπολογιστών για να ελέγξει τις επιχειρησιακές δραστηριότητες παρέχει επίσης αποτελεσματικά μέσα ανίχνευσης της απάτης και αποτρέπει τα άτομα από το να ενεργήσουν παράνομα.

4.19.1.-Προσωπικός προσδιορισμός

Η επικύρωση της ταυτότητάς κάποιου είναι κρίσιμη στην παρεμπόδιση της ηλεκτρονικής απάτης. Αυτή τη στιγμή, οι περισσότερες διαδικασίες επικύρωσης περιλαμβάνουν τη χρήση των κωδικών πρόσβασης ή PINs. Η εξασφάλιση ότι αυτοί χρησιμοποιούνται προσεκτικά και δεν είναι ικανοί να εκτεθούν σε κίνδυνο αντιπροσωπεύει ένα θεμελιώδες μέτρο ελέγχου της απάτης. Εκτός από την εκπαίδευση χρηστών, ποικίλες καινοτόμες ιδέες έχουν αναπτυχθεί για να προστατεύσουν τους κωδικούς πρόσβασης και να ενισχύσουν την επικύρωση χρηστών[90]. Υπάρχουν διαθέσιμα συστήματα που αλλάζουν τους κωδικούς πρόσβασης τακτικά ή αρνούνται την πρόσβαση μετά από έναν διευκρινισμένο αριθμό διαδοχικών δοκιμών χρησιμοποιώντας λάθος κωδικούς πρόσβασης. Τα τερματικά έχουν επινοηθεί με αυτόματες εγκαταστάσεις κλεισίματος που λειτουργούν όταν δεν χρησιμοποιηθούν για καθορισμένες περιόδους.

Οι μιας χρήσεως κωδικοί πρόσβασης όπου ο κωδικός πρόσβασης αλλάζει με κάθε διαδοχική σύνδεση σύμφωνα με ένα συμφωνηθέν πρωτόκολλο που είναι γνωστό στο χρήστη και το χειριστή συστημάτων είναι επίσης διαθέσιμοι. Τα πρωτόκολλα πρόκλησης-απάντησης και τα συστήματα επανάκλησης έχουν επινοηθεί επίσης ως μέσο πραγματοποίησης της αναγνώρισης των χρηστών. Τέλος, γεωδαιτικές μέθοδοι χώρου έχουν επινοηθεί για να επικυρώσουν τις φυσικές θέσεις των χρηστών.

Στο μέλλον, πολλά συστήματα επικύρωσης χρηστών θα χρησιμοποιήσουν τα αποκαλούμενα βιομετρικά προσδιοριστικά που χρησιμοποιούν τα μοναδικά φυσικά χαρακτηριστικά ενός ατόμου. Κοινά παραδείγματα περιλαμβάνουν τα δακτυλικά αποτυπώματα, τον τόνο της φωνής, τα σχέδια δακτυλογράφησης, τις αμφιβληστροειδικές εικόνες, την γεωμετρία του προσώπου ή των χεριών, και ακόμη και τον προσδιορισμό των υποδόριων δομών φλεβών ενός προσώπου ή των μυρωδιών σωμάτων[91] (Johnson 1996). Αν και τέτοια συστήματα επιτυγχάνουν πολύ πιο υψηλά επίπεδα ασφάλειας από εκείνα που στηρίζονται επάνω στους

---

[90] Alexander, M. 1995, *The Underground Guide to Computer Security*, Addison-Wesley Longman Inc., New York.

[91] Johnson, E. 1996, 'Body of evidence: How biometric technology could help in the fight against crime', *Crime Prevention News*, December, σσ.17–19.

κωδικούς πρόσβασης, είναι ακριβά για να εισαγάγουν και να προκαλέσουν πιθανά προβλήματα από την άποψη της μυστικότητας και της εχεμύθειας των προσωπικών στοιχείων που αποθηκεύονται στα δίκτυα. Είναι επίσης δύσκολο να ανακληθούν τα βιομετρικά προσδιοριστικά ταυτότητας.

Η αυθεντικότητα των χρηστών είναι επίσης απαραίτητη όταν χρησιμοποιούνται οι δημόσιες βασικές υποδομές. Τα δημόσια βασικά συστήματα είναι ένας τρόπος να εξασφαλίσθεί ότι και οι καταναλωτές και οι έμποροι είναι βέβαιοι για την ταυτότητα του προσώπου με το οποίο συνεργάζονται. Τέτοιες τεχνολογίες, εντούτοις, δεν θα απέτρεπαν τα άτομα από το να αποκτήσουν παράνομα πρόσβαση στα ιδιωτικά κρυπτογραφικά κλειδιά με την κλοπή των σημείων που κρατούν τα κλειδιά ή με την παρουσίαση της κατασκευασμένης τεκμηρίωσης προκειμένου να ληφθούν τα βασικά ζευγάρια με απάτη[92]. Εντούτοις, αντιπροσωπεύουν έναν ασφαλέστερο τρόπο στη διεύθυνση των σε απευθείας σύνδεση συναλλαγών από το να εμπιστευθούν απλά το υλικό που επιδεικνύεται στο Διαδίκτυο και ελπίζουν ότι θα είναι ασφαλείς οι υπηρεσίες πληροφοριών .

4.19.2.-Η Προληπτική Δράση

Η Προληπτική Δράση μπορεί επίσης να λάβει τη μορφή κανονικής επιτήρησης του Διαδικτύου από τους ρυθμιστές προκειμένου να βρεθούν οι απαράδεκτες και παράνομες πρακτικές, που παρέχουν εκπαιδευτικό υλικό προειδοποιώντας τους χρήστες για επικίνδυνα σχέδια και τη χρήση των τεχνολογιών επικύρωσης για να επιτρέψει στα άτομα να ξέρουν με βεβαιότητα με ποιόν συνεργάζονται μέσα στον σε απευθείας σύνδεση κόσμο.

Οι περισσότερες ρυθμιστικές αντιπροσωπείες παρέχουν σε όλο τον κόσμο τις πληροφορίες με έντυπο και ηλεκτρονικά μέσω των ιστοχώρων που προειδοποιούν τους καταναλωτές για τις παραπλανητικές και απατηλές πρακτικές. Ένα από τα περιεκτικότερα βιβλία που απευθύνονται στους Αυστραλούς καταναλωτές είναι το μικρό μαύρο βιβλίο 'Scams' που δημοσιεύεται από το υπουργικό Συμβούλιο σχετικά με τις καταναλωτικές υποθέσεις (1999). Με ηλεκτρονική μορφή[93], ο ιστοχώρος του ACCC δίνει συμβουλές για τα σχέδια πώλησης πυραμίδων, τα σχέδια επιχειρησιακής ευκαιρίας και τα τηλεφωνικά βραβεία και τις λαχειοφόρες αγορές. Τα παραδείγματα των δημοφιλών παραπλανητικών πρακτικών παρατίθενται μαζί με τις νομικές ποινικές ρήτρες που ισχύουν για εκείνους που κάνουν ή συμμετέχουν σε τέτοιες δραστηριότητες. Επιπλέον, και προκειμένου να ενισχυθεί η καταναλωτική εμπιστοσύνη στο Διαδίκτυο, η Αυστραλιανή κυβέρνηση έχει παραγάγει μια σειρά ενημερωτικών δελτίων που παρέχουν τις πληροφορίες στους καταναλωτές για τους κινδύνους των σε απευθείας σύνδεση αγορών, και ορισμένα άλλα ζητήματα όπως η πληρωμή των φόρων και δασμών και θέματα εχεμύθειας[94].

Το ACCC[95] έχει διατυπώσει επίσης την ιδέα της χρησιμοποίησης των μεσαζουσών πληροφοριών για να παρέχει τις πληροφορίες για τους σε απευθείας σύνδεση εμπόρους και τις διαδικασίες που περιλαμβάνονται στη

---

[92] Office of Government Information Technology 1998.
[93] Australian Competition and Consumer Commission '
http://www.accc.gov.au
[94] Department of Communications, Information Technology and the Arts 2000a 'Shopping on the Internet: Facts for Consumers',
http://www.dcita.gov.au/shoponline
[95] Australian Competition and Consumer Commission, 1997b.

διεύθυνση της επιχείρησης σε απευθείας σύνδεση, παρόμοιες με τα είδη πληροφοριών που οι μεσίτες ασφάλειας ή υποθηκών παρέχουν. Διάφορες ιδιωτικές επιχειρήσεις, συμπεριλαμβανομένης της Αυστραλιανής Ένωσης Καταναλωτών, έχουν οργανώσει μια ανεξάρτητη υπηρεσία συμβουλών στα δάνεια και υποθήκες που προσφέρθηκαν on-line από τους χρηματοδοτικούς οργανισμούς ενώ οι διάφορες υπηρεσίες καταναλωτικής συνδρομής δημοσιεύουν τις ανεξάρτητα πραγματοποιημένες αξιολογήσεις των προϊόντων που πρόσφεραν σε απευθείας σύνδεση. Οι καταναλωτικές ομάδες παρέχουν γενικά μια καλή πηγή εμπιστευμένων πληροφοριών για το πώς να αποφύγουν την απάτη.

Οι ομάδες, όπως η Αυστραλιανή Ένωση Καταναλωτών, διευθύνουν τη δοκιμή προϊόντων τους και τις υπηρεσίες και κοινοποιούν τα αποτελέσματα μέσω συνδρομητικών περιοδικών όπως η 'Επιλογή'(Αυστραλία). Αν και οι οργανώσεις καταναλωτών παρέχουν ήδη τις καταναλωτικές πληροφορίες με τα διάφορα μέσα, συμπεριλαμβανομένου του Διαδικτύου, ίσως ο ρόλος των καταναλωτικών ομάδων στην παροχή των υπηρεσιών πληροφοριών θα μπορούσε να αυξηθεί.

---

http://www.accc.gov.au

Κεφάλαιο V:

Περίληψη, συζήτηση και συστάσεις

5.1.-Περίληψη

Διάφοροι επαγγελματίες της εγκληματολογίας λένε ότι τα οικονομικά αδικήματα αποτελούν τη μέγιστη απειλή για την κοινωνία, αν και δεν είναι τόσο θεαματικά όσο τα βίαια εγκλήματα και τα εγκλήματα ιδιοκτησίας (ο πληθυσμός φοβάται πιο πολύ) ή οι παραβάσεις που προτιμώνται από τους δυνατούς, όπως τα εγκλήματα που έχουν σχέση με τα ναρκωτικά ή τις περιπτώσεις δωροδοκίας. Συνεπώς, η περισσότερη ζημιά γίνεται από τα οικονομικά αδικήματα που διαπράττονται σε μια οργανωμένη μορφή.

Η λεπτομερής ανάλυση αυτών των παραβάσεων θα υπερέβαινε το πεδίο της παρούσας μελέτης. Επομένως, στρέφουμε ακριβώς την προσοχή σε μερικές απόψεις. Το πεδίο της εγκληματολογικής έννοιας του οικονομικού εγκλήματος είναι αρκετά ευρύτερο από τον κύκλο των εγκλημάτων που οι Εγκληματικοί Κώδικες των διαφορετικών χωρών και οι διαφορετικές χρονικές περίοδοι καθορίζουν.

Το οικονομικό έγκλημα σχετίζεται μόνο σ'ένα βαθμό με το έγκλημα 'λευκού περιλαμίου'[96]. Με την πάροδο του χρόνου όμως οι δύο έννοιες απομακρύνονται η μία από την άλλη. Τα οικονομικά εγκλήματα δεν πρέπει να περιοριστούν στα διανοητικά εγκλήματα, αν και είναι κυρίως το οικονομικό έγκλημα που μπορεί πρώτιστα να χαρακτηριστεί ως μια διανοητική παράβαση.

Υπάρχουν κάποιοι τύποι οργανωμένων εγκλημάτων που δεν προκαλούν μεγάλη ζημιά στην οικονομία. Αυτό μπορεί να αποδειχθεί από το γεγονός ότι όλες οι μορφές οργανωμένου εγκλήματος αναμειγνύονται στα ενδιαφέροντα της νόμιμης οικονομίας, δεδομένου ότι αυτές οι παραβάσεις συμβαδίζουν με μερικές ιδιαίτερες και ανεξέλεγκτες μετακινήσεις χρημάτων. Περαιτέρω, ο κρατικός έλεγχος και ο προγραμματισμός της απασχόλησης θα επηρεαστούν επίσης από το οργανωμένο έγκλημα. Και τελικά, το οργανωμένο έγκλημα έχει πάρει επίσης μια λειτουργία παρέκκλισης των τιμών και των αμοιβών.

Το οργανωμένο έγκλημα γενικά, το οργανωμένο οικονομικό έγκλημα ειδικότερα, δεν θα περιοριστεί στις παράνομες επιχειρήσεις. Οι κεφαλαιοκρατικές οργανώσεις (τυπικά απολύτως νομικές, αλλά που κάνουν κακή χρήση της μονοπωλιακής θέσης τους) έχουν έναν αποφασιστικό ρόλο στην νέο-αποίκιση της οικονομίας από μερικές μικρότερές ή μεγαλύτερες ομάδες χωρών και ορισμένες περιοχές ή ηπείρους. Οι χώρες, όπου η αλλαγή του πολιτικού συστήματος πραγματοποιήθηκε στο τέλος του 20ού αιώνα, έπρεπε να παλέψουν ενάντια και στις δύο μορφές οργανωμένου εγκλήματος ταυτόχρονα.

Συζήτηση

5.2.-Απάτη στο μέλλον

Η πιο πρόσφατη έκθεση από τους εμπειρογνώμονες στην Εθνική Εγκληματική Υπηρεσία Πληροφοριών λέει ότι το οργανωμένο έγκλημα θα γίνει περιπλοκότερο και πιο δικτυωμένο στο εγγύς μέλλον. Αναμένουν τις αποδόσεις των 'τσιπ' υπολογιστών και των σπάνιων μετάλλων να κυκλοφορήσουν στο εμπόριο μεταξύ των κυκλωμάτων εγκλήματος για να αποφύγουν τα ηλεκτρονικά ίχνη.

---

[96] Ferenc Irk and Géza Finszter, Organized crime in East-Central Europe, on the Verge of the European Union), 2000

Οι εγκληματίες έχουν εκμεταλλευτεί ήδη τις σε απευθείας σύνδεση τραπεζικές εργασίες και το τζόγο, σύμφωνα με μια πηγή, και αναπτύσσουν τα εικονικά ναρκωτικά - μηχανές που θα υποκινήσουν τα μέρη του εγκεφάλου. Αυτή η τεχνολογία καλείται 'cybernarcotics'. Αυτά τα φάρμακα εικονικής πραγματικότητας μπορούν να μεταδοθούν μέσω Διαδικτύου ή με τη χρησιμοποίηση των ραδιοκυμάτων.

Λόγω των προόδων στα συστήματα προσδιορισμού μέσω της βιομετρικής οι πράκτορες προσδοκούν ότι τα περιστατικά απαγωγής θα αυξηθούν, δεδομένου ότι η πρόσβαση στα κεφάλαια δεν μπορεί να γίνει χωρίς ένα ζωντανό θέμα. Η αυξανόμενη κατάρτιση στην αντιμετώπιση της απαγωγής έχει αρχίσει ήδη να πραγματοποιείται σε αρκετές από τις ημερήσιες διατάξεις των αντιπροσωπειών.

Εκτός από τη γνωστή χάραξη στους υπολογιστές, οι πρόσφατα ανεπτυγμένες μέθοδοι διάσπασης του ευαίσθητου εξοπλισμού υπολογιστών που χρησιμοποιούν τις συσκευές ακτινοβολίας υψηλής έντασης μπορούν να είναι η πηγή σχεδίων εκβιασμού και αισχροκέρδειας ή τρομοκρατικών δραστηριοτήτων, σύμφωνα με τους σύγχρονους τεχνικούς.

Οι εμπειρογνώμονες ασφάλειας επιμένουν ότι η κατάσταση δεν είναι μάταιη. Ο Bill Wipprecht, διευθυντής ασφάλειας της τράπεζας Wells Fargo στο Σαν Φραντσίσκο, δηλώνει ότι ενώ φαίνεται ότι το "παιχνίδι και τα κίνητρα" ευνοούν τον εγκληματία, με την ασφάλεια που παίζει 'πρόληψη' δεν λύνεται το θέμα.

Η "τρέχουσα και η μελλοντική τεχνολογία είναι το μέγιστο προτέρημά μας στον πόλεμο ενάντια στα οικονομικά εγκλήματα," είπε. "Ενώ συχνά φαίνεται ότι ο εγκληματίας μπορεί να κερδίζει βραχυπρόθεσμα, είμαστε στο στάδιο της εκτεταμένης χρήσης των έξυπνων καρτών, της βιομετρικής, της περαιτέρω ανάπτυξης των νευρικών-δικτύων, της υιοθέτησης της κρυπτογράφησης παγκοσμίως και της διαμόρφωσης νέων συμμαχιών μεταξύ των παραδοσιακών ομάδων ασφάλειας και των αντίστοιχων IT τους. Έχουμε δει τη θέσπιση των καλύτερων νόμων υπολογιστών και των επιθετικών καταδιώξεων. Αυτά θα είναι τα εργαλεία πρόληψης εγκλήματος της οικονομικής βιομηχανίας του 21ου αιώνα.

"Στην πραγματικότητα, είναι πάντα οι εγκληματίες που παίζουν "τρέξιμο" αφού αναγκάζονται να εφεύρουν νέα εργαλεία ή μεθόδους για να παρακάμψουν τις τεχνολογικές προόδους στην ασφάλεια."

Ο Roger Snell, Ανώτερο Στέλεχος Επίλυσης Θεμάτων Απάτης στην Carreker- Antinori στο Ντάλλας συμφωνεί. "Πολλές τράπεζες ξεπερνούν ήδη την καμπύλη, εφαρμόζοντας τα συστήματα ανίχνευσης απάτης για τα στοιχεία βάρους, καταθέσεις και σχετικές με τον αφηγητή συναλλαγές," είπε. "Αυτά τα συστήματα, μαζί με άλλες διοικητικές λύσεις κινδύνου όπως η ανίχνευση τοκογλύφων, η θετική πληρωμή, η νέα διαλογή λογαριασμού, κ.λπ. έχουν μειώσει εντυπωσιακά τη σχετική με έλεγχο απάτη στο παρελθόν, και καθώς καθορίζονται, θα διαχειριστούν επίσης τις μελλοντικές εξελίξεις.

"Καθώς η ηλεκτρονικοποίηση του συστήματος πληρωμής συνεχίζεται, η οικονομική βιομηχανία έχει συνειδητοποιήσει την σημασία της γνώσης ότι ο πελάτης των POS ή POP θα γίνει ακόμα σημαντικότερος από σήμερα. Με όλα αυτά τα συστήματα διαχείρισης κινδύνου, ο εγκληματίας θα είναι ακόμα ο ηττημένος.[97]"

Μερικά κράτη και δήμοι έχουν χρησιμοποιήσει τη βιομετρική, για να αποτρέψουν την απάτη σε όφελος των προγραμμάτων κοινωνικής ευημερίας. Έχουν συνειδητοποιήσει ουσιαστική μείωση κόστους με την απαίτηση των υποψηφίων προγράμματος να υποβάλλονται σε ηλεκτρονική ανίχνευση δακτυλικών αποτυπωμάτων ως τμήμα της διαδικασίας εγγραφής. Χρησιμοποιώντας αυτήν την μέθοδο, έχουν αρνηθεί τα οφέλη στα άτομα που προσπάθησαν να λάβουν τα διπλά οφέλη. Ο ηλεκτρονικός προσδιορισμός δακτυλικών

[97] Bankers' Hotline,2000, Vol. 9, No. 12, 1/00

αποτυπωμάτων προσφέρει μια ελπιδοφόρο λύση για την αποτροπή της απάτης και στις φάσεις εγγραφής και εκταμίευσης του κυβερνητικού προτεινόμενου προγράμματος EBT[98]. Από τα βιομετρικά συστήματα προσδιορισμού που αναθεωρήσαμε, επιλέξαμε τη δακτυλοσκοπία ως το πιο βιώσιμο για την επαλήθευση της ταυτότητας ενός παραλήπτη σε ένα περιβάλλον EBT. Το επιλέξαμε λόγω (1) της καθολικής αποδοχής του ως θετικό μέσο για την επαλήθευση ταυτότητας και (2) της εκτενούς ιστορίας αξιοπιστίας του στο χώρο επιβολής νόμου. Η δακτυλοσκοπία ωφελεί τους υποψηφίους κατά τη διάρκεια της φάσης εγγραφής θα μείωνε τις απώλειες σχετικές με την υποβολή αιτήσεων των υποψηφίων για τις διπλές πληρωμές με διαφορετικά ονόματα και θα απέτρεπε εκείνες άλλων που έχουν την τάση .Τέτοια επαλήθευση στη φάση εκταμίευσης θα συνέδεε άμεσα τις αποσύρσεις με τους παραλήπτες και θα επίλυε αποτελεσματικά το ζήτημα των πιθανών απωλειών και των αυξανόμενων δαπανών. Οι ομοσπονδιακοί κανονισμοί θα περιόριζαν την καταναλωτική ευθύνη όταν χρησιμοποιούνται κατα τρόπο άσχημο οι χαμένες ή κλεμμένες κάρτες EBT. Εντούτοις, το ζήτημα σχετικά με το ποιος θα είναι υπεύθυνος για τις απώλειες πέρα από το καταναλωτικό όριο, το οποίο θα μπορούσε να είναι εκτενές, είναι ακόμα εκκρεμές.

Η αποτελεσματικότητα ενός προγράμματος EBT που εξασφαλίζεται από το βιομετρικό προσδιορισμό για να αποτρέψει την απάτη πρέπει να εξεταστεί σε ένα περιβάλλον EBT, προτού το πρόγραμμα επεκταθεί σε εθνικό επίπεδο. Η ανάπτυξη και η δοκιμή ενός βιομετρικού συστήματος μπορούν να καθυστερήσουν την προτεινόμενη ημερομηνία εφαρμογής της ομάδας εργασίας για το πρόγραμμα EBT 1999 και θα αύξαναν το αρχικό κόστος του προγράμματος. Εντούτοις, τα μακροπρόθεσμα οφέλη ενός βιομετρικού συστήματος θα συνέβαλαν σε ένα πιο φορολογικά υγιές και ασφαλές πρόγραμμα EBT.

Η διαθέσιμη τεχνολογία, συμπεριλαμβανομένης της βιομετρικής, υπάρχει για να βοηθήσει τη μείωση δυνατοτήτων απάτης στα προγράμματα EBT. Παραδείγματος χάριν, μερικά κράτη και τοπικές κυβερνήσεις έχουν αρχίσει να χρησιμοποιούν το αυτοματοποιημένο σύστημα προσδιορισμού δακτυλικών αποτυπωμάτων (AFIS) για να αποτρέψουν την απάτη στα κοινωνικά προγράμματα υπηρεσιών κατά τη διάρκεια του σταδίου εγγραφής με τον προσδιορισμό των επόμενων αιτημάτων για διπλά οφέλη από ένα άτομο. Η ευρύτατα κοινοποιημένη προσπάθεια —το νομικό τμήμα δημόσιων κοινωνικών υπηρεσιών του Λος Άντζελες —άρχισε να χρησιμοποιεί τη ζωντανή ανίχνευση των δακτυλικών αποτυπωμάτων δεικτών για να εγγράψει τους υποψηφίους για τη συμμετοχή σε ένα από τα προγράμματα κοινωνικής ευημερίας της το 1991 . Το EBT αποτρέπει αποτελεσματικά την απάτη στα οφέλη από την παράδοση σφραγίδων τροφίμων. Κατά συνέπεια, ένα πρόγραμμα EBT χωρίς την ενισχυμένη ασφάλεια της βιομετρικής επαλήθευσης προκαλεί μια γνήσια ανησυχία για τη δυνατότητα αυξανόμενων δαπανών και απωλειών προγράμματος. Η ανησυχία αυξάνεται με την πρόταση να επεκταθεί το EBT σε άλλα ομοσπονδιακά, κρατικά, ή προγράμματα τοπικής κυβέρνησης που περιλαμβάνουν δισεκατομμύρια δολαρίων —όπως AFDC, WIC, η κοινωνική ασφάλιση και τα ομοσπονδιακά οφέλη αποχώρησης —και με την πλήρη εφαρμογή του κανονισμού E[99].

Λόγω της καθολικής αποδοχής των δακτυλικών αποτυπωμάτων ως μέσα για τις ταυτότητες, της εκτενούς ιστορίας αξιοπιστίας της στο χώρο επιβολής νόμου, και τις επιτυχίες με την τεχνολογία AFIS, πιστεύουμε ότι η επαλήθευση δακτυλικών αποτυπωμάτων είναι η βιομετρική μορφή που προσφέρει τη μέγιστη δυνατότητα για την επιτυχία και την αποδοχή στην εξασφάλιση των συστημάτων EBT από την απάτη.

---

[98]EBT,1995: Electronic Benefits Transfer, Use of Biometrics to Deter Fraud in the Nationwide EBT Program,
[99] EBT,1995: Electronic Benefits Transfer, Use of Biometrics to Deter Fraud in the Nationwide EBT Program.

Περαιτέρω, ένα σύστημα ΕΒΤ με επαλήθευση δακτυλικών αποτυπωμάτων θα απομάκρυνε αποτελεσματικά τις ανησυχίες δαπανών /απωλειών που προκαλούνται από την εφαρμογή του κανονισμού Ε.

Τα δακτυλικά αποτυπώματα έχουν χρησιμοποιηθεί από τις αντιπροσωπείες επιβολής νόμου για σχεδόν 100 έτη για να προσδιορίσουν τους εγκληματίες και επάνω στη σύλληψη και μετά από τη σύγκριση των δακτυλικών αποτυπωμάτων στον τόπο του εγκλήματος με τα ήδη καθιερωμένα εγκληματικά αρχεία δακτυλικών αποτυπωμάτων. Τα δακτυλικά αποτυπώματα παρέχουν και ένα σύστημα μόνιμου και θετικού προσδιορισμού για την επιβολή νόμου καθώς και για πολιτικούς λόγους. Αν και δύο σχέδια δακτυλικών αποτυπωμάτων μπορούν να είναι παρόμοια, κανένα δακτυλικό αποτύπωμα δεν έχει βρεθεί που να περιέχει τα ίδια μεμονωμένα χαρακτηριστικά κορυφογραμμών. Αυτά τα χαρακτηριστικά υπάρχουν στα φυσιολογικά χέρια και πόδια μερικούς μήνες πριν από τη γέννηση και είναι σταθερά, εκτός από τυχαία ζημία, μέχρι την αποσύνθεση μετά από το θάνατο[100].

5.3.-Σύσταση

Μερικά νέα αξιοσημείωτα γεγονότα είναι τα ακόλουθα:

Η Ευρωπαϊκή Ένωση έχει προτείνει μια χονδροειδή κίνηση από το έγγραφο στα ηλεκτρονικά τιμολόγια Φ.Π.Α. Για τις επιχειρήσεις που συμμετέχουν στο ευρωπαϊκό ηλεκτρονικό εμπόριο, αυτό είναι ένα τεράστιο βήμα προς τα εμπρός στην πραγματοποίηση μεγαλύτερης απόδοσης από τις χωρίς χαρτί συναλλαγές. Είναι μια πρόταση που στοχεύει στην αφαίρεση ενός τεράστιου όγκου τιμολογίων κάτω από τον οποίο αυτές οι επιχειρήσεις θάβονται. Εντούτοις, τα ηλεκτρονικά τιμολόγια που κινούνται μέσω του ανοικτού Διαδικτύου παρουσιάζουν πολλές ευκαιρίες για απάτη. Οι Επίτροποι της ΕΕ βασίζονται στις προηγμένες ηλεκτρονικές υπογραφές για να προστατεύσουν την ακεραιότητα του συστήματος τιμολογίων Φ.Π.Α.

Στις 17 Νοεμβρίου, 2000 η Ευρωπαϊκή Επιτροπή εξέδωσε μια πρόταση οδηγίας σχετικά με την τιμολόγηση Φ.Π.Α. Η πρόταση περιέλαβε τις διατάξεις να παρουσιαστεί το σύστημα Φ.Π.Α στο 21ο αιώνα. Αυτά περιλαμβάνουν τις απαιτήσεις να εναρμονιστεί η μορφή και το περιεχόμενο των τιμολογίων Φ.Π.Α των διαφορετικών κρατών μελών. Η πρόταση καθορίζει επίσης τους κανόνες για την έκδοση και την αποθήκευση των ηλεκτρονικών τιμολογίων Φ.Π.Α και κινείται τώρα προς τα μεμονωμένα κράτη μέλη της ΕΕ για έγκριση.

Πιθανώς, η χρήση των ηλεκτρονικών υπογραφών για να ασφαλισθεί η ακεραιότητα των τιμολογίων θα αποζημιώσει την τρέχουσα αβεβαιότητα του ανοικτού Διαδικτύου. Εν πάση περιπτώσει, η πρόταση δεν υποβάλλει οποιεσδήποτε άλλες συστάσεις ασφάλειας. Παραδείγματος χάριν, η πρόταση δεν συστήνει την υποχρεωτική χρήση της κρυπτογράφησης. Επίσης, η πρόταση απαγορεύει συγκεκριμένα τα κράτη μέλη από την απαίτηση της προηγούμενης έγκρισης της ηλεκτρονικής τιμολόγησης.

Αυτήν την περίοδο, οι χρήστες των τιμολογίων Φ.Π.Α εγγράφου πρέπει να αποθηκεύσουν αυτά για μια ορισμένη χρονική περίοδο. Η εξέταση του όγκου του τιμολογίου είναι ένα μεγάλο φορτίο. Η απαίτηση αποθήκευσης παραμένει για τα ηλεκτρονικά τιμολόγια. Εντούτοις, αυτά τα τιμολόγια μπορούν να αποθηκευτούν σε ηλεκτρονική μορφή. Η πρόταση απαιτεί αυτά τα αποθηκευμένα ηλεκτρονικά τιμολόγια να είναι αμέσως προσιτά για μια ορισμένη χρονική περίοδο. Επιπλέον, τα τιμολόγια πρέπει να αποθηκευτούν κατά τέτοιο τρόπο ώστε το περιεχόμενό τους να μην μπορεί να αλλάξει.

---

[100] EBT,1995: Electronic Benefits Transfer, Use of Biometrics to Deter Fraud in the Nationwide EBT Program.

5.4.-Παραχάραξη και ασφάλεια

Η αύξηση του ηλεκτρονικού εμπορίου σε μια δικτυωμένη εποχή υπολογιστών αυξάνει τα νέα διλήμματα ασφάλειας για τους χρηματοδοτικούς οργανισμούς. Οι πελάτες θέλουν εικοσιτετράωρη πρόσβαση Διαδικτύου στους λογαριασμούς, αλλά απαιτούν επίσης περισσότερη μυστικότητα και εχεμύθεια των οικονομικών αρχείων.

Αυτές οι απαιτήσεις φαίνονται να συγκρούονται, επειδή η εικοσιτετράωρη πρόσβαση Διαδικτύου ανοίγει νέες πύλες για τους σοβαρούς ελέγχους ασφάλειας. Εξετάστε τα γεγονότα κατωτέρω:

Οι πρόσφατες έρευνες του FBI αποκάλυψαν ότι διάφορες οργανωμένες ομάδες 'χάκερ' από την Ανατολική Ευρώπη είχαν διαπεράσει τα συγκροτήματα ηλεκτρονικών υπολογιστών Αμερικάνικου ηλεκτρονικού εμπορίου για να μεταφορτώσουν τις πληροφορίες ιδιοκτησίας, τις βάσεις δεδομένων πελατών, και τις πληροφορίες πιστωτικών καρτών. Σε μερικές περιπτώσεις, οι πληροφορίες πωλούνται στις οργανωμένες ομάδες εγκλήματος.

Η Ομάδα Αντιμετώπισης Έκτακτης Ανάγκης υπολογιστών στο Πανεπιστήμιο Carnegie Mellon εκθέτει ότι έγιναν κατ' εκτίμηση 21.000 επιθέσεις στους ιστοχώρους πέρυσι, μια δεκαπλάσια αύξηση σε μόλις τρία έτη. Πολλές παρεμβάσεις είναι εσωτερικές. Μια έρευνα που πραγματοποιήθηκε από το Ίδρυμα Ασφάλειας Υπολογιστών και το FBI αναφέρει ότι 71% των εναγομένων ανακάλυψε ότι αναρμόδια πρόσβαση στα δίκτυα υπολογιστών γίνεται από τους υπαλλήλους τους.

Οι χάκερ, εσωτερικοί ή εξωτερικοί, προσπαθούν σπάνια να αλλάξουν τα αρχεία. Ψάχνουν για εμπιστευτικές οικονομικές πληροφορίες, όπως οι αριθμοί πιστωτικών καρτών, οι αριθμοί λογαριασμού, οι προσωπικές πληροφορίες, και η οικονομική αξία.

Οι καταναλωτές ξέρουν την αξία των προσωπικών πληροφοριών, και θέλουν να τις προστατεύσουν. Το Κογκρέσο αποκρίθηκε με το νόμο Gramm-Leach- Bliley του 1999 (GLBA). Το GLBA περιγράφει τις διαδικασίες με σκοπό να βοηθήσουν στην προστασία της ασφάλειας των οικονομικών πληροφοριών των πελατών. Αυτό περιλαμβάνει περισσότερα από την αποκάλυψη της πολιτικής εχεμύθειας στους πελάτες ετησίως και της προσφοράς μιας επιλογής αποχώρησης. Περιλαμβάνει ένα ενσωματωμένο πρόγραμμα ασφάλειας πληροφοριών στο εκάστοτε ίδρυμα και συστήνει έναν ανεξάρτητο τρίτο φορέα να εξετάσει τους βασικούς ελέγχους μέσα στο σύστημα ασφάλειας πληροφοριών πριν από την επόμενη ρυθμισμένη εξέτασή .

Εν ολίγοις, κάνετε όλα τα απαραίτητα για να εξασφαλιστούν οι πληροφορίες πελατών από την απώλεια μέσω κλοπής, ατυχήματος, αμελών διαδικασιών, απροσεξίας στη λεπτομέρεια, αφού το εμπιστευτήκατε στην προσοχή του ανεκπαίδευτου προσωπικού, αφήνοντας το αφύλακτο, παραμελώντας να δώσετε λόγο για αυτό, ξεχνώντας που τις βάζετε και επιτρέποντας αναρμόδια πρόσβαση σε αυτές.

Οι περισσότερες παραβιάσεις ασφάλειας είναι αποτρέψιμες με απλές προφυλάξεις. Οι εμπειρογνώμονες βιομηχανίας υπολογίζουν ότι πάνω από 80% των επιτυχών επιθέσεων 'χάκερ' θα μπορούσε να έχει αποτραπεί μέσω αυτών των απλών βημάτων:

5.4.1.-Βελτιώσεις λογισμικού

Όταν οι χάκερ ανιχνεύουν την ευπάθεια στο εταιρικό λογισμικό, μοιράζονται τις πληροφορίες μεταξύ τους, συνήθως μέσω του Διαδικτύου. Οι προμηθευτές λογισμικού αναπτύσσουν τις βελτιώσεις εισάγοντας έτσι την τεχνολογία των αντιβιοτικών[101] για να επιδιορθώσουν αυτές τις αδυναμίες. Οι εξουσιοδοτημένοι χρήστες των προγραμμάτων τους μπορούν να μεταφορτώσουν αυτές τις αδυναμίες , που ταχυδρομούνται στο διαδίκτυο, ελεύθερα. Οι χρήστες παραμελούν συχνά να ακολουθήσουν τις ταχυδρομήσεις και δεν μεταφορτώνουν τις αδυναμίες .

Είναι ευθύνη του διευθυντή συστημάτων σας να κρατήσει το λογισμικό σας συμπεριλαμβανομένης της αντιπυρικής ζώνης που αναβαθμίζεται. Αυτό απαιτεί το δυναμικό καθημερινό έλεγχο για τις αδυναμίες συστημάτων. Ανάλογα με τον αριθμό προγραμμάτων λογισμικού που τρέχουν στο σύστημά σας, δεν είναι ασυνήθιστο να υπάρξουν διάφορα ελαττώματα εβδομαδιαίως για να μεταφορτώσει και να εγκαταστήσει.

Οι 'χάκερ' είναι ενημερωμένοι. Το ίδρυμά σας πρέπει να είναι, επίσης.

5.4.2.-Κωδικοί πρόσβασης

Η ασφάλεια που περιβάλλει τους κωδικούς πρόσβασης είναι συχνά χαλαρή. Οι κωδικοί πρόσβασης πρέπει να συνδυάζουν αριθμούς και γράμματα. Οι υπάλληλοι πρέπει να τα απομνημονεύσουν και να μην τα μοιραστούν με τους συναδέλφους. Οι παραβιάσεις κωδικού πρόσβασης που αναφέρονται συνήθως στους λογιστικούς ελέγχους ασφάλειας περιλαμβάνουν:

Συστήματα που δεν αρνούνται την πρόσβαση όταν πληκτρολογεί ένας χρήστης το λανθασμένο προσωπικό κωδικό τρεις φορές: Το λογισμικό 'χάκερ' θα εξετάσει κάθε λέξη στο λεξικό ως κωδικό πρόσβασης έως ότου κάποια λειτουργήσει. Οι κωδικοί πρόσβασης που συνδυάζουν αριθμούς και γράμματα επίσης θα αρνηθούν την πρόσβαση σε αυτούς τους 'χάκερ'.

Αποτυχία από το διευθυντή συστημάτων να αλλαχτεί ο κωδικός πρόσβασης προεπιλογής στο νέο λογισμικό δικτύων ή/ και αντιπυρικών ζωνών: Οι 'χάκερ' ξέρουν τους κωδικούς πρόσβασης προεπιλογής, επίσης.

Πορεία λιγότερης αντίστασης: Θα μπορούσατε να ξοδέψετε εκατομμύρια ενισχύοντας το σύστημα ασφάλειάς σας. Ακόμα όμως, ένας πολυμήχανος χάκερ μπορεί πιθανώς να το διαπεράσει. Ευτυχώς, εν τούτοις, οι περισσότεροι 'χάκερ' ακολουθούν την πορεία της μικρότερης αντίστασης. Εάν είναι πάρα πολύ δύσκολο να εισβάλουν στο σύστημά σας, θα κινηθούν προς έναν ευκολότερο στόχο.

Δεν μπορείτε πιθανώς να εξουδετερώσετε τους 'χάκερ', αλλά μπορείτε να εξουδετερώσετε άλλα ιδρύματα έτσι οι χάκερ δεν θα σας ενοχλήσουν[102]. (B on-line, 2002)

5.5.-Η ανάγκη για νομοθεσία υπολογιστών

Σύμφωνα με το FBI, περίπου 10.000 καταγγελίες κυβερνό-εγκλήματος ήταν αρχειοθετημένες μόνο το 2000. Από τα 10.000 που αρχειοθετήθηκαν, 4.000 ήταν αρκετά σοβαρά να αναφερθούν στις αντιπροσωπείες επιβολής νόμου, και 273 από τις συμβιβασμένες οργανώσεις υπέβαλαν αριθμούς οικονομικής απώλειας που

---

[101] Γ.Λάζος., Πληροφορική και Έγκλημα, Νομική Βιβλιοθήκη, 2001.σ. 115.
[102] Bankers, 2002 website, on the web at:
http://www.BankersOnline.com

συμπληρώνουν συνολικά $265.589.940. Η συνολική απώλεια της κατά προσέγγιση ίδιας έρευνας για τα τρία προηγούμενα έτη συμπλήρωσε συνολικά $120.240.180. Προφανώς το έγκλημα υπολογιστών βρίσκεται σε άνοδο. Θυμηθείτε ότι αυτές είναι ακριβώς οι αναφερόμενες επιθέσεις! Οι περισσότερες επιθέσεις όχι μόνον καταλήγουν να μην καταγγέλλονται, αλλά και συχνά δεν ανιχνεύονται. Αν λάβουμε υπ' όψιν ότι η φυσική παρουσία του δράστη στο χώρο που σκοπεύει να παραβιάσει ή η άμεση επαφή του με τον υπολογιστή – στόχο είναι αυξανόμενα περιττή[103] οδηγούμαστε στο συμπέρασμα ότι οι κυβερνό-εγκληματίες έχουν ελεύθερο πεδίο μέσα στις καθορισμένες εφαρμογές δικτύων και επιχειρήσεων.

Οι περισσότερες οργανώσεις έχουν άριστες πολιτικές και διαδικασίες σχετικά με τη χρήση υπολογιστών. Έχουν επίσης μια αντιπυρική ζώνη για να προστατεύσουν τα προτερήματά τους από τις εισβολές Διαδικτύου και για να καταγράψουν τις παραβιάσεις. Έχουν έναν ανώτερο υπάλληλο ασφάλειας ή έναν διευθυντή αντιπυρικών ζωνών που είναι αρμόδιοι για την επιβολή της ασφάλειας. Το ζήτημα, όπως το βλέπουμε, είναι ότι δεν ξέρουν πώς να καθορίσουν πότε μια επίθεση πρέπει να ερευνηθεί ή να εμποδιστεί απλά. Στις περισσότερες περιπτώσεις, οι σοβαρές επιθέσεις εμποδίζονται χωρίς έρευνα. Οι δράστες μπορούν έπειτα να ηρεμήσουν έως ότου χαλαρώσουν οι έλεγχοι και κατόπιν δοκιμάζουν πάλι. Είναι επίσης ελεύθεροι να επιτεθούν σε άλλα δίκτυα, δεδομένου ότι οι ενέργειές τους δεν έχουν αναφερθεί στις αρχές.

Από τις 11 Σεπτεμβρίου, πιστεύουμε ότι πρέπει να αυξήσουμε την επαγρύπνηση για να προστατεύσουμε τα εταιρικά προτερήματα και την εθνική υποδομή. Αυτό σημαίνει ότι τα σοβαρά γεγονότα θα πρέπει να ερευνηθούν, τα στοιχεία θα πρέπει να συγκεντρωθούν και οι αρχές θα πρέπει να ειδοποιηθούν εάν ένα έγκλημα έχει διαπραχτεί. Πολλοί ανώτεροι υπάλληλοι ασφάλειας και διοικητές αντιπυρικών ζωνών δεν έχουν τις δικανικές δεξιότητες που απαιτούνται για να καθορίσουν εάν ένα γεγονός αξίζει την έρευνα ούτε γνωρίζουν πως να διεξάγουν την απαραίτητη έρευνα. Είναι τώρα η ώρα να αποκτηθούν αυτές οι νέες δεξιότητες και να εφαρμοστούν οι νέες τεχνικές.

Το πρώτο βήμα σε αυτήν την διαδικασία είναι να μάθει κανείς πώς να χωρίσει τις αβλαβείς ανιχνεύσεις που εμφανίζονται εκατοντάδες φορές ημερησίως από τις καθορισμένες επιθέσεις. Όχι μόνο τα κίνητρα αντιπυρικών ζωνών πρέπει να αναθεωρηθούν προσεκτικά, αλλά και τα εσωτερικά συστήματα πρέπει να είναι στο επίκεντρο μιας επιτυχούς παραβίασης αντιπυρικών ζωνών ή διαποδιαμορφωτών. Εάν τα σημάδια είναι παρόντα, κατόπιν μια πλήρης δικανική έρευνα αξίζει. (Η δικανική έρευνα υπολογιστών Α είναι η ανάλυση των ηλεκτρονικών συσκευών όπως οι υπολογιστές, τα τηλέφωνα, PDA, οι δίσκοι, οι διακόπτες, οι δρομολογητές, οι πλήμνες και ο υπόλοιπος ηλεκτρονικός εξοπλισμός).

Για τις πιστωτικές κάρτες και τις απάτες του ATM, οι συστάσεις δεν μπορούν ποτέ να είναι αρκετές. Ιδιαίτερα, αναθεωρήστε τις δηλώσεις λογαριασμού σας προσεκτικά και δηλώστε στην τράπεζά σας αμέσως για οποιεσδήποτε αποκλίσεις. "Εξετάζει εκείνη την δήλωση το λεπτό που έρχεται," λέει η Linda Sherry, εκδοτικός διευθυντής της καταναλωτικής δράσης στο Σαν Φραντσίσκο. Ο Jim Smith του Μιλγουόκι το έμαθε άσχημα. Απέτυχε να παρατηρήσει τρεις αναλήψεις $19.95 από τον λογαριασμό ελέγχου του μέσω του αριθμού χρεωστικών καρτών του το 1998. Τις ανακάλυψε τελικά όταν έγινε πέρυσι μια τέταρτη ανάληψη, προκαλώντας έναν έλεγχο. Ενώ η τράπεζά του τον αποζημίωσε για την πρόσφατη απόσυρση, αρνήθηκε να τον αποζημιώσει για τις προηγούμενες, λέγοντας ότι περίμενε πάρα πολύ να το δηλώσει στην τράπεζα. "Δίνω μεγάλη προσοχή στις δηλώσεις μου τώρα," λέει η Smith. "Πηγαίνω κάθε εβδομάδα και κάνω έναν έλεγχο στον λογαριασμό μου στο ATM για να σιγουρευτώ ότι όλα είναι εντάξει." (Αφότου κάλεσαν οι US ειδήσεις την

---

[103] Γ.Λάζος., Πληροφορική και Έγκλημα, Νομική Βιβλιοθήκη, 2001.σ. 48.

τράπεζα Smith στην υποβολή εκθέσεων αυτής της ιστορίας, συμφώνησαν να τον αποζημιώσουν για τις προηγούμενες αποσύρσεις.)

Αν και η βιομηχανία πιστωτικών καρτών συμπονάει τα θύματα, λέει ότι ελέγχει την απάτη. Η παραβίαση έχει αυξηθεί τα τελευταία χρόνια, "η αύξηση δεν είναι αυτό που θεωρούμε εκρηκτική," λέει ο John Shaughnessy, ανώτερος αντιπρόεδρος της διαχείρισης κινδύνου για συστήματα των αμερικάνικων νευρικών δικτύων θεωρήσεων, τα οποία μπορούν να πάρουν τα ύποπτα σχέδια χρήσης κατόχων κάρτας, και άλλα μέτρα υψηλής τεχνολογίας βοηθούν την μάχη για την απάτη έκδοσης. Ακόμα, κανένα σύστημα ανίχνευσης δεν είναι αδιάβλητο, και η βιομηχανία έχει διάφορες νέες αποτυπώσεις στον πίνακα σχεδίων. Η Visa και η MasterCard έχουν εισαγάγει έναν άλλο κώδικα επικύρωσης, που τυπώνεται στο πίσω μέρος της κάρτας, την οποία οι έμποροι που δέχονται συναλλαγές με 'την κάρτα μη παρούσα' μπορούν να ζητήσουν τους κατόχους κάρτας. 'Άλλες λύσεις περιλαμβάνουν την τεχνολογία που θα διαβάσει τις ιδιότητες της μαγνητικής λωρίδας.

Οι ενώσεις συνεργάζονται επίσης με τους εμπόρους για να βοηθήσουν να ανιχνεύσουν την απάτη στις συναλλαγές τηλεφώνων και Διαδικτύου. Τελικά, είναι ο λιανοπωλητής που μένει κολλημένος με την πλαστή συναλλαγή. "Χαρακτηριστικά, ο έμπορος καταλήγει να το τρώει " λέει ο Robert McKinley, Πρόεδρος CardWeb, ένα Gettysburg, PA, εταιρία που ερευνά πιστωτικές κάρτες. Εν τω μεταξύ, η βιομηχανία προωθεί τη διαδεδομένη έγκριση ενός ασφαλούς ηλεκτρονικού πρωτοκόλλου συναλλαγής που θα δημιουργούσε μια ψηφιακή ταυτότητα για τους κατόχους κάρτας και τους εμπόρους. Οι εκδότες ζυγίζουν μέσα, επίσης. Οι κάτοχοι κάρτας Citibank, παραδείγματος χάριν, μπορούν να υπογράψουν επάνω για "ClickCredit," μια χωριστή γραμμή αριθμού πίστωσης και λογαριασμού που χρησιμοποιείται αποκλειστικά για αγορές on-line. Άλλες εταιρίες δημιουργούν ασφαλείς μεθόδους πληρωμής, όπως τα εικονικά "πορτοφόλια" για τις αγορές Ιστού.

Στο μέλλον, πολλοί ανησυχούν ότι περισσότεροι απατεώνες καρτών θα πάνε ένα βήμα περαιτέρω. Η κλοπή ταυτότητας είναι ένα τεράστιο πρόβλημα και ένας έξυπνος καλλιτέχνης con μπορεί να χρησιμοποιήσει τις πληροφορίες λογαριασμού, για να δημιουργήσει μια παρόμοια ταυτότητα. Τα θύματα της απάτης μαθαίνουν γρήγορα τις ανταλλαγές της τεχνολογίας 'πυροτέχνημα'. "Η εχεμύθεια είναι ένα σπάνιο είδος αυτές τις μέρες και γίνεται σπανιότερη κάθε φορά που προσκαλούμε κάποιον, για να έχουμε πρόσβαση στις προσωπικές πληροφορίες μας χάριν της ευκολίας," λέει η Foote. Είναι ένα μάθημα που όλοι οι κάτοχοι κάρτας πρέπει να προσέξουν[104].

[104] Margaret Mannix, High-tech card fraud goes on right behind your back, 2002, on the web at: http://www.usnews.com/usnews/nycu/money/articles/000214/nycu/credit.htm

Βιβλιογραφία – Αναφορές

Alexander, M. (1995), '*The Underground Guide to Computer Security*', Addison - Wesley Longman Inc., New York.

Anderson, K. (1997), *'Criminal Threats to Business on the Internet'*.

Australian Bureau of Statistics 2000, '*Use of the Internet by Householders*', *Australia*, (Cat. No. 8147.0), Australian Bureau of Statistics, Canberra.

Australian Competition and Consumer Commission
http://www.accc.gov.au

APACS, '*Card Watch Definitions*', web article, April 2002 at:
http://www.cardwatch.org.uk/html/definitions.html

Bankers' Hotline, Vol. 9, No. 12, 1/00

Bankers website, on the web at:
http://www.BankersOnline.com

Busch, M. (1997), '*Worried About Credit Card Fraud*? Web article, at:
http:// www.av.com/fraud

Bonney R. (1992), '*Preventing Credit Card Fraud*' , New South Wales Bureau of Crime Statistics and Research.

BBC Business News, '*Credit Card Fraud Rise*', web article, 20 February, 2001 at:
http://news.bbc.co.uk/hi/english/business/newsid_1179000/1179590.stm

Bloombecker, J.J.(1990)., ' *Computer Crime and Abuse* ', The EDD Auditor Journal, 1990.ii.

Card Facts (2002): '*Card fraud; the facts*', *web article*, April 2002, web at:
http://www.cardwatch.org.uk/html/card_fraud_facts.html

Call for Papers (2001): '*Research into Economic Crime*', 2001.

Crime and Justice Bulletin No. 17 , NSW, '*Bureau of Crime Statistics and Research*', Sydney.
Clausing, J. (1999), *'FTC Holds Meeting on International E-Commerce'*, New York Times, June 8.

Cohen A.K.(1997), 'The Concept of Criminal Organization', The British Journal of Criminology, 2/1997,n 17

Cook, V. (1999), 'Trust Me, I'm a Computer', *Communications Newsletter*, September 1999.

Copyright Law Review Committee (1996), *'Copyright Reform: A Consideration of Rationales, Interests and Objectives'*, AGPS, Canberra.

Copyright Act. (1976), Section 106A of the 1976 Copyright Act.

Copyright Act . (1976), Sections 107 through 121 of the 1976 Copyright Act.

Copyright Law. (2001): Fact sheet No. P-01 Issue: April 2000 Amended July 2001..

Commission On Crime Prevention and Criminal Justice , Seventh session (1998).

CSU-SUNNY-CUNNYJOINT COMMITTEE, '*Fair Use of Copyrighted Works*', 1995, http:// www.fairindex.html.

Daniel C. Lynch & Leslie Lundquist (1996), '*Digital Money: the new area of Internet commerce*', at 99.

David Cline, Term Paper, '*Cryptographic Protocols for Digital Cash*', George Washington University, School of Engineering and Applied Science (Computer Security I). Available online at URL: http://www.seas.gwu.edu/student/clinedav/.

Denning, D. E. (1999), '*Information Warfare and Security*', ACM Press, Reading, Massachusetts.

Department of Communications, Information Technology and the Arts 2000a, '*Shopping on the Internet: Facts for Consumers*', http://www.dcita.gov.au/shoponline (visited 21 July 2000).

Division's Computer Crime and Intellectual Property Section , http://www.cybercrime.gov/append.htm (visited 5 July 2000).

Duncan, M. D. G. (1995), '*The Future Threat of Credit Card Crime*', RCMP Gazette, vol. 57, no. 10.

EBT(1995): Electronic Benefits Transfer, '*Use of Biometrics to Deter Fraud in the Nationwide EBT Program*'.

EU Directive (1998) to be extended, ' Money laundering' web article, 13 July 1998 at: http://europa.eu.int/comm/internal_market/en/finances/general/launden.htm

Επιτροπής της Κοινότητας .(1984), '*Οδηγία υπ' αριθμ. 84-4.50*' ,10 της Σεπτεμβρίου 1984.

Φαρσεδάκης, Ι. (1996), ' *Στοιχεία Εγκληματολογίας*', Νομική Βιβλιοθήκη 1996

Financial Crimes: '*How They Effect Europe*', a web article at: http://web.ukonline.co.uk/p.mordecai/europe_financial.htm

Federal Trade Commission v Audiotex Connection Inc E.D.N.Y. Filed 13 February 1997.

Ferenc Irk and Géza Finszter. (2000*), 'Organized Crime in East-Central Europe, on the Verge of the European Union'.*

Fox, B. (1995), '*Speedy Net Threatens Movie Moguls*', New Scientist, 16 December.

Froomkinm, Saul M. (2001), '*Organized Economic Crime: The Risk To World Economic Stability*'.

Gamble Richard H. (2001), '*Short Circuiting Wire Transfer Fraud*'.

Grau, J. J. (ed.), (1992),' *Criminal and Civil Investigation Handbook*', 2nd ed., McGraw-Hill Inc., New York.

Gordon Smith. (2002), '*Securing the Internet for 2002*',President, Canaudit Inc. on the web at: http://www.canaudit.com/Articles_Pubs/past_articles/sept01_perspective.htm

Goldring, J, L.Maher, J.McKeogh and G.Pearson.(1998), ' Consumer Protection Law' (Federation Press, 1998 5th ed)

Grabosky P.W. & R .G.Smith. (1998), '*Crime in the Digital Age*', Annesdale : Transaction, 1998.

Halber, D. (1994), '*Computer Technology and Legal Discource*' , at: ftp/pub/subj/law/jnl/elaw/comment/halbert.txt.

Helsinki (1998), '*Proceedings of the VI European Colloquium on Crime and Criminal Policy*', December 1998.

Holland, K. (1995), '*Bank Fraud, The Old-Fashioned Way*', *Business Week*, 4 September.

Information Infrastructure Task Force (1995), '*The Report of the Working Group on Intellectual Property Rights, Intellectual Property on the National Information Infrastructure*', 193 (Sept. 1995) at: gopher://ntian1.ntia.doc.gov:70/00/papers/documents/files/ipnii.txt

Internet Fraud Complaint Center (2001b), '*Internet Auction Fraud*', May. At, http://www1.ifccfbi.gov/strategy/AuctionFraudReport.pdf (visited 17 October2002).

Johnson, E. (1996), '*Body of Evidence: How Biometric Technology Could Help in the Fight against Crime*', *Crime Prevention News*, December.

Κουράκης, Ν.(1999), '*Το Οργανωμένο Έγκλημα: Φαινομενολογία του Προβλήματος και Δυνατότητες Αντιμετώπισης του στην Ελλάδα*'. Ποιν.Δικ, 10/1999.

Κουράκης, Ν.(1998), '*Τα οικονομικά εγκλήματα*', Εκδόσεις Σακκούλα.

Λάζος, Γρ.(1997), '*Μορφές Εγκληματικότητας Ι: Πληροφορική κ΄ Έγκλημα*', Αθήνα: Πάντειο, 1997.

Λαμπροπούλου, Ε.(2000), '*Οργανωμένη Εγκληματικότητα κ΄ Εσωτερική (αν-) Ασφάλεια*', Ποιν.Δικ.,8-9/2000.

Λαμπροπούλου, Ε.(1999), '*Κοινωνιολογία του Ποινικού Δικαίου και Θεσμών της Ποινικής Δικαιοσύνης*', Αθήνα Ελληνικά Γράμματα, 1999.

Louis Harris & Associates Inc. (1999), '*Consumers and the 21st Century: A Survey Conducted for the National Consumers League*', Louis Harris & Associates Inc, New York.

Μανωλεδάκη, Ι .(1992), '*Η τυποποίηση οικονομικών εγκλημάτων σε ειδικούς ποινικούς νόμους και η συρροή τους με αντίστοιχα εγκλήματα,τυποποιημένα στον ποινικό κώδικα*'. (Πανηγυρικός Τόμος Α για τα εικοσάχρονα του Ελληνικού Τμήματος της Διεθνούς Εταιρίας Κοινωνικής Αμύνης, Θεσσαλονίκη,1992.

Margaret Mannix. (2002), '*High-Tech Card Fraud Goes on Right Behind your Back*', 2002, on the web at: http://www.usnews.com/usnews/nycu/money/articles/000214/nycu/credit.htm

Meijboom, A.P. (1988), '*Problems Related to the Use of EFT and TeleShopping Systems by the Consumer*', *in Telebanking, Teleshopping and the Law*, eds. Y.Poullet & G.P.V. Vandenberghe, Kluwer, Deventer.

NES Database, 2002 on the web at:
http://www.oldburetto.com/pirates

Nigel Morris-Cotterill. (1999), '*How Not to Be a Money Launderer*', 2nd edition (Brentwood: Silkscreen Publications.

O'Brien, Chris (2000), '*The Next Revolution*?' The Age (Melbourne), I.T. (2), 27 June 2000.
Office of Government Information Technology 1998

Paper 1: '*Organized Crime in Estonia*'. Paper presented to the Pre-Congress on Organized Crimes in the Baltic Sea Area, June 6-8 1997, Saltsjöbaden, Sweden.

Paper 2: ' *Situation in Estonia Regarding Organized Crime*'. Paper presented to the Pre-Congress on Organized Crimes in the Baltic Sea Area, June 6-8 1997.

Rothchild, (1999), "*Protecting the Digital Consumer: The Limits of Cyberspace Utopianism*" (1999) 74 Indiana Law Journal.

Russell G. Smith. (2000), *'Confronting Fraud in the Digital Age'*, Australian Institute of Criminology, August 2000.

Russell G. Smith. (1997), *'Trends & Issues in Crime and Criminal Justice'*, No. 65 Internet Piracy, 1997.

Smith, R. G. (1997), *'Plastic Card Fraud'*, in Trends and Issues in Crime and Criminal Justice, No.71, Australian Institute of Criminology, Canberra.

Spinks, P. (1996), *'Tests Show Up Smart Card Flaws', The Age (Melbourne)*, 6 December.

St. Lucia.(2002), *'Fraud Detection'*, on the web at:
http://www.stlucia.gov.lc/pr2002/new_legislation_to_address_electronic_fraud.htm

Sullivan, C. 1987, *'Unauthorised Automatic Teller Machine Transactions: Consequences for Customers of Financial Institutions'*, Australian Business Law Review, vol. 15, no. 3.

Tech Glossary at Lycos website
at webopedia.lycos.com

The National Fraud Information Center.(2001), *'ATM Safety & Security Tips'*, web article, 2001 at: http://www.lapdonline.org/bldg_safer_comms/prevention/personal_safety/ATM.htm

The Lectric Law Library's Lexicon on *'Money Laundering'*. Web dictionary, April 2002 at:
http://www.lectlaw.com/def2/m038.htm

Titdemann,.K. (1996), ' Η Εγκληματικότητα στον Χώρο των Ηλεκτρονικών Υπολογιστών και η Γερμανική Μεταρρύθμιση του Ποινικού Δικαίου,1996.(Μετάφραση Μπιτζελέκη. Δημοσιεύματα του Ελληνικού Τμήματος της Διεθνούς Εταιρείας Κοινωνικής Αμύνης, Τευχ.-4/1999

United States, Department of Justice 2000, *'Internet Fraud: Appendix B'*, Report of the Criminal Division's Computer Crime and Intellectual Property Section,
http://www.cybercrime.gov/append.htm (visited 5 July 2000).

Van Leeuwen, H. (1996), *'A Surge in Credit Card Fraud'*, Financial Review, 24 September.

Van-Rhoda, T.(1991), "Credit card fraud", Journal of the Australasian Society of Victimology, Special Edition, April 1991.

Visa International (1997), *'SET Draft Reference Implementation'*,
http://www.visa.com/ (visited 2 May 2000).

Wasic M.(1991) , *'Crime and the Computer'*, Oxford: Claredin Press.

Webb, B. 1996, "*Preventing Plastic Card Fraud in the UK*", Security Journal. vol. 7.

Wireless lan. (2002): *'The Hacker's Best Friend'*, Chad Parks, Canaudit Inc. November 2002.

Ζησιάση,Β.(2001), *'Οικονομική Εγκληματικότητα: Το Ουσιαστικό και Δικονομικό Οικονομικό Ποινικό Δίκαιο'*, Εκδ.Σακκούλα, Αθήνα 2001.