ΑΣΦΑΛΕΙΑ ΣΤΟ ΔΙΑΔΙΚΤΥΟ – ΜΕΘΟΔΟΙ ΠΡΟΣΤΑΣΙΑΣ

Η εργασία υποβάλλεται για τη μερική κάλυψη των απαιτήσεων με στόχο την απόκτηση του διπλώματος

ΜΕΤΑΠΤΥΧΙΑΚΟ ΔΙΠΛΩΜΑ ΕΙΔΙΚΕΥΣΗΣ:

ΕΦΟΔΙΑΣΜΟΣ & ΔΙΑΚΙΝΗΣΗ ΠΡΟΙΟΝΤΩΝ (LOGISTICS)

από

ΤΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ ΚΑΙ ΤΟ ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ

ΚΥΖΙΡΟΓΛΟΥ ΠΑΝΑΓΙΩΤΑ

ΕΠΙΒΛΕΠΩΝ:ΕΠΙΚΟΥΡΟΣ ΚΑΘΗΓΗΤΗΣ ΓΡ. ΧΟΝΔΡΟΚΟΥΚΗΣ

ΤΜΗΜΑΤΟΣ ΒΙΟΜΗΧΑΝΙΚΗΣ ΔΙΟΙΚΗΣΗΣ ΚΑΙ ΤΕΧΝΟΛΟΓΙΑΣ

ΠΑΝΕΠΙΣΤΗΜΙΟΥ ΠΕΙΡΑΙΩΣ 2003

ΠΡΟΛΟΓΟΣ

Το θέμα της εργασίας αυτής είναι η «ΑΣΦΑΛΕΙΑ ΣΤΟ ΔΙΑΔΙΚΤΥΟ – ΜΕΘΟΔΟΙ ΠΡΟΣΤΑΣΙΑΣ» και χωρίζεται σε τέσσερα κεφαλαία. Στο πρώτο κεφάλαιο ορίζονται οι έννοιες του “Διαδικτύου” και του “Ηλεκτρονικού Εμπορίου”, παρουσιάζονται οι τεχνολογίες του Ηλεκτρονικού Εμπορίου, τα οφέλη του στους προμηθευτές και στους αγοραστές, καθώς τα τεχνικά και μη τεχνικά εμπόδια ανάπτυξης του. Στο δεύτερο κεφάλαιο αναλύονται οι κίνδυνοι για την ασφάλεια του δικτύου και κυρίως για το διακομιστή δικτύου.

Στη συνέχεια στο τρίτο κεφάλαιο παρουσιάζονται μέθοδοι επίλυσης και μηχανισμοί ασφαλείας. Επιπλέον περιγράφονται τα διάφορα συστήματα ηλεκτρονικών πληρωμών π.χ πιστωτικές κάρτες, ηλεκτρονικό χρήμα κ.λ.π., καθώς και τα ψηφιακά πιστοποιητικά και οι υπηρεσίες πιστοποιητικών (π.χ CA, ETO, RA) Ιδιαίτερο ενδιαφέρον έχει το τέταρτο κεφάλαιο, το οποίο αναφέρεται στις κοινοτικές ρυθμίσεις για τη προστασία του καταναλωτή σε σχέση με το Ηλεκτρονικό Εμπόριο.

Στο παράρτημα δίνονται κάποιες συμβουλές σε σχέση με τις πλαστές αγορές στο Διαδίκτυο ή για το τρόπο αξιολόγησης μιας εταιρείας ή προσφοράς αν είναι νόμιμη ή αυθεντική. Τέλος υπάρχει ανάλυση μιας έρευνας βασισμένη σε ένα ερωτηματολόγιο που στάλθηκε σε υπευθύνους τμημάτων μηχανογράφησης. Τα διαγράμματα που ακολουθούν δίνουν την εικόνα που επικρατεί στον κόσμο / εταιρείες για την ασφάλεια του Διαδίκτυου.

Η βιβλιογραφία που παρατίθεται στο τέλος της εργασίας οδηγεί σε μερικές από τις πηγές που μπορεί κανείς να εμβαθύνει στα αντίστοιχα αντικείμενα.

ΠΕΡΙΕΧΟΜΕΝΑ

ΧΡΗΣΙΜΕΣ ΣΥΝΤΟΜΟΓΡΑΦΙΕΣ

- B2B = ΕΠΙΧΕΙΡΗΣΗ ΠΡΟΣ ΕΠΙΧΕΙΡΗΣΗ (BUSINESS TO BUSINESS)
- B2C = ΕΠΙΧΕΙΡΗΣΗ ΠΡΟΣ ΚΑΤΑΝΑΛΩΤΗ (BUSINESS TO CONSUMER)
- B2E = ΕΠΙΧΕΙΡΗΣΗ ΠΡΟΣ ΥΠΑΛΛΗΛΟΥΣ (BUSINESS TO EMPLOYEE)
- BBB = BETTER BUSINESS BUREAU
- C2C = ΚΑΤΑΝΑΛΩΤΗΣ ΠΡΟΣ ΚΑΤΑΝΑΛΩΤΗ (CONSUMER TO CONSUMER)
- CA = ΑΡΧΗ ΠΙΣΤΟΠΟΙΗΣΗΣ (CERTIFICATION AUTHORITY)
- DZM =ΑΠΟΣΤΡΑΤΙΚΟΠΟΙΗΜΕΝΗ ΖΩΝΗ (DEMILITARIZED ZONE)
- EDI = ΗΛΕΚΤΡΟΝΙΚΗ ΑΝΤΑΛΛΑΓΗ ΔΕΔΟΜΕΝΩΝ (ELECTRONIC DATA INTERCHANGE)
- ΕΤΟ = ΕΜΠΙΣΤΗ ΤΡΙΤΗ ΟΝΤΟΤΗΤΑ
- EMAIL = ΗΛΕΚΤΡΟΝΙΚΟ ΤΑΧΥΔΡΟΜΕΙΟ
- IP = ΠΡΩΤΟΚΟΛΛΟ ΔΙΑΔΙΚΤΥΩΣΗΣ (INTERNET PROTOCOL)
- ISP = ΠΑΡΟΧΕΑΣ ΥΠΗΡΕΣΙΩΝ ΔΙΑΔΙΚΤΥΟΥ (ISP)
- NAT = ΠΑΡΑΦΡΑΣΗ ΤΗΣ ΔΙΕΥΘΥΝΣΗΣ ΤΟΥ ΔΙΚΤΥΟΥ (NETWORK ADDRESS TRANSLATION)
- PKI = ΚΡΥΠΤΟΓΡΑΦΗΣΗ ΔΗΜΟΣΙΟΥ ΚΛΕΙΔΙΟΥ (PUBLIC KEY CRYPTOGRAPHY)
- RA = ΑΡΧΕΣ ΕΚΔΟΣΗΣ ΕΓΓΡΑΦΩΝ (REGISTRATION AUTHORITY)
- SSL = ΑΣΦΑΛΕΣ ΕΠΙΠΕΔΟ ΑΠΟΔΟΧΗΣ (SECURE SOCKETS LAYER)
- TCP = ΠΡΩΤΟΚΟΛΛΟ ΕΛΕΓΧΟΥ ΕΠΙΚΟΙΝΩΝΙΑΣ (TRANSMISSION CONTROL PROTOCOL)
- VANS = ΔΙΚΤΥΑ ΠΡΟΣΤΙΘΕΜΕΝΗΣ ΑΞΙΑΣ (VALUE ADDED NETWORKS)
- VPN = ΕΙΚΟΝΙΚΟ ΙΔΙΩΤΙΚΟ ΔΙΚΤΥΟ (VIRTUAL PRIVATE NET WORK)
- WWW = ΔΙΚΤΥΑΚΟΣ ΙΣΤΟΣ (WORLD WIDE WEB)
- Η/Ε = ΗΛΕΚΤΡΟΝΙΚΟ ΕΜΠΟΡΙΟ
- Η/Υ = ΗΛΕΚΤΡΟΝΙΚΟΣ ΥΠΟΛΟΓΙΣΤΗΣ (PC)
- ΟΟΣΑ = ΟΡΓΑΝΙΣΜΟΣ ΟΙΚΟΝΟΜΙΚΗΣ ΣΥΝΕΡΓΑΣΙΑΣ & ΑΝΑΠΤΥΞΗΣ

Στη διεκπεραίωση της διπλωματικής μου εργασίας είχα δίπλα μου ανθρώπους για τους οποίους νιώθω την ανάγκη να τους ευχαριστήσω για τις συμβουλές τους, τις γνώμες τους και τη βοήθεια που μου πρόσφεραν.

Θερμές ευχαριστίες για την βοήθεια του και τις πολύτιμες υποδείξεις κατά την εγγραφή της εργασίας, στον επίκουρο καθηγητή μου Γρ. Χονδροκούκη.

Θα ήθελα να ευχαριστήσω συναδέλφους και φίλους για τις πολύτιμες συμβουλές και τα στοιχεία που μου έδωσαν.

Ένα μεγάλο ευχαριστώ σε όλους.

ΚΕΦΑΛΑΙΟ Α.

ΕΙΣΑΓΩΓΙΚΕΣ ΕΝΝΟΙΕΣ

Α.1 ΤΙ ΕΙΝΑΙ ΤΟ ΔΙΑΔΙΚΤΥΟ - INTERNET

Το Διαδίκτυο (Internet) είναι ένα πλέγμα από εκατομμύρια διασυνδεόμενους υπολογιστές, που εκτείνεται σχεδόν σε κάθε γωνιά του πλανήτη και παρέχει τις υπηρεσίες του σε εκατομμύρια χρήστες. Αποτελεί μια ‘‘**Παγκόσμια Ηλεκτρονική Κοινωνία**’’, της οποίας τα μέλη ανεξάρτητα από υπηκοότητα, ηλικία, θρήσκευμα και χρώμα, μοιράζονται πληροφορίες και ανταλλάσσουν ελεύθερα απόψεις πέρα από γεωγραφικά και κοινωνικά σύνορα. Προσφέρει εξαιρετικά πολύτιμες υπηρεσίες σε εκατομμύρια ανθρώπους και οργανισμούς σε όλο το κόσμο, αποτελεί μια διεθνή πηγή πληροφοριών και μέσο συνεργασίας μεταξύ αμέτρητων χρηστών διαφορετικών ομάδων, κοινοτήτων, εθνοτήτων και κρατών. **[13]**

Το σημερινό Διαδίκτυο (Internet) αποτελεί εξέλιξη του **ARPANET**, ενός δικτύου που άρχισε να αναπτύσσεται πειραματικά στα τέλη της δεκαετίας του ’60 στις ΗΠΑ. Το **ARPANET** γεννιέται το 1969 με πόρους του προγράμματος ARPA (*Advanced Research Project Agency*) του Υπουργείου Άμυνας. Στόχος ήταν η δημιουργία ενός Διαδικτύου που θα εξασφάλιζε την επικοινωνία μεταξύ απομακρυσμένων δικτύων, έστω και αν κάποια από τα ενδιάμεσα συστήματα βρίσκονταν προσωρινά εκτός λειτουργίας. Το 1973, ξεκινά ένα νέο ερευνητικό πρόγραμμα που ονομάζεται

Πρόγραμμα Διαδικτύωσης (*Internetting Project*) προκειμένου να ξεπεραστούν οι διαφορετικοί τρόποι που χρησιμοποιεί κάθε δίκτυο για να διακινεί τα δεδομένα του. Από την έρευνα γεννιέται μια νέα τεχνική, το Πρωτόκολλο Διαδικτύωσης **(Internet Protocol)** (**IP**), από την οποία θα πάρει αργότερα το όνομα του το Διαδίκτυο (Internet). Διαφορετικά δίκτυα που χρησιμοποιούν το κοινό πρωτόκολλο (IP) μπορούν να συνδέονται και να αποτελούν ένα Διαδίκτυο. Με τον όρο Διαδίκτυο (Internet) εννοούμε δηλαδή τη συνένωση των χιλιάδων δικτύων διαφόρων μεγεθών που καλύπτει σχεδόν ολόκληρη την υδρόγειο.

Είναι προφανές ότι το Διαδίκτυο δεν αποτελεί πλέον ένα δίκτυο των φοιτητών και των ερευνητών, αλλά ότι επεκτείνεται και επιδρά στις καθημερινές πρακτικές όλων των ανθρώπων. Ήδη ισχύει το ηλεκτρονικό εμπόριο, η τηλεεργασία, η τηλεκπαίδευση, η τηλεϊατρική, κλπ. μέσα από αυτό. Σύμφωνα με σχετικές εκτιμήσεις, αυτός ο παγκόσμιος ιστός υπολογιστών και χρηστών αριθμεί σήμερα πάνω από δέκα εκατομμύρια υπολογιστές και εκατό εκατομμύρια χρήστες, ενώ επεκτείνεται διαρκώς με εκθετικούς ρυθμούς. Στα τέλη του 1999 το Διαδίκτυο είχε περισσότερους από 450 εκατομμύρια χρήστες η πλειοψηφία των οποίων στις ανεπτυγμένες χώρες, ενώ το 2000 το Διαδίκτυο (Internet) εξυπηρέτησε περισσότερο από ένα δισεκατομμύριο χρήστες.

Τα βασικά του χαρακτηριστικά είναι:

- ότι μπορεί να συνδέει υπολογιστές διαφορετικού τύπου δηλαδή υπολογιστές που μπορεί να διαφέρουν όσον αφορά την αρχιτεκτονική του υλικού (hardware), το λειτουργικό σύστημα που χρησιμοποιούν και το πρωτόκολλο διαδικτύωσης που εφαρμόζεται στο τοπικό τους δίκτυο. Ακριβώς εξαιτίας

αυτής της ευελιξίας του, εξαπλώθηκε σε ολόκληρο το πλανήτη κατά τη διάρκεια των τελευταίων δεκαετιών.

- είναι αποκεντρωμένο και αυτοδιαχειριζόμενο. Καθένα από τα μικρότερα δίκτυα που το αποτελούν διατηρεί την αυτονομία του και είναι το ίδιο υπεύθυνο για το είδος των πληροφοριών που διακινεί, τις υπηρεσίες που προσφέρουν οι υπολογιστές και τη διαχείριση του.

Τα πλεονεκτήματα του είναι :

- Μικρό κόστος χρήσης, το οποίο όλο και μειώνεται
- Γραφικό περιβάλλον για χρήστες κάθε επιπέδου
- Ευρεία εξάπλωση, η οποία αυξάνεται με λογαριθμικούς ρυθμούς

Τα μειονεκτήματα του είναι:

- Μέτρια σταθερότητα στη ποιότητα. Άλλωστε δεν έχει σχεδιαστεί ποτέ για εμπορική χρήση, αλλά μόνο στρατιωτική
- Σχετικά μικρή ασφάλεια για τα συναλλασσόμενα μέρη. Γίνεται σοβαρή προσπάθεια να ξεπεραστεί το πρόβλημα, αλλά η πλήρης λύση είναι δύσκολη, ασύλληπτων διαστάσεων και έχει σημαντικές νομικές και πολιτικές παρενέργειες. **[1]**

Τα εργαλεία και οι εφαρμογές που απαρτίζουν το Διαδίκτυο είναι το ηλεκτρονικό ταχυδρομείο (e-mail), ο δικτυακός ιστός (world wide web), οι κοινότητες (communities) και τα chat - rooms (άλλος τύπος καφενείου).

Α.2 *ΤΙ ΕΙΝΑΙ E-COMMERCE*

Η έννοια του ηλεκτρονικού εμπορίου (e –commerce) δεν ταυτίζεται μεμονωμένα με αυτή του Διαδικτύου ή με την ανταλλαγή δεδομένων (EDI), το ηλεκτρονικό ταχυδρομείο κλπ. Όλα τα παραπάνω είναι επιμέρους τεχνολογίες ή δίκτυα τα οποία αποτελούν ένα μέρος των εργαλείων, συστημάτων, τεχνολογιών, τεχνικών, επιχειρηματικών μοντέλων και πρακτικών που συνθέτουν την έννοια ηλεκτρονικό εμπόριο. Σε καμία όμως περίπτωση δεν θα πρέπει το ηλεκτρονικό εμπόριο να αντιμετωπίζεται από τις επιχειρήσεις ως συλλογή τεχνολογιών αλλά ως παράγοντας επανασχεδιασμού των επιχειρησιακών διαδικασιών και ανάπτυξης νέων επιχειρηματικών μοντέλων.

Ηλεκτρονικό Εμπόριο είναι η ανταλλαγή επιχειρηματικής και εμπορικής πληροφορίας ή / και ψηφιακού προϊόντος ή υπηρεσίας σε ηλεκτρονική μορφή με χρήση τεχνολογίας πληροφορικής (υπολογιστές, λογισμικό) και τηλεπικοινωνιών (δίκτυα). Ο όρος <<ηλεκτρονικό εμπόριο>> ή e-commerce αποτελεί εννοιολογικά μέρος του e-business ή <<ηλεκτρονικού επιχειρήν>>. Το ηλεκτρονικό επιχειρήν περιγράφει επιχειρήσεις, η ύπαρξη και η στρατηγική των οποίων στηρίζεται στο Διαδίκτυο ή / και επιχειρήσεις που έχουν αναθεωρήσει – προσαρμόσει την αποστολή τους, τη στρατηγική τους και τις λειτουργίες τους με βάση τα δεδομένα του Διαδικτύου.

Για τη καλύτερη κατανόηση της έννοιας του ηλεκτρονικού εμπορίου ας δούμε τις πέντε βασικές κατηγορίες λειτουργιών που περιλαμβάνει:

- Ηλεκτρονική δημιουργία εμπορικής σχέσης / ηλεκτρονική διαπραγμάτευση, ηλεκτρονική παραγγελία

- Ηλεκτρονική παροχή / ανταλλαγή πληροφοριών σχετικά με το προϊόν.
- Ηλεκτρονική παράδοση προϊόντος
- Ηλεκτρονική πληρωμή
- Ηλεκτρονική ανταλλαγή εμπορικών εγγράφων

Οι εφαρμογές ηλεκτρονικού εμπορίου χωρίζονται σε δύο κατηγορίες αναλόγως την ιδιότητα του χρήστη. Και στις δυο περιπτώσεις από τη μια πλευρά βρίσκεται επιχείρηση ή οργανισμός. Στην άλλη πλευρά εάν πρόκειται για εφαρμογή ηλεκτρονικού εμπορίου μεταξύ εταιρειών για την οποία έχει επικρατήσει ο όρος B2B (Business to Business) βρίσκεται το σύστημα ή ο υπάλληλος εταιρείας. Εάν βρίσκεται τελικός καταναλωτής ή χρήστης πρόκειται για εφαρμογή εταιρείας με καταναλωτή γνωστή ως B2C (Business to consumer). Υπάρχει και η περίπτωση όπου και στις δύο πλευρές βρίσκεται ο καταναλωτής, γνωστή ως C2C (Consumer to Consumer). Σ' αυτή τη κατηγορία ο καταναλωτής πουλάει απευθείας στο καταναλωτή π.χ οι δημοπρασίες ή η διαφήμιση και η πώληση προσωπικών αντικειμένων. Οι συναλλαγές μεταξύ επιχειρήσεων και υπαλλήλων ονομάζεται B2E (business to employee). Αυτός ο τρόπος εσωτερικής επικοινωνίας μπορεί να περιλάβει ηλεκτρονικό ταχυδρομείο, λογισμικό συνεργασίας, τηλεσυνδιάσκεψη και εταιρικές πύλες. **[3]**

Τα μεγέθη αγοράς αναφορικά με το ηλεκτρονικό εμπόριο που δίνουν οι διάφοροι αναλυτές ποικίλλουν. Οι τελευταίες εκτιμήσεις της Forrester Research προβλέπουν πως τα έσοδα των ηλεκτρονικών συναλλαγών θα φτάσουν το 2004, το ποσό των $7 τρις για την παγκόσμια αγορά. Από το σύνολο των συναλλαγών ηλεκτρονικού εμπορίου εκτιμάται ότι το 89% θα πραγματοποιηθεί ως εξής:

- $3,5 τρις στην Αμερική.
- $1,5 τρις στην Ασία, εκ των οποίων $ 880 δις στην Ιαπωνία.
- $1,5 τρις στην Ευρώπη (ισοδυναμεί με 6% της συνολικής Ευρωπαϊκής Οικονομίας).
- $68 δις στην Αν. Ευρώπη, στην Αφρική και στη Μέση Ανατολή.

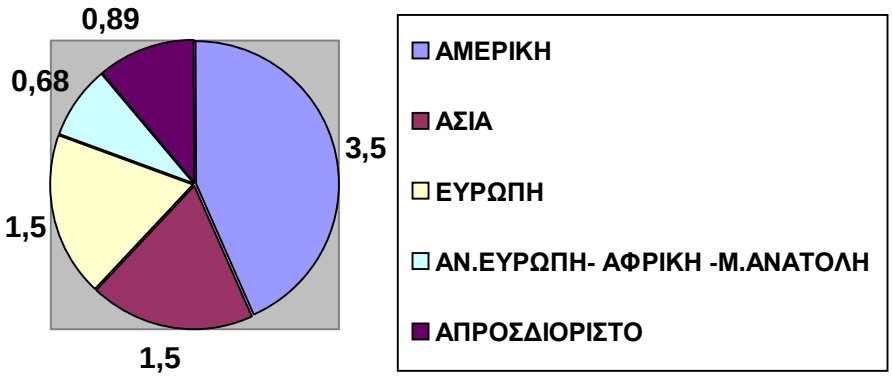
Σαν ποσοστό του συνολικού εμπορίου μεταξύ επιχειρήσεων, η αξία των συναλλαγών μέσω ηλεκτρονικού εμπορίου αναμένεται να εκτιναχθεί από 0,2% το έτος 1997 στο 2,1% το έτος 2000 και στο 9,4% το έτος 2003. **[12]**

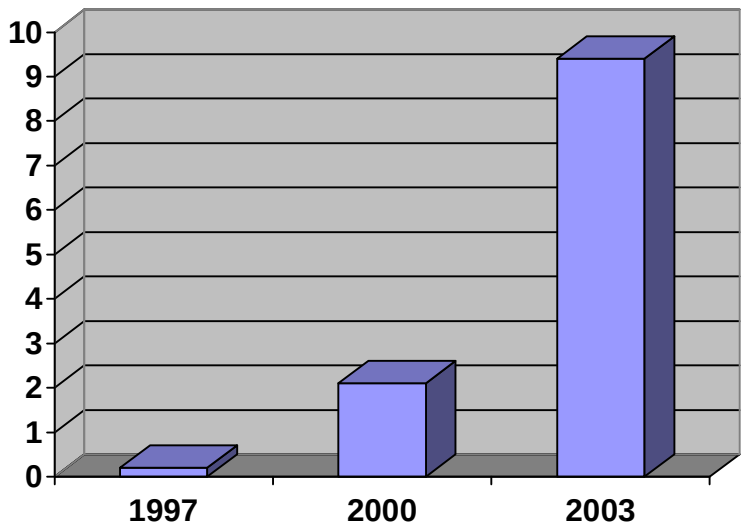
Σύμφωνα με στοιχεία της Ευρωπαϊκής Ένωσης που παρουσιάστηκαν πρόσφατα στο e-Commerce Forum στην Ελλάδα, η αγορά ηλεκτρονικού εμπορίου θα είναι ίση σε μέγεθος με την αγορά τηλεπικοινωνιών ή την αεροπορική αγορά. Αξίζει ακόμη να σημειωθεί πως τελευταίες μελέτες αναφέρουν ότι σε χώρες που το ηλεκτρονικό εμπόριο αναπτύσσεται γρήγορα, θα υπάρξει αύξηση 5% του ΑΕΠ μόνο από τη δραστηριότητα αυτή.

Έρευνα της IDC δείχνει πως το μέγεθος της Ελληνικής αγοράς ηλεκτρονικού εμπορίου θα διαμορφωθεί για το 2003 στο ποσό των $1,6 δις.

Από τη συνολική αξία των συναλλαγών ηλεκτρονικού εμπορίου, το 80% εκτιμάται ότι θα αφορά ηλεκτρονικό εμπόριο μεταξύ επιχειρήσεων και μόνο το 20% θα αφορά το λιανικό ηλεκτρονικό εμπόριο. Επισημαίνεται επίσης ότι σύμφωνα με σχετική οδηγία της Ευρωπαϊκής Ένωσης, μέχρι το 2005 το 25% των συναλλαγών των Δημοσίων Οργανισμών υποχρεωτικά θα πρέπει να διενεργείται με ηλεκτρονικό τρόπο, προκειμένου να διασφαλίζεται η διαφάνεια και η μείωση του κόστους. Το γεγονός επισφραγίζει τη ραγδαία ανάπτυξη του ηλεκτρονικού εμπορίου μεταξύ των επιχειρήσεων στο άμεσο μέλλον.

ΣΥΝΟΛΟ ΣΥΝΑΛ/ΓΩΝ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΜΠΟΡΙΟΥ





Α.3 ΤΕΧΝΟΛΟΓΙΕΣ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΜΠΟΡΙΟΥ

Οι τεχνολογίες που συνθέτουν την έννοια του Η/Ε δεν είναι όλες νέες. Οι περισσότερες απ' αυτές χρησιμοποιούνται εδώ και αρκετά χρόνια από σημαντικό αριθμό επιχειρήσεων διαφόρων κλάδων. Αυτό που τους έδωσε ώθηση και επέτρεψε την αντιμετώπιση τους ενιαία κάτω από την ομπρέλα του ηλεκτρονικού εμπορίου, ήταν η αποδοχή διεθνών προτύπων που έχουν να κάνουν με αυτές τις τεχνολογίες και κυρίως την εκρηκτική ανάπτυξη του Διαδικτύου. Τα δεδομένα αυτά δημιουργούν την ανάγκη για νέες μορφές οργάνωσης και διαχείρισης των λειτουργιών των επιχειρήσεων ώστε να μπορέσουν να αντεπεξέλθουν στις νέες συνθήκες.

a) Γραμμωτός κώδικας (Bar code)

Η τεχνολογία του γραμμωτού κώδικα είναι μια από τις τεχνολογίες αυτόματης αναγνώρισης. Είναι ένα χρήσιμο εργαλείο, το οποίο βοηθά καταλυτικά στην ομαλή και χωρίς λάθη διακίνηση και διαχείριση προϊόντων καθώς και υπηρεσιών σε όλη την εφοδιαστική αλυσίδα.

b) Ηλεκτρονική ανταλλαγή δεδομένων (EDI)

Η ηλεκτρονική ανταλλαγή δεδομένων είναι η ανταλλαγή εμπορικών ή και διοικητικών δεδομένων μεταξύ εμπορικών εταίρων απ' ευθείας από υπολογιστή σε υπολογιστή με ελάχιστη ή καμία παρέμβαση χειρόγραφων διαδικασιών.

c) Imaging

Πρόκειται για το συνδυασμό πολλών τεχνολογιών οι οποίες χρησιμοποιούνται για τη σάρωση, αποθήκευση, ανάκτηση και διαβίβαση δεδομένων ή εγγράφων. Τα συστήματα εικόνας δημιουργούν ένα ψηφιακό ηλεκτρονικό αντίγραφο του

εγγράφου. Η εικόνα στη συνέχεια αποθηκεύεται, συνήθως συμπιεσμένη ψηφιακή μορφή σε οπτικούς δίσκους ή και σε άλλα μέσα.

Η τεχνολογία των συστημάτων ηλεκτρονικής αρχειοθέτησης δεν έχει γνωρίσει ιδιαίτερη αποδοχή έως σήμερα κυρίως εξ αιτίας του υψηλού της κόστους.

d) Έξυπνες κάρτες (smart cards)

Οι έξυπνες κάρτες μπορούν να αποθηκεύσουν μεγάλες ποσότητες δεδομένων και παρέχουν δυνατότητες κρυπτογράφησης ή χειρισμού ηλεκτρονικών υπογραφών για την ασφάλεια των περιεχομένων τους. Σήμερα κυριαρχεί η λανθασμένη άποψη ότι οι έξυπνες κάρτες είναι μόνο τραπεζικές ή πιστωτικές με αποτέλεσμα να μη αναγνωρίζεται το μεγάλο εύρος των δυνατοτήτων τους. Οι γενικές λειτουργίες που μπορεί να προσφέρει ένα τέτοιο σύστημα είναι:

1. Προστασία δεδομένων
2. Αναγνώριση του κατόχου κάρτας
3. Ασφάλεια πρόσβασης σε συστήματα & χώρους
4. Πιστοποίηση υπογραφής
5. Κρυπτογράφηση. **[3]**

Α.4 ΟΦΕΛΗ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΜΠΟΡΙΟΥ

Τα προηγούμενα χρόνια πολλές δραστηριότητες της εφοδιαστικής αλυσίδας διεκπεραιώνονταν χειρόγραφα και με τη χρήση εντύπων (π.χ αιτήσεις αγοράς, εντολές αγοράς, τιμολόγια κλπ). Η υιοθέτηση του ηλεκτρονικού εμπορίου κατά μήκος της εφοδιαστικής αλυσίδας μπορεί να διαδραματίσει σημαντικό ρόλο και να προσφέρει ανταγωνιστικά οφέλη. Συγκεκριμένα οδηγεί σε αύξηση της αποτελεσματικότητας σε όλες τις επιμέρους δραστηριότητες που περιλαμβάνει η

αλυσίδα εφοδιασμού. Ειδικότερα, είναι δυνατόν να επιτευχθεί σμίκρυνση της προμηθευτικής αλυσίδας, άμεση επικοινωνία μεταξύ προμηθευτή και πελάτη, ευκολότερος εντοπισμός πηγών προμήθειας σε τοπικό και διεθνές επίπεδο, μεγαλύτερη διαφάνεια και ορθολογικότητα στις συναλλαγές, ελαχιστοποίηση του κόστους και παροχή άνεσης χρόνου και διενέργεια κινήσεων στρατηγικού χαρακτήρα.

Οφέλη που παρέχει το ηλεκτρονικό εμπόριο στις αγοράστριες επιχειρήσεις είναι :

- Μεγαλύτερη ποικιλία προϊόντων και προμηθευτών
- Άμεση επικοινωνία με το προμηθευτή
- Αυτοματοποίηση της διαδικασίας παραγγελιών και συναλλαγών
- Περιορισμός σφαλμάτων κατά τη σύνταξη των εγγράφων (π.χ τιμολογίων, εντολών αγοράς)
- Σμίκρυνση του χρόνου του αγοραστικού κύκλου. Οι καταναλωτές μέσω του ηλεκτρονικού εμπορίου μπορούν να επιλέξουν ανάμεσα σε πολλά προϊόντα και υπηρεσίες, όχι ακριβά, και κάνοντας γρήγορες συγκρίσεις να αγοράζουν. Σε ορισμένες περιπτώσεις, ειδικά στα ψηφιακά προϊόντα, το Η/Ε διευκολύνει τη γρήγορη παράδοση.
- Μείωση του κόστους αγοράς αγαθών και υπηρεσιών από

  α) Προσφορές των πωλητών β) μείωση χρονοβόρων διαδικασιών για τη παραγγελία γ) έρευνας αγοράς και σύγκριση τιμών και δ) ηλεκτρονική παρακολούθηση παραγγελίας.
- Άμεση γνώση των επιμέρους στοιχείων (τεχνικά χαρακτηριστικά, τιμές) της προσφοράς του προμηθευτή

- Βελτίωση των σχέσεων πωλητή – αγοραστή. Αυτό οδηγεί σε καλύτερη εξυπηρέτηση του τελικού πελάτη, σε αποτελεσματικότερο προγραμματισμό, σε εφαρμογή τεχνικών μείωσης του κόστους και σε δημιουργία ευκαιριών κοινής επιχειρηματικής συνεργασίας αγοραστή – προμηθευτή.
- Εξάλειψη γεωγραφικών εμποδίων εφόσον το Η/Ε δίνει τη δυνατότητα ο αγοραστής να ψωνίζει ή να συναλλάσσεται σχεδόν απ' οποιοδήποτε σημείο του κόσμου όλο το χρόνο 24 ώρες το 24ωρο.
- Μέσω του ηλεκτρονικού εμπορίου ο καταναλωτής συμμετέχει σε ζωντανές δημοπρασίες και σε «ηλεκτρονικές επικοινωνίες» για ανταλλαγή ιδεών και σύγκριση εμπειριών.

Οφέλη που παρέχει το ηλεκτρονικό εμπόριο στους πωλητές είναι :

- Επαρκής γνώση των συνθηκών της αγοράς εφόσον το Η/Ε διευρύνει το κύκλο της αγοράς της επιχείρησης σε εθνικό και διεθνές επίπεδο. Με ελάχιστο κεφάλαιο, μια επιχείρηση μπορεί να προσελκύσει εύκολα και γρήγορα περισσότερους πελάτες, καλύτερους προμηθευτές και κατάλληλους επιχειρηματικούς συνεταίρους σε όλο το κόσμο.
- Αύξηση του όγκου των πωλήσεων που οφείλεται είτε:

Α) από άνοιγμα αγορών

Β) από την αύξηση τους κατά 10% των πωλήσεων ως προς τους υπάρχοντες πελάτες που προτιμούν / επηρεάζονται από το νέο αυτό κανάλι

Γ) από δημοπρασίες προϊόντων και αποθέματα.

- Μειωμένο λειτουργικό κόστος και κόστος πώλησης. Π.χ επιχειρήσεις με ηλεκτρονικό σύστημα προμηθειών μειώνουν τα κόστη διαχείρισης

προμηθειών κατά 85%. «Παρατηρούμε το κόστος των συναλλαγών να μειώνεται 10 φορές όταν πραγματοποιούμαι μια διαδικασία στο Δίκτυο. Βλέπουμε ευκαιρίες να μειώσουμε το κόστος πωλήσεων, γενικό και διαχείρισης κατά 20,30,40% στην επιχείρηση μας και δεν είναι ούτε 5 χρόνια στην αγορά. Είναι κάτι που συντελείται βραχυπρόθεσμα.» Dennis Dammerman, Γενικός Διευθυντής της GE Capital Services και αντιπρόεδρος της General Electric.

- Άμεση επαφή με τους αγοραστές και καλύτερη επικοινωνία σε 24ωρη βάση 7 μέρες τη βδομάδα.
- Καλύτερη εξυπηρέτηση του πελάτη
- Το Η/Ε μειώνει τα κόστη τηλεπικοινωνίας – το Διαδίκτυο είναι φθηνότερο από το Vans.
- Μειωμένα μεταφορικά κόστη
- Βελτιωμένη διαφάνεια στην αγορά
- Μειωμένη γραφειοκρατία. **[1]**

Οφέλη που παρέχει στη κοινωνία είναι τα εξής:

- Το Η/Ε συμβάλει στη μείωση του κυκλοφοριακού στους δρόμους και της μόλυνσης του περιβάλλοντος εφόσον ενθαρρύνει περισσότερο κόσμο να δουλεύει και να ψωνίζει από το σπίτι.
- Μέσω του ηλεκτρονικού εμπορίου άνθρωποι από Τρίτες Χώρες έχουν την δυνατότητα και την ευχαρίστηση να απολαμβάνουν αγαθά και υπηρεσίες που δεν τους είναι διαθέσιμα με άλλο τρόπο.

- Το Η/Ε συμβάλει στη παράδοση δημόσιων υπηρεσιών όπως εκπαίδευση ή στη διανομή κυβερνητικών υπηρεσιών σε μειωμένο κόστος και υψηλή ποιότητα.

Ως εμπόδια στην αποτελεσματική εφαρμογή του ηλεκτρονικού εμπορίου αναφέρονται τα εξής:

Α) Τεχνικά εμπόδια

- Έλλειψη τεχνολογικών γνώσεων από εμπλεκόμενους
- Υψηλό αρχικό κόστος μεταβίβασης και προσαρμογής στη νέα Η/Α i) σε λογισμικό και σε εξοπλισμό ii) σε χρόνο εκπαίδευσης προσωπικού iii) σε χρόνο εγκατάστασης συστήματος iv) για τη διατήρηση παράλληλου σχήματος μέχρι το σύστημα παραγγελιοδοσίας / παραγγελιοληψίας να αποδώσει.
- Δύσκολη η εμπλοκή του λογισμικού του Διαδικτύου και του Η/Ε με τις ήδη υπάρχουσες εφαρμογές και βάσεις δεδομένων.
- Για να αποκομίσει μια εταιρεία το πλήρες όφελος από τη συναλλαγή της μέσω ενός δικτυακού τόπου π.χ B2B θα πρέπει να μπορεί να εκτελεί όλη τη διαδικασία συναλλαγής ηλεκτρονικά. Αυτό σημαίνει αυτόματη ενημέρωση του λογιστηρίου, της αποθήκης και του τμήματος marketing / πωλήσεων της εταιρείας όταν αυτή πραγματοποιεί συναλλαγές μέσω μιας B2B. Πόσες όμως εταιρείες έχουν τη μηχανογραφική δυνατότητα να το κάνουν αυτό σήμερα;
- Περιορισμένη ασφάλεια στη χρήση εμπιστευτικών δεδομένων της επιχείρησης, έλλειψη αξιοπιστίας και εγγυήσεων.

Β) Μη Τεχνικά Εμπόδια

- Κοστολογικά προβλήματα. Το κόστος ανάπτυξης του Η/Ε, ιδιαίτερα στο σπίτι είναι ψηλό και χρονοβόρο και η έλλειψη εμπειρίας μπορεί να οδηγήσει σε καθυστερήσεις.
- Αντίδραση εκ μέρους των προμηθευτών για δημοσιοποίηση τιμών.
- Ανεπάρκεια ηλεκτρονικών καταλόγων προμηθευτών
- Έλλειψη εμπιστοσύνης. Οι καταναλωτές δεν εμπιστεύονται εύκολα έναν απρόσωπο πωλητή, τις απρόσωπες συναλλαγές και το ηλεκτρονικό χρήμα, επομένως η στροφή από το φυσικό κόσμο στο κόσμο του Η/Ε είναι δύσκολη.
- Ανεπαρκή ηλεκτρονικά συστήματα πληρωμών
- Το Η/Ε μπορεί να συμβάλει στην εξάλειψη ανθρώπινων σχέσεων
- Η πρόσβαση στο Διαδίκτυο είναι ακόμα ακριβή και μη προσβάσιμη για μελλοντικούς πελάτες.
- Ιδιαιτερότητες που δεν υπάρχουν στο B2C. Είναι ίσως το πιο σημαντικό πρόβλημα και πρέπει να λυθεί απο τους αρχιτέκτονες του Διαδικτυακού B2B τόπου. Μερικές από τις ιδιαιτερότητες που δεν συναντά κανείς σε ιστοσελίδες B2C είναι:
    - Τιμές και εκπτώσεις τζίρου και τρόπου πληρωμής ανά πελάτη
    - Προϊόντα που απαιτούν τροποποίηση ανά πελάτη
    - Επιλεκτική πρόσβαση του κάθε πελάτη στο κατάλογο προϊόντων
    - Απαίτηση, από τον αγοραστή μιας αρχικής τιμής για να προχωρήσει στη παραγγελία.

- Έλλειψη αφής. Μερικοί θεωρούν σημαντικό παράγοντα της αγοράς την αφή, δηλαδή να νιώθουν πριν αγοράσουν π.χ ρούχα
- Πολλά νομικά ζητήματα είναι ακόμα άλυτα και οι νόμοι της κυβέρνησης δεν έχουν ξεκαθαρίσει κάποιες περιστάσεις.
- Ασφάλεια. Το ζήτημα της ασφάλειας των συναλλαγών συχνά αναφέρεται ως ένα από τα μεγαλύτερα εμπόδια ανάπτυξης του Ηλεκτρονικού Εμπορίου. Πολλά από τα θέματα που αναφέρονται ως θέματα ασφαλείας για το Διαδικτυακό Εμπόριο αντιστοιχούν σε ανάλογα προβλήματα που υπάρχουν στις on-line συναλλαγές στον πραγματικό, φυσικό κόσμο, όπως κάποια είδη επικοινωνίας να είναι μυστικά, πληρωμές με φυσικό χρήμα, απαιτήσεις για αυθεντικές ιδιόχειρες υπογραφές στα συμβόλαια, κλπ.

Αυτές οι απαιτήσεις μας και τα μέσα που χρησιμοποιούμε για να τις ικανοποιήσουμε έχουν αναπτυχθεί εδώ και χιλιάδες χρόνια, στη διάρκεια όλης της ιστορίας του εμπορίου. **[8]**

Στο Διαδίκτυο ουσιαστικά αντιμετωπίζονται αυτά ακριβώς τα ίδια προβλήματα αλλά σε άλλη μορφή κι έτσι υπάρχει η ανάγκη να τεθούν επί τάπητος και να επινοηθούν νέες λύσεις μέσα σε σχετικά περιορισμένο χρόνο. Η ασφάλεια των συστημάτων του ηλεκτρονικού εμπορίου αποτελεί ένα σοβαρό ζήτημα των επιχειρήσεων περισσότερο και όχι τόσο της τεχνολογίας. Τεχνολογίες όπως ένα “Public Key Encryption” παρέχουν κρίσιμα στοιχεία μίας γενικής, ολοκληρωμένης λύσης, όμως δεν είναι αρκετά. Πολλοί έχουν ακούσει διάφορα περιστατικά και αναφορές σχετικά με την ασφάλεια του ηλεκτρονικού εμπορίου στο Διαδίκτυο και η πρώτη αντίδραση είναι «ΠΡΟΣΟΧΗ». Άλλοι αναρωτιούνται γιατί όλη αυτή η ανησυχία και ο προβληματισμός αφού ούτε στις συμβατικές συναλλαγές δεν

απασχολεί σε τέτοιο βαθμό. Σε τι διαφέρει το Διαδίκτυο και γιατί εμπνέει τόση ανησυχία; Υπάρχουν όντως πολλοί λόγοι που διαφοροποιούν το θέμα της ασφάλειας στο Διαδίκτυο και πραγματικά αξίζουν την προσοχή:

a) Οι υπολογιστές μας είναι διασυνδεδεμένοι – Our computers are connected.

Στη μέχρι τώρα γνωστή ιστορία των υπολογιστών η ασφάλεια του συστήματος δεν απασχολούσε ιδιαίτερα, εφόσον οι χρήστες είτε δούλευαν μέσα στον ίδιο χώρο ή σε άμεσα συνδεδεμένα τερματικά. Στο Διαδίκτυο όμως, ουσιαστικά επιτρέπεται στον οποιονδήποτε στον κόσμο, να χρησιμοποιήσει τον υπολογιστή, έστω και σε κάποιον περιορισμένο βαθμό όπως π.χ να κατεβάσει μία ιστοσελίδα. Μοιάζει σαν να έχει ανοιχτεί μία «*διέξοδο στο φράγμα*» και πρέπει ο σχεδιασμός, η εφαρμογή και η διαχείριση του συστήματος να γίνει με ιδιαίτερη προσοχή, ώστε να διασφαλιστεί ότι δεν θα «ξεπηδήσει» ολόκληρο το φράγμα μέσα από αυτή τη δίοδο.

b) Το Δίκτυο ανήκει σε όλους – The Network is Public

Ένα δια-δίκτυο δεν είναι τίποτα άλλο παρά μία δια-συνδεδεμένη ομάδα δικτύων και κατ' επέκταση το Διαδίκτυο διεκδικεί τον τίτλο του μεγαλύτερου δια-συνδεδεμένου δικτύου δεδομένων στον κόσμο.

Τα μεμονωμένα δίκτυα ανήκουν σε χιλιάδες διαφορετικά άτομα ή οργανισμούς και δεν υπάρχει κάποιος κεντρικός διαχειριστής.

Το συνδετικό υλικό, αυτό που ενώνει το Διαδίκτυο σε ένα «όλο» είναι η συμφωνία για τη χρήση κοινών πρωτοκόλλων και το γεγονός ότι τα δίκτυα αποτελούν τους φορείς διακίνησης δεδομένων μεταξύ τους.

c) *Το Δίκτυο είναι ψηφιακό – The Network is Digital.*

Ακόμα και εάν κάποιος αποκτήσει πρόσβαση σε ένα τηλεφωνικό σύστημα είναι αρκετά δύσκολο και χρονοβόρο να μάθει χρήσιμες πληροφορίες κρυφακούγοντας τις ξένες συνομιλίες. Φυσικά εάν κάποιος μπορέσει να μπει σε συγκεκριμένη γραμμή και να παρακολουθήσει το άτομο που τον ενδιαφέρει άμεσα, τότε τα πράγματα είναι εύκολα. Αν όμως κάποιος απλώς ακούει συνδιαλέξεις στην τύχη περιμένοντας να ακούσει π.χ έναν αριθμό πιστωτικής κάρτας, θα περιμένει προφανώς πολύ. Ένα δίκτυο υπολογιστών από την άλλη μεριά, προσφέρει τη δυνατότητα να «ακούσει» κανείς πολλές συνομιλίες ταυτόχρονα. Επιπλέον ένας υπολογιστής μπορεί να ξεχωρίσει και να απομονώσει μέσα από διάφορες “συνομιλίες” συγκεκριμένα patterns, όπως π.χ το αριθμητικό υπόδειγμα-πρότυπο του αριθμού μιας πιστωτικής κάρτας χωρίς ο εισβολέας να χρειαστεί να εμπλακεί προσωπικά σε αυτή τη δουλειά.

d) Οι Υπολογιστές είναι δεξαμενές συλλογής δεδομένων.

Ας φανταστούμε ότι μια εταιρεία κρατάει στο αρχείο της καρτέλες για κάθε έναν πελάτη της ξεχωριστά με όλα τα στοιχεία που την αφορούν. Εάν κάποιος θελήσει να παραβιάσει ή να υποκλέψει αυτά τα στοιχεία π.χ αριθμούς πιστωτικών καρτών θα πρέπει να ψάξει καρτέλα - καρτέλα, έργο εφικτό μεν αλλά εξαιρετικά χρονοβόρο δε και μάλλον κουραστικό. Σε ένα σύστημα υπολογιστών αντιθέτως, τα επιθυμούμενα και ευαίσθητα αυτά στοιχεία είναι εύκολα προσβάσιμα και συνήθως σε μορφή που τα θέλουμε π.χ όλα τα νούμερα πιστωτικών καρτών σε έναν συγκεντρωτικό κατάλογο.

e) Οι υπολογιστές μπορούν να προγραμματιστούν

Όπως προαναφέρθηκε, ένα από τα προβλήματα είναι ότι ένας εισβολέας μπορεί να προγραμματίσει έναν υπολογιστή κατά τρόπον ώστε να εντοπίζει μέσα από μεγάλες ποσότητες πληροφοριών αυτές ακριβώς που τον ενδιαφέρουν. Οι υπολογιστές μπορεί επίσης να προγραμματιστούν και για άλλες παράνομες δραστηριότητες, όπως π.χ να υποβάλλουν εκατοντάδες, ή χιλιάδες πλαστές παραγγελίες ή να διερευνήσουν τρόπους να αποκτήσουν πρόσβαση σε ένα σύστημα υπολογιστών. Ειδικότερα, οι πιο σοφιστικέ εισβολείς μπορούν να γράψουν και να διανείμουν προγράμματα για χρήση από άλλους μη – επιτήδειους εισβολείς, γεγονός που καθιστά τους δεύτερους ιδιαίτερα επικίνδυνους.

f) Το Διαδίκτυο φαίνεται ανώνυμο και απόμακρο.

Η επικοινωνία μέσω του Διαδικτύου φαίνεται πιο αφηρημένη, πιο απρόσωπη ή λιγότερο πραγματική, σε σύγκριση με τη διαπροσωπική επικοινωνία ή ακόμα και σε σχέση με την τηλεφωνική επικοινωνία. Αυτή του η ιδιότητα, παρακινεί πολλούς ανθρώπους να προσπαθήσουν να εξαπατήσουν ή να προκαλέσουν σύγχυση, ή να κάνουν φάρσα στην απόμακρη, απρόσωπη ιστοσελίδα, ενώ οι ίδιοι άνθρωποι ούτε που θα διανοούνταν να κάνουν κάτι παρόμοιο σε ένα γειτονικό κατάστημα.

Αντίστροφα, αυτή η απόσταση που χαρακτηρίζει το Διαδίκτυο, κάνει ακόμα πιο επιτακτική την ανάγκη των καταναλωτών να σιγουρευτούν ότι όντως συναλλάσσονται με την σωστή εταιρεία. Είναι δύσκολο στον πραγματικό κόσμο να κάνεις κάποιον να πιστέψει ότι βρίσκεται π.χ σε ένα μεγάλο γνωστό πολυκατάστημα ενώ δεν είναι, αλλά στο Διαδίκτυο αυτό μπορεί να γίνει πολύ πιο εύκολα.

g) Το Εμπόριο Πληροφοριών παρουσιάζει ιδιομορφίες.

Πολλοί από τους προβληματισμούς ως προς την ασφάλεια που παρέχεται στο δια-δίκτυο, αφορούν το εμπόριο των πληροφοριών. Οι πληροφορίες που μεταδίδονται διαμέσου του δικτύου είναι εύκολο να αντιγραφούν, να διανεμηθούν, να μετατραπούν. Όταν κάποιος πουλάει πληροφόρηση απαιτεί να παραδοθεί το προϊόν του μόνο στον αγοραστή και όχι στον οποιονδήποτε που μπορεί να "κρυφακούσει". Στον φυσικό κόσμο π.χ ο ταχυδρόμος μπορεί να φωτοτυπήσει ένα περιοδικό, όμως αυτή η ενέργεια απαιτεί κάποια προσπάθεια εκ μέρους του, ενώ η αντιγραφή του σε ηλεκτρονική μορφή, απαιτεί μονάχα μερικά κτυπήματα στο πληκτρολόγιο. Ως αγοραστές πληροφοριών θέλουμε να είμαστε βέβαιοι ότι οι πληροφορίες που παραλάβαμε είναι όντως αυτές που μας έστειλαν.

Πάλι, απαιτεί αρκετή προσπάθεια να υποκλέψει και να παραποιήσει κανείς ένα πραγματικό γράμμα, αλλά ηλεκτρονικά αυτό είναι αρκετά εύκολο. Ως πωλητές πληροφοριών, συνήθως θέλουμε να παραδίδουμε τα προϊόντα μας αμέσως, έτσι δεν έχουμε την ευκαιρία για απολογιστικούς ελέγχους, όπως στις ταχυδρομικές παραγγελίες.

Το νομοθετικό πλαίσιο πρέπει να εκσυγχρονιστεί για να παρακολουθεί τις εξελίξεις. Πολλά από τα θέματα που αναφέρθηκαν καλύπτονται από κάποιο νομοθετικό πλαίσιο. Όμως η νομοθεσία, στηρίζεται σε φυσικά και απτά αποδεικτικά μέσα, έγγραφα συμβόλαια, υπογραφές, διευθύνσεις παραλαβής, κλπ. για να στοιχειοθετήσει μία υπόθεση.

Στο ηλεκτρονικό εμπόριο μέσω Διαδικτύου, αυτό που μπορεί να αντικαταστήσει μία υπογραφή στις περισσότερες περιπτώσεις, εάν όχι σε όλες, είναι οι ψηφιακές υπογραφές. Αυτές αποτελούν μία σχετικά νέα τεχνολογία, και χρειάζεται αρκετά

μεγάλη προσπάθεια να κατανοήσει κανείς τις λεπτομέρειές της. Ομοίως, κι άλλες περιοχές του νόμου καλούνται να αντιμετωπίσουν τις αλλαγές της τεχνολογίας.

h) Τα συστήματα υπολογιστών είναι ευάλωτα σε επιθέσεις.

Στο παρελθόν, τα συστήματα των υπολογιστών έχουν αποδειχθεί εξαιρετικά ευαίσθητα και ευάλωτα στις οποιεσδήποτε επιθέσεις και έτσι θα πρέπει να είμαστε προσεκτικοί και να επαγρυπνούμε για τα νέα συστήματα του Διαδικτυακού εμπορίου. Κυριαρχεί η αντίληψη ότι υπάρχει πρόβλημα. Η ασφάλεια στο Διαδίκτυο έχει γίνει πρωτοσέλιδο στους "*New York Times*" και στη "*Wall Street Journal*" κι έτσι πολλοί άνθρωποι και αγοραστές και πωλητές, προβληματίζονται και ανησυχούν σοβαρά για τα θέματα ασφαλείας. Ακόμα και όταν οι κίνδυνοι μπορεί να φαίνονται μικρότεροι από αυτούς στον πραγματικό κόσμο, η γενική αντίληψη είναι ότι οι κίνδυνοι είναι πολύ μεγαλύτεροι, κατά συνέπεια είναι σημαντικό αυτοί να αντιμετωπιστούν στη φάση του σχεδιασμού και της εφαρμογής των συστημάτων που προορίζονται για εμπορική χρήση στο Διαδίκτυο. **[4]**

Σήμερα μια εταιρεία μπορεί να ακούσει τους πελάτες της απ' ευθείας. Επιπλέον μπορεί να μάθει πολλά γι' αυτούς και ταυτόχρονα να τους εκπαιδεύσει. Γιατί όμως μια σχετικά μικρή εταιρεία κάνει όλες αυτές τις προσπάθειες;

Όπως είναι γνωστό οι εταιρείες δουλεύουν κάτω από συνεχόμενες αυξανόμενες πιέσεις του επιχειρηματικού περιβάλλοντος. Πιέσεις γνωστές ως 3C, δηλαδή ανταγωνισμός (competition), πελάτες (customers) και αλλαγή (change). Η εύρεση και η διατήρηση πελατών από μια εταιρεία είναι ο πιο σημαντικός παράγων επιτυχίας για τις περισσότερες. Η παρουσία των 3C δεν είναι καινούργια. Οι

εταιρείες «παλεύουν» για πελατεία, δεκαετίες. Τα νέα δεδομένα είναι η ένταση του ανταγωνισμού, η δύναμη των πελατών αλλά και το μέγεθος των αλλαγών.

Όλα αυτά οδηγούν σε μια στρατηγική: Πρέπει να ελέγχεις τα 3C για να επιτύχεις, ακόμα και για να επιβιώσεις.

Το Η/Ε είναι το νέο κανάλι διανομής, το οποίο ανταγωνίζεται τα παραδοσιακά. Η προσέλκυση των πελατών από εταιρείες που πουλούν μέσω Ηλεκτρονικού Εμπορίου είναι δύσκολη, διότι πρέπει πρώτα να πείσουν τους πελάτες να αγοράσουν και ύστερα να γίνει επιλογή της δικής τους εταιρείας ανάμεσα από τόσους ανταγωνιστές. Πάντως η επιτυχία της κάθε επιχείρησης στηρίζεται στη κατανόηση της συμπεριφοράς του αγοραστή.

ΚΕΦΑΛΑΙΟ Β.

ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΟΥ

Το Διαδίκτυο μπορεί να ανοίξει πολλές δυνατότητες στις επιχειρήσεις, επιτρέποντας πρόσβαση σε ατελείωτους πόρους. Δυστυχώς, με όλες αυτές τις επιπλέον δυνατότητες, δημιουργούνται και επιπλέον κίνδυνοι. Αν το δίκτυο μιας εταιρείας μπορεί να προσπελάσει το Διαδίκτυο, οποιοσδήποτε στο Διαδίκτυο μπορεί να έχει πρόσβαση στο δίκτυο της εταιρεία αυτής. Οι αποφάσεις που παίρνει κάποιος, σαν διαχειριστής, για την ασφάλεια του δικτύου, είναι οι πιο σημαντικές αποφάσεις για το δίκτυο.

Γενικά η ασφάλεια δικτύου μπορεί να οριστεί σαν προστασία ενός δικτύου από οποιονδήποτε κίνδυνο. Επειδή αυτός ο ορισμός είναι γενικός, ο κόσμος σπάνια συνειδητοποιεί το πραγματικό βάθος όλων όσων περιλαμβάνονται στη σχεδίαση της ασφάλειας. Η αλήθεια είναι ότι η ασφάλεια μπορεί να είναι το πιο χρονοβόρο μέρος της συντήρησης οποιουδήποτε δικτύου και ειδικά ενός δικτύου ηλεκτρονικής επιχείρησης, επειδή τα θέματα ασφαλείας συνεχώς αλλάζουν.

Μια χρήσιμη, νοητική εικόνα της διαδικασίας είναι να σκεφτείτε την ασφάλεια του δικτύου σαν μια τραμπάλα, στην οποία η μια πλευρά είναι το δίκτυο της εταιρείας και η άλλη πλευρά είναι ο υπόλοιπος online κόσμος και η ασφάλεια βρίσκεται στο μέσον, εξισορροπώντας τον φόρτο. Λογικά συνεπώς οποιαδήποτε

στιγμή γίνει μια αλλαγή σε οποιαδήποτε πλευρά της τραμπάλας, η ασφάλεια στο μέσο πρέπει να αλλάξει για να διατηρηθεί η ισορροπία.

Β.1 ΑΝΑΛΥΣΗ ΤΩΝ ΚΙΝΔΥΝΩΝ

Ένα σημαντικό ζήτημα στον σχεδιασμό μίας πολιτικής ασφαλείας αποτελεί ο προσδιορισμός του επιθυμητού επιπέδου προστασίας απέναντι σε γνωστούς και καθορισμένους κινδύνους και απειλές. Για παράδειγμα, μια τράπεζα αντιμετωπίζει διαφορετικούς κινδύνους από ότι ένα ιδιώτης και επομένως η τράπεζα έχει σοβαρούς λόγους να πληρώσει περισσότερα για να προστατευθεί από αυτούς τους κινδύνους.

Πολλές από τις επιλογές ασφαλείας προσδιορίζονται από το κόστος των μέτρων ασφαλείας – κόστος που μπορεί να μετρηθεί σε χρήμα, σε απόδοση κλπ. Χωρίς μία βαθιά κατανόηση των ωφελειών που μπορεί να προσφέρουν κάποια συγκεκριμένα μέτρα ασφαλείας, είναι αδύνατον να εκτιμηθούν οι υπάρχουσες επιλογές από επιχειρηματική άποψη.

Β.1.1 Εχθροί

Το πρώτο βήμα κάθε μελέτης ασφαλείας είναι η γνωριμία με τον εχθρό. Οι περισσότεροι επικεντρώνονται σε διάφορες μορφές επιθέσεων και στις επακολουθούσες συνέπειες, ξεχνώντας ότι τα μέσα των επιθέσεων είναι απλά και μόνον τα εργαλεία. Ένας αποφασισμένος εισβολέας, για παράδειγμα, μπορεί να είναι πρόθυμος να δουλέψει πολύ σκληρά για να εισχωρήσει σε ένα σύστημα, ενώ ένας περιστασιακός, ίσως εγκαταλείψει νωρίς την προσπάθεια. Και οι δύο

ενδέχεται να κάνουν επιθέσεις κατά τον ίδιο τρόπο αλλά εδώ η επιμονή είναι που κάνει τη διαφορά. Άρα, θα πρέπει να τεθούν τα εξής ερωτήματα :

1) Ποίος ή ποίοι είναι οι εχθροί;
2) Τι σκοπεύουν – Ποίοι είναι οι σκοποί τους – τι ακριβώς επιδιώκουν;
3) Τι μέσα διαθέτουν;

Στη συνέχεια δίνεται ένας κατάλογος ***πιθανών εχθρών.***

- **Οι εισβολείς (hackers)**

Ως εισβολέας θεωρείται ο ερασιτέχνης χομπίστας. Συνήθως μπορεί να αποτελέσει την πιο σοβαρή απειλή για την ασφάλεια των συστημάτων Ηλεκτρονικού Εμπορίου. Τα άτομα αυτά έχουν πρόσβαση σε ευαίσθητα συστήματα και πληροφόρηση. Το πρόβλημα έγκειται στο απροσδόκητο της συμπεριφοράς τους, καθώς ο στόχος σπανίως είναι το κέρδος. Υπάρχουν περιπτώσεις όπου έχει παραβιασθεί η ασφάλεια κεντρικού υπολογιστή τράπεζας και, αντί να γίνει κλοπή, όλα τα υπόλοιπα πολλαπλασιάστηκαν επί 1000. Αυτό έγινε αντιληπτό 3 μέρες αργότερα, όταν η τράπεζα έκανε μια μεταφορά χρημάτων πάνω από το όριο που είχε ορισθεί από την κεντρική τράπεζα. Το ξεκαθάρισμα της κατάστασης πήρε αρκετές μέρες με σημαντικό συνολικό κόστος.

Μια τέτοια άσκοπη ουσιαστικά παραμόρφωση των δεδομένων είναι πολύ δύσκολο να εντοπισθεί. Αν η παραμόρφωση κρατήσει κάποιες μέρες χωρίς να γίνει αντιληπτή, το κόστος επαναφοράς στην αρχική κατάσταση γίνεται σημαντικό.

Γενικά οι εισβολείς είναι άτομα μικρής σχετικά ηλικίας, με σημαντική τεχνογνωσία. Χρησιμοποιούν διάφορες μεθόδους, οι περισσότερες από τις οποίες είναι αποτέλεσμα πειραματισμών και εμπειρίας. Με δεδομένο ότι χρειάζεται αρκετή

υπομονή, οτιδήποτε μπορεί να παραβιαστεί. Ακόμα και το ασφαλέστερο σύστημα δεν είναι άτρωτο. Εξάλλου για κάθε κλειδαριά υπάρχει και ένα κλειδί που την ανοίγει. Πάντως το hacking δεν είναι εύκολη υπόθεση. Ανάμεσα στους βασικούς παράγοντες είναι η ευφυΐα και η δημιουργικότητα.

- **Crackers**

Οι crackers είναι οι γνωστοί «πανκ του κυβερνο-χώρου» που αρέσκονται να εισβάλλουν σε συστήματα υπολογιστών ή για βανδαλισμό, ή για προσωπικό όφελος. Είναι εμπαθείς εισβολείς (hackers) και χαρακτηρίζονται περισσότερο από την επιθυμία τους να καταστρέψουν παρά από τις ικανότητες τους στον προγραμματισμό.

Οι crackers, συχνά είναι έφηβοι, χωρίς ιδιαίτερες ικανότητες, χρησιμοποιούν έτοιμο λογισμικό επιθέσεων από το δίκτυο, ή από περιοδικά, τις περισσότερες φορές χωρίς να είναι καν σε θέση να το κατανοήσουν. Δε διαθέτουν ισχυρό και σοβαρό εξοπλισμό υπολογιστών. Συχνά προκαλούν σημαντικές ζημιές, είτε καταστρέφοντας συστήματα, είτε επιδιδόμενοι σε βανδαλισμούς συστημάτων είτε διακόπτοντας τη λειτουργία τους, είτε απλώς απασχολώντας το προσωπικό ενός οργανισμού, που προσπαθεί να εντοπίσει τις ζημιές και να τις αποκαταστήσει.

Οι πραγματικοί crackers είναι πολύ λίγοι. Αυτοί είναι άνθρωποι που ξέρουν να σπάνε την ασφάλεια διαφόρων συστημάτων. Κάτι τέτοιο απαιτεί πολλή μελέτη, υψηλή ευφυΐα και αρκετή διάθεση για πρόκληση κακού. Αν και σπάνια συναντώνται, οι crackers αυτοί είναι εξαιρετικά επικίνδυνοι επειδή είναι αρκετά έξυπνοι ώστε να κάνουν κακό και επειδή πολλοί απ’ αυτούς γράφουν τα προγράμματα που χρησιμοποιούν οι λιγότεροι ικανοί.

- **Ιοί**

Αυτόνομα, κακόβουλα προγράμματα. Ο μεγαλύτερος κίνδυνος από όλους. Ένας ιός Η/Υ είναι ένα πρόγραμμα με την ικανότητα να αντιγράφει τον εαυτό του. Με αυτόν τον μηχανισμό οι ιοί προχωρούν από υπολογιστή σε υπολογιστή. Είναι ένα πρόβλημα ακόμα και εάν δεν είναι προγραμματισμένοι να κάνουν κάτι το καταστροφικό. Χαρακτηριστικό παράδειγμα ο ιός Impostor, ο οποίος δε φαίνεται να κάνει τίποτα εκτός από το να αναπαραγάγει τον εαυτό του. Παρά ταύτα, στο τέλος μολύνονται όλα τα αρχεία του Microsoft Office με σημαντική καθυστέρηση του Η/Υ, όταν δουλεύουν αυτά τα αρχεία.

- **Criminals**

Ακόμα και χωρίς το Διαδίκτυο, υπάρχει τεράστιος όγκος “συγκεκαλυμμένου εγκλήματος”, που εκμεταλλεύεται τις αδυναμίες των υπολογιστικών συστημάτων. Επειδή το Διαδίκτυο είναι πανταχού παρόν και ανώνυμο, έχει γίνει ένα πολύ δελεαστικό «άντρο» εγκλήματος. Το Διαδικτυακό έγκλημα μπορεί να έχει πολλές διαβαθμίσεις, από απλή απάτη με κλεμμένα νούμερα πιστωτικών καρτών σε πιο σοφιστικέ επιθέσεις για πρόσβαση σε χρήματα ή πληροφορίες.

Οι «εγκληματίες» αυτού του είδους, ίσως δεν έχουν τα μέσα να σπάσουν κρυπτογραφικούς κώδικες, αλλά έχουν την οικονομική δυνατότητα να δωροδοκήσουν υπαλλήλους ή άλλα άτομα που έχουν πρόσβαση σε συστήματα Ηλεκτρονικού Εμπορίου. Απώτερος σκοπός τους σε όλες τις περιπτώσεις είναι το οικονομικό όφελος.

- **Cookies**

Πως θα μπορούσε κάτι που ακούγεται τόσο αθώο, όπως ένα cookie να δημιουργεί κινδύνους ασφαλείας; Στον κόσμο της Web περιήγησης, τα cookie – αυτά τα μικρά τμήματα δεδομένων που διατηρούν πολλές τοποθεσίες στο σκληρό δίσκο, είναι συνήθως ακίνδυνα. Για παράδειγμα σε μια τοποθεσία που προσφέρει προσαρμοσμένα περιεχόμενα, όπως το Amazon.com τα cookie χρησιμοποιούνται για να προσδιορίζουν, ώστε να εμφανίζουν προσαρμοσμένα περιεχόμενα (και να προσπαθήσουν να πουλήσουν βιβλία και DVD βασισμένα σε αυτά που αγοράσθηκαν προηγουμένως). Αλλά μερικοί ειδικοί προειδοποιούν ότι τα cookie μπορεί να χρησιμοποιηθούν με επικίνδυνο τρόπο. Ανησυχούν ότι οι εταιρείες μπορεί να χρησιμοποιήσουν τα cookie για να παρακολουθούν τους χρήστες χωρίς αυτοί να το ξέρουν.

- **Οι ανταγωνιστές**.

Ένας ανταγωνιστής ίσως να μην ενδιαφέρεται τόσο να κλέψει τα χρήματά ή να καταστρέψει τα αρχεία μιας εταιρείας, αλλά η πρόσβαση στις λίστες των πελατών της ή στα επιχειρηματικά της πλάνα ίσως αποδειχθεί εξαιρετικά πολύτιμη για αυτούς. Ακόμα, ένας ανταγωνιστής που κατορθώνει να μάθει τις αδυναμίες του συστήματος ασφαλείας της, ίσως χρησιμοποιήσει αυτήν την πληροφορία εναντίον της σε περιπτώσεις ανταγωνιστικών πωλήσεων ή γενικά για να της δυσφημίσει. Αν και οι μεγάλες επιχειρήσεις έχουν μεγάλη οικονομική ευχέρεια, είναι μάλλον απίθανο να δαπανήσουν μεγάλα ποσά σε παράνομες ή ανήθικες δραστηριότητες.

- **Οι Ερευνητές**

Ένας ερευνητής μπορεί να δουλέψει πολύ σκληρά για να εντοπίσει αδυναμίες στα πρωτόκολλα ασφαλείας και να τα δημοσιεύσει στο δίκτυο. Αυτές οι αποκαλύψεις προκαλούν δημοσιότητα και κάποια αμηχανία, αλλά έμμεσα οδηγούν στη δημιουργία πιο ασφαλών συστημάτων. Οι ερευνητές συνήθως έχουν πρόσβαση σε ισχυρούς υπολογιστές και συστήματα.

- **Οποιοσδήποτε έχει φυσική πρόσβαση στα συστήματα** .

Οποιοσδήποτε έχει πρόσβαση στις φυσικές εγκαταστάσεις ενός οργανισμού αποτελεί μία πιθανή απειλή. Σε αυτούς συγκαταλέγονται π.χ τα συνεργεία καθαρισμού, το προσωπικό παραδόσεων, επισκέπτες, υπεργολάβοι και προσωρινοί υπάλληλοι.

Συγκεκριμένα οι υπάλληλοι μιας εταιρείας είναι εξίσου σημαντικός κίνδυνος. Υπάλληλοι που ήθελαν να προαχθούν αλλά δεν προήχθησαν, υπάλληλοι που πιστεύουν ότι δεν πληρώνονται αρκετά κλπ. Αν κάποιος το σκεφτεί είναι λογικό: τι καλύτερο για ένα υπάλληλο που θέλει να εκδικηθεί από το να χαλάσει κάτι που χαλάει εύκολα και κανείς δε μπορεί να το επιδιορθώσει εύκολα;

Συμπερασματικά, ο κάθε οργανισμός θα πρέπει να εκτιμήσει τους κινδύνους που απορρέουν από τις προαναφερθείσες ομάδες, ανάλογα με τις ιδιαίτερες ανάγκες του. **[4] – [1]**

Β.1.2 Απειλές

Αφού έγινε μια σύντομη αναφορά στους πιθανούς εχθρούς συνεχίζεται η μελέτη ασφαλείας στο δεύτερο στάδιο της διερεύνησης των πιθανών επιθέσεων και η εκτίμηση του πιθανού κινδύνου:

Για παράδειγμα, οι επικοινωνίες μέσω ανοικτών δικτύων είναι εκτεθειμένες σε πολλούς κινδύνους, όπως π.χ σε υποκλοπές, «μεταμφιέσεις» κλπ.

Επιπλέον, είναι πιθανόν να δεχθούν επίθεση οι υπολογιστές των πελατών και των διακομιστών και ακόμα μία εφαρμογή μπορεί να γίνει αντικείμενο επίθεσης εκτός του περιβάλλοντος πελάτη - διακομιστή.

Οι κίνδυνοι οι οποίοι απειλούν το ηλεκτρονικό κατάστημα έχουν ως εξής:

- *Υποκλοπή πακέτων*

Ένας τρόπος που κάποιος απ' έξω θα μπορούσε να αποκτήσει πρόσβαση σε ένα ιδιωτικό δίκτυο είναι με την υποκλοπή και το διάβασμα των πακέτων του δικτύου - είναι δεδομένα που περνούν γρήγορα το ένα μετά το άλλο, δημιουργώντας μια αλυσίδα που διαβάζεται σαν μια μεγάλη πρόταση και επιτρέπει να επικοινωνούν υπολογιστές δικτύων. Περίπου σαν το πέρασμα της μπάλας στο ποδόσφαιρο, αν λάθος άτομα υποκλέψουν αυτά τα πακέτα, μπορούν να συμβούν άσχημα πράγματα.

Αν και η λέξη «εισβολέας» παραπέμπει σε ένα εξωτερικό άτομο που προσπαθεί να σπάσει το δίκτυο, είναι σημαντικό να θυμάστε ότι τα περισσότερα κενά ασφαλείας προέρχονται από εσωτερικούς χρήστες. Αυτό ισχύει ιδιαίτερα στην περίπτωση υποκλοπών πακέτων. Αυτός που επιτίθεται πρέπει να βρει τρόπο να έχει άμεση σύνδεση με τα δεδομένα καθώς περνούν διάφορους πόρους, για να μπορεί να πάρει αυτές τις πληροφορίες. Αυτό αναφέρεται επίσης σαν ‘‘παρακολούθηση καλωδίων’’.

Τα περισσότερα δίκτυα στέλνουν πακέτα με παρόμοια μοτίβα και έτσι είναι εύκολο να διαβαστούν τα πακέτα αν υποκλαπούν. Τα πιο συνηθισμένα τμήματα πληροφοριών που παίρνονται από τα κλεμμένα πακέτα είναι κωδικοί πρόσβασης ή οι λογαριασμοί χρηστών, που παρέχουν στον εισβολέα ένα επιπλέον τρόπο να προσπελάσει το δίκτυο. Αν ένας εισβολέας μπορεί να διαβάσει τα πακέτα του δικτύου, οι πιθανότητες είναι ότι έχει τη δυνατότητα να τ' αλλάξει. Αυτό σημαίνει ότι θα μπορούσε να δημιουργήσει ένα δικό του λογαριασμό για να το χρησιμοποιήσει οποιαδήποτε στιγμή. Αφού δημιουργηθεί το όνομα χρήστη και ο κωδικός πρόσβασης θα έχει το νόμιμο δικαίωμα να μπει στο δίκτυο και να αλλάξει πληροφορίες στις βάσεις δεδομένων της εταιρείας.

Εάν γίνει μια επίθεση με αυτό το τρόπο, είναι συνήθως δύσκολο να εντοπιστεί ή να σταματήσει. Είναι πολύ συνηθισμένο να χρησιμοποιούν οι χρήστες το ίδιο όνομα χρήστη και κωδικό πρόσβασης σε πολλές εφαρμογές, ώστε να περιορίσουν τον αριθμό των πραγμάτων που πρέπει να θυμούνται. Έχοντας ένα κλειδί που μπαίνει σε πολλές κλειδαριές ανοίγουν πολλές πόρτες για τον εισβολέα που θέλει να λειτουργήσει σαν ένας νόμιμος χρήστης. Παρόμοιο πρόβλημα είναι η επίθεση στα ίδια πακέτα, που είναι δύσκολο να εντοπιστεί, επειδή οι διαχειριστές δικτύου συνήθως χρησιμοποιούν τα ίδια εργαλεία εντοπισμού για να βρουν ή να διορθώσουν προβλήματα στο δίκτυο τους.

- *Κλοπή Αρχείων*

Ένας attacker μπορεί να αποκτήσει πρόσβαση στα αρχεία της εταιρείας, σε ευαίσθητα απόρρητα δεδομένα, σχετικά με το σύστημα ή σε απόρρητα στοιχεία

που αφορούν τους πελάτες. Π.χ ένας εισβολέας μπορεί να κλέψει φακέλους πελατών που ίσως εμπεριέχουν αριθμούς πιστωτικών καρτών.

- *Εξαπάτηση IP*

Η εξαπάτηση IP είναι ένας άλλος τρόπος να κερδίσει πρόσβαση στο δίκτυο κάποιος που επιτίθεται. Η εξαπάτηση των IP συμβαίνει όταν μια εξωτερική πηγή εμφανίζεται σαν μια εσωτερική IP διεύθυνση. Το δίκτυο μπερδεύεται μετά και στέλνει πακέτα στη λάθος IP διεύθυνση. Κι πάλι εάν αυτά τα πακέτα δεν είναι κρυπτογραφημένα, μπορούν εύκολα να διαβαστούν, δίνοντας εμπιστευτικές πληροφορίες σε ένα εξωτερικό άτομο. Και πάλι στο χειρότερο σενάριο, ο εισβολέας θα μπορούσε να πάρει πληροφορίες για ένα όνομα χρήστη και κωδικό πρόσβασης. Αν ένας εισβολέας έχει τη δυνατότητα να ξέρει την ταυτότητα ενός πιστοποιημένου χρήστη, ο εισβολέας έχει πολλή ελευθερία μέσα στο δίκτυο και μπορεί να το χρησιμοποιήσει για να αλλάξει πληροφορίες ή προγράμματα.

Οι πληρωμές νόμιμων και εξουσιοδοτημένων χρηστών είναι δυνατόν να “δρομολογηθούν” σε ένα μη-εξουσιοδοτημένο προορισμό. Αν και αυτή η μορφή απάτης είναι δύσκολο να εφαρμοστεί στις πληρωμές μέσω πιστωτικών καρτών, εν τούτοις μπορεί να χρησιμοποιηθεί σε άλλα πιο ευάλωτα συστήματα πληρωμών. Για παράδειγμα, ένας πωλητής – φαινομενικά καθ’ όλα νόμιμος - μπορεί να πουλήσει “πρόσβαση” στα αρχεία ή στα συστήματα ενός άλλου πωλητή. Η πληρωμή θα πάει σε λάθος προορισμό χωρίς ο αγοραστής να αντιληφθεί αυτή την παρέκκλιση.

- *Εξαπάτηση με άρνηση υπηρεσιών*

Μερικές φορές, όταν ένας εισβολέας βρει ένα τρόπο πρόσβασης στο δίκτυο μιας εταιρείας, χρησιμοποιεί τις πληροφορίες που έχει υποκλέψει για να χαλάσει τις πληροφορίες που βρίσκονται σε αυτό το δίκτυο. Ένα παράδειγμα είναι η επίθεση άρνησης υπηρεσίας. Οι επιθέσεις αυτές είναι αυτό που λέει το όνομα τους, δηλαδή επιθέσεις που κλειδώνουν πιστοποιημένους χρήστες έξω από εφαρμογές ή πόρους του ιδίου του δικτύου. Αυτές οι επιθέσεις έχουν σχεδιαστεί και χρησιμοποιούνται για να παρέμβουν στην κανονική λειτουργία της εταιρείας. Η έλλειψη πρόσβασης σε μια εφαρμογή ενοχλεί τους χρήστες και μπορεί να κοστίσει πολύ σε χαμένη απόδοση.

- *Διακοπή της λειτουργίας ενός υπολογιστικού συστήματος και πρόκληση προβλημάτων στη λειτουργία του.*

Αυτή η μορφή προβλήματος, μπορεί να προκληθεί από διακοπή της λειτουργίας των συσκευών ή πρόκληση δυσλειτουργιών π.χ του δίσκου, του υπολογιστή, ή των δικτύων. Ακόμα χειρότερα μία επίθεση “άρνησης λειτουργίας” εκ των έξω μπορεί να παραλύσει τη λειτουργία του συστήματος. Για παράδειγμα, ένας εισβολέας μπορεί να αναπτύξει έναν ιό στο λειτουργικό σύστημα ενός διακομιστή και να προκαλέσει καταστροφή ή διακοπή του συστήματος. Σε μία τέτοια μορφή επίθεσης, δεν υπάρχει αποκάλυψη ευαίσθητων πληροφοριών, αλλά την παρακώλυση της αποδοτικής και ομαλής λειτουργίας μίας επιχείρησης.

- *Μολυσμένα Δεδομένα.*

Σε αυτή τη μορφή επίθεσης, ολόκληρα αρχεία μπορεί να καταστραφούν ή να κατασταθούν αναξιόπιστα. Αυτό θα μπορούσε να προκληθεί από έναν ιό

λογισμικού, ή από μία βλάβη του εξοπλισμού, ή από μία άμεση επίθεση. Αυτού του είδους η επίθεση, μπορεί να πάρει διάφορες μορφές: ο εισβολέας μπορεί να αλλοιώσει νόμιμα αρχεία ή να εισάγει σκόπιμα, πλαστά δεδομένα μέσα στο σύστημα. Το πρόβλημα που μπορεί να προκύψει με τα «μολυσμένα» δεδομένα, μπορεί να είναι πολύ σοβαρό και να μην αντιμετωπίζεται.

Για παράδειγμα, εάν χαθούν τα αρχεία μίας επιχείρησης, οποιοσδήποτε γίνεται γνώστης του γεγονότος, μπορεί να αμφισβητήσει την αξιοπιστία των συναλλαγών εκ του ασφαλούς, γνωρίζοντας ότι τα στοιχεία δεν υπάρχουν πλέον ως αποδεικτικό στοιχείο.

- *Αλλοίωση Δεδομένων ή Περιεχομένου*

Οι εισβολείς μπορεί να “σπάσουν” ένα σύστημα και να αλλοιώσουν το περιεχόμενο του. Για παράδειγμα crackers μπορεί να εισβάλλουν σε μία ιστοσελίδα και να ζωγραφίσουν πάνω στις εικόνες κλπ.

- *Μεταμφίεση - Πλαστοπροσωπία*

Μια ιδιόμορφη περίπτωση που μοιάζει με πλαστοπροσωπία είναι η χρήση ενός ονόματος ενός δικτυακού τόπου που να διαφέρει μόνο σε ένα γράμμα από ένα άλλο. Αν τα δυο αυτά γράμματα είναι κοντά στο πληκτρολόγιο τότε ένας υποψήφιος πελάτης, κάνοντας ένα συνηθισμένο λάθος θα βρεθεί σε άλλο δικτυακό τόπο. Αν ο τόπος αυτός μοιάζει με αυτόν που πραγματικά ήθελε ο πελάτης υπάρχει η πιθανότητα να γίνουν συναλλαγές χωρίς να γίνει αντιληπτό το λάθος. Αυτό το κόλπο χρησιμοποιείται με τα ονόματα των εταιρειών (π.χ αντί

WWW.IBM.COM να ονομάσουμε το κόμβο WWW.IVM.COM) με γνωστό όνομα ώστε να «υποκλέπτεται» ένα ποσοστό της πελατείας της γνωστής εταιρείας.

Οι εισβολείς σε αυτή την περίπτωση δημιουργούν μία ιστοσελίδα που μοιάζει με αυτή κάποιας εταιρείας και τραβούν έτσι την προσοχή ανυποψίαστων χρηστών.

Οι μέθοδοι που χρησιμοποιούνται σε αυτές τις επιθέσεις είναι σύνθετες και ποικίλες. Παραθέτουμε μερικούς από τους πιο συνηθισμένους μηχανισμούς επίθεσης :

1) Υποκλοπή συνομιλιών – μηνυμάτων

Ο εισβολέας ακούει τα μηνύματα που διακινούνται διαμέσου του δικτύου. Τα μηνύματα μπορεί να είναι ή και να μην είναι κωδικοποιημένα, αλλά ακόμα και εάν γίνει μπορεί να μαγνητοφωνηθούν για μεταγενέστερη ανάλυση.

2) Ανάλυση Κυκλοφορίας

Ένας εισβολέας κατορθώνει να μάθει ότι κάποιοι συγκεκριμένοι πελάτες χρησιμοποιούν συγκεκριμένους διακομιστές. Ιστορικά, η ανάλυση κυκλοφορίας υπήρξε πολύτιμη σε στρατιωτικές και διπλωματικές περιπτώσεις.

Β.2 ΑΣΦΑΛΕΙΑ ΔΙΑΚΟΜΙΣΤΗ ΔΙΚΤΥΟΥ

Ο διακομιστής που συνδέει την εταιρεία με το Διαδίκτυο και το Διαδίκτυο με την εταιρεία είναι ένας σταθερός κίνδυνος. Είναι σημαντικό να υπάρχει μια σαφή ιδέα ποιοι είναι οι κίνδυνοι που περιβάλλουν τον διακομιστή και τι μέτρα ασφαλείας να παρθούν για να προστατευθεί.

Ο διακομιστής δικτύου είναι η μεγαλύτερη απειλή ασφαλείας στο δίκτυο. Αντίθετα με τις εφόδους στην ασφάλεια ιδιωτικών δικτύων, όπου πολλά προβλήματα συμβαίνουν εξ αιτίας λαθών χρηστών, οι επιθέσεις στο Web διακομιστή γίνονται με σαφή πρόθεση. Οι επιθέσεις στους διακομιστές δικτύου γίνονται για δυο λόγους. Ο πρώτος λόγος είναι ότι μια επίθεση κάποιου είδους μπορεί να δώσει στον εισβολέα σημαντικές πληροφορίες που μπορεί να χρησιμοποιήσει στο μέλλον για να κερδίσει πρόσβαση σε ένα ιδιωτικό δίκτυο. Ο δεύτερος πιθανός λόγος πίσω από μια επίθεση σε διακομιστή είναι για την ίδια τη διασύνδεση με το Διαδίκτυο και για να αλλάξουν οι πληροφορίες που δημοσιεύονται στο Διαδίκτυο.

Αν ένας εισβολέας έχει πρόσβαση στο ιδιωτικό δίκτυο, υπάρχουν διάφορα άμεσα προβλήματα ασφαλείας. Μέσα από το δίκτυο, οι εισβολείς μπορούν να κλέψουν ονόματα χρηστών και κωδικούς πρόσβασης ή ακόμα να δημιουργήσουν τους δικούς τους λογαριασμούς, ώστε να έχουν πρόσβαση σε εσωτερικούς διακομιστές με το όνομα ενός πιστοποιημένου χρήστη. Αν ένας εισβολέας έχει πρόσβαση σε ένα ιδιωτικό δίκτυο με το όνομα χρήστη και κωδικό πρόσβασης, έχει τη δυνατότητα να χειριστεί εφαρμογές, προκαλώντας προβλήματα πρόσβασης για τους εργαζόμενους που έχουν το δικαίωμα να χρησιμοποιήσουν αυτές τις εφαρμογές. Αυτός ο εισβολέας θα είχε επίσης τη δυνατότητα να κλέψει εμπιστευτικά δεδομένα ή να αλλάξει τα δεδομένα που είναι ήδη αποθηκευμένα στο δίκτυο, μειώνοντας την εμπιστευτικότητα της εταιρείας. Τέλος, ο εισβολέας θα μπορούσε επίσης να στείλει αυτές τις εμπιστευτικές ή αλλαγμένες πληροφορίες σε πελάτες ή σε άλλες εταιρείες, που θα έχουν την εντύπωση ότι προέρχονται από νόμιμο χρήστη μέσα από την εταιρεία.

Το δεύτερο είδος της επίθεσης που μπορεί να συμβεί, είναι μια επίθεση στο ίδιο το διακομιστή δικτύου. Μερικοί εισβολείς δεν μπορούν να κλέψουν ευαίσθητες πληροφορίες από την εταιρεία, ή ακόμα να μπουν στο ιδιωτικό δίκτυο. Μερικοί εισβολείς απλώς εισβάλλουν για την ίδια τη πρόκληση. Ίσως η εταιρεία είναι πολύ γνωστή και έχει πολλές επισκέψεις στην ιστοσελίδα της, κάνοντας τη ένα καλό στόχο για τους εισβολείς που θέλουν να σπάσουν ένα διακομιστή δικτύου και μετά να αφήσουν τα σημάδια τους, αποδεικνύοντας τις ικανότητες τους. Ή ίσως ένας εισβολέας αισθάνεται ενόχληση για κάτι που έχει διαφημιστεί ή δημοσιευτεί στην ιστοσελίδα μιας εταιρείας και εισβάλλει στο διακομιστή δικτύου για να αλλάξει τη τοποθεσία της ή για να διαμαρτυρηθεί. Όποια και εάν είναι η περίπτωση, είναι σημαντικό να προστατευθεί η ακεραιότητα της ίδιας της ιστοσελίδας και ότι οι πληροφορίες που δημοσιεύονται δεν έχουν αλλάξει.

Οι λόγοι για ασφάλιση της Web τοποθεσίας είναι πολύ προφανείς. Αν ο διακομιστής δικτύου σπάσει και ένας εισβολέας μπορεί να αλλάξει τις πληροφορίες της Web τοποθεσίας, οι πληροφορίες μπορεί να αντικατασταθούν από άσχετο ή προσβλητικό υλικό. Οι πελάτες που θα προσβληθούν από την τοποθεσία της εταιρείας δεν θα αγοράσουν τίποτα ή θα παραμείνουν μακριά από την εταιρεία για να ανακαλύψουν την αλήθεια. Αν ο κόσμος αισθάνεται ότι μια εταιρεία δεν έχει ασφάλεια, δεν θα αγοράσει τίποτα από τη τοποθεσία της, ούτε θα αισθάνονται άνετα να κάνουν συναλλαγές βασισμένες στο Διαδίκτυο.

ΚΕΦΑΛΑΙΟ Γ

ΤΡΟΠΟΙ ΠΡΟΣΤΑΣΙΑΣ ΤΟΥ (WEB) ΔΙΑΚΟΜΙΣΤΗ ΔΙΚΤΥΟΥ

Γ.1 ΠΟΛΙΤΙΚΗ

Η ασφάλεια του διακομιστή δικτύου είναι ένα άλλο περίπλοκο θέμα ασφαλείας. Το πιο σημαντικό πράγμα που μπορεί να κάνει για το διακομιστή και τη τοποθεσία μια εταιρεία είναι να ορίσει μια σαφή πολιτική για τη Web ασφάλεια.

Αφού η εταιρεία αναπτύξει μια πολιτική, συνεχίζει στη επιλογή των συσκευών που θα συμπεριλαμβάνονται στο σύστημα. Η επιλογή του διακομιστή θα επηρεάσει τις προσπάθειες ασφαλείας του Διαδικτύου. Ένας από τους ευκολότερους τρόπους να γίνει πιο αυστηρή η ασφάλεια του διακομιστή είναι να θυμάται η εταιρεία ότι όσο πιο βασικές είναι οι λειτουργίες του διακομιστή, τόσο πιο δύσκολο είναι να σπάσει ο διακομιστής.

Ο διακομιστής δικτύου είναι το κλειδί για το Διαδίκτυο. Αυτός ο διακομιστής είναι ο τρόπος με τον οποίο όλοι οι χρήστες της εταιρείας μπορούν να έχουν πρόσβαση στο δίκτυο. Είναι επίσης ο τρόπος με τον οποίο όλοι οι άλλοι προσωπικοί υπολογιστές στο Διαδίκτυο μπορεί να έχουν πρόσβαση στην εταιρεία.

Επειδή αυτός ο διακομιστής είναι τόσο βασικό σημείο, είναι πολύ σημαντικό η επιλογή της θέσης για τη τοποθέτηση του διακομιστή στο δίκτυο. Ένας διακομιστής δικτύου, όπως και οποιοσδήποτε διακομιστής, κινδυνεύει προφανώς από ιούς και

επιθέσεις. Τις περισσότερες φορές, οι διακομιστές προστατεύονται περισσότερο από ένα ηλεκτρονικό τείχος που ενεργεί σαν φίλτρο, παρακολουθώντας τι και ποιος προσπελαύνει το διακομιστή πίσω από το ηλεκτρονικό τείχος.

Αν ο διακομιστής δικτύου είναι πίσω από το ηλεκτρονικό τείχος, τότε οποιοσδήποτε έχει πρόσβαση σε αυτόν, επιτρέπεται αυτόματα να έχει πρόσβαση και πίσω από το ηλεκτρονικό τείχος και έτσι στο ιδιωτικό δίκτυο. Αν το ηλεκτρονικό τείχος είναι αυτό που κρατά όλους τους εισβολείς έξω από το ιδιωτικό δίκτυο, τότε ένας εσωτερικός διακομιστής δικτύου θα ερχόταν σε αντίθεση με το σκοπό του ηλεκτρονικού τοίχου. Οι περισσότεροι αισθάνονται ότι είναι λιγότερο περίπλοκο να παρακολουθούν το διακομιστή δικτύου για πιθανές επιθέσεις ή κινδύνους ασφαλείας και να αντιμετωπίζουν τις συνέπειες όταν συμβαίνουν, παρά να πρέπει να κάνουν συντήρηση και να ψάχνουν για επιθέσεις σε ολόκληρο το δίκτυο. Είναι επίσης πολύ πιο αποτελεσματικό σε σχέση με το κόστος, να διορθώσουν τον διακομιστή δικτύου παρά να αντιμετωπίσουν τα επακόλουθα της εισβολής σε ένα ιδιωτικό δίκτυο.

Οι περισσότερες εταιρείες που έχουν αυτό το πρόβλημα, βάζουν τους διακομιστές δικτύου στη Αποστρατικοποιημένη Ζώνη (DMZ), σε μια προσπάθεια τους να προστατέψουν το ιδιωτικό τους δίκτυο. Ένα DMZ, ενεργεί σαν το δικό του μικρό δίκτυο. Δημιουργείται όταν ο διακομιστής δικτύου μένει έξω από το ιδιωτικό δίκτυο, αλλά εξακολουθεί να είναι πίσω από το ηλεκτρονικό τείχος.

Η διαμόρφωση του DMZ χρησιμοποιεί ένα διακομιστή μεσολάβησης για να χωρίσει το δίκτυο σε δυο τελείως ξεχωριστά μέρη. Στο ένα μέρος υπάρχει το ιδιωτικό δίκτυο, που περιλαμβάνει όλους τους χρήστες και τις ιδιωτικές βάσεις δεδομένων. Στην άλλη πλευρά του δικτύου, κατευθείαν πίσω από το ηλεκτρονικό

τείχος, είναι οι διακομιστές δικτύου και μερικές φορές οι διακομιστές αλληλογραφίας. Σε αυτό το μοντέλο, όποιος θέλει πρόσβαση στο διακομιστή δικτύου, πρέπει να περάσει από το ηλεκτρονικό τείχος για να το κάνει. Ωστόσο, οι χρήστες που έχουν πρόσβαση στο διακομιστή δικτύου, εξακολουθούν να έχουν ελεύθερη πρόσβαση στο ιδιωτικό δίκτυο. Ο διακομιστής μεσολάβησης, σε αυτή τη περίπτωση ενεργεί σαν ένα άλλο μικρό ηλεκτρονικό τείχος, εντοπίζοντας ποίος και τι μπορεί να περάσει προς και από το ιδιωτικό δίκτυο.

Υπάρχουν μερικά σαφή πλεονεκτήματα στη διαμόρφωση της αποστρατικοποιημένης ζώνης. Πρώτα απ' όλα, το DZM ξεχωρίζει το ιδιωτικό δίκτυο από το Web διακομιστή, ενώ ο Web διακομιστής εξακολουθεί να έχει την ασφάλεια ενός ηλεκτρονικού τείχους. Το ηλεκτρονικό τείχος, φιλτράρει τις πληροφορίες που περνούν και αποφασίζει τι θα περάσει και τι όχι. Το δημόσιο δίκτυο ποτέ δεν συσχετίζεται με το Web διακομιστή, έτσι εάν υπάρχει κάποιο είδος εισβολής, το ιδιωτικό δίκτυο παραμένει ασφαλές. Τέλος, αυτή η διαμόρφωση βοηθά επίσης στην παρακολούθηση της εξωτερικής χρήσης του Web διακομιστή. Όλοι οι εσωτερικοί χρήστες θα πρέπει να περάσουν από το διακομιστή μεσολάβησης για έχουν πρόσβαση στο Web διακομιστή. Ο διακομιστής μεσολάβησης μπορεί να χρησιμοποιηθεί για την πιστοποίηση της πρόσβασης των εργαζομένων στο Διαδίκτυο.

Ένας Web διακομιστής μπορεί να διαμορφωθεί και να περιορίσει κάποιες συνδέσεις, σύμφωνα με προγραμματισμένες πληροφορίες. Ο διακομιστής μπορεί να προγραμματίσει να απορρίπτει τη σύνδεση ή να περιορίζει τη σύνδεση σε συγκεκριμένα αρχεία. Οι δύο βασικοί περιορισμοί είναι κανονικά οι περιορισμοί IP διεύθυνση ή ονόματος τομέα και οι περιορισμοί χρήστη και κωδικού πρόσβασης.

Συνήθως αυτά τα μέτρα ασφαλείας είναι αποτελεσματικά, επειδή δίνουν στον διαχειριστή του δικτύου περισσότερο έλεγχο πάνω στο διακομιστή δικτύου. Ο διακομιστής δεν μπορεί να προσπελαστεί ελεύθερα από οποιονδήποτε, εκτός και αν είναι «κλειδωμένος» από κάποιους περιορισμούς. Αν και οι περιορισμοί είναι ένας καλός τρόπος για τον έλεγχο της πρόσβασης και της κίνησης, δεν θα πρέπει να χρησιμοποιηθούν σαν η μόνη μέθοδος ασφαλείας, αφού ακόμα και αυτά τα μέτρα ασφαλείας μπορεί να υπερπηδηθούν.

Περιορισμοί IP Διεύθυνσης ή Τομέα. Οι περιορισμοί IP διεύθυνσης ή ονόματος τομέας είναι οι πιο συχνοί που χρησιμοποιούνται για να επιτρέψουν σε ένα χρήστη να συνδεθεί στο διακομιστή δικτύου. Αυτοί οι περιορισμοί διαμορφώνονται ώστε να μη επιτρέπουν συνδέσεις από κάποιες IP διευθύνσεις. Αυτός ο μηχανισμός περιορισμών δεν είναι μια πλήρης μέθοδος ασφαλείας, για διαφόρους λόγους. Πρώτα απ' όλα, ένας έμπειρος εισβολέας μπορεί να κάνει την IP διεύθυνση από την οποία έρχεται να φαίνεται στον διακομιστή σαν να είναι μια επιτρεπόμενη IP διεύθυνση. Αν κάποιος μπει με φυσικό τρόπο σε ένα PC που δεν είναι περιορισμένο, αυτό το άτομο μπορεί να φτάσει επίσης στο διακομιστή. Οι περιορισμοί μπορούν επίσης να καταλήξουν σε προβλήματα για τους χρήστες στους οποίους πραγματικά επιτρέπεται η πρόσβαση, εξαιτίας του τρόπου που θα εμφανίζονται οι IP διευθύνσεις τους αφού περάσουν μέσα από τον διακομιστή μεσολάβησης.

Περιορισμοί Ονόματος και Κωδικού Πρόσβασης. Μερικά αρχεία σε ένα διακομιστή δικτύου μπορεί να είναι περιορισμένα μέχρι οι χρήστες να δώσουν όνομα και κωδικό πρόσβασης. Για παράδειγμα, για να συνδεθεί κάποιος με μια Web τοποθεσία, αλλά και για να έχει τις πληροφορίες που θέλει θα πρέπει να εγγραφεί

για να γίνει μέλος. Με άλλα λόγια, έχουν διαμορφωθεί κλειδώματα σε κάποια αρχεία. Ο χρήστης θα πρέπει να δώσει στο διακομιστή προσωπικές πληροφορίες για να πάρει όνομα χρήστη και κωδικό πρόσβασης που θα του δώσει πρόσβαση. Ωστόσο, όπως και οι περιορισμοί από την IP διεύθυνση, οι περιορισμοί ονόματος και κωδικού πρόσβασης έχουν επίσης προβλήματα ασφαλείας. Ένα πρόβλημα που μειώνει την ασφάλεια είναι ότι υπάρχουν πραγματικά προγράμματα που μπορούν να βοηθήσουν να προσδιορίσετε τους κωδικούς πρόσβασης, κάνοντας εύκολο για ένα εισβολέα να βρει ένα κωδικό πρόσβασης και να αποκτήσει πρόσβαση. Πιο συχνά ωστόσο, οι κίνδυνοι ασφαλείας προκαλούνται από λάθη χρηστών. Οι περισσότεροι χρήστες χρησιμοποιούν κωδικούς πρόσβασης που είναι εύκολο να τους μαντέψει κάποιος, όπως τα ονόματα τους ή τις ημερομηνίες γέννησης τους. Επιπλέον χρησιμοποιούν συνήθως τους ίδιους κωδικούς πρόσβασης σε πολλές εφαρμογές, μερικές από τις οποίες είναι εύκολο να σπάσουν και προσδιορισθούν οι κωδικοί πρόσβασης. Τέλος, οι χρήστες γράφουν επίσης τους κωδικούς πρόσβασης και τους κολλάνε πάνω στα PC τους, κάνοντας πολύ εύκολη την εισβολή.

Διορθώσεις. Ανεξάρτητα από ποια μορφή επιλέγεται να έχει ο διακομιστής δικτύου, θα πρέπει να υπάρχουν και κενά ασφαλείας. Ανακαλύπτονται κάθε μέρα νέοι τρόποι εισβολής. Όταν εμφανίζονται αυτές οι νέες μέθοδοι εισβολής, οι εταιρείες που παράγουν προγράμματα για διακομιστές δικτύου, δημιουργούν μια γρήγορη διόρθωση. Τις περισσότερες φορές η διόρθωση είναι μια απλή γρήγορη προσθήκη στο πρόγραμμα και ονομάζεται hotfix. Οι διορθώσεις αυτές είναι μικρές και διορθώνουν συγκεκριμένα προβλήματα στο πρόγραμμα ασφαλείας. Αυτές συνήθως βρίσκονται σε μια Web σελίδα που τρέχει από τον κατασκευαστή του

προγράμματος και είναι ελεύθερα διαθέσιμες για μεταφορά. Οι διαχειριστές των δικτύων θα πρέπει να μαθαίνουν ότι υπάρχουν νεώτερες ενημερώσεις για το πρόγραμμα και ποια κενά διορθώνουν. **[7]**

Οι βασικές απαιτήσεις για την ασφαλή διεξαγωγή του Ηλεκτρονικού Εμπορίου είναι η εμπιστευτικότητα, η ακεραιότητα και ο έλεγχος αυθεντικότητας.

- **Εμπιστευτικότητα.** Εμπιστευτικότητα είναι απαραίτητο στοιχείο της ιδιωτικότητας του χρήστη καθώς και της προστασίας των μυστικών πληροφοριών. Η εμπιστευτικότητα είναι συνυφασμένη με την αποφυγή μη εξουσιοδοτημένης τροποποίησης μιας πληροφορίας και παρέχεται μέσω κρυπτογράφησης. Σ' ένα ηλεκτρονικό περιβάλλον θα πρέπει να υπάρχει η βεβαιότητα ότι το περιεχόμενο των μηνυμάτων που ανταλλάσσονται παραμένει αναλλοίωτο.
- **Ακεραιότητα.** Ακεραιότητα σημαίνει αποφυγή μη εξουσιοδοτημένης τροποποίησης των πληροφοριών που ανταλλάσσονται και παρέχεται μέσω ψηφιακής υπογραφής. Τα δεδομένα που αποστέλλονται ως μέρος της συναλλαγής πρέπει να είναι μη τροποποιήσιμα κατά τη διάρκεια της μεταφοράς και αποθήκευσης τους στο δίκτυο.
- **Έλεγχος αυθεντικότητας**. Η διαδικασία επαλήθευσης της ορθότητας του ισχυρισμού ενός χρήστη ότι κατέχει μια συγκεκριμένη ταυτότητα αλλά και η βεβαιότητα ότι το περιεχόμενο του μηνύματος παρέμεινε αναλλοίωτο κατά τη μεταφορά οριοθετούν την έννοια ελέγχου της αυθεντικότητας. Σύμφωνα με τον ορισμό η πιστοποίηση της ταυτότητας των επιχειρήσεων που συμμετέχουν σε μια συναλλαγή

είναι απαραίτητη ώστε, κάθε συναλλασσόμενο μέρος να μπορεί να πεισθεί για τη ταυτότητα του άλλου. Ο έλεγχος αυθεντικότητας παρέχεται μέσω ψηφιακής υπογραφής.

- **Εξουσιοδότηση.** Η εξουσιοδότηση αφορά την παραχώρηση δικαιωμάτων από τον ιδιοκτήτη στον χρήστη. Για παράδειγμα, ο πελάτης εξουσιοδοτεί τον έμπορο ώστε ο τελευταίος να ελέγξει αν ο αριθμός της πιστωτικής κάρτας είναι έγκυρος και εάν τα χρήματα στο λογαριασμό μπορούν να καλύψουν το ποσό των συναλλαγών.
- **Εξασφάλιση.** Η εμπιστοσύνη ότι κάποιος αντικειμενικός σκοπός ή απαίτηση επιτυγχάνονται. Για παράδειγμα, μια από τις απαιτήσεις του πελάτη είναι η βεβαιότητα ότι ο έμπορος με τον οποίο συναλλάσσεται είναι νόμιμος και έμπιστος.
- **Μη αποποίηση ευθύνης.** Κανένα από τα συναλλασσόμενα μέρη δεν πρέπει να έχει τη δυνατότητα να αρνηθεί τη συμμετοχή του σε μια συναλλαγή. **[1]**

Ένα δίκτυο μπορεί να χαλάσει σκόπιμα ή κατά λάθος, μέσα ή έξω. Για την αντιμετώπιση των κινδύνων, η ασφάλεια του δικτύου λειτουργεί σε δυο επίπεδα, στο επίπεδο βασισμένο στο χρήστη και στο επίπεδο ροής της κίνησης. Μια επιτυχημένη λύση ασφαλείας συνήθως χρησιμοποιεί ένα συνδυασμό ασφαλείας βασισμένη στο χρήστη και ασφαλείας βασισμένη στην κίνηση, για να ελέγχει το δίκτυο.

Η *ασφάλεια βασισμένη στην κίνηση* ομαλοποιεί τη ροή της κίνησης στο δίκτυο. Η βασική λειτουργία αυτού του επιπέδου είναι να σταματήσει τους εισβολείς έξω

από το δίκτυο που προσπαθούν να κερδίσουν πρόσβαση σ' αυτό, όπου θα μπορούσαν να έχουν πρόσβαση σε εμπιστευτικές πληροφορίες ή να χρησιμοποιήσουν το δίκτυο με ένα τρόπο που θα ήταν ενοχλητικός για την εταιρεία. Η *ασφάλεια σε επίπεδο κίνησης* μπορεί να χρησιμοποιηθεί σαν μια μορφή ελέγχου συντήρησης, επειδή ειδοποιεί τους διαχειριστές του δικτύου όταν συμβεί κάτι εξαιρετικό σε επίπεδο εφαρμογής.

Η *ασφάλεια βασισμένη στο χρήστη* είναι το επίπεδο ασφαλείας που ξέρουν οι χρήστες ότι υπάρχει. Είναι η ασφάλεια που εξαναγκάζει τους χρήστες να συνδέονται χρησιμοποιώντας όνομα και κωδικό πρόσβασης. Όσο παράξενο και αν φαίνεται, ένα δίκτυο θα πρέπει να προστατεύεται από τους χρήστες που δουλεύουν με αυτό καθημερινά. Αυτό σημαίνει ότι κάθε χρήστης πρέπει να έχει τη δυνατότητα να χρησιμοποιεί μόνο τους πόρους που οι καθημερινές διαδικασίες του χρήστη απαιτούν να χρησιμοποιεί.

Είναι δυνατόν εξωτερικοί χρήστες να έχουν πρόσβαση στο δίκτυο μιας εταιρείας χρησιμοποιώντας διάφορες μεθόδους επίθεσης. Αν όμως αποτύχει μια ασφάλεια επιπέδου κίνησης, ένας εισβολέας μπορεί να σταματήσει μέσα από την ασφάλεια την βασισμένη στο χρήστη. Αν ένας εισβολέας μπορεί να μπει μέσα στο δίκτυο της εταιρείας, αυτός ο εισβολέας δεν θα μπορέσει να ταξιδέψει ελεύθερα μέσα στο δίκτυο. Η ασφάλεια η βασισμένη στο χρήστη είναι επίσης σημαντική για τη βασική διαχείριση ενός δικτύου. Παρέχει στους διαχειριστές δικτύου ένα τρόπο να ελέγχουν τι μπορεί να κάνει κάθε χρήστης, χωρίς να στέκονται πίσω από τους χρήστες και να παρατηρούν τι κάνουν. Με την ασφάλεια τη βασισμένη στο χρήστη, κάθε χρήστης προσδιορίζεται ξεχωριστά, πιστοποιείται και ελέγχεται. Για παράδειγμα κάθε χρήστης έχει ένα κωδικό πρόσβασης που συνδέεται με το όνομα

χρήστη του. Το όνομα χρήστη και ο κωδικός πρόσβασης πρέπει να δίνονται σωστά, για να γίνει μία έγκυρη σύνδεση. Αφού γίνει αυτή η σύνδεση, ο χρήστης έχει περιορισμένα δικαιώματα. Η διαδικασία της ασφαλείας χρήστη, που συνδέει το όνομα χρήστη με τον κωδικό πρόσβασης και επιτρέπει σε ένα χρήστη πρόσβαση στο δίκτυο ονομάζεται έλεγχος ταυτότητας, εκχώρηση δικαιωμάτων και λογαριασμοί (authentication, authorization, accounting – AAA).

- Έλεγχος Ταυτότητας

Στο Διαδίκτυο, μπορεί να πει κάποιος ότι είναι ο πρόεδρος των ΗΠΑ και κανείς δεν μπορεί να αποδείξει ότι δεν είναι. Στη διάρκεια της κανονικής περιήγησης στο Web αυτό δεν είναι πολύ σπουδαίο, αλλά όταν έρχεται η στιγμή για να αλλάξουν χέρια κάποια χρήματα, είναι σαφές η ανάγκη γνώσης του άλλου προσώπου. Εδώ βοηθάει ο έλεγχος ταυτότητας.

Ο έλεγχος ταυτότητας είναι μια διαδικασία πιστοποίησης του χρήστη που ζητά πρόσβαση στο δίκτυο και αποφασίζει αν αυτός ο χρήστης θα πρέπει να έχει πρόσβαση. Κάθε χρήστης έχει μοναδικό όνομα χρήστη και κωδικό πρόσβασης. Όταν ο χρήστης δώσει σωστό το όνομα χρήστη και τον κωδικό πρόσβασης, πιστοποιείται και ο χρήστης έχει πλέον πρόσβαση στο δίκτυο. Αυτό το μέτρο ασφαλείας εξαναγκάζει όποιον θέλει πρόσβαση στο δίκτυο, να ξέρει ένα συγκεκριμένο όνομα χρήστη και κωδικό πρόσβασης.

- Εκχώρηση Δικαιωμάτων

Η εκχώρηση δικαιωμάτων είναι μία λίστα από άδειες που δίνονται σε ένα χρήστη για να έχει πρόσβαση σε μία συγκεκριμένη εφαρμογή του δικτύου. Επειδή

αυτή κατανέμεται ως προς το όνομα χρήστη, δεν έχουν όλοι οι χρήστες την ίδια πρόσβαση σε όλες τις εφαρμογές. Αυτός ο περιορισμός βοηθά να ασφαλίζετε το δίκτυο από εξωτερικούς χρήστες. Κρατά επίσης τους χρήστες έξω από εφαρμογές που δεν θα πρέπει να χρησιμοποιούν, ώστε να μη χαλάσουν το δίκτυο.

- Λογαριασμοί

Οι λογαριασμοί είναι ένα τμήμα που διατηρεί εγγραφές για την ασφάλεια την βασισμένη στο χρήστη. Οι λογαριασμοί παρακολουθούν από που είναι συνδεδεμένος ο κάθε ένας και για πόσο. Χρησιμοποιώντας αυτές τις καταγραφές, οι διαχειριστές των δικτύων μπορούν να παρακολουθούν τους χρήστες και τι κάνουν όταν συνδέονται στο δίκτυο. Αυτό το σύστημα παρακολούθησης παρέχει στους διαχειριστές μια ιδέα περί του τι κάνουν οι εργαζόμενοι και για πόσο χρόνο. Χρησιμοποιείται επίσης σαν ένας μηχανισμός ειδοποίησης προς τον διαχειριστή του δικτύου για ένα εισβολέα, που μπορεί να χρησιμοποιήσει τις δυνατότητες παρακολούθησης για να εντοπίσει κάποια ύποπτη συμπεριφορά.

Το ΑΑΑ παρέχει μια σπουδαία πηγή για ασφάλεια δικτύων. Ωστόσο, επειδή η ασφάλεια βασίζεται στο χρήστη, όταν χρησιμοποιείται σαν μόνη μορφή ασφαλείας, είναι πολύ περιορισμένη. Αν ένας εισβολέας έχει το όνομα του χρήστη και κωδικό πρόσβασης ενός χρήστη, αυτός ο εισβολέας μπορεί να περάσει ελεύθερα σε ολόκληρο το σύστημα.

Στη συνέχεια μετά την αναφορά στις επιθέσεις που μπορούν να γίνουν σε ένα δίκτυο είναι σαφές γιατί απαιτείται ασφάλεια. Ο κύριος στόχος της πολιτικής ασφαλείας είναι η παρακολούθηση και ο έλεγχος της χρήσης του δικτύου. Είναι σημαντικό να διατηρείται η ισορροπία, όταν δημιουργείται αυτή η πολιτική. Ένας

καλός τρόπος για να υπάρχει ισορροπία της ασφάλειας είναι με τη στρατηγική τοποθέτηση συστημάτων ασφαλείας σε διαφορετικές θέσεις του δικτύου. Ορίζοντας συγκεκριμένες θέσεις μπορεί να μπει η ασφάλεια σε επίπεδα. Ορίζονται συνήθως τρία σημεία του δικτύου σαν πιθανές θέσεις μέτρων ασφαλείας: η εξωτερική περίμετρος, η εσωτερική περίμετρος και η εσώτερη περίμετρος. Αυτά τα όρια ενεργούν σαν φανταστικές γραμμές που χωρίζουν το δίκτυο.

Εξωτερική περίμετρος

Η εξωτερική περίμετρος είναι η γραμμή μεταξύ του δικτύου της εταιρείας και του εξωτερικού κόσμου. Συνήθως, αυτό το σημείο είναι ένας δρομολογητής ή κάποιες συσκευές, όπως ένα ηλεκτρονικό τείχος, που συνδέουν το δίκτυο με το Διαδίκτυο. Το πιο σημαντικό σε αυτή τη θέση είναι ότι η εταιρεία ελέγχει τα πάντα που βρίσκονται στη πλευρά του δικτύου αλλά όχι πέρα απ' αυτό το σημείο. Η εξωτερική περίμετρος είναι μια προφανή θέση ασφαλείας, αφού είναι η πιο πιθανή περιοχή να γίνει επίθεση.

Εσωτερικοί Περίμετροι

Οι εσωτερικές περίμετροι ορίζονται από τις θέσεις στις οποίες το δίκτυο έχει μέτρα ασφαλείας. Για παράδειγμα, τα ηλεκτρονικά τείχη ή οι δρομολογητές που βρίσκονται μέσα στο δίκτυο ή που ενεργούν σαν όρια μεταξύ του εξωτερικού και του εσωτερικού του δικτύου, είναι οι εσωτερικές περίμετροι. Η ασφάλεια σε αυτή τη θέση δουλεύει για να ταξινομεί δεδομένα και να τα κατευθύνει εκεί που πρέπει να πάνε. Οι δρομολογητές συνήθως χρησιμοποιούνται σε αυτά τα σημεία για να κατευθύνουν την κίνηση του δικτύου. Αυτή η ασφάλεια είναι πιο επικεντρωμένη σε

εσωτερικές σχέσεις παρά σε εξωτερικές επιθέσεις αν και είναι ένα καλό σημείο ελέγχου του δικτύου για τον έλεγχο περίεργης συμπεριφοράς.

Εσώτερη Περίμετρος

Η εσώτερη περίμετρος είναι η καρδιά του δικτύου, το μέρος όπου οι χρήστες συνδιαλέγονται μαζί του σε καθημερινή βάση. Αυτή είναι η θέση ασφαλείας της βασισμένης στο χρήστη, που βεβαιώνει ότι οι χρήστες είναι αξιόπιστα μέλη της εταιρείας και προσπελαύνουν μόνο τις πληροφορίες που πρέπει. **[7]**

Αφού ενεργοποιηθεί η ασφάλεια στον Web διακομιστή, θα πρέπει να ενεργοποιηθεί και η ασφάλεια στις συναλλαγές που γίνονται μεταξύ του Web διακομιστή και των άλλων PC που είναι συνδεδεμένα στο Διαδίκτυο.

Η ασφάλεια του Διαδικτυακού πρωτοκόλλου ή IPSec είναι η βάση για την ασφάλεια των διαδικτυακών συναλλαγών, γιατί ο χειρισμός τους γίνεται σε επίπεδο πρωτοκόλλου. Είναι το IPSec που βεβαιώνει ότι είναι ασφαλείς οι συναλλαγές προς και από το Web διακομιστή. Το IPSec λειτουργεί κλείνοντας το πακέτο των πληροφοριών το οποίο στέλνεται σε ένα άλλο πακέτο, πριν σταλεί μέσω του Διαδικτύου. Στο παραλήπτη το πακέτο αποκωδικοποιείται και διαβάζεται από μια συσκευή που έχει καθορίσει ο αποστολέας.

Το IPSec αποτελείται από τρεις διαφορετικούς μηχανισμούς ασφαλείας: την επικεφαλίδα ελέγχου ταυτότητας, το ωφέλιμο φορτίο συμπυκνωμένης ασφαλείας και το πρωτόκολλο διαχείρισης κλειδιού Internet.

Είναι το IPSec όπως το PKI στο τρόπο που ορίζει την εμπιστοσύνη μεταξύ διαφορετικών πλευρών. Σαν καθολική βάση, το παρέχει τρεις σημαντικές

λειτουργίες ασφαλείας για διαδικτυακές συναλλαγές: εμπιστοσύνη, ακεραιότητα και έλεγχος ταυτότητας.

Αν το IPSec φαίνεται πολύ παρόμοιο με τη προσέγγιση PKI, υπάρχει μια πολύ βασική διαφορά. Τα άλλα μέτρα ασφαλείας συναλλαγών λειτουργούν σε επίπεδο εφαρμογής, ενώ το IPSec λειτουργεί σε επίπεδο πρωτοκόλλου. Αυτό κάνει το IPSec ευκολότερο στη χρήση, επειδή οι εφαρμογές των δυο πλευρών που επικοινωνούν δεν χρειάζεται να είναι συμβατές. Επιπλέον το IPSec επιτρέπει στους χρήστες να πιστοποιούν και να επικοινωνούν μέσω μιας σύνδεσης, αντί να επικοινωνούν με μηνύματα. Το IPSec είναι ένα θαυμάσιο μέτρο ασφαλείας για μηνύματα ηλεκτρονικού ταχυδρομείου. Το IPSec είναι πιο κατάλληλο για χρήση στο Διαδίκτυο.

Γ.2 ΜΗΧΑΝΙΣΜΟΙ ΑΣΦΑΛΕΙΑΣ

Οι μηχανισμοί ασφαλείας μέσω των οποίων εκπληρώνονται οι προαναφερθείσες απαιτήσεις παρουσιάζονται στη συνέχεια:

Κρυπτογράφηση

Από τη στιγμή που άρχισαν να μεταφέρονται πληροφορίες, ξεκίνησε και η ιδέα της κρυπτογράφησης ή του κώδικα για να ασφαλιστούν τα μηνύματα. Αν το μήνυμα είναι γραμμένο σε κώδικα, είναι ασφαλές ακόμα και αν υποκλαπεί. Οι άνθρωποι στη διάρκεια των αιώνων ξέρουν και βασίζονται σε αυτό το γεγονός.

Το παρόν σύστημα αποστολής ασφαλών μηνυμάτων μέσω του Διαδικτύου βασίζεται στην ίδια γενική ιδέα κρυπτογράφησης που έχει χρησιμοποιηθεί για αιώνες, με μια βασική βελτίωση.

Η διαφορά μεταξύ των προηγούμενων και των τωρινών μορφών κρυπτογράφησης βρίσκεται στο κλειδί που αποκρυπτογραφεί τον κώδικα. Στο παρελθόν, ο παραλήπτης για να μπορεί να επαναφέρει το μήνυμα ξανά σε αναγνώσιμη μορφή, χρειαζόταν το κλειδί του μυστικού κώδικα. Το σύστημα δούλευε θαυμάσια τις περισσότερες φορές, επειδή σε κάποιο σημείο τα δυο μέρη συναντιόντουσαν προσωπικά και μπορούσαν να ανταλλάξουν το κώδικα, ώστε να είναι σίγουρο ότι θα είναι μυστικός. Αν μια προσωπική συνάντηση δεν είναι δυνατή, τα δυο μέρη έχουν τον κίνδυνο να υποκλαπεί ο μυστικός κώδικας και να αντιγραφεί.

Ωστόσο στις συναλλαγές μέσω του Διαδικτύου δεν βλέπετε το πρόσωπο του άλλου ατόμου. Το μυστικό κλειδί θα μπορούσε να σταλεί με την ίδια μέθοδο, όπως το μήνυμα που θέλετε να στείλετε κρυπτογραφημένο. Αν υπήρχε ο κίνδυνος να υποκλαπεί και να διαβαστεί το αρχικό μήνυμα, προφανώς θα υπήρχε η αίσθηση μιας μη ασφαλής επικοινωνίας ή δεν θα γινόταν χρήση καθόλου της κρυπτογράφησης. Σε σχέση με το Διαδίκτυο χρειάζεται ένα διαφορετικό σύστημα κρυπτογράφησης.

Κρυπτογραφικός κώδικας ή κρυπτογραφικός αλγόριθμος είναι ένα πρόγραμμα Η/Υ το οποίο παίρνει ένα κείμενο κατανοητό απ' όλους και το μετατρέπει σε ένα άλλο κείμενο κατανοητό μόνο σε αυτούς που γνωρίζουν το τρόπο να το διαβάσουν. Για να λειτουργήσει αυτός ο αλγόριθμος χρειάζεται μια ή περισσότερες κλείδες. Η κλείδα είναι το στοιχείο εκείνο που ελέγχει τη λειτουργία του αλγόριθμου. Ένα **κρυπτογραφημένο σύστημα** είναι ένα σύνολο από διαδικασίες, Η/Υ κλπ. που χρησιμοποιεί, μεταξύ άλλων, έναν ή περισσότερους

κρυπτογραφικούς κώδικες για να λύσει διάφορα συστήματα ασφαλείας ενός γενικότερου συστήματος τηλεπικοινωνιών ή διαχείρισης δεδομένων.

Ένας τρόπος να κατηγοριοποιηθούν οι κρυπτογραφικοί κώδικες είναι με βάση το είδος κλειδιού. Υπάρχουν κώδικες με συμμετρική κλείδα και περίπτωση όπου είναι αδύνατος ο υπολογισμός της μίας κλείδας από την άλλη.

- *Συμμετρική κρυπτογράφηση (Symmetric key encryption).* Η κρυπτογράφηση ιδιωτικού κλειδιού ή συμμετρική κρυπτογράφηση βασίζεται σε ένα κοινό κλειδί το οποίο διαμοιράζεται μεταξύ των συναλλασσομένων μερών. Το κλειδί αυτό χρησιμοποιείται τόσο για την κρυπτογράφηση όσο και για την αποκρυπτογράφηση των μηνυμάτων. Γίνεται χρήση του αλγόριθμου DES – Data Encryption Standard. Το βασικό πρόβλημα της κρυπτογράφησης του τύπου αυτού αφορά τη δημιουργία, την αποθήκευση, και τη μετάδοση του μυστικού κλειδιού. Συγκεκριμένα:
  - Και τα δύο συναλλασσόμενα μέρη θα πρέπει να συμφωνήσουν για ένα κοινό μυστικό κλειδί.
  - Κάθε χρήστης θα πρέπει να έχει τόσα μυστικά κλειδιά όσα και τα μέλη με τα οποία συναλλάσσεται.
  - Δεν ικανοποιείται η απαίτηση για αυθεντικότητα, γιατί δεν μπορεί να αποδειχθεί η ταυτότητα των συναλλασσόμενων μέρων. Από την στιγμή που δύο άτομα κατέχουν το ίδιο κλειδί, τότε και οι δυο μπορούν να κρυπτογραφήσουν κάποιο μήνυμα και να ισχυριστούν ότι το έστειλε το άτομο. Κατά συνέπεια, η μη αποποίηση της ευθύνης για την αποστολή ενός μηνύματος καθίσταται και αυτή αδύνατη. Το πρόβλημα αυτό επιλύεται με τη κρυπτογράφηση δημοσίου κλειδιού ή ασύμμετρη κρυπτογράφηση.

v *Ασύμμετρη κρυπτογράφηση (Asymmetric Key encryption).* Η βάση του PKI είναι μια τεχνολογία που ονομάζεται κρυπτογράφηση δημοσίου κλειδιού. Η κρυπτογράφηση δημοσίου κλειδιού (public key cryptography), είναι η τεχνολογική λύση στο πρόβλημα που δημιουργείται από τα άτομα που υποκλέπτουν τα εμπιστευτικά μηνύματα που στέλνονται μέσω του Διαδικτύου. Είναι ένας μαθηματικός μυστικός κώδικας με τον οποίο κάθε γράμμα αλλάζει σε ένα διαφορετικό γράμμα, αριθμό, σύμβολο δημιουργώντας μια σελίδα που δεν έχει έννοια, ώστε το μήνυμα να μη μπορεί να διαβαστεί, ακόμα και αν υποκλαπεί. Βασίζεται σε ένα ζεύγος κλειδιών εκ των οποίων το ένα είναι δημόσια γνωστό, ενώ το άλλο είναι ιδιωτικό. Στην κρυπτογράφηση δημοσίου κλειδιού οτιδήποτε κρυπτογραφείται με το ένα κλειδί μπορεί να αποκρυπτογραφηθεί χρησιμοποιώντας μόνο το άλλο κλειδί. Το κύριο πλεονέκτημα που προσφέρει η κρυπτογράφηση δημοσίου κλειδιού είναι η αυξημένη ασφάλεια που παρέχει. Η κρυπτογράφηση δημοσίου κλειδιού θεωρείται κατάλληλη για το Ηλεκτρονικό Εμπόριο για τους εξής λόγους:

- Εξασφαλίζει την εμπιστευτικότητα του μηνύματος.
- Παρέχει πιο ευέλικτα μέσα αυθεντικοποίησης των χρηστών.
- Υποστηρίζει ψηφιακές υπογραφές (ακεραιότητα μηνύματος).

Τα δύο αυτά κλειδιά μπορούν να χρησιμοποιηθούν με δύο διαφορετικούς τρόπους: να εξασφαλίσουν την εμπιστευτικότητα του μηνύματος και να αποδείξουν την αυθεντικότητα του δημιουργού του.

Στην πρώτη περίπτωση, για την παραγωγή ενός εμπιστευτικού μηνύματος, ο αποστολέας χρησιμοποιεί το δημόσιο κλειδί του παραλήπτη για να

κρυπτογραφήσει το μήνυμα, έτσι ώστε να παραμείνει απόρρητο έως ότου αποκρυπτογραφηθεί από το ιδιωτικό κλειδί του παραλήπτη.

Στη δεύτερη περίπτωση, ο αποστολέας κωδικοποιεί ένα μήνυμα με το ιδιωτικό του κλειδί, το οποίο είναι απόρρητο. Το ιδιωτικό κλειδί αποδεικνύει την ταυτότητα του χρήστη (αυθεντικοποίηση). Δηλαδή, η χρήση ιδιωτικού κλειδιού για την κρυπτογράφηση ενός μηνύματος είναι αντίστοιχη με την προσθήκη της υπογραφής του αποστολέα σε κάποιο έγγραφο. Έτσι λοιπόν οποιοσδήποτε χρησιμοποιήσει το δημόσιο κλειδί του αποστολέα για να αποκρυπτογραφήσει το μήνυμα θα είναι σίγουρος για την ταυτότητα του πρώτου.

Το PKI έχει επίσης μια επιλογή που μπορεί να αποδείξει ότι ένα μήνυμα έχει δημιουργηθεί μια συγκεκριμένη ημέρα και ώρα. Αυτή η λειτουργία ονομάζεται ψηφιακή σφραγίδα. Συνήθως σε επαγγελματικές συναλλαγές είναι σημαντικό να δείξετε ότι τα μηνύματα ή οι σημειώσεις δημιουργήθηκαν και στάλθηκαν ένα συγκεκριμένο χρόνο. Ο ευκολότερος τρόπος είναι να σταλεί ένα αντίγραφο του μηνύματος, σε μη αναγνώσιμη μορφή στη CA (Certification Authority). Η CA μπορεί να στείλει μετά ένα αντίγραφο του μηνύματος στους παραλήπτες του μηνύματος. Η CA θα στείλει επίσης ένα πιστοποιητικό που λέει ότι έλαβαν αυτό το μήνυμα την ‘τάδε’ ημερομηνία και ‘τάδε’ ώρα.

Η κρυπτογράφηση είναι μια θαυμάσια εξέλιξη στην επικοινωνία ασφαλείας μέσω του Διαδικτύου. Ωστόσο, επειδή είναι σχετικά νέα ιδέα, υπάρχουν μερικά λάθη όπως, η κρυπτογράφηση ενός μηνύματος με ένα δημόσιο κλειδί χρειάζεται περισσότερο χρόνο παρά με ένα μυστικό κωδικό, επειδή οι αλγόριθμοι είναι πολύ πιο περίπλοκοι για να αποκρυπτογραφηθούν.

Εξ αιτίας του χρόνου που απαιτείται για την κρυπτογράφηση και την αποκρυπτογράφηση ενός μηνύματος έχει ξεκινήσει μια εναλλακτική πρακτική όπου κάποιος κωδικοποιεί το μήνυμα με ένα μυστικό κώδικα και μετά στέλνει το μυστικό κώδικα κρυπτογραφημένο με ένα δημόσιο κλειδί. Ο ίδιος ο μυστικός κωδικός χρειάζεται συνήθως λιγότερο χρόνο να αποκρυπτογραφηθεί. **[7]**

Απόκρυψη

Η απόκρυψη είναι η ευκολότερη και λιγότερη ακριβή άμυνα εναντίον επιθέσεων εισβολής και πιθανώς η ευκολότερη τεχνική για τα μικρά γραφεία και σπίτια.

Μπορούμε να κρύψουμε τον εαυτό μας στο Διαδίκτυο μέσω μιας τεχνικής που λέγεται Παράφραση της Διεύθυνσης Δικτύου (Network Address Translation) ή NAT. Η NAT, είναι διαθέσιμη σε κάθε ηλεκτρονικό τείχος καθώς ακόμα και στις λιγότερο εξελιγμένες πύλες δικτύου που έχουν σα στόχο τα σπίτια και τα μικρά γραφεία. Καμουφλάροντας τους υπολογιστές που είναι σε δίκτυο με διευθύνσεις IP, οι κακοί δεν μπορούν να δουν από το Διαδίκτυο. Μια συσκευή NAT παραφράζει τις ασφαλείς διευθύνσεις του τοπικού δικτύου με τις δικές της μόνιμες διευθύνσεις. Σαν ένα μόνιμο προνόμιο, το NAT εξαφανίζει τους μπελάδες με τις IP διευθύνσεις που πολλές επιχειρήσεις αντιμετωπίζουν όταν προσπαθούν να χρησιμοποιήσουν ένα μπλοκ από δρομολογήσιμες διευθύνσεις που έχουν δοθεί από τον ISP. Το NAT είναι εύκολο στη χρήση και αποτελεσματικό εναντίον των περισσότερων απειλών εισβολής. Ωστόσο, δεν μπορεί να σας βοηθήσει εναντίον επιθέσεων απαγόρευσης της εξυπηρέτησης ή εξεζητημένων επιθέσεων εισβολής. **[2]**

Ηλεκτρονικό τείχος - Firewall

Η εναλλακτική άμυνα είναι να χτίσετε ένα τείχος να προστατεύσει το δίκτυο σας. Ένα ηλεκτρονικό τείχος είναι ένα πρόγραμμα που δημιουργεί τα όρια μεταξύ δικτύων. Είναι τα προγράμματα που χειρίζονται την ασφάλεια την βασισμένη στη κίνηση. Οι συσκευές που καλούνται ηλεκτρονικά τείχη (firewalls) χρησιμοποιούν αρκετές τεχνικές για να αναγνωρίσουν, ελέγξουν και να φιλτράρουν τα πακέτα που μπαίνουν ή βγαίνουν από ένα δίκτυο. Η εγκατάσταση και συντήρηση ενός ηλεκτρονικού τείχους χρειάζεται κάποια ειδίκευση, έτσι μπορεί να χρειαστεί η βοήθεια ενός μεταπωλητή προστιθέμενης αξίας. Υπάρχουν τέσσερα είδη firewall, και η επιλογή του εξαρτάται από την ισορροπία που είναι επιθυμητή μεταξύ ασφάλειας και πρόσβασης.

- Ηλεκτρονικό τείχος φίλτρου πακέτων

Εξετάζει την κίνηση του δικτύου σε επίπεδο πακέτου. Ένα πακέτο στέλνεται στο δίκτυο, εξετάζεται προσεκτικά και είτε επιτρέπεται να περάσει είτε απορρίπτεται σύμφωνα με τους γενικούς κανόνες και κανονισμούς που έχουν προγραμματίσει στο ηλεκτρονικό τείχος (firewall). Το φιλτράρισμα των πακέτων διευθύνσεων που γίνεται από τους δρομολογητές, ελέγχει για τη νομιμότητα των εισερχόμενων και εξερχόμενων διευθύνσεων IP. Μια πιο εξεζητημένη εφαρμογή διαμεσολαβητή ηλεκτρονικού τείχους τοποθετεί τον εαυτό της μέσα στην συναλλαγή μεταξύ των προγραμμάτων πελάτη και διακομιστή και παρακολουθεί για αντικανονικές αιτήσεις.

Αυτό το ηλεκτρονικό τείχος είναι ιδανικό για μικρές ανάγκες ασφαλείας, επειδή είναι γρήγορο και εύκολο στη διαχείριση. Επειδή η επεξεργασία της κίνησης γίνεται σε επίπεδο πακέτου, η επεξεργασία γίνεται γρήγορα. Επίσης το σύστημα αυτό κρύβει τις εσωτερικές IP διευθύνσεις. Όμως αυτό το ηλεκτρονικό τείχος δεν είναι το

πιο ασφαλές, διότι δεν έχει τη δυνατότητα να χειρίζεται πληροφορίες επειδή λειτουργεί σε επίπεδο πακέτου. Επιπλέον δεν παρακολουθεί τι γίνεται μέσα και έξω και είναι δύσκολο να παρακολουθήσει τα πιθανά προβλήματα.

- Ηλεκτρονικό τείχος επιπέδου κυκλώματος

Διαβάζει τις πληροφορίες σε επίπεδο πακέτου. Όπως και το ηλεκτρονικό τείχος φίλτρο πακέτου, έτσι και το ηλεκτρονικό τείχος επιπέδου κυκλώματος εξετάζει κάθε πακέτο και αποφασίζει αν θα δεχτεί ή θα απορρίψει το πακέτο σε σχέση με ένα σύνολο από στόχους. Αν το πακέτο σύνδεσης ανταποκρίνεται σε όλα τα έγκυρα κριτήρια σύνδεσης, η σύνδεση γίνεται αποδεκτή. Αν όχι το πακέτο απορρίπτεται και η σύνδεση δε γίνεται.

Το μεγαλύτερο πλεονέκτημα του είναι η ταχύτητα του. Μπορεί να προστατεύσει ολόκληρο το δίκτυο, επειδή θα απορρίψει μια ολόκληρη σύνδεση αν βρει ότι έχει πρόβλημα. Κάνει επίσης τα εξερχόμενα πακέτα να φαίνονται ότι έχουν δημιουργηθεί στο ηλεκτρονικό τείχος (firewall) αντί σε μια εσωτερική πηγή, έτσι κρύβεται η IP διεύθυνση προέλευσης. Αυτός ο μηχανισμός απόκρυψης, που αναφέρεται σαν NAT, μεταφράζει τις IP διευθύνσεις από την ιδιωτική διεύθυνση, σε IP διευθύνσεις που δεν θα αγνοηθούν από το Διαδίκτυο.

- Ηλεκτρονικό τείχος επιπέδου εφαρμογής

Τα ηλεκτρονικά τείχη (firewall) αυτής της γενιάς εκτιμούν τα πακέτα σε επίπεδο εφαρμογής, παρακολουθεί όλες τις πληροφορίες σύνδεσης και έχει τη δυνατότητα να χειρίζεται δεδομένα ώστε να δίνει άδεια στο πακέτο. Περιέχουν υπηρεσίες μεσολάβησης σαν μέρος της ασφάλειας τους. Αυτά τα προγράμματα ενεργούν σαν μια διασύνδεση μεταξύ των εσωτερικών δικτύων και του εξωτερικού Διαδικτύου.

Επειδή αυτό το ηλεκτρονικό τείχος δουλεύει σε επίπεδο εφαρμογής, μπορεί να χειρίζεται περιεχόμενα πακέτων. Κρατά μια λεπτομερή εγγραφή για το ποιες πληροφορίες περνούν μέσα από τους διακομιστές μεσολάβησης, ώστε οι διαχειριστές του δικτύου να μπορούν να παρακολουθούν τους πιθανούς κινδύνους ασφαλείας. Είναι το πιο αργό από όλα τα ηλεκτρονικά τείχη (firewall) εξαιτίας των περίπλοκων διαδικασιών με τις οποίες ελέγχουν τα δεδομένα. Το μειονέκτημα του είναι η πίεση που ασκείται στα άτομα που χρησιμοποιούν και συντηρούν αυτό το δίκτυο.

- Δυναμικά Φίλτρα Πακέτων

Αυτό το ηλεκτρονικό τείχος (firewall) είναι παρόμοιο με το firewall φίλτρο πακέτου, με την αξιοσημείωτη εξαίρεση ότι ο διαχειριστής του δικτύου μπορεί να αλλάξει τους κανόνες αποδοχής / απόρριψης οποιαδήποτε στιγμή. Ξέρει επίσης από που ξεκίνησαν τα πακέτα και θα δεχτεί την απόκριση από πακέτα που στέλνονται ξανά στην ίδια διεύθυνση.

Αυτό το ηλεκτρονικό τείχος παρέχει περιορισμένη ασφάλεια. Είναι γρήγορο και έχει το επιπλέον πλεονέκτημα ότι επιτρέπει μια απόκριση, ακόμα και από ένα μη αξιόπιστο δίκτυο.

Τα σημαντικά πράγματα που παρέχουν τα συστήματα ηλεκτρονικού τείχους είναι η αποτελεσματικότητα, η οικονομική ανεκτικότητα και τη διαθεσιμότητα άλλων χαρακτηριστικών.

Ένα πραγματικό ηλεκτρονικό τείχος θα έπρεπε να μη επιτρέπει πρόσβαση σε κανένα PC ή υπηρεσία που τρέχει σε τοπικό δίκτυο. Άλλα αυτό δεν είναι πάντα εφικτό αν υπάρχει ηλεκτρονικό ταχυδρομείο, Web, ή ένα διακομιστή FTP για εξωτερική πρόσβαση. Υπάρχουν δυο βασικοί τρόποι για να ανοιχτεί το δίκτυο και

παρόλα αυτά να παραμείνει ασφαλές: Ή χρήση αποστρατικοποιημένης ζώνης ή χρήση φιλτραρίσματος.

Μια αποστρατικοποιημένη ζώνη είναι ένα κομμάτι ανάμεσα στη σύνδεση με το Διαδίκτυο και το τοπικό δίκτυο όπου θα τοποθετηθεί το ηλεκτρονικό τείχος. Ένα απομονωμένο δίκτυο, πίσω από το ηλεκτρονικό τείχος ακόμα και ξεχωριστά από το τοπικό δίκτυο. Οι συσκευές που απαιτούν κάποια δημόσια πρόσβαση περνούν μέσα από την αποστρατικοποιημένη ζώνη. **[7]**

Φίλτρα περιεχομένου

Οι περισσότεροι άνθρωποι βλέπουν το ηλεκτρονικό τείχος σαν το εργαλείο που θα αποτρέψει την εξωτερική πρόσβαση στο τοπικό σας δίκτυο, αλλά επίσης να χρησιμεύει για να ελέγξετε τι προσπελαύνουν οι χρήστες σας το Διαδίκτυο. Τα περισσότερα προϊόντα ηλεκτρονικού τείχους περιέχουν αυτό που λέγεται φιλτράρισμα ή χαρακτηριστικά φιλτραρίσματος περιεχομένου. Αυτά τα χαρακτηριστικά περιέχουν μια άλλη άποψη της ασφάλειας: ελευθερία από παρενοχλήσεις και περισπασμό.

Για τις εταιρείες που σκέφτονται ότι πρέπει να περιορίσουν τους υπαλλήλους τους από τη σχεδίαση ταξιδιών ή τον έλεγχο του χαρτοφυλακίου τους, τα προϊόντα φιλτραρίσματος περιλαμβάνουν δυνατότητες που μπλοκάρουν τέτοιου τύπου δραστηριότητες. Αυτά τα λεγόμενα φίλτρα παραγωγικότητας μπορούν να καταστρέψουν ιστοσελίδες ταξιδιών, σπορ και λόγου, για να επιτρέψουν στις εταιρείες να αποφασίσουν μόνες τους πια εξερεύνηση είναι χρήσιμη και πια δεν είναι.

Εικονικό Ιδιωτικό Δίκτυο

Μια εταιρεία επιθυμεί οι υπάλληλοι της και οι επιχειρηματικοί της συνεργάτες να χρησιμοποιούν την εταιρική τους πύλη και να έχουν πρόσβαση στις εφαρμογές παραγωγικότητας αλλά πώς θα το πετύχουν αυτό ανεξάρτητα από τη τοποθεσία τους; Ένα εικονικό ιδιωτικό δίκτυο (virtual private network-VPN) είναι η απάντηση στη παροχή ασφαλούς και ευέλικτης πρόσβασης για υπαλλήλους που ταξιδεύουν και για αυτούς που δουλεύουν από το σπίτι. Επίσης λειτουργεί και για την ασφαλή σύνδεση μεταξύ των γραφείων. Το εικονικό ιδιωτικό δίκτυο είναι ένας τρόπος για να δημιουργηθεί μια ασφαλή σύνδεση διαμέσου ενός ιδιωτικού δικτύου ή του Διαδικτύου έτσι ώστε οι εξουσιοδοτημένοι χρήστες να μπορούν να προσεγγίσουν τις πηγές της εταιρείας από οπουδήποτε. Τα VPNs γίνονται ολοένα και περισσότερο σημαντικά καθώς οι υπάλληλοι αποκτούν γρήγορη πρόσβαση στο Διαδίκτυο μέσω καλωδιακών διαμορφωτών – αποδιαμορφωτών (modem) και συνδέσεων DHL. **[7]**

Προστασία από Ιούς

Τα εργαλεία προστασίας εναντίον των ιών είναι η καλύτερη προστασία εναντίον αυτών των προγραμμάτων. Αυτά τα αντιβιοτικά προγράμματα μπορούν να αγοραστούν απ' ευθείας και εκτός σύνδεσης και να εγκατασταθούν κατευθείαν σε υπολογιστές ή διακομιστές. Τα προγράμματα προστασίας σαρώνουν το σύστημα ψάχνοντας και μετά καταστρέφοντας, προγραμματισμένες απειλές πριν δημιουργήσουν πρόβλημα. Είναι σημαντικό να είναι ενημερωμένα τα αντιβιοτικά προγράμματα, επειδή δημιουργούνται νέες απειλές κάθε μέρα. Ο πίνακας 1 δείχνει μερικές γρήγορες συμβουλές για τη προστασία του δικτύου από ιούς.

ΣΥΜΒΟΥΛΕΣ	ΑΙΤΙΑ
Ψάχνετε το Διαδίκτυο συχνά για να βρείτε νέες ενημερώσεις ιών	Εμφανίζονται νέες πληροφορίες καθημερινά. Η ασφάλεια δικτύων έχει συνεχώς προβλήματα και μετά βελτιώνεται.
Τρέξτε το αντιβιοτικό πρόγραμμα ανίχνευσης εκτός σύνδεσης	Αν ένας ιός μπει στο δίκτυο σας, μπορεί να χαλάσει το αντιβιοτικό σας πρόγραμμα τόσο εύκολα, όπως οποιαδήποτε άλλη εφαρμογή. Ένα πρόγραμμα που τρέχει εκτός σύνδεσης είναι η καλύτερη προστασία.
Εκπαιδεύστε τους χρήστες για να προσδιορίζουν πιθανές προγραμματισμένες απειλές	Οι ιοί συνήθως μπαίνουν στα δίκτυα μέσα από PC χρηστών. Για παράδειγμα, οι χρήστες ανοίγουν προγράμματα ή έγγραφα από μολυσμένες δισκέτες, ανοίγουν χαλασμένα μηνύματα ηλεκτρονικού ταχυδρομείου ή μεταφέρουν προγράμματα από το διαδίκτυο που εκθέτουν το δίκτυο σε ιούς.
Μεταφέρετε νέα αντιβιοτικά, προγράμματα όταν γίνονται διαθέσιμα	Επειδή οι ιοί αλλάζουν κάθε φορά που συναντιούνται νέοι ιοί, είναι σημαντικό να διατηρείτε το πρόγραμμα ενημερωμένο όσο γίνεται.

ΠΙΝΑΚΑΣ 1

Υπάρχουν πολλά αντιβιοτικά προγράμματα και πολλές διαφορετικές επιλογές. Το καλό αντιβιοτικό πρόγραμμα είναι αυτό που ψάχνει για πολλά διαφορετικά

σημάδια. Ένας προμηθευτής θα πρέπει να εξηγεί τις διαφορετικές αναβαθμίσεις, αν είναι οι αναβαθμίσεις εύκολα προσπελάσιμες και αν είναι μια αξιόπιστη εταιρεία.

Backups (Αντιγραφείς Ασφαλείας)

Τις περισσότερες φορές η ασφάλεια λέγεται απλά καλό back up. Δε νοείται μηχανογραφική παραγωγή η οποία να μη έχει καλό backup. Όλα τα μηχανογραφικά συστήματα πάσχουν απ' αυτό το πρόβλημα της καταστροφής / φθοράς των δεδομένων που έχουν αποθηκευμένα. Θα πρέπει να ληφθούν ισχυρά μέτρα προστασίας των δεδομένων τόσο από τυχαία όσο και από προμελετημένη καταστροφή. Θα πρέπει να γίνεται ένα αντίγραφο τουλάχιστον μια φορά την ημέρα και πιο συχνά αν υπάρχει ειδικός λόγος. Η συχνότητα με την οποία παίρνονται τα αντίγραφα έχει να κάνει με το χρόνο χειροκίνητης αποκατάστασης των δεδομένων. Θα πρέπει να υπάρχουν δυο αντίγραφα κάθε αντίγραφου. Το ένα φυλάσσεται επί τόπου και το άλλο σε ασφαλές μέρος σε άλλο απομακρυσμένο κτίριο. Θα πρέπει να υπάρχει η δυνατότητα να αποκατασταθεί το σύστημα ολικά. Με άλλα λόγια να υπάρχουν αντίγραφα τόσο των προγραμμάτων όσο και των δεδομένων. Τα αντίγραφα των δεδομένων θα πρέπει να πηγαίνουν αρκετές μέρες πίσω, πιθανόν και εβδομάδες. Το χρονικό θέμα εξαρτάται από το θέμα κόστους και απαξίωσης δεδομένων. Για παράδειγμα στο θέμα των πληρωμών μόλις η τράπεζα δεχθεί τις πληρωμές τις Visa, δεν είναι πλέον η ανάγκη να έχουν αντίγραφο ασφαλείας των σχετικών δεδομένων. Λόγω της σημαντικής τεχνικής δυσκολίας στο να υπάρχουν αντίγραφα ασφαλείας δεδομένων υψηλής αξίας που να πηγαίνουν πολλές μέρες πίσω θα πρέπει να ληφθεί σοβαρά υπόψη η πιθανότητα να αλλάξουν οι εξωτερικές διαδικασίες (δηλ. οι εκτός Η/Υ συστήματος). **[1]**

Παρακάτω θα ακολουθήσουν διαφορετικές λύσεις ασφαλείας, σε σχέση με τις κύριες προτεραιότητες της εταιρείας.

Υπάρχουν τέσσερις στόχοι που πρόκειται να επιτύχουν με τη λύση ασφαλείας για κάθε μια απ' αυτές τις περιπτώσεις. Οι στόχοι είναι οι βασικοί στόχοι και είναι σημαντικοί για οποιαδήποτε ηλεκτρονική επιχείρηση, αλλά όλοι έχουν πιθανούς κινδύνους ασφαλείας.

Στόχος 1: Παρέχει Διαδίκτυο, πρόσβαση στους εργαζόμενους

Στόχος 2: Παρέχει υπηρεσίες ηλεκτρονικού ταχυδρομείου στους εργαζόμενους

Στόχος 3: Παρέχει πρόσβαση στη Web τοποθεσία της εταιρείας

Στόχος 4: Επιτρέπει απομακρυσμένη πρόσβαση σε ένα ασφαλές δίκτυο

Και οι τέσσερις στόχοι παρουσιάζουν πιθανούς κινδύνους ασφαλείας

Η πρώτη εταιρεία αποφάσισε ότι οι προτεραιότητες της είναι το χαμηλό κόστος και η απλότητα και ότι θέλει να έχει μικρότερο επίπεδο ασφαλείας για να επιτύχει αυτές τις δυο προτεραιότητες. Αυτή η λύση ασφαλείας αποτελείται από ένα ηλεκτρονικό τείχος, που ενεργεί σαν φίλτρο μεταξύ του διαδικτύου και του HTPP της εταιρείας ή του διακομιστή, του FTP διακομιστή και του διακομιστή ανταλλαγής αλληλογραφίας. Σε αυτή τη περίπτωση το ηλεκτρονικό τείχος είναι ένα ηλεκτρονικό τείχος φίλτρο πακέτου, που εξετάζει όλα τα πακέτα που περνούν μεταξύ του δικτύου και του Διαδικτύου.

Ένα ηλεκτρονικό τείχος φίλτρου πακέτου δουλεύει είτε αποδεχόμενο είτε απορρίπτοντας κάθε πακέτο, σε σχέση με ένα σύνολο από προγραμματισμένους στόχους. Σε αυτή την περίπτωση η εταιρεία θα μπορούσε να διαμορφώσει το ηλεκτρονικό τείχος ώστε να αρνείται όλα τα πακέτα, εκτός απ' αυτά που στέλνονται ή λαμβάνονται από τη TCP θύρα 80, τη TCP θύρα 25 και τη TCP θύρα 53. Οι

πιθανοί απομακρυσμένοι χρήστες θα πρέπει να μπουν ατομικά στο ηλεκτρονικό τείχος, για να γίνουν αποδεκτές οι συγκεκριμένες IP διευθύνσεις προέλευσης και πρέπει να οριστούν επίσης οι συγκεκριμένες θύρες προέλευσης και προορισμού.

Αυτή η λύση ασφαλείας είναι μια από τις πιο φθηνές διαθέσιμες λύσεις. Το μόνο πρόγραμμα που απαιτείται είναι το πρόγραμμα ηλεκτρονικό τείχος φίλτρου πακέτου. Είναι επίσης μια πολύ απλή διαμόρφωση ασφάλειας. Υπάρχει ένα ηλεκτρονικό τείχος και όλα είναι συνδεδεμένα με αυτό. Η διαμόρφωση στο ηλεκτρονικό τείχος είναι επίσης πολύ εύκολη. Το ηλεκτρονικό τείχος μπορεί να επεξεργαστεί μόνο πακέτα έτσι το μόνο που χρειάζεται να δοθεί είναι οι στόχοι πρόσβασης ή απόρριψης. Ωστόσο αν διάφοροι απομακρυσμένοι χρήστες καλέσουν το δίκτυο θα πρέπει να μπει ξεχωριστά κάθε IP διεύθυνση προορισμού ή προέλευσης και κάθε θύρα.

Προφανώς εξ αιτίας της απλότητας και του χαμηλότερου κόστους, το επίπεδο της ασφαλείας υποφέρει. Για παράδειγμα μπορεί να γίνει στο δίκτυο μια επίθεση από μια από τις καθορισμένες θέσεις. Επίσης, αυτό το μοντέλο ασφαλείας δεν παρέχει καθόλου ασφάλεια επιπέδου χρήστη. Εφόσον μπει μέσα στο ηλεκτρονικό τείχος ένας εισβολέας έχει μεγάλη ελευθερία. Παρόμοια, οι τελικοί χρήστες έχουν πρόσβαση σε όλο το δίκτυο, όπως επίσης και στο Διαδίκτυο.

Για την δεύτερη εταιρεία αυτή η ασφάλεια είχε την υψηλότερη προτεραιότητα, ανεξάρτητα από το κόστος και τη πολυπλοκότητα. Ήθελαν να δημιουργήσουν το πιο ασφαλές δίκτυο που μπορούσαν. Σε αυτή τη λύση ασφαλείας είναι κρυμμένα δυο διαφορετικά δίκτυα πίσω από τα ηλεκτρονικά τείχη. Το ένα δίκτυο, που έχει τον Web διακομιστή, τον διακομιστή αλληλογραφίας και τον FTP διακομιστή, αναφέρεται σαν DMZ ή demilitarized zone. Από την άλλη ο διακομιστής

μεσολάβησης καταλήγει στην εσώτερη περίμετρο διατηρώντας τους τελικούς χρήστες και τα δεδομένα.

Το μεγαλύτερο πλεονέκτημα σε αυτό το μοντέλο είναι το επίπεδο ασφαλείας. Ένας διακομιστής μεσολάβησης ελέγχει την ασφάλεια που βασίζεται στο χρήστη. Ωστόσο εκτός από την περιήγηση στον διακομιστή μεσολάβησης, η κίνηση του τελικού χρήστη πρέπει να ταξιδέψει μέσα από το ηλεκτρονικό τείχος για να φθάσει στο Web, στην αλληλογραφία ή στο διακομιστή FTP. Το πλεονέκτημα αυτής της μεθόδου είναι ότι δημιουργεί μια κατάσταση κατά την οποία ένας εξωτερικός χρήστης μπορεί να έχει πρόσβαση στην Web τοποθεσία μιας εταιρείας, χωρίς να είναι στο ίδιο δίκτυο με τα εμπιστευτικά δεδομένα της εταιρείας. Τα μειονεκτήματα είναι προφανώς το κόστος και η πολυπλοκότητα. Θα χρειαστεί περισσότερο χρόνο και προσπάθεια να γίνει διαχείριση αυτού του συστήματος ασφαλείας. Θα είναι πιο περίπλοκο για τους χρήστες να φθάσουν στους πόρους που χρειάζονται. **[7]**

Γ.3 ΗΛΕΚΤΡΟΝΙΚΕΣ ΠΛΗΡΩΜΕΣ

Το κρισιμότερο σημείο κάθε εμπορικής συναλλαγής είναι η πληρωμή. Εμπόριο χωρίς χρήμα δεν έχει νόημα. Το Διαδίκτυο παρουσιάζει την ιδιομορφία να μην υπάρχει προσωπική επαφή μεταξύ του εμπόρου και του πελάτη, ιδιαίτερα στις λιανικές συναλλαγές. Κατά συνέπεια το θέμα των πληρωμών είναι το σημαντικότερο κομμάτι του ηλεκτρονικού εμπορίου.

Οι πληρωμές των λιανικών πωλήσεων έχουν το σημαντικότερο πρόβλημα καθώς τις περισσότερες φορές η επαφή πελάτη – εμπόρου είναι πολύ σπάνια ή και μοναδική (λ.χ. η αγορά ενός ασφαλιστηρίου συμβολαίου από ένα πράκτορα που διαπραγματεύεται πολλές εταιρείες), πληρωμές του χονδρικού εμπορίου έχουν

διαφορετική λογική και άλλα μέσα (λ.χ εγγυητικές επιστολές, φορτωτικές κλπ) και δεν έχουν τα ίδια προβλήματα. Η ύπαρξη παραστατικών που απαιτούν οι αρχές, κάνει δύσκολη τη δημιουργία νέων κόλπων από κακοπληρωτές ή τη διείσδυση νέου τύπου απατεώνων. Αν η κύρια χρήση του δικτυακού τόπου είναι το χονδρεμπόριο, τότε λίγα πράγματα θα αλλάξουν από πλευράς πληρωμών. Απλά θα υπάρχει ένα κανάλι ακόμα διανομής στο οποίο η επιχείρηση πρέπει να χρησιμοποιήσει την τακτική της συγκεκριμένης αγοράς.

Δυο πράγματα πάντως θα πρέπει να παρακολουθεί κάποιος. Πρώτον, το θέμα της νομικής υπόστασης της ηλεκτρονικής ανταλλαγής εγγραφών, κατά πόσο δηλαδή είναι δυνατόν να θεωρηθεί κάποιας μορφής ηλεκτρονική ανταλλαγή ως νόμιμο αντίστοιχο λ.χ του τιμολογίου. Αυτό προσπαθεί να το κάνει η κοινότητα, όποτε μπορεί να θεσμοθετηθεί απότομα. Το άλλο είναι το γεγονός ότι οι αυτόματες διαδικασίες πολλές φορές είναι δύσκολο να παρακολουθούνται με τους παραδοσιακούς τρόπους γι' αυτό καλό θα ήταν να μελετηθούν προσεκτικά τα πιστωτικά όρια και μετά να αυτοματοποιηθούν. Η συνεχώς αυξανόμενη εμπορευματοποίηση του Διαδικτύου και η χρήση του Web έχουν ωθήσει τις επιχειρήσεις στην εύρεση μεθόδων και συστημάτων πληρωμών για την υποστήριξη του Ηλεκτρονικού Εμπορίου.

Η πρακτική εφαρμογή του Ηλεκτρονικού Εμπορίου στο σύγχρονο επιχειρηματικό περιβάλλον απαιτεί την ύπαρξη συστημάτων ηλεκτρονικών πληρωμών μέσω των οποίων θα διεκπεραιώνονται ηλεκτρονικά οι οφειλές των εμπλεκομένων μερών. Ήδη έχουν υιοθετηθεί διάφορα συστήματα ηλεκτρονικών πληρωμών π.χ πιστωτικές κάρτες, ηλεκτρονικό χρήμα κλπ, κατάλληλα για την εξυπηρέτηση των συναλλαγών.

Πιστωτικές κάρτες.

Σε μία παραδοσιακή συναλλαγή με πιστωτική κάρτα, ο προμηθευτής καταγράφει τα στοιχεία της πιστωτικής κάρτας του πελάτη δημιουργώντας ένα έγγραφο συναλλαγής. Το εν λόγω έγγραφο υπογράφεται από τον αγοραστή και προωθείται στη συνέχεια στην τράπεζα για διεκπεραίωση. Στο τέλος η τράπεζα χρεοπιστώνει τους αντίστοιχους λογαριασμούς ενημερώνοντας τα εμπλεκόμενα μέρη για τη συναλλαγή που έγινε.

Σε ένα μηχανισμό ηλεκτρονικής πληρωμής με χρήση πιστωτικής κάρτας, ακολουθείται περίπου το ίδιο σενάριο με αυτό που αναφέρθηκε στην προηγούμενη παράγραφο. Επιπλέον το σενάριο αυτό, εμπλουτίζεται με μηχανισμούς ασφαλείας (π.χ έλεγχος ταυτότητας πελάτη και εμπόρου). Το γεγονός αυτό έχει οδηγήσει στην ύπαρξη μίας γκάμας συστημάτων ηλεκτρονικών πληρωμών με πιστωτικές κάρτες. Δύο από αυτά τα χαρακτηριστικά που προσδιορίζουν και διαφοροποιούν τα συστήματα αυτά, είναι *το επίπεδο της ασφάλειας των συναλλαγών* και *το λογισμικό* που απαιτείται από όλα τα εμπλεκόμενα μέρη (αγοραστής, τράπεζα).

Κατά τη διάρκεια μιας on-line συναλλαγής, τα στοιχεία της πιστωτικής κάρτας ενός αγοραστή μπορούν να μεταφερθούν με δύο τρόπους. Ο πρώτος τρόπος θεωρείται μη ασφαλής και υποστηρίζει την αποστολή των στοιχείων της ηλεκτρονικής πληρωμής από τον πελάτη στον έμπορο (ή την τράπεζα) σε μη κρυπτογραφημένη μορφή. Η μέθοδος αυτή κρίνεται ως μη ασφαλής, γιατί κατά τη μεταβίβαση των στοιχείων μπορεί να παρεισφρήσει κάποιος "εισβολέας" και να τροποποιήσει τα στοιχεία της συναλλαγής ή ακόμα και να τα υποκλέψει.

Ο δεύτερος τρόπος, θεωρείται πιο ασφαλής και προβλέπει την κρυπτογράφηση όλων των πληροφοριών που σχετίζονται με την πληρωμή πριν την αποστολή τους στον έμπορο (ή την τράπεζα) μέσω του Διαδίκτυου.

Για την αποφυγή της παρεμβολής κάποιου τρίτου κατά τη διεξαγωγή των συναλλαγών μεταξύ του πελάτη και του εμπόρου, μια καλή επιλογή αποτελεί εκείνος ο συνδυασμός web browser και web server που θα υποστηρίζει το πρωτόκολλο Secure Sockets Layer (SSL). Η χρησιμοποίηση διακομιστή web και web browser που υποστηρίζουν το πρωτόκολλο SSL, εξασφαλίζει την προστασία των δεδομένων από κάποιο τρίτο. Δεν εγγυάται όμως ότι τα δεδομένα αυτά δεν θα χρησιμοποιηθούν σκόπιμα από τον έμπορο. Το SSL αποτελεί τα αρχικά για το ασφαλές επίπεδο υποδοχής. Ο όρος περιγράφει μια μέθοδο κρυπτογράφησης της ροής δεδομένων μεταξύ ενός προγράμματος πλοήγησης και του διακομιστή Web. Ο κόσμος το χρησιμοποιεί καθημερινά για να ανακτήσει οικονομικές πληροφορίες και για να παραγγείλει μέσω Διαδικτύου. Visa και MasterCard ανέπτυξαν ένα νέο πιο ασφαλές πρωτόκολλο το Secure Electronic Transaction (SET), το οποίο θεωρητικά είναι τέλειο. Για την αποφυγή εξαπάτησης του πελάτη από τον έμπορο (για παράδειγμα, χρήση των στοιχείων της πιστωτικής κάρτας από τον έμπορο για τη διεξαγωγή μη εξουσιοδοτημένων αγορών), θα μπορούσε να χρησιμοποιηθεί ένας ανεξάρτητος φορέας διασφάλισης των συναλλαγών γνωστός ως «Έμπιστη Τρίτη Οντότητα (ΕΤΟ)».

Μία ΕΤΟ μεσολαβεί ανεξάρτητα στην όλη διαδικασία αποκρυπτογραφώντας τα στοιχεία της πιστωτικής κάρτας επικυρώνοντας τη συναλλαγή. Σε αρκετές περιπτώσεις, εταιρείες που παράγουν συστήματα ηλεκτρονικών πληρωμών, όπως η Cyber cash, η Verifone ή η First Virtual, χρησιμοποιούν μηχανισμούς με τους

οποίους παρέχουν υπηρεσίες ΕΤΟ. Και η Cyber cash και η Verifone χρησιμοποιούν τον μηχανισμό των wallet. Ο μηχανισμός αυτός μεταφέρει τον κρυπτογραφημένο αριθμό της πιστωτικής κάρτας από τον έμπορο στον δικό τους επεξεργαστή για τον έλεγχο αυθεντικότητας και την έγκριση της συναλλαγής. Η εταιρεία First Virtual εκδίδει κάποιο Virtual Pin στον πελάτη που το χρησιμοποιεί αντί του αριθμού της πιστωτικής κάρτας. Αφού λάβει τις πληροφορίες των πωλήσεων από τον έμπορο, η First Virtual μετατρέπει το Virtual PIN στον αριθμό λογαριασμού της πιστωτικής κάρτας, προκειμένου να διεκπεραιωθεί η πληρωμή.

Σε αυτή την περίπτωση η ηλεκτρονική ολοκλήρωση των συναλλαγών παρουσιάζει το εξής πλεονέκτημα έναντι του παραδοσιακού τρόπου πληρωμής με πιστωτική κάρτα: κρυπτογραφώντας τα στοιχεία της πιστωτικής κάρτας και με την μεσολάβηση μίας Τρίτης Έμπιστης Οντότητας, όπως η Cyber cash ή η First Virtual, η επεξεργασία των στοιχείων αυτών δεν γίνεται από τον έμπορο, οπότε και εξαλείφεται ο κίνδυνος απάτης από την πλευρά του τελευταίου.

Σε αυτό το σημείο θα πρέπει να σημειωθεί ότι παρά την πρόοδο που έχει σημειωθεί στα συστήματα ηλεκτρονικών πληρωμών με χρήση πιστωτικών καρτών, εξακολουθούν να υπάρχουν ακόμη ορισμένα προβλήματα. Το σημαντικότερο πρόβλημα που εξακολουθεί να υφίσταται ακόμη είναι η τυποποίηση. Θα πρέπει να υιοθετηθεί μια κοινά αποδεκτή μέθοδος (ή πρότυπο) διεκπεραίωσης των ηλεκτρονικών συναλλαγών στο Διαδίκτυο, που θα επιτρέπει την επικοινωνία μεταξύ των διαφορετικών τύπων λογισμικού των συναλλασσομένων μερών. Η εξασφάλιση ή όχι αυτής της δια-λειτουργικότητας θα καθορίσει και την μελλοντική πορεία των ηλεκτρονικών συστημάτων πληρωμών μέσω πιστωτικής κάρτας.

Ανατύπωση του τεύχους #23 από το Internet Scam busters, της 31ης Μαΐου 1998.

Στη διάρκεια των τελευταίων τεσσάρων ετών έχει απασχολήσει έντονα τη δημοσιότητα το ζήτημα της απάτης που σχετίζεται με την παράνομη χρήση πιστωτικών καρτών στο Διαδίκτυο. Εάν προστεθεί στα σχετικά άρθρα του τύπου την προβολή ταινιών, όπως το «Δίκτυο» είναι απόλυτα φυσιολογικό να έχει δημιουργηθεί στον κόσμο φοβία, που συνεπάγεται μεγάλη επιφύλαξη στο να δίνει ελεύθερα τον αριθμό της πιστωτικής κάρτας στο Διαδίκτυο.

Παρόλα αυτά, ο κάθε νοήμων πολίτης, αντιλαμβάνεται πολύ καλά ότι στην πραγματικότητα είναι πολύ πιο ασφαλές να καταχωρεί κανείς τον κωδικό του αριθμό σε ένα on-line ασφαλές «έντυπο παραγγελίας» από το να παραδίδει την πιστωτική του κάρτα σε έναν σερβιτόρο στο εστιατόριο.

Ας το πάρουμε λογικά, τι εμποδίζει τον σερβιτόρο να καταγράψει τον αριθμό της πιστωτικής σας κάρτας και να τοποθετήσει παραγγελίες τηλεφωνικά κάποια στιγμή; Σύμφωνα με έρευνες, το ποσοστό των αγορών με παράνομη χρήση πιστωτικών καρτών, από κινητό τηλέφωνο είναι κατά πολύ μεγαλύτερο αυτού στο Διαδίκτυο.

Παρόλα αυτά, αυτό το άρθρο δεν διαπραγματεύεται τους κινδύνους που ελλοχεύουν από την παράνομη χρήση πιστωτικών καρτών για τους ιδιώτες-καταναλωτές. Θα λέγαμε ότι εξετάζει ένα πολύ πιο φλέγον αλλά λιγότερο δημοσιοποιημένο ζήτημα, και συγκεκριμένα το πρόβλημα των επιχειρήσεων που κάνουν αποδεκτές τις πιστωτικές κάρτες σαν μέσο πληρωμής. Και πραγματικά, ο αριθμός των εμπόρων – εταιρειών που έχουν πέσει θύματα απατεώνων που βάζουν παραγγελίες χρησιμοποιώντας κλεμμένες πιστωτικές κάρτες παρουσιάζει τεράστια αύξηση. Δυστυχώς οι έμποροι δεν τυγχάνουν της ίδιας προστασίας όπως

οι καταναλωτές, όταν βρίσκονται αντιμέτωποι με τέτοιου είδους προβλήματα. Στην πραγματικότητα είναι απόλυτα εκτεθειμένοι.

Παραθέτουμε ένα πραγματικό περιστατικό :

Η εταιρεία Χ είχε την πρώτη της εμπειρία παράνομης χρήσης με πιστωτική κάρτα πριν από ένα μήνα. Κάποιος έκλεψε τον αριθμό πιστωτικής κάρτας και χρησιμοποίησε τον κλεμμένο αριθμό για να αγοράσει ένα προϊόν αξίας $500 από την εταιρεία. Ο απατεώνας γνώριζε την πραγματική διεύθυνση του κατόχου την οποία και κοινοποίησε στην εταιρεία, αλλά ζήτησε η παράδοση να γίνει σε διαφορετική διεύθυνση. Δεδομένου ότι είναι σύνηθες φαινόμενο κάποιοι από τους πελάτες να ζητούν η διεύθυνση παράδοσης να είναι διαφορετική από τη διεύθυνση τιμολόγησης, το αίτημα του συγκεκριμένου πελάτη δεν κίνησε υποψίες. Η πολιτική της εταιρείας είναι να στέλνονται τα τιμολόγια στη διεύθυνση του κατόχου, πράγμα που έγινε. Μερικές μέρες αργότερα, η εταιρεία δέχθηκε ένα τηλεφώνημα από τον νόμιμο κάτοχο της κλεμμένης κάρτας που τη πληροφόρησε ότι ουδέποτε είχε κάνει αγορά από την εταιρεία αυτή.

Ο συγκεκριμένος απατεώνας είχε κάνει χρήση μίας δωρεάν υπηρεσίας e-mail και συγκεκριμένα της Juno για να ανοίξει λογαριασμό e-mail στο όνομα του κατόχου της κάρτας, γεγονός που έδωσε στη συναλλαγή έναν νομιμοφανή χαρακτήρα. Η εταιρεία ενημέρωσε το τμήμα ασφαλείας της Juno για την διαπραχθείσα απάτη και η Juno έκλεισε το λογαριασμό του απατεώνα. Αν και είχε πάρει κανονικά την απαιτούμενη εξουσιοδότηση και έγκριση από την εταιρεία που διαχειρίζεται τον εταιρικό της λογαριασμό πιστωτικών καρτών, πλήρωσε εξ ολοκλήρου τη ζημιά. Επικοινώνησε και με την τράπεζα και με όλους τους εμπλεκόμενους ακόμα και με την αστυνομία. Κανείς τους δεν φάνηκε διατεθειμένος

να τη βοηθήσει, ίσως επειδή ήταν πολύ απασχολημένοι ή επειδή αισθανόντουσαν ότι το εν λόγω ποσόν των $500 δεν ήταν τόσο σημαντικό για να κινήσουν περαιτέρω διαδικασίες.

Μετά από αυτό το πάθημά τους, αποφάσισαν να κάνουν κάποιες έρευνες και να γνωρίσουν με ποιόν τρόπο οι άλλες εταιρείες αντιμετωπίζουν αυτό το πρόβλημα. Ανακάλυψαν ότι η απάτη με τις πιστωτικές κάρτες γιγαντώνεται ολοένα και περισσότερο για τις εταιρείες που κάνουν πωλήσεις μέσω Διαδικτύου. Τους έκανε εντύπωση πώς ένα τόσο μεγάλο πρόβλημα δεν έχει ακόμα λάβει τη σχετική δημοσιότητα. Ανακάλυψαν ακόμα ότι αυτού του είδους οι απατεώνες είναι σε θέση πλέον να δημιουργούν φανταστικούς αριθμούς πιστωτικών καρτών (δηλ. που δεν έχουν εκδοθεί ακόμα) βασιζόμενοι στους εφαρμοζόμενους αλγόριθμους για την παραγωγή των αυθεντικών αριθμών. Όπως είναι αναμενόμενο, αυτοί οι αριθμοί περνούν άνετα το στάδιο της επαλήθευσης και λαμβάνουν τους απαραίτητους κωδικούς έγκρισης.

Ακόμα υπάρχουν ομάδες δημοσίευσης πληροφοριών (Newsgroups) οι οποίες δημοσιεύουν κλεμμένα στοιχεία πιστωτικών καρτών, και έτσι εάν κλαπεί ο αριθμός της πιστωτικής σας κάρτας μπορεί να δημοσιευθεί ανά τον κόσμο μέσα σε λίγα λεπτά.

Ηλεκτρονικές επιταγές

Μία έντυπη επιταγή είναι ουσιαστικά μια εντολή μεταφοράς κεφαλαίων από ένα λογαριασμό σε ένα άλλο. Η εντολή αυτή αποστέλνεται αρχικά στον αποδέκτη των κεφαλαίων, ο οποίος με τη σειρά του παρουσιάζει την επιταγή στην τράπεζα προκειμένου να λάβει το αντίστοιχο ποσό.

Μια ηλεκτρονική επιταγή έχει όλα τα χαρακτηριστικά που διαθέτει μια έντυπη επιταγή και χρησιμοποιείται σαν ένα μήνυμα προς την τράπεζα του αποστολέα για τη μεταφορά κεφαλαίων από ένα λογαριασμό σε άλλο. Σε αντιστοιχία με τη παραδοσιακή διαδικασία, η ηλεκτρονική επιταγή αποστέλνεται αρχικά στον αποδέκτη ο οποίος υπογράφει και την προωθεί στην τράπεζα προκειμένου να λάβει το αντίστοιχο ποσό.

Από άποψη ασφάλειας η ηλεκτρονική επιταγή θεωρείται καλύτερη από την έντυπη επιταγή. Και αυτό, γιατί ο αποστολέας μπορεί να προστατέψει τον εαυτό του από μια απάτη. Αυτό γίνεται με τη κωδικοποίηση του αριθμού του λογαριασμού του με το δημόσιο κλειδί της τράπεζας χωρίς έτσι να αποκαλύπτει τον αριθμό του λογαριασμού του στον έμπορο.

Το FSTC αποτελεί μια συνεργασία τραπεζών και πιστωτικών οργανισμών, που έχουν υλοποιήσει μια ηλεκτρονική επιταγή. Στηριγμένη στην παραδοσιακή επιταγή, η επιταγή του FSTC επιτρέπει την ψηφιακή υπογραφή του αποδέκτη. Για την προσθήκη μεγαλύτερης ευελιξίας σε αυτό το σύστημα πληρωμών, το FSTC προσφέρει στους χρήστες διάφορες επιλογές επιταγών ανάλογα με τις ανάγκες του χρήστη. Οι ηλεκτρονικές επιταγές μπορούν να παραδοθούν είτε με άμεση παράδοση μέσω ενός δικτύου ή μέσω ηλεκτρονικού ταχυδρομείου. Σε κάθε περίπτωση, τα υπάρχοντα τραπεζικά κανάλια μπορούν να εκκαθαρίσουν τις πληρωμές, μέσω των δικτύων τους. Κάτι τέτοιο οδηγεί σε μια ικανοποιητική αναβάθμιση της υπάρχουσας τραπεζικής υποδομής και του Διαδικτύου.

Η μέθοδος είναι αποτελεσματική, αλλά μάλλον ακατάλληλη για την Ελλάδα. Δεδομένης της ανυπαρξίας λιανικών συναλλαγών με επιταγή η αξία αυτής της διαδικασίας είναι μάλλον ακαδημαϊκή στην Ελλάδα. Αν όμως υπάρχει σημαντικός

αριθμός πελατών από Αγγλοσαξονικές κυρίως χώρες, θα πρέπει να μελετηθεί το θέμα προσεκτικά με τελικό στόχο την υλοποίηση.

Ψηφιακές Υπογραφές

Οι ψηφιακές υπογραφές είναι μια από τις βασικές ιδιότητες του PKI, που κάνουν τις συναλλαγές πιο ασφαλείς μέσω του Διαδικτύου. Υπάρχει η σφραγίδα ταυτότητας που ταξιδεύει με μήνυμα μέσω Διαδικτύου. Μια ψηφιακή υπογραφή περιέχει την πιστοποιημένη ταυτότητα του θέματος με ιδιότητες, όπως το όνομα, τον εργοδότη ή τη διεύθυνση. Η ψηφιακή υπογραφή είναι νομικό έγγραφο αν χρησιμοποιηθεί σωστά και με εμπιστοσύνη. Ωστόσο δεν έχουν υπάρξει ακόμα υποθέσεις σε δικαστήρια που να έχουν καθορίσει τους κανόνες που πρέπει να ισχύουν και να γίνουν αποδεκτές στο δικαστήριο. Γενικά, οι ψηφιακές υπογραφές που χρησιμοποιούν κλειδί κρυπτογράφησης και πιστοποιούν την ταυτότητα κάποιου είναι νομικά έγγραφα. Το κόστος απόκτησης της είναι όσο και το κόστος μιας πιστωτικής κάρτας. Για τη δημιουργία της ψηφιακής υπογραφής το μήνυμα στην ιστοσελίδα του παραλήπτη συγχωνεύεται σε μέγεθος 160 bits (message digest). Η σύγκριση τους δίνει την ακεραιότητα του μηνύματος**.**

Ψηφιακό Χρήμα

Το ψηφιακό χρήμα είναι ένας μηχανισμός εξόφλησης μικροποσών μέσω Διαδικτύου. Ένας τέτοιος μηχανισμός μπορεί να αποτελέσει το επόμενο βήμα στις εφαρμογές ηλεκτρονικών πληρωμών. Σε ένα σύστημα ψηφιακού χρήματος, το νόμισμα δεν είναι τίποτα άλλο παρά μια σειρά από ψηφία.

Ένας χρήστης μπορεί να κάνει ανάληψη ψηφιακού χρήματος από μια τράπεζα μεταφέροντας το ποσό αυτό στον ηλεκτρονικό του υπολογιστή. Το ψηφιακό χρήμα που παραχωρείται από την τράπεζα σημαδεύεται κατάλληλα για λόγους εγκυρότητας και ασφάλειας. Σε περίπτωση αγοράς προϊόντων μέσω του Διαδικτύου, ο αγοραστής αποστέλνει στο προμηθευτή το αντίτιμο σε ψηφιακό χρήμα. Ο τελευταίος με τη σειρά του, προωθεί στην τράπεζα τη ψηφιακή ροή που έλαβε προκειμένου να διευρυνθεί κατά πόσο η ροή αυτή αποτελεί έγκυρη χρηματο-ροή ή όχι.

Για να διασφαλίσει ότι κάθε χρηματο-ροή χρησιμοποιείται μόνο μια φορά, η τράπεζα καταγράφει τον σειριακό αριθμό κάθε χρηματο-ροής που ξοδεύεται. Αν ο σειριακός αριθμός της χρηματοροής υπάρχει ήδη στην βάση δεδομένων, τότε η τράπεζα έχει εντοπίσει κάποιον που προσπάθησε να χρησιμοποιήσει περισσότερες από μια φορές και θα πληροφορήσει τον έμπορο ότι αυτή η χρηματική μονάδα είναι άχρηστη.

Μια εναλλακτική λύση που αναπτύχθηκε από την DigiCash επιτρέπει στους χρήστες να διατηρήσουν την ανωνυμία τους. Ο εν λόγω μηχανισμός, που ονομάζεται ‘blind signature’, επιτρέπει στον αγοραστή να λάβει ηλεκτρονικό χρήμα από μια τράπεζα χωρίς η τράπεζα να μπορεί να συσχετίσει το όνομα του αγοραστή με τις χρηματοροές που διανέμονται. Η τράπεζα πρέπει να εκτιμήσει τις χρηματοροές που λαμβάνει από τον έμπορο, μέσω της ψηφιακής στάμπας που έχει αρχικά τοποθετηθεί στις χρηματοροές του χρήστη αλλά η τράπεζα δεν μπορεί να καταλάβει ποίος έκανε την πληρωμή.

Αυτό το καιρό η Ελλάδα είναι σε δεύτερο κύκλο προσπαθειών για δημιουργία ψηφιακού χρήματος. Ο πρώτος απέτυχε για εμπορικούς λόγους, αλλά και λόγω

εχθρότητας των κεντρικών τραπεζών. Μολονότι το ψηφιακό χρήμα είναι τεχνικά εφικτό, τα διαφορά γενικότερα προβλήματα που δημιουργούνται είναι τεράστια. Είναι η προβληματική μορφή πληρωμών στο Διαδίκτυο. Τα προβλήματα, εκτός από τα τεχνικά, είναι και γενικότερης κοινωνικής και πολιτικής φύσεως, Για τους ανθρώπους που ασχολούνται παραγωγικά με το ηλεκτρονικό εμπόριο, το μόνο που ενδιαφέρει είναι να παρακολουθούν τις εξελίξεις, καθώς η γενική εντύπωση είναι ότι μόλις αρχίσει να λειτουργεί θα είναι απαραίτητο.

Γ.4 ΨΗΦΙΑΚΑ ΠΙΣΤΟΠΟΙΗΤΙΚΑ ΚΑΙ ΠΑΡΟΧΕΣ ΥΠΗΡΕΣΙΩΝ ΠΙΣΤΟΠΟΙΗΣΗΣ

Προκειμένου να γίνει χρήση της κρυπτογράφησης δημοσίου κλειδιού θα πρέπει να παραχθεί ένα δημόσιο και ένα ιδιωτικό κλειδί. Βέβαια, κάτι τέτοιο θα μπορούσε να γίνει με κάποιο πρόγραμμα πού θα χρησιμοποιήσει το κλειδί αυτό (π.χ ο web browser ή το e-mail). Έπειτα ο κάτοχος θα πρέπει να φροντίσει για τη φύλαξη του ιδιωτικού του κλειδιού αλλά και τη δημοσίευση του δημοσίου κλειδιού. Η δημοσίευση θα μπορούσε να γίνει με την αποστολή του δημοσίου κλειδιού στους παραλήπτες μέσω e-mail.

Οι αρχές πιστοποίησης αποτελούν έναν πιο έμπιστο τρόπο για τη δημοσίευση και διανομή των δημοσίων κλειδιών. Οι αρχές πιστοποίησης λαμβάνουν το δημόσιο κλειδί του ενδιαφερομένου χρήστη. Εάν ο χρήστης ενεργεί στην συγκεκριμένη περίπτωση ως άτομο θα πρέπει να παραχωρήσει όλα τα απαραίτητα στοιχεία που αποδεικνύουν την ταυτότητά του. Σε αντίθετη περίπτωση, ο χρήστης θεωρείται ότι ενεργεί για λογαριασμό κάποιας επιχείρησης και θα πρέπει να παραχωρήσει όλες τις νομικές πληροφορίες που απαιτούνται για την αξιοπιστία και

τη νόμιμη λειτουργία της. Έτσι λοιπόν, οι υπόλοιποι μπορούν να ζητήσουν την αυθεντικοποίηση του δημοσίου κλειδιού από την αρχή πιστοποίησης.

Το Certification Authority (CA) είναι ένας οργανισμός, ιδιωτικός ή δημόσιος, που έχει στόχο να καλύψει την ανάγκη για εμπιστοσύνη στο χώρο του Ηλεκτρονικού Εμπορίου. Αυτό το κάνει προσφέροντας ψηφιακά πιστοποιητικά για το αντικείμενο που του ζητάνε να πιστοποιήσουν.

Στην ουσία, ένα ψηφιακό πιστοποιητικό αποτελεί μία ψηφιακά υπογεγραμμένη δήλωση από μία αρχή πιστοποίησης, η οποία :

* προσδιορίζει την αρχή πιστοποίησης που εξέδωσε,

* περιέχει το όνομα και κάποιες άλλες ιδιότητες του εγγεγραμμένου,

* το δημόσιο κλειδί του εγγεγραμμένου, και

* είναι ψηφιακά υπογεγραμμένο από την αρχή πιστοποίησης που το εξέδωσε

Τα πιστοποιητικά είναι οι τεχνικές συσκευές που βεβαιώνουν τη ταυτότητα του αποστολέα και έτσι καθορίζουν την εμπιστοσύνη μεταξύ των μερών που επικοινωνούν στο Διαδίκτυο. Ένα πιστοποιητικό αποτελείται από δυο μέρη, το δημόσιο κλειδί και τη ψηφιακή υπογραφή. Η μορφή των πιστοποιητικών είναι σημαντική.

Υπάρχουν τρεις διαφορετικοί τύποι πιστοποιητικών.

- Πιστοποιητικά προσδιορισμού. Είναι ο πιο κοινός τύπος και σημαίνει ότι συνδέει τον αποστολέα του πιστοποιητικού στο δημόσιο κλειδί του αποστολέα.
- Πιστοποιητικά συναλλαγών. Παρέχει στο παραλήπτη του μηνύματος πληροφορίες για την ίδια τη συναλλαγή. Για παράδειγμα ένα τέτοιο πιστοποιητικό μπορεί να αποδείξει σε κάποιον ότι έκανε μια αλλαγή ή

υπέγραψε ένα έγγραφο, με τη παρουσία κάποιου άλλου. Αυτού του είδους το πιστοποιητικό είναι καλό μόνο για μια φορά.

- Πιστοποιητικά ελέγχου ταυτότητας. Παρέχει στο παραλήπτη του μηνύματος περισσότερες πληροφορίες για το άτομο που στέλνει το μήνυμα. Π.χ ένα τέτοιο πιστοποιητικό μπορεί να περιλαμβάνει πληροφορίες για τη διεύθυνση του αποστολέα, την ηλικία και την εταιρεία.

ΨΗΦΙΑΚΑ ΠΙΣΤΟΠΟΙΗΤΙΚΑ

Ο δρόμος για τη χρήση ψηφιακών πιστοποιητικών άνοιξε και για την Ελλάδα το Μάιο του 2002 με τη δημοσίευση Κανονισμού Παροχής Υπηρεσιών Πιστοποίησης Ηλεκτρονικής Υπογραφής στην Εφημερίδα της Κυβερνήσεως με απόφαση της ΕΕΤΤ. Σύμφωνα με το κανονισμό, ρυθμίζονται θέματα σχετικά με τη παροχή υπηρεσιών πιστοποίησης ηλεκτρονικής υπογραφής, ζητήματα Αναγνωρισμένων Πιστοποιητικών και η εποπτεία και ο έλεγχος των εγκατεστημένων στην Ελλάδα Παροχών Υπηρεσιών Πιστοποίησης ηλεκτρονικής υπογραφής, οι οποίοι εκδίδουν αναγνωρισμένα και μη πιστοποιητικά. Η ΕΕΤΤ ασκεί την εποπτεία και τον έλεγχο των εγκατεστημένων στην Ελλάδα Παροχών Υπηρεσιών Πιστοποίησης, τηρώντας παράλληλα και το μητρώο των εγκατεστημένων στην Ελλάδα Παροχών. Το γεγονός της έναρξης του θεσμικού πλαισίου γύρω από τα ψηφιακά πιστοποιητικά πρόκειται να προσφέρει ώθηση στην ασφάλεια των online συναλλαγών. Και αυτό γιατί με τη λήψη ενός μηνύματος με ηλεκτρονική υπογραφή, ο παραλήπτης επαληθεύοντας την ηλεκτρονική υπογραφή βεβαιώνεται ότι το μήνυμα είναι ακέραιο. Ο παραλήπτης για την επαλήθευση της ηλεκτρονικής υπογραφής, χρησιμοποιεί το δημόσιο κλειδί του αποστολέα.

Γ.5 ΥΠΗΡΕΣΙΕΣ ΠΙΣΤΟΠΟΙΗΤΙΚΩΝ

Ένα πολύ σημαντικό μέρος του PKI είναι η υπηρεσία των πιστοποιητικών. Μια αρχή έκδοσης πιστοποιητικών είναι μια ανεξάρτητη εταιρεία που ενεργεί σαν μια έμπιστη πηγή, αποδεικνύοντας τις ταυτότητες των ατόμων που προσπαθούν να επικοινωνήσουν. Η CA είναι μια υπηρεσία που δίνει επίσημα έγγραφα που βεβαιώνουν ότι αυτός που φέρει το πιστοποιητικό είναι πραγματικά ένα συγκεκριμένο άτομο. Η εταιρεία CA δίνει και διαχειρίζεται τα ψηφιακά πιστοποιητικά.

Η πρώτη υπευθυνότητα της CA είναι να πιστοποιήσει την ταυτότητα ενός ατόμου χρησιμοποιώντας παραδοσιακές μορφές ελέγχου ταυτότητας. Αφού οριστεί μια ταυτότητα, είναι η CA που δίνει σε ένα άτομο ένα ψηφιακό πιστοποιητικό με ένα δημόσιο και ένα ιδιωτικό κλειδί. Έτσι η CA βεβαιώνει τελικά ότι το άτομο με το οποίο επικοινωνεί κάποιος είναι πραγματικά το άτομο που πιστεύει ότι είναι, επειδή έχει το ζευγάρι με το δημόσιο και ιδιωτικό κλειδί.

Αφού το ψηφιακό πιστοποιητικό είναι στη κατοχή του πιστοποιημένου ατόμου, η CA θα πιστοποιήσει την ταυτότητα μόνο για κάποιο χρονικό διάστημα ή μέχρι να αλλάξει κάτι στο πιστοποιητικό, όπως το όνομα του ατόμου ή η θέση. Αν συμβεί μια αλλαγή ή τελειώσει το χρονικό διάστημα το πιστοποιητικό λήγει και η CA θα βάλει το πιστοποιητικό σε μια λίστα από ληφθέντα πιστοποιητικά.

Όταν λήξει το πιστοποιητικό, η CA το προσθέτει στη λίστα των ληγμένων πιστοποιητικών. Εξαρτάται από το άτομο να ελέγξει τα εισερχόμενα πιστοποιητικά για εγκυρότητα. Το πιο συνηθισμένο πρόβλημα που δημιουργείται με αυτό το σύστημα είναι ότι κάποιος δεν μπορεί να μάθει ποια πιστοποιητικά έχουν λήξει και συνεπώς δεν είναι πλέον πιστοποιημένα. Εξ αιτίας αυτού του προβλήματος

ασφαλείας, διάφορες CA έχουν μια συνεχώς ενημερωμένη βάση δεδομένων, που είναι προσπελάσιμη από το κοινό. **[7]**

Μερικές γενικές προφυλάξεις για την CA

Επειδή το PKI εξακολουθεί να είναι νέο και το σύστημα των CA δεν είναι πλήρως τέλειο, υπάρχουν διάφορα θέματα για σκέψη πριν επιλεχθεί μια εταιρεία CA. Πρώτα απ' όλα υπάρχουν ερωτηματικά για την αξιοπιστία της εταιρείας της ίδιας της CA. Και τα δυο μέρη πρέπει να θεωρούν ότι η CA είναι τίμια και κάνει τους απαραίτητους ελέγχους για να πιστοποιήσει μια ταυτότητα. Για παράδειγμα μια εταιρεία ή άτομο που θέλει να έχει πρόσβαση στα ιδιωτικά μηνύματα κάποιου μπορεί να εμφανιστεί σαν CA για να έχει αντίγραφο του κλειδιού αποκρυπτογράφησης.

Για να προστατευθούν οι εταιρείες από ψεύτικα CA και να βεβαιωθούν για τη ποιότητα της CA, οι περισσότερες CA έχουν μια δική τους υπηρεσία πιστοποιητικών. Μπορεί να έρθει κάποιος σε επαφή με αυτή τη δεύτερη εταιρεία για επιπλέον πιστοποιητικά.

Όταν η CA δίνει ένα ψηφιακό πιστοποιητικό, δίνει ένα πιστοποιητικό πρακτικής εντολής, που είναι ένα νομικό έγγραφο που εξηγεί με λεπτομέρεια την ταυτότητα του χρήστη, πότε εκδόθηκε το πιστοποιητικό, τι βεβαιώνει η CA με αυτό το πιστοποιητικό και πότε αυτό λήγει. Αυτή η τεκμηρίωση χρησιμοποιείται συνήθως σαν οδηγός για τις εταιρείες, προκειμένου να αποφασίσουν σε ποίο βαθμό μπορούν να εμπιστεύονται μια CA.

Η CA θα δημοσιεύσει επίσης μια γενική πολιτική πιστοποιητικών, που στέλνεται με την ψηφιακή υπογραφή. Αυτή η πολιτική βοηθά μια εταιρεία να προσδιορίσει

πόση εμπιστοσύνη μπορεί να έχει στην ψηφιακή υπογραφή κάποιου άλλου και στην CA.

Οι *αρχές έκδοσης εγγράφων (Registration Authority – RA)* είναι εταιρείες διαφορετικές από τις CA που εγγράφουν ή ορίζουν νέους χρήστες στο PKI. Η RA είναι ένας ενδιάμεσος που λαμβάνει την αίτηση για τα πιστοποιητικά από το χρήστη, κάνει τη νόμιμη δουλειά πιστοποιώντας την ταυτότητα του χρήστη και μετά έρχεται σε επαφή με τη CA. Το RA δεν μπορεί να δώσει ψηφιακές υπογραφές.

Ένα πραγματικό παράδειγμα

Το PKI είναι ευκολότερο να κατανοηθεί με τη χρήση ενός παραδείγματος 'βήμα προς βήμα', του τρόπου που θα πρέπει να χρησιμοποιήσει το σύστημα ασφαλείας μια εταιρεία. Σ' αυτό το παράδειγμα δυο άτομα ο Κώστας και η Μαρία, θέλουν να έχουν ασφαλείς επαγγελματικές συναλλαγές και πρέπει να βεβαιωθούν ότι κάποιος δεν κλέβει τις απόρρητες πληροφορίες τους.

Ο Κώστας έρχεται σε επαφή με τη τοπική RA και κάνει αίτηση για PKI. Η RA πιστοποιεί το Κώστα χρησιμοποιώντας παραδοσιακές μορφές ελέγχου ταυτότητας, όπως προσωπικές συναντήσεις, την άδεια οδήγησης κλπ. Αφού η RA έχει ελέγξει τον Κώστα, στέλνει τις πληροφορίες και την αποδοχή στη διεθνή εταιρεία CA.

Η CA δημιουργεί ένα πιστοποιητικό για το Κώστα που λέει το όνομα του, την διεύθυνση του και την εταιρεία στην οποία δουλεύει. Επισυνάπτουν ένα αντίγραφο του δημοσίου κλειδιού του Κώστα, μια σύνδεση για τους λόγους που είναι σωστό αυτό το πιστοποιητικό και τις προσωπικές τους πιστοποιήσεις για τους λόγους που εκδόθηκε το πιστοποιητικό. Στέλνουν στο Κώστα ένα αντίγραφο του πιστοποιητικού και ένα αντίγραφο του ιδιωτικού του κλειδιού.

Ο Κώστας μετά στέλνει στη Μαρία ένα μήνυμα ηλεκτρονικού ταχυδρομείου μέσω του Διαδικτύου, με ένα αντίγραφο του κρυπτογραφημένου πιστοποιητικού με το ιδιωτικό του κλειδί και ένα αντίγραφο του δημοσίου κλειδιού του. Το κρυπτογραφημένο πιστοποιητικό είναι τώρα μια ψηφιακή υπογραφή από το Κώστα, που αποδεικνύει την ταυτότητα του. Αφού η Μαρία λάβει το μήνυμα, μπορεί να αποκρυπτογραφήσει τη ψηφιακή υπογραφή με το δημόσιο κλειδί που της δίνεται. Επειδή η CA έχει βεβαιώσει ότι το δημόσιο κλειδί δόθηκε στο Κώστα και η RA έχει πιστοποιήσει ότι ο Κώστας είναι πραγματικά ο Κώστας, η Μαρία ξέρει ότι αυτός ο κώδικας όχι μόνο θα διατηρήσει τις ιδιωτικές πληροφορίες που στέλνει αλλά το άτομο με το οποίο επικοινωνεί είναι πραγματικά ο Κώστας. Επειδή έγιναν όλα αυτά τα βήματα, η Μαρία μπορεί να αισθάνεται ασφαλής ότι δεν επικοινωνεί με κάποιον που υποκρίνεται το Κώστα και στέλνει ένα δεύτερο δημόσιο κωδικό. Η Μαρία κάνει ένα τελευταίο έλεγχο ασφαλείας στο πιστοποιητικό πηγαίνοντας στη βάση δεδομένων της CA για τα πιστοποιητικά που έχουν λήξει. Η Μαρία βεβαιώνεται ότι το πιστοποιητικό του Κώστα είναι καλό και τώρα ο Κώστας και η Μαρία είναι έτοιμοι να επικοινωνήσουν.

Ο Κώστας μπορεί να στείλει στη Μαρία μηνύματα κρυπτογραφημένα με το ιδιωτικό του κλειδί και η Μαρία μπορεί να τα αποκρυπτογραφήσει με τα δημόσιο κλειδί που υπήρχε προηγουμένως στη ψηφιακή υπογραφή του Κώστα. Η Μαρία μπορεί να διαβάσει το μήνυμα, να αποκριθεί και να κρυπτογραφήσει το μήνυμα της με το δημόσιο κλειδί, πριν το στείλει στο Κώστα. Όταν ο Κώστας λάβει το μήνυμα χρησιμοποιεί το ίδιο ιδιωτικό κλειδί, που χρησιμοποίησε για να κρυπτογραφήσει το μήνυμα στη Μαρία, για να αποκρυπτογραφήσει το μήνυμα που του έστειλε αυτή.

Έμπιστες Τρίτες Οντότητες

Με σκοπό τη διασφάλιση της ακεραιότητας των δεδομένων και προστασίας των πληροφοριών που διακινούνται στο δίκτυο αναπτύχθηκαν τα τελευταία χρόνια μηχανισμοί ασφαλείας με μικρό κόστος για τον τελικό χρήστη και δυνατότητα υλοποίησης ασφαλών πλέον ηλεκτρονικών συναλλαγών. Θεωρείται λοιπόν απαραίτητη η ύπαρξη μίας αρχής που θα εξασφαλίζει την εμπιστευτικότητα και αυθεντικότητα των συναλλαγών και θα προσφέρει υπηρεσίες Έμπιστης Τρίτης Οντότητας.

Μια Έμπιστη Τρίτη Οντότητα θα μπορούσε να οριστεί ως μία αρχή ασφαλείας ή μία υπηρεσία την οποία εμπιστεύονται άλλες οντότητες για την διασφάλιση των συναλλαγών τους, καθώς επίσης και για τις λειτουργίες – υπηρεσίες ασφαλείας που παρέχει. Μία Έμπιστη Τρίτη Οντότητα παρέχει τους μηχανισμούς εκείνους μέσω των οποίων εξασφαλίζεται η εμπιστευτικότητα, η ακεραιότητα και η αυθεντικότητα των ηλεκτρονικών συναλλαγών και των πληροφοριών που διακινούνται στο Δια-δίκτυο.

Μια ΕΤΟ προσδιορίζεται ως μία αρχή που εξυπηρετεί άλλες οντότητες. Οι οντότητες που πιστοποιούνται από μία ΕΤΟ μπορεί να περιλαμβάνουν τα άτομα που χρησιμοποιούν τις υπηρεσίες ενός οργανισμού, ή τους servers (εξυπηρετητές) του οργανισμού που προσφέρουν τις συγκεκριμένες υπηρεσίες. Μια Έμπιστη Τρίτη Οντότητα ενεργεί είτε ως :

- Αρχή Πιστοποίησης (Certification Authority), είτε ως
- Υπηρεσία Καταλόγου (Registration) στην οποία καταγράφονται οι χρήστες και πελάτες της ΕΤΟ.

Ένα κλασσικό σενάριο λειτουργίας μίας ΕΤΟ είναι το ακόλουθο: Ο τελικός χρήστης είναι συνδεδεμένος στο Web και μπορεί να επικοινωνήσει άμεσα με την Αρχή Πιστοποίησης, για να κάνει αίτηση ή να λάβει ένα νέο πιστοποιητικό. Ουσιαστικά το πιστοποιητικό αυθεντικοποιεί την ταυτότητα του χρήστη στους servers άλλων οργανισμών. Η λειτουργία της αυθεντικοποίησης πραγματοποιείται ως εξής: όταν ένας χρήστης πρόκειται να επικοινωνήσει με servers άλλων οργανισμών για να πραγματοποιήσει κάποια ηλεκτρονική συναλλαγή ή απλώς να πάρει κάποιες πληροφορίες, αποστέλλει το πιστοποιητικό του στους servers αυτούς. Στη συνέχεια οι servers (παραλήπτες), ελέγχουν την ορθότητα του πιστοποιητικού και αν εξακριβώσουν την αυθεντικότητα αυτού, τότε παραχωρούν στον χρήστη τα ανάλογα δικαιώματα πρόσβασης στον server. Η εξακρίβωση της αυθεντικότητας του πιστοποιητικού πραγματοποιείται με τον έλεγχο της ψηφιακής υπογραφής η οποία είναι ενσωματωμένη στο πιστοποιητικό και ανήκει στην Αρχή Πιστοποίησης.

Τα χαρακτηριστικά που πρέπει να διαθέτει μια ΕΤΟ, έτσι ώστε αυτή να θεωρείται αποτελεσματική και με σαφής, περιεκτική λειτουργία, μπορούν να συνοψισθούν στα ακόλουθα. Η ΕΤΟ θα πρέπει

- Να λειτουργεί με ασφάλεια
- Να λειτουργεί μέσα σε συγκεκριμένο πλαίσιο
- Να μπορεί να προσφέρει μεγάλο πλήθος διαφορετικών Υπηρεσιών
- Να ακολουθεί τα Ευρωπαϊκά ή τα διεθνή πρότυπα
- Να είναι σε θέση να παίζει το ρόλο του διαιτητή (διαμεσολαβητή)

Better Business Bureau (BBB)

Το BBB είναι ένας ιδιωτικός μη κερδοσκοπικός οργανισμός, ο οποίος παρέχει πληροφορίες για τις επιχειρήσεις, διευκολύνοντας έτσι τους καταναλωτές πριν προχωρήσουν σε αγορές. Το BBB ανταποκρίνεται σε εκατομμύρια τέτοιες απαιτήσεις κάθε χρόνο. Οι επιχειρήσεις οι οποίες συμμετέχουν στο πρόγραμμα του BBB έχουν ένα σήμα στην ιστοσελίδα τους το οποίο δηλώνει το <<ενδιαφέρον>> τους για τους πελάτες τους. Οι καταναλωτές μαθαίνουν για την επιχείρηση που τους ενδιαφέρει πατώντας με ένα κλικ το σήμα.

Βιομετρικοί Έλεγχοι:

Μια ευρεία περιοχή τεχνολογίας που καλείται βιομετρική χρησιμοποιεί κωδικοποιημένες εκδόσεις της φυσικής φωνής, του ματιού, του προσώπου, ή χαρακτηριστικά του προσώπου ή του χεριού για να αναγνωρίσει μοναδικά κάποιον. Ο βιομετρικός έλεγχος ορίζεται σαν «την αυτοματοποιημένη μέθοδο πιστοποίησης ταυτότητας του ατόμου βασισμένη σε φυσιολογικά χαρακτηριστικά ή χαρακτηριστικά συμπεριφοράς του» (Forte 1998). Η διαδικασία εγκατάστασης σχετίζει την ταυτότητα κάποιου με τα δικά του βιομετρικά χαρακτηριστικά. Το σύστημα χρησιμοποιεί αυτά τα χαρακτηριστικά για να πιστοποιήσει τη ταυτότητα.

SCAM: Fraud Watch dogs' στο διαδίκτυο

Στις ΗΠΑ υπάρχουν μερικές εταιρείες που λειτουργούν με πρότυπο το BBB - Better Business Bureau και έχουν αυτό-αποκαλεστεί "μαντρόσκυλα" κατά της οποιασδήποτε μορφής απάτης στο Διαδίκτυο. Μερικές από αυτές τις εταιρείες είναι νόμιμες, άλλες όχι. Η βασική τους αρχή είναι η προώθηση της ηθικής

επιχειρηματικής δραστηριότητας σε ολόκληρο τον κόσμο και η καλλιέργεια εμπιστοσύνης τόσο από την πλευρά των ιδιωτών όσο και από των εταιρειών για αγορά προϊόντων και υπηρεσιών μέσω Διαδικτύου. Διαθέτουν μία βάση δεδομένων που αποτελείται από παράπονα τα οποία οι καταναλωτές μπορούν να αναζητήσουν αναφορικά με την νομιμότητα και την εγκυρότητα μιας εταιρείας.

Όσες επιχειρήσεις επιθυμούν, μπορούν να γίνουν μέλη και να υποστηρίξουν τις ηθικές διαδικτυακές επιχειρησιακές πρακτικές καταβάλλοντας μια ετήσια συνδρομή.

ΚΕΦΑΛΑΙΟ Δ

ΗΛΕΚΤΡΟΝΙΚΟ ΕΜΠΟΡΙΟ & ΚΟΙΝΟΤΙΚΕΣ ΡΥΘΜΙΣΕΙΣ ΓΙΑ ΤΗ ΠΡΟΣΤΑΣΙΑ ΤΟΥ ΚΑΤΑΝΑΛΩΤΗ

Στο ερώτημα για το αν ο καταναλωτής ωφελείται από τη χρησιμοποίηση του Διαδικτύου για τις αγορές του η απάντηση μπορεί να είναι μόνο θετική, αν αγνοηθεί το θέμα της αποξένωσης του ατόμου και της απομόνωσης στο σπίτι του. Και αυτό γιατί μπορεί να επιτύχει κανείς πολύ χαμηλές τιμές, τεράστιες δυνατότητες επιλογής και ευελιξία στους τρόπους πληρωμής και τελικά συμμετέχει ο ενδιαφερόμενος σε μια διαδικασία ταχεία, φθηνή και εύκολη. Όμως πραγματική εκμετάλλευση των δυνατοτήτων που προσφέρει το Διαδίκτυο προς όφελος τόσο των καταναλωτών όσο και των επιχειρήσεων θα υπάρξει μόνο όταν εξασφαλιστεί κλίμα εμπιστοσύνης, επαρκής ασφάλεια στις συναλλαγές και ένα υψηλό επίπεδο προστασίας των καταναλωτών.

Τα νομικά προβλήματα που δημιουργούνται από την πραγματοποίηση αγορών με ηλεκτρονικά μέσα, λαμβάνοντας υπόψη και το γεγονός ότι πρόκειται κυρίως για διασυνοριακές συναλλαγές είναι πολλά. Ενδεικτικά αναφέρονται ζητήματα όπως υπό ποιες προϋποθέσεις και ποια χρονική στιγμή θεωρείται ότι καταρτίστηκε η σύμβαση, ποιο θα είναι το εφαρμοστέο για την επίλυση διαφορών δίκαιο και ποιας πολιτείας το δικαστήριο θα είναι αρμόδιο για την επίλυση τους, πως μπορούν να αντιμετωπιστούν οι κίνδυνοι από τη πληρωμή και ιδιαίτερα πως θα αποτραπεί η

καταχρηστική χρησιμοποίηση της πιστωτικής κάρτας του αποδέκτη των υπηρεσιών από τρίτους που έλαβαν γνώση του αριθμού της, πως θα προστατευτεί ο τελευταίος από τη διαρροή προσωπικών δεδομένων που υποχρεωμένος να δηλώσει για αν πραγματοποιήσει μια συναλλαγή, πως θα αποφευχθεί η διατάραξη της ιδιωτικής τους ζωής από τον κατακλυσμό εμπορικής ηλεκτρονικής αλληλογραφίας.

Η συνειδητοποίηση αυτών των προβλημάτων τα τελευταία χρόνια οδήγησε την Ευρωπαϊκή Ένωση αλλά και ορισμένους διεθνείς οργανισμούς στην πρόταση ή τη θέσπιση ομοιόμορφων κανόνων που ρυθμίζουν πολλά από τα σημαντικότερα θέματα του ηλεκτρονικού εμπορίου.

Η UNCITRAL έχει δημιουργήσει το νόμο-υπόδειγμα για το ηλεκτρονικό εμπόριο του 1996. Ο ΟΟΣΑ έχει καταρτίσει πρόταση για την φορολογία στο Διαδίκτυο. Ο Παγκόσμιος Οργανισμός Εμπορίου έχει ήδη από το 1980 παρουσιάσει οδηγίες για την προστασία της ιδιωτικής ζωής και την διασυνοριακή ροή προσωπικών δεδομένων. Το Συμβούλιο της Ευρώπης έχει καταρτίσει σύμβαση για την προστασία των ατόμων σε σχέση με την συλλογή και επεξεργασία προσωπικών δεδομένων στο Διαδίκτυο. Το Διεθνές Εμπορικό Επιμελητήριο έχει καταρτίσει όρους-υποδείγματα για χρήση σε συμβάσεις που σχετίζονται με την διασυνοριακή ροή δεδομένων και έχει εκδώσει αναμορφωμένες οδηγίες για την διαφήμιση και το marketing στο Διαδίκτυο. Στην Ευρωπαϊκή Ένωση η προσπάθεια που καταβάλλεται είναι μεγάλη για να ρυθμιστούν ζητήματα που αφορούν συναλλαγές στο Διαδίκτυο και χρήζουν άμεσης αντιμετώπισης. Μάλιστα, η Ευρωπαϊκή Ένωση σε σχέση με τις ΗΠΑ, που είναι ο μεγαλύτερος χρήστης του Διαδικτύου θεωρείται πρωτοπόρος στις προσπάθειες ρύθμισης ζητημάτων του ηλεκτρονικού εμπορίου.

Με την ανάπτυξη της ηλεκτρονικής τεχνολογίας βρισκόμαστε ήδη σε μια περίοδο όπου στις εμπορικές συναλλαγές ο έγγραφος τύπος έχει εν πολλοίς αντικατασταθεί από τις ηλεκτρονικές εγγραφές. Για να γίνει όμως αποδεκτή βασική προϋπόθεση είναι η εξασφάλιση της γνησιότητας της, η οποία για να εξακριβωθεί προϋποθέτει την υπογραφή του προσώπου από το οποίο προέρχεται. Το ζήτημα είναι αν η ηλεκτρονική υπογραφή μπορεί να εξομοιωθεί με την ιδιόχειρη.

Οι κανόνες που διέπουν τη νομική αναγνώριση των ψηφιακών υπογραφών και τη διαπίστευση «παροχών υπηρεσιών πιστοποίησης» μπορούν να διαφέρουν από χώρα σε χώρα της Κοινότητας, πράγμα το οποίο μπορεί να δημιουργήσει φραγμούς στο ηλεκτρονικό εμπόριο, ενώ ένα κοινοτικό θεσμικό πλαίσιο ενισχύει την εμπιστοσύνη στις νέες τεχνολογίες και προωθεί την ελεύθερη κυκλοφορία των αγαθών και υπηρεσιών μέσα στην Ευρωπαϊκή Ένωση, κρίθηκε απαραίτητη από το Κοινοτικό Νομοθέτη η ρύθμιση του θέματος των ηλεκτρονικών υπογραφών με Οδηγία. Η οδηγία θεσπίζει το θεσμικό πλαίσιο που εξασφαλίζει τη νομική αναγνώριση των ηλεκτρονικών υπογραφών σε όλη την Ευρωπαϊκή Κοινότητα, καθώς και τα θέματα των υπηρεσιών πιστοποίησης.

ΕΡΕΥΝΑ - ΑΠΟΤΕΛΕΣΜΑΤΑ

Πραγματοποιήθηκε μια δημοσκόπηση σχετικά με το «Ηλεκτρονικό Εμπόριο και την Ασφάλεια του». Στάλθηκαν 100 ερωτηματολόγια (βλέπε παρακάτω ερωτηματολόγιο) σε υπεύθυνους (IT) μηχανογραφικών τμημάτων. Οι απαντήσεις που δόθηκαν αναλύονται στη συνέχεια.

ΕΡΩΤΗΜΑΤΟΛΟΓΙΟ

1. Η εταιρεία σας έχει site και κάθε πόσο συχνά το ανανεώνεται;

2. Δίνεται τη δυνατότητα στους πελάτες σας εμπορικών συναλλαγών μέσω του site σας; (on-line & off-line)

   ΐΝΑΙ ΐΟΧΙ

3. Αν ναι, αυτές οι υπηρεσίες είναι on-line ή off-line;

   ΐ On-line ΐ Off-line

4. Αν όχι, για ποιους λόγους;

5. Η εταιρεία πραγματοποιεί περισσότερες συναλλαγές

   ΐΜε ιδιώτες ΐ Εταιρείες ή ΐΚαι τα δυο

6. Δίνεται τη δυνατότητα πληρωμής μέσω διαδικτύου;

   ΐΝΑΙ ΐΟΧΙ

7. Η εταιρεία σας πραγματοποιεί ηλεκτρονικές συναλλαγές για τη τροφοδοσία της;

   ΐΝΑΙ ΐΟΧΙ

8. Το ηλεκτρονικό σας κατάστημα είχε θετικά αποτελέσματα τόσο οικονομικά όσο και προωθητικά;

Οικονομικά: ΐΠολύ ΐΛίγο ΐΑρκετά ΐΚαθόλου

Διαφήμιση: ΐΠολύ ΐΛίγο ΐΑρκετά ΐΚαθόλου

9. Θεωρείται την ασφάλεια ανασταλτικό παράγοντα ανάπτυξης του Η/Ε;

ΝΑΙ ΟΧΙ

10. Ποιους μηχανισμούς ασφαλείας χρησιμοποιείται;

11. Έχετε δεχθεί επίθεση στο σύστημά σας;

ΝΑΙ ΟΧΙ

12. Πιστεύεται ότι οι εταιρείες έχουν ασφαλή συστήματα συναλλαγών;

ΝΑΙ ΟΧΙ

13. Σημειώστε με βαθμό σπουδαιότητας ποια από τα παρακάτω εμποδίζουν την εξάπλωση του Η/Ε:

Κόστος

Έλλειψη τεχνολογικών γνώσεων

Μηχανογραφική δυνατότητα των εταιρειών

Ασφάλεια

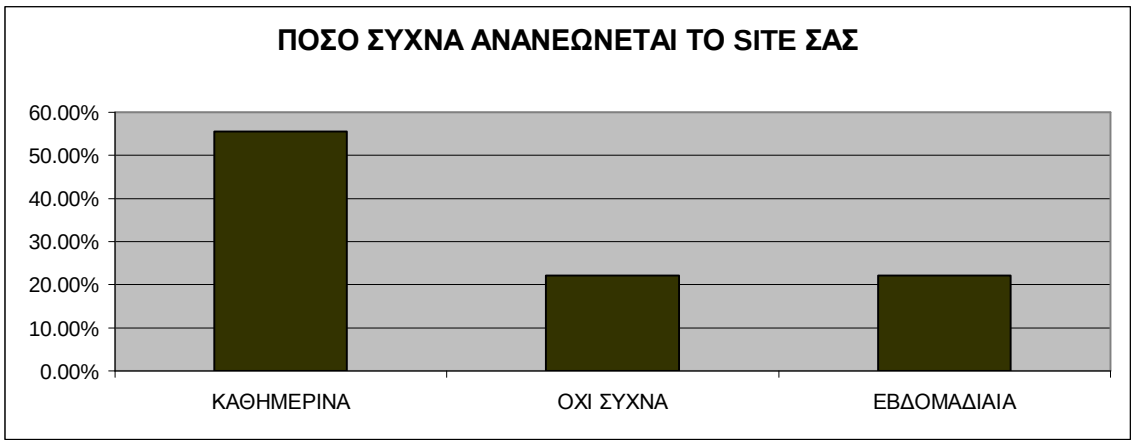
Νομικά ζητήματα

Έλλειψη αφής (Αδυναμία προσωπικής επαφής με το προϊόν)

Έλλειψη εμπιστοσύνης

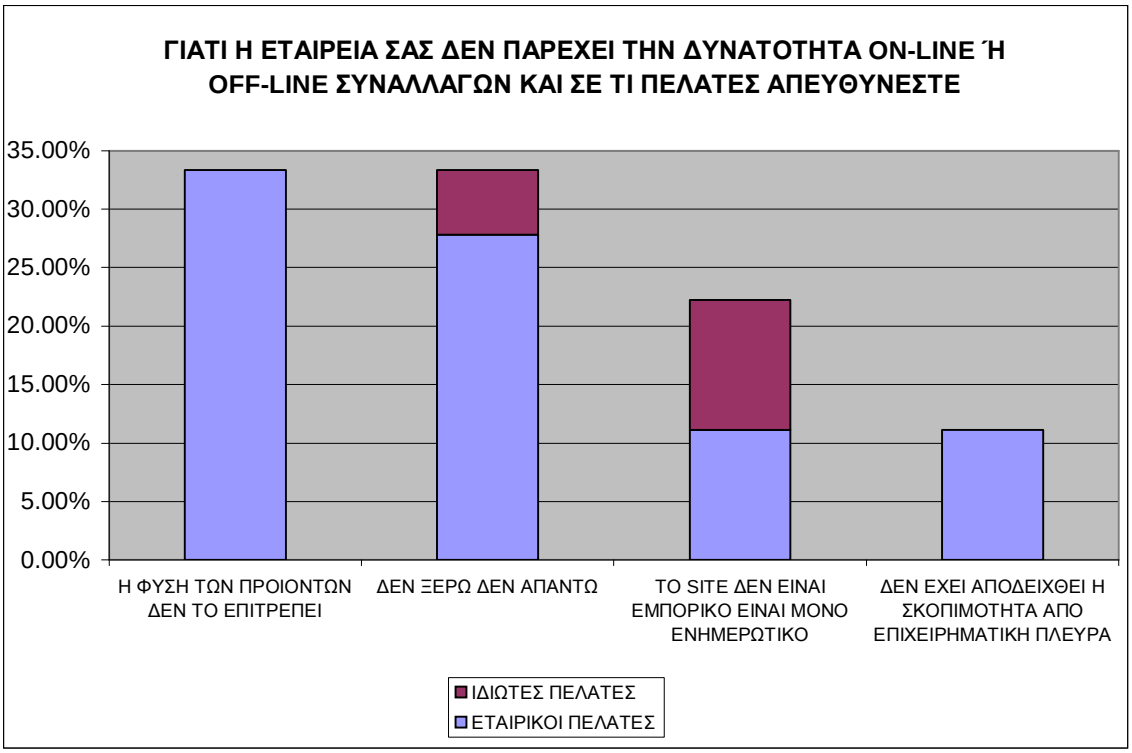
ΑΠΟΤΕΛΕΣΜΑΤΑ

1. Στη ερώτηση εάν έχετε ιστοσελίδα και κάθε πόσο την ανανεώνεται, το 55% απάντησε καθημερινά, ενώ το 22% εβδομαδιαία και το άλλο 22% όχι συχνά.

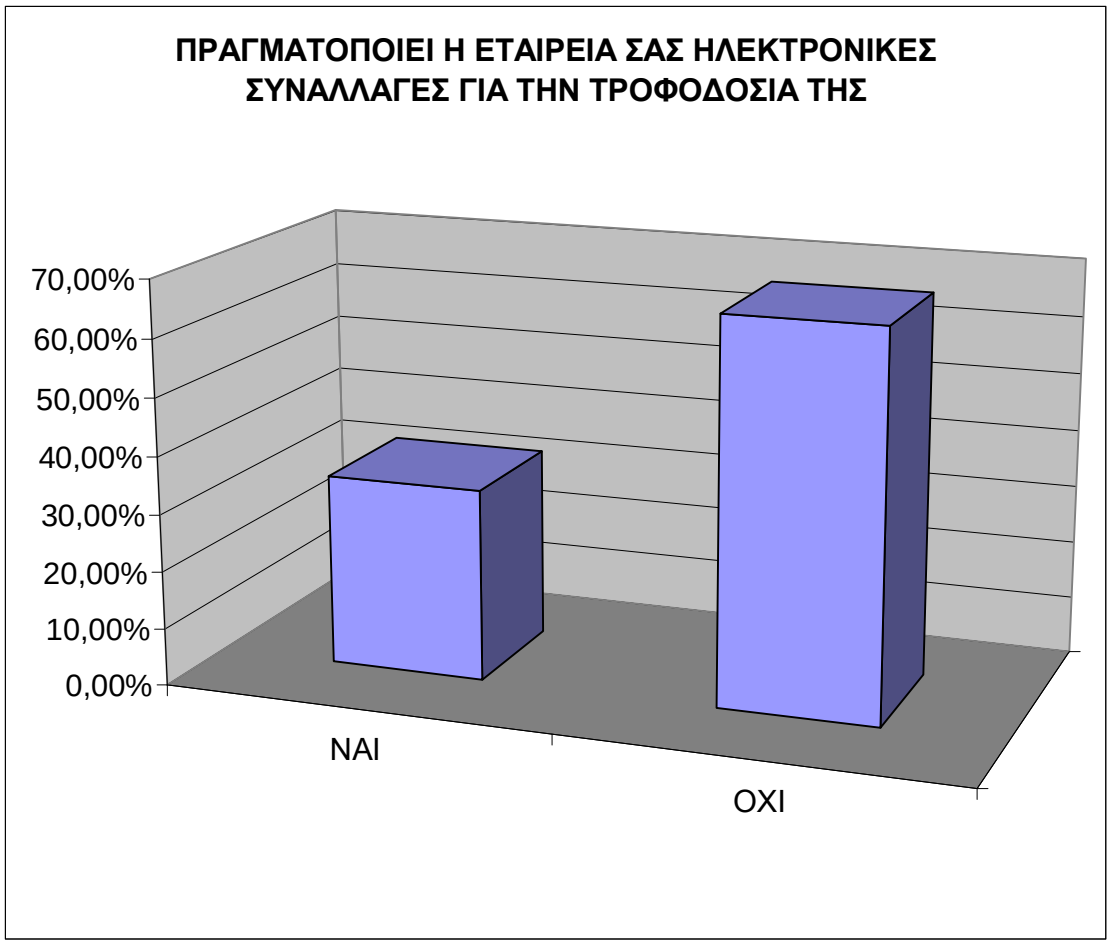


2. Στη ερώτηση εάν δίνεται στους πελάτες τη δυνατότητα on-line ή off-line συναλλαγών το 89% απάντησε ότι δεν παρέχει αυτή τη δυνατότητα.

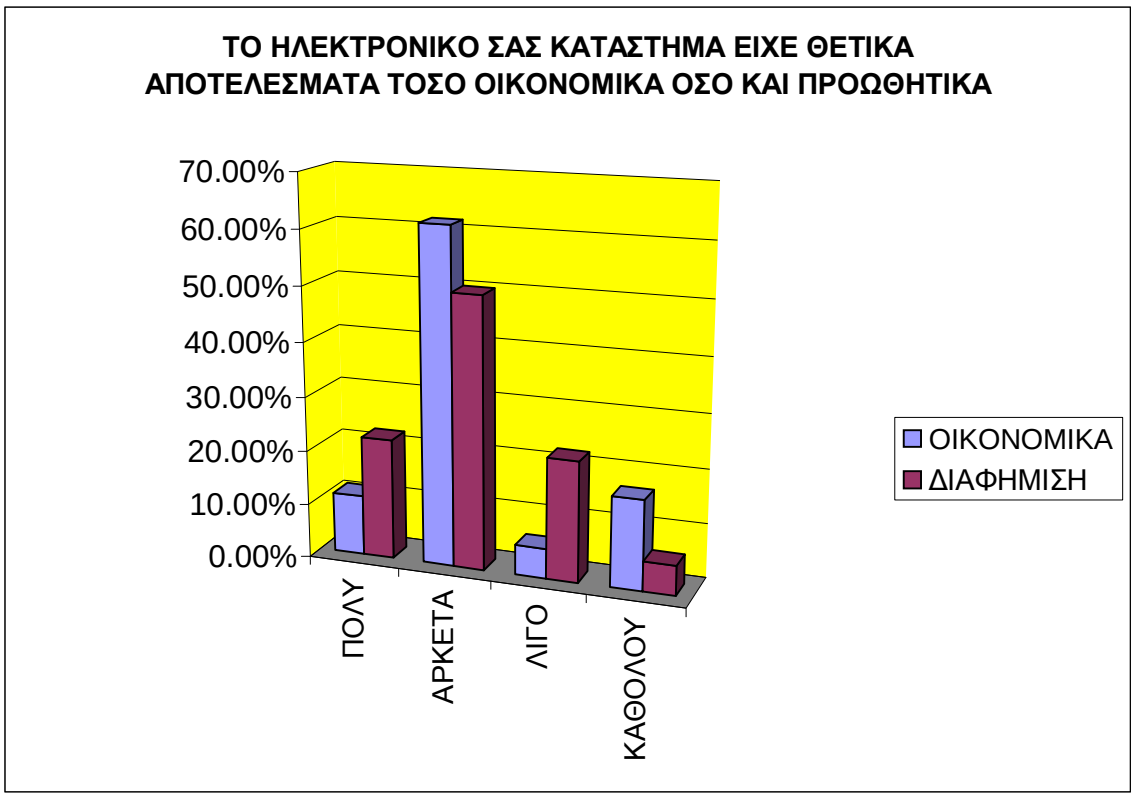
3. Στην ερώτηση γιατί η εταιρεία δεν παρέχει τη δυνατότητα on-line ή off-line συναλλαγών και σε τι πελάτες απευθύνεστε, το 32% απάντησε ότι η φύση των προιόντων τους δεν τους παρέχει τη δυνατότητα να έχουν on-line ή off-line συναλλαγές και απευθύνονται σχεδόν κατά αποκλειστικότητα σε εταιρικούς πελάτες. Το 22% απάντησε ότι η ιστοσελίδας τους είναι ενημερωτική και όχι εμπορική, ενώ οι πελάτες στους οποίους απευθύνονται είναι 50% εταιρικοί και 50% ιδιώτες. Το 11% δεν έχει προχωρήσει στη δυνατότητα on-line ή off-line συναλλαγές αφού δεν έχει κρίνει σκόπιμο από επιχειρηματική πλευρά το εγχείρημα και οι πελάτες στους οποίους απευθύνεται είναι κατά αποκλειστικότητα εταιρικοί.



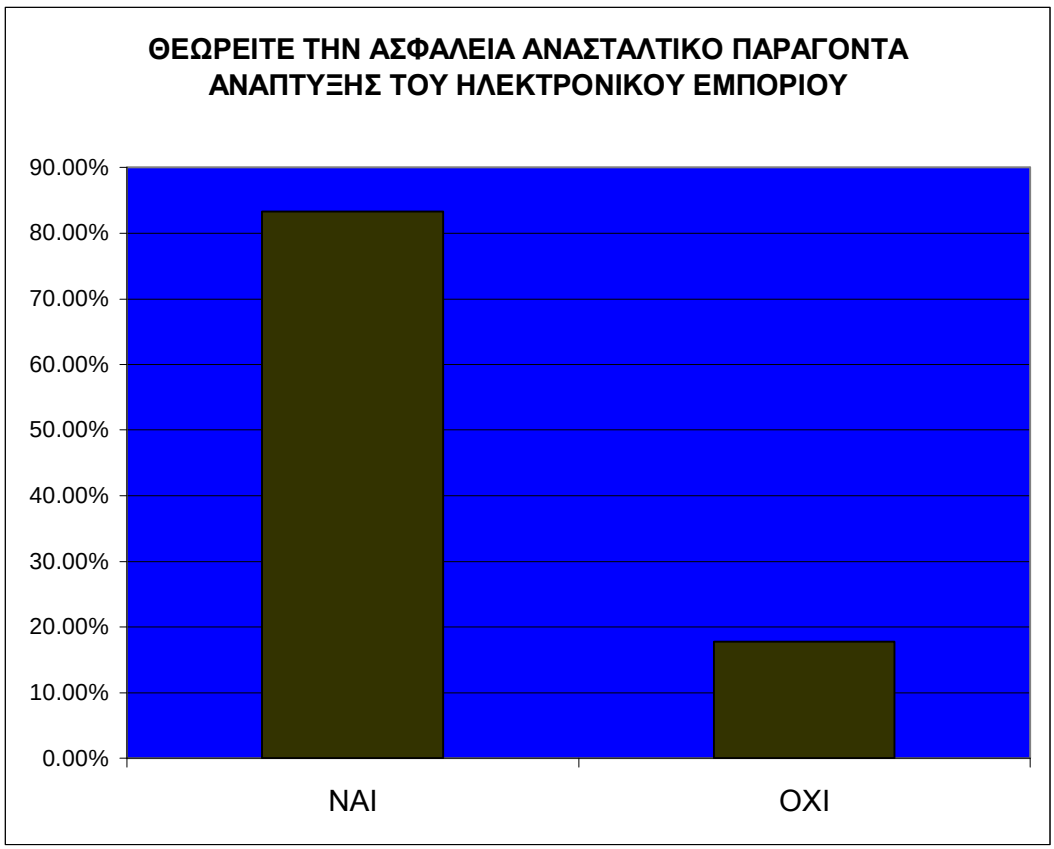
4. Στη δεύτερη ερώτηση περίπου το 60% απάντησε ότι δεν έχει εμπορικές συναλλαγές μέσω της ιστοσελίδας τους.



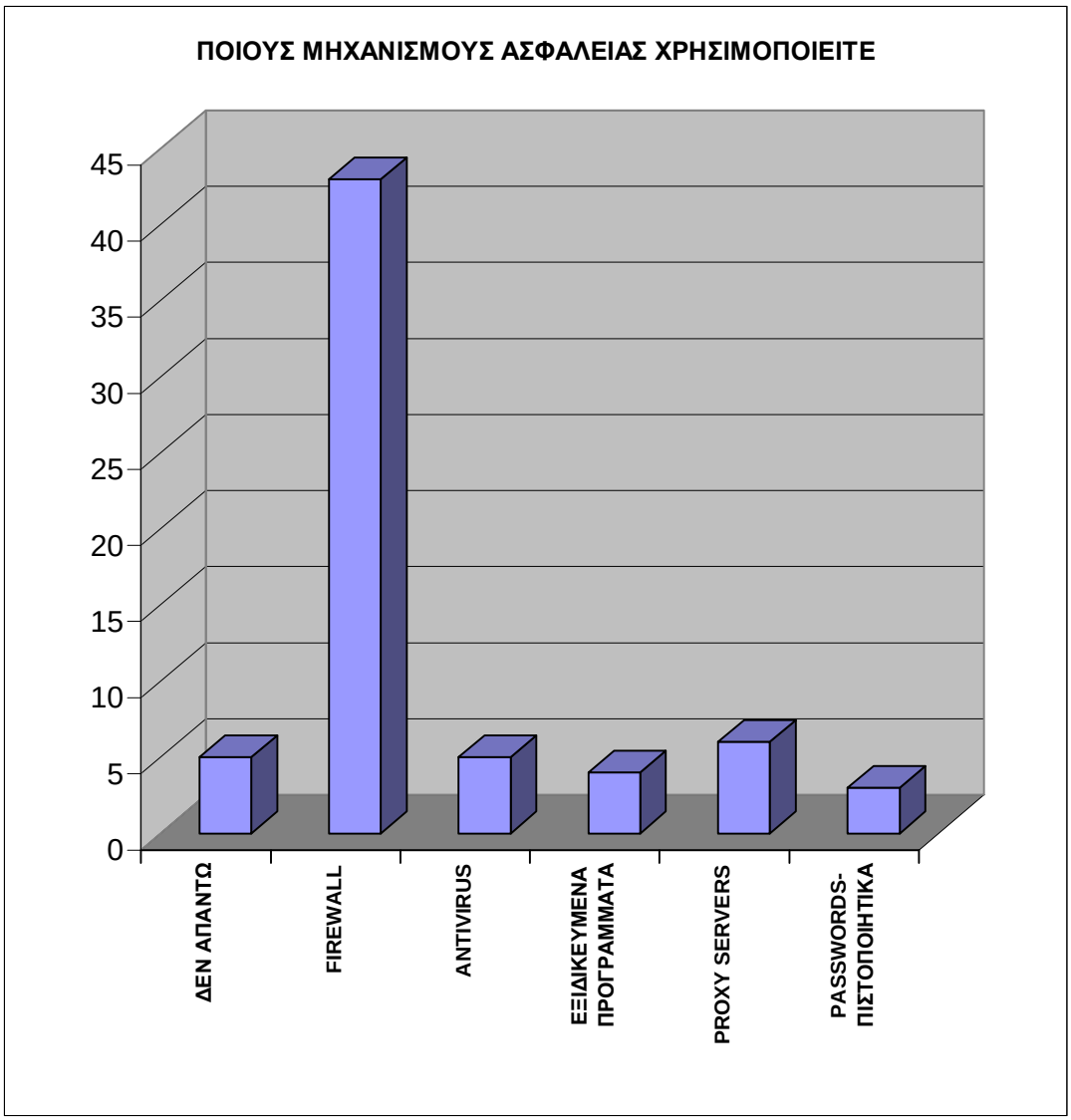
5. Στην ερώτηση «το ηλεκτρονικό κατάστημα είχε θετικά αποτελέσματα τόσο οικονομικά όσο και προωθητικά» το μεγαλύτερο ποσοστό(50%-60%) απάντησε αρκετά τόσο οικονομικά όσο και προωθητικά. Το 20% απάντησε ότι βοήθησε πολύ προωθητικά ενώ μόνο το 10% αντίστοιχα οικονομικά. Αντίθετα το 15% απάντησε ότι δεν βοηθήθηκε καθόλου οικονομικά, με μόνο το 5% να απαντάει ότι δεν βοηθήθηκε καθόλου προωθητικά.



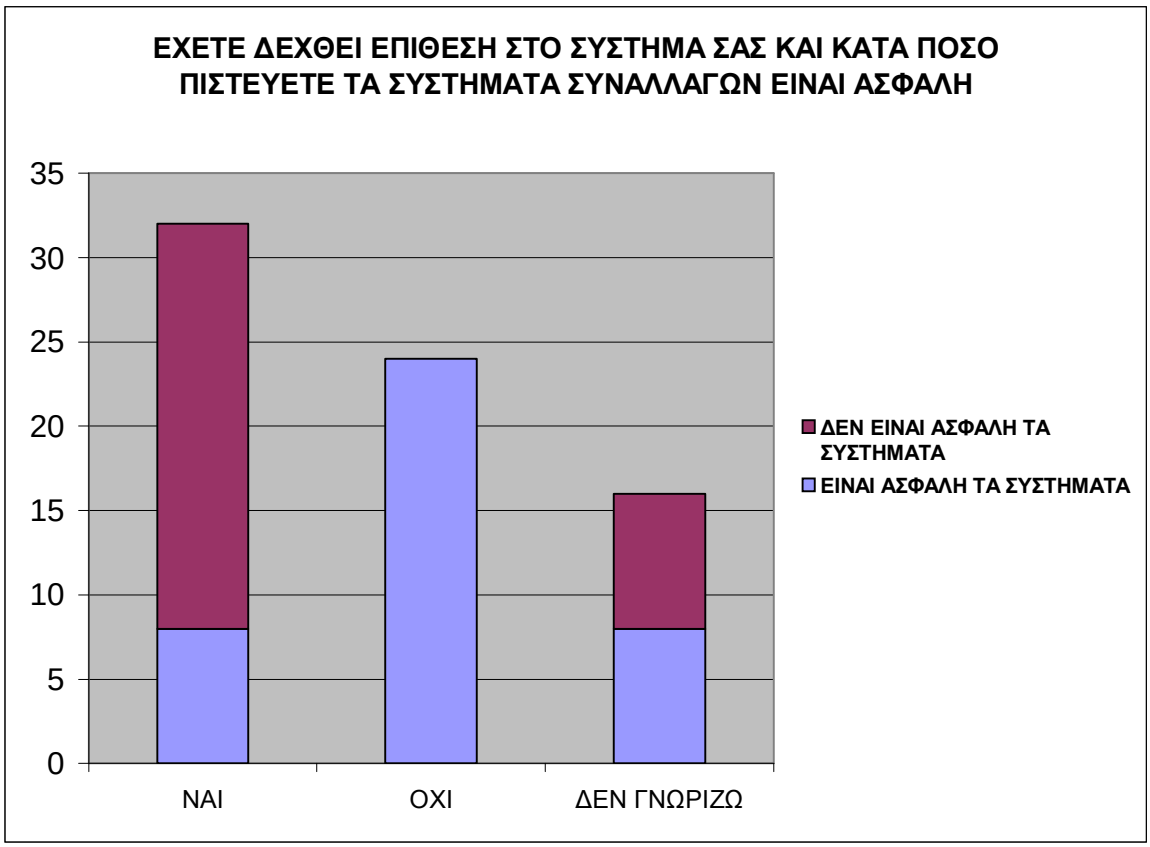
6. Στην ερώτηση «θεωρείται την ασφάλεια ανασταλτικό παράγοντα ανάπτυξης ηλεκτρονικού εμπορίου», το 83% απάντησε θετικά.



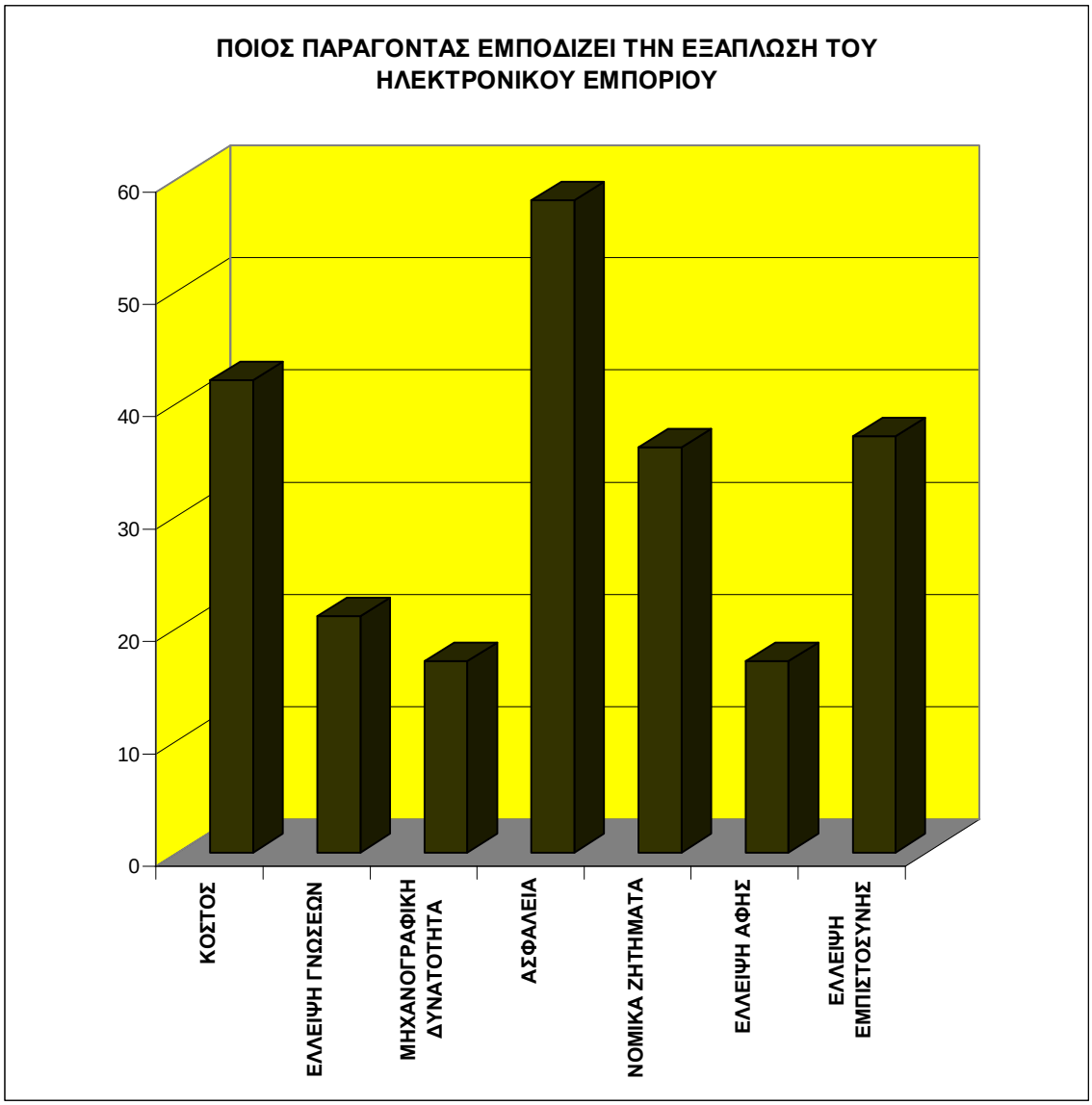
7. Η έρευνα απέδειξε ότι το 45% χρησιμοποιεί για μηχανισμό ασφαλείας τα ηλεκτρονικά τείχη (firewalls),το 5% proxy servers ενώ σε μικρότερα ποσοστά χρησιμοποιούν αντιβιοτικά προγράμματα, πιστοποιητικά – κωδικοί πρόσβασης και εξειδικευμένα προγράμματα. Υπήρχε ένα ποσοστό περίπου 4% που δεν απάντησαν.



8. Το παραπάνω σχεδιάγραμμα μα ενημερώνει ότι περίπου το 32% έχει δεχθεί επίθεση, από τους οποίους το 1/5 πιστεύει ότι τα συστήματα είναι ασφαλή, ενώ τα άλλα 4/5 όχι. Το 24% απάντησε ότι δεν έχει δεχθεί επίθεση, ενώ το 16% δεν γνωρίζουν εάν έχουν δεχθεί επίθεση.



9. Το 60% περίπου υποστηρίζουν ότι η ασφάλεια είναι ο πιο σημαντικός παράγοντας που εμποδίζει την εξάπλωση του Η/Ε. Στη συνέχεια το 40% ισχυρίζεται ότι το κόστος είναι εμπόδιο ανάπτυξης του Η/Ε. Ακολουθεί με 35% ο παράγοντας έλλειψη εμπιστοσύνης με ελάχιστη διαφορά με το παράγων «νομικά ζητήματα».



ΠΑΡΑΡΤΗΜΑ

Συμβουλές για να αποφεύγετε τις πλαστές αγορές στο Internet

1. Ποτέ μην αγοράζετε προϊόντα μέσω διαφημιστικών φυλλαδίων (φει-βολάν). Οι στατιστικές λένε ότι οι πιθανότητες να παραλάβετε τα προϊόντα που αγοράσατε είναι μόνο 45% και η πιθανότητα να είναι τα προϊόντα όπως τα περιμένετε και σε καλή τιμή είναι λιγότερο από 5%.
2. Πάντοτε να χρησιμοποιείτε την πιστωτική σας κάρτα για αγορές on-line. Αυτό είναι μία επιπλέον προστασία. Το μεγαλύτερο ποσό που μπορεί να χάσετε είναι $50 και τις περισσότερες φορές δεν θα χάσετε ούτε και αυτά εάν αποδειχθεί ότι πέσατε θύμα απάτης.
3. Εάν κάνετε μία αγορά μέσω μίας γνωστής και αξιόπιστης ιστοσελίδας δημοπρασιών, πάντοτε να ελέγχετε τις συστάσεις και τα πιστοποιητικά των πωλητών και να επιλέγετε μονάχα πωλητές με καλές συστάσεις. Καλό είναι επίσης να εκμεταλλεύεστε τις εγγυήσεις που προσφέρονται σε on-line πωλήσεις, όπως αυτές που προσφέρονται από την Amazon.com.
4. Αποφεύγετε τις συναλλαγές με ανώνυμους χρήστες. Ζητήστε το πραγματικό όνομα του ατόμου, το όνομα της επιχείρησης, διεύθυνση και αριθμό τηλεφώνου. Επαληθεύσατε αυτές τις πληροφορίες πριν προχωρήσετε σε κάποια αγορά. Και κυρίως ποτέ μη στέλνετε πληρωμές σε ταχυδρομική θυρίδα.
5. Να είσαστε ιδιαίτερα προσεκτικοί εάν ο πωλητής χρησιμοποιεί δωρεάν e-mail υπηρεσίες, όπως π.χ hotmail, yahoo κλπ. Βέβαια, πολλοί άνθρωποι που χρησιμοποιούν αυτές τις δωρεάν υπηρεσίες είναι έντιμοι, όμως πάρα πολλά προβλήματα συνήθως προκύπτουν όταν χρησιμοποιείται μία δωρεάν υπηρεσία. Σε μια τέτοια περίπτωση είναι πολύ εύκολο για τον πωλητή να κρατήσει κρυφή την πραγματική του ταυτότητα.

6. Να κρατάτε αντίγραφα όλων των e-mails και των εγγράφων που χρησιμοποιήθηκαν στη συναλλαγή διότι εάν ανακαλύψετε ότι ένα προϊόν είναι πλαστό, θα έχετε κάποια αποδεικτικά στοιχεία που θα σας βοηθήσουν να αντιμετωπίσετε το πρόβλημα.
7. Χρησιμοποιήστε κοινή λογική και εμπιστευθείτε τη διαίσθησή σας. Εάν διατηρείτε κάποιες αμφιβολίες για ένα προϊόν, μην το αγοράσετε, είναι πιθανόν η διαίσθησή σας να σας δικαιώσει.

15 Συμβουλές που θα σας βοηθήσουν να αξιολογήσετε εάν μια εταιρεία ή μια προσφορά είναι νόμιμη και αυθεντική.

1) Πάντοτε να χρησιμοποιείτε την λογική και το ένστικτό σας. Εάν σας δημιουργηθεί η εντύπωση ότι κάτι δεν είναι έγκυρο, το πιθανότερο είναι ότι έχετε δίκιο.
2) Επιβεβαιώσατε ότι η εταιρεία έχει αριθμό κινητού τηλεφώνου και πραγματική διεύθυνση. Κάντε ένα δοκιμαστικό τηλεφώνημα. Ελέγξατε μέσω της υπηρεσίας πληροφοριών εάν ο αριθμός όντως ανήκει στη συγκεκριμένη εταιρεία.
3) Πάντοτε να ζητάτε συστάσεις και να τις ελέγχετε προσεκτικά. Μία αξιόπιστη και σωστή εταιρεία θα σας στείλει με προθυμία συμπληρωματικές πληροφορίες και θα σας δώσει όσες συστάσεις ζητήσετε από ικανοποιημένους πελάτες.
4) Ζητήστε να μάθετε που είναι καταχωρημένη η εταιρεία αυτή, εάν π.χ είναι μέλος κάποιου επιμελητηρίου κ.λ.π.

5) Αναζητήστε μέσω κρατικών φορέων πληροφορίες για υπάρχουσες καταγγελίες εναντίον της εταιρείας.

6) Απευθυνθείτε στο Εθνικό Κέντρο Πληροφόρησης για απάτες πχ στις ΗΠΑ στο National Fraud Information Center στο http://www.fraud.org όπου μπορείτε να πληροφορηθείτε για τηλεφωνικούς, ταχυδρομικούς και on line απατεώνες.

7) Πάντοτε να εξασφαλίζετε κάποια μορφή ισχυρής εγγύησης. Ζητήστε να μάθετε τι διαδικασίες ισχύουν εάν θελήσετε να επιστρέψετε το προϊόν ή την υπηρεσία που θα αγοράσετε. Μπορείτε επιπρόσθετα να ζητήσετε συστάσεις από καταναλωτές που επέστρεψαν το προϊόν και τους επεστράφησαν χρήματα.

8) Να είστε επιφυλακτικοί σε πωλητές που ασκούν μεγάλη πίεση να αγοράσετε άμεσα. Οι scamsters πάντοτε θέλουν τα λεφτά σας αμέσως. Δεν θέλουν να σας αφήσουν περιθώριο να σκεφθείτε καλά πριν αποφασίσετε. Εάν σας πιέσουν να αποφασίσετε αμέσως, καλύτερα να αρνηθείτε.

9) Πληρώνετε πάντοτε με πιστωτική κάρτα. Σας δίνει τη δυνατότητα νομικής προσφυγής εάν αντιμετωπίσετε κάποιο πρόβλημα. Εάν πληρώσετε με πιστωτική κάρτα και εμφανιστεί κάποιο πρόβλημα μπορείτε να καλέσετε την τράπεζα σας και να ζητήσετε ανάκληση της πληρωμής. Αποφύγετε να δώσετε τον αριθμό της πιστωτικής σας κάρτας ελεύθερα ιδίως μέσω ηλεκτρονικού ταχυδρομείου.

10) Μην απαντάτε σε μαζικής μορφής e-mail. Να είστε επιφυλακτικοί όταν σας στέλνουν προσφορές γραμμένες με κεφαλαία γράμματα και πολλά θαυμαστικά.
11) Πάντοτε να συνηθίζετε να τυπώνετε ένα hardcopy από όλες τις προσφορές που σας ενδιαφέρουν. Κρατήστε τη διεύθυνση e-mail, τη διεύθυνση διαδικτύου και όσες σημαντικές πληροφορίες κρίνετε σκόπιμο, όπως πχ την ημέρα και ώρα που είδατε την προσφορά, ώστε να τα έχετε διαθέσιμα εάν τα χρειαστείτε αργότερα.
12) Προσοχή στους διαφημιστές που προσπαθούν να σας πουλήσουν πράγματα χρησιμοποιώντας μία ανώνυμη διεύθυνση e-mail όπως anon1234@anon.company.com, user@domain.com ή σε μια διεύθυνση ταχυδρομικής θυρίδας.
13) Μη συμμετέχετε σε σχήματα *πυραμίδας.* Πχ εάν σας ζητήσουν να στείλετε χρήματα σε 10 άτομα εκ των οποίων ο καθένας θα πρέπει να στείλει χρήματα σε άλλα δέκα άτομα κλπ.
14) Εάν σας ανακοινώσουν ότι κερδίσατε ένα βραβείο να είστε επιφυλακτικοί. Εάν πρέπει να πληρώσετε κάποιο ποσό για να το παραλάβετε, πάντοτε να αρνείστε το βραβείο.
15) Γίνετε συνδρομητής των Internet Scam busters.

Οκτώ βήματα για να μειωθεί η απάτη των πιστωτικών καρτών για τους εμπόρους.

1) Προσπαθήστε να διασταυρώσετε τις ανταλλασσόμενες πληροφορίες που αφορούν την ταυτότητα και των δύο πλευρών. Μην επιβεβαιώνετε

παραγγελίες εάν δεν έχετε εξακριβώσει την βασιμότητα των πληροφοριών που αφορούν το έτερο συναλλασσόμενο μέρος πχ πλήρη διεύθυνση και αριθμό τηλεφώνου.

2) Να είστε ιδιαίτερα προσεκτικοί όταν παίρνετε παραγγελίες, όπου η διεύθυνση τιμολόγησης είναι διαφορετική από αυτή της αποστολής. Καλό θα είναι να ζητάτε από τον πελάτη σας να σας στέλνει συμπληρωματικά ένα φαξ με την υπογραφή του και τον αριθμό της πιστωτικής του κάρτας καθώς και να εξουσιοδοτεί την συναλλαγή.

3) Να είστε ιδιαίτερα προσεκτικοί με τις παραγγελίες που προέρχονται από δωρεάν υπηρεσίες ηλεκτρονικού ταχυδρομείου - υπάρχει πολύ μεγαλύτερος κίνδυνος απάτης από αυτές τις υπηρεσίες (πχ. hotmail.com, juno.com, usa.net). Πολλές επιχειρήσεις δεν κάνουν αποδεκτές πλέον όσες παραγγελίες προέρχονται από τέτοιους λογαριασμούς. Και αυτό διότι είναι τόσο εύκολο για έναν scamster να ανοίξει έναν δωρεάν ανώνυμο λογαριασμό e-mail στο όνομα ενός άλλου ατόμου και μετά να στείλει σε εσάς τον έμπορο, μία παραγγελία.

   Μπορείτε βέβαια να ζητήσετε κάποιες συμπληρωματικές πληροφορίες όταν λαμβάνετε παραγγελίες από λογαριασμούς που προέρχονται από δωρεάν e-mail, όπως πχ το όνομα και το τηλέφωνο της τράπεζας που εξέδωσε την πιστωτική κάρτα, το ακριβές όνομα κατόχου της πιστωτικής κάρτας, και την ακριβή διεύθυνση όπου θα σταλεί το τιμολόγιο. Συχνά μπορεί να μη λάβετε καν απάντηση. Εάν όμως λάβετε θα μπορέσετε εύκολα να επιβεβαιώσετε τις πληροφορίες.

4) Να είστε ιδιαίτερα προσεκτικοί εάν οι παραγγελίες που λαμβάνετε είναι κάπως μεγαλύτερες σε αξία από αυτές που λαμβάνετε συνήθως και με αυτές που ζητούν παράδοση την επομένη ημέρα. Οι απατεώνες συνήθως δεν απασχολούνται με την αξία της παραγγελίας αφού έτσι κι αλλιώς δεν είναι διατεθειμένοι να τις πληρώσουν.
5) Να είστε προσεκτικοί με τις παραγγελίες που προέρχονται από το εξωτερικό. Πάρτε όλες τις απαραίτητες προφυλάξεις πριν αποστείλετε τα προϊόντα σας σε μία χώρα του εξωτερικού, και ιδιαίτερα όταν η διεύθυνση της τιμολόγησης διαφέρει από αυτήν της παράδοσης.
6) Εάν κάτι σας κινεί υποψίες, επιβεβαιώστε την παραγγελία καλώντας τηλεφωνικά τον πελάτη σας. Είναι ένα μέτρο που μακροπρόθεσμα θα εξοικονομήσετε χρήματα.
7) Σκεφθείτε σοβαρά την αγορά λογισμικού ή σχετικών υπηρεσιών που θα σας εξασφαλίσουν απέναντι σε τέτοιας μορφής απάτες.
8) Εάν εσείς ως έμπορος πέσετε θύμα ενός scamster που έχει κλέψει κάποια πιστωτική κάρτα, θα πρέπει να επικοινωνήσετε με τον φορέα έκδοσης της συγκεκριμένης πιστωτικής κάρτας. Πολλές φορές οι κάτοχοι πιστωτικών καρτών δεν έχουν καν πάρει είδηση ότι έχουν χάσει την κάρτα τους.

ΒΙΒΛΙΟΓΡΑΦΙΑ

1) Αρσένης Πασχόπουλος & Παναγιώτης Σκαλτσάς (2001) «Ηλεκτρονικό Εμπόριο / Ανάπτυξη και Εφαρμογή Επιχειρηματικής Στρατηγικής και Marketing στο Διαδίκτυο»
   Εκδόσεις Κλειδάριθμος

2) Frank J.Derfler και οι εκδότες του PC Magazine «e-Business / Επιχειρηματικές Εφαρμογές στο Internet»
   Εκδόσεις Β.Γκοιύρδας Εκδοτική

3) Β. ΜΑΣΣΕΛΟ (2000) «Οδηγός Ηλεκτρονικού Εμπορίου»

4) G.Winfield Treese & Lawrence C. Stewart (1998) «Designing Systems for Internet Commerce»
   Addison Wesley Longman Inc

5) Hahn, Harley (1994) «The Internet Complete Reference»

6) Robert C.Elsenpeter & Toby J. Velte (2001) «e - ΕΠΙΧΕΙΡΕΙΝ»
   Εκδότης: Μ. Γκιούρδας

7) E.Turban, J.Lee, D.king, H.M.Chung (2000) «Electronic Commerce»
   Prentice Hall International,Inc.

8) Λάμπρος Λάιος – Σωκράτης Μοσχούρης «Εφαρμογή του E-COMMERCE στην αλυσίδα εφοδιασμού. Τι είδους δραστηριότητες διευκολύνονται;»

9) Μαρία Στυλιανίδου «Ηλεκτρονικό Εμπόριο & Κοινοτικές ρυθμίσεις για τη προστασία του καταναλωτή»

10)«Set Secure Electronic Transaction LLC Home page» 1999 (www.setco.org)

11)Freeman L. «Net Drives B2B to new Highs Worldwide» Net Marketing (www.netb2b.com)

12)ΚΕ.Δ.Δ – Εκπαιδευτικό Υλικό «Η λειτουργία του Internet» (www.noc.uom.gr)

13)«Report on background and Issues of Cryptography Policy» (www.1oecd.org)

14)«Secure Mail and S/MIME Public-Key Cryptography - Digital Certificates» **(**www.aspencrypt.com)

15)«Digital Certificates and the Columbia Certificate Authority» (www.columbia.edu)

16)«Εταιρεία διασφάλισης ιστοσελίδων» (www.verisign.com)

17)«Εταιρεία διασφάλισης ιστοσελίδων» (www.belsign.be)