PHANTOM s.r.l
IMPOSSIBLE IS OUR TARGET

Digital Risk Manager - S1/L1

RISKS AND PROCESSES

Phantom srl

Phantom Team:

Alessio D'Ottavio
Davide Di Turo
Francesco Pio Scopece
Giuseppe Pinatello
Luca Iannone
Manuel Di Gangi
Marco Fasani
Oliviero Camarota

INDEX

03 Exercise

04-06 Introduction and Processing

07-08 Risk chain

09 Recommendations and Conclusions

EXECERCISE

Define a (simplified) process for updating a web server (e.g. Apache), including procedures for each activity. Example of activities only:

1. Assess the need for the upgrade

2.Make complete backups of the web server

3.Choose update method

4.Download the update it

5....

On the process just defined, identify 3 risk "chains" in a qualitative and descriptive form:

Threat agent → Threat → Vulnerability → Impact → Risk

RISK MANAGEMENT:
WEB APACHE SERVER UPDATE

Introduction:

Updating the Apache web server is a critical practice for maintaining optimal security, performance, and functionality of our server environment. However, this process presents risks
that must be carefully managed to ensure smooth operation and protection of our digital assets.

Upgrade Process Steps:

1. Update Management:

- We analyze Apache changelogs to identify new features, bug fixes, and resolved security vulnerabilities.
- We evaluate the urgency of the update based on the associated risks, as potential security breaches or performance degradation.

At this stage, it is crucial to carefully analyze Apache changelogs to understand new features introduced, bug fixes, and security vulnerabilities resolved. This assessment helps us determine the urgency of the upgrade based on the associated risks. For example, critical security patches require immediate installation to mitigate the risk of server compromise.

2. Full Web Server Backup:

- We make a complete backup of all configuration files, site documents
web and databases.
- We use reliable and tested backup tools to ensure data integrity and the possibility of recovery in case of need.

Before proceeding with the upgrade, it is essential to perform a complete backup of all configuration files, website documents and databases. By using reliable backup tools, we ensure data integrity and the ability to restore it should the need arise. This step is crucial to mitigate the risk of data loss during the upgrade.

3. Update method:

- We evaluate whether to use the operating system's package manager or run manual updating.
- We consider the risks and benefits of each method in relation to the complexity of ours server environment and the criticality of the website.

The decision on the update method (via the operating system package manager or manual update) depends on the complexity of the server environment and the criticality of the website. It is important to carefully evaluate the risks and benefits of each method to ensure a safe and efficient process.

4. Download and Install Update:

- We use the package manager of the operating system or download manually the update from the official Apache site.
- We follow the installation instructions carefully to ensure that the process it's safe.

During this phase, we download the update from trusted sources and carefully follow the installation instructions to ensure an error-free and safe process. We verify that the update is authentic and not compromised, thus reducing the risk of installing malicious or vulnerable software.

5. Test update on Server in safe enviroment:

- We start the Apache web server and test all critical features to ensure that operate correctly.
- We monitor server logs for any errors or problems during startup.

We start the Apache web server and test all critical features to ensure they operate correctly. We carefully monitor server logs for any errors or problems during startup. This helps us promptly identify and resolve any post-update issues.

6. Monitoring After-Update:

- We carefully monitor the server to identify any bad performance or compatibility issues
- We use performance monitoring tools to detect any problems in real time.

After the upgrade, we carefully monitor the server for any performance anomalies or compatibility issues. We use tools performance monitoring to promptly detect and resolve any issues in real time.

7. Management of Problems Encountered:

- We intervene promptly to resolve any problems encountered during or after the update.
- We evaluate the rollback option if necessary to restore operational continuity in case of critical malfunctions.

In case of problems during or after the update, we intervene promptly update. We carefully record the date, time and details of the update for audit and traceability purposes. resolve them and restore server operational continuity. We evaluate the rollback option if necessary to return to a stable and working configuration.

8. Update Documentation:

- We update the web server documentation with information regarding the updated Apache version and changes made during the deployment process 7. Management of Problems Encountered: update.
- We record the date, time and details of the update for audit purposes and traceability.

Finally, we update the web server documentation with information about the updated version of Apache and the changes made during the deployment process update. We carefully record the date, time and details of the update for audit and traceability purposes.

RISK CHAINS IDENTIFIED IN SERVER UPDATE PROCESS ON APACHE:

Risk chain - Attack by an external attacker:

Hackers or groups of hackers.

Using known or zero-day exploits to exploit unpatched vulnerabilities in the Apache server not yet updated.

Presence of unpatched vulnerabilities in the current version of Apache financial losses and reputational damage.

Potential compromise of server security and hosted data financial losses and reputational damage.

High risk of security breaches and resulting financial losses to unauthorized access to sensitive data.

Risk Chain - Human Error During Update:

Human operators responsible for updating the server.

Human operators make mistakes during installation Using known or zero-day exploits to exploit unpatched vulnerabilities in the Apache server not yet updated. of the update.

Incorrect installation of the update or failure to verify post installation.

The server may stop working properly or they may data loss may occur due to human errors.

Moderate, as human errors are inevitable, but can be mitigated through quality control and verification procedures.

Risk Chain: Insider Threat (Malicious User):

Employees or former employees with privileged access to the server.

A malicious insider attempts to gain unauthorized access to the Apache web server to corrupt or steal sensitive data.

The server may have unpatched security flaws as a result of missing or incomplete updates.

The malicious user could compromise the security of the server and data, causing financial and reputational damage to the company.

High, as internal users are familiar with the system and can exploit vulnerabilities for malicious purposes if not adequately mitigated.

These risk chains illustrate how different threats, vulnerabilities, and impacts can interact within the Apache web server upgrade process, highlighting the importance of thorough risk management to ensure system security and reliability.

RECOMMENDATIONS AND CONCLUSIONS

Effectively managing the risks associated with upgrading your Apache web server is essential to ensuring a secure and reliable server environment. By following a rigorous procedure and carefully monitoring the process, we can mitigate risks and ensure optimal operation of our system.

These risk chains illustrate how different threats, vulnerabilities, and impacts can interact within the Apache web server upgrade process, highlighting the importance of thorough risk management to ensure system security and reliability.

Thank you!

BY: