Free term paper on potential attacks, threats, and vulnerabilities to network org...

Business, Company

Introduction

Computer networks are dedicated infrastructure setups that handle data, video, voice, file sharing, e-mail services, and remote access, among others, ensuring that these information and tasks are carried out correctly from one computer station to another. As companies' business transactions happen online, including employees' personal use of a company's network systems and the availability of many online resources, possible threats to network infrastructure becomes a living reality that companies must address to protect the availability, integrity, and confidentiality of information system resources. This paper is limited to discussion of possible attacks, threats, and vulnerabilities presented to this company, which is a videogames development company.

Potential Attacks and Threats

The videogames industry is not immune to computer attacks and threats. The many users who access the games networks expose the network to various security threats (Mohr & Rahman, 2011, p. 1). Because of this, it is important to understand that attacks and threats take many forms and the end-result is still the same – loss of privacy, damage in resources and date, and huge monetary losses for the company (Designing Network Security, 2005, p. 241).

Attacks may be in the form of reconnaissance, access, denial of service (DoS), or worms, viruses, and Trojan Horses. Reconnaissance " is the unauthorized discovery and mapping of systems, services, or vulnerabilities" (" Vulnerabilities, Threats, and Attacks", n. d., p. 22) in a network system.

Eavesdropping is a form of reconnaissance attack and is a common occurrence of network attacks (Understanding Network Attacks). This allows an attacker to listen in and interpret internet traffic in a company's network infrastructure. This is usually known as " sniffing" or " snooping", which only needs the internet protocol (IP) of the network to read, monitor, capture and interpret data exchanges. Because the Transmission Control Protocol/Internet Protocol (TCP/IP) is an open architecture, data can be read as it traverses the network. In such situations, a strong encryption services based on cryptography helps in protecting data (" Understanding Network Attacks"). Otherwise, sniffer applications can analyze network information, read confidential communications, and then cause network crashes or data corruption.

Attackers may also use password-based attacks to gain access to computer and network resources by posing as a valid user (" Vulnerabilities, Threats, and Attacks", n. d., p. 22). This means an attacker finds a valid user account and cracks the password by guessing until the correct password is hit. This gives the attacker the same access rights as the original user, which gives the attacker the opportunity to gather network information, computer names, and list of valid users. They can also change network configuration settings and access controls, including deleting important information (" Understanding Network Attacks").

The denial-of service (DoS) attack disallows valid users from accessing the computer or the network. It means an attacker has disabled the access rights of valid users or corrupted the networks that could result to system crashes. In most instances, there is no immediate noticeable intrusion

occurring on the network until incorrect data, abnormal termination of videogames services, or heavy network traffic occur (" A Beginner's Guide to Network Security", n. d., p. 4).

Worms, viruses, and Trojan Horses are common in video games as they are known as " delivery vehicles for destructive code" (" A Beginner's Guide to Network Security", n. d., p. 4). Worms create copies of itself and are spread though emails, while viruses reproduce by attaching itself to executable files. These three not only overwork the network with the traffic they generate, they can also steal vital company and business information as well as wipe out the content of the hard drives (" Vulnerabilities, Threats, and Attacks", n. d., p. 23).

Causes of Network Vulnerability

Network vulnerability is " anything that poses a potential avenue for attack or security breach against a system" (Awodele, Onuiri, & Okolie, 2012, p. 56). It is anything that puts the system at risk that no matter how careful or diligent the IT group is during implementation and deployment, unauthorized intruders will still be able to hack the system (Awodele, Onuiri, & Okolie, 2012, p. 56). This includes storing passwords on materials that can easily be compromised like notebooks or papers as these can easily be stolen. Another source of network vulnerability includes weak implementation of passwords as it could lead to attacks on the system. If the hacker personally knows the user, manually guessing the password is easy, otherwise, there are tools that help come up with various combinations of user IDs and passwords. Poor anti-virus implementation makes it easy for viruses to enter the system and

append on email attachments especially when employees themselves access sites that are not trusted (Awodele et al., 2012, p. 57).

Use of USB thumb drives exposes the network to various threats as well. Despite the size of the USB, it may contain a huge amount of data and since it is portable, can be used in various computer types. As such, hackers have devised a way to target network systems by creating malware that executes as soon as it connects with a live USB port (Manky, 2010).

Human Trojans also present a big problem for the company as some employees who hold grudges towards the company may also think of ways to wreak havoc to the network systems when they leave the company (Awodele et al., 2012, p. 57).

These are just some of the many attacks, threats, and vulnerabilities confronting the videogames companies. Thus, it is of prime importance that the company reviews its network security policies and come up with tighter rules when implementing said policies.

References

" A beginner's guide to network security." (n. d.). Cisco Systems. Retrieved from http://www. cisco. com/warp/public/cc/so/neso/sqso/beggu_pl. pdf

Awodele, O., Onuiri, E. E., & Okolie, S. E. (2012). " Vulnerabilities in network infrastructures and prevention/containment measures". Proceedings of Informing Science & IT Education Conference (InSITE). Retrieved from http://proceedings. informingscience. org/InSITE2012/InSITE12p053-067Awodele0012. pdf

Designing Network Security. (2005). Threats in an enterprise network.

Indianapolis: Pearson Education, Inc. Retrieved from http://www. doubleshotsecurity. com/pdf/design-network-security. pdf

Manky, D. (2010). Top 10 vulnerabilities inside the network. Network World. Retrieved from http://www. networkworld. com/news/tech/2010/110810-network-vulnerabilities. html? page= 1

Mohr, S. & Rahman, S. (2011). " IT security issues within the video game industry". International Journal of Computer Science & Information Technology (IJCSIT). 3(5). Retrieved from http://arxiv. org/ftp/arxiv/papers/1111/1111. 1769. pdf

" Understanding network attacks". (n. d.). Tech-FAQ. Retrieved from http://www. tech-faq. com/network-attacks. html

" Vulnerabilities, threats, and attacks." (n. d.). Retrieved from http://ptgmedia. pearsoncmg. com/images/1587131625/samplechapter/1587131625content. pdf