Topic 2 Discussion 1

Explain when manual patching is primarily used, and discuss two risks associated with this practice. Assume you are the director of an organization and construct a short letter of intent to your directors that describes when you would permit manual patching. Discuss whether you agree or disagree with peers on their manual patching policy communication and justify your stance with specific reasons, facts, and examples.

Hello Class,

Manual patching is primarily used when:

* When automated patch installs are not available. This might occur for legacy systems or those not compatible with automated patch management tools.
* In critical situations where a vulnerability requires immediate action, manual patching might be necessary before an automated solution is available.
* When systems have significant customizations, manual patching might be required to ensure the patch does not disrupt the system's functionality.
* It helps organizations ensure that all software is patched properly and that the patching process does not introduce new vulnerabilities. (*What is Manual patch management? - A Practical Guide*. 2023)

Risks of Manual Patching

* Manual patching is prone to human error, leading to misconfigurations, incomplete patches, or even system instability.
* Delaying patching due to manual processes can leave systems vulnerable to exploits, increasing the risk of data breaches and other security incidents.
* Possibility of faults during patching, causing breaks in programs and or operating systems. (*Patching Applications and Operating Systems*. 2011)

Letter of Intent

To: Board of Directors

Subject: Manual Patching Policy

Dear Directors,

We recognize that manual patching is a less secure practice compared to automated patching. However, there are situations where it may be necessary, such as:

* For systems not compatible with automated patching tools.
* In critical situations where a vulnerability requires immediate action.
* When systems have significant customizations that may be incompatible with automated patching.

It is crucial to understand that manual patching carries inherent risks:

* Manual processes are prone to human error, potentially leading to system instability or incomplete patches.
* Delaying patching due to manual processes can leave systems vulnerable to exploits.

Therefore, manual patching will only be permitted under strict conditions, with thorough documentation and oversight. We are committed to minimizing the risks associated with manual patching by:

* Utilizing experienced personnel: Only highly skilled IT professionals will be authorized to perform manual patching.
* Thorough testing: All patches will be rigorously tested in a controlled environment before deployment.
* Detailed documentation: Every manual patch will be documented, including the reason, steps taken, and any potential issues encountered.

This policy aims to balance the need for flexibility with the imperative of maintaining a strong security posture. We will continue to prioritize automated patching solutions and actively explore options to reduce the reliance on manual patching in the future.

Sincerely,

Ryan Coon Director of IT

Peer Discussion

With many discussions with peers on manual patching, I will have to agree to limit manual patching to only extreme cases such as applying manual patches to legacy systems or needing customized patching. Without testing or documentation that identifies the risks, we could have the possibility of a faulty or failed patch, leaving us susceptible to a multitude of hacking attacks. A staggering majority of CIOs and CISOs even say that they delay putting security patches through to avoid interrupting business growth(*IT Horror Stories: Why Unpatched Software Hurts Business. 2018*). With this I would like to have our IT department ahead of the game in testing and applying patches that are deemed necessary, even if it were to interrupt work for an hour. An hour could save our company millions in unnecessary ransomware attacks.

References:

*IT Horror Stories: Why Unpatched Software Hurts Business. (2018, October 22). NinjaOne. https://www.ninjaone.com/blog/it-horror-stories-why-unpatched-software-hurts-business/*

*Patching Applications and Operating Systems. (2011). https://www.cyber.gov.au/sites/default/files/2023-11/PROTECT%20-%20Patching%20Applications%20and%20Operating%20Systems%20%28November%202023%29.pdf*

*Souppaya, M., & Scarfone, K. (2013). Guide to Enterprise Patch Management Technologies. NIST Special Publication 800-40 Revision 3. https://doi.org/10.6028/nist.sp.800-40r3*

*Stallings, W. (2018). Operating systems : internals and design principles. Pearson.*

*What is Manual patch management? - A Practical Guide. (2023). Reasonlabs.com. https://cyberpedia.reasonlabs.com/EN/manual%20patch%20management.html*