Incident Response Case Study

CISOSHARE
MOVING SECURITY PROGRAMS FORWARD

CISOSHARE Incident Response Team quickly triages incident and implements improvements to client security environment.

"Today, incident response is about communication and organization as it is about digital forensics and reverse engineering files. The new privacy and regulatory requirements mean management needs to quickly and repeatably be informed as an incidents progress. It's beyond knowing if your systems are up. It's asking questions such as; what is the sales and marketing impact? How will it be communicated to the public, partners, clients, etc. Are there internal resource damages and cultural impacts? Often these questions need to be answered before or during the technical analysis" – Adam Couch, Vice President of Professional Services at CISOSHARE

Executive Summary

For privacy reasons, we cannot disclose client names. References are available upon service agreement.

After a company's clinic management software is hit by a crypto-ransomware attack, the CISOSHARE team responds quickly using best practices and a proven methodology. The incident response team determined and met the client's main objectives, which included identifying the root cause, conducting malware forensics, and confirming that no sensitive data was exfiltrated from the environment. During the investigation, the CISOSHARE team also quickly restored daily operation and remediated the client's overall security environment.

Attack Timeline

The attack on the clinic brought down the initial firewall, at which point all traffic was immediately directed through their secondary firewall. Unfortunately, this firewall was misconfigured and had no restrictions on their RDP (remote desktop protocol) that allowed for the lateral movement between machines and servers. Logs later revealed 40,000 attempts to login using admin credentials, after which the malware entered the client system and encrypted specific files on a single end user's machine.

The day that the attack occurred, a user attempting to use the client's services found suspiciously-labeled files. After bringing this to the attention of the onsite IT team, the machine was taken off the network but not turned off for the sake of preserving the disk image of the RAM (random-access memory).

It was at this point that the client contacted CISOSHARE to assess and remediate the incident.

Response Timeline

The CISOSHARE Incident Response Team completed the entire engagement through a fully remote process to save on the overall customer cost and lasted for a total of 45 days from the beginning of the engagement to the completion of the client's goals and providing recommendations for recovery and improvement.

The team began with an initial set of meetings to introduce the team and the methodology, as well as identify the goals the client wanted to meet and understand the background of their security environment.

Following the introductory meetings, the CISOSHARE team conducted several discovery meetings to identify critical information. Through these meetings, the team identified the initial point of entry, received the malware sample identified by the client's internal response team, and received a snapshot of the disk image of the compromised machine. The CISOSHARE team established their operating protocol, the formal roles of the team, and the three goals that the client wanted to meet:

1. To identify the root cause of the incident and understand the initial point of compromise.
2. To conduct malware forensics and understand how the malware works.
3. To confirm that no sensitive data was exfiltrated.

The incident response team utilized the provided disk image of the compromised machine to build a timeline analysis of the attack and discovered the malware that the attacker used.

Using the data from this machine and the client's available firewall logs, the team was able to determine that the attack occurred after the initial firewall had failed. Traffic was automatically routed to a secondary firewall, but this was misconfigured, allowing the attacker to exploit the RDP and plant the malware and encrypt client files.

Approximately two hours passed between encryption and the discovery of the incident and the isolation of the compromised machine.

Once the malware sample was taken from the machine, the CISOSHARE team worked to develop a signature of the malware to hunt and eradicate any persistent versions of it living in the client network.

The team utilized a tool to establish a malware signature, which was then used to hunt for any traces of it that existed in the network. No additional malware instances were discovered, although the team monitored the network for 2 weeks and checked IPs that were hardcoded in the malware instance to ensure that there were no open connections or committed control servers in the memory. No data was exfiltrated from the system.

Recovery and Improvements

During the investigation, the team noted gaps in logging and monitoring, as well as other areas for improvement in the client network that were identified, recorded, and included in the go-forward plan.

The team discovered that, along with the improperly-configured restrictions on RDP on the second firewall, their firewalls overall were not retaining sufficient logs. These firewall logs were only retained for 2-week time periods, meaning the initial attack that brought the firewall down was not captured. The client increased the life of their logs based on our team recommendation.

During the investigation, the team also noted a lack of lateral segmentation and latency in moving between the servers, as well as tie-ins to different parts of the network that should have been more restricted.

As the incident response team conducted their investigation, we also ensured that their business was fully operational within a week of the start of our engagement. Based on the findings in the environment, the team gave strategic recommendations including compliance with certain best practices in NIST 800-62.

Specific recommendations included creating a policy to rotate and change admin names and passwords with an identity management program, a more complete security architecture program to help understand and properly monitor logs, as well as lateral segmentation to prevent access to prevent unrestricted access across different areas of the environment.

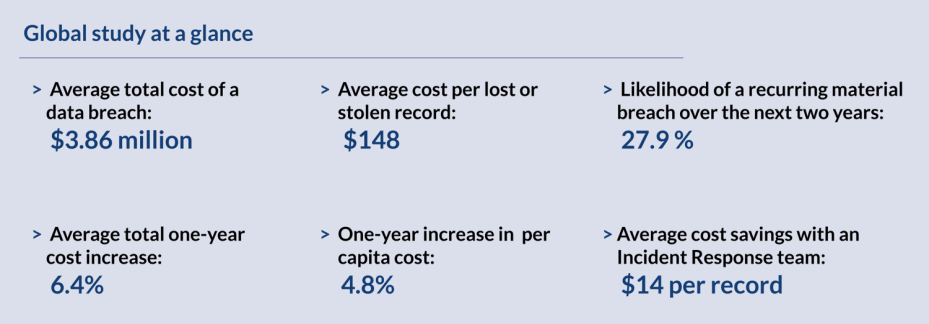
Results

The CISOSHARE's incident response team was successful in eradicating and validating the eradication of remaining malware samples in the environment, including malware samples that had the potential to steal resources for bitcoin mining and compromise regulated patient records. The team was successfully able to consider the business risk and impact in all the actions that the client requested in response to the incident.

Statistics

Ponemon 2018 Study

The research also recommends putting in place an incident response team. This, according to the study, can decrease the cost of a data breach by up to $14 per compromised record from the $148 average per-capita cost.



IBM Security and Ponemon Institute 2018 Report

Conclusion

Based on the data from the 2018 cost of a data breach study, being able to contain a breach in less than 30 days will save you more than USD 1 million compared to a company that does not.