Ηλεκτρονικό εμπόριο

ΗΕ 6

Ασφάλεια

Ηλεκτρονικό εμπόριο και ασφάλεια

- Δισταγμός χρηστών στην χρήση του ηλεκτρονικού εμπορίου
- Αναζήτηση ασφαλούς περιβάλλοντος ηλεκτρονικού εμπορίου
- Ζητούμενο είναι η ασφάλεια συναλλαγών

Δεν υπάρχει μια λύση ασφάλειας που να μπορεί να εφαρμοστεί σε **όλες** τις επιχειρήσεις.

Προβλήματα ασφάλειας

- Καταστροφή δεδομένων
- Εξαπάτηση πελατών
- Κλοπή χρημάτων
- Παραποίηση εγγράφων
- Υποκλοπή προσωπικών δεδομένων
- Υποκλοπή οικονομικών πληροφοριών

Απειλές κατά των ηλεκτρονικών συναλλαγών

- Πρόσβαση χωρίς εξουσιοδότηση σε δικτυακούς πόρους
- Καταστροφή πληροφοριών
- Παραποίηση πληροφοριών
- Αποκάλυψη πληροφοριών σε μη εξουσιοδοτημένα άτομα
- Διακοπή δικτυακών υπηρεσιών
- Κλοπή πληροφοριών και δικτυακών πόρων
- Άρνηση λήψης υπηρεσιών και άρνηση αποστολής ή λήψης πληροφοριών
- Ισχυρισμός παροχής υπηρεσιών χωρίς άδεια
- Αποκάλυψη προς τρίτους εμπιστευτικών στοιχείων συναλλαγών

Πλάνο ασφάλειας

- Διαχειριστής ασφάλειας e-shop
  - Ανάλυση κινδύνων
  - Χρήση τεχνολογιών με ικανοποιητικό λόγο κόστους προς απόδοση
- Πολιτική ασφάλειας
  - Περιγράφει τις απειλές ασφάλειας που αντιμετωπίζονται
  - Καθορίζει τι προστατεύεται και γιατί
  - Περιγράφει διαδικασίες που πρέπει να ακολουθηθούν όταν εντοπιστεί ένα πρόβλημα ασφάλειας

Αιτίες προβλημάτων ασφάλειας στο Διαδίκτυο

- Οι υπολογιστές είναι διασυνδεδεμένοι
- Το δίκτυο είναι δημόσιο
- Οι υπολογιστές καταγράφουν πληροφορίες
- Ελλειπής ενημέρωση χρηστών
- Οι υπολογιστές μπορούν να προγραμματιστούν
- Σε ένα μη ασφαλές σύστημα μια επίθεση μπορεί να μην αφήσει ίχνη

Η ασφάλεια ως πρόβλημα διαχείρισης κινδύνων

- Το επίπεδο ασφάλειας εξαρτάται από το τι θέλει κανείς να προστατέψει.
- Επιπρόσθετη ασφάλεια σημαίνει περισσότερο κόστος
- Η ασφάλεια κάθε τμήματος ενός συστήματος θα πρέπει να είναι το ίδιο δυνατή με όλων των άλλων τμημάτων αλλιώς μπορεί να λειτουργήσει ως αδύναμος κρίκος.

Βασικές συνιστώσες ασφάλειας

- Πολιτικές ασφαλείας και διαδικασίες
  - Αλλάζουν όταν οι εξελίξεις το επιβάλλουν
- Τεχνολογία
  - Κρυπτογράφηση, πρωτόκολλα ασφαλών επικοινωνιών
- Προσωπικό
  - Εκπαίδευση σε θέματα ασφάλειας

Απαιτήσεις ασφαλείας συστημάτων e-εμπορίου

- Έλεγχος αυθεντικότητας (authentication)
- Εξουσιοδότηση (authorization)
- Εμπιστευτικότητα (confidentiality)
- Ακεραιότητα (integrity)
- Μη αποποίηση ευθύνης (non-reputiation)

Έλεγχος αυθεντικότητας (Authentication)

- Εξακρίβωση ταυτότητας χρήστη – αποφυγή ψηφιακής πλαστοπροσωπίας.
- Παράγοντες στους οποίους στηρίζονται οι μέθοδοι αυθεντικότητας:
  - Επιβεβαίωση γνώσης ιδιοκτησιακών πληροφοριών
  - Κατοχή ιδιοκτησιακής πληροφορίας (π.χ. κάρτα)
  - Βιομετρικά χαρακτηριστικά
  - Απόδειξη ταυτότητας από έμπιστο τρίτο μέλος

Πριν γίνει μια ηλεκτρονική συναλλαγή απαιτείται έλεγχος αυθεντικότητας

Εξουσιοδότηση (Authorization)

- Η ταυτότητα του χρήστη έχει ήδη εξακριβωθεί
- Η εξουσιοδότηση καθορίζει τις ενέργειες που μπορεί να πραγματοποιήσει ο χρήστης με βάση το επίπεδο ασφάλειας που διαθέτει
- Δικαιώματα πρόσβασης
  - Δημιουργία περιεχομένου (create)
  - Ανάγνωση περιεχομένου (read)
  - Τροποποίηση περιεχομένου (update)
  - Διαγραφή περιεχομένου (delete)

Η εξουσιοδότηση καθορίζει τα δικαιώματα πρόσβασης σε πόρους

Εμπιστευτικότητα (Confidentiality)

- Αποφυγή μη εξουσιοδοτημένης ανάγνωσης πληροφοριών
- Επιτυγχάνεται μέσω της κρυπτογράφησης
- Κρισιμότητα εμπιστευτικότητας σε επιχειρήσεις που διαχειρίζονται οικονομικά στοιχεία

- Η εμπιστευτικότητα θα πρέπει να εξασφαλίζει ότι ευαίσθητη πληροφορία δεν μπορεί **να διαβαστεί**, **να αντιγραφεί** ή **να μετατραπεί** χωρίς την απαραίτητη εξουσιοδότηση

Η εμπιστευτικότητα έχει να κάνει με την διασφάλιση ότι η πληροφορία είναι διαθέσιμη μόνο σε όσους έχουν το δικαίωμα πρόσβασης σε αυτή

Ακεραιότητα (Integrity)

- Αποφυγή μη εξουσιοδοτημένης τροποποίησης των δεδομένων κατά την διάρκεια μεταφοράς τους ή αποθήκευσής τους
- Για να διασφαλιστεί ότι τα δεδομένα θα φτάσουν στον προορισμό τους όπως ακριβώς στάλθηκαν μπορούν να χρησιμοποιηθούν οι ψηφιακές υπογραφές

Μη αποποίηση ευθύνης (non reputiation)

- Διασφάλιση ότι κανένας από τους συναλλασσόμενους δεν έχει την δυνατότητα να αρνηθεί την συμμετοχή του σε μια συναλλαγή
- Μια υπηρεσία μη αποποίησης ευθύνης θα πρέπει να είναι σε θέση να αποδείξει την προέλευση, τη μετάδοση και την παράδοση των δεδομένων

Σχεδιασμός ασφάλειας

- Βασικά βήματα σχεδιασμού ασφάλειας σε ένα ηλεκτρονικό κατάστημα:
  - Καθορισμός πολιτικής ασφάλειας
  - Σχεδιασμός ασφάλειας περιβάλλοντος εφαρμογής
  - Σχεδιασμός ασφάλειας εφαρμογής e-shop
  - Επίβλεψη και περιοδικός ελέγχος για την διασφάλιση της ορθής λειτουργίας του συστήματος

Πολιτική ασφάλειας eshop

- Αφορά υλικό (Η/Υ και δίκτυα), δεδομένα και ανθρώπινο δυναμικό.
- Περιέχει αναφορές σχετικά με:
  - Τι προστατεύεται;
  - Τι είδος προστασίας απαιτείται;
  - Ποιος είναι ο υπεύθυνος για κάθε μέρος του συστήματος;
  - Τι εκπαίδευση απαιτείται;
  - Τι επίβλεψη και περιοδικός έλεγχος απαιτείται;

Σχεδιασμός ασφάλειας περιβάλλοντος εφαρμογής

- Αφορά θέματα ασφάλειας που δεν σχετίζονται με την εφαρμογή eshop
- Αφορά φυσικές εγκαταστάσεις, δίκτυα, υπολογιστές και το επίπεδο ασφάλειας που παρέχουν

Σχεδιασμός μηχανισμών ασφάλειας εφαρμογής e-shop

- Η ίδια η εφαρμογή μπορεί να χρησιμοποιεί διάφορες τεχνολογίες έτσι ώστε να ενισχύει το επίπεδο ασφάλειας που διαθέτει. Για παράδειγμα:
  - Χρήση κρυπτογράφησης στις συναλλαγές
  - Χρήση ψηφιακών υπογραφών

Επίβλεψη και περιοδικός έλεγχος

- Εξετάζει την ποιότητα των υπηρεσιών που παρέχονται στους πελάτες
- Διασφαλίζει ότι μηχανισμοί καταγραφής και ανάκτησης είναι λειτουργικοί
- Αφορά πληροφορίες όπως:
  - Ταχύτητα απόκρισης εφαρμογής
  - Επαναλειτουργία συστήματος από σφάλμα
  - Καταγραφή και ανάλυση επιθέσεων
- Αξιολογεί την αποτελεσματικότητα της πολιτικής ασφάλειας που εφαρμόζεται

Εχθροί - Απειλές

Κατηγορίες εχθρών

- Hackers-Crackers
- Εγκληματίες
- Ανταγωνιστές
- Κυβερνήσεις
- Εσωτερικοί εχθροί

Κατηγορίες απειλών

- Διακοπή υπηρεσιών
- Κλοπή ταυτότητας και απάτη
- Κατάχρηση
- Παραποίηση δεδομένων
- Κλοπή αρχείων
- Αλλαγή περιεχομένου
- Μεταμφίεση

Τεχνικές επιθέσεων

- Κοινωνική μηχανική (Social engineering)
- Denial of Service
- Trojan Horse
- Buffer overflow
- Port Scan
- Ακρόαση και ανάλυση κυκλοφορίας δικτύου

Πλάνο ασφάλειας

- Αναγνώριση και έλεγχος αυθεντικότητας
- Έλεγχος πρόσβασης
- Απόδοση ευθυνών
- Προστασία από ιούς
- Διαχείριση ασφάλειας δικτύου
- Έλεγχος πρόσβασης μέσω δικτύου
- Φυσική προστασία δικτύου
- Διαχείριση συστήματος
- Σχέδιο αδιάλειπτης λειτουργίας
- Προστασία από δυσλειτουργία του εξοπλισμού
- Φυσική προστασία του κτιρίου
- Παροχή ηλεκτρικής ενέργειας
- Προσωπικό
- Αντιμετώπιση περιστατικών