Table Top Exercise Simulation

Institution Introduction

For our Table Top Exercise (TTX), we are imagining that we are conducting it with executives from a fictitious hospital named "Vincennes Hospital." Vincennes Hospital is a regional hospital with a major presence in the Midwest of the United States. The institution offers a variety of medical services including cancer treatment, neurological services, cardiology services, and provides some of the most progressive technology available today. The hospital is concerned about cyber attacks that could result in patient safety concerns, data breaches, financial losses, and reputation damage.

Intelligence Report

The intelligence report titled "DEV-0569 Finds New Ways to Deliver Royal Ransomware, Various Payloads" is posted on the Microsoft website by the Microsoft Threat Intelligence Team. Microsoft gives an unknown and/or evolving cluster of threat activity the interim label DEV-XXXX. In this report, Microsoft researchers analyze various DEV-0569's delivery tactics and provide insight into the group's historical activities. The threat intelligence team also recommends various ways to defend against DEV-0569. The link to the report is available at https://www.microsoft.com/en-us/security/blog/2022/11/17/dev-0569-finds-new-ways-to-deliver-royal-ransomware-various-payloads/.

Risk Register Entries

*Likelihood Score (0-10), Impact Score (0-10), and Resulting Risk Score (0-100)

1) The threat intelligence report from Microsoft notes that DEV-0569 has developed new techniques for bypassing anti-malware solutions, including using macro-enabled Excel files and malicious PDFs that contain JavaScript. In our TTX, we would identify that (1) our current anti-malware solutions do not adequately protect against these specific techniques; (2) our organization has limited backups and disaster recovery capabilities, making us vulnerable to such attacks; (3) we would not pay a ransom.
    - Risk: Malicious files could evade our anti-malware solutions and lack of backup capabilities could hinder recovery
    - Threat Objective(s): Based on the report, DEV-0569 is delivering ransomware and other payloads for financial gain. In the meantime, reputational damage is caused by data theft and public exposure of sensitive data.
    - Likelihood: 8. Based on the intelligence in the report, we know that DEV-0569 has successfully used these techniques in real-world attacks against a range of targets,

including the healthcare industry. While our current anti-malware solutions are effective against some types of attacks, it is clear that we are vulnerable to these specific tactics. Additionally, our backup system is likely not capable of fully recovering the loss of data.

- Impact: 10. Ransomware attacks can have a severe impact on our business operations, potentially leading to data loss, financial loss, and reputational damage. The use of malicious PDFs and macro-enabled Excel files suggests that the attackers are targeting users in our organization, which could lead to widespread compromise. We have limited backups and disaster recovery capabilities, which could exacerbate the impact of such an attack.
- Risk Score: 8 x 10 = 80 or CRITICAL.
- Remediation task: We assign the IT security team to evaluate and deploy additional anti-malware solutions that can detect and prevent attacks that use malicious PDFs and macro-enabled Excel files. The IT Operations team should improve our organization's backup and disaster recovery capabilities. This could include implementing a regular backup schedule, storing backups offsite, and testing backup and disaster recovery procedures to ensure they are effective. The IT Operations team should also work with other teams, such as security and risk management, to ensure that the backup and disaster recovery plan aligns with our organization's overall risk management strategy. Since we would not pay the ransom, keeping our data safe and backed up after a ransomware attack is a top priority task.
    - Assigned Teams: IT Security, IT Operation, and Risk Management.
    - Due date: Within 3 months Based on SLA and priority.

2) The report notes that DEV-0569 has been using phishing emails and social engineering tactics to deliver its payloads, often using language that is specific to the target organization. These tactics involve distributing harmful links to targets via malicious advertisements and fake forum pages. In our TTX, we would identify that our employees may not be adequately trained to recognize and report these types of attacks.
    - Risk: Employees may fall for phishing emails and social engineering tactics
    - Threat Objective(s): According to the research, DEV-0569 employs social engineering strategies to persuade users to open dangerous attachments or click on sites that trigger the download of malware.
    - Likelihood: 7. Based on the intelligence in the report, we know that DEV-0569 is using sophisticated social engineering tactics to deliver its payloads. While we have some training programs in place for our employees, it is possible that some users may not be adequately prepared to recognize and report these types of attacks. In addition, the usage of employee cybersecurity training has been decreasing since its launch in the first year. Furthermore, while multi-factor authentication (MFA) is deployed, there are still a few departments that are not forced to use MFA.
    - Impact: 6. If an attacker is successful in tricking a user into downloading malware or providing sensitive information, it can lead to data loss, financial loss, and

reputational damage. While the impact of these types of attacks can be significant, we believe that our current security controls can help to mitigate the majority of the risks.

- Risk Score: 7 x 6 = 42 or MEDIUM.
- Remediation task: We assign the HR and IT security teams to work together to improve our employee training programs around social engineering and phishing attacks. For the phishing email attacks, we assigned internal IT to ensure the completeness of the MFA deployment. For malicious installer and VHD file attacks, we sent an internal memo to sensitive groups such as IT to warn employees to only download files from reputable sources. For the contact form attack, we advise and train the recipients to not click on any links and report suspicious senders.
    - Assigned Teams: HR and IT Security
    - Due date: Within 6 months based on SLAs.

3) The report notes that DEV-0569 has been using PowerShell scripts to deliver their payloads, often using obfuscation techniques to evade detection by anti-malware solutions. In our TTX, we would identify that our current security controls do not adequately monitor PowerShell activity on our network, leaving us vulnerable to this technique.

- Risk: PowerShell scripts used by DEV-0569 could deliver ransomware or other payloads undetected
- Threat Objectives: Based on the report, DEV-0569 is actively distributing Royal ransomware and other malware payloads, which could lead to the encryption of our sensitive data and significant disruption to our business operations.
- Likelihood: 8. PowerShell is a popular attack method for threat actors since it is a widely used scripting language on Windows computers. The report notes that DEV-0569 is using obfuscation techniques to evade detection, which increases the likelihood of successful exploitation. However, our organization has implemented some security controls that may reduce the likelihood of a successful attack.
- Impact: 7. The impact of a successful ransomware attack could be significant, resulting in financial loss, reputational damage, and operational disruption. While we have backup systems in place to help recover from a ransomware attack, there may still be a period of downtime and potential data loss.
- Risk Score: 8 x 7 = 56 or HIGH.
- Remediation Task: Implement more comprehensive monitoring of PowerShell activity on our network including deploying additional security controls and tools that specialized in PowerShell activity response. One of the promising solutions in the market is driven by AI and behavior monitoring and detection. The IT security team should thoroughly evaluate potential solutions and conduct tests to ensure their effectiveness.

- Assigned Team: IT Security
- Due Date: Within 30 days based on SLAs

References

Intelligence, M. T. (2022, November 17). *DEV-0569 finds new ways to deliver Royal ransomware, various payloads*. Microsoft Security Blog. https://www.microsoft.com/en-us/security/blog/2022/11/17/dev-0569-finds-new-ways-to-deliver-royal-ransomware-various-payloads/