Security product problem course work

Business, Company

Problem

A security product problem is anything that offers a potential room for attack against a system set up for a specific purpose or for private use. This may include virus, hackers, etc. The security product will attempt to check any flows in the domain that might make the system vulnerable to threats. Antleaks is a new product developed to act as firewall software for the domain that the company uses to offer after sales services to its customers. In its functions, the software detected several flows in the domain. This weakness included unauthorized access to the company’s classified files through mobile phones. The software also discovered that some employees were accessing private customer information. Cases of dishonest employees colluding with some individuals make false compensation claims. The system was prone to viruses because employees were downloading infected files from the internet.

This was an overly severe problem that led to adverse effects being felt by the company. This ranged from the loss of clients who were very offended by their confidentiality being accessed through simple operational devices such as mobile phones and other Bluetooth as well as simple wireless connectivity devices. Besides the loss of clients, the company also faced severe lawsuits that almost left it bankrupt, not only from the lawyers cuts but also through compensations to the clients. The company had to retaliate and act in accordance to the presented problem.

Requirements for the software that is to solve the problem

1. Software that manages to block wireless devices from accessing the information.

2. A defense mechanism that will prevent the events of possible hacking through jamming the devices of crashing their systems.

This will eventually manage to prevent people from daring to access the information.

3. A more strict security management strategy in the systems operation that will feature the blocking of wireless devices from infiltrating into the systems data.

4. A possible password protection policy implemented in the strategic operational aspects of the software that prevented access from wireless and directly connected hardware devices.

5. An expandable system that could successfully accommodate new clients into the company and yet assign them IP addresses and access into the system without risking data loss or unauthorized sources from accessing the data.

6. Maximum security protection for the information in the new system.

Response

The system responded to this security threats by enabling the system to filter every IP address and locate its source. This resulted in reduced cases employees changing their IP addresses and installing new software at will. Files from unknown sources could not be accessed from the company’s domain. Antleaks made it impossible for any individuals to access the company’s domain from the website. The software had to ensure that customers had to key in the product code as a requirement to gain entry into the company’s domain. This lessened to great extend the chances of some individuals forging compensation claims. Filtering of incoming and leaving traffic proved success. The fact that the system monitored every communication within and outside the domain limited employees from accessing any information except the under their custody.

The software jammed any wireless devices that attempted to access the information through unauthorized means. The software did not only act as a firewall that prevented access if the confidential information from outside sources but also acted as a form of protective mechanism that in some way managed to destroy the mobile phones, Bluetooth devices and Wi-Fi connected interfaces that attempted to access the companies’ information. Besides this, the response protocol instituted by the company also managed to gain back the clients’ confidence though it had to do this through practical demonstration of the convenience of this new software.

This new system, also managed to ensure that the information was solely accessed from the prescribed locations. The incompetence and maliciousness of some of the company employees was nabbed and automatically contained. The company also managed to expand the server capacity through the introduction of the new software, in that it could now serve more companies and add their IP addresses, incase new companies were added to the list of clients. This new software did not only manage to address the issue but also add an unbelievable number of clients.