**Network Design**

Computer Network is a distributed system consisting of loosely coupled computers and other devices any of these devices or network nodes elements must be control by set of rules and protocols.

Security is a continuous process of protecting an organization from attack. Organization like this one requires sophisticated security of all its resources due to its business type “selling software products” and its version control system requires continuous check and processing, verification and updating of all its service packs and bug fixes available.

Below are some important guidelines regarding network design

* To avoid unauthorized access of information to third parties.
* To avoid unauthorized modification of network resources
* To avoid unauthorized suppression of system resources from those who need them.

**Fire wall**

A firewall is a layer combination of hardware and software that monitor and filter incoming and outgoing network data packets, firewall offer two type of services the one is accept or deny based on security policy and also provides services to inside user and protect inside user from a bad one outside who wants to steal the creative artwork.

**Authentication**

There are two types of users who want to access the network the one is internal staff and others are clients

**Lan Authentication**

The developer must login to the system with appropriate user id and password and only access for his or her folder only.

**WAN Authentication**

The customer or client must access system through web server and validated by a secure id only related to the client and only download his or her software only.

**Security policy**

* A risk analysis must be done before network design evaluate the fundamental assets and its protection and estimate the potential damage.
* Implement a security policy with respect to technology and people either client or developer.
* IP addresses of client and developer must be track and logged.
* Security monitoring to detect possible intrusions and also security including firewall and bug fixes.
* E-mail and Web access ( DNS, WWW, SMTP)
* Hardware access (logon passwords/Usernames)
* Databases (Data backup).
* Ensure every security patched updated on every system in an organization
* Construct the very detail table for the following security risk.
  + 1. DDOS attacks
    2. Unauthorized access

|  |  |  |
| --- | --- | --- |
| What you know | Password, PIN | Can be forgotten, guessed, duplicated |
| What you have | Token, ID Card, Keys | Can be lost, stolen, duplicated |

Authentication Factors and Their vulnerabilities

**Payment policies**

* Identify the security risks in electronic payment and the personal information that being held.
* Buildup and create procedures to reduce the risk involved in electronic transactions.
* Update customer security and authentication mechanisms over time to make sure the security offered is maintained, at an appropriate level
* Site security, how well secured is the e commerce web site

|  |
| --- |
| SSL with server certificate |
| SSL with server/client certificate |
| other fraud detection mechanisms |
| payer authentication (Verified by Visa, Secure Code) |

Realization of payment security model

**Anonymous Web Access**

* Make sure any Anonymous access to system and download the software without paying any amount to the company.
* All the creative work and source code must be protected by the help of user id and password.
* Only trusted clients and customer gain access to relative file and folders.