Mohanad Horani

Final Project

Incident Response

University of Advancing Technology

Final Project

My company that I own is a gaming company called “GamersGeeks”. GamersGeeks is a company that has not an experienced a ton of incidents in terms of breaches and hacks in quite a while. In fact, GamersGeeks is known for mitigating incidents rapidly and having an outstanding incident response record. In most cases, it only takes GamersGeeks about 1 hour to mitigate almost any incident no matter how large the size. Even for the largest incidents, it only takes GamersGeeks approximately one to two days before fixing the incident. Some examples of attacks and breaches GamersGeeks have been able to resolve includes threats, malware, and physical incidents that occur on site of the company. Others include scams, hacks, and ransomware. Those are just some of the incidents that our gaming company has had to deal with. Overall, GamersGeeks is performing an action called “wargaming an incident” which in other words means preparing for possible scenarios and outcomes for any incident no matter what type and preparing for defensive measures against such an attack. Wargaming an incident (such as malware or any other incident) does not only involve anticipation and rehearsing, but also involves meetings/discussions (Drage, 2020).

One example of a major incident that GamersGeeks has had to unfortunately wargame for (i.e. anticipate & rehearse) includes malware which is extremely common for gamers to encounter across the globe. Almost every day, GamersGeeks has had to deal with at least one if not two malware incidents to mitigate and resolve. Unfortuantely, not too long ago, one of the incidents that GamersGeek mitigated had to do with a malware attack involving an advanced trojan horse attack. Now although my company wargamed against malware attacks in the past, we indeed committed the grave mistake of thinking that we never had to worry against a trojan

horse attack like the one we had encountered since we already had the latest Norton Antivirus upgraded on all of our employees' computers in the workroom.

I would like to first explain how the trojan horse affected our gaming company before going into further detail. Although trojan horses are a form of malware, they are quite different from both computer viruses and worms (Comodo, 2018). Unlike computer viruses, trojan horses are not able to replicate inside of a computer (Comodo, 2018). Now what happened recently was that one of our employees received a file that looked exactly like it was sent from our chief executive employee that works at GamersGeeks. At first, we did not recognize that a trojan has been sent, so our employees opened the file regardless. Unfortunately, we had to learn the hard way not to trust every file being sent (i.e. even if it appeared to be real). The trojan then infected about half of our employees' computers and we had to reset them as a result.

There are multiple steps that our employees could have taken to prevent such a malware breach. First of all, we did not utilize a firewall which could have helped with blocking unimportant connections including trojans and other forms of malware (Comodo, 2018). Also, one of the most important steps that we did not take to prevent such an incident from ever occurring included almost always trusting email attachments and links especially if they seemed/appeared to be real (Comodo, 2018). Also, we could have also trained our employees on how to access only websites do not look suspicious and not to trust every website/email that they see (Comodo, 2018). Although we had an antivirus, antiviruses alone are not ideal enough to prevent such an attack from occurring even if they have the latest update (Comodo, 2018). Overall, GamersGeeks employees did not take preventive measures against such a large attack which costed tons of money and time to repair. Lastly, this is one of the biggest mistakes that our company has had in about 2-3 years.

There is one incident however that GamersGeeks had the chance to handle recently due to recent wargaming which is a recent phishing attack. In fact, the phishing attack that our company dealt with included a phone call that was designed to be a fraud in terms of demanding personal information about some of our hard-working employees that are working on a secret gaming project. On top of that, the hacker that was talking to one of our employees over the phone demanded a certain amount of money. This type of phishing attack is also known as "vishing" or voice phishing (University of Michigan, n.d.).

Thankfully, our company's employees detected this phishing attack from the very start and spotted some of the warning signs of a voice phishing attack as well. Some of the signs as mentioned earlier included demanding a certain amount of money, threats over the phone, and not professional words/tone (University of Michigan, n.d.). Not only did we hang up as soon as we noticed that this call was a total scam, but we also reported the call online to the correct authorities as part of our incident response process (University of Michigan, n.d.). Overall, this was all thanks to wargaming the incident beforehand and preparing for such an incident.

Overall, wargaming incidents that are common are crucial, but sometimes even wargaming the most unexpected incidents is also just as essential. One benefit of wargaming the unexpected incidents includes being prepared for the most unexpected incidents that occur in the world of incident response (Drage, 2020). The best time of wargaming is not only anticipating and rehearsing for an incident, but it is also actively engaging in the process of learning as well as utilizing critical thinking skills (Drage, 2020). Overall, wargaming an incident at any business or company is a skillset that is required for better incident response management.

My gaming company (GamersGeeks) has had many incidents that were both either wargamed for not prepared/rehearsed for as much as they should have been. All in all, one

example of an incident that involved wargaming and one that clearly did not involve wargaming was written in this paper. One question to ponder is the following: Without wargaming, how can one be powerful in terms of incident response?

References

Comodo. (2018, June 5). *What is a Trojan horse virus?* Comodo Enterprise. https://enterprise.comodo.com/forensic-analysis/what-is-a-trojan-horse-virus.php

Drage, N. (2020, July 1). *How to train for your next security crisis: Let the wargames begin*. TechBeacon. https://techbeacon.com/security/how-train-your-next-security-crisis-let-wargames-begin

University of Michigan. (n.d.). *Phone scams and voice phishing (Vishing) / safecomputing.umich.edu*. U-M Safe Computing / safecomputing.umich.edu. https://safecomputing.umich.edu/be-aware/phone-scams