Cyber Attacks

Cyber security has been increasingly more important as of late. With technology becoming more prevalent in today’s world cyber security threats and solutions are on the rise as well. Tom Gaffney, IT specialist, said “Employees can now easily leak company data through the use of insecure public Wi-Fi . If employees do not use VPNs to encrypt their data, they run the risk of exposing their traffic to cybercriminals. This means that passwords and usernames can be seen and intercepted by others on the network. Although public WiFi hotspots are an invaluable services, there is a strong need for businesses to stay on top of the potential threats and security risks.” Gaffney showing us that cyber security is just as important as having access to wifi in today’s world.

Cyber attacks is an attempt by attackers or hackers to damage or destroy a computer network or system. Cyber security is the state of being protected against the criminal or unauthorized use of electronic data, or the measures taken to achieve this. Cyber attacks started making waves in the early 1900 with the first prominent one being the Magician and inventor Nevil Maskelyne. Maskelyne destroyed John Ambrose Fleming’s supposedly secure wireless telegraph technology, by sending insulting morse code messages through the the auditorium’s projector during the public demonstration. This attack proved current security standards had to be updated. A more recent attack happened in April of 2017, where a hacker group, named "The Dark Overlord", posted unreleased episodes of [Orange Is the New Black](https://en.wikipedia.org/wiki/Orange_Is_the_New_Black) TV series online after they failed to extort online entertainment company [Netflix](https://en.wikipedia.org/wiki/Netflix). This attack proved that cyber attacks have almost always have malicious intent behind them.

On July 22 of 2016, wikileaks published the documents from the 2016 Democratic National Committee email leak. The leaks were a breach of confidentiality and integrity. The information contained in the emails were meant to be private and not for the public. When it was released to the public it caused civil unrest across the nation. This is goes to show that information in the wrong hands can cause damage and breach confidentiality. Also the integrity of the people and information were also put into question. Since unauthorized personnel accessed the information, who’s to say whether the information has been altered? This cyber attack and leak showed how the security of a personal email account is very important and some times all the measures put in place are not enough or lacking because there can be unforeseen entries/holes in a cyber security system.

Leon Panetta former defense secretary once stated, “cyber attack perpetrated by nation states or violent extremists groups could be as destructive as the terrorist attack on 9/11”. In June of 2015 “the records of 21.5 million people, including social security numbers, dates of birth, addresses, fingerprints, and security-clearance-related information, were stolen from the United States Office of Personnel Management. Most of the victims are employees of the United States government along with unsuccessful applicants as well.” At the time of the attack, The Wall Street Journal and the Washington Post reported that government sources believed the hacker was done on behalf of the Chinese government. This proves that cyber attacks were not only performed by activist groups or criminals but sometimes it was governments around the world doing it to acquire sensitive information and spy on other nations as well. This last example is a cyber attack perpetuated for the benefit of a criminal organization. In September of 2016 where, “a hacker named Ardit Ferizi was sentenced to 20 years in prison after being arrested for hacking U.S. servers and passing the leaked information to members of ISIL terrorist group back in 2015.” This was a big case because it gave major sentencing out to criminal. It also served as a warning, if you were caught in any cyber related crimes you were going to be punished for it. The attack breached confidentiality and integrity of the service agents their personal information were acquired. This breach endangered the lives of the families related to the victims.

All the above attacks could have been avoided if measures and counter measures are put in place before to mitigate the vulnerability in the system or address the threat this can achieved with control. Control is a way to prevent harm from happening, or reduce it's impact if it does happen. This can be done by either neutralizing or discouraging the threat, or by fixing or minimizing the vulnerability. The following counter measures can reduce cyber attacks; Education, employees of an organization must be aware of the kinds of attacks that can occur and what they can do to prevent them. This includes learning proper operating procedures, the key attack targets (like passwords), and the classic attack methods. Some studies have shown education to be more effective than any other countermeasure for protecting information systems since knowledge of information-systems security is not a requirement for most jobs.

Automated access controls are important for cyberspace (Pfleeger & Pfleeger, 2002). Access controls for computers are generally managed by passwords that must be supplied to log on and use resources. Controls can be set for individuals or for groups of people, and they can be applied separately to reading, writing, execution of resources, the ability to extend those privileges to other users. Access controls for networks are enforced by "firewalls". Firewalls are dedicated computers on a local-area network that restrict traffic to and from the network according to simple rules on such features as origin and communications protocol. Unfortunately, access controls are vulnerable to many attacks, and will not generally protect against attacks by insiders like staff. Also, encryption hides data in a form that cannot easily be read; you then supply a character-string "key" to decode it when you need it (Pfleeger & Pfleeger, 2002). Any attempts to modify encrypted data will result in indecipherability, so you can tell if encrypted messages or programs have been modified (or repeated, if a time is included in the message). Strong and virtually unbreakable methods of encryption have been developed recently with "public-key cryptography", and software for it is available for free download from a number of Web sites. Encryption methods can also be used for "authentication" or to provide digital "signatures" on documents to prove who wrote them and when. Encryption has been touted as a solution to many security problems, but is overrated. If an attacker gains system-administrator privileges, they may be able to get keys or disable encryption methods without your knowledge. The other countermeasure such as; back tracing, legal response, intrusion prevention systems, back ups etc.

In closing, cyber attacks can not be a hundred percent avoided but there can be some measures taken to counter the issue and reduce the harm they cause.

Bibliography

Balkhi, S. (2014, May 11). 25 Biggest Cyber Attacks In History. Retrieved July 02, 2017, from <http://list25.com/25-biggest-cyber-attacks-in-history/>

Introduction Cyber Attacks. (n.d.). Retrieved July 02, 2017, from <http://faculty.nps.edu/ncrowe/edg_attacks.htm>

Pfleeger, C. P., Pfleeger, S. L., & Margulies, J. (2015). Security in computing. Upper Saddle River, NJ: Prentice Hall.

Review, N. (n.d.). The history of cyber attacks - a timeline. Retrieved July 02, 2017, from <http://www.nato.int/docu/review/2013/Cyber/timeline/EN/index.htm>

Tom Gaffney. (n.d.). Retrieved July 02, 2017, from <http://www.goodreads.com/author/show/15145072.Tom_Gaffney>