Free report on security design plan

Business, Management

Security design plan

The implementation of a good security plan undergoes a lot of steps. There is need to ensure that all aspects of operations are considered. These include the need to have a consideration for policies put in place, the risks involved and the strategy that will be used in the deployment. This paper will cover the issues that need to be taken into consideration when undertaking the aspects of security.

PKI implementation

The implementation of the PKI will be done after there is an auditing done by independent auditing firms in the presence of IT managers. After this, the internal Certificate Authority (CA) which is managed by local firms will then go through the laid down procedures. The graphical representation

Strategies to complete PKI infrastructure

In the design of a PKI infrastructure in organization, there is need for the government to consider the different needs of the businesses which are to be catered for in the design of the PKI infrastructure. For businesses which deal with computer software for example, there is need to ensure that the software which is in form of code that is sent to the client is still intact and no alteration has been done to the coding. If it deals with newspaper and the distribution of news on the Internet, it will require that the integrity of information is intact and that there is no alteration to the original information.

Defining the requirements

Planning: there should be careful planning in the implementation process of the PKI structure in the organization. This will entail the collection of all the information concerning the business models that are available in the organization. All forms of business should be analyzed and their requirements well taken care of. There are different requirements and different modes of operating the different businesses in the Internet.

Interoperability: when there is the rolling out of a new model of business, there is need to have the platform requirements of the systems that will be rolled out in the system. There is need to have platform analysis that is in operation in the organization. There are universal standards which can be used to have a common standard and platform for all the security policies in a given organization. These include ISO, ANSI, IETF, IEEE, and PKCS; they are under development for PKI. Because there are different standards which are competing in the market, there is need to have a common standard for developing PKI on.

PKI system and vendor: after the determination of a common platform for the implementation of the PKI, the next step is determining the PKI system that will be used in the organization. There are many vendors that are competing in the market of organization. Because of this competition, there are different protocols, platforms and certificate formats that are available in the organization. There is need to do some investigation to look for the best PKI system that will be used in the organization.

Performance and capacity: In situations where a large amount of data is to be enciphered for confidentiality, the use of public key cryptography may not

be the best option available for this; this is attributed to the fact that performance will be deteriorated. There is need to use symmetric or secret key cryptography. The organization should look into situations where this is required.

Digital certificates

Digital certificate are tools which are used for authentication. This should be implemented so that the users of the network will be authenticated in the network. These are the authentication tools which are issued by Certificate Authority (CA). In summary, the working of CA is as follows. For entities which are unknown to each other, they will each establish a trust relationship with a CA. The CA will perform some form of entity authentication according to the rules that have been established as has been noted by the Certificate Practices Statement (CPS). After this process, each entity is then issued with a digital certificate. The beauty of this is the fact that the certificate is signed by CA and thus the identity of the entities is vouched. With this, individuals who are unknown to each other can then establish trust between them because they have trust with the CA that it has performed some form of authentication on both of the entities. What is more, the signing of the CA is an attestation to this fact.

IPSEC

IPsec is a security standard that is meant to provide security for peers which are engaged with data protection and transfer in a given peer. The paper will entail having the design take care of such issues as intrusion design issues

and denial of service. There will also be a need to integrate firewall issues in the design.

Encrypting file systems

Since the organization will be sending files from time to time, there will be the need to have an encrypting file system. This will require that there will be a file system that will be integrated with the proxy server. The proxy server will be designed in such a way that the files that are sent are encrypted and those which are received are equally decrypted. This will avoid files which are sent and have viruses attached.

PGP (Pretty Good Privacy)

There is also the need to make use of pretty good privacy protocol. This protocol is an hybrid of privacy protocols. It is a strong protocol that is used by many organizations. The biggest problem they encountered was the retrieval of information contained on the device the criminals possessed. This was thwarted by the encryption software used by the criminals. Fantasy Games network should make use of this privacy as it combines various technology for privacy. This technology is used in management of files.

Active directory rights management services

The design of the active directory should be such that the users are grouped according to the roles that they play in the organization. This will ensure that management of the various users will be simple. The various users will be managed basing on the roles and the privileges they have. The active directory should be well segmented so that actions in one domain do not affect the other domains.

Wireless network security

With the increase of wireless networks due to devices that can access the network, there is the need to consider security of the wireless spectrum. This will require that the wireless network will be made secure. Just like any other system, wireless security is prone to threats. Threats can be caused by poor management of the system or intentional violations of the system functionality. Rogue access points should be assessed. This becomes a threat to the network if the same is not carefully managed. Unmanaged devices in the network provide easy backdoor and route of entry for attackers. This problem can be solved by ensuring strict policies and follow-ups on all the access points. An attacker can use WAPs to influence the wireless systems transmissions, which he can then monitor closely. All users of laptops and PDAs should have security plan that should be followed. All users of these mobile device users should use passwords and usernames. They will be tracked if there is some errors and intrusion in the network.

The common concepts in wireless security currently are WEP, VPN, WPA and IDS.

WEP

WEP stands for the Wired Equivalent Protocol. It is the most widely used protocol in the wireless field. It actually was the first protocol established in the security of wireless networks sector. Though this method is widely used in the in wireless industry, it is prone to many problems. The first problem has to do with the fact that the system is based on alphanumeric keys. It becomes easier for a hacker to uncover private and public key by use of hacking methods such as dictionary or brute force approach. Another

problem associated with these methods of authentication in wireless security is the length of the keys. The keys used are short in length hence giving a hacker easy time in guessing the possible combinations of the same. Moreover, the same keys are static. It means that the same do not change unless done so manually. Static keys are easier to guess or hack into; however, the server can change dynamic keys frequently. In static key approach offered by the WEP technology, an administrator has to change the keys of every device in each location.

WAPs

Wireless access points are radio devices, which have low frequency and can transmit over short distances. The distances covered by the broad cast could be as short as ten meters or a few blocks away. WAP cards can be used in PCs at home to connect to WAP cable modem, which is cheaply available. There is a disadvantage, however, associated with the WAP. Just like any radio device, the WAP is subject to interferences or attenuation. Buildings or walls can block or reduce the signal receive. Mountains and long distances also affect the same. High-tension electrical signals cannot be forgotten as another source of problem to WAP. The same can jam the signals.

WAP offers the potential of responding to the strongest radio frequency signal. The same, however, can be a disadvantage since any one can eavesdrop on someone’s WAP by just going or moving closer to it and setting its device to default. The most important advantage that WAP allows is the ability to implement dynamic WEP.

References

Fourazan, B. (2008). Cryptography and computer security. New York:

Cengage Learning.