Topic 2 Discussion 2

Provide an example of an occurrence where a patch could not be installed on all enterprise systems. Describe the compensating controls you would recommend to protect your systems given that the patch would not be used on your production network. Research zero-day patching and explain when this would be utilized in a production network.

Hello Class,

In the enterprise scenario, one way a patch could not be installed would be that the company has a legacy system that is crucial for business operations. Therefore the system is no longer supported by the hardware/software vendor, and there are no available patches for these systems. In cases such as this, compensating controls would need to be implemented to mitigate the risk.

Compensating controls are measures taken to address any weaknesses of existing controls or to compensate for the inability to meet specific security requirements due to various different constraints(Team 82, 2023).

Some compensating controls that could be used are:

Network Segmentation - Isolate the legacy system on a separate network segment, limiting its exposure to the rest of your production network.

Intrusion Detection Systems (IDS) - Deploy an IDS to monitor the legacy system's network traffic for suspicious activity and alert you to potential attacks.

Firewall Rules - Configure strict firewall rules to block unauthorized access to the legacy system.

Access Control - Restrict access to the legacy system to only authorized personnel.

Regular Monitoring - Implement regular security monitoring and vulnerability scanning to identify any potential issues.

When patches are released for vulnerabilities that were previously labeled as zero-days, they're called zero-day patches(ManageEngine, 2024). These are vulnerabilities that are unknown to the vendor and for which no patch is available. Zero-day patching is typically used in a production network when a critical vulnerability is discovered and a patch is released. This is a high-priority situation, as the vulnerability could be exploited by attackers before the patch is widely deployed.

In this case, you would need to quickly assess the risk posed by the vulnerability and determine if the patch can be applied to your production network without causing any disruption(Ballejos, 2024). If the patch is deemed safe and necessary, it would be deployed as soon as possible.

References:

Ballejos, L. (2024, June 3). How to Address Zero-Day Vulnerabilities | NinjaOne. NinjaOne. https://www.ninjaone.com/blog/how-to-address-zero-day-vulnerabilities/

ManageEngine, communications@manageengine.com. (2024). Zero Day Vulnerability: Definition, Examples & Prevention - ManageEngine Vulnerability Manager Plus. Manageengine.com. https://www.manageengine.com/vulnerability-management/zero-day-vulnerability-mitigation.html#:~:text=When%20patches%20are%20released%20for

Team82. (2023, April 6). The Importance of Compensating Controls in Cybersecurity. Claroty. https://claroty.com/blog/ot-icefall-vulnerabilities-underscore-the-importance-of-compensating-controls#:~:text=What%20are%20Compensating%20Controls%3F