Ioannis Haviaras

ISACA Philadelphia

Scholarship Essay

03 April 2017

Cyber Attacks in Today's Digital World

Currently, in 2017, an estimated 28.4 billion devices are connected to the internet ("IoT"). By 2020, MorganStanley believes that number could rise to an estimated 75 billion ("Danova"). As transistors inside processors become smaller, and more powerful, mobile and IoT devices have become a target for numerous cyber-attackers. These devices, unbeknownst to the user, can be used to perform major DDoS attacks across the world similar to the one that took down a large portion of the internet in October 2016. Though, the motivation of this attack was unknown, various attackers, such as nation states, attack extremely sensitive information for use against other nation states. In order for cyber-attackers to obtain access to information systems, attackers use phishing as a technique to install malware on a victim's machine. To protect organizations and ultimately citizens, government agencies have put in place regulations to combat these cyber-attacks. Most recently in New York State, Governor Andrew Cuomo announced a first of its kind in the nation regulation titled, "Cybersecurity Requirements for Financial Services Companies." These regulations were designed to promote safety of customer information as well as the information technology systems of regulated entities ("Vullo"). The regulations presented by Cuomo, are not meant to be overly restrictive, allowing organizations to keep pace with emerging technological advances. With smart watches, thermostats, smoke alarms, light bulbs and even baby cameras being connected to the internet, IoT device security

needs to be held at a higher standard on the manufacturer's end. This in turn, will enable consumers to be more cognizant of their security online.

From nation states to cyber terrorist organizations, cyber attackers are utilizing more sophisticated methods than ever before to gain access to vulnerable systems. While the motivation between different cyber criminals may vary, the goal of obtaining access to sensitive information is unanimous. Many cyber criminals use phishing scams as a personalized avenue for a victim to infect their system. For example, a phishing scheme could send a victim to a replica of the Discover Card website, if the victim were to sign-in using their credentials, this could be used to ultimately obtain their credit card number. When a cyber-criminal obtains credit card information, more often than not, it is sold on dark web markets for a price; in this instance, the criminal's motivation is profit ("Know"). However, profit is not always a motive for attackers. Many attackers, such as nation states, have different motivations when it comes to cyber espionage. In Kiev, Ukraine a group of Russian hackers took down parts of the power grid, which was performed by sending malware to employees to steal login credentials ("Condliffe"). In this attack, it was clear that sabotage of an international entity involved in conflict with the Russian Federation was the main motivational factor. Some attackers, however, do not have a motivational factor when performing an attack. Such was the case in a major DDoS attack that occurred on October 21, 2016, which targeted IoT devices such as DVR players and webcams. These devices, which were infected with the Mirai botnet, involved over 100,000 endpoints and attacked with a strength of 1.2Tbps ("Woolf"). By utilizing IoT devices, cyber-attackers were able to attack a major portion of the internet, the largest of its kind in history.

By setting regulations for corporations and other entities, government agencies can attempt to safeguard its citizens against future attacks. A first of its kind in the nation regulation

titled, “Cybersecurity Requirements for Financial Services Companies,” was put in place in New York State on March 1, 2017. Several sections of this regulation play a vital role in protecting consumers and the privacy of their data. The regulation requires that a Cybersecurity Program and Policy be put in place to asses both internal and external risk associated in the organization. With these policies in place, the regulation also requires that a Chief Information Security Officer (CISO) be hired to enforce and advise senior officials on these policies (“Vullo”). The regulation also requires that the organization, in cooperation with the CISO, perform bi-annual vulnerability assessments as well as annual Penetration Testing. Other than performing these assessments, organizations under this regulation need to make sure their access privileges and application security are assessed periodically. A major requirement of this regulation also includes encrypting non-public data that is not readily available. The most important section of this regulation, I believe, is the requirement to notify a designated superintendent of an incident within 72 hours (“Vullo”). This prevents companies from hiding cybersecurity events from the public which occurs quite often due to consequences to the company’s reputation. This first-of-a-kind regulation is a step forward in protecting citizens and keeping them aware in the event of a major cyber-attack, that could not only compromise their financial well-being, but also the critical infrastructure of the nation.

With IoT devices becoming more common in today’s digital world, manufacturers need to focus on securing these products, starting from the assembly line. In order for these manufacturers to implement security into the production line, basic security concepts need to implemented, such as separating data and code, protecting data when not in use, and authenticating users through trusted parties. Since products will only get more powerful, the manufacturer can prevent security issues by future-proofing their hardware from the start. Since

many IoT devices require an initial setup when purchased, manufacturers should put rules in place to prevent default passwords from being accepted as well as silently pushing updates ("Rosenquist"). By performing these initial steps in the manufacturing process, manufacturers can combat the security risks their devices are susceptible to. However, manufacturers are not the only entity responsible in keeping the world safer online. Ultimately, the consumer is the only one that has the ability to keep themselves safe. By educating consumers across the world to practice online safety, such as using unique passwords for every login and making sure 2FA is enabled, can go a long way not only protecting the internet now, but also in the future.

Works Cited

Condliffe, Jamie. "Ukraine has its military and power grid hacked (again), and signs point to Russia." *MIT Technology Review*. MIT Technology Review, 22 Dec. 2016. Web. 29 Mar. 2017. < https://goo.gl/xSibAU>.

Danova, Tony. "Morgan Stanley: 75 Billion Devices Will Be Connected To The Internet Of Things By 2020." *Business Insider*. Business Insider, 02 Oct. 2013. Web. 29 Mar. 2017. < https://goo.gl/dlfpd3>.

"IoT: number of connected devices worldwide 2012-2020." *Statista*. N.p., n.d. Web. 29 Mar. 2017. < https://goo.gl/H9pEic>.

"Know Your Enemy: Understanding the Motivation Behind Cyberattacks." *Security Intelligence*. N.p., 13 Sept. 2016. Web. 29 Mar. 2017. < https://goo.gl/fPVsfG>.

Rosenquist, Matthew L. "How to Secure the Future of IoT." *Intel® Software*. Intel, 18 Nov. 2016. Web. 29 Mar. 2017. < https://goo.gl/o9kSmn>.

Vullo, Maria. "Cyber Security Requirements for Financial Service Companies." *Department of Financial Services*. New York State, 01 Mar. 2017. Web. 29 Mar. 2017. < https://goo.gl/NzGgwa>.

Woolf, Nicky. "DDoS attack that disrupted internet was largest of its kind in history, experts say." *The Guardian*. Guardian News and Media, 26 Oct. 2016. Web. 29 Mar. 2017. <https://goo.gl/MHqKKX>.