MADHURI HIMA BINDU SATTURI

CIS515 IT INFRASTRUCTURE

Find a recent article (Within the past 4 months) of a company who has experienced a computer network threat summarize the type of threat, how it affected the company and what the company has done about the situation. How could this have been prevented?

Computer Network Threat:

Computer network threat refers to anything that causes harm to a computer system. These network threats could cause serious damage. When the computer systems, network etc. are affected, business are at great risk. Therefore businesses have to attend to these weaknesses. If their weakness is known to the attacker their systems can be easily affected.

Most businesses are investing in securing their networks from advanced malware. Almost every company allows the employees to work from home, by providing a company laptop, which the employee uses on the internet at home office to connect to the company's control network through a VPN. If a hacker has information he hack the laptop with Virus through the internet. This virus slowly propagates over the VPN connection into the control network and slowly infects the main control system. Therefore control networks are more vulnerable to cyber incidents.

Recent article (Within the past 4 months) of a company who has experienced a computer network threat:

Dyn Inc. (Dynamic Network Services Inc.) recently was affected by DDoS attack (Distributed Denial of Service). It is an attempt to make an online service unavailable by increasing the traffic through different resources.

Summary of the type of threat Dyn's Inc was affected:

In October, Dyn Inc., a New Hemisphere based company that offers a platform to optimize websites online performance, was attacked by DDoS (Distributed Denial of Service), which resulted in shutting down their website across the East coast.

According to research this attack was well planned and executed coming from ten millions IP addresses. Further research showed that attack was coming from devices such as DVRS, printers and appliances connected to the internet. It was also found that the attack was being waged from devices infected with a malware code that was released on the web in recent weeks.

How it affected the company:

Dyn Inc. was affected by DDoS attack around 7:00 AM Eastern time. Dyn's Network operations center determined quickly that the attack was different from their regular network Jam. After it was clear that it was attack it took them 2hours for their NOC (Network operations Team to mitigate the attack and restore services to customers. During this 2 hours internet users in the East coast who were directed to Dyn servers could not access the sites. But the users from the other parts of the country i.e. West Coast etc. could access the site.

Dyn Inc. experienced a second attack again in the afternoon of the same day. It was a sophisticated attack and highly distributed attack involving of millions of IP addresses. Based on the analysis from Flash point and Akamai, They said that one source of the traffic for the attack were devices affected by Mirai botnet. As they observed 10,s of millions of discrete IP addresses associated with the Mirai botnet that were part of the attack. The attack traffic reached as high as 1.2 Tbps.

As per reports, there was a third attack attempted, but the third attack wave was verified by DYN's Network operations center (NOC) and they were able to successfully mitigate it without customer impact.

Dyn's defense against the DDoS began with its automated response techniques. Their NOC (Network Operations Center) team once after understanding the magnitude of the attack. They used additional mitigation tactics. These techniques included traffic shaping incoming traffic, rebalancing the traffic by manipulation of any cast policies, applications of internal filtering and deployment of scrubbing services.

How could have Dyn's Inc. prevent this:

Dyn's Inc could have prevented by applying "Internet of Things (IOT) Trust framework". It is 31 principles designed to improve the security and privacy of connected devices. New York Times which was also attacked, easily got prevented by applying "Internet of Things (IOT) Trust framework"

The security experts mention that every business is exposed to a threat even with sophisticated security system, so there is nothing as 100 percent security. But definitely by updating the system with latest technology the Business can prevent themselves from different network threats.

References:

http://www.foxnews.com/tech/2016/10/21/major-disruptions-online-as-cyber-attack-hits-internet-services-company.html

http://dyn.com/blog/dyn-statement-on-10212016-ddos-attack/

http://searchsecurity.techtarget.com/news/450401962/Details-emerging-on-Dyn-DNS-DDoS-attack-Mirai-IoT-botnet