IR Response Report

Group: Ethan Nesel, Rachel Solem, Jeff Rennie, Joshua Davis

Immediate Action:

On Monday morning, Mike notices that the application server is running slowly, and error messages are randomly showing up. Mike does some basic troubleshooting to try and resolve these issues. He runs a set of security scans when he cannot locate the source of the sluggishness. These sweeps include a primary virus and rootkit scan using the company's antivirus solution. According to Mike, the rootkit scan returned positive, and he now has good reason to believe the application server is infected with a rootkit. To briefly assess the possible timeline of the newly discovered breach, Mike looks at the log files and finds suspicious logins going back three weeks. Mike calls you down, as his direct supervisor, to assess the situation and personally examine the logs and scans to verify that his suspicions are correct. After confirming that the logins are suspicious and you have no reason to doubt Mike, you call in those available to assist with incident response. Mike, Jill, Wanda, Ed, James, and yourself will be designated to handle this situation. You brief the team that they will all be handling this matter, and no information is to leave the circle, even to others within the company, without your approval or instruction, as all of the facts have not been discovered yet. The incident response framework of the business follows an identify, stop, quarantine, recovery, and report model. However, the specifics are vague, and varying situations will change response tactics.

You let your team know they will be divided into pairs or remain as individuals to handle the various aspects of the incident response. Tasks will continue to be assigned as progress is made. First, Jill is designated to reach out to the cloud backup provider and check in to see what backups are available for a hot-cut. Wanda and Mike are tasked with preparing the devices needed to set up a hot-cut within the next 24 hours. James is assigned to analyze the database for obvious modification. Ed is tasked with validating Mike's initial scans, checking for additional vulnerabilities, and assisting with his regular duties.

Within the Next 24 Hours and Long Term:

As the IT Director, you would conduct a phone call to a lawyer consultant to determine the company's legal requirements per the State of New Mexico, the FTC, and any other specific requirements associated with current cybersecurity laws based on data breaches.

Ed conducts a series of five scans, starting with a network-based vulnerability scan to identify possible network security attacks and vulnerable systems on wired or wireless networks. During his search, he found no unknown or unauthorized devices and systems on the network. Next, he performs a host-based scan to locate and identify vulnerabilities in servers, workstations, or other network hosts and provide greater visibility into scanned systems' configuration settings and patch history. The third scan Ed performs is a wireless scan to identify rogue access points and validate that the company's network is securely configured, which he discovers is still secure. Next, he conducts an application scan to test the website and detect software vulnerabilities and erroneous configurations. Finally, Ed and James examine the database and web application for apparent malicious modifications by utilizing the database vulnerability scanner Scuba and Acunetix, a scanner for web application vulnerabilities. Scuba scans enterprise databases for vulnerabilities and misconfigurations. In contrast, Acunetix is a web vulnerability scanner with advanced crawling technology to find vulnerabilities by searching every type of web page—even password-protected ones. During the scan, Ed validates Mike's discovery of the rootkit on the application server, while James does not find any apparent malicious modifications on the database.

Upon completion of scans and verification of what information has been compromised, you inform the two CEO's that a breach has occurred via an official report documenting what happened when it happened, what information was involved, what we are doing, and other important information.

Jill informs you that full backups for the past six months are available. Comparing versions of our off-site backups, we can tell there is a safe full backup dating back three weeks just before the suspicious logins and rootkit were installed. As a group, we do not trust that all the problems have been found and would like to continue analyzing all that has happened in the 3-week timeframe.

After speaking to the lawyer, you've been instructed to contact the major credit bureaus advising them that we are recommending that people request fraud alerts and credit freezes on their files. The lawyer also suggests that a letter from the CEO is mailed out to each customer who has been impacted, informing them of what happened, how it happened, what information was potentially compromised, what actions we have taken to remedy the situation, what we are doing to further protect customer information, and contact information to a representative in HR who can answer further questions.

Mike and Wanda are responsible for identifying the server currently in spares and will install the replacement in the same rack as the infected server. This will take a couple of hours to gather the materials and complete the installation. While on-site, they will also prepare a Method or Procedure (MOP) to do the hot-cut. This MOP Identifies current power, NIC, ports, cables, and hardware configurations on the server and the router used to establish the connection. The MOP will need to be approved by several of the IT staff. They will continue provisioning the new server hardware and prepare for the cutover at midnight. They will bring the new server up and connect to their router to give management access needed for remote work for Wanda and Jill.

Wanda is designated with the task of installing the OS and supporting applications needed for the new server. Wanda will proceed with a clean OS install to restore trust. She installs the OS and supporting applications and then runs updates to prepare for the entire image backup. At this point, she will go through the hardening process on the OS and all applications to prevent the attack from returning to the new server.

Jill starts the download of the full image backup, knowing it will take several hours. During this process, Jill tells the team she will need to create a new full image backup of the infected server in the event they need to restore the image in case it becomes corrupted. Restoring the full backup means three weeks of data is missing on the new server. She will need to identify all valid data on the infected server. This will take several days to complete the full analysis and safely restore the data. Jill successfully restores the uncorrupted full image backup and is awaiting the transition. She then starts a new full image backup based on everything being updated and hardened on the clean install.

The IT Director instructs a message to be sent out to all current clients that the server will be going down at midnight for emergency maintenance. This will signal all clients to pay attention to this day/time to go back to in case of any questions or follow-ups.

Mike has presented the MOP to the team, which has been approved and is ready for the hot-cut at midnight. Jill and Wanda are on a bridge for this emergency maintenance as this is a critical event and requires all hands on deck. The server and router will be remotely switched to live data on the new server. At midnight, Mike provisions the router to direct traffic to the new server, which takes a couple of minutes for the traffic to propagate, leaving the server down for only a short time.

After recovering from the cyberattack, we must determine exactly what we lost in this attack and what we can do to further harden our systems to prepare for another attack. To determine how the rootkit entered our workspace, we will do a complete forensic autopsy of the compromised server. This process may be completed within a few days but will likely take several weeks to months. While that process plays out, we will start hardening the most likely vectors, phishing attacks, and the customer-facing website which lives in the application server.

To mitigate phishing attacks, we will create monthly internal simulated attacks to raise awareness of the problem within the company. To lower our click rate below the industry average of 10%, we will encourage this by offering incentives for alerting the information security team of possible phishing emails instead of penalizing them for clicking on our bait. The initial step that we will take to secure our website is to limit the ability of the public to upload documents onto the site to send them to Slippery Slope LLC.

Following the advice from the lawyer, we assist the CEOs in sending an email to all of our affected customers notifying them of the attack and that their data was within the tranche stolen by the malicious actors and that while the data was secured by the highest level of commercial encryption available, that doesn't mean that it cannot be unencrypted with future algorithms. We recommend changing their credit card numbers and offering free credit monitoring for two years. We additionally reach out to the credit bureaus as instructed.

We will also commit to doing quarterly penetration tests instead of yearly, which is the industry minimum. Slippery Slope LLC will also audit log data daily and hire an analyst specifically dedicated to that task, in addition to adding more qualifications for alerts so that we get more specific notifications about suspicious activity. We will also prepare more specific incident response documents with assigned roles to respond to the next security incident with even greater speed and accuracy. Lastly, we will do quarterly audits of the admin permissions that our users hold to comply with the principle of least privilege and make it less likely for a hacker to gain access to an account that can give them root access.

Founder #1 - Argument in favor of reporting and/or against not reporting

According to the first founder, reporting the breach is imperative for integrity. Customers who are informed about the breach will be able to be vigilant about the malicious use of their data if it is decrypted and used. They can even purchase detection services to do it for them. Keeping customers in the loop will also make the company appear transparent and forthcoming. Additionally, the lack of a breach reporting law is not a guarantee that all legal and financial issues are automatically avoided. Other laws may apply due to the events following a breach. Furthermore, if the breach is not officially announced but is discovered by customers due to a leak, it could destroy the business. The company should not put itself into a situation where it could be extorted. Unfortunately, customers will likely be unhappy even if the company is forthcoming. They will probably expect the company to spend a lot of money hiring security staff and purchasing expensive protection software. However, to this founder, the pros outweigh the cons. Additionally, the business will be updating security to prevent further breaches that could be worse.

Founder #2 - Argument in favor of not reporting and/or against reporting

According to the second founder, keeping the breach from customers is risky but overall a better financial decision. If a breach is revealed, it will be a PR nightmare, and the business will lose trust and create financial uncertainty. This could signify the end of operations and a shutdown for their business size. If the company avoids reporting, customers will remain in the dark, and the business should remain stable. The data the hackers could access is encrypted, so it is unlikely they can do anything with it. The company can still work on improving security. However, it can select more budget options, train existing employees on new measures, and avoid hiring expensive specialists. No doubt, there are risks. Agreeing with the first founder, the second acknowledges that customers may find out through a leak, or the data could be decrypted in the future leading to significant financial issues. Both civil and criminal legal issues could occur, but taking the chance they won't is worth it if it saves the company from certain financial ruin. While there are many risks and perhaps more cons, founder two remains firm on his stance, framing it as a business toppling decision if they go with founder one.