Improved information sharing for cyber threats

Abstract

This paper discusses the need for improved information sharing amongst industries for the continued prevention of cyber threats and improved threat intelligence. This will specifically focus on government, financial and healthcare sectors. Cyber attacks can happen to individuals, government, hospitals and banks. Hackers are always looking for PII (Personally Identifiable Information) and other valuable information to exploit for profit. Within this paper the writer will discuss the importance of sharing cyber threats and vulnerabilities and the need for improved information sharing between theses sectors to diminish these threats. Cyber threats known in one sector may not be known in another. The writer proposes improvements to current rules and laws and the introduction of an information sharing ‘ hub’ for these sectors.

Keywords : threat intelligence, cyber-attacks, cyber threats, PII, information sharing ‘ hub’, information sharing, vulnerabilities

Improved Information Sharing for Cyber Threats

Cyber-attacks happen every day and in every aspect of life from cell phones, personal computers, banks, government, hospitals and places of work. According to Zimski (2011) “ The threat landscape has evolved. It’s no longer just the disgruntled employee or even the opportunistic hacker with which organizations need to be concerned. Highly sophisticated and targeted attacks are on the rise.” (Zimski, 2011). When a cyber threat is identified, the appropriate action is then taken, and a solution is remedied. These solutions need to be shared with other industries and businesses to protect them as one against a common enemy. For example, an attack or threat that is thwarted at one institution may not be known at another. This is the reason that there is a need for a central, secure information sharing ‘ hub’ for cyber threats that have been previously stopped and recorded.

The purpose of this paper is to discuss current cyber threats and how these different sectors are defending against them. It will delve into threat intelligence (TI) and how this evidence-based knowledge can lead to better decisions among the cyber security team. The writer will discuss the importance of sharing information on cyber threats and why it is important in the protection of the infrastructure of these sectors (government, financial, healthcare). Next, the writer will discuss some rules and regulations that are already in place for sharing between these sectors and propose a solution to improve on these. The writer will explore if these sectors are doing enough to share information against a common cyber threat and suggest areas in which they can improve. The writer will analyze the benefits for a central information sharing ‘ hub’ to defend against known cyber threats. The writer will explore if this ‘ hub’ can be financially feasible and mutually beneficial to everyone that will use it. Lastly, the writer will summarize the main points of the paper, including strengths, weaknesses, and constraints regarding policy writing of existing rules and regulations.

Literature Review

During the writer’s research, the writer has come across many articles that elaborate on today’s ever-changing cyber threat landscape. Most companies and institutions are not financially equipped or technically aware to defend against a cyber-attack that will compromise their classified information. According to Tounsi & Rais (2018), a cyber security scientist and a senior in charge of security services, “ Organizations need to gather and share real-time cyber threat information and to transform it to threat intelligence in order to prevent attacks or at least execute timely disaster recovery.” (Tounsi & Rais, 2018). Cyber attacks will never stop and the need to improve on sharing information on how to stop these threats are important to everyone.

Current Threats and Defense

The biggest threat hospitals have today is losing protected health information (PHI) of their patients. There are many ways for hackers to attempt to gain access to this information. One of the most popular ways to get information is phishing. This is a common practice of hackers to obtain a user’s computer credentials through manipulation. An example would be impersonating someone of importance to disclose pertinent information. According to Rekouche (2011), “ This early scheme was the basis for the automated tools that would be developed in the following year. One of us named it “ fishing,” the term that I later used in AOHell along with a change of spelling to “ phishing.” (Rekouche, 2011). “ Although organizations are required to announce breaches of protected health information (PHI), not all phishing attacks lead to disclosures of PHI, nor are all investigated.” (Wright, Aaron, & Bates, 2016). This is common practice amongst all types of institutions. If important information about the company or individuals is not lost in a cyber-attack, they usually do not get reported. Since 2014, Wright, Aaron & Bates (2016) “ identified at least ten incidents since 2014 where hackers gained unauthorized access to hospital systems through phishing in the United States, including two separate attacks against our organization.” (Wright, Aaron, & Bates, 2016). These breaches were in eight different states and were successful in gaining access to patient demographic information through phishing alone. This included names, birth dates, Social Security numbers and some diagnosis of individual patients.

Cyber security is just as important for financial institutions as it is for hospitals. According to Choo (2011), “ It is widely accepted that the financial and insurance industry is the ‘ target of choice’ for financially motivated cyber criminals.” (Choo, 2011). Unlike hospitals, in which phishing is the cyber attack method of choice, hackers of financial institutions will employ malware, spyware, phishing, social engineering and back doors. Malware is basically software that is designed by a hacker (or disgruntled employee), to gain unauthorized access to a system or computer. Spyware allows a hacker to obtain information about another user’s computer activity through deceptive or covert actions. Social engineering encompasses a broad range of activities revolving around human interactions. The ability to trick or manipulate a user into making a mistake or giving away sensitive information. Back doors refer to accessing a computer system by bypassing the usual security mechanisms. One noteworthy attack happened in 2012, “ A massive financial cyber-heist dubbed ‘ Operation High Roller’ was launched from servers in Russia, Albania and China. The attack caused significant damage to the global banking system including between $78 million and $2. 5 billion in losses from bank accounts across Europe, the US, and Latin America.” (Watkins, 2014). The threat of losing sensitive information, damage to critical sectors of the institution and financial loss makes cybersecurity a very important priority for everyone. For every threat defended against, a new one emerges that has to be prepared for.

Another sector not immune to cyberattacks is the government. This would encompass all types of government. Local, federal as well as legislative and judicial sectors are equally affected by financially motivated individuals. The city of Atlanta in 2017, was the victim of a ransomware attack in which hackers demanded bitcoin payment in return for a key to regain access to their systems. In 2018, Leeds, Alabama also experienced a ransomware attack in which hackers took control of the city’s computers. The Colorado Department of Transportation suffered two attacks within a week in 2018. Hackers renamed encrypted files and requested bitcoin to return control of their systems. They also requested bitcoin payment. In November of 2018 Russian hackers impersonating U. S. State Department officials attempted to gain unauthorized access to military, law enforcement and defense computer systems. According to Judge Dixon (2018), “ In 2017, over 7. 8 billion records were hacked from the numerous cyberattacks that occurred during the year. That computes to slightly more than one record per person in the world considering that the estimated world population at the end of 2017 was 7. 6 billion people.” (Dixon, 2018). These numbers alone should put fear into governmental institutions and the need for informational sharing to better defend against cyber threats. Imagine the attacks that are successful and don’t get reported.

The writer could not possibly list the multitude of successful breaches on hospitals, banks and governments, but recommendations can still be made on how to proceed and how they are currently being defended against. So how can these different sectors better defend against a cyber-attack and future cyber threats? All need to implement training on how to recognize different threats. Using different types of filtering, encryption, and detection to lessen exposure in case of a successful breach. The writer would also use a two-factor authentication system. This would employ an extra step in identifying a user. A good example of this is a biometric (retinal or fingerprint scan). This makes things more difficult for a hacker. So, if a hacker gains access to a password, access to an account would be impossible without being able to access the second factor.

Heading 3

Above is where you have your third heading, in bold and centered. The first line again is indented one tab. You may have many more headings that help to separate sections of your paper/project, but the will all follow this basic format.

Conclusion

Above is where you have your conclusion heading, in bold and centered. This is where you wrap up your paper, highlighting key findings, points, etc.

References

- Choo, K. K. R. (2011). Cyber threat landscape faced by financial and insurance industry. *Trends and issues in crime and criminal justice* , (408), 1.

- Dixon Jr, H. B. (2018). Cyberattacks on Courts and Other Government Institutions. *The Judges' Journal* , *57* (3), 37-39.
- Rekouche, K. (2011). Early phishing. *arXiv preprint arXiv: 1106. 4692* .
- Tounsi, W., & Rais, H. (2018). A survey on technical threat intelligence in the age of sophisticated cyber-attacks. *Computers & Security, 72* , 212-233. doi: 10. 1016/j. cose. 2017. 09. 001
- Watkins, B. (2014). The impact of cyber-attacks on the private sector. *no. August* , 1-11.
- Wright, A., Aaron, S., & Bates, D. W. (2016). The Big Phish: Cyberattacks Against U. S. Healthcare Systems. *Journal of General Internal Medicine, 31* (10), 1115-1118. doi: 10. 1007/s11606-016-3741-z
- Zimski, P. (2011). Navigating the new threat landscape. *Computer Fraud & Security, 2011* (5), 5-8. doi: 10. 1016/S1361-3723(11)70049-5
- American Association of Community Colleges (AACC). (2014). 2014 fact sheet. Retrieved from http://www. aacc. nche. edu/AboutCC/Documents/Facts14_Data_R3. pdf
- Brown, J. C. (2007). Full- and part-time employee stress and job satisfaction at two upstate New York colleges. *Dissertation Abstracts International* , 68 (08), (UMI No. 3277201)
- Creswell, J. W. (2005). *Educational research: Planning, conducting, and evaluating quantitative and qualitative research* . Upper Saddle River, NJ: Pearson.

Above I have inserted some sample references. Notice the formatting and that lines 2 and beyond are always indented. Your References page is always its own page. Please remember to take the time to carefully review the properly formatted samples in our online classroom. In addition, please see both the APA itself, and the samples for additional guidance on the proper formatting of your References page, and each individual reference. The References page must be its own page. Remember that all in APA is Times New Roman, 12 point font, and double-spaced throughout on an APA References page and alphabetical order from A-Z, with the second and third lines etc indented underneath the first line. Please see the APA itself and/or theUC Library’s APA LibGuide available from the citation’s link from the College Library’s main webpage.