Final Project

Allan Wheelock

University of Advancing Technology

Author Note

This paper was prepared for NTS 405 Incident Response, taught by Michael Velasquez.

Final Project

Using all of the skills and tools I have acquired throughout the duration of this course, to produce an incident report as if I was apart of a security team for a company that had been hit with some sort of attack.

# Scenario

The scenario for this incident report is a company that does medical insurance gets hit with an attack. The company is called Insuracare. The attack Insuracare was hit with is a malware attack. The attack came from an email that someone opened and released a virus into the network of the company. There has been a report generated by the security team involving all of the specifics of the attack and how it started in order to make sure everyone is on the same page of their response.

# Potential Events that Could Occur

Some potential events that could occur due to this attack is mainly data being stolen. Due to this being a medical company that is a huge HIPAA violation. Any medical records or personal identifiable information that gets stolen could cause a lot of legal trouble for Insuracare. If the threat isn’t neutralized relatively quickly the company would suffer mass data loss.

# How I Would Respond

The first step I would take in response to this threat is trying to identify some indicators of compromise. This would be identifying the specific email that the malware attack was in. Once we found the email that it originally came from I would begin analyzing that email to find some clear indicators of compromise in order to identify other emails that might contain more attacks, which would increase the speed of this attack against Insuracare.

Once we have a solid list of indicators of compromise for the emails I would make sure to notify everyone in the company of these specific indicators of compromise. That way we would have the whole company aware of the attack so that they would be able to report it if they saw anything suspicious. It is important to spread awareness of an attack like this so that it doesn’t have the ability to spread as easy. Ideally if everyone knows what to look for they won’t continue to spread the malware around the company.

Once everyone is aware of the attack and has the tools to report it and stop the spread of the malware, the security team needs to work on a plan of attack to rid the network of the threat. This is a process that will likely take some extra planning. I believe that it’s better to take the little bit of extra time to make sure the plan is effective before just jumping in there and trying to get rid of the threat. That way you can make sure that it is actually all the way gone before you decide to stop trying to get rid of it. It’s more common than I originally thought for a company to think they rid their network of a threat only to realize they missed a spot.

After the security has developed a plan that we feel will be the most effective way to rid the network of this threat, we will begin to work on it. If the malware is trying to steal information about our patients and their records, the place I would recommend starting to look for data loss would be the servers that house all of this data. Hopefully no data is stolen but that is unfortunately an unlikely outcome of this type of attack. By the time it gets discovered and there is a plan in place, some data is likely to have been stolen.

There are likely to be more than one server infected, as well as some regular machines that the emails were originally opened on. The best way I can think of to handle the attack from here would be to take those machines off the network, and then if possible without creating massive downtime, do the same with the servers. This way you could isolate the threat and back that virus into a corner so you could fully get it off the network.

Once these machines are off the network and the virus has been eradicated, I would want to run scans on all of these machines and servers before putting them back on the network and into production. That way we could make sure that we didn’t miss anything. One additional thing we could do if necessary is to restore the device or server from backup to a time before the attack happened. I believe that would get rid of any remains of the virus.

Insuracare should be able to go back to business as usual after everything has been checked for the virus and is ready to go back on the network.

# Conclusion

In conclusion, every incident will need to be handled differently, and this is just an example of a basic malware attack. I don’t think this was an overly complicated scenario however there are some important steps that I believe would make this an effective response. One of the biggest of those being the scans and checks done to all of the infected machines before bringing them back on the network. Doing a check like this to ensure no one missed anything from the attacker is an effective way to make sure that everything is safe to go back to business as usual. Another step that I think would make this a successful response is the removal of these devices from the network, ensuring that we cut communications between infected devices and safe devices.

Overall, I think this would be an effective way to respond to this type of incident. If the security team followed these steps I firmly believe they would be able to remove the threat from the network.

References

Synchronic.uat.edu. 2021. *Sign In*. [online] Available at: <https://synchronic.uat.edu/courses/4162/assignments/148464?module\_item\_id=377594> [Accessed 9 August 2021].