Η ΚΡΥΠΤΟΓΡΑΦΙΑ ΤΩΝ ΗΛΕΚΤΡΟΝΙΚΩΝ ΣΥΝΑΛΛΑΓΩΝ

ΑΝΔΡΙΑΝΑ ΛΙΝΑΡΔΟΥ

ΣΤΑΥΡΟΣ ΙΑΣΙΜΟΠΟΥΛΟΣ

Πτυχιακή εργασία που υποβάλλεται προς μερική εκπλήρωση των απαιτήσεων για την απόκτηση του πτυχίου

ΔΙΟΙΚΗΣΗΣ ΕΠΙΧΕΙΡΗΣΕΩΝ

ΑΝΩΤΑΤΟ ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ (Α.Τ.Ε.Ι.) ΠΑΤΡΑΣ

2005

Εγκρίθηκε από τον: Βλαχόπουλο Γεώργιο

ΕΙΣΑΓΩΓΗ

Η ραγδαία εξάπλωση του διαδικτύου την τελευταία δεκαετία και η χρήση του για εμπορικούς σκοπούς δημιούργησε νέες ανάγκες στο χώρο των επιχειρήσεων. Οι επιχειρήσεις προκειμένου να συμβαδίσουν με αυτές τις τεχνολογικές αλλαγές και να παραμείνουν ανταγωνιστικές στον ολοένα και μεταβαλλόμενο επιχειρηματικό κόσμο, καλούνται να δημιουργήσουν τις υποδομές εκείνες που θα επιτρέψουν στους καταναλωτές την αγορά προϊόντων και υπηρεσιών μέσω του διαδικτύου.
Αρχικά, στα πρώτα εμβρυϊκά στάδια ανάπτυξης του ηλεκτρονικού εμπορίου, οι ηλεκτρονικές συναλλαγές γίνονταν δίχως την χρήση του διαδικτύου, απλά με την καταβολή του χρηματικού ποσού σε κάποια Τράπεζα. Όμως αυτός ο τρόπος πραγματοποίησης ηλεκτρονικών συναλλαγών ήταν χρονοβόρος και ορισμένες φορές αναξιόπιστος σε σχέση με τον σημερινό τρόπο διεκπεραίωσης διαδικτυακών συναλλαγών. Έτσι άρχισε σιγά σιγά να αναπτύσσετε μία σειρά από ηλεκτρονικά συστήματα πληρωμών, τα οποία έφεραν με την σειρά τους την επανάσταση στον χώρο του διαδικτύου. Αυτά τα ηλεκτρονικά συστήματα πληρωμών έδωσαν στο καταναλωτικό κοινό την δυνατότητα χρήσης μιας γκάμας καινοτομιών όπως την χρήση πιστωτικής κάρτας μέσω του Internet για την αγορά προϊόντων και την εξόφληση λογαριασμών κ.α.
Στην Ελλάδα το ηλεκτρονικό εμπόριο άρχισε να αναπτύσσεται από την τελευταία πενταετία του 1990 με την υποστήριξη του Β' και Γ΄ Κοινοτικού πλαισίου στήριξης, επίσης σημαντικό ρόλο στην ανάπτυξη και διάδοση των ηλεκτρονικών συναλλαγών έπαιξαν και οι θυγατρικές εταιρείες μεγάλων πολυεθνικών του εξωτερικού. Αυτές οι εταιρείες είχαν αποκτήσει γνώσεις και εμπειρία όσον αφορά το ηλεκτρονικό εμπόριο στο εξωτερικό και προσφέροντας οικονομική ενίσχυση, προσπάθησαν να ενισχύσουν την ανάπτυξη του και στην Ελλάδα, όπου βρισκόταν ακόμα σε εμβρυϊκό επίπεδο. Όμως παρ' όλες τις προσπάθειες που έγιναν, η Ελλάδα υστερεί κατά πολύ όσον αφορά την χρήση των συστημάτων ηλεκτρονικών συναλλαγών, το οποίο οφείλεται κυρίως στην δυσπιστία που έχουν οι Έλληνες καταναλωτές για το μέγεθος της ασφάλειας που μπορούν να τους παρέχουν τα συστήματα αυτά.
Σκοπός της εργασίας μας είναι την εξέταση των υπαρχόντων συστημάτων ηλεκτρονικών συναλλαγών στην Ελλάδα καθώς και η εξέταση εκείνων των παραγόντων που προκάλεσαν την καθυστέρηση της ανάπτυξης των συστημάτων αυτών στο επίπεδο που παρατηρείται στις υπόλοιπες Ευρωπαϊκές χώρες. Στην συνέχεια αναλύονται και θέματα που αφορούν το επίπεδο ηλεκτρονικών συναλλαγών που παρατηρείται στις υπόλοιπες Ευρωπαϊκές χώρες, η νομοθεσία που καλύπτει την ασφάλεια την ηλεκτρονικών συναλλαγών τόσο στην Ελλάδα όσο και στην υπόλοιπη Ευρώπη. Επίσης γίνεται εκτενής αναφορά στα είδη των ηλεκτρονικών συναλλαγών καθώς και στους τρόπους ασφάλειας των ηλεκτρονικών συστημάτων.

Η σημασία των ηλεκτρονικών πληρωμών για την επιτυχημένη ανάπτυξη του ηλεκτρονικού και κινητού επιχειρείν αποτέλεσε το έναυσμα για την διερεύνηση του φαινομένου. Η σημαντική άνθηση του ηλεκτρονικού και κινητού επιχειρείν κυρίως στο εξωτερικό αλλά και στην Ελλάδα, δυστυχώς δεν συνοδεύεται από μία ανάλογη εξέλιξη των συστημάτων ηλεκτρονικών πληρωμών. Συνέπεια αυτού του γεγονότος είναι η εμφάνιση σημαντικών προβλημάτων στις συναλλαγές τα οποία αποδυναμώνουν τη δυναμική αυτών των δύο καινοτομικών καναλιών διανομής αγαθών και υπηρεσιών.

Οι **άξονες** πάνω στους οποίους κινηθήκαμε προκειμένου να εξετάσουμε τους παράγοντες που επηρέασαν την ανάπτυξη του ηλεκτρονικού εμπορίου είναι οι ακόλουθοι:

Τεχνολογικές εξελίξεις:

Στην ενότητα αυτή διερευνήθηκαν οι διαθέσιμες τεχνολογικές λύσεις και τα ζητήματα ασφαλείας, αξιοπιστίας και προστασίας δεδομένων.

Οικονομικά δεδομένα:

Στην ενότητα αυτή διερευνήθηκαν ζητήματα όπως το κόστος των ηλεκτρονικών συναλλαγών, η δυνατότητα συναλλαγών από ιδιώτες, το εύρος των χρηστών, η δυνατότητα χρήσης επιτυχημένων συστημάτων και από άλλες εταιρείες πέραν αυτών που τα ανέπτυξαν, και ο χρηματοοικονομικός κίνδυνος τέτοιων συναλλαγών.

Κοινωνικοί προβληματισμοί:

Στην ενότητα αυτή εξετάστηκε ο βαθμός αποδοχής της ελληνικής κοινωνίας σε θέματα ηλεκτρονικών πληρωμών και τα χαρακτηριστικά που πρέπει να διαθέτει ένα σύστημα προκειμένου να αναπτυχθεί εμπιστοσύνη γύρω από αυτό.

Νομικό πλαίσιο:

Η ενότητα αυτή εξέτασε το νομικό πλαίσιο σε επίπεδο Ευρωπαϊκής Ένωσης αλλά και ελληνικής νομοθεσίας.

ΟΡΙΣΜΟΣ ΗΛΕΚΤΡΟΝΙΚΩΝ ΠΛΗΡΩΜΩΝ- ΔΙΑΚΡΙΣΕΙΣ

Ηλεκτρονικές πληρωμές (electronic payments) είναι κάθε είδος πληρωμής προς τις επιχειρήσεις, τις τράπεζες ή τις δημόσιες υπηρεσίες από πολίτες ή επιχειρήσεις οι οποίες εκτελούνται με την μεσολάβηση ενός τηλεπικοινωνιακού ή ηλεκτρονικού δικτύου με χρήση της σύγχρονης τεχνολογίας.

Είναι σαφές ότι με τον όρο ηλεκτρονικές πληρωμές αναφερόμαστε στο γεγονός ότι οι πληρωμές γίνονται από τον ίδιο τον πληρωτή είτε αυτός είναι καταναλωτής είτε επιχείρηση και χωρίς την μεσολάβηση κάποιου άλλου φυσικού προσώπου. Επίσης η διαδικασία της πληρωμής γίνεται εξ αποστάσεως, χωρίς την φυσική παρουσία του πληρωτή και χωρίς την χρήση φυσικού χρήματος δηλαδή μετρητών. Η μεταφορά χρημάτων από τον πληρωτή στον αποδέκτη θα γίνεται μέσω διαδικτύου. Η διαδικασία αυτή μπορεί να πραγματοποιηθεί με την απλή γνώση των στοιχείων των λογαριασμών των ατόμων που περιλαμβάνονται στην διαδικασία της ηλεκτρονικής πληρωμής.

- **Οι ηλεκτρονικές πληρωμές διακρίνονται σε δύο κατηγορίες:**
  - Σε αυτές που στηρίζονται στην μεταφορά πληροφοριών και
  - Σε αυτές που στηρίζονται στην μεταφορά αξίας.

Στην πρώτη κατηγορία μεταφέρονται πληροφορίες που αφορούν πληροφορίες για την ίδια την συναλλαγή και για τους τραπεζικούς λογαριασμούς των εμπλεκομένων ενώ στην δεύτερη κατηγορία μεταφέρονται χρηματικές αξίες μέσω των συστημάτων ηλεκτρονικών συναλλαγών. Η χρηματική συναλλαγή πραγματοποιείται είτε off-line είτε με την χρήση ιδιόκτητων ηλεκτρονικών δικτύων χρηματοπιστωτικών ιδρυμάτων ή εταιρειών. Σήμερα, οι ηλεκτρονικές πληρωμές στο μεγαλύτερο μέρος τους πραγματοποιούνται μέσω των συστημάτων ηλεκτρονικών πληρωμών που στηρίζονται στην μεταφορά πληροφοριών.
Επίσης, οι ηλεκτρονικές πληρωμές με βάση την τεχνολογία που χρησιμοποιείται, διακρίνεται στις εξής κατηγορίες:

Πληρωμές μέσω τηλεφώνου:
Οι πληρωμές που πραγματοποιούνται μέσω της χρήσης του τηλεφωνικού δικτύου αποτελούν μία καινούργια μορφή ηλεκτρονικών πληρωμών. Στόχος ήταν η εκμετάλλευση του ευρέως διαδεδομένου τηλεφωνικού δικτύου ως μέσο με το οποίο όλα τα άτομα ανεξαρτήτως κοινωνικής θέσεως να μπορούν να εξοφλούν τους λογαριασμούς τους. Αυτά τα συστήματα πληρωμών ολοένα κερδίζουν την εμπιστοσύνη του κοινού μια και το βασικό πλεονέκτημα που τους προσφέρει είναι η εξοικονόμηση χρόνου (εξάλειψη αναμονής στις ουρές των δημόσιων υπηρεσιών για την εξόφληση των λογαριασμών).

Πληρωμές μέσω διαδικτύου (Internet):
Πρόκειται για την πιο σύγχρονη μορφή ηλεκτρονικών πληρωμών. Η άνθηση του ηλεκτρονικού επιχειρείν καθιστά ιδιαίτερα σημαντική την ύπαρξη συστημάτων ηλεκτρονικών πληρωμών με τα οποία είναι δυνατή η πραγματοποίηση ηλεκτρονικών πληρωμών και η διευκόλυνση του κοινού που χρησιμοποιεί το διαδίκτυο στην καθημερινότητα του.

Πληρωμές μέσω κινητής τηλεφωνίας (m-payments)
Τα τελευταία χρόνια η κινητή τηλεφωνία έχει γνωρίσει ραγδαία ανάπτυξη. Τα κινητά τηλέφωνα πλέον, αποτελούν αναγκαίο μέσο για την επικοινωνία ατόμων που βρίσκονται σε μακρινές αποστάσεις μεταξύ τους και επιπλέον βρίσκονται σε εξωτερικούς χώρους, με αποτέλεσμά να καθίσταται αδύνατη η επικοινωνία μέσω ψηφιακού τηλεφωνικού δικτύου. Η δημιουργία της υπηρεσίας WAP και I-MODE επιτρέπει πλέον στους χρήστες κινητής τηλεφωνίας να πραγματοποιούν πληρωμές λογαριασμών μπαίνοντας στο διαδίκτυο μέσω του κινητού τους τηλεφώνου ενώ βρίσκονται εν κινήσει.

ΣΥΣΤΗΜΑΤΑ ΗΛΕΚΤΡΟΝΙΚΩΝ ΠΛΗΡΩΜΩΝ

Η συνεχής αύξηση των συναλλαγών μέσω διαδικτύου έχει καταστήσει απαραίτητη την δημιουργία συστημάτων ηλεκτρονικών συναλλαγών τα οποία ναι μεν θα επιτρέπουν την γρήγορη και εύκολη διεκπεραίωση των διάφορων συναλλαγών αλλά δεν θα υποτιμήσουν και την ασφάλεια που παρέχουν τα παραδοσιακά συστήματα πληρωμών. Μέχρι σήμερα έχει διαπιστωθεί ότι υπάρχουν 150 διαφορετικά συστήματα ηλεκτρονικών πληρωμών που υποστηρίζουν συναλλαγές στο διαδίκτυο, ενώ μόνο στην Ευρώπη έχουν καταγραφεί ήδη 60 διαφορετικές λύσεις.

Οι ηλεκτρονικές πληρωμές ταξινομούνται σε δύο κατηγορίες:

- **Ανάλογα με το είδος της πληροφορίας που ανταλλάσσεται.**
  Σε αυτήν την κατηγορία ανήκουν τα συστήματα πληρωμών που απαιτείται η ύπαρξη τραπεζικού λογαριασμού όπως οι πιστωτικές και χρεωστικές κάρτες και τα συστήματα που λειτουργούν με την ανταλλαγή ηλεκτρονικών γραμματίων δηλαδή των τραπεζογραμματίων όπως είναι το ηλεκτρονικό χρήμα.

- **Ανάλογα την καινοτομικότητα του συστήματος.**
  Σε αυτήν την κατηγορία ανήκουν τα συστήματα ηλεκτρονικών πληρωμών που προϋπήρχαν του επιχειρείν και απλά προσαρμόστηκαν για την χρήση του στο διαδίκτυο όπως οι πιστωτικές κάρτες.

Στον πίνακα που ακολουθεί παρουσιάζεται η προτεινόμενη ταξινόμηση των συστημάτων ηλεκτρονικών πληρωμών.

		ΥΠΟΘΕΜΑ	
	ΣΥΣΤΗΜΑΤΑ ΗΛΕΚΤΡΟΝΙΚΩΝ ΠΛΗΡΩΜΩΝ	ΓΡΑΜΜΑΤΙΟ	ΛΟΓΑΡΙΑΣΜΟΣ
Παραδοσιακά συστήματα προσαρμοσμένα στο Διαδίκτυο	Πιστωτικές Κάρτες		X
	Μεταφορά ποσών επί πιστώσει		X
	Πάγιες εντολές		X
	Χρεωστικές Κάρτες		X
Καινούργια συστήματα για χρήση στο Διαδίκτυο	Ηλεκτρονικές επιταγές		X
	Ηλεκτρονικό χρήμα	X	
	Πληρωμές μεταξύ ομότιμων		X

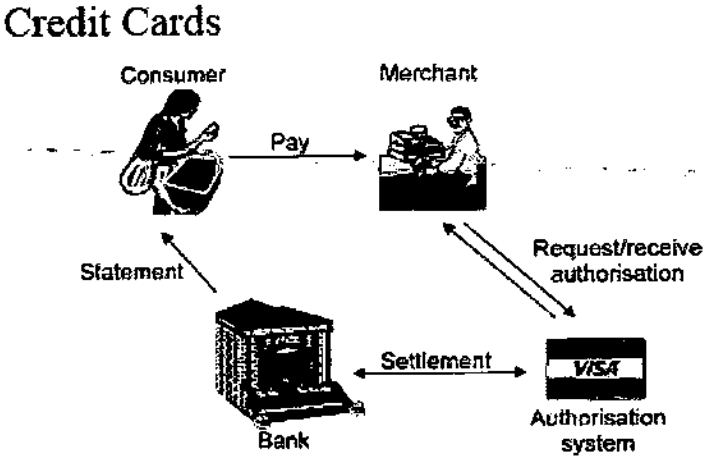
Όπως παρατηρούμε από τον παραπάνω πίνακα, τα περισσότερα συστήματα ηλεκτρονικών συναλλαγών απαιτούν την ύπαρξη λογαριασμού με αποτέλεσμα να μην διατηρείται η ανωνυμία των ατόμων, ενώ για κάποια άτομα που για κάποιον λόγο δεν έχουν τραπεζικό λογαριασμό είναι αδύνατο να πραγματοποιήσουν ηλεκτρονικές πληρωμές.

Όσον αφορά τα συστήματα ηλεκτρονικών συναλλαγών που δημιουργήθηκαν μεταγενέστερα του επιχειρείν όπως είναι το ηλεκτρονικό χρήμα παρέχουν μεγαλύτερη ασφάλεια μια και διατηρείται η ανωνυμία των ατόμων που εμπλέκονται στην διαδικασία ηλεκτρονικής πληρωμής.

ΠΑΡΑΔΟΣΙΑΚΑ ΣΥΣΤΗΜΑΤΑ ΠΡΟΣΑΡΜΟΣΜΕΝΑ ΣΤΟ ΔΙΑΔΙΚΤΥΟ.

Όπως αναφέραμε παραπάνω τα συστήματα αυτά προϋπήρχαν της εμφάνισης του Διαδικτύου και απλά υπέστησαν κάποιες προσαρμογές προκειμένου να μπορούν να πραγματοποιούνται μέσω διαδικτύου.
Τα συστήματα αυτά είναι τα εξής:

Πιστωτικές κάρτες.
Σε μια 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 στην συνέχεια στην τράπεζα για διεκπεραίωση. Στο τέλος η τράπεζα χρεοπιστώνει τους αντίστοιχους λογαριασμούς ενημερώνοντας τα εμπλεκόμενα μέρη για την συναλλαγή που έγινε.
Σε έναν μηχανισμό ηλεκτρονικής πληρωμής με χρήση της πιστωτικής κάρτας, ακολουθείται το ίδιο περίπου σενάριο με αυτό που αναφέρθηκε παραπάνω. 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.
Οι πιστωτικές κάρτες έχουν τύχει ευρείας χρήσης στο διαδίκτυο επειδή διαθέτουν σημαντικά πλεονεκτήματα έναντι εναλλακτικών μεθόδων πληρωμής. Κατ΄ αρχήν είναι διεθνώς γνωστές και αποδέκτες από τους εμπόρους. Η χρήση τους στο διαδίκτυο δεν διαφέρει σημαντικά από τον τρόπο που χρησιμοποιούνταν μέχρι τώρα στις συναλλαγές στον φυσικό κόσμο.
Στα πρώτα στάδια του ηλεκτρονικού εμπορίου, οι καταναλωτές απλά έστελναν τον αριθμό της πιστωτικής τους κάρτας και την ημερομηνία λήξης στους εμπόρους με την μορφή απλού μηνύματος χωρίς κρυπτογράφηση. Σύντομα όμως αυτός ο τρόπος χρήσης της πιστωτικής κάρτας στο διαδίκτυο εγκαταλείφθηκε καθώς το μήνυμα ήταν πολύ εύκολο να υποκλαπεί με αποτέλεσμα να παρατηρηθούν κρούσματα απάτης με πιστωτικές κάρτες. Προκειμένου να λυθούν τα προβλήματα απάτης οι οργανισμοί πιστωτικών καρτών προχώρησαν στην δημιουργία προτύπων όπως το SET(Secure Electronic Transaction) που ήταν πρωτοβουλία της VISA και της MASTERCARD. Τα πρότυπα αυτά ενίσχυσαν σημαντικά την ασφάλεια των συναλλαγών στο διαδίκτυο μέσω πιστωτικής κάρτας δεν έτυχαν όμως ευρείας αποδοχής από το καταναλωτικό κοινό.



Μεταφορά ποσών επί πιστώσει:
Σε αυτό το σύστημα πληρωμών ο καταναλωτής δίνει εντολή στην τράπεζα του να μεταφέρει χρηματικά ποσά ανάλογα της πληρωμής που θέλει να πραγματοποιήσει στον λογαριασμό του εμπόρου. Αυτή η μέθοδος πληρωμής υποστηρίζεται σημαντικά από τις τράπεζες στα πλαίσια των εφαρμογών ηλεκτρονικής τραπεζικής που προσφέρουν στους πελάτες τους. Ειδικά για συναλλαγές στο διαδίκτυο οι πελάτες μπορούν να επιλέξουν την μεταφορά ποσών επί πιστώσει ως την επιθυμητή μέθοδο πληρωμής και απλά να αποδεχθούν τον λογαριασμό που θα εμφανιστεί στην οθόνη τους. Εφόσον ο πελάτης αποδέχεται την συναλλαγή μεταφέρεται στον δικτυακό τόπο της τράπεζας όπου ολοκληρώνει την συναλλαγή του και κατόπιν επιστρέφει στο ηλεκτρονικό κατάστημα στο οποία βρισκόταν.
Το συγκεκριμένο σύστημα πληρωμών προϋποθέτει την ύπαρξη συμφωνίας μεταξύ της τράπεζας και του εμπόρου. Επιπλέον ο πελάτης πρέπει να χρησιμοποιεί τις υπηρεσίες ηλεκτρονικής τραπεζικής που του προσφέρει η τράπεζα του. Σύμφωνα με μελέτη της Ευρωπαϊκής Κεντρικής Τράπεζας, τα εν λόγω συστήματα ηλεκτρονικών πληρωμών λειτουργούν προς το παρόν σε αυστηρά εθνικά πλαίσια με αποτέλεσμα να μην είναι βολικά για διεθνείς συναλλαγές.

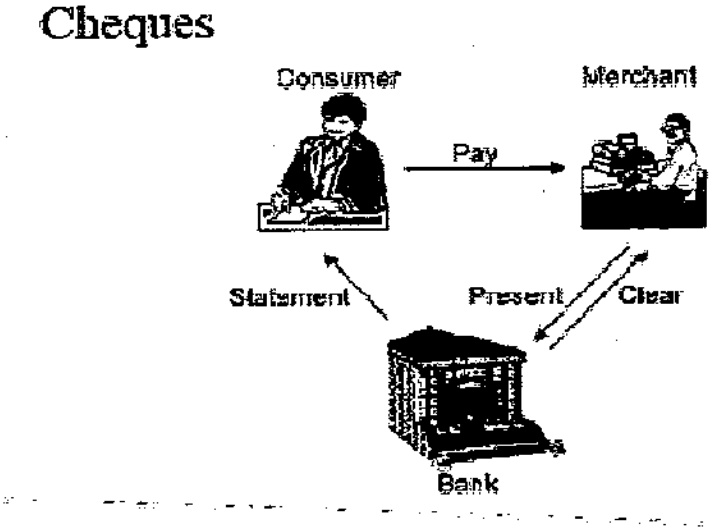
Πάγιες εντολές:
Πρόκειται για προεγκριμένα χρεωστικά ποσά από τον τραπεζικό λογαριασμό του πελάτη που εκχωρούνται στον δικαιούχο. Οι πάγιες εντολές χρησιμοποιούνται συνήθως για επαναλαμβανόμενες πληρωμές όπως αυτές για λογαριασμούς ΔΕΚΟ ή για εφάπαξ πληρωμές όταν δεν υπάρχει άμεση επαφή μεταξύ εμπόρου και αγοραστή. Στις πάγιες εντολές, ο δικαιούχος αποστέλλει στον οφειλέτη ένα ειδικό έντυπο το οποίο ο τελευταίος συμπληρώνει αναγνωρίζοντας κατ' αυτό τον τρόπο την οφειλή του δικαιούχου. Στην συνέχεια ο τελευταίος προωθεί το ειδικό έντυπο στην συμβεβλημένη τράπεζα για την ολοκλήρωση της συναλλαγής.
Οι πάγιες εντολές χρησιμοποιούνται και για πληρωμές στο Διαδίκτυο. Στην περίπτωση αυτή όλη η ανωτέρω διαδικασία γίνεται ηλεκτρονικά και ομοιάζει αρκετά στις πληρωμές στο διαδίκτυο με τη χρήση πιστωτικής κάρτας. Η βασική διαφορά έγκειται στο γεγονός ότι ο οφειλέτης αποστέλλει το νούμερο του τραπεζικού του λογαριασμού και όχι αυτό της πιστωτικής του κάρτας.

Χρεωστικές κάρτες:
Το εν λόγω σύστημα ηλεκτρονικών πληρωμών αποτελεί μια παραλλαγή των πάγιων εντολών όπου οι απαιτούμενες για τη συναλλαγή πληροφορίες περιέχονται σε ειδική κάρτα με μαγνητική ταινία ή μικροεπεξεργαστή. Για την πραγματοποίηση συναλλαγών απαιτείται η ύπαρξη ειδικού τερματικού το οποίο θα επαληθεύει την εγκυρότητα των πληροφοριών που είναι αποθηκευμένες στην κάρτα και θα ελέγχει αν αυτή βρίσκεται σε ισχύ. Η διαδικασία πληρωμής είναι ακριβώς ίδια με αυτή των παγίων εντολών με τη διαφορά ότι οι απαιτούμενες πληροφορίες είναι αποθηκευμένες στην κάρτα με αποτέλεσμα η συναλλαγή να είναι ασφαλέστερη. Ο κάτοχος της κάρτας πρέπει να διαθέτει ειδικό μηχάνημα υποδοχής συνδεδεμένο με τον υπολογιστή του που σημαίνει βέβαια ότι απαιτείται επιπλέον εξοπλισμός για τη χρήση της.
Εντούτοις, το ειδικό αυτό μηχάνημα συχνά εκχωρείται στον πελάτη από την ίδια την τράπεζα. Το βασικό μειονέκτημα των χρεωστικών καρτών είναι ότι από την σκοπιά του πελάτη δεν είναι σαφή τα πλεονεκτήματα τους έναντι των πιστωτικών καρτών.

Ειδικά στις συναλλαγές στο διαδίκτυο, οι χρεωστικές κάρτες προσφέρουν μικρότερη προστασία έναντι των πιστωτικών σε περιπτώσεις που τα αντικείμενα που αγοράστηκαν δεν παραδίδονται ή είναι ελαττωματικά. Από την πλευρά των εμπόρων πάντως οι χρεωστικές κάρτες είναι προτιμότερες καθώς δεν επιβαρύνουν με προμήθεια τους εμπόρους. Επιπλέον, στις επιχειρηματικές συναλλαγές μέσω διαδικτύου (B2B) οι χρεωστικές κάρτες μπορεί να αποδειχθούν φθηνότερη λύση ακριβώς για τον ίδιο λόγο.

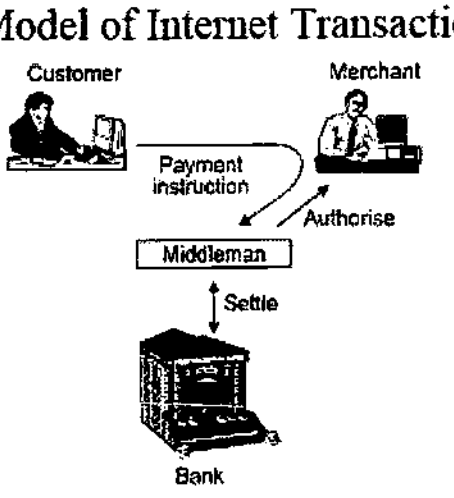
Ηλεκτρονικές επιταγές:

Οι ηλεκτρονικές επιταγές είναι η φυσιολογική συνέχεια των παραδοσιακών επιταγών. Μια επιταγή είναι μια γραπτή εντολή από τον εκδότη προς τον αποδέκτη που είναι συνήθως τράπεζα με την οποία ο εκδότης απαιτεί από τον αποδέκτη την καταβολή ενός συγκεκριμένου ποσού είτε στον εκδότη είτε σε τρίτο πρόσωπο που ορίζεται από αυτόν. Οι ηλεκτρονικές επιταγές ακολουθούν κατά βάση τον ίδιο κανόνα με τη διαφορά ότι η επιταγή είναι σε ηλεκτρονική μορφή. Επιπλέον, καθώς ο εκδότης πρέπει να υπογράψει την επιταγή προκειμένου να είναι έγκυρη στις ηλεκτρονικές επιταγές χρησιμοποιείται η ψηφιακή υπογραφή προκειμένου να ολοκληρωθεί η διαδικασία. Στην χρήση ηλεκτρονικών υπογραφών εντοπίζονται και τα περισσότερα προβλήματα που συναντά στην διάδοση του το συγκεκριμένο σύστημα πληρωμής. Η χρήση κρυπτογραφικών μεθόδων αλλά και η τεχνολογία που απαιτείται για να υποστηρίξει τις ηλεκτρονικές υπογραφές έχουν μέχρι τώρα δημιουργήσει αρκετά εμπόδια στην χρήση των ηλεκτρονικών επιταγών τα οποία και θα αναλυθούν σε επόμενη ενότητα.



ΚΑΙΝΟΤΟΜΙΚΑ ΣΥΣΤΗΜΑΤΑ ΓΙΑ ΤΟ ΔΙΑΔΙΚΤΥΟ

Στην κατηγορία αυτή υπάρχουν συστήματα πληρωμών τα οποία κάνουν χρήση καινοτομικών τεχνολογιών που μέχρι πρόσφατα δεν ήταν διαθέσιμες για την διεξαγωγή πληρωμών. Επιπλέον, πολλά από τα συστήματα αυτά είναι προσαρμοσμένα στις τρέχουσες τάσεις του ηλεκτρονικού επιχειρείν και προσπαθούν να ικανοποιήσουν τις καταναλωτικές τάσεις που φαίνεται να διαμορφώνονται στο διαδίκτυο όπως η αγορά άϋλων αγαθών μικρής αξίας κ.α. Μερικά από τα συστήματα αυτά όπως οι έξυπνες κάρτες αρχίζουν να χρησιμοποιούνται και στον φυσικό κόσμο ενώ άλλα είναι σχεδιασμένα αποκλειστικά για χρήση στο διαδίκτυο.



Ειδικότερα τα συστήματα αυτά είναι:

Σχήματα ηλεκτρονικού χρήματος:

Ως ηλεκτρονικό χρήμα, η Ευρωπαϊκή Κεντρική Τράπεζα ορίζει «την αποθήκευση χρηματικής αξίας σε ψηφιακή μορφή μέσω μιας συσκευής που μπορεί να χρησιμοποιηθεί ευρέως για την πραγματοποίηση πληρωμών σε δίκτυα χωρίς την χρήση τραπεζικών λογαριασμών. Το ηλεκτρονικό χρήμα θα λειτουργεί ως προπληρωμένο υπόθεμα. Ενώ τα δίκτυα θα είναι είτε ανοικτά δηλαδή θα επιτρέπουν την άμεση μεταφορά χρημάτων μεταξύ υποθεμάτων είτε κλειστά όπου η χρέωση του υποθέματος θα γίνεται από συγκεκριμένο τραπεζικό λογαριασμό αποκλειστικά». Είναι επομένως εμφανές ότι το ηλεκτρονικό χρήμα έχει ανάλογες ιδιότητες με τα κοινά τραπεζογραμμάτια. Μέχρι τώρα τα ισχύοντα σχήματα ηλεκτρονικού χρήματος στηρίζονται είτε σε κάρτες αποθηκευμένης αξίας είτε σε ειδικό λογισμικό. Στην πρώτη περίπτωση η κάρτα περιέχει ένα χρηματικό ποσό ανάλογο με αυτό που έχει προπληρώσει ο κάτοχος της. Η κάρτα μπορεί δε να είναι είτε ανώνυμη είτε ονομαστική.

Ο κάτοχος της μπορεί να τη φορτίζει κάθε φορά με το ποσό που επιθυμεί. Για λόγους ασφαλείας, η κάρτα προστατεύεται από τετραψήφιο κωδικό. Στα σχήματα ηλεκτρονικού χρήματος μέσω λογισμικού πραγματοποιείται έκδοση ηλεκτρονικών νομισμάτων από έναν παρόχεα υπηρεσιών πληρωμών. Τα ηλεκτρονικά αυτά νομίσματα είναι αποθηκευμένα σε ένα ηλεκτρονικό πορτοφόλι στον υπολογιστή του χρήστη ο οποίος μπορεί να τα χρησιμοποιήσει για αγορές μέσω διαδικτύου.

Μέχρι τώρα οι περισσότερες πρωτοβουλίες με σχήματα ηλεκτρονικού χρήματος μέσω ειδικού λογισμικού δεν έτυχαν ευρείας αποδοχής καθώς δεν είναι ιδιαίτερα ευέλικτα. Οι όποιες προσπάθειες έμειναν σε πιλοτικό στάδιο.

Το βασικό πλεονέκτημα πάντως των σχημάτων ηλεκτρονικών πληρωμών και στις δύο περιπτώσεις είναι ότι διατηρείται η ανωνυμία των συναλλαγών που είναι ιδιαίτερα σημαντική για τους πελάτες. Επιπλέον, ειδικά οι κάρτες αποθηκευμένης αξίας είναι ιδιαίτερα ευέλικτο μέσο πληρωμής που επιτρέπει και διεθνείς συναλλαγές.

Πληρωμές μεταξύ ομοτίμων:
Η μεγάλη επιτυχία των ηλεκτρονικών δημοπρασιών στο διαδίκτυο οδήγησε και στην δημιουργία συστημάτων πληρωμών προσαρμοσμένων στις ανάγκες των συμμετεχόντων.
Ειδικότερα, αναπτύχθηκαν συστήματα που στόχο είχαν να παρέχουν την δυνατότητα σε χρήστες του διαδικτύου να πραγματοποιούν απευθείας συναλλαγές χωρίς την μεσολάβηση κάποιου χρηματοπιστωτικού οργανισμού. Τα συστήματα πληρωμών μεταξύ ομοτίμων λειτουργούν κατά βάση όπως οι τράπεζες καθώς οι πελάτες ανοίγουν λογαριασμούς σε παροχείς υπηρεσιών πληρωμών όπου καταθέτουν χρηματικά ποσά. Η βασική καινοτομία προέρχεται από το γεγονός ότι τα συστήματα αυτά χρησιμοποιούν τις ηλεκτρονικές διευθύνσεις των δικαιούχων καθώς και τον δικτυακό τόπο της εταιρείας υπηρεσιών πληρωμών προκειμένου να συνεννοηθούν τα μέρη για την συναλλαγή. Επιπλέον, η απόκτηση λογαριασμού είναι πιο εύκολη απ' ότι στον πραγματικό κόσμο.
Ειδικότερα, ένας οποιοσδήποτε χρήστης του διαδικτύου μπορεί να προβεί σε απευθείας πληρωμές εφόσον εγγραφεί στο σύστημα του παρόχεα που προσφέρει την υποδομή για τις συναλλαγές αυτές. Η εταιρεία ζητά συνήθως από τους πελάτες της να πραγματοποιήσουν κατάθεση σε τραπεζικό λογαριασμό της εταιρείας χρησιμοποιώντας κάποιο παραδοσιακό μέσο πληρωμής όπως η πιστωτική κάρτα ή η επιταγή. Με την πραγματοποίηση της κατάθεσης ο πελάτης αποκτά ηλεκτρονικό λογαριασμό στην εταιρεία ο οποίος είναι πιστωμένος με το ποσό που κατέθεσε. Όταν θέλει να πραγματοποιήσει την πληρωμή ο κάτοχος του λογαριασμού συνδέεται με το σύστημα του παρόχεα ηλεκτρονικών πληρωμών και δίνει εντολή μεταφοράς χρημάτων. Ο παροχέας απλά μεταφέρει τα ποσά από τον ένα λογαριασμό στον άλλο. Το σύστημα χρησιμοποιεί τις ηλεκτρονικές διευθύνσεις των δικαιούχων για την πιστοποίηση τους ενώ τα στοιχεία της συναλλαγής αποστέλλονται στους δικαιούχους μέσω ηλεκτρονικού ταχυδρομείου.
Το βασικό πλεονέκτημα αυτού του συστήματος πληρωμών είναι ότι υποστηρίζει διεθνείς συναλλαγές ενώ δεν απαιτείται ειδικός εξοπλισμός όπως κάρτες ή τερματικά για την χρήση του. Επιπλέον δεν παρακρατείται προμήθεια από τον παρόχεα με αποτέλεσμα να είναι φθηνότερη λύση για τους καταναλωτές.

Πληρωμές μέσω κινητού τηλεφώνου (mobile payments)
Με την εμφάνιση και ραγδαία διάδοση της κινητής τηλεφωνίας εμφανίστηκε ένας σημαντικός αριθμός πρωτοβουλιών για πληρωμές μέσω κινητού τηλεφώνου. Στην ανάληψη τέτοιων πρωτοβουλιών συνέβαλε φυσικά και η απότομη πτώση των εταιρειών ηλεκτρονικού εμπορίου στις αρχές του 2000 που οδήγησε πολλούς οργανισμούς να στραφούν προς την εκμετάλλευση της υπάρχουσας τεχνολογίας, σε άλλους χώρους ώστε να αυξήσουν την κερδοφορία τους.
Στην προσπάθειά τους αυτή δεν θα μπορούσαν να αγνοήσουν τους περίπου ένα δισεκατομμύριο χρήστες κινητών τηλεφώνων ανά των κόσμο το 2002, σύμφωνα με τον παγκόσμιο οργανισμό κινητής τηλεφωνίας (UMTS).

Σύμφωνα με το επιχειρηματικό μοντέλο που αναπτύσσει η Ernst & Young (2002) συνήθως αναγνωρίζονται οι παρακάτω συμμετέχοντες στην αγορά αγαθών και υπηρεσιών μέσω κινητού:

- ο παροχέας περιεχομένου (content provider),
- παροχέας αυθεντικοποίησης του καταναλωτή (authentication provider),
- ο οργανισμός που εγκρίνει την πληρωμή (payment authorisation),
- ο διεκπεραιωτής της συναλλαγής (settlement provider),
- παροχέας υπηρεσιών πληρωμών (Payment Service Provider) και τέλος
- ο καταναλωτής (consumer).

Ο **καταναλωτής** είναι αυτός που έχει στην κατοχή του την συσκευή κινητής τηλεφωνίας και προχωρά σε αγορά περιεχομένου ή υπηρεσιών από τον **παροχέα περιεχομένου.** Ο **παροχέας αυθεντικοποίησης** της ταυτότητας του καταναλωτή ή αλλιώς Έμπιστη Τρίτη Οντότητα (ΕΤΟ) είναι ένας ανεξάρτητος οργανισμός που φροντίζει για την πιστοποίηση της ταυτότητας του καταναλωτή. Ο **διεκπεραιωτής της συναλλαγής** θα μπορούσε να είναι μια τράπεζα, μία εταιρεία παροχής κινητής τηλεφωνίας ή ακόμη και ένας εκδότης πιστωτικών καρτών.

Ο **παροχέας υπηρεσιών πληρωμών** (Payment Service Provider), είναι κεντρική οντότητα για την διαδικασία της πληρωμής μέσω κινητού. Αυτός δέχεται το μήνυμα για αγορά αγαθού και το κατευθύνει στην ΕΤΟ. Το μήνυμα μπορεί να σταλεί με μία πληθώρα τεχνολογιών που υιοθετούνται από τις συσκευές κινητής τηλεφωνίας όπως SMS, WAP, SIM application toolkit (SAT), USSD, IVR, dual slot phones, dual SIM Phones, Bluetooth, Infrared, Bar code readers και contactless chips.

Οι ηλεκτρονικές πληρωμές μέσω κινητού συνήθως περιλαμβάνουν μια εφαρμογή ηλεκτρονικού πορτοφολιού που επιτρέπει στους καταναλωτές να αποθηκεύουν τις πληροφορίες της αγοράς του αγαθού, όπως τον αριθμό της πιστωτικής τους κάρτας ή και τη διεύθυνση αποστολής του αγαθού σε έναν ασφαλή διακομηστή (server) του παροχέα υπηρεσιών πληρωμών.
Χαρακτηριστικό είναι ότι πίσω από τους ρόλους των Παροχέα Υπηρεσιών Πληρωμών, της Έμπιστης Τρίτης Οντότητας, και του Παροχέα Περιεχομένου συνήθως βρίσκεται μια εταιρεία παροχής υπηρεσιών κινητής τηλεφωνίας.

Οι μεταβλητές που προσδίδουν ιδιαίτερα χαρακτηριστικά στις αγορές μέσω κινητού τηλεφώνου είναι συνήθως ο χρόνος διεκπεραίωσης της συναλλαγής, το περιεχόμενο αυτής και το ύψος της αγοράς.

Έτσι λοιπόν έχουμε τα παρακάτω είδη συναλλαγών μέσω κινητού τηλεφώνου.

Προπληρωμένες αγορές:
Ο καταναλωτής προπληρώνει στον PSP (παροχέα) ένα συγκεκριμένο ποσό για το περιεχόμενο της υπηρεσίας ή των αγαθών που θα αγοράσει, με την μορφή αγοραστικών μονάδων ή μονάδων μιας κάρτας ομιλίας.

Πληρωμές μετά την αγορά:
Ο καταναλωτής αφού προβεί στην αγορά του αγαθού πληρώνει εκ των υστέρων συνήθως με χρέωση της πιστωτικής του κάρτας ή με χρέωση του λογαριασμού του κινητού του τηλεφώνου.

Αγορά σε πραγματικό χρόνο:
Ο καταναλωτής προχωρά στην αγορά ενός αγαθού τη στιγμή που εξερευνά την ηλεκτρονική ιστοσελίδας μιας εταιρείας μέσω της συσκευής του. Για παράδειγμα όταν θέλει να αποθηκεύει στη συσκευή του ένα τραγούδι σε μορφή MP3, απλά το επιλέγει και το αποθηκεύει στο κινητό του. Η χρέωση γίνεται με τις διαδικασίες που ακολουθούνται στο ηλεκτρονικό εμπόριο.

Το είδος των αγαθών που μπορεί να αγοράσει ο καταναλωτής συνήθως χωρίζονται στις παρακάτω κατηγορίες:
Ψηφιακά αγαθά (MP3, ringtones, ή πληροφορία επιπλέον αξίας, όπως παρακολούθηση των τιμών των μετοχών στο χρηματιστήριο κ.α.)
Παραδοσιακά αγαθά (αγορά τηλεόρασης, DVD κλπ.)
Ψηφοφορίες (ψήφος σε ένα τηλεπαιχνίδι)
Αγορά εισιτηρίων (κινηματογράφου, θεάτρου κλπ.)

Επίσης αναλόγως του περιεχομένου της αγοράς χωρίζονται σε μίκρο και μάκρο πληρωμές. Συνήθως το διαχωριστικό όριο αξίας του αγαθού είναι το ποσό των 10 Ευρώ.
Όμως θα πρέπει να αναφέρουμε ότι είναι πλέον δύσκολος ο διαχωρισμός και η κατηγοριοποίηση των υπηρεσιών που προσφέρονται για αγορές μέσω του διαδικτύου και για αγορές μέσω ενός κινητού τηλεφώνου. Στην πραγματικότητα χρησιμοποιούνται παραδοσιακές υπηρεσίες μέσω καινούριων μέσων, συσκευών.
Για παράδειγμα οι πιστωτικές κάρτες και πολλές τραπεζικές υπηρεσίες χρησιμοποιούνται για αγορές είτε μέσω του διαδικτύου, είτε μέσω συσκευών κινητής τηλεφωνίας παράλληλα με τον παραδοσιακό τρόπο. Άρα στην ουσία μιλάμε για νέα κανάλια παροχής υπηρεσιών.

ΕΦΑΡΜΟΓΗ ΤΗΣ ΚΡΥΠΤΟΓΡΑΦΙΑΣ ΣΤΙΣ ΗΛΕΚΤΡΟΝΙΚΕΣ ΣΥΝΑΛΛΑΓΕΣ.

Εδώ περιγράφεται ο τρόπος με τον οποίο η κρυπτογραφία εφαρμόζεται στις ηλεκτρονικές συναλλαγές, και το επίπεδο ασφάλειας που παρέχει σε αυτές.

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 εταιρείας 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 θεωρήσουμε την ασφάλεια του δικτύου σαν μια τραμπάλα, στην οποία η μια πλευρά είναι το δίκτυο της εταιρείας και η άλλη πλευρά είναι ο υπόλοιπος on line κόσμος και η ασφάλεια βρίσκεται στο μέσον, εξισορροπώντας τον φόρτο. Συνεπώς οποιαδήποτε στιγμή γίνει μια αλλαγή σε οποιαδήποτε πλευρά της τραμπάλας, η ασφάλεια στο μέσο πρέπει να αλλάξει για να διατηρηθεί η ισορροπία.

ΑΝΑΛΥΣΗ ΚΙΝΔΥΝΩΝ

Ένα σημαντικό ζήτημα στον σχεδιασμό μιας 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 ένας 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 κ.λ.π. Χωρίς μία βαθιά κατανόηση των ωφελειών που μπορεί να προσφέρουν κάποια συγκεκριμένα μέτρα ασφαλείας, είναι δυνατόν να εκτιμηθούν οι υπάρχουσες επιλογές από επιχειρηματική άποψη.

ΕΧΘΡΟΙ

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 ποιοι είναι οι εχθροί;
2) Τι σκοπεύουν – Ποιοι είναι οι σκοποί τους – τι ακριβώς επιδιώκουν;
3) Τι μέσα διαθέτουν;

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

❖ **Ο εισβολέας (hacker).**

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 παραβιαστεί 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 έχει 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 συνολικό κόστος.

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 εισβάλουν 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 αντικαταστήσει.

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 και προγράμματα που χρησιμοποιούν οι λιγότεροι ικανοί.

❖ **Ιοί.**

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 αλλά 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 cookies για να παρακολουθούν τους χρήστες χωρίς αυτοί να το ξέρουν.

❖ **Οι ανταγωνιστές.**

Ένας ανταγωνιστής ίσως να μην ενδιαφέρεται τόσο να κλέψει τα χρήματα 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 την 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 έμεσα 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 κ.λ.π. Αν κάποιος το σκεφτεί είναι λογικό: τι καλύτερο για έναν υπάλληλο που θέλει να εκδικηθεί από το να χαλάσει κάτι που χαλάει εύκολα και κανείς δεν 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.

❖ **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, 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:

o ***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 θυμόμαστε 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 δημιουργήσει 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 τον 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 στην λάθος IP διεύθυνση. Και 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 άτομο 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 νομίμων 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 παρεμπόδιση 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 – Πλαστογραφία.***

Μια ιδιόμορφη περίπτωση που μοιάζει με πλαστογραφία 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 το τόπος αυτός μοιάζει με αυτόν που πραγματικά ήθελε η/ο πελάτης υπάρχει η πιθανότητα να γίνουν συναλλαγές χωρίς να γίνει αντιληπτό το λάθος. Αυτό το κόλπο χρησιμοποιείται με τα ονόματα των εταιρειών με γνωστό όνομα ώστε να «υποκλέπεται» σε 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) **<u>Υποκλοπή συνομιλιών – μηνυμάτων.</u>**

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..

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 για το ποιοι είναι οι κίνδυνοι που περιβάλλουν τον διακομιστή και τι μέτρα ασφάλειας να παρθούν για να προστατευθεί.
Ο διακομιστής δικτύου είναι η μεγαλύτερη απειλή ασφάλειας στο δίκτυο. Αντίθετα, με τις εφόδους στην ασφάλεια ιδιωτικών δικτύων, όπου πολλά προβλήματα συμβαίνουν εξ αιτίας λαθών χρηστών, οι επιθέσεις στο Web διακομιστή γίνονται για δύο 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 μία 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 την 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 μία επίθεση στον 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 την πρόκληση. Ίσως, η εταιρεία να 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 την 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 την τοποθεσία της, ούτε θα αισθάνονται άνετα να κάνουν συναλλαγές βασισμένες στο Διαδίκτυο.

ΤΡΟΠΟΙ ΠΡΟΣΤΑΣΙΑΣ ΤΟΥ (WEB) ΔΙΑΚΟΜΙΣΤΗ ΔΙΚΤΥΟΥ

ΠΟΛΙΤΙΚΗ

Η ασφάλεια του διακομιστή δικτύου είναι ένα άλλο περίπλοκο θέμα ασφαλείας. Το πιο σημαντικό πράγμα που μπορεί να κάνει για το διακομιστή και την τοποθεσία μία εταιρεία ή τράπεζα είναι να ορίσει μια σαφή πολιτική για την Web ασφάλεια.
Αφού η εταιρεία αναπτύξει μια πολιτική, συνεχίζει στην επιλογή των συσκευών που θα συμπληρώνονται 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 την 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.

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 στον 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 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 διάφορους 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 κα κωδικό πρόσβασης που θα του δώσει πρόσβαση. Ωστόσο, όπως και οι περιορισμοί IP διεύθυνσης, 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 έναν 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 της 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 προσθήκη στο πρόγραμμα που 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.

Οι βασικές απαιτήσεις για την ασφαλή διεξαγωγή των ηλεκτρονικών συναλλαγών είναι οι εξής:

- **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.**
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 την ταυτότητα του άλλου. Ο έλεγχος αυθεντικότητας παρέχεται μέσω ψηφιακής υπογραφής.

- **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.

ΜΗΧΑΝΙΣΜΟΙ ΑΣΦΑΛΕΙΑΣ.

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

Κρυπτογράφηση.
Από την 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 μία 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 δύο 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 δύο 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 θέλουμε να στείλουμε 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 καθόλου χρήση 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 τον τρόπο να το διαβάσουν. Για να λειτουργήσει αυτός ο αλγόριθμος χρειάζεται μία 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 κ.α. 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.

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 συναλλασσομένων μερών. Από την στιγμή που δύο άτομα κατέχουν το ίδιο κλειδί, τότε και οι δύο μπορούν να κρυπτογραφήσουν κάποιο μήνυμα και να ισχυριστούν ότι το έστειλε το άλλο άτομο. Κατά συνέπεια, η μη αποποίηση της ευθύνης για την αποστολή ενός μηνύματος καθίσταται και αυτή αδύνατη. Το πρόβλημα αυτό επιλύεται με την κρυπτογράφηση δημόσιου κλειδιού ή ασύμμετρη κρυπτογράφηση.

Όπως και με την συμμετρική μέθοδο κρυπτογράφησης, τα χαρακτηριστικά ασφαλείας που περιγράφονται στην παραπάνω ενότητα, μπορούν επίσης να επιτευχθούν και με την κρυπτογράφηση δημοσίου κλειδιού, όπως δείχνει και ο παρακάτω πίνακας.

Αποστολέας / Κρυπτογραφεί		Δέκτης / Αποκρυπτογραφεί	
Ιδιωτικό κλειδί Αποστολέα	Ακεραιότητα	Δημόσιο κλειδί Αποστολέα	Ο δέκτης συγκρίνει την περιγραφή του μηνύματος με το γνήσιο μήνυμα.
Ιδιωτικό κλειδί Αποστολέα	Πιστοποίηση της Ταυτότητας του Αποστολέα	Δημόσιο κλειδί Αποστολέα	Υποθέτουμε ότι ο πραγματικός αποστολέας έχει στην κατοχή του το ιδιωτικό κλειδί.
Δημόσιο κλειδί Δέκτη	Εμπιστευσιμότητα	Ιδιωτικό κλειδί Δέκτη	Μόνο ο δέκτης μπορεί να διαβάσει το μήνυμα με το ιδιωτικό κλειδί.

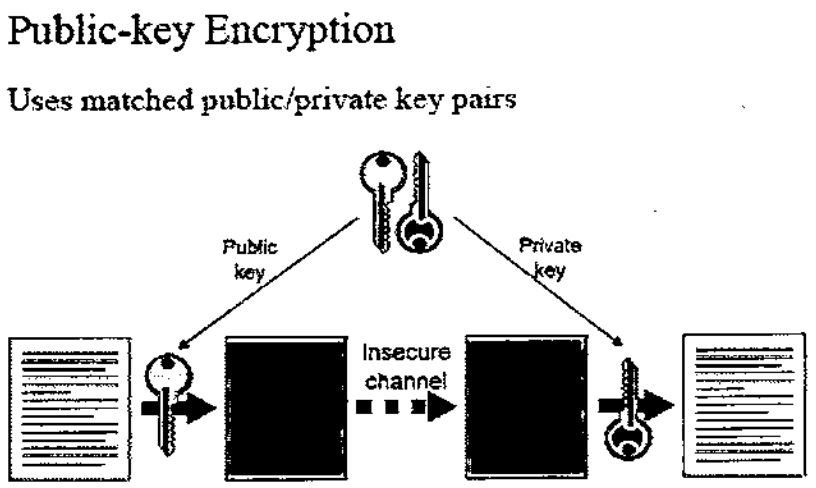
Πίνακας 2: Κρυπτογράφηση Δημοσίου Κλειδιού (Public Key Encryption)

❖ ***Ασύμμετρη κρυπτογράφηση (Asymmetric Key Encryption)***

Η βάση του PKI (Public- Key Encryption) είναι μια τεχνολογία που ονομάζεται κρυπτογράφηση δημόσιου κλειδιού. Η κρυπτογράφηση δημόσιου κλειδιού, 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 δημόσιου κλειδιού οτιδήποτε κρυπτογραφείται με το ένα κλειδί μπορεί να αποκρυπτογραφηθεί χρησιμοποιώντας μόνο το άλλο κλειδί.

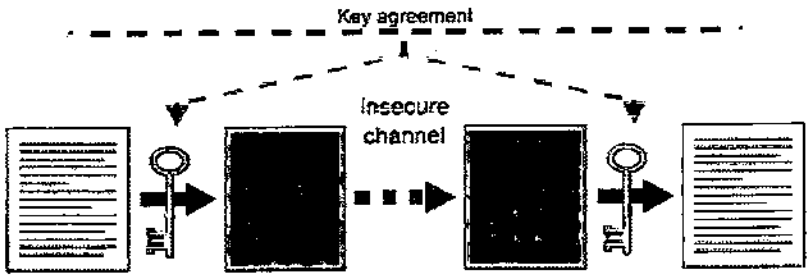
Το κύριο πλεονέκτημα που προσφέρει η κρυπτογράφηση δημόσιου κλειδιού θεωρείται κατάλληλη για το Ηλεκτρονικό Εμπόριο για τους εξής λόγους:

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



Key Agreement

Allows two parties to agree on a shared key



<u>Τα δύο αυτά κλειδιά μπορούν να χρησιμοποιηθούν με δύο διαφορετικούς τρόπους:</u>
Να εξασφαλίσουν την εμπιστευτικότητα του μηνύματος.
Να αποδείξουν την αυθεντικότητα του δημιουργού τους.

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 χρησιμοποιεί 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 δειχθεί 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 "X" ημερομηνία και "Y" 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.

Σε γενικές γραμμές, η τεχνολογική υποδομή ασύμμετρης κρυπτογράφησης θα πρέπει να στηρίζεται όπως τονίζεται και στις οδηγίες της Ευρωπαϊκής Κεντρικής Τράπεζας, στις παρακάτω λειτουργίες και πιστοποιητικά ασφαλείας:

Registration Authority (RA).
Ο ρόλος της Αρχής Εγγραφής είναι να ανιχνεύει την ταυτότητα του προσώπου ή του οργανισμού που διενεργεί την συναλλαγή πριν την έκδοση του ζευγαριού των κλειδιών.

Certification Authority (CA).
Το ζεύγος κλειδιών ασφαλείας εκδίδεται από την Αρχή Πιστοποίησης αφού πρώτα έχουν καταγραφεί τα στοιχεία του ενδιαφερομένου στην Αρχή Εγγραφής (RA). Αναλόγως του επιθυμητού επιπέδου ασφαλείας, το ιδιωτικό κλειδί αποθηκεύεται σε μια έξυπνη κάρτα (smart card), ή σε μία κάρτα SIM ή στον σκληρό δίσκο ενός υπολογιστή. Το δημόσιο κλειδί ασφαλείας αποθηκεύεται στις Υπηρεσίες Καταλόγου.

Directory Services.
Στις υπηρεσίες καταλόγου γίνεται η αποθήκευση των δημοσίων κλειδιών ασφαλείας καθώς και η ανάκτηση τους.
Οι παραπάνω υπηρεσίες προσφέρονται συνήθως από εταιρείες παροχής τέτοιων πιστοποιητικών (Certification Service Providers).

Ασφάλεια Ηλεκτρονικών Καταστημάτων.
Ένα ηλεκτρονικό κατάστημα δεν θα μπορούσε να υλοποιήσει με ασφάλεια τις εμπορικές του συναλλαγές με τους διαφορετικούς πελάτες που εμφανίζονται μέσα από το Internet, αν έπρεπε καθένας από αυτούς να έχει το δικό του προσωπικό κλειδί. Θα ήταν σαν να ζητούσε ο περιπτεράς την ταυτότητα κάθε αγοραστή. Ακόμα χειρότερα, ο επισκέπτης στο Internet θα έπρεπε να διαθέτει διαφορετικές ταυτότητες για κάθε ηλεκτρονικό μαγαζί.
Στο ηλεκτρονικό εμπόριο τα πράγματα, όσον αφορά στην ασφάλεια δεδομένων, είναι πιο απλά. Εδώ χρειάζεται να δώσει ο επισκέπτης τα στοιχεία της πιστωτικής του κάρτας. Φυσικά, απαιτείται και εδώ η ασφαλής συναλλαγή, καθώς αυτά τα στοιχεία είναι απόρρητα και δεν θα πρέπει να καταλήξουν σε άλλα χέρια.

SSL και ασφαλείς συνδέσεις.
Θα έχετε παρατηρήσει ένα λουκετάκι που εμφανίζεται στο κάτω μέρος της οθόνης του υπολογιστή σας, όταν το πρόγραμμα αναζήτησης βρίσκεται σε ασφαλές περιβάλλον.
Πριν περάσετε σε αυτό το «ασφαλές περιβάλλον» (Secure Socket Layer – SSL), εμφανίζεται συνήθως ένα ή περισσότερα προειδοποιητικά μηνύματα από το πρόγραμμα αναζήτησης (φυλλομετρητή). Ακόμα, θα προσέξατε ότι οι «ασφαλείς» σελίδες αρχίζουν από «https://» αντί από το σύνηθες «http://». Στο ασφαλές αυτό περιβάλλον, όλες οι πληροφορίες που διακινούνται από το πρόγραμμα αναζήτησης μέχρι το διακομιστή του ηλεκτρονικού καταστήματος είναι κρυπτογραφημένες.

Ο δημοφιλέστερος μηχανισμός ασφαλούς αποστολής των στοιχείων μιας φόρμας σε ένα e-shop είναι το Secure Socket Layer. Πρόκειται για ένα επίπεδο διαδικασιών το οποίο παρεμβάλλεται μεταξύ του http (που χρησιμοποιεί το browser) και του TCP/IP, το οποίο αποτελεί τη βάση όλων των επικοινωνιών μέσα στο Internet. Με απλά λόγια, θα μπορούσαμε να πούμε ότι το SSL δημιουργεί ένα προσωρινό κανάλι (pipe) δεδομένων μεταξύ δύο σημείων (τον browser του αγοραστή και το δικτυακό τόπο του καταστήματος). Τα δύο άκρα αυτού του καναλιού ονομάζονται sockets και μέσα σε αυτό κυκλοφορούν τα δεδομένα που ανταλλάσσουν οι δύο πλευρές, κρυπτογραφημένα με το public- and- private key encryption system της RSA.
Στην εφαρμογή του SSL οι δύο πλευρές (τα δύο άκρα του καναλιού) χρησιμοποιούν για την επικοινωνία τους μια πιο ασφαλή παραλλαγή του http γνωστή με το όνομα HTTPS (Secure Hypertext Transfer Protocol). Για να ελέγξετε αν μια σελίδα χρησιμοποιεί SSL μπορείτε να δείτε την διεύθυνση της (URL). Αν αυτή αρχίζει από https://, τότε η σελίδα υλοποιεί πράγματι SSL.
Σε όλη αυτή τη διαδικασία συμμετέχει και ένας τρίτος παράγοντας (γνωστός με το όνομα "Έμπιστη Τρίτη Οντότητα" ή Trusted Third Party), ο οποίος εγγυάται ότι οι δύο πλευρές είναι πράγματι εκείνες που ισχυρίζονται και δεν έχει γίνει κάποια «πλαστοπροσωπία» (π.χ. ο δικτυακός τόπος ανήκει πράγματι στην εταιρεία Χ και ο πελάτης δεν έχει δρομολογηθεί εν αγνοία του σε έναν «πειρατικό» δικτυακό τόπο ο οποίος θα τον χρεώσει, αλλά δεν θα παραδώσει τα προϊόντα). Η έμπιστη τρίτη οντότητα πιστοποιεί την ταυτότητα του server με τη χρήση ενός digital certificate. Το πιστοποιητικό αυτό αποτελεί ένα είδος ηλεκτρονικής κάρτας αναγνώρισης, η οποία περιέχει έναν ειδικό αναγνωριστικό αριθμό, μια ημερομηνία λήξεως, το δημόσιο κρυπτογραφικό κλειδί του καταστήματος (για την κρυπτογράφηση και την αποκρυπτογράφηση δεδομένων και ηλεκτρονικών υπογραφών), καθώς και την ηλεκτρονική υπογραφή της έμπιστης τρίτης οντότητας.
Σήμερα, υπάρχουν πολλές εταιρείες οι οποίες παρέχουν αυτή την υπηρεσία. Ενδεικτικά αναφέρουμε τις Belsign (http://www.belsign.com), CyberTrust (http://www.cybertrust.com), Entrust (http://www.entrtust.com) και Verisign (http://www.verisign.com) . Παρά τις διαφορετικές τιμολογιακές τους πολιτικές, όλες παρέχουν την ίδια βασική υπηρεσία και ο τελικός χρήστης δεν θα καταλάβει καμία διαφορά, όποια από αυτές και αν επιλέξει το κατάστημα. Είναι βέβαιο ότι κάποιες από τις εταιρείες που παρέχουν παρόμοιες υπηρεσίες είναι πολύ πιο ασφαλείς και αξιόπιστες από τις άλλες. Δυστυχώς, ο χρήστης (στην περίπτωση μας το ηλεκτρονικό κατάστημα) δεν έχει συνήθως τη δυνατότητα ή τη γνώση να ελέγξει ποια από αυτές είναι η πιο ασφαλής, ενώ η μέχρι σήμερα εμπειρία έχει δείξει ότι ο ακριβότερος δεν είναι πάντοτε ο καλύτερος.
Η ιδανική μέθοδος πιστοποίησης είναι εκείνη στην οποία και οι δύο πλευρές διαθέτουν τα δικά τους αυτόνομα πιστοποιητικά. Έτσι, το λογισμικό του πελάτη (στην προκείμενη περίπτωση ο browser) ελέγχει το πιστοποιητικό του πελάτη για να εξασφαλίσει ότι ο πελάτης είναι πράγματι αυτός που ισχυρίζεται και όχι κάποιος τρίτος, ο οποίος θέλει να αγοράσει προϊόντα, χρεώνοντας τα σε έναν άλλο. (Αυτή τη μέθοδο υλοποιεί το https μέσω public- and- private key encryption).
Δυστυχώς, μέχρι σήμερα οι χρήστες του δικτύου έχουν αποδειχθεί απρόθυμοι να αποκτήσουν πιστοποιητικά αυτής της μορφής. Έτσι, ενώ ο πελάτης μπορεί να είναι σίγουρος για την ταυτότητα του πωλητή (όσο σίγουρος δηλαδή μπορεί να είναι κανείς για οτιδήποτε σε αυτό τον κόσμο), ο πωλητής δεν γνωρίζει ποιος είναι αυτός με τον οποίο συναλλάσσεται (το SSL, πιστοποιεί μόνο την ταυτότητα του server). Αυτό σημαίνει ότι, αν κάποιος τρίτος γνωρίζει τα στοιχεία της κάρτας ενός χρήστη,

μπορεί να επισκεφθεί οποιοδήποτε ηλεκτρονικό κατάστημα και να αγοράσει ότι επιθυμεί, χρεώνοντας το λογαριασμό του πραγματικού κατόχου της κάρτας.
Για να προστατευτούν οι καταναλωτές από αυτό τον κίνδυνο, υπάρχει ειδική νομοθεσία, τόσο στην Ευρωπαϊκή Ένωση όσο και στις ΗΠΑ, η οποία ορίζει ότι ο κάτοχος της κάρτας μπορεί να αρνηθεί τη χρέωση οποιασδήποτε συναλλαγής έχει πραγματοποιηθεί χωρίς την παρουσίαση του φυσικού σώματος της κάρτας. Η συλλογιστική για τη διάταξη αυτή είναι ότι εγώ είμαι υπεύθυνος για την κάρτα μου και αν τη χάσω η ευθύνη της ακύρωσης της βαραίνει μόνο εμένα. Τα στοιχεία της όμως μπορεί να τα αποκτήσει οποιοσδήποτε (π.χ. ο πωλητής του πολυκαταστήματος από τον οποίο αγόρασα ένα ζευγάρι κάλτσες) χωρίς δική μου γνώση ή υπαιτιότητα.

Έτσι, σε περίπτωση συναλλαγών on-line με κλεμμένα στοιχεία καρτών, ο κάτοχος όταν δει τη χρέωση στο αντίγραφο του λογαριασμό του μπορεί να αρνηθεί να πληρώσει και η τράπεζα όχι μόνο δεν θα καταβάλει το ποσό αυτό στον πωλητή, αλλά θα χρεώσει και το κατάστημα 15 δολάρια για τα έξοδα ακύρωσης (η χρέωση αυτή αποτελεί απόφαση της MasterCard η οποία θα τέθηκε σε ισχύ).
Εννοείται φυσικά πως το ηλεκτρονικό κατάστημα έχει το δικαίωμα να δϊώξει δικαστικά τον παραλήπτη των προϊόντων που παραγγέλθηκαν με αυτή την κάρτα, ζητώντας αποζημίωση. Δυστυχώς όμως, το δύσκολο έργο της ανακάλυψης του ενόχου και της τιμωρίας του σπάνια έχει αίσιο τέλος. Στην πλειονότητα των περιπτώσεων μάλιστα αυτό είναι πρακτικώς αδύνατον (π.χ. τα έξοδα δίωξης κατοίκου άλλης χώρας είναι τόσο υψηλά που δεν αξίζει τον κόπο να ασχοληθεί κανείς με το θέμα). Γι' αυτό και τα ηλεκτρονικά καταστήματα προτιμούν την πρόληψη από τη θεραπεία.

Παραδείγματα Ασύμμετρων τεχνικών κρυπτογράφησης.
Secure Socket Layer Security:
Η τεχνολογία του SSL, είναι ένα από τα πιο γνωστά πρωτόκολλα επικοινωνίας που εξυπηρετούν μεθόδους ασύμμετρης κρυπτογράφησης. Συγκεκριμένα χρησιμοποιείται για να εξασφαλίσει ασφαλή σύνδεση μεταξύ του χρήστη και του κεντρικού διακομιστή. Το πρωτόκολλο SSL παρέχει ακεραιότητα και ασφάλεια στα δεδομένα που διακινούνται, μεταξύ του καταναλωτή και του εμπόρου. Πρώτα υλοποιήθηκε από την εταιρεία Netscape αργότερα υιοθετήθηκε από την Internet Engineering Task Force (IETF) σαν γενικό πρωτόκολλο ασφαλείας. Χρησιμοποιείται επίσης ευρέως και σε πολλά συστήματα ηλεκτρονικής τραπεζικής (Internet Banking). Εικονικά θα μπορούσαμε να πούμε ότι τα περισσότερα προγράμματα προβολής ιστοσελίδων (Web Browsers), χρησιμοποιούν την τεχνολογία SSL για να αυθεντικοποιούν και να κρυπτογραφούν τα δεδομένα που διακινούνται. Τέλος, πρέπει να τονίσουμε ότι η τεχνολογία SSL, δεν παρέχει το χαρακτηριστικό συνολικής ασφαλείας περί της απόδειξης πραγματοποίησης της συναλλαγής (non-repudiation). Η μετεξέλιξη του πρωτοκόλλου επικοινωνίας SSL αναφέρεται να είναι το Transport Layer Security (TLS).

Συστήματα ασφαλείας που χρησιμοποιούνται για την αγορά μέσω πιστωτικών καρτών:
Ένα από τα ποιο διαδεδομένα συστήματα ασφαλείας στις αγορές μέσω πιστωτικών καρτών αναφέρεται να είναι το SET (Security Electronic Transaction), βασίζεται στη μέθοδο PKI. Υλοποιήθηκε στις αρχές τις δεκαετίας του 1990 από τις εταιρίες παροχής πιστωτικών καρτών και χρηματοπιστωτικών συναλλαγών VISA και MasterCard.

Το SET παρέχει τα ακόλουθα χαρακτηριστικά ασφαλείας: αυθεντικοποίηση, ακεραιότητα, ασφάλεια των δεδομένων από τρίτους και δυνατότητα απόδειξης της συναλλαγής. Επιπλέον, παρέχει τη δυνατότητα κρυπτογράφησης των δεδομένων που διακινούνται μέσω του διαδικτύου αλλά και φύλαξης ευαίσθητων πληροφοριών που περιέχονται πάνω στην πιστωτική κάρτα, όπως η ημερομηνία έκδοσής της, από τρίτα μέρη όπως ο έμπορος.

Το πρωτόκολλο SET βασίζεται σε μια ιεραρχική διαδικασία αυθεντικοποίησης (trust chaining). Παρόλα αυτά το SET, είναι ένα ακριβό σύστημα και η διαδικασία εισαγωγής του σε έναν οργανισμό αρκετά περίπλοκη. Έτσι, το 2001 μεγάλες εταιρείες έκδοσης πιστωτικών καρτών προχώρησαν στην υλοποίηση νέων συστημάτων αυθεντικοποίησης, για την ασφάλεια διαδικτυακών συναλλαγών. Η VISA για παράδειγμα εισήγαγε ένα νέο σύστημα με την επωνυμία 3-D Secure ή αλλιώς είναι ευρέως γνωστό ως "Verified by VISA", και αντίστοιχα η MasterCard εισήγαγε το SPA (Secure Payment Application). Και τα δύο αυτά συστήματα χρησιμοποιούν τεχνολογία SSL για να εξασφαλίσουν τα προαναφερθέντα χαρακτηριστικά ασφάλειας στις συναλλαγές. Το 3-D Secure χρειάζεται ένα αποθηκευμένο όνομα χρήστη (Username) και έναν προσωπικό κωδικό πρόσβασης (Password), από τον πελάτη που θέλει να προχωρήσει σε μία αγορά και επαληθεύει τα στοιχεία του με τον κεντρικό διακομηστή της VISA. Τα πιστοποιητικά ασφαλείας PKI χρησιμοποιούνται μόνο για το μέρος της συναλλαγής μεταξύ του εμπόρου και της τράπεζας που έχει εκδώσει την κάρτα VISA. Το Mastercard SPA παρέχει διάφορους τρόπους αυθεντικοποίησης της ταυτότητας του πελάτη, για παράδειγμα μέσω του αποθηκευμένου ονόματος χρήστη (Username) και προσωπικού κωδικού πρόσβασης (Password), μέσω μίας έξυπνης κάρτας (Smartcard), μέσω ψηφιακών πιστοποιητικών ή ακόμα και βιομετρικών μεθόδων. Ο χρήστης είναι αυτός που προσδιορίζει τον τρόπο που θα έχει πρόσβαση στον λογαριασμό του.

CEPS – Common Electronic Purse Specification:
Το CEPS είναι ένα πρωτόκολλο διαχείρισης ηλεκτρονικού χρήματος που χρησιμοποιεί ως μέσω συναλλαγής τις πλαστικές κάρτες. Σχεδιάστηκε για να εξυπηρετεί τη διακίνηση χρήματος ηλεκτρονικά και κυρίως εξυπηρετεί όταν πρόκειται για μεταφορά νομισμάτων διαφορετικών εθνικοτήτων. Το σύστημα αυτό παρέχει υψηλά επίπεδα ασφάλειας χρησιμοποιώντας τεχνολογία τύπου PKI.

Συστήματα PKI σε δίκτυα κινητής τηλεφωνίας:
Όπως αναφέρθηκε πιο πάνω, τα δίκτυα κινητής τηλεφωνίας παρουσιάζουν σημαντικές ευκαιρίες ανάπτυξης ηλεκτρονικών πληρωμών. Το κινητό τηλέφωνο έχει τη δυνατότητα να χρησιμοποιηθεί ως μία τερματική συσκευή διεκπεραίωσης ηλεκτρονικών πληρωμών. Τα τελευταία χρόνια γίνεται εκτενής έρευνα σχετικά με τη συμβατότητα του πρωτοκόλλου PKI και τις συσκευές κινητών τηλεφώνων. Τα αποτελέσματα αυτά τα βλέπουμε πλέον στα κινητά τηλέφωνα τρίτης γενιάς, στα οποία σε συνδυασμό με τα ασύρματα δίκτυα επικοινωνίας GPRS και UMTS διευκολύνεται σημαντικά η πραγματοποίηση ηλεκτρονικών πληρωμών.

ΣΥΣΤΗΜΑΤΑ ΑΣΦΑΛΕΙΑΣ ΗΛΕΚΤΡΟΝΙΚΩΝ ΠΛΗΡΩΜΩΝ ΣΤΙΣ ΧΩΡΕΣ ΤΗΣ ΕΥΡΩΠΑΪΚΗΣ ΈΝΩΣΗΣ

Πολλά συστήματα PKI χρησιμοποιούνται στην Ευρώπη τα τελευταία χρόνια, παρακάτω αναφέρονται τα σημαντικότερα από αυτά.

Στο Βέλγιο, οι μεγαλύτερες τράπεζες μαζί με τον κεντρικό οργανισμό χρεωστικών καρτών (Banksys), το κεντρικό διατραπεζικό σύστημα (ISABEL), και το Βελγικό οργανισμό ταχυδρομείων ίδρυσαν μία εταιρεία που παρέχει ψηφιακά πιστοποιητικά αυθεντικοποίησης, την ECERTIO. Οι πελάτες των παραπάνω οργανισμών χρησιμοποιούν αυτά τα πιστοποιητικά για να εκτελέσουν ηλεκτρονικές συναλλαγές, με τις τράπεζες τους, την κυβέρνηση και για να πραγματοποιήσουν επίσης ηλεκτρονικές αγορές.

Στη Φινλανδία, αρκετά συστήματα που χρησιμοποιούν τεχνολογία τύπου PKI έχουν υλοποιηθεί επίσης,ο οργανισμός καταμέτρησης πληθυσμού έχει προχωρήσει στην έκδοση ηλεκτρονικών καρτών αναγνώρισης προσώπων. Οι χρήστες μπορούν μέσω αυτών των καρτών να συναλλαγούν ηλεκτρονικά με κρατικές υπηρεσίες. Επίσης έχουν υλοποιηθεί αρκετά συστήματα που βασίζονται σε τεχνολογίες τύπου SET, EMV (Euro pay, MasterCard, Visa) και SIM. Ο οργανισμός Certall είναι το αποτέλεσμα μια κοινής προσπάθειας μεταξύ των χρηματοπιστωτικών ιδρυμάτων και των φινλανδικών ταχυδρομείων, στη δημιουργία ενός κοινού προτύπου PKI το οποίο θα υιοθετηθεί από τους παραπάνω φορείς.

Στην Γαλλία, συστήματα που χρησιμοποιούν τεχνολογία τύπου PKI χρησιμοποιούνται για την ηλεκτρονική εκκαθάριση φόρων, αλλά επίσης έχουν γίνει και πολλές προσπάθειες στο χώρο της υγείας, όπου οι ασθενείς μπορούν να πληρώνουν ηλεκτρονικά της υπηρεσίες που δέχονται (SESAME/VITALE).

Στην Γερμανία, πολλά παραδείγματα χρησιμοποίησης τεχνολογιών τύπου PKI έχουν καταγραφεί στον χώρο της υγείας, των συναλλαγών με το δημόσιο τομέα, στο εμπόριο, στη βιομηχανία και τέλος και στον τραπεζικό τομέα. Ακολουθώντας την Ευρωπαϊκή οδηγία σχετικά με τις ηλεκτρονικές υπογραφές που εκδόθηκε στις 16 Μαΐου 2001 η γερμανική κυβέρνηση προχώρησε στην ίδρυση του οργανισμού Regulierungsbehorde fur Post und Telekommunikation, που λειτουργεί ως ρυθμιστικό όργανο στην τηλεπικοινωνιακή αγορά και στις ταχυδρομικές υπηρεσίες. Στον χώρο

της ηλεκτρονικής διακυβέρνησης, η γερμανική κυβέρνηση προχώρησε στην πρωτοβουλία υλοποίησης του συστήματος «Bund Online», το οποίο είναι ένα σύστημα που βασίζεται σε τεχνολογία τύπου PKI και εξυπηρετεί τις ηλεκτρονικές συναλλαγές του πολίτη με το κράτος.

Στην Ιταλία ο βαθμός συνεργασίας μεταξύ δημοσίων και ιδιωτικών φορέων κρίνεται ικανοποιητικός, αν και ακολουθείται μία παραδοσιακή ιεραρχική μορφή συνεργασίας. Η κεντρική τράπεζα της Ιταλίας (Banca d'Italia), το κράτος και αρκετοί ιδιωτικοί οργανισμοί έκδοσης ψηφιακών πιστοποιητικών έχουν προχωρήσει σε συνεργασία για να σχεδιάσουν ένα κοινό πλαίσιο συνεργασίας σε εθνικό επίπεδο, σχετικά με την υλοποίηση μίας κοινής τεχνολογικής υποδομής που θα βασίζεται σε τεχνολογία τύπου PKI.

Στη Νορβηγία, έχει δημιουργηθεί μια ενιαία τεχνολογική πλατφόρμα, βασιζόμενη σε τεχνολογία τύπου PKI η οποία λειτουργεί σε εθνικό επίπεδο επιτρέποντας την αναγνώριση φυσικών προσώπων μέσω της χρήσης έξυπνων καρτών.

Τα πλεονεκτήματα της εφαρμογής μιας κοινής τεχνολογικής πλατφόρμας σε εθνικό επίπεδο είναι αρκετά και τα σημαντικότερα από αυτά είναι:
α) μεγαλύτερη εμπιστοσύνη των καταναλωτών,
β) χαμηλότερα κόστη συναλλαγών,
γ) απλοποίηση διαδικασιών και
ε) περισσότερες και ενοποιημένες υπηρεσίες.

Στην Ισπανία, έχουν καταγραφεί αρκετές πρωτοβουλίες σχετικά με την υιοθέτηση ψηφιακών υπογραφών, επιτρέποντας την αποτελεσματική διεξαγωγή ηλεκτρονικών συναλλαγών σε ιδιωτικό αλλά και σε δημόσιο τομέα. Τα πιστοποιητικά έκδοσης ψηφιακών συναλλαγών βασίζονται κυρίως στο πρωτόκολλο X.509 ή σε τεχνολογίες τύπου SET.

Οι προβληματισμοί που ακολουθούν σχετικά με την υιοθέτηση μιας δημόσιας πλατφόρμας διεξαγωγής ηλεκτρονικών πληρωμών χωρίζεται σε θέματα που αφορούν τη νομοθεσία, τεχνικά και οργανωσιακά θέματα και τέλος σε ζητήματα συμβατότητας και συνεργασίας με άλλα συστήματα.
Η υιοθέτηση ενός PKI συστήματος απαιτεί ακριβείς κανόνες εφαρμογής και υλοποίησης ώστε να εγγυηθούν την ορθή χρήση των ψηφιακών πιστοποιητικών, αλλά και την γνησιότητα τους.

Τα θέματα που προκύπτουν λοιπόν είναι:
Πώς μπορεί να διασφαλιστεί η εμπιστοσύνη στους οργανισμούς που παρέχουν τα δημόσια κλειδιά πιστοποίησης (CA certificates);
Πόσο προσεχτικά θα γίνεται ο έλεγχος δημοσίων κλειδιών πιστοποίησης;
Πώς θα προστατεύονται τα ιδιωτικά κλειδιά ασφαλείας από κλοπές και που θα διαφυλάσσονται;
Ποιος οργανισμός θα αναλάβει τη φύλαξή τους;
Πώς θα εξασφαλίζεται η ακεραιότητα των ψηφιακών πιστοποιητικών και υπογραφών, και ποιοι οργανισμοί θα έχουν δικαίωμα έκδοσης αυτών;

Μέχρι σήμερα η υλοποίηση συστημάτων βασιζόμενα σε τεχνολογία PKI επικεντρώνεται στην κάλυψη ενός μεγάλου αριθμού χρηστών σε συγκεκριμένα οργανωσιακά περιβάλλοντα. Αυτά τα συστήματα υλοποιούνται από μεγάλα επιχειρησιακά σχήματα με σκοπό να καλύψουν τις επιχειρησιακές τους ανάγκες (όπως χρηματοοικονομικές υπηρεσίες). Για να επιτύχουν όμως τον μέγιστο βαθμό ασφαλείας σε επίπεδο οργανισμού, και όχι μόνο κάλυψης των ηλεκτρονικών συναλλαγών, αναγκάζονται να στραφούν σε άλλες τεχνολογικές πλατφόρμες, που βασίζονται επίσης σε εργαλεία κρυπτογράφησης και σε τεχνολογία τύπου PKI, αλλά κρατούν την πληροφορία σε ένα άλλο επίπεδο, ενδο-οργανωσιακό. Έχει παρατηρηθεί όμως ότι πολλές φορές είναι δύσκολο, ή προκύπτει χρονική καθυστέρηση για τον συγχρονισμό της πληροφορίας σε αυτά τα δύο επίπεδα.

Ακόμη, πολλές φορές η διαχείριση των ηλεκτρονικών πιστοποιητικών και πληροφοριών των πελατών γίνεται από ανεξάρτητες εταιρίες. Πολλές φορές όμως επειδή οι πληροφορίες που διαχειρίζονται είναι ιδιαίτερα ευαίσθητες και πολύτιμες, οι εταιρίες αυτές συνήθως εξαγοράζονται από μεγάλους τραπεζικούς ομίλους που αποκτούν πρόσβαση στα μητρώα πελατών μικρότερων χρηματοπιστωτικών ιδρυμάτων. Έτσι λοιπόν προκύπτει ένα μεγάλο θέμα σχετικά με τη διαχείριση αυτών των πληροφοριών καθώς οι μικρότερες τράπεζες υποστηρίζουν ότι πέφτουν θύματα αθέμιτου ανταγωνισμού.

Η ΗΛΕΚΤΡΟΝΚΗ ΤΡΑΠΕΖΙΚΗ (E- BANKING) ΣΤΗΝ ΕΛΛΑΔΑ.

Τράπεζες που δραστηριοποιούνται στην ηλεκτρονική τραπεζική (e- banking) στην Ελλάδα.

Με την διαχείριση του Internet, οι τραπεζικές συναλλαγές έχουν γίνει πιο εύκολες, πιο κατανοητές και ουσιαστικά γρηγορότερες. Επίσης, οι ενδόμυχοι φόβοι μας για την ασφάλεια του τραπεζικού μας λογαριασμού έχουν εξαφανιστεί, καθώς οι τράπεζες αποδεικνύονται ιδιαίτερα προσεκτικές στον τομέα της ασφάλειας και της πιστοποίησης του χρήστη, ακολουθώντας κατά γράμμα τις διεθνείς πρακτικές.
Εκτός από την άνεση του σπιτιού και την 24ωρη εξυπηρέτηση, οι συναλλαγές από το Internet αρχίζουν σιγά σιγά να γίνονται επιτακτική ανάγκη για τον καθένα. Κι αυτό γιατί οι τράπεζες έχουν ήδη ξεκινήσει να αποτρέπουν τους πελάτες τους από την χρήση του γκισέ, θεωρώντας πιο οικονομική την λύση του ATM, του Internet ή ακόμα και του τηλεφώνου (Phone Banking). Δεν είναι άλλωστε λίγα τα παραδείγματα των τραπεζών που χρεώνουν τους πελάτες με προμήθεια για όποια συναλλαγή γίνετε μέσω γκισέ και δεν αφορούν δικούς μας λογαριασμούς, όπως είναι η κατάθεση μετρητών σε τρίτους.
Τι μπορεί όμως να κάνει κανείς από το Internet; Σχεδόν τα πάντα, εκτός από το να πάρει στο χέρι του μετρητά. Μπορεί να δει το υπόλοιπο του λογαριασμού του, να πληρώσει την ΔΕΗ και τον ΟΤΕ, να μεταφέρει ένα ποσό σε έναν άλλο λογαριασμό, να πληρώσει μια οφειλή και να βεβαιωθεί για το υπόλοιπο της πιστωτικής του κάρτας πριν πάει για ψώνια. Όλα αυτά γίνονται χωρίς καμία χρέωση και χωρίς την αντίστοιχη προμήθεια, όπως γίνεται στα γκισέ των τραπεζών και στο ταχυδρομείο στην περίπτωση της εξόφλησης λογαριασμών. Αφού λοιπόν κάποιος διαθέτει Internet, καλό είναι να αποκτήσει πρόσβαση και στους τραπεζικούς του λογαριασμούς. Δεν κοστίζει τίποτα, αλλά εξοικονομεί πολύτιμο χρόνο, μερικά έως αρκετά ευρώ και γλιτώνει τον κόσμο από άγχος και ταλαιπωρία.
Σύμφωνα με τις τελευταίες μετρήσεις, αν και τα ATM παραμένουν πρώτα στις προτιμήσεις, το Internet φαίνεται να κερδίζει ολοένα και περισσότερο έδαφος χάρη στα πλεονεκτήματα και στις χαμηλότερες χρεώσεις που προσφέρει. Με το e-banking μπορεί κανείς να «μεταφέρει» την τράπεζα στο σπίτι του. Η λειτουργία του είναι απλή και μοιάζει με αυτή των ATM (Automatic Teller Machine ή Αυτόματη Ταμειολογιστική Μηχανή), των γνωστών σε όλους μηχανημάτων για αυτόματες συναλλαγές. Υπάρχει όμως μια ουσιαστική διαφορά που δείχνει τον ανθρώπινο χαρακτήρα του e-banking και γενικότερα του Internet: η δυνατότητα να κάνει κάποιος συναλλαγές από το σπίτι του οποιαδήποτε μέρα και ώρα θελήσει, τα Σαββατοκύριακα, τις αργίες ακόμα και στις 3 τα ξημερώματα. Επιπλέον, οι συναλλαγές δεν περιορίζονται σε αυτές τις δύο, τρεις που διαθέτουν τα ATM. Το e-banking επιτρέπει να έχει κανείς μια εικόνα από όλα τα τραπεζικά του προϊόντα, τους λογαριασμούς, τις πιστωτικές κάρτες και τα δάνεια. Στην περίπτωση των λογαριασμών μπορεί να δει το υπόλοιπο, τις κινήσεις των λογαριασμών σε αρκετό βάθος χρόνου και φυσικά το e-banking υποστηρίζει πολλαπλούς λογαριασμούς από διαφορετικά υποκαταστήματα. Στην περίπτωση των πιστωτικών καρτών είναι δυνατή η ενημέρωση για το πιστωτικό όριο, το τρέχον υπόλοιπο, καθώς και για όλες τις συναλλαγές. Το πιο σημαντικό όμως είναι η δυνατότητα των πληρωμών και των εμβασμάτων. Μπορεί κανείς να πληρώσει τη δόση της πιστωτικής του κάρτας ή του δανείου του, αλλά και να εξοφλήσει τους λογαριασμούς ΔΕΗ, ΟΤΕ, κινητής τηλεφωνίας κ.λ.π.. Επιπλέον, μπορεί να ορίσει την πληρωμή του ενοικίου του την

πρώτη ημέρα του μήνα, δίνοντας μια πάγια εντολή αλλά και να μεταφέρει λεφτά στο εξωτερικό αν το παιδί του σπουδάζει σε μια ξένη χώρα. Όλες αυτές οι συναλλαγές που είναι εφικτές από το σπίτι είναι ιδιαίτερα χρήσιμες σε περιόδους διακοπών και εορτών. Επιπλέον μέσω του e-banking, εξοφλούνται οι οφειλές στο ΙΚΑ, στο ΤΕΒΕ και ο ΦΠΑ. Ορισμένες τράπεζες μάλιστα δίνουν στον πελάτη τους την δυνατότητα τηλεειδοποίησης μέσω μηνυμάτων SMS ή e-mail, με μια μικρή χρέωση, ενημερώνοντας τους άμεσα για οποιαδήποτε κίνηση του λογαριασμού τους.
Για τους αμετανόητους προσφέρεται και η δυνατότητα άμεσης πρόσβασης στο χαρτοφυλάκιο των μετοχών τους, με άμεση ενημέρωση των τιμών των μετοχών και φυσικά την αγοραπωλησία τους.

Κέρδος για τις τράπεζες

Οι συναλλαγές μέσω του Internet, δεν εξασφαλίζουν μόνο στον πολίτη την άνεση που επιθυμεί αλλά και στις τράπεζες ένα πολύ μικρότερο κόστος συναλλαγών. Την τελευταία δεκαετία οι τράπεζες επένδυσαν σημαντικά ποσά σε τεχνολογικές υποδομές προκειμένου να αποσυμφορήσουν τις ουρές στα γκισέ των υποκαταστημάτων τους. Ακόμα ένας λόγος είναι ότι οι παραδοσιακές συναλλαγές στο γκισέ κοστίζουν ακριβά σε αντίθεση με τα εναλλακτικά δίκτυα που κοστίζουν ελάχιστα και εξοικονομούν πολύτιμο χρόνο στους καταναλωτές. Σύμφωνα με μελέτη του Booz Allen & Hamilton, μια τυπική τραπεζική συναλλαγή, όπως η κατάθεση, η ανάληψη, η ερώτηση υπολοίπου και η μεταφορά ποσού σε άλλο λογαριασμό, όταν πραγματοποιείται στο γκισέ και απασχολεί ανθρώπινο δυναμικό κοστίζει 1,01€. Η ίδια συναλλαγή όταν πραγματοποιείται σε μηχάνημα ATM κοστίζει 0,24€, ενώ μέσω Internet το κόστος της ουσιαστικά μηδενίζεται, αφού υπολογίζεται ότι κοστίζει μόλις 0,01€.

Τα απαραίτητα βήματα για να μπορέσει κάποιος να κάνει e-banking είναι τα εξής:

Στην συνέχεια ακολουθεί μία αναλυτική παρουσίαση των υπηρεσιών που προσφέρουν 12 τράπεζες που δραστηριοποιούνται στον χώρο της Ελλάδας.

Alpha bank

Η ιστοσελίδα της τράπεζας χαρακτηρίζεται ισορροπημένη και παρουσιάζει πλούσια γκάμα υπηρεσιών, λιτό και προσεγμένο σχεδιασμό και προσφορά εργαλείων στους χρήστες. Μαζί με την Eurobank έχουν τους περισσότερους εγγεγραμμένους χρήστες, περίπου 15,000. Η Alpha Bank διαθέτει ένα από τα καλύτερα sites και προσφέρει υπηρεσίες όπως υπόλοιπα λογαριασμών και πρόσφατες κινήσεις, παραγγελία μπλοκ επιταγών και αντίγραφα λογαριασμών, εντολές αυτόματης εξόφλησης λογαριασμών (ΔΕΗ, ΟΤΕ, ΕΥΔΑΠ κ.α.) και ανάκληση των εντολών, μεταφορές χρημάτων στην ίδια τράπεζα, πληρωμές καρτών και δανείων της Alpha, πληρωμές ΦΠΑ και Vodafone, ισοτιμίες ξένων νομισμάτων, πληροφορίες για μετοχές, επενδυτικά και ασφαλιστικά προϊόντα, επιτόκια, υποβολή βιογραφικού σημειώματος, τιμές μετοχών κ.α. Υπάρχει δυσκολία στο να εντοπίσει κανείς τηλέφωνα επικοινωνίας για την υποστήριξη πελατών αλλά προσφέρονται αρκετά κατατοπιστικά εργαλεία για την διευκόλυνση των χρηστών. Επίσης, υπάρχει χάρτης πλοήγησης και μηχανή αναζήτησης. Γενικά η ιστοσελίδα της Alpha Bank θα λέγαμε ότι ικανοποιεί τον μέσο χρήστη αλλά θα πρέπει να βελτιωθεί για να φτάσει στην κορυφή.

Eurobank

Η ιστοσελίδα της Eurobank αποτελεί μία αξιόλογη πρόταση που διεκδικεί τα σκήπτρα και σε κάποιους τομείς τα καταφέρνει παρά τον σκληρό ανταγωνισμό. Η μεγάλη γκάμα προϊόντων, ο επαγγελματικός σχεδιασμός των σελίδων και η άρτια υποστήριξη των πελατών αποδεικνύουν το πόσο η τράπεζα αναγνωρίζει την σημασία του ηλεκτρονικού επιχειρείν (e- business) και επενδύει σε αυτό. Είναι από τις λίγες τράπεζες που δραστηριοποιούνται και στον χώρο του ηλεκτρονικού εμπορίου προσφέροντας υπηρεσίες σε επιχειρήσεις που δρουν στον χώρο αυτό. Μέσω του διαδικτύου προσφέρει υπηρεσίες όπως: υπόλοιπα λογαριασμών και προηγούμενες κινήσεις, μεταφορές χρημάτων μεταξύ λογαριασμών της ίδιας τράπεζας στην Ελλάδα, αγοραπωλησία μετοχών, δημόσιες εγγραφές, ενημέρωση για το χαρτοφυλάκιο του πελάτη, αγοραπωλησία αμοιβαίων κεφαλαίων, πληρωμές καρτών και δανείων της Eurobank, πληρωμή ΦΠΑ, ενημέρωση για τις τιμές μετοχών, πληροφορίες για το ευρώ, ανακοίνωση θέσεων εργασίας, υποβολή αίτησης για παροχή υπηρεσιών ηλεκτρονικά κ.α. Θα πρέπει εδώ να τονίσουμε ότι η ιστοσελίδα της Eurobank είναι "portal" δηλαδή παρέχει πληροφορίες και για άλλα θέματα όπως για παράδειγμα νέα από το Χρηματιστήριο εκείνη την στιγμή "on line". Η αρτιότητα και η αισθητική των σελίδων είναι από τις καλύτερες, αλλά θα πρέπει να αναφέρουμε σαν μειονέκτημα την απουσία χάρτη πλοήγησης και μηχανών αναζήτησης τα οποία διευκολύνουν ιδιαίτερα τον χρήστη.

Τράπεζα Πειραιώς (Winbank)

Η ιστοσελίδα της κρίνεται πάρα πολύ καλή καθώς έχει γίνει εξαιρετική δουλειά και η Winbank θεωρείται η πρώτη ολοκληρωμένη ηλεκτρονική τράπεζα στην Ελλάδα με περίπου 10,000 χρήστες. Το φάσμα των προσφερόμενων υπηρεσιών είναι ευρύτατο, ο σχεδιασμός του site εξαιρετικός με μεγάλη λειτουργικότητα και πλήθος υπηρεσιών. Οι πληροφορίες είναι πάντοτε ενημερωμένες και προσφέρονται με φιλικό και εύληπτο τρόπο και επίσης η ισορροπία κειμένου και γραφικών είναι ιδιαίτερα προσεγμένη. Η τράπεζα δραστηριοποιείται στον χώρο του ηλεκτρονικού εμπορίου προσφέροντας υπηρεσίες σε επιχειρήσεις που δρουν στον χώρο αυτό. Μερικές από τις υπηρεσίες που προσφέρει η τράπεζα μέσω διαδικτύου είναι: ενημέρωση για τους λογαριασμούς και τις επενδύσεις των πελατών, πληροφόρηση για τις αναλυτικές κινήσεις των λογαριασμών, παραγγελία για μπλοκ επιταγών και αντίγραφα λογαριασμών, μεταφορά μεταξύ λογαριασμών στην ίδια τράπεζα αλλά και σε άλλες, αυτόματες εντολές πληρωμής υπηρεσιών όπως ΔΕΗ, ΟΤΕ, ΕΥΔΑΠ, κινητής τηλεφωνίας Vodafone και συνδρομητικής τηλεόρασης Multichoice, πληρωμές καρτών της Τράπεζας Πειραιώς, πληρωμή ΦΠΑ, υποβολή βιογραφικού σημειώματος, αίτηση χορήγησης πιστωτικών καρτών και καταναλωτικού δανείου, αίτηση για άνοιγμα λογαριασμού και σύνδεσης με την υπηρεσία της ηλεκτρονικής τραπεζικής κ.α. Επίσης, παρέχεται η δυνατότητα διαρκούς επικοινωνίας με τον πελάτη μέσω ηλεκτρονικού ταχυδρομείου (e- mail) και έτσι παράλληλα εξασφαλίζεται και η προώθηση των προϊόντων και υπηρεσιών της τράπεζας καθώς και η προσέλκυση νέων πελατών. Μία έλλειψη που παρατηρείται στην ιστοσελίδα της Τράπεζας Πειραιώς είναι η απουσία χάρτη πλοήγησης (site map).

Hsbc bank

Η ιστοσελίδα της HSBC Bank χαρακτηρίζεται ιδιαίτερα λιτή και προσφέρει κυρίως χρηματιστηριακές υπηρεσίες. Δεν διεκδικεί ιδιαίτερες διακρίσεις καθώς ο σχεδιασμός είναι αρκετά φτωχός και η τράπεζα περιορίζεται στην παροχή πληροφοριών σχετικά με το δίκτυο των καταστημάτων, το ευρώ, τα επενδυτικά και δανειακά προϊόντα, τις ευκαιρίες εργασίας, τους λογαριασμούς καταθέσεων. Οι προσφερόμενες υπηρεσίες περιορίζονται σε χρηματιστηριακές εφαρμογές που υλοποιούνται σε συνεργασία με την Παντελάκης ΑΧΕΠΕΥ. Παρέχεται η πρωτοποριακή υπηρεσία του InvestDirect, δηλαδή της άμεσης επένδυσης, και μέσω αυτής υπάρχει πρόσβαση στο Χρηματιστήριο και στον λογαριασμό του πελάτη στην HSBC Παντελάκης ΑΧΕΠΕΥ. Έτσι, υπάρχει η δυνατότητα πραγματοποίησης αγοραπωλησίας μετοχών, ενημέρωση για τις τιμές μετοχών, ενημέρωση για το χαρτοφυλάκιο του πελάτη, την κατάσταση των εντολών του, τις προσεχείς δημόσιες εγγραφές και γενικότερα τις ειδήσεις της αγοράς.

Εμπορική τράπεζα

Οι υπηρεσίες που προσφέρει η τράπεζα μέσω δικτύου είναι καλές. Προσφέρει καλή ποικιλία προϊόντων αλλά με εμφανείς αδυναμίες στον σχεδιασμό. Η Εμπορική Τράπεζα στην προσπάθεια της να βελτιώνει και να εκσυγχρονίζει τις υπηρεσίες της, παρέχει στους πελάτες την δυνατότητα να διεκπεραιώνουν τις εξής συναλλαγές μέσω διαδικτύου: υπόλοιπα λογαριασμών και τελευταίες κινήσεις, μεταφορά μεταξύ λογαριασμών του ίδιου πελάτη αλλά και σε άλλον πελάτη της ίδιας τράπεζας, υπόλοιπα, κινήσεις και πληρωμές πιστωτικών καρτών, κατάσταση προθεσμιακών καταθέσεων, χαρτοφυλακίου μετοχών και χρηματιστηριακών εντολών, δήλωση απώλειας – κλοπής πιστωτικής κάρτας, παραγγελία μπλοκ επιταγών, ηλεκτρονική πληρωμή ΦΠΑ, ενημέρωση για τον IBAN (International Bank Account Number), αλλαγή του κωδικού πρόσβασης του πελάτη, ενημέρωση για το τι ασφάλεια παρέχεται από την τράπεζα στους πελάτες που πραγματοποιούν συναλλαγές μέσω διαδικτύου κ.α. Στην πρώτη σελίδα παρέχεται η δυνατότητα επιλογής γλώσσας (ελληνικά ή αγγλικά), η πληρότητα όμως του μενού της πρώτης σελίδας θα μπορούσε να είναι καλύτερη. Επίσης δεν είναι τόσο καλή η ισορροπία μεταξύ κειμένου και γραφικών, και δεν υπάρχει χάρτης πλοήγησης (site map) ούτε μηχανή αναζήτησης. Γενικώς, θα λέγαμε ότι η ιστοσελίδα της Εμπορικής Τράπεζας είναι μια πολύ καλή προσπάθεια αλλά σίγουρα χρειάζεται συνέχεια δεδομένων των υψηλών στόχων αυτής της μεγάλης τράπεζας.

Ctitibank

Η ιστοσελίδα της Citibank χαρακτηρίζεται από εξαιρετική λειτουργικότητα και πολύ καλή σχεδίαση, γεγονός που μαρτυρά ότι είναι μια τράπεζα με διεθνή εμπειρία. Οι λειτουργίες και υπηρεσίες που προσφέρει στους πελάτες της δεν είναι πολλές συγκριτικά με άλλες τράπεζες, έχει δοθεί όμως ιδιαίτερη βαρύτητα στον σχεδιασμό και την ευχρηστία του μενού λειτουργίας. Ο συνδυασμός κειμένου και γραφικών είναι ισορροπημένος και η λειτουργικότητα των σελίδων θυμίζει ξένες αντίστοιχες ιστοσελίδες, κάτι που δεν είναι τυχαίο βέβαια αφού ελέγχονται και πιστοποιούνται από την επιτροπή πιστοποίησης δικτύου "web authoring" της αμερικανικής διεύθυνσης της τράπεζας. Η γκάμα προϊόντων και υπηρεσιών υστερεί σε σχέση με τον ανταγωνισμό αφού απουσιάζει η παροχή χρηματιστηριακών και επενδυτικών υπηρεσιών, καθώς οι υπηρεσίες που παρέχονται από την τράπεζα στους πελάτες της είναι ενημέρωση για τα υπόλοιπα λογαριασμών και τις πρόσφατες κινήσεις, μεταφορά χρημάτων μεταξύ λογαριασμών του ίδιου πελάτη και επίσης σε άλλο πελάτη στην Citibank Ελλάδος ή εξωτερικού, ενημέρωση για υπόλοιπα πιστωτικών καρτών της τράπεζας και πληρωμές των καρτών, αλλαγή του προσωπικού κωδικού (PIN), παραγγελία μπλοκ επιταγών. Η ασφάλεια του παρέχει η τράπεζα είναι σε υψηλά επίπεδα καθώς οι πληροφορίες που διακινούνται "ταξιδεύουν" σε κρυπτογραφημένη μορφή και το CitiDirect (όπως ονομάζεται η υπηρεσία του e-banking της Citibank) απαιτεί από την εφαρμογή πλοήγησης που είναι εγκατεστημένη στον υπολογιστή του πελάτη να υποστηρίζει ισχυρή κρυπτογράφηση 128 bit. Επίσης οποιαδήποτε νέα εφαρμογή ηλεκτρονικής τραπεζικής ελέγχεται πριν λανσαριστεί στην παραγωγή για να εξασφαλιστεί η ασφάλεια και η προστασία του πελάτη. Η σχεδίαση της ιστοσελίδας προσφέρει χάρτη πλοήγησης και μηχανή αναζήτησης με δυνατότητα σύνθετης αναζήτησης. Η τεχνική υποστήριξη είναι πολύ καλή, συνέπεια της μεγάλης σημασίας που αποδίδει η τράπεζα στην εξυπηρέτηση του πελάτη. Σαν συμπέρασμα θα λέγαμε ότι η πρόταση της Citibank χαρακτηρίζεται από υψηλό επαγγελματισμό και είναι αντάξια του μεγέθους και της φήμης της τράπεζας.

Novabank

Η πρόταση της Novabank είναι πολύ αξιόλογη και αποδεικνύει ότι μία πολύ νέα ελληνική τράπεζα επενδύει σε ένα μέσο που υπόσχεται πολλά για το μέλλον των τραπεζικών συναλλαγών. Οι παρεχόμενες υπηρεσίες καλύπτουν σχεδόν όλο το φάσμα των τραπεζικών προϊόντων και εφαρμογών και η πληροφόρηση είναι πλήρης. Οι πελάτες της τράπεζας μπορούν μέσω δικτύου να ενημερώνονται για τα υπόλοιπα των λογαριασμών τους και τις πρόσφατες κινήσεις, να παραγγέλνουν μπλοκ επιταγών, να κάνουν μεταφορές χρημάτων σε πελάτες της ίδιας τράπεζας αλλά και εμβάσματα σε άλλες τράπεζες της Ελλάδας αλλά και του εξωτερικού, να αλλάζουν τον προσωπικό τους κωδικό (PIN), να ζητούν έκδοση τραπεζικών επιταγών και ανάκληση επιταγής, να κάνουν αίτηση χορήγησης πιστωτικής κάρτας ή δανείου, να καθορίζουν την συχνότητα αγοραπωλησίας μετοχών και αμοιβαίων κεφαλαίων, η πλήρης αποτίμηση του χαρτοφυλακίου του πελάτη, η συμμετοχή του σε δημόσιες εγγραφές, η παρουσίαση ιστορικού των εντολών του, νέα για το Χρηματιστήριο κ.α. Η τεχνική υποστήριξη που παρέχεται είναι πολύ καλή και η λειτουργικότητα των σελίδων ικανοποιεί. Υπάρχει μηχανή αναζήτησης αλλά δεν υπάρχει χάρτης πλοήγησης στις σελίδες. Θα πρέπει να αναφέρουμε ότι η παρουσία της Novabank στην ηλεκτρονική τραπεζική κρίνεται πολύ καλή και μπορεί να κοιτάξει επιθετικά τον ανταγωνισμό που αναπτύσσεται στον χώρο.

Εθνική Τράπεζα

Η τράπεζα προσφέρει – όπως ήταν βέβαια αναμενόμενο βάσει του μεγέθους της – πλούσια γκάμα προϊόντων και υπηρεσιών κάτι που δεν αρκεί όμως για να διακριθεί απέναντι στον ανταγωνισμό. Οι υπηρεσίες που παρέχονται στον πελάτη μέσω internet είναι: ενημέρωση για το υπόλοιπο λογαριασμών του και τις πρόσφατες κινήσεις, μεταφορά χρημάτων από έναν λογαριασμό σε άλλον του ίδιου πελάτη ή σε άλλον πελάτη της τράπεζας, πληρωμή ΦΠΑ και ΙΚΑ, πληρωμή πιστωτικών καρτών της Εθνικής και ασφαλίστρων ζωής της Εθνικής Ασφαλιστικής, ενημέρωση για το χαρτοφυλάκιο των μετοχών και των αμοιβαίων κεφαλαίων του πελάτη, διεκπεραίωση αγοραπωλησίας μετοχών ή ακύρωση της εντολής πριν την πραγματοποίηση της, υποβολή αίτησης συμμετοχής σε δημόσιες εγγραφές στο Χρηματιστήριο, αλλαγή προσωπικού κωδικού (PIN).Η σχεδίαση της ιστοσελίδας της Εθνικής Τράπεζας υστερεί σημαντικά στην αρτιότητα των γραφικών αλλά και στην ομοιομορφία των σελίδων, ενώ επίσης αρνητική κρίνεται η απουσία χάρτη πλοήγησης και μηχανή αναζήτησης από τις σελίδες της. Συνολικά η παρουσία της τράπεζας στο διαδίκτυο δεν κρίνεται ιδιαίτερα ικανοποιητική αν αναλογιστεί κανείς το μέγεθος και την ιστορία της.

Εγνατία Τράπεζα

Ηταν η πρώτη τράπεζα που δραστηριοποιήθηκε στον χώρο της ηλεκτρονικής τραπεζικής το 1997 γεγονός που αποδεικνύει τη σημασία που δίνει η διοίκηση της τράπεζας στο νέο αυτό μέσο διεκπεραίωσης τραπεζικών συναλλαγών. Στην προσπάθεια της να δώσει κίνητρα για την προσέλκυση πελατών στην ηλεκτρονική τραπεζική (e- banking) εξασφάλισε ειδικά για τους πελάτες της 20% έκπτωση στις τιμές σύνδεσης της ForthNet, μιας από τις δημοφιλέστερες εταιρείες παροχής υπηρεσιών διαδικτύου (internet service providers) στην Ελλάδα. Η ιστοσελίδα (web site) της τράπεζας παρέχει ενημέρωση για τις τιμές συναλλάγματος, τα επιτόκια, τα αμοιβαία κεφάλαια, το Χρηματιστήριο. Επίσης, παρέχεται η δυνατότητα διεκπεραίωσης συναλλαγών όπως πραγματοποίηση αυτόματης μισθοδοσίας του προσωπικού εταιρειών και γενικότερα εκτέλεση εντολών πληρωμής προ τρίτους που τηρούν λογαριασμό στην Εγνατία Τράπεζα, παρακολούθηση των τιμών μετοχών και της τρέχουσας αξίας του χαρτοφυλακίου των πελατών, εκτέλεση χρηματιστηριακών εντολών, υπόλοιπα λογαριασμών και πρόσφατες κινήσεις, πληρωμή ΦΠΑ και ΙΚΑ, μεταφορές χρημάτων μεταξύ των λογαριασμών του ίδιου πελάτη αλλά και σε άλλο πελάτη της Τράπεζας, πληρωμή ΔΕΗ και ΟΤΕ με πάγια εντολή, πληρωμή πιστωτικής κάρτας Εγνατία Visa και παρακολούθηση αναλυτικού λογαριασμού κ.α. Μία άλλη σημαντική δυνατότητα που προσφέρει η χρήση της ιστοσελίδας της Εγνατίας είναι η πραγματοποίηση αγορών με άνεση και ασφάλεια μέσω δικτύου από τα συνεργαζόμενα ηλεκτρονικά καταστήματα. Αυτό αποδεικνύει περίτρανα ότι η συγκεκριμένη τράπεζα δραστηριοποιείται και στο ηλεκτρονικό εμπόριο προκειμένου να εξυπηρετήσει όσο το δυνατόν καλύτερα τους πελάτες της. Θα λέγαμε επομένως ότι οι προσφερόμενες υπηρεσίες της καλύπτουν όλο το φάσμα τραπεζικών εργασιών και παράλληλα υπάρχει χάρτης πλοήγησης αλλά απουσιάζουν οι μηχανές αναζήτησης. Η επιλογή δεύτερης γλώσσας υπάρχει αλλά παραπέμπει σε μελλοντική υλοποίηση. Γενικότερα, μέσω της ιστοσελίδας καλύπτονται οι ανάγκες των πελατών και η τράπεζα αντιμετωπίζει επάξια τον ανταγωνισμό αλλά θα πρέπει να στοχεύσει υψηλότερα αν θέλει να παραμείνει ανάμεσα στους πρώτους στην ηλεκτρονική τραπεζική.

Λαϊκή Τράπεζα

Το φάσμα των υπηρεσιών που προσφέρει είναι καλό αλλά υστερεί από τον ανταγωνισμό αφού δεν προσφέρει βασικές λειτουργίες όπως χρηματιστηριακές υπηρεσίες. Μέσω του δικτύου της τράπεζας παρέχεται η δυνατότητα ενημέρωσης για τους λογαριασμούς και τις τελευταίες αναλύσεις τους, τις επιταγές, τις κάρτες. Ο πελάτης μπορεί να κάνει μεταφορά κεφαλαίων, πληρωμή καρτών και δανείων, παραγγελία βιβλιαρίου επιταγών. Επίσης, ο χρήστης ενημερώνεται για την ασφάλεια που υπάρχει στην ιστοσελίδα της τράπεζας και την μέθοδο κρυπτογράφησης που χρησιμοποιείται προκειμένου να εξασφαλιστεί η προστασία του πελάτη. Αναφέρεται στην αρχική σελίδα ότι σύντομα θα τεθεί στην διάθεση των πελατών η δυνατότητα διεκπεραίωσης χρηματιστηριακών συναλλαγών και εντολών, κάτι που σίγουρα θα βελτιώσει την υπηρεσία ηλεκτρονικής τραπεζικής. Υπάρχει η επιλογή δεύτερης γλώσσας (αγλλικά) αλλά απουσιάζει χάρτης πλοήγησης και μηχανές αναζήτησης, και επίσης διαπιστώνεται έλλειψη ομοιομορφίας μεταξύ των σελίδων και όχι μεγάλη ισορροπία μεταξύ κειμένου και γραφικών. Επιπλέον, παρέχονται οδηγίες και υποστήριξη στους χρήστες που αντιμετωπίζουν πρόβλημα σύνδεσης με την υπηρεσία. Η ιστοσελίδα της Λαϊκής Τράπεζας είναι γενικώς καλή αλλά υπάρχει ανάγκη βελτίωσης σε αρκετούς τομείς προκειμένου να ανταγωνιστεί τους αντιπάλους της.

Τράπεζα Κύπρου

Η ιστοσελίδα της Τράπεζα Κύπρου είναι ιδιαίτερα λειτουργική και καλύπτει τον μέσο χρήστη, καθώς το φάσμα των προϊόντων που περιέχει είναι καλό. Πιο συγκεκριμένα, οι υπηρεσίες που παρέχονται από την εξυπηρέτηση μέσω του διαδικτύου είναι: διαχείριση λογαριασμών, δηλαδή πληροφορίες για τα υπόλοιπα και τις κινήσεις από την ημερομηνία ανοίγματος ή από την ημερομηνία έκδοσης της τελευταίας ενημέρωσης ή γενικών για συγκεκριμένο προεπιλεγμένο διάστημα, τελευταίες δέκα χρεώσεις ή πιστώσεις του λογαριασμού, μεταφορά χρημάτων μεταξύ λογαριασμών του πελάτη, αίτηση εμβάσματος, αίτηση πάγιας εντολής πληρωμής, πληρωμή ΦΠΑ, παραγγελία βιβλιαρίου επιταγών και αντίγραφα λογαριασμών, αλλαγή μυστικού κωδικού πρόσβασης, αλληλογραφία με τους αρμόδιους του internet banking της τράπεζας, πληροφορίες για τα ισχύοντα επιτόκια, αποστολή αρχείου μισθοδοσίας. Επίσης υπάρχει η δυνατότητα διεκπεραίωσης χρηματιστηριακών συναλλαγών και εντολών, καθώς και ενημέρωσης για χρηματιστηριακούς τίτλους και κινήσεις εφόσον ο πελάτης έχει κωδικό επενδυτή. Η ιστοσελίδα προσφέρει επιπλέον ενημέρωση στους επενδυτές για μερίσματα, μετοχές και διάφορα άλλα οικονομικά νέα της τράπεζας, και επίσης την δυνατότητα να λαμβάνουν ανακοινώσεις, νέα και προσφορές της τράπεζας μέσω ηλεκτρονικού ταχυδρομείου εφόσον το επιθυμούν και εγγραφούν στην υπηρεσία αυτή. Στην αρχική σελίδα αναφέρεται η επιλογή της δεύτερης γλώσσας αλλά οδηγεί σε μελλοντική υλοποίηση. Προσφέρεται χάρτης πλοήγησης αλλά δεν συμβαίνει το ίδιο στην περίπτωση μηχανών αναζήτησης. Οι σελίδες παρουσιάζουν καλή αισθητική και ομοιογένεια και υπάρχει ισορροπία μεταξύ κειμένου και γραφικών. Οι πληροφορίες για την επικοινωνία και υποστήριξη των πελατών είναι πολύ καλές και παρέχεται επίσης πληροφόρηση για την ασφάλεια των συναλλαγών μέσω διαδικτύου. Γενικότερα, θα λέγαμε ότι η ιστοσελίδα της Τράπεζα Κύπρου αποτελεί μια αρκετά φιλόδοξη προσπάθεια που όμως πρέπει να εμπλουτιστεί αν θέλει να σταθεί απέναντι στον ανταγωνισμό.

Ασπίς Bank

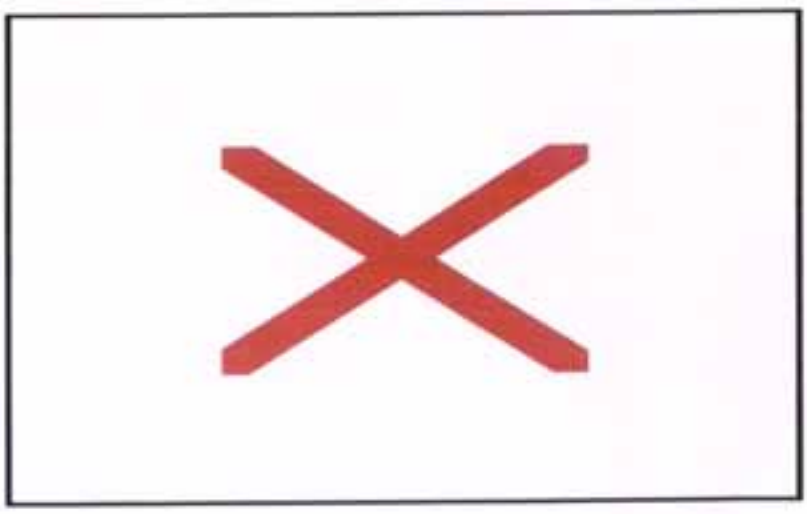
Το site της Ασπίς Bank είναι καλοφτιαγμένο και προσφέρει πλούσια γκάμα προϊόντων και υπηρεσιών. Οι πελάτες μπορούν μέσω δικτύου να ενημερώνονται για τα υπόλοιπα των λογαριασμών και την κίνηση τους, να έχουν ανάλυση και ενημέρωση των δανειακών λογαριασμών και των προθεσμιών που έχουν συνάψει με την τράπεζα, να κάνουν μεταφορές χρημάτων μεταξύ δικών τους λογαριασμών ή σε άλλο πελάτη της τράπεζας ή ακόμη και σε άλλη τράπεζα, να κάνουν πληρωμές πιστωτικών καρτών και κινητής τηλεφωνίας, να κάνουν αίτηση ανάθεσης παγίων εντολών για πληρωμή ΟΤΕ, ΔΕΗ, ΕΥΔΑΠ, κινητής τηλεφωνίας και ασφαλίστρων, αίτηση σύναψης δανείων, αίτηση έκδοσης πιστωτικής κάρτας, ταχυδρομικής αποστολής κινήσεων των λογαριασμών, έκδοσης μπλοκ επιταγών και επίσης διαχείριση του προσωπικού κωδικού πρόσβασης. Υπάρχει επίσης η δυνατότητα διεκπεραίωσης χρηματιστηριακών συναλλαγών, δηλαδή εντολές για αγορά και πώληση μετοχών, παρουσίαση του προσωπικού χαρτοφυλακίου του πελάτη, ενημέρωση για τις τρέχουσες τιμές όλων των μετοχών του Χρηματιστηρίου Αθηνών, ενημέρωση για την κατάσταση εκτέλεσης των εντολών που έχουν δοθεί και παρουσίαση των εντολών σε λίστα. Παρέχεται η δυνατότητα τεχνικής υποστήριξης στους πελάτες που ενδεχομένως αντιμετωπίσουν κάποιο πρόβλημα στη σύνδεση, ενώ δεν υπάρχει χάρτης πλοήγησης και μηχανή αναζήτησης ούτε δεύτερη γλώσσα. Γενικώς, το περιεχόμενο της ιστοσελίδας είναι καλό και ενημερωμένο και

συνεισφέρει στην εξυπηρέτηση των πελατών αλλά σίγουρα μπορεί να γίνει πολύ καλύτερο για να αντιμετωπίσει επάξια τον ανταγωνισμό. Οι ιστοσελίδες των υπολοίπων ελληνικών τραπεζών έχουν μόνο ενημερωτικό και πληροφοριακό χαρακτήρα και δεν επιτρέπουν προς το παρόν την διεκπεραίωση τραπεζικών συναλλαγών ηλεκτρονικά. Στοχεύουν απλά στην ενημέρωση του κοινού σχετικά με τα προϊόντα και τις υπηρεσίες που παρέχουν γενικά, της ιστορία της τράπεζας, την εξέλιξη, την παρουσίαση των νέων προϊόντων που υπάρχουν, τις διάφορες προσφορές, το δίκτυο διανομής, τα επιτόκια, το ευρώ και γενικώς άλλες οικονομικού και τραπεζικού χαρακτήρα πληροφορίες. Με τον τρόπο αυτό εξασφαλίζουν ένα σύγχρονο, δυναμικό και διαρκές κανάλι ενημέρωσης και επικοινωνίας με τους πελάτες τους.

ΕΛΛΗΝΙΚΑ ΗΛΕΚΤΡΟΝΙΚΑ ΚΑΤΑΣΤΗΜΑΤΑ E-SHOPS: ΙΣΧΥΟΥΣΕΣ ΜΕΘΟΔΟΙ ΠΛΗΡΩΜΗΣ

Τα ηλεκτρονικά καταστήματα που παρατηρούνται στην χώρο του διαδικτύου και τα οποία προέρχονται από την ελληνική αγορά έχουν τις εξής ιστοσελίδες:
www.wineshop.gr,
www.dvdclub.gr,
www.creatashop.gr,
www.myshops.gr,
www.heliosagora.com,
www.oops.gr,
www.books.gr,
www.protoporia.gr,
www.kastaniotis.gr,
www.plaisio.gr,
www.bookmarket.gr,
www.e-shop.gr,
www.applestore.gr,
www.cosmodata.gr,
www.1OneWay.gr,
www.infoshop.gr,
www.pc-shop.gr
www.greekbooks.gr,
www.mad.gr,
www.cdbase.gr,
www.ianos.gr,
www.cdnow.com,
www.shop21.gr,
www.dvdcool.gr,

Τα προϊόντα που προσφέρουν αυτά τα ηλεκτρονικά καταστήματα καλύπτουν μια ευρεία γκάμα που περιλαμβάνει βιβλία, είδη γραφικής ύλης, είδη υπολογιστών, ηλεκτρονικές συσκευές, άνθη, cd/dvd, αλλά και προϊόντα όπως βρεφικά είδη, είδη ένδυσης, είδη δώρων κ.α.
Οι διαθέσιμοι τρόποι πληρωμής σε αυτά τα ελληνικά ηλεκτρονικά καταστήματα παρουσιάζονται στο γράφημα που ακολουθεί:



Όπως φαίνεται και από το σχήμα, οι βασικοί μέθοδοι πληρωμής που προσφέρονται στους έλληνες καταναλωτές αυτή την στιγμή είναι τέσσερις:

- Πληρωμή με αντικαταβολή, ειδικά για κατοίκους Αθηνών και μεγάλων αστικών κέντρων γενικότερα.
- Πληρωμή με πιστωτική κάρτα.
- Κατάθεση σε τράπεζα.
- Προπληρωμένες κάρτες.

Από το παραπάνω γράφημα είναι επίσης προφανές ότι από αυτές τις τέσσερις μεθόδους πληρωμών, τα ηλεκτρονικά καταστήματα προκρίνουν κυρίως τις πληρωμές με κατάθεση του ποσού σε τραπεζικό λογαριασμό.

ΕΙΣΑΓΩΓΗ ΣΤΗΝ ΝΟΜΟΘΕΣΙΑ ΠΡΟΣΤΑΣΙΑΣ ΤΩΝ ΔΙΚΑΙΩΜΑΤΩΝ ΤΟΥ ΑΤΟΜΟΥ-ΧΡΗΣΤΗ ΤΟΥ ΔΙΑΔΙΚΤΥΟΥ.

Στην ενότητα αυτή παρουσιάζονται όλοι οι νόμοι που αφορούν την προστασία τις ιδιωτικής ζωής των ατόμων και κυρίως όσων χρησιμοποιούν το διαδίκτυο. Επίσης δίδονται απαντήσεις σε ερωτήματα που απασχολούν όλους τους χρήστες του internet. Αυτά είναι τα εξής:

Παν πρόσωπο δικαιούται το σεβασμό της ιδιωτικής και οικογενειακής ζωής του, της κατοικίας του και της αλληλογραφίας του.
- Ευρωπαϊκή σύμβαση για την προστασία των δικαιωμάτων του ανθρώπου και των θεμελιωδών ελευθεριών.

Οι πληροφορίες που αφορούν τα πρόσωπα και ονομάζονται «δεδομένα προσωπικού χαρακτήρα» συγκεντρώνονται και χρησιμοποιούνται σε πολλές πτυχές της καθημερινής ζωής. Ένα πρόσωπο παρέχει δεδομένα προσωπικού χαρακτήρα όταν, για παράδειγμα, δίνει τα στοιχεία του για να λάβει κάρτα βιβλιοθήκης, να εγγραφεί μέλος σε γυμναστήριο, να ανοίξει τραπεζικό λογαριασμό κλπ. Τα δεδομένα προσωπικού χαρακτήρα μπορούν να συγκεντρώνονται είτε άμεσα από ένα άτομο είτε από υπάρχουσες βάσεις δεδομένων. Τα δεδομένα αυτά μπορούν στη συνέχεια να χρησιμοποιούνται για άλλους σκοπούς και/ή να γνωστοποιούνται σε άλλους φορείς. Δεδομένα προσωπικού χαρακτήρα μπορεί να είναι τα στοιχεία που προσδιορίζουν ένα άτομο, όπως το όνομα, το τηλέφωνο ή μια φωτογραφία.

Η πρόοδος της τεχνολογίας των υπολογιστών και τα νέα δίκτυα τηλεπικοινωνιών επιτρέπουν τη διαβίβαση δεδομένων προσωπικού χαρακτήρα διαμέσου των συνόρων με μεγαλύτερη ευκολία. Έτσι, τα δεδομένα που αφορούν πολίτες ενός κράτους μέλους ορισμένες φορές γίνονται αντικείμενο επεξεργασίας σε άλλο κράτος μέλος της Ευρωπαϊκής Ένωσης (ΕΕ). Επειδή τα δεδομένα προσωπικού χαρακτήρα συλλέγονται και ανταλλάσσονται συχνότερα, απαιτείται νομοθετική ρύθμιση της διαβίβασης των δεδομένων.

Κατά κανόνα, οι εθνικές νομοθεσίες για την προστασία των δεδομένων απαιτούν ορθές πρακτικές διαχείρισης των δεδομένων εκ μέρους των φορέων που επεξεργάζονται τα δεδομένα και οι οποίοι αποκαλούνται «υπεύθυνοι της επεξεργασίας δεδομένων». Μεταξύ αυτών συγκαταλέγονται η υποχρέωση επεξεργασίας των δεδομένων με έντιμο και ασφαλή τρόπο και χρησιμοποίησης των δεδομένων προσωπικού χαρακτήρα για διαφανείς και θεμιτούς σκοπούς. Οι εθνικοί νόμοι εξασφαλίζουν επίσης ορισμένα δικαιώματα των προσώπων, όπως το δικαίωμα ενημέρωσης όταν τα δεδομένα προσωπικού χαρακτήρα αποτελούν αντικείμενο επεξεργασίας, καθώς και σχετικά με το σκοπό της επεξεργασίας αυτής, το δικαίωμα πρόσβασης στα δεδομένα και, όπου αυτό είναι αναγκαίο, το δικαίωμα τροποποίησης ή διαγραφής των δεδομένων.

Παρόλο που οι εθνικές νομοθεσίες για την προστασία των δεδομένων είχαν ως στόχο να εξασφαλίσουν τα ίδια δικαιώματα, ωστόσο ορισμένες διαφορές εξακολουθούσαν να υπάρχουν. Οι διαφορές αυτές μπορούσαν να δημιουργήσουν εμπόδια στην ελεύθερη ροή των πληροφοριών και πρόσθετη επιβάρυνση των οικονομικών φορέων και των πολιτών. Μεταξύ των προβλημάτων αυτών συγκαταλέγονταν: η ανάγκη καταγραφής σε μητρώο ή λήψης άδειας από τις αρχές ελέγχου των διαφόρων κρατών

μελών για την επεξεργασία δεδομένων, η ανάγκη συμμόρφωσης προς διάφορα πρότυπα και η δυνατότητα περιορισμού της διαβίβασης δεδομένων σε άλλο κράτος μέλος της ΕΕ. Επιπλέον, ορισμένα κράτη μέλη δεν είχαν νομοθεσία για την προστασία των δεδομένων.Για τους λόγους αυτούς, υπήρξε ανάγκη λήψης μέτρων σε ευρωπαϊκό επίπεδο, που έλαβε τη μορφή οδηγιών της ΕΕ.

Η ΕΥΡΩΠΑΪΚΗ ΝΟΜΟΘΕΣΙΑ ΓΙΑ ΤΗΝ ΠΡΟΣΤΑΣΙΑ ΤΩΝ ΔΕΔΟΜΕΝΩΝ

Με στόχο την άρση των εμποδίων στην ελεύθερη κυκλοφορία των δεδομένων, χωρίς να μειωθεί το επίπεδο της προστασίας των δεδομένων προσωπικού χαρακτήρα, εκδόθηκε η οδηγία 95/46/ΕΚ (οδηγία για την προστασία των δεδομένων) για την εναρμόνιση των εθνικών διατάξεων στον τομέα αυτό.

Στο πλαίσιο αυτό, τα δεδομένα προσωπικού χαρακτήρα θα έχουν ισότιμη προστασία σε όλη την Ένωση. Ζητήθηκε από τα 15 κράτη μέλη της ΕΕ να εναρμονίσουν την εθνική τους νομοθεσία με τις διατάξεις της οδηγίας έως τις 24 Οκτωβρίου 1998.

Οι οδηγίες αποτελούν τμήματα της ευρωπαϊκής νομοθεσίας που απευθύνονται στα κράτη μέλη. Αφού εγκριθεί μια τέτοια νομοθετική πράξη σε ευρωπαϊκό επίπεδο, κάθε κράτος μέλος πρέπει να διασφαλίζει την αποτελεσματική ενσωμάτωσή της στο νομικό του σύστημα. Η οδηγία προσδιορίζει ένα τελικό αποτέλεσμα. Η μορφή και τα μέσα πραγματοποίησης αποφασίζονται από τα ίδια τα κράτη μέλη. Κατ' αρχήν, η οδηγία επιφέρει αποτελέσματα μέσω εθνικών μέτρων εφαρμογής (εθνική νομοθεσία). Ωστόσο, είναι δυνατόν, ακόμα και στην περίπτωση που ένα κράτος μέλος δεν έχει ακόμα μεταφέρει στο εθνικό του δίκαιο μια οδηγία, να εφαρμόζονται άμεσα ορισμένες από τις διατάξεις της. Αυτό σημαίνει ότι, εάν μια οδηγία παρέχει άμεσα δικαιώματα σε άτομα, τότε τα άτομα μπορούν να επικαλούνται την οδηγία στα εθνικά δικαστήρια, χωρίς να περιμένουν τη θέσπιση εθνικής νομοθεσίας για την εφαρμογή της. Επιπλέον, εάν τα άτομα πιστεύουν ότι υπέστησαν ζημίες επειδή οι εθνικές αρχές δεν εφάρμοσαν ορθά μια οδηγία, τότε μπορεί να δικαιούνται να ζητήσουν δικαστικώς αποζημίωση. Για την επιδίκαση των αποζημιώσεων αυτών αρμόδια είναι τα εθνικά δικαστήρια.

Η οδηγία για την προστασία των δεδομένων εφαρμόζεται σε «κάθε εργασία ή σειρά εργασιών που πραγματοποιείται σε δεδομένα προσωπικού χαρακτήρα» και αποκαλείται «επεξεργασία» δεδομένων. Οι εργασίες αυτές περιλαμβάνουν τη συλλογή δεδομένων προσωπικού χαρακτήρα, την αποθήκευση, τη γνωστοποίησή τους κλπ. Η οδηγία εφαρμόζεται στα δεδομένα που αποτελούν αντικείμενο επεξεργασίας με αυτοματοποιημένες διαδικασίες (π.χ. βάση δεδομένων υπολογιστή για πελάτες) και στα δεδομένα που αποτελούν τμήμα ή προορίζονται να αποτελέσουν τμήμα μη αυτοματοποιημένων «συστημάτων αρχειοθέτησης» και είναι προσβάσιμα σύμφωνα με συγκεκριμένα κριτήρια (για παράδειγμα, τα παραδοσιακά αρχεία σε χαρτί, όπως οι κάρτες αρχείων που περιλαμβάνουν στοιχεία των πελατών ταξινομημένες με αλφαβητική σειρά).

Η οδηγία για την προστασία των δεδομένων δεν εφαρμόζεται σε δεδομένα που αποτελούν αντικείμενο επεξεργασίας για καθαρά προσωπικούς λόγους ή για δραστηριότητες των νοικοκυριών (π.χ. προσωπικό ηλεκτρονικό ημερολόγιο ή αρχείο με στοιχεία μελών της οικογένειας ή φίλων). Δεν εφαρμόζεται επίσης σε τομείς όπως η δημόσια ασφάλεια, η άμυνα ή η εφαρμογή της ποινικής νομοθεσίας που δεν εμπίπτουν στο πλαίσιο των αρμοδιοτήτων της ΕΚ και παραμένουν προνόμιο των εθνικών κυβερνήσεων. Η εθνική νομοθεσία, κατά κανόνα, παρέχει προστασία στα φυσικά πρόσωπα στους τομείς αυτούς.

Επιπροσθέτως, υπάρχει μια άλλη οδηγία, η οδηγία 97/66/ΕΚ, με αντικείμενο την προστασία της ιδιωτικής ζωής στις τηλεπικοινωνίες. Η εν λόγω οδηγία προβλέπει ότι τα κράτη μέλη διασφαλίζουν το απόρρητο των επικοινωνιών μέσω των εθνικών νομοθετικών ρυθμίσεων. Αυτό σημαίνει ότι κάθε ακρόαση, λαθραία λήψη, αποθήκευση και κάθε άλλη μορφή παρεμβολής ή παρακολούθησης των επικοινωνιών χωρίς την άδεια των χρηστών είναι παράνομη. Όταν παρέχεται ένδειξη της ταυτότητας καλούσας γραμμής, οι χρήστες πρέπει να έχουν τη δυνατότητα να μην εγγράφονται συνδρομητές στην υπηρεσία αυτή ή να ζητούν να μην αποκαλύπτονται τα στοιχεία τους όταν τηλεφωνούν. Αντίθετα, οι συνδρομητές στην υπηρεσία αυτή πρέπει να έχουν τη δυνατότητα να απορρίπτουν εισερχόμενες κλήσεις από πρόσωπα που έχουν απενεργοποιήσει την ένδειξη της ταυτότητας καλούσας γραμμής. Επίσης, η οδηγία προβλέπει ότι, όπου υπάρχουν έντυποι ή ηλεκτρονικοί κατάλογοι τηλεπικοινωνιών, τα άτομα έχουν το δικαίωμα να ζητήσουν τη διαγραφή τους από τον κατάλογο, κατά κανόνα, χωρίς χρέωση.

ΚΑΝΟΝΕΣ ΤΟΥΣ ΟΠΟΙΟΥΣ ΠΡΕΠΕΙ ΝΑ ΕΦΑΡΜΟΖΟΥΝ ΟΙ ΥΠΕΥΘΥΝΟΙ ΕΠΕΞΕΡΓΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ

Ποιος μπορεί να είναι υπεύθυνος της επεξεργασίας δεδομένων;

Οι υπεύθυνοι της επεξεργασίας δεδομένων είναι πρόσωπα ή φορείς που «καθορίζουν τους στόχους και τον τρόπο της επεξεργασίας των δεδομένων» τόσο στον δημόσιο όσο και στον ιδιωτικό τομέα. Ένας ιατρός είναι συνήθως ο υπεύθυνος για την επεξεργασία των δεδομένων των πελατών του. Μια επιχείρηση είναι υπεύθυνη για την επεξεργασία των δεδομένων των πελατών και υπαλλήλων της. Ένας αθλητικός σύλλογος ελέγχει τα δεδομένα των μελών του που επεξεργάζεται και μια δημόσια βιβλιοθήκη είναι υπεύθυνη για την επεξεργασία των δεδομένων των χρηστών της.

Οι υπεύθυνοι της επεξεργασίας δεδομένων οφείλουν να τηρούν ορισμένες αρχές. Οι αρχές αυτές δεν αποσκοπούν μόνο στην προστασία των ατόμων στα οποία αναφέρονται τα δεδομένα, αλλά αποτελούν επίσης την έκφραση ορθών πρακτικών των επιχειρήσεων που συμβάλλουν στην αξιόπιστη και αποτελεσματική επεξεργασία των δεδομένων.

Κάθε υπεύθυνος επεξεργασίας δεδομένων οφείλει να τηρεί τους κανόνες για την επεξεργασία των δεδομένων του κράτους μέλους στο οποίο είναι εγκατεστημένος, ακόμα και αν τα δεδομένα τα οποία επεξεργάζεται αφορούν φυσικό πρόσωπο που κατοικεί σε άλλο κράτος μέλος. Όταν ο υπεύθυνος της επεξεργασίας των δεδομένων δεν είναι εγκατεστημένος στην Κοινότητα (π.χ. αλλοδαπή επιχείρηση), οφείλει να τηρεί τους νόμους του κράτους μέλους ή των κρατών μελών εάν ο εξοπλισμός της επεξεργασίας ευρίσκεται εντός της Ευρωπαϊκής Κοινότητας.

ΟΙ ΚΑΝΟΝΕΣ ΕΙΝΑΙ ΟΙ ΕΞΗΣ:

- Τα δεδομένα πρέπει να υφίστανται θεμιτή και σύννομη επεξεργασία.
- Πρέπει να συλλέγονται για καθορισμένους, ρητούς και νόμιμους σκοπούς και να χρησιμοποιούνται σύμφωνα με τους σκοπούς αυτούς.
- Τα δεδομένα πρέπει να είναι συναφή προς το θέμα και όχι υπερβολικά σε σχέση με τους σκοπούς για τους οποίους υφίστανται επεξεργασία.
- Τα δεδομένα να είναι ακριβή και, εφόσον χρειάζεται, να ενημερώνονται.
- Οι υπεύθυνοι της επεξεργασίας των δεδομένων πρέπει να λαμβάνουν κάθε εύλογο μέτρο ώστε να διορθώνουν ή να διαγράφουν ανακριβή δεδομένα σχετικά με τα άτομα στα οποία αναφέρονται τα δεδομένα αυτά.
- Τα δεδομένα που επιτρέπουν τον προσδιορισμό της ταυτότητας δεν πρέπει να διατηρούνται για μεγαλύτερο χρονικό διάστημα απ' όσο είναι αναγκαίο.
- Η οδηγία προβλέπει ότι κάθε κράτος μέλος ορίζει μία ή περισσότερες αρχές ελέγχου που παρακολουθούν την εφαρμογή της οδηγίας. Μία από τις υποχρεώσεις της αρχής ελέγχου είναι να τηρεί ενημερωμένο δημόσιο μητρώο, ώστε το κοινό να έχει πρόσβαση σε όλα τα ονόματα των υπευθύνων της επεξεργασίας δεδομένων και να πληροφορείται το είδος της επεξεργασίας που κάνουν.
- Κατά κανόνα, όλοι οι υπεύθυνοι επεξεργασίας δεδομένων πρέπει να ενημερώνουν τις αρχές ελέγχου όταν πραγματοποιούν επεξεργασία δεδομένων. Τα κράτη μέλη μπορούν να προβλέπουν απλούστευση της κοινοποίησης ή εξαίρεση από την κοινοποίηση για συγκεκριμένα είδη επεξεργασίας που δεν παρουσιάζουν ιδιαίτερους κινδύνους. Δυνατότητα εξαίρεσης ή απλούστευσης μπορεί να παρασχεθεί επίσης όταν, σύμφωνα με το εθνικό δίκαιο, ο υπεύθυνος για την επεξεργασία των δεδομένων ορίζει ανεξάρτητο φορέα υπεύθυνο για την προστασία των δεδομένων. Τα κράτη μέλη μπορούν να ζητήσουν από την αρχή ελέγχου να πραγματοποιεί προηγούμενο έλεγχο πριν από την εκτέλεση πράξεων επεξεργασίας δεδομένων που παρουσιάζουν ιδιαίτερους κινδύνους. Τα κράτη μέλη καθορίζουν ποια είδη πράξεων επεξεργασίας παρουσιάζουν ιδιαίτερους κινδύνους.

Σε ποιες περιπτώσεις μπορούν τα δεδομένα προσωπικού χαρακτήρα να αποτελέσουν αντικείμενο επεξεργασίας;

Τα δεδομένα προσωπικού χαρακτήρα μπορούν να αποτελέσουν αντικείμενο επεξεργασίας (δηλαδή να συγκεντρωθούν και να χρησιμοποιηθούν περαιτέρω) μόνον εάν:

- το πρόσωπο στο οποίο αναφέρονται τα δεδομένα έχει δώσει την αδιαμφισβήτητη συγκατάθεσή του, δηλαδή έχει συμφωνήσει ελεύθερα και ρητά αφού ενημερώθηκε καταλλήλως·
- η επεξεργασία είναι απαραίτητη για την εκτέλεση σύμβασης ή για ενέργειες που πραγματοποιούνται πριν από τη σύναψη συμβάσεως από το άτομο στο οποίο αναφέρονται τα δεδομένα, π.χ. επεξεργασία δεδομένων για χρέωση ή επεξεργασία δεδομένων που αφορούν άτομα τα οποία έχουν υποβάλει αίτηση εργασίας ή δανείου·
- η επεξεργασία απαιτείται από το νόμο·
- η επεξεργασία δεδομένων είναι απαραίτητη για την προστασία ζωτικών συμφερόντων του ατόμου στο οποίο αναφέρονται τα δεδομένα. Για παράδειγμα, σε περίπτωση αυτοκινητικού ατυχήματος, όπου το άτομο το οποίο αφορούν τα δεδομένα έχει χάσει τις αισθήσεις του, οι νοσοκόμοι πρώτων βοηθειών μπορούν να γνωστοποιούν τα αποτελέσματα εξέτασης αίματος, εάν τούτο θεωρείται αναγκαίο, προκειμένου να σωθεί η ζωή του τραυματία στον οποίο αναφέρονται τα δεδομένα·
- η επεξεργασία είναι απαραίτητη για την εκπλήρωση καθήκοντος δημοσίου συμφέροντος ή καθήκοντος που εκτελείται από δημόσιες αρχές (π.χ. κυβέρνηση, φορολογικές αρχές, αστυνομία κλπ.)·
- τέλος, τα δεδομένα μπορούν να αποτελούν αντικείμενο επεξεργασίας όποτε οι υπεύθυνοι της επεξεργασίας ή τρίτα πρόσωπα έχουν έννομο συμφέρον. Ωστόσο, το συμφέρον αυτό δεν μπορεί να υπερισχύει των συμφερόντων ή θεμελιωδών δικαιωμάτων των ατόμων στα οποία αναφέρονται τα δεδομένα, και ιδίως του δικαιώματος σεβασμού της ιδιωτικής ζωής. Η διάταξη αυτή επιδιώκει να επιφέρει στην πράξη μια λογική ισορροπία μεταξύ των επιχειρηματικών συμφερόντων των υπευθύνων για την επεξεργασία των δεδομένων και της προστασίας της ιδιωτικής ζωής των ατόμων στα οποία αναφέρονται τα δεδομένα. Η ισορροπία αυτή αξιολογείται σε πρώτο βαθμό από τους υπευθύνους της επεξεργασίας των δεδομένων υπό την επίβλεψη των αρχών για την προστασία των δεδομένων, παρόλο που, αν χρειαστεί, την τελική απόφαση λαμβάνουν τα δικαστήρια.

Ευαίσθητα δεδομένα

Πολύ αυστηροί κανόνες ισχύουν για την επεξεργασία ευαίσθητων δεδομένων: δεδομένων που αφορούν τη φυλετική ή εθνοτική καταγωγή, τις πολιτικές απόψεις, τη θρησκευτική ή φιλοσοφική πίστη, τη συμμετοχή σε εργατικά συνδικάτα, δεδομένων που αφορούν την υγεία ή τις σεξουαλικές προτιμήσεις. Κατά κανόνα, τα δεδομένα αυτά δεν μπορούν να αποτελέσουν αντικείμενο επεξεργασίας. Παρεκκλίσεις μπορούν να γίνουν ανεκτές κάτω από συγκεκριμένες συνθήκες, π.χ. για την επεξεργασία δεδομένων ύστερα από ρητή συγκατάθεση του ατόμου στο οποίο αναφέρονται όπως ορίζεται από το εργατικό δίκαιο, για περιπτώσεις όπου η συγκατάθεση του ατόμου στο οποίο αναφέρονται τα δεδομένα είναι αδύνατη (π.χ. ανακοίνωση των

αποτελεσμάτων εξέτασης αίματος του θύματος αυτοκινητικού ατυχήματος), για την επεξεργασία δεδομένων που έχει ανακοινωθεί δημοσίως ή την επεξεργασία δεδομένων των μελών εκ μέρους εργατικών συνδικάτων, πολιτικών κομμάτων ή εκκλησιών. Τα κράτη μέλη μπορούν να προβλέπουν και άλλες εξαιρέσεις σε ορισμένες περιπτώσεις, π.χ. για την προστασία ζωτικών δημόσιων συμφερόντων.

Η οδηγία ισχύει για τη μεταφορά δεδομένων μέσω του Διαδικτύου;

Θα ήταν παράλογο και από νομική άποψη αδικαιολόγητο να εξαιρεθεί ένα τόσο σημαντικό μέσο μεταφοράς όπως το Διαδίκτυο από το πεδίο εφαρμογής της οδηγίας για την προστασία των δεδομένων. Αντίθετα, η διαβίβαση τεράστιου όγκου ποικίλων δεδομένων προσωπικού χαρακτήρα μέσω του Διαδικτύου σε όλο τον κόσμο, ειδικά σε χώρες χωρίς κατάλληλα μέτρα προστασίας, είναι φαινόμενο που απαιτεί ιδιαίτερη προσοχή. Κατά συνέπεια, η οδηγία για την προστασία των δεδομένων είναι επομένως τεχνολογικά ουδέτερη: οι διατάξεις της ισχύουν ανεξάρτητα από το τεχνολογικό μέσο που χρησιμοποιείται για την επεξεργασία δεδομένων προσωπικού χαρακτήρα. Για παράδειγμα, η οδηγία εφαρμόζεται για την αφανή συλλογή δεδομένων προσωπικού χαρακτήρα στο Διαδίκτυο (π.χ. τα «cookies» που χρησιμοποιούνται για τον εντοπισμό των συνηθειών πλοήγησης των ατόμων στο Διαδίκτυο). Από την άλλη πλευρά, εάν τα δεδομένα προσωπικού χαρακτήρα συλλέγονται με φανερό τρόπο, μπορεί να υποστηριχθεί ότι το άτομο που μεταφέρει τα προσωπικά του δεδομένα έχει δώσει τη συγκατάθεσή του για τη μεταφορά αυτή, υπό την προϋπόθεση ότι έχει ενημερωθεί σωστά σχετικά με τους κινδύνους που μπορεί να παρουσιαστούν.

Εάν ένα άτομο λαμβάνει επανειλημμένα μηνύματα ηλεκτρονικού ταχυδρομείου που δεν επιθυμεί. Με ποιο τρόπο μπορεί να εμποδίσει κάτι τέτοιο, ειδικά όταν τα μηνύματα αυτά προέρχονται από διάφορες πηγές;

Το άτομο έχει το δικαίωμα να απαγορεύει την επεξεργασία προσωπικών δεδομένων του για σκοπούς του άμεσου μάρκετινγκ. Επιπλέον, το άτομο μπορεί να ζητήσει από το φορέα παροχής υπηρεσιών Διαδικτύου να εγκαταστήσει φίλτρα ηλεκτρονικού ταχυδρομείου ή μπορεί να έρθει σε επαφή με οργανισμό, σκοπός του οποίου είναι η παρεμπόδιση άχρηστων ηλεκτρονικών μηνυμάτων (CAUCE, Privacy International κλπ.). Υπάρχουν επίσης άλλες υπηρεσίες που βοηθούν τους χρήστες να αποφεύγουν άχρηστα ηλεκτρονικά μηνύματα, όπως η www.spamfree.org Εάν το πρόβλημα εξακολουθεί να υφίσταται, το άτομο μπορεί να απευθυνθεί στην εθνική αρχή ελέγχου.

ΤΑ ΔΙΚΑΙΩΜΑΤΑ ΣΑΣ ΩΣ ΑΤΟΜΟΥ ΣΤΟ ΟΠΟΙΟ ΑΝΑΦΕΡΟΝΤΑΙ ΤΑ ΔΕΔΟΜΕΝΑ

Έχετε το δικαίωμα να ενημερώνεστε σχετικά με επεξεργασία δεδομένων όταν είστε το άτομο στο οποίο αναφέρονται τα δεδομένα.

Οι υπεύθυνοι της επεξεργασίας δεδομένων οφείλουν να σας ενημερώνουν όποτε συγκεντρώνουν δεδομένα προσωπικού χαρακτήρα που σας αφορούν, εκτός εάν έχετε ενημερωθεί εκ των προτέρων. Έχετε δικαίωμα να ενημερώνεστε σχετικά με: την ταυτότητα του υπευθύνου της επεξεργασίας, τους σκοπούς της επεξεργασίας (ορισμένες φορές πρέπει να εξηγούνται οι κατηγορίες των δεδομένων), τους παραλήπτες των δεδομένων και τα συγκεκριμένα δικαιώματά σας ως ατόμων στα οποία αναφέρονται τα δεδομένα. Δικαιούστε να λαμβάνετε τις πληροφορίες αυτές όποτε τα δεδομένα αποκτώνται άμεσα ή έμμεσα από τρίτους. Παρεκκλίσεις επιτρέπονται στην τελευταία περίπτωση, εάν η παροχή των πληροφοριών αποδεικνύεται αδύνατη ή εξαιρετικά δύσκολη.

Έχετε δικαίωμα πρόσβασης στα δεδομένα που σας αφορούν.

Έχετε το δικαίωμα να έρθετε σε επαφή με οποιονδήποτε υπεύθυνο επεξεργασίας δεδομένων για να πληροφορηθείτε κατά πόσο ασχολείται με δεδομένα προσωπικού χαρακτήρα που σας αφορούν, να λαμβάνετε αντίγραφο των δεδομένων σε κατανοητή μορφή, καθώς και κάθε διαθέσιμη πληροφορία σχετικά με την πηγή τους. Εάν τα δεδομένα προσωπικού χαρακτήρα είναι ανακριβή, ή εάν έχουν αποτελέσει αντικείμενο παράνομης επεξεργασίας, δικαιούστε να ζητήσετε τη διόρθωση ή τη διαγραφή τους. Στις περιπτώσεις αυτές, το άτομο στο οποίο αναφέρονται τα δεδομένα μπορεί επίσης να ζητήσει από τον υπεύθυνο της επεξεργασίας να ειδοποιήσει τρίτους που έχουν ήδη λάβει γνώση των λανθασμένων δεδομένων, εκτός εάν αυτό είναι αδύνατο. Σε ορισμένες περιπτώσεις μπορεί να επιβληθεί κάποια εύλογη χρέωση για την παροχή πρόσβασης.

Έχετε επίσης δικαίωμα να ενημερώνεστε για τη λογική στην οποία βασίζονται οι αυτοματοποιημένες αποφάσεις.

Οι αποφάσεις που επηρεάζουν ουσιαστικά το άτομο στο οποίο αναφέρονται τα δεδομένα, όπως η απόφαση για τη χορήγηση δανείου ή την έκδοση ασφάλειας, μπορεί να λαμβάνονται αποκλειστικά βάσει αυτοματοποιημένης επεξεργασίας των δεδομένων. Επομένως, ο υπεύθυνος της επεξεργασίας πρέπει να έχει προβλέψει κατάλληλες ασφαλιστικές δικλείδες, όπως να παρέχεται στο άτομο στο οποίο αναφέρονται τα δεδομένα η δυνατότητα να εξετάζει τη λογική βάσει της οποίας συγκεντρώνονται τα δεδομένα ή να αμφισβητεί αποφάσεις που βασίζονται σε ανακριβή δεδομένα.

Εξαιρέσεις και περιορισμοί

Το δικαίωμα σεβασμού της ιδιωτικής ζωής μπορεί ορισμένες φορές να συγκρούεται με την ελευθερία έκφρασης και ιδίως με την ελευθερία του τύπου και των μέσων ενημέρωσης. Εναπόκειται επομένως στα κράτη μέλη να προβλέψουν εξαιρέσεις στη νομοθεσία τους περί προστασίας των δεδομένων, προκειμένου να επιτύχουν την εξισορρόπηση διαφορετικών αλλά εξίσου θεμελιωδών δικαιωμάτων.

Οι εθνικές νομοθεσίες μπορούν να προβλέπουν άλλες εξαιρέσεις στις διατάξεις της οδηγίας (οι εξαιρέσεις αυτές περιλαμβάνουν την υποχρέωση ενημέρωσης του ατόμου στο οποίο αναφέρονται τα δεδομένα, τη δημοσίευση πράξεων επεξεργασίας δεδομένων, την υποχρέωση σεβασμού των βασικών αρχών της ορθής διαχείρισης των δεδομένων). Οι εξαιρέσεις αυτές επιτρέπονται εφόσον είναι αναγκαίες για λόγους εθνικής ασφάλειας, άμυνας, εξιχνίασης εγκλημάτων, επιβολής της ποινικής νομοθεσίας ή για να προστατευθούν τα άτομα στα οποία αναφέρονται τα δεδομένα είτε τα δικαιώματα και οι ελευθερίες των άλλων. Επιπλέον, μπορεί να εγκριθεί παρέκκλιση από το δικαίωμα πρόσβασης στα δεδομένα τα οποία αποτελούν αντικείμενο επεξεργασίας για επιστημονικούς ή στατιστικούς σκοπούς.

ΤΙ ΜΠΟΡΕΙΤΕ ΝΑ ΚΑΝΕΤΕ ΑΝ ΠΑΡΑΒΙΑΖΟΝΤΑΙ ΤΑ ΔΙΚΑΙΩΜΑΤΑ ΣΑΣ

Η πρώτη σας ενέργεια, εάν πιστεύετε ότι έχουν παραβιαστεί τα δικαιώματά σας, είναι να έρθετε σε επαφή με το άτομο που φαίνεται ότι είναι η πηγή της παραβίασης προκειμένου να πιστοποιήσετε ποιος είναι υπεύθυνος της επεξεργασίας δεδομένων.

Εάν οι ενέργειές σας δεν καρποφορήσουν, μπορείτε να έρθετε σε επαφή με την τοπική αρχή για την προστασία των δεδομένων. Σύμφωνα με την οδηγία, κάθε κράτος μέλος συγκροτεί μία ή περισσότερες αρχές που εξασφαλίζουν την ορθή εφαρμογή της νομοθεσίας περί προστασίας των δεδομένων. Η αρχή αυτή, που συχνά αναφέρεται ως αρχή ελέγχου, είναι αρμόδια για την εξέταση καταγγελιών που υποβάλλουν άτομα ή επιχειρήσεις. Η αρχή ελέγχου οφείλει να διερευνήσει την καταγγελία και μπορεί να απαγορεύσει προσωρινά την επεξεργασία. Εάν διαπιστώσει ότι υπάρχει παράβαση της νομοθεσίας περί προστασίας των δεδομένων, τότε μπορεί να διατάξει τη διαγραφή ή την καταστροφή των δεδομένων και/ή να απαγορεύσει την περαιτέρω επεξεργασία.

Αν ένας φορέας παροχής τηλεπικοινωνιακών υπηρεσιών έδωσε πληροφορίες σχετικά με το λογαριασμό τηλεφώνου ή ηλεκτρονικού ταχυδρομείου σας σε άλλη επιχείρηση. Αποτέλεσμα είναι να λαμβάνετε τηλεφωνικές κλήσεις ή μηνύματα ηλεκτρονικού ταχυδρομείου που δεν έχετε ζητήσει. Τι μπορείτε να κάνετε;

Εάν τα δεδομένα προσωπικού χαρακτήρα συγκεντρώνονται αποκλειστικά για λόγους χρέωσης και δεν έχετε συναινέσει στην περαιτέρω διαβίβασή τους, έχετε δικαίωμα να αρνηθείτε τη μεταφορά των δεδομένων σας σε τρίτους. Η πρώτη σας ενέργεια θα είναι να απευθυνθείτε στο φορέα παροχής υπηρεσιών και να υποβάλετε με σαφήνεια την καταγγελία σας. Σε περίπτωση μη ικανοποιητικής απάντησης, μπορείτε να απευθυνθείτε στην εθνική αρχή ελέγχου.

Εάν η αίτηση δανείου σας απορρίπτεται εξαιτίας ανακριβών στοιχείων στο αρχείο της τράπεζας. Ζητάτε πρόσβαση στο αρχείο της τράπεζας προκειμένου να πληροφορηθείτε ποια στοιχεία έχουν καταγραφεί στον υπολογιστή της τράπεζας σχετικά με το πιστωτικό σας μητρώο. Ωστόσο, η τράπεζα δεν ανταποκρίνεται στο αίτημά σας για πρόσβαση. Κάνετε αρκετά τηλεφωνήματα στην τράπεζα σχετικά με το αίτημά σας, αλλά χωρίς αποτέλεσμα. Ποιες μπορούν να είναι οι επόμενες ενέργειές σας;

Η οδηγία αναφέρει ότι έχετε δικαίωμα πρόσβασης «χωρίς υπερβολική καθυστέρηση» σε όλα τα δεδομένα προσωπικού χαρακτήρα που υπάρχουν για το άτομό σας. Εάν τα δεδομένα είναι ανακριβή, έχετε το δικαίωμα να ζητήσετε τη διόρθωσή τους. Γι' αυτό, εάν δεν έχετε απάντηση από την τράπεζα μέσα σε εύλογο χρονικό διάστημα, μπορείτε να παραπονεθείτε άμεσα στην εθνική αρχή ελέγχου. Σύμφωνα με την οδηγία, η εθνική αρχή ελέγχου οφείλει να διερευνήσει την καταγγελία και να ενημερώσει τον καταγγέλλοντα σχετικά με το αποτέλεσμα.

Κατά την επαφή σας με την εθνική αρχή ελέγχου πρέπει (κατά προτίμηση εγγράφως) να περιγράψετε το πρόβλημα και να παράσχετε επαρκείς πληροφορίες ώστε να γίνει πλήρως κατανοητό. Σε ορισμένα κράτη μέλη η εθνική αρχή ελέγχου έχει τυποποιημένα έντυπα που μπορείτε να συμπληρώσετε για να υποβάλετε την καταγγελία σας. Εάν υπάρχουν τα έντυπα αυτά, θα πρέπει να τα χρησιμοποιήσετε γιατί έτσι θα επιταχυνθεί η εξέταση της καταγγελίας σας και θα λάβετε απάντηση συντομότερα. Σε ορισμένα κράτη μέλη είναι εφικτή η υποβολή καταγγελιών μέσω ηλεκτρονικού ταχυδρομείου. Σε άλλα, δεν υπάρχει ακόμα η δυνατότητα αυτή.

Εάν τα αποτελέσματα δεν είναι ικανοποιητικά, μπορεί να χρειαστεί να προσφύγετε στα δικαστήρια. Στην περίπτωση αυτή καλό θα ήταν να ζητήσετε τη συμβουλή νομικού. Η προσφυγή στα δικαστήρια μπορεί επίσης να είναι αναγκαία σε περίπτωση που έχετε υποστεί ζημιές εξαιτίας της παραβίασης των δικαιωμάτων σας. Μπορεί να σας επιδικαστεί αποζημίωση.

Αν ο εργοδότης σας κοινοποίησε τον ιατρικό σας φάκελο χωρίς τη συγκατάθεσή σας. Ο ιατρικός φάκελος περιείχε πληροφορίες, το περιεχόμενο των οποίων μπορεί να αποτελέσει αιτία για την οποία η τράπεζα αρνείται να σας χορηγήσει ενυπόθηκο δάνειο. Δικαιούστε αποζημίωσης;

Δικαιούστε αποζημίωσης εάν έχετε υποστεί ζημία λόγω παράνομης αποκάλυψης των δεδομένων σας προσωπικού χαρακτήρα. Αυτό μπορεί να ισχύει στην περίπτωση που τα ιατρικά σας στοιχεία έχουν κοινοποιηθεί χωρίς την άδειά σας.

Κάθε άτομο ή επιχείρηση μπορεί να υποβάλει καταγγελία στην Επιτροπή σχετικά με επικαλούμενη παράβαση του κοινοτικού δικαίου εκ μέρους κράτους μέλους.

Η Ευρωπαϊκή Επιτροπή εξασφαλίζει την ορθή εφαρμογή της κοινοτικής νομοθεσίας στα κράτη μέλη. Εάν χρειάζεται, η Επιτροπή υπενθυμίζει στα κράτη μέλη τις ευθύνες τους για την έγκαιρη και ορθή εφαρμογή της κοινοτικής νομοθεσίας. Σε ορισμένες περιπτώσεις, εάν ένα κράτος μέλος δεν έχει εκπληρώσει αυτές τις υποχρεώσεις του, η Επιτροπή μπορεί να εγείρει προσφυγή στο Ευρωπαϊκό Δικαστήριο, το οποίο αποφασίζει κατά πόσο υπάρχει παράβαση του κοινοτικού δικαίου.

Δεν χρειάζεται να αποδείξετε ότι επηρεάζεστε άμεσα από την παράβαση που επικαλείστε.

Ωστόσο, διαφορές μεταξύ ιδιωτών δεν μπορούν να διευθετηθούν από την Επιτροπή στο πλαίσιο αυτό.

Οι καταγγελίες υποβάλλονται χωρίς χρέωση και δεν είναι απαραίτητη η συνδρομή δικηγόρου. Κατά την υποβολή της καταγγελίας σας δεν πρέπει να παραλείψετε να συμπεριλάβετε σχετικές πληροφορίες και έγγραφα τεκμηρίωσης (π.χ. σχετικούς εθνικούς κανόνες).

Μπορείτε να υποβάλετε καταγγελία στην Επιτροπή με επιστολή σας στη διεύθυνση:

Commission of the European Communities (for the attention of the Secretary-General), Rue de la Loi 200, B- 1049 Brussels

ή χρησιμοποιώντας το τυποποιημένο έντυπο που διατίθεται από τις κατά τόπους υπηρεσίες της Επιτροπής στα κράτη μέλη και στο Διαδίκτυο στη διεύθυνση: http://europa.eu.int/comm/sg/lexcomm

ΔΙΑΒΙΒΑΣΕΙΣ ΔΕΔΟΜΕΝΩΝ ΣΕ ΧΩΡΕΣ ΕΚΤΟΣ ΕΕ

Σε περιπτώσεις διαβίβασης δεδομένων σε χώρες μη μέλη της Ευρωπαϊκής Ένωσης, μπορεί να χρειάζεται να ληφθούν ειδικές προφυλάξεις, εάν το επίπεδο προστασίας των δεδομένων στην τρίτη χώρα δεν είναι αντίστοιχο με εκείνο του ευρωπαϊκού δικαίου. Χωρίς τέτοιους κανόνες, το υψηλό επίπεδο προστασίας των δεδομένων που καθιερώνει η οδηγία μπορεί γρήγορα να υπονομευθεί, με δεδομένη την ευκολία με την οποία τα δεδομένα μπορούν να μεταφερθούν μέσω των διεθνών δικτύων.

Η αρχή της οδηγίας είναι ότι τα δεδομένα προσωπικού χαρακτήρα μπορούν να διαβιβαστούν σε χώρες εκτός ΕΕ που εξασφαλίζουν «ικανοποιητικό» επίπεδο προστασίας. Ήδη πραγματοποιούνται αναλύσεις των νομοθεσιών περί προστασίας των δεδομένων και διεξάγονται συζητήσεις με τους κυριότερους εμπορικούς εταίρους της ΕΕ, προκειμένου να αποφασιστεί ποιες χώρες μπορούν να θεωρηθούν ότι παρέχουν ικανοποιητική προστασία.

Όταν μια χώρα μη μέλος της Ευρωπαϊκής Ένωσης δεν εξασφαλίζει ικανοποιητικό επίπεδο προστασίας, η οδηγία απαγορεύει τη διαβίβαση ορισμένων δεδομένων. Τα κράτη μέλη οφείλουν να ενημερώνουν την Επιτροπή σχετικά με τέτοια μέτρα απαγόρευσης. Μετά από κάθε σχετική ενημέρωση κινείται μια κοινοτική διαδικασία, προκειμένου να εξασφαλιστεί ότι η απόφαση κράτους μέλους να απαγορεύσει συγκεκριμένη διαβίβαση είτε θα επεκταθεί σε όλη την ΕΕ είτε θα ανατραπεί.

Τι μπορούν να πράξουν οι επιχειρήσεις τρίτων χωρών;

Η απαγόρευση διαβιβάσεων δεδομένων προσωπικού χαρακτήρα αποτελεί λύση έσχατης ανάγκης. Υπάρχουν άλλοι τρόποι για να εξασφαλιστεί ότι τα δεδομένα εξακολουθούν να προστατεύονται επαρκώς χωρίς να διαταράσσονται οι διεθνείς ροές δεδομένων και οι εμπορικές συναλλαγές με τις οποίες συνδέονται τα δεδομένα. Εάν οι επιχειρήσεις της ΕΕ δεν είναι σίγουρες κατά πόσο η νομοθεσία ή τα συστήματα αυτορρύθμισης τρίτης χώρας παρέχουν ικανοποιητική προστασία, θα πρέπει να τους υποδειχθεί να παράσχουν οι ίδιες την προστασία αυτή. Αυτό μπορεί να επιτευχθεί μέσω σύμβασης μεταξύ της επιχείρησης που διαβιβάζει τα δεδομένα και της επιχείρησης της τρίτης χώρας που είναι ο αποδέκτης των δεδομένων. Το αντικείμενο

μιας τέτοιας σύμβασης μπορεί να είναι η εξασφάλιση επαρκών εγγυήσεων για την προστασία της ιδιωτικής ζωής και των θεμελιωδών δικαιωμάτων και ελευθεριών των προσώπων καθώς και την άσκηση των σχετικών δικαιωμάτων. Εφόσον υπάρξουν επαρκείς διασφαλίσεις, δεν συντρέχει λόγος για τα κράτη μέλη να απαγορεύουν διαβιβάσεις δεδομένων που αφορούν τους πολίτες τους.

ΠΕΡΙΕΧΟΜΕΝΑ

ΒΙΒΛΙΟΓΡΑΦΙΑ

Applied Cryptography, Second Edition
Bruce Schneier Copyright 1996 Εκδοτικός Οίκος Willey

Wiley
Building Set Applications For Secure Transactions
MARK S. MARKOW/ JIM BREITHUPT/ KEN L. WHEELER

Information technology – Code of practice for information security management
BS ISO / IEC 17799:2000
BS 7799-1:2000

Περιοδικό: Financial Ram, τεύχος Μαΐου 2005, Αρ. Φύλλου 5, σελ.19-29

Περιοδικό: Ram, τεύχος 184 Οκτωβρίου 2004
e-banking σελ. 115-140

Περιοδικό: Ram, τεύχος 172 Σεπτεμβρίου 2003
e-banking, σελ. 84-105

Περιοδικό: Ram, τεύχος 158 Μαΐου 2002
Επικοινωνία και ασφάλεια στο Internet σελ. 204-207

ΗΛΕΚΤΡΟΝΙΚΟΙ ΤΟΠΟΙ (sites):

www.eos.uom.gr (Cryptography and its products)
(Forms of attack)
(SSL: a case study)
(Technologies based on encryption)
(Payment Systems)
(Techniques and software tools)
(Web sites and security)

e-business forum: Ηλεκτρονικές πληρωμές: Προβλήματα και προοπτικές

www.europa.eu.int (Προστασία Δεδομένων)
www.eurobank.gr
www.winbank.gr
www.egnatiabank.gr
www.alpha.gr
www.aspisbank.gr
www.novabank.gr
www.nbg.gr
www.citibank.gr
www.laikiebank.gr
www.emporiki.gr
www.bankofcyprus.gr

e-books: An Introduction of Cryptography, Copyright 1990-1998
Network Associates, Inc and its Affiliated Companies

Applied Cryptography, Copyright 1997 by Press, Inc
(Δημοσίευμα)