Replace
with **LOGO**

Patch management

Version:	**1.0**
Date:	01.09.2021
Author:	Head of IT (John Smith)
Released by:	Information Security Officer ((ISO) Jane Smith)
Scope of application:	Entire company
Responsibilities:	Employees of the IT department

Date	***Version***	***Author***	***Change***
01.09.2021	*1.0*	*Head of IT*	*Newly added section "Example" in chapter 2.3*

Table of contents

1 Aim and purpose

The term patch management refers to the strategic control of the installation of so-called patches or updates, which are used to adapt software and systems and to close security gaps in the software applications or systems that were only recognised or arose after their market launch.

First and foremost, the availability of patches must be monitored in a targeted manner and existing patches must be installed as quickly as possible. Patch management includes the planning, procurement and testing of patches. This means that the software inventory is constantly kept up to date, patches are tested for compatibility with other software applications and distributed in the network after successful testing.

If errors occur during patch distribution, these so-called reports are analysed immediately. This analysis serves to improve the distribution process. If problems occur with other network functions during the distribution of patches despite a successful test phase, the system administrator should be able to withdraw a patch centrally.

2 Procedure

Part of the patch management process is automated; part is done manually. We encourage the regular checking of systems for vulnerabilities and the timely closure of these. Regular updating of systems is encouraged.

2.1 General rules and manual patch management

The management of the patches is as follows:

Regularly obtain information on vulnerabilities and patches

- Standard patches are usually installed immediately, as patching is also automatically required by the systems.
- All manufacturers of the products used have corresponding mailing lists to inform themselves about security vulnerabilities and available patches. In addition, the usual German and international sources are used, such as Heise Newsticker, RSS feeds or the CERT Bund.
- IT staff are encouraged to inform themselves about current security vulnerabilities through specialised publications.
- The IT department regularly obtains information from the following sources:
    - Microsoft: https://www.microsoft.com/en-us/msrc/technical-security-notifications
    - Heise: https://www.heise.de/newsticker/
    - CERT Europe: https://www.cert.europa.eu/cert/
- The IT staff member responsible for the respective system decides on the installation of updates:
    - The staff member classifies the patches according to the matrix under chapter 2.4.
- The modification of standard software packages (e.g., individualisation, adaptation, or removal of modules as well as undocumented configuration changes) is generally prohibited.

Define the procedure according to your company and adapt the handling.

2.2 Automated patch management

The following patch activities are covered by automated patch management (e.g., Barracuda)

Regular scanning of systems for required updates

- Systems are scanned for software updates every 24 hours

Automatic distribution of patches

- Patches are distributed every day at 5 p.m.

Patched software

- Software that is part of the automatic patch management is also patched automatically

2.3 Handling

Procedure:
All patches will be classified by the IT staff according to the following matrix and handled according to the same.

Test:
If it is possible with reasonable effort, patches are tested in advance by technical staff in a representative test environment, smaller test group or on test devices. For products without testing capability (server products from Microsoft or similar), there is at least one support contract that covers testing of patches before release and support from the manufacturer. After the installation, it is checked again whether the patch has been installed correctly and is functional.

Documentation:
For all classifications except (Normal x Normal), the treatment is according to the handling of incidents, as these cases are vulnerabilities or events or even incidents in case of damage. The vulnerabilities, events or incidents are documented in the "List of Incidents" with date, more detailed information, and the like.

If you work with a ticket system, the documentation will of course take place there. In this case, you should describe this accordingly under the item "Documentation".

		Damage potential of the vulnerability		
		Normal	High	Very high
Possible risk due to patch installation	Normal	Patch will be rolled out within 24 hours	Patch will be rolled out within 8 hours	Patch will be rolled out immediately
	High	The patch is tested within 24 hours in the test environment and then rolled out (see chapter 2.4)	The patch is tested within 8 hours in the test environment and then rolled out (see chapter 2.4)	The patch is tested within 4 hours in the test environment and then rolled out (see chapter 2.4)
	Very high	The patch is tested within 48 hours in the test environment and then rolled out (see chapter 2.4)	The patch is tested within 24 hours in the test environment and then rolled out (see chapter 2.4)	The patch is tested within 4 hours in the test environment and then rolled out (see chapter 2.4)

2.4 Test results

Proceed according to the test result:

- *Positive result (patch installation does not lead to any operational impairments):*
    - A backup is created before the installation so that a recovery is possible in case of emergency.
    - Patch is installed within the patch cycle according to the damage potential class of the vulnerability.
- Negative result (patch installation leads to operational impairments):
    - Carry out the following risk-reducing measures:
        - Unless indispensable, shut down or disconnect the affected systems or services until the vulnerability is fixed.
        - Alternatively, reduce the attack surface (e.g., through access restrictions), increase monitoring measures or raise staff awareness of the vulnerability.
    - Further steps:
        - Defects are identified
        - Contact is made with the software company
    - After problem solving:
        - Re-classification and repetition of the loop