Security technologies and methodologies essay sample

Law, Security

In today’s computer based world there are several potential and devastating threats like hackers, viruses, worms, and Trojans etc. to our computers, networks, and confidential information. So to protect our computers, networks, and confidential information we install security applications and hardware systems to protect our confidential information, computers, and networks. Some of the most popular Internet security systems are firewalls, intrusive prevention system, intrusive detection system, access control, and cryptographic tools and processes. However, there is no Internet security application or hardware system that can block every threat every time, so one must up caution where the Internet is concerned. Firewalls

Firewalls are basically a wall between your computer or network and destructive forces from the Internet. They protect a company’s network and computers by filtering the information that comes through any Internet connection. They use certain methods like packet filtering, proxy service, or stateful inspection to protect computers or networks. This type of protection system is use for keeping computers or networks secure by running any information through filters and discarding all information that cannot pass through the filters. By creating a wall between the confidential information that a company needs to keep secure and any potential threat then the company will not need to worry about who has access to their confidential information. Intrusion Prevention Systems

The intrusion prevention systems (IPS) are network security applications that examine the activities on a network or system for malicious activities. These systems identify malicious activity then they log the information that was retrieved from the malicious activity and then they try to block or stop the

malicious activity. These types of systems are extremely helpful for a company to use for their network security. For these systems actively scan the network for malicious activity and then prevents the malicious activity from damaging the company’s network and system. When companies install intrusion prevention systems they do have to worry about manually monitoring the activities on their network or computer because this system automatically does that for the company, and this system also makes it harder for hackers to gain access to the company’s network or computers. Intrusion Detection Systems

Intrusion detection systems (IDS) are a device or software that also searches a network and/or computers for malicious activities and sends a report to management. The intrusion detection systems and intrusion prevention systems are similar because they both search a network and/or computers for malicious activities and send a report of their finding to management. However, intrusion prevention systems have an extra feature for protecting their network and/or computers because they can block and/or stop the malicious activities before it can do any damage to a company’s network and computers. Access Control

Access control systems are systems or applications that limit the access of information or places to the users that have the authority to be there or view the information that the user has been granted permission to view. When a company installs a keypad lock on their doors and has users IDs and passwords in order to access company information these are called access control systems. These types of systems help companies to keep confidential

information and/or systems secure. For they limit the exposure of their confidential information and/or systems to employees who have shown the company that they can be trusted with the information and/or systems. One of the most common access control systems for a company is the use of user ID logins and passwords for accessing company information. Cryptographic Tools & Processes

Cryptographic is the secure communication of information even when third parties are around. For cryptographic is basically a mathematical algorithm build to secure a network and/or computers from potential Internet threats. When a company installs cryptographic tools to secure their network and computers they make it extremely hard for an average hacker from accessing the company's confidential information and damaging the company.

While these Internet security applications will help protect a company's network, computers, and confidential information, they cannot stop every attack so companies must also train their employees about potential Internet threats and how to be smart while on the Internet. For knowledge is the greatest asset for a company when dealing with Internet security and the safety of their networks, computers, and confidential information.

References

1. What is a Firewall? 2014. How Stuff Works.
Retrieved from www. computer. howstuffworks. com
2. What are Intrusion Prevention Systems? 2014. eHow.

Retrieved from www. ehow. com

3. Intrusion Prevention System. 2014. Wikipedia.

Retrieved from www. wikipedia. com

4. Intrusion Detection System. 2014. Wikipedia.

Retrieved from www. wikipedia. com

5. What is an Intrusion Detection System? 2014. eHow.

Retrieved from www. ehow. com

6. Access Control. 2014. Wikipedia.

Retrieved from www. wikipedia. com