CYB 320 Project One

Douglas Few

June 11th, 2022

Assets

At first glance, it may seem like the described incident has only affected one workstation in the Financial department. However, upon closer inspection, it’s clear that there is more at play here. The financial records that were being held on the workstation have also been compromised, which brings into question the integrity of said files at this stage. It is also currently unknown whether this incident has spread across the network to other departments, so it should be assumed that the network as a whole is currently compromised until we can safely and definitely rule out that possibility.

Contain

The first step I would take to contain the incident is to immediately remove the workstation from the network. While we are still unsure whether the ransomware virus spread to any other workstations or any other departments across the network, the quickest way to stop it from spreading any further is to remove the source workstation from the network as soon as possible. If we do so quickly, we may find ourselves lucky enough to have stopped it before it was able to spread at all. From there, we should scan the network in an attempt to identify if a spread did in fact take place. If we discover that the ransomware made it to other workstations or departments, the best course of action may be to take the entire network offline while we work to remedy the issue.

Remediation

Immediate remediation of the ransomware issue may look something like removing the workstation from the network and performing anti-malware procedures. If the monthly backup was recent enough that data won’t end up being reverted back too far, then recovering the workstation from the backup may be the simplest and quickest solution to the problem. Since we don’t know at this time whether the ransomware spread out of the financial department, however, we will have to scan the network to see if any malicious traffic has been detected. Using a network intrusion detection system (NIDS), a security practitioner can analyze network traffic to identify if and when malicious intrusions were detected on a network (N-able, 2021). If the network is equipped with an anomaly based detection system, the NIDS will automatically detect any unusual or out of the ordinary traffic on the network. The security practitioner can then track the unusual traffic to see where it has spread to. If the ransomware did in fact spread, we would just follow the same steps we followed for the original workstation to remedy the situation.

Minimize

In order to minimize the potential of attacks like this taking place in the future, I believe it is important to enforce the policy that was already supposed to be in place. That is to say that the departments that were originally designed to be segmented off of the network should be taken off and segmented as planned. That will prevent spreadable malware like the ransomware experienced in this scenario from being able to affect those departments. Assuming that the financial department was one of those meant to be segmented, it would also have prevented this malware from being able to travel to outside departments.

Another way to prevent attacks like this from happening in the future is to make sure all employees are properly trained on cybersecurity best practices (Buchanan, 2022). This can be done in a number of ways, but I recommend mandatory training sessions held regularly. They need to be held regularly so the information remains fresh in the minds of employees that have internet and network access. The sessions would include topics relating to security, so as to inform users about the dangers of phishing scams and other cybersecurity threats. They would also teach users safe ways of using external devices and BYOD policy.

Normal Business Operations

If the workstation that the ransomware was discovered on is the only computer that is affected, normal business operations should be able to continue relatively unaffected. However, the user states that the affected file is critical to company finances. Assuming the file exists somewhere on the network and is unrecoverable without utilizing the backup, normal business operations won’t be able to continue in the financial department until that file is recovered. In this situation, the best course of action may be to recover the backed up files as quickly as possible so that the department can continue working as usual.

In the event that the ransomware has spread past the financial department, normal business operations depend on how far it spread. If the ransomware has affected the entire network, the only way to continue with business operations as usual may be to succumb to paying the ransom, though this is the least ideal outcome. From that point, it would be best to invest in means of making sure nothing like this happens again, such as the aforementioned security training for all employees.

Failover

In a situation like the one described, an adequate failover solution may be to maintain physical paper copies of all financial files so that there is always something to reference in the event that digital files are no longer usable. This would be a benefit to the corporation because compromises like ransomware would not have a great effect on normal business operations. It would take some time to copy the information on paper back over to a digital format, but that is not as critical of a loss as paying a ransom or regenerating an entire network from a backup.

Backup Strategy

An update to the backup strategy that I would propose is to perform backups more frequently (Data Recovery Labs, 2022). Only creating a backup file once a month leaves too large of a gap for incidents like this one. In a worse case scenario, the corporation is having to revert back to data that was relevant an entire month ago, but no longer relevant today. This situation could lead to losing new customers as their information was lost, or missing shipments because purchase orders are no longer available. By creating new backups every week, or even every night, the corporation can be better protected from attacks that result in lost or compromised data.

References

Buchanan. (2022, March 10). *5 major benefits of Security Awareness Training*. Buchanan Technologies. Retrieved June 12, 2022, from https://www.buchanan.com/benefits-security-awareness-training/

Data Recovery Labs. (2022). *How often should you backup your files?* Data Recovery Labs. Retrieved June 12, 2022, from https://www.datarecoverylabs.com/company/resources/how-often-should-you-backup-your-files#:~:text=Important%20files%20should%20be%20backed,of%20the%20day%20or%20week.

N-able. (2021, May 5). *Intrusion detection system (IDS): Signature vs. anomaly-based*. N-able. Retrieved June 12, 2022, from https://www.n-able.com/blog/intrusion-detection-system