Security Advisory Ransomware

Ransomware (also called blackmail, crypto or encryption trojan) is a malicious program that can prevent the access to data or to the entire computer system. In a successful attack, data is encrypted on the computer by cryptological methods. The restoration of the encrypted data is only possible with the appropriate key, for the provision of which a ransom is claimed.

Ransomware spreads through security vulnerabilities in Microsoft Windows operating systems. The most common attacks are spam e-mails with executable files (eg doc, xls, docx, zip, rar, exe) that are opened by careless users. But an attack can also be carried out by a web page equipped with malware that exploits a vulnerability in the used web browser (drive-by-exploit).

Currently cyber criminals use variants from the ransomware families ***WannaCry*** and ***Petya*** for digital blackmail attempts.

Endangerment

Generally all **computer systems with Microsoft Windows operating systems** are endangered and thus also different Dallmeier products like:

- Workstation Tower (004904)
- Workstation Rack-Mount 4RU (004903)
- Server Rack-Mount 1RU (004847)
- Discontinued products like PView Station 7 (000307) or SeMSy® III Workstation Hardware (003304)

Dallmeier products with Windows operating systems are always delivered with the latest updates and security patches released at the time of production.

*Dallmeier **recording systems** are equipped with a **Linux operating system** that is strongly adapted and sealed of (hardened) with regard to system security. They are not endangered by the currently spread ransomware.*

Procedure

Basically, the **Microsoft Windows operating system** should always be kept **up to date**.
This can be done directly via the update function of the operating system. However, Microsoft also informs on the following web page about the availability of security patches for the various operating systems and platforms (32 or 64 bit):

https://technet.microsoft.com/en-us/library/security/ms17-010.aspx

In addition, Microsoft offers the direct download of updates that can be installed via a USB stick on the appropriate computer system. For example, a patch for the currently exploited SMB security vulnerability for Microsoft Windows 7 64 bit or Microsoft Windows 10 Build 1607.

Keep computer systems running Windows operating system up-to-date with current updates and security patches.

In addition to a current operating system, the **established measures and procedures of IT security** should be taken into account. For example, for detailed information about this topic, see the **situation dossier ransomware** (document available only in German language) of the Federal Office for Information Security.

- Perform regular backups of important data
- Use current virus protection programs
- Use current web browsers
- Avoid the execution of suspicious files
- Avoid running scripts or macros
- Employee awareness

Never start an executable file that doesn't seem to be 100 % trustworthy.
Make your employees aware of this.

Windows XP

Computer systems with a **Microsoft Windows XP** operating system should be **disconnected** immediately from the **network**, **especially from the Internet**.

The **Windows XP** operating system is hopelessly **obsolete** (End of Life). Microsoft does not offer **any updates or support** (End of Support) since 2014. For more information, visit the following Microsoft web site:

https://www.microsoft.com/en-us/windowsforbusiness/end-of-xp-support

For the vulnerability exploited by **WannaCry**, Microsoft has provided a **security patch** despite the support end. This can be obtained via the internet directly from Microsoft and installed via a USB stick on the network separated Windows XP system. **However, a further use of the Windows XP system is strongly discouraged**, as this security patch **only fixes one of many known vulnerabilities**.

The Dallmeier sales team or your sales partner will gladly advise you on a migration to computer systems with a modern Microsoft Windows 10 operating system.