Analytics in Big Data

CIS 4640

2015-09-29

Assignment 1

# What is Information Security?

Information security, or InfoSec, is the practice of protecting information from unauthorized user, disclosure, disruption, modification or destruction (Aggarwal & Chaturvedi, 2013). This includes all data regardless of type. This paper will pertain mainly to information security of information technology (IT) data. This data can include database systems, sensitive files on personal workspaces, website security such as secure socket layer protection, big data, and much more.

Analytics in the field of information security provides threat intelligence, in a timely fashion before, during, and after a security breach (Tarzey, 2014). Tarzey gives some great examples of security analytics during an attack includes:

* Identifying unusual traffic between servers, which can be a characteristic of undetected malware;
* Matching data egress from a device with access records from a suspicious IP address, user or location;
* Preventing non-compliant movement of data (which may be simply down to an employee being ignorant of the rules);
* Linking IT security events with physical security systems (for example, maintenance of plant infrastructure restricted to certain employees known to be on the premises);
* Identifying unusual access routes, (for example some databases are only normally accessed via certain applications and not directly by users)

# Why is analytics important in InfoSec?

According to Aggarwal & Chaturvedi, the idea of analytics in information security is to identify vulnerabilities before the vulnerabilities are taken advantage of maliciously, providing threat intelligence (p. 11). Analyzing systems is important to help preventing incidents in IT security from happening in the first place. Unfortunately this is not always the case. Incidents happen regardless of how careful businesses are. When these incidents occur, it is important to analyze how and why it happened to prevent the same incident from happening again in the future. A good example where information security analytics is used is in big data. Due to the large and complex nature of big data, normal surety devices such as firewall, anti-virus, VPN, IDS and Security auditing have been deemed ineffective when reviewing Big Data infrastructures (Boukri & Chaoui, 2015).

Analytics in information security is becoming more and more important with the birth of a fairly new type of hacker. The hacker that is simply bringing corporations down for moral reasons. A more recent case of this happened in July 2015 by a group called “The Impact Team” (Thomsen, 2015). The group felt Ashley Madison, a website which enables extramarital affairs, was immoral and threatened to release user information if the website was not immediately shut down. The company did not agree to their terms resulting in the release of around 37 million account information including name, address, transaction history, and search history.

# How do companies use analytics in Information Security?

## Who, What, & When

Between the dates of April 17 and April 19, 2011, Sony Entertainment was hacked (PlayStation Network Restoration Begins, 2011). This in turned forced Sony to turn off the PlayStation Network on April 20. It was on May 4, that Sony confirmed that personally identifiable information from each of the 77 million accounts may have been exposed resulting in one of the largest data breaches in history (Chung, 2011).

## Analytics of the Situation

Sony had to perform analytics on the situation for multiple reasons: they needed to find out how it happened, how they can prevent it in the future, and what was affected. Through analysis, it was found that data containing name, address, country, email, birthdate, username, password, billing history, password security answers (Chung, 2011). Here lies the issue at hand, aside from the credit card information, essentially all information pertaining to a user has been exposed. If it was not bad enough that these hackers, known as Anonymous, had all of this data, they went ahead and released it to the public. Sony never actually released the source of the breach to the public.

This information being release to the public is where the real issue lies. Anyone with a little bit of technical knowhow was able to access this information by use of a torrent service called The Pirate Bay. Most people do not take password differentiation seriously and use the same password for everything. With that in mind, having a person’s email address and a password they used on another site would allow you to access their email account. For example, if I saw an email address, john.example@gmail.com, and their password was, 123sample, I would then be able to access their Google account. With access to this, I could then see what kind of sites they frequent, for this example, say I noticed an email from their bank in their inbox. I now can go to their bank’s website, and given our assumption that they use the same password for all accounts, not have access to their bank account, which on most bank sites provide bank statements with account and routing numbers. The release of this information affected a lot more than just PlayStation Network accounts.

# Conclusion

According to Verizon, 85% of attacks on IT infrastructures happen within hours. 66% of successful attacks were not discovered for months or more (2013 data breach investigations report, 2013, p. 50-52). One reason these attacks are so hard to detect is due to speed at which they occur.

Between the Sony and Ashley Madison hack, more than 100 million users were exposed. It is possible that with proper information security analytics, the companies could have been aware of the vulnerability before it was utilized. Even if the hacks were due to human error of leaving a password on a desk, conducting an analysis of which employees were aware of security standard would have caught that. Analytics during the breach could have told them there was unusual activity occurring in their servers, allowing the companies to act. For all they knew, the hackers had been in their systems for months, waiting for an opportune moment to strike.

The issue is that many companies feel they are immune to attacks. I work for a marketing company which stores personal information about customers who respond to a mailer we send out. I have brought up many times how insecure our facilities are and how lax our security standards for employees are. My boss will reply most of the time with, “why would anyone want to hack us, we don’t store anything of value.” What he fails to see is that does not matter anymore. Simply paying for the service to provide us with information when/if we get distributed denial of service attacked would be useful beyond comprehension. The company sends leads from these mailers via email. If we were to experience a DDOS attack, we would be out of business until we contacted our dedicated server provider to shut down our server. That could be days. Which is plenty of time to lose many clients.

Security analytics are far from the point where we receive real-time intelligence of vulnerabilities. That would be an ideal world to live in, but the fact of the matter is, having none is foolish. Information security analytics has become part of the game of allowing availability of data all the time in the cloud. It is a necessity.

# References

Aggarwal, P., & Chaturvedi, M. (2013). Application of Data Mining Techniques for Information

Security in a Cloud: A Survey. International Journal of Computer Applications IJCA, 11-17.

Tarzey, B. (2014, March 1). IT security analytics: The before, during and after. Retrieved

September 30, 2015, from http://www.computerweekly.com/feature/IT-security-analytics-the-before-during-and-after

Boukri, K., & Chaoui, H. (2015). Security Analytics in Big Data Infrastructures. International

Journal of Computer Science and Information Security, 13(5), 91-95.

2013 data breach investigations report [electronic resource]. (2013). New York, NY: Verizon

Business.

Thomsen, S. (2015, July 20). Extramarital affair website Ashley Madison has been hacked and

attackers are threatening to leak data online. Retrieved September 29, 2015, from http://www.businessinsider.com/cheating-affair-website-ashley-madison-hacked-user-

data-leaked-2015-7

Chung, E. (2011, April 27). PlayStation data breach deemed in 'top 5 ever' - Technology &

Science - CBC News. Retrieved September 29, 2015, from http://www.cbc.ca/news/technology/playstation-data-breach-deemed-in-top-5-ever-1.1059548