Patch management in an SME environment

Running updates is an effective measure to eliminate existing security vulnerabilities of complex digital systems. Good patch management will facilitate smooth implementation in an SME environment, too.

The most important points to remember:

- Define regular time slots outside production periods to maintain your systems.
- Only ever obtain security updates from reliable sources.
- Check effectiveness and “side effects” of security updates before installing them on production systems.
- Establish a plan for distributing security updates on your systems.
- Keep an up-to-date back-up at hand, just in case something goes wrong with an update.
- Document all maintenance work undertaken on a system.

Security updates

IT systems are developing at an ever faster pace. Application functionalities keep increasing, and hardware and software life cycles have a tendency to become shorter. Manufacturers therefore try to circulate their latest innovations quickly using updates.

In an SME environment, you might well demonstrate a certain degree of restraint in this regard, since not every innovation can be efficiently integrated into your operations. One firm exception though are **security updates**, which should be run as soon as possible.

Every complex system has some hidden errors or vulnerabilities. However, these frequently remain undetected and harmless. Once they have been discovered though, they pose an increasing risk of IT vulnerabilities, since this is when a race against time starts.

On the one hand, hackers start to look for ways of exploiting such exposed vulnerabilities for their own ends, and to develop so-called exploits. If they succeed, malicious third parties can for instance obtain unauthorised access to your systems and data.

On the other hand, manufacturers begin to fix these vulnerabilities as soon as they can with the help of security updates or patches, so to forestall any potential exploits or to render any existing exploits harmless.

Patch management

Basically, security updates should therefore be run comprehensively and as quickly as possible. Something which is generally easy to handle on a private single-user system though could prove tricky in an SME environment. It is therefore necessary to proceed systematically by way of a patch management process.

To install your security updates, the following steps should be followed:

- Identification of any systems affected, and appropriate security updates.
- Obtaining security updates from a trustworthy source, in particular even for systems without their own direct Internet access.
- Preliminary testing of the effectiveness and “side effects” of security updates on non-critical systems.
- System-dependent clearance of security updates and completion of installations outside production periods.
- For critical systems: Planning temporary fallback solutions and scenarios.
- Documentation of all changes made.

Since this is a rolling process, we recommend establishing periodic, fixed time slots for maintaining your systems. This way, you can collect, check and prepare security updates over a certain period of time, but delay their installation until the next time slot for security update installations.

Patch management involves procuring, testing and installing software updates. Their main purpose is to close security gaps in operating systems and applications.

Further information

There are several factors contributing to **identifying any systems affected, and appropriate security updates.** On the one hand, hardware itself plays a role. It is mainly firmware and drivers which will need to be kept up-to-date. Then there's the operating system and applications installed which will need to be checked for available updates.

There are automatic scanner functions for systems with direct Internet access which will periodically establish an inventory of all hardware and software and then look for available updates online. In an SME environment though, such systems should only be used in a support function, if at all. We strongly advise against any unmonitored installation of updates though. It should always be an engineer who is in control of the installation process.

Obtaining security updates can also prove tricky, since updates most easily found on the Internet are not always "original products". In such cases there is a risk of purported security updates actually introducing an exploit into your system. If at all possible, you should always stick with a manufacturer's official distribution channels.

Before you run any update on a production or even critical system, you should ensure it is compatible with the system and its environment concerned. Optimally, this should be done by **testing the effectiveness and "side effects"** (i.e. any potential adverse reactions) of security updates in an isolated, non-production environment. The problem is that frequently, no such thing is available in an SME environment.

Yet it is still advisable to **provide for a system-independent clearance of security updates**, e. g. by running them on less critical systems first. Only after a certain period of observation and some testing should you then also update your other systems.

For critical systems in particular, you should reserve sufficiently extensive time slots outside of production hours to install any updates. Similarly, you should prepare a **fallback scenario and solutions** with the help of back-ups (https://www.ebas.ch/en/data-back-ups-in-an-sme-environment/) , just in case you are unable to install an update successfully.

All steps of the update process should be recorded in **documentation** in a transparent manner. In case you have to find any errors later, you can draw important conclusions as to their origins from this.