Network administrator essay

The kind of information stored in a business database is confidential, personal or financial which makes securing the information a critical part of every business operation which wants to carry out transmission of data over a network.

When operating a network, especially if information is being communicated over a public network or to other stakeholders' data security and integrity is paramount to creating an aspect of trust between customer and business.

These security problems need to be addressed by examining the entire network architecture and the protocols used, for the weakest link in the chain, and devising a solution to making it secure (Vacca, 2002). How these holes can be identified is the first major task when performing security tasks, followed by implementing a robust solution which does not impinge on performance or uptime of the network or business operations. SSL and TLS provide a platform for implementing increased security for communication across public networks such as the internet.

This is done by encrypting all of the network segments which reside on the application layer of the protocol to facilitate the secure transit of any data which uses the transmission control protocol (TCP). The use of a certificate to do this makes the system more efficient, because any web server being queried already holds the certificate until it is needed, and a quick check from the browser is able to verify that the web server that is being connected to is what it says it is.

This certificate is deployed to the browser, which after running the cross check initiates a secure tunnel between the two end points where

information can be passed in a secure environment without the threat of being hacked. The secure endpoint is a seamless way of integrating the remote connection onto the local network through this SSL tunnel. There are many ways of communicating data over the internet in today’s global high speed business environment, and sending confidential, personal or financial information over the internet can present security issues.

There are many different groups of people who are unscrupulous and want to steal information, block client access, harass webmasters and prevent organizations from conducting their genuine business operations.

Hacking and hackers present a different set of problems for network administrators as well as users and managers of the companies. The various kinds of internet attack represent different software and hardware vulnerabilities, which must be stopped in order to prevent data compromise.

Having a set of secure network protocols is an important factor in preventing any attack on data integrity. Along with this, a secure network policy should be developed and implemented to prevent unauthorized access to anything, especially by someone with unauthorized access. If a secure network policy is not applied to a network then the risk of being compromised increases, which can cause a situation which is very dangerous for an organization considering the data that may be available on a network, which may be both financial and personal.

The scope for conducting criminal activities once a site or network has been hacked increases, due to the control asserted over the network and its operational functionality by the malicious user. According to Lane Mills the

best example of a network security policy is demonstrated by one of the most prominent networking corporations in the world, Cisco Systems, who offer “ an excellent example of a network security policy that addresses network security in three areas: preparation, prevention and response” (Mills, 2005, p. 8).

Every network administrator should ensure that these three areas are covered, and that the information, as well as the systems used to store this information, is deemed to be secure from unauthorized access, or use by unauthorized persons or organizations, as well as protecting them from modification or destruction.

The following controls for the protection of information and system resources must be implemented along with an administrative system of controls, which should include written policies, a framework for a high standard of work as well should have a set of guidelines to deal with any problems or potential situations, and how to resolve them, however it is much better to implement technologies such as SSL in order to prevent them from occurring, as the old adage goes, “ prevention is better than cure”.

The general network security policy must ensure that strong passwords are used and that intrusion detection is included, with a system of firewalls in place to prevent any unauthorized external access. Data must be secured using high levels of encryption, and finally the physical location of the network, the server rooms and telecommunications points, must pass basic security checks, with entry points protected and security in place to prevent unauthorized physical access.

All of “ the types of sensitive information that will reside on that system and the rules and restrictions that applies to the users who access the system” (Donnely, 1992, p.

90) must be combined under a totally secure network environment policy, which is all inclusive.