

Πτυχιακή Εργασία με θέμα:
«Ασφάλεια & Ιδιωτικότητα στο
Διαδίκτυο»

Επιμέλεια

Νικόλαος Γιανναράκης

Στόχοι Της Εργασίας

- 1) Να αναδείξει και να αναφέρει πόσο σημαντική είναι η ασφάλεια στο διαδίκτυο.
- 2) Να εξηγήσει την εμπιστευτικότητα και το ρόλο της κρυπτογράφησης.
- 3) Να προτείνει λύσεις για αύξηση προστασίας στους Η/Υ οι οποίοι συνδέονται στο Διαδίκτυο.

Ορισμός και Σκοπός Ασφάλειας στο Διαδίκτυο

- Σκοπός είναι να μειώσουμε την επίθεση από κακόβουλους χρήστες τόσο σε υλικό και λογισμικό επίπεδο όσο και σε προσωπικό.
- Η ασφάλεια στο Διαδίκτυο, τα ζητήματα προστασίας της ιδιωτικής ζωής, η παρενόχληση στον κυβερνοχώρο δεν είναι παρά μερικά από τα προβλήματα της εποχής μας.

Ασφάλεια του Εξυπηρέτη Web

Για την ασφάλεια του εξυπηρέτη Web και κατ' επέκταση για την ασφάλεια όλου του δικτύου, πρέπει να υπάρχει ένα ολοκληρωμένο σύστημα προστασίας.

- Διαγραφή όλων των άχρηστων λογαριασμών.
- Διαγραφή όλων των μεταφραστών γλωσσών(compilers).
- Παροχή των απαιτούμενων υπηρεσιών και μόνο αυτών.

Ασφάλεια του χρήστη

Ένα χρήστης για την ασφάλεια του και για να προστατευτεί από κακόβουλα λογισμικά χρησιμοποιεί διάφορα φράγματα προστασίας(firewall) και διάφορα λογισμικά προστασίας από ιός και σκουλήκια

Κρυπτογράφηση

Η ανάγκη για εμπιστευτικότητα στην ηλεκτρονική συναλλαγή ικανοποιείται με την κρυπτογραφία.

Υπάρχουν δυο είδη κρυπτογράφησης:

- Συμμετρική κρυπτογράφηση
- Ασύμμετρη κρυπτογράφηση

Πιστοποίηση και τρόποι κρυπτογράφησης

Χρησιμοποιώντας κατάλληλα τους κρυπτογραφικούς αλγορίθμους δημοσίου κλειδιού μπορεί να επιτευχθεί πιστοποίηση, δηλαδή ο παραλήπτης να γνωρίζει με ασφάλεια την ταυτότητα του αποστολέα.

Υπάρχουν διάφοροι αλγόριθμοι κρυπτογράφησης όπως RSA, DES και άλλοι πολλοί.

Φράγματα ασφαλείας

Φράγμα ασφάλειας ονομάζεται ένα σύστημα που αποτελείται από δικτυακά στοιχεία τα οποία τοποθετούνται μεταξύ δύο δικτύων και το οποίο έχει τα ακόλουθα χαρακτηριστικά:

- Όλη η δικτυακή κίνηση από και προς το εσωτερικό δίκτυο πρέπει να περάσει μέσα από αυτό το σύστημα.
- Η διέλευση επιτρέπεται μόνο σε εξουσιοδοτημένους χρήστες, όπως αυτή καθορίζεται από την τοπική πολιτική ασφάλειας.
- Είναι αδιαπέραστο σε απόπειρες διείσδυσης.

Ασφάλεια στο Ηλεκτρονικό

Εμπόριο

Ένα από τα πιο σημαντικά ζητήματα που σχετίζονται άμεσα με τη χρήση και τη διάδοση του Ηλεκτρονικού Εμπορίου αφορά το επίπεδο ασφάλειας των ηλεκτρονικών συναλλαγών. Οι βασικές απαιτήσεις για την ασφαλή διεξαγωγή του Ηλεκτρονικού Εμπορίου είναι:

- Η Εμπιστευτικότητα
- Η Ακεραιότητα
- Ο Έλεγχος Αυθεντικότητας

Συμπεράσματα

Σήμερα υπάρχει πληθώρα πληροφορίας και εργαλείων τα οποία μπορεί να χρησιμοποιήσει ο οποιοσδήποτε ώστε να διαπιστώσει και να εκμεταλλευτεί τις αδυναμίες ενός δικτύου. Έτσι τώρα ακόμη περισσότερο από ποτέ, καθώς είναι εύκολο ακόμη και για τον πλέον αρχάριο στο hacking να σκανάρει, να διεισδύσει και να προσβάλει να συστήματά μας, καθίσταται πολύ σημαντικό να έχουμε τους κατάλληλους συμβούλους στα θέματα ασφαλείας.

ΤΕΛΟΣ ΠΑΡΟΥΣΙΑΣΗΣ

Ευχαριστώ