Example of essay on identifying potential malicious attacks

Business, Company

ICT systems and networks are very sensitive, and it is crucial for the ICT system and network of the firm to be well secured rom the various threats that exist. The network of the firm ought to be protected from such threats since it could lead to huge losses financially or intellectually. The firm may lose information stored in the database. This could stall normal operations or even result in sudden shutdown of all business operations. Thus, the security of the firm's network is central to perpetuity of the firm.

Vulnerabilities and Threat to the Network

When analyzing the effect of various threats it is crucial to understand the potential risks that could arise from such threats. Any network, and hence ICT system, comprises of an articulate combination of various software and accompanying hardware components. Threats can include those that are related to the set-up of new wireless networks. This includes threats on internet security due to certain infrastructural facilities such as DNS and routing.

Threats on the network might also arise from the existence of malicious hardware components. This may facilitate the migration of control to virtual computers. This means that virtualization and malicious hardware threaten the safety of a computer network. Cloud computing has become a very popular form of data storage. However, it poses great risks to the safety of the network (Kizza, 2009).

Most network systems make use of complex systems whose installation calls for hiring of big professional companies. These systems are usually complex and as such unforeseen or even unknown dependencies and interactions between different systems belonging to different companies may arise.

Furthermore, the professional firms may be in a position to access the various databases belonging to different clients without any authorization from the client. Digital systems are prone to manipulation. Therefore, professionals with the necessary technical knowledge always have an upper hand.

Threats might also arise from the use of botnets and other software and programs that make use of internet communication for functionality to be fully implemented. These are just some of the offensive infrastructures that set themselves in the internet and then carry out continuous malicious attacks on various networks that make use of the internet. Networks are also employing data storage mechanisms that stored data online. This is advantageous in terms of ease of access. However, this data is also prone to manipulation by the fact that it is online. Professional hackers can manipulate such data. The firm may suffer the fate of several large firms that have been subjected to the torture of data manipulation.

Firms have in the recent past become fond of using digital systems to carry out their business transactions. This means that even money transfer and the accompanying authorization is exposed to the risk of phishing. Phishing allows for imposters to act as trusted entities and hence carry out various illegal transactions. This may lead to huge financial losses. This is especially if the network administrator is careless and accepts emails from unknown senders. Such emails may contain malware that allows or the hackers to access and use digital passwords and credit card details that are required for any financial transactions to be viable. Therefore, the network is at a great

risk of attack by the simple fact that it is easy for imposters to masquerade as administrators (Bidgoli, 2006).

Potential Impact of All Identified Malicious Attacks and Threats to the Network and the Organization

The security of computer networks is largely affected by the type of spyware that is brought by the threat. This means that the data in the network can be automatically profiled. This type of security breach is often used by hackers to bypass firewalls. Security breaches may be curbed through the network intrusion detection system (NIDS) and the firewalls. However, malicious malware can easily find their way past firewalls. Some malware can hide against the firewall and slowly gather private information such as social security numbers of the employees and even their bank account details. The host of such a malware can then fetch such private information from the malware. Employees ought to be keen while making internet searches and downloading files from different websites.

Another threat to the security of the computer network of the firm is the fact that the security attacks are becoming more sophisticated by the day. This has occurred as a consequence of the increased complexity of the infrastructure and software used to fight simple attacks on the networks. Companies are sometimes overwhelmed by the number of attacks that exist. Therefore, they source such services from cloud providers. This, however, is an extra cost to the firm; one which the firm must incur.

Protection of Network from Vulnerabilities and Threats to the Network of the Firm

Protection at the system level can be achieved through the use of human interface devices and utilization of encryption. Encryption allows for hiding of the electronic identities and passwords of the users of the network. This prevents the occurrence of phishing by hackers. The network's security can also be largely improved by the establishment of a network perimeter that filters the items downloaded. The network administrator can activate content filtering and spam filters to ensure malware in the form of worms that are attached to emails are kept at bay. IT consultants can also be hired to set up vulnerability assessments. These will be responsible for checking the effect of downloading a certain item (prior to opening a certain web page) on the stability of the whole network system. Leakage of data can also be prevented through the installation of highly efficient, though expensive, software and hardware. Firewalls should be constantly updated so that they not become redundant. New and more improved firewalls are constantly being made, and it is only wise for the firm to invest in the installation of stronger firewalls. The data stored in disks can be protected via disk encryption procedures (Kumar et. al, 2005).

The firm can also adopt end-point compliance procedures on the individual laptops and desktops within the organization. Such technology is offered by companies such as Fiberlink and Symantec. This ensures that even end users are making use of the firewall and the antivirus. This is especially crucial since some users opt to bypass the firewall to suit their search needs. The use of cloud services also limits threats arising from DDoS attacks since it

redirects security issues away from the network.

Screening of traffic prior to entry into the network's premises is another crucial element in the protection of network from threats such as phishing. However, in order for the firm to successfully fight off the numerous threats and vulnerabilities that affect the network, it must use a combination of all these protection mechanisms. This includes the use of intrusion prevention services, especially on the network's perimeter.

References

Bidgoli, H. (2006). Handbook of Information Security Volume 3. Hoboken: John Wiley & Sons.

Kizza, J. M. (2009). A Guide to Computer Network Security. London: Springer.

Kumar, V., Srivastava, J., & Lazarevic, A. (2005). Managing Cyber Threats: Issues,

Approaches, and Challenges. New York: Springer.