Best Practices for Network Security

Name

University/College

Unit Name

Unit Code

Lecturer

27 March 2014

Outline

Introduction

The present day IT infrastructure and the general IT security systems face numerous security threats and challenges. These present a big concern to IT experts as the rate at which these security threats mutate at is quite alarming. This has over time changed the traditional view of Network Security as an institutional expense to the present day situation where network security is viewed as an investment.

Ashley (2003) literates that, "Network Security has over time become a crucial mission that every enterprise, organization or governmental agency must take maximum care of. As she points out, this has been necessitated by the increased threats of cyber-terrorism, increased hacking activity and the pronounced existence of disgruntled employees. Network security concerns have also been proven to evolve methodically leading to a mandatory requirement for institutions to invest heavily in network security management systems. As she further explains, the rapid evolution of information security compromising technologies further exposed corporate and other institutional information systems to numerous security threats thus, the need for the development, adoption and commissioning of Network Security practices.

According to Moss & Allan (2010), institutions need to develop mechanisms of enhancing their data security as well as securing their systems. As they observe, developing and implementing such a system needs to be based on enterprise security best practices. As such, an enterprise security best practice framework has three layers of divergence; the security backgrounders, security primers and security best practices. With each layer in the network security enforcement, implementation of each layer and all the processes and activities is required. The security backgrounders include the issues regarding to the security threats, strategies as well as the security planning process. On the other hand, security primers include the security architectural building blocks on which security concerns of a given network are anchored, the end system security considerations as well as the security system administration procedures. A further consideration into the best practice should include definition of the administrative authority on data availability and security, communication channel authentication and security management as well as security monitoring and auditing, Moss & Allan (2010)

In maintaining adequate security in any network, the architectural design of the network plays a crucial part, Megg (2009). Megg further discusses that network security is not an individual affair but an institutional concern to which every person in the institution has a stake in. He further state, "Network security systems play a crucial part in determining the informational integrity of an institution. Consequently, informational and network security should be a major investment that every institution takes part in."

This paper gives a guideline on Network Security Best Practice. The procedures required as well as the conditions to be observed in creating, enforcing and commissioning Network Security Best Practices are also detailed.

Developing Network Security Best Practices

I. The Pillars of network Security

In coming up with network security best practices, one should take into account all the pillars on which a network system relies on (Megg, 2009). These pillars include; confidentiality, authentication, and integrity and form the essentials that every secure network system must poss (Cisco, 2012).

(i) Confidentiality

The confidentiality pillar requires that the information transmitted through the network should be kept in the most secure and confidential manner; and without access by unauthorized parties. There are various factors that must be considered as to enhance confidentiality of the information being transmitted via the network in question. By ensuring that the information is highly secure, you also give the network a high degree of privacy as the information cannot be compromised while under transmission. Today, there are various ways used in enforcing informational security including data encryption, data hashing or data shielding among others. A secure network should have an independent architectural design whose structure bars unauthorized access to the information under transmission. In addition to this, there should be adequate policy provision in the framework as to prevent threats that the data under transmission may face such as wiretapping and electronic skimming among others, (Moss & allan, 2003).

(ii) Integrity

Next is data integrity. Data integrity means the quality of the data from the time of sending to the time of reception. Secure data should pose a high degree of similarity with the initially transmitted data. Any deviation from the norms of the initially send data arriving to the receiver or getting to the recipient in an unintended form maybe termed as a compromise to the data integrity. (Cisco, 2012) According to this white paper, policy considerations should be put in place to ensure that the integrity of the data under transmission within a given network is not compromised. Today, the commonly used data integrity enforcement procedures involve the use of cryptographic algorithms in hashing the information under transfer. Such algorithms used today include SHA and MD5 both of which rely on having the data securely hashed into a format which is not human readable and not easy to decrypt using simple means. In hashing the data, the process begins with creation of an arithmetic algorithm which uses the key and the data. As the arithmetic function splits into unique values (hashes), reading and decrypting the data becomes impossible hence reserving the integrity of the data at a high level. In accessing the data, only an authorized person with the right decrypting key can access the data. This ensures that the data is kept secure from external access by unauthorized parties (Dodd, 2011).

(iii) Authentication

This refers to the process of ensuring the data under transmission is only readable to the intended persons. As a result of having the data sent via a given network system, one needs to ascertain that the receiver of the data is the intended person. The process of attaining this is called authentication. Today, there are various data authentication processes used today including; the use of passwords and digital certificates among others (Cisco, 2012). As the author points out, well authenticated data is secure and safe; free from unauthorized access. As a result, the use of various state-of-the art data authentication procedures should be used to prevent the data under transmission from fraudulent access. Other modes of authenticating users today include the use of biometric readers where only the specific users biometric can be able to access the particular information.

II. Network Security Support Systems

Network security is anchored on various support systems such as support policy, administrative support, security planning and strategy, security auditing and threat detection among others, (Megg, 2009).

(i) Network security Policing

According to Megg (2009), these form the network security support pillar. As observed in the report, the three main stream pillars heavily rely on these support systems to enhance the security measures within a given framework. As the report further indicates, "network security is compromised without policy provisions." This illustrates the weight carried by the need for adequate policing when planning and implementing a network security plan. A network policy defines the administrative and the supportive roles as well as spells the punishments for breach of the network security policies and practices.

(ii) Security Planning

This involves the procedural laying down of the processes and activities to be used in enforcing security within a given network or institution. Corporate players use security planning for their network operations as to ensure efficiency of the transmission system as well as be able to enhance and promote a healthy and high level of security. Consequently, one needs to adequately plan the network security before choosing a particular network security enforcement strategy. The planned security measure should prevent, detect and possibly respond to any form of attack to the network system.

(iii) Architecture

The architecture of the system being used plays a significant role in determining the security level of the network. Consequently, the architectural structure of the information or data transmission system used should adequately allow for the transmission of the data while observing a high level of data security. A good system should not allow for the data being stored or transmitted to be compromised, (Ashley, 2003).

Network Security Best Practices

The goal of having an ideal security in a network is impossible. With no environment invulnerable, a more complex environment is more challenging and difficult to enhance security than a simplistic environment. This is so because every security plan operates within a budget, a set of policies, staff and technology among other determinants of security level, (Pfeil, 2010). As the author observes, different network users within an institutions have different roles. This is mainly used as the basis for grouping the network users as well as defining their corresponding duties.

For instance, a network should contain among others; administrators and analysts. This allows the roles and responsibilities towards the network to be set. Therefore, the roles taken by the various personnel accessing and working with the system should be defined and their right and privileges defines also. Through this, it becomes possible to track down the access to the network by the various users. The administrator should for instance have the right to allocate and deprive other users with non-administrative roles the access rights to the network, (Pfeil, 2010).

In the trial to maintain a secure environment within the system, one should ensure that the use of top security enforcement facilities such as firewalls, strong passwords, encryption of data under transmission as well as physical security enforcement within the operational area. This is important as in facilitates accountability. For the best results, institutions should ensure that proper policing regarding the various activities done by the network users whose misuse can lead to the network being compromised are avoided. In the case of use of the internet portal, the network administrator should be able to track the actions done over the network by the different users. This helps in managing the activity of different system users leading to high levels of accountability, (Dodd, 2011).

When considering having a network system, you should consider having more enhanced user access. Through the use of enhanced access capabilities for the users, you are able to detect, prevent or even track down fraudulent activities such as spoofing, hacking or even unauthorized access into the system using impersonated details. A good network system should also have a capability of detecting and barring repudiation acts which may compromise the integrity of the system. As Dodd (2011) observed, highly secure networks have higher levels of user authentication as to promote user identity and authentication before accessing the system. He further notes that for the system to remain highly secure, all the users accessing the system should have user access rights with different access privileges as to promote high integrity of the system. At an advanced level, the security should have well-structured access denial privileges for those not clearly authenticated into the system, (Dodd, 2011).

The network system should also have a good monitoring system from where all the access statistics are kept. This includes the use of such mechanism as access logs being embedded onto the network. Consequently, the network should periodically be checked by the systems administrator or analyst to detect any issues that might compromise or might have compromised with the network's integrity. As a result, periodic network audit should be done with in a depth analysis being done on the access logs and other logs showing network user activity. As Dodd (2011) observes, regularly audited networks are rarely compromised. This implies that as a practice rule, the system should be periodically analyzed. Through this analysis of the activity level of the various operations within the network also helps you detect issues that might have occurred such as information log deletion whose occurrence might compromise the network's integrity.

Conclusion

From the above discussion, it is worth noting that in the security enforcement in a network system or any other system, there is no ideal situation at which the network security is guaranteed. However, measures aimed at facilitating and promoting security improvement on the network are deployed, used and enforced. These are called the best practices for a network security and include; periodic checking, analysis and auditing of the network with the aim of identifying any form of fraudulent activity. Next, is the use of controlled access rights and privileges for the users at different levels. This ensures that the network does not get compromised on the grounds of having the users violate the system policies. In such a case, the system should have a system of handling such a user whose actions exposes the network to potential data loss of compromised network security among others.

References

Ashley, W. (2003). Layered Network Security: *A best-practices approach*. Latis Networks, Inc.

Dodd, T. (2011). *Monitoring and auditing for End Systems*. Retrieved March 26, 2014, from http://technet.microsoft.com/en-us/library/cc750908.aspx

Pfeil, K. (2010). *Data Security and Data Availability for End Systems*. Retrieved March 26, 2014 from http://technet.microsoft.com/en-us/library/cc722919.aspx

Cisco. (2012). Network Security Policy: *Best Practices White paper*. Doc.ID 13601

Megg, T.S. (2009). *Network Security Essentials*. New Jersey, Tx Pub.

Moss, R & Allan, S. (2010). Network Security: *A simplified approach to network security*. New York: Perennial.