advenica

SOLUTION DESCRIPTION

Secure Updates

Updates for Windows and Linux systems are an important part of maintaining the security of the digital information in these systems. However, the updates themselves may be a security risk - to avoid these risks and to maintain the integrity and availability of the systems, special solutions are required.

Challenge

Secure Updates of Windows and Linux Systems

Since Windows and/or Linux-based systems were implemented in ICS/SCADA, the need to be able to update these systems has increased. This need is due to the fact that complex software often contains bugs which should be corrected to ensure stability of the systems. In addition to correcting bugs, the manufacturers behind operating systems and applications drive a function growth which means that operating systems and applications gradually become obsolete if they are not updated.

Security flaws, or in some cases bugs, can be exploited by someone wanting to damage or steal information, or wanting to perform reconnaissance. These are the most important reasons for updating one's systems. However, conducting these updates is also something that can be a security risk if not done properly. The integrity and availability of the systems must be maintained, and most system updates are normally not sufficiently evaluated in the environment in which they are used or in combination with the applications that are running. In addition, an update means that information is imported or added to the system, and this can lead to unwanted malware entering the system.

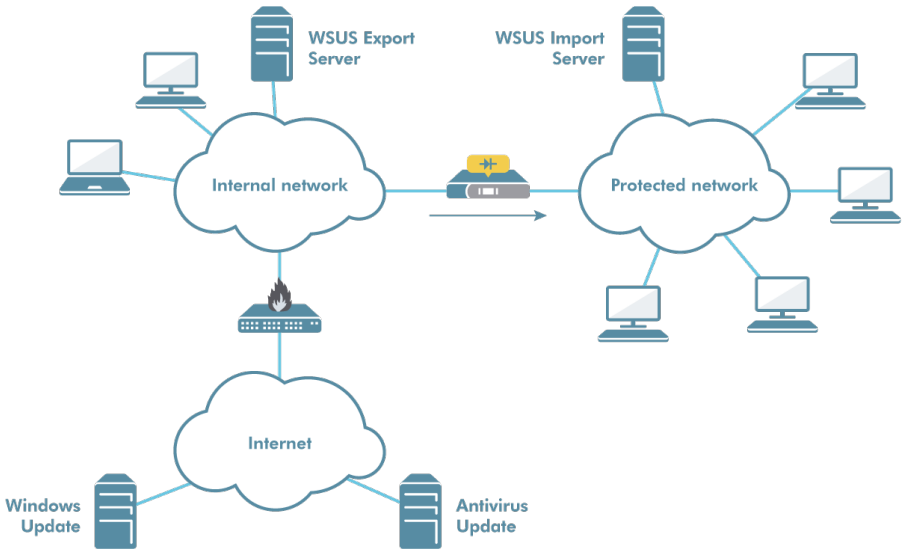
Solution 1

Data Diode Ensures One-Way Communication

The update can be conducted securely by using a data diode that ensures unidirectional communication. The data diode is connected in a way that secures that information can be imported into the system, but since no traffic can be transferred in the opposite direction, information leakage is not possible.

What must be remembered is that a data diode does not have any function that prevents arbitrary information from entering the protected system. The server that receives the update package must therefore, with the help of digital signatures, ensure the accuracy of update packages before they are allowed to be distributed to other systems in the environment.

The WSUS Export server has control of which updates that are installed. You have the opportunity to select and install update packages after ensuring that the update packages you would like to install can be imported and installed in the various systems in ICS/SCADA. This assurance is achieved either by testing the systems in a separate test environment or by receiving this information from the subcontractors who have delivered the systems to ICS/SCADA. Updates can be scheduled to a time when availability is less critical and when down-time can be accepted.

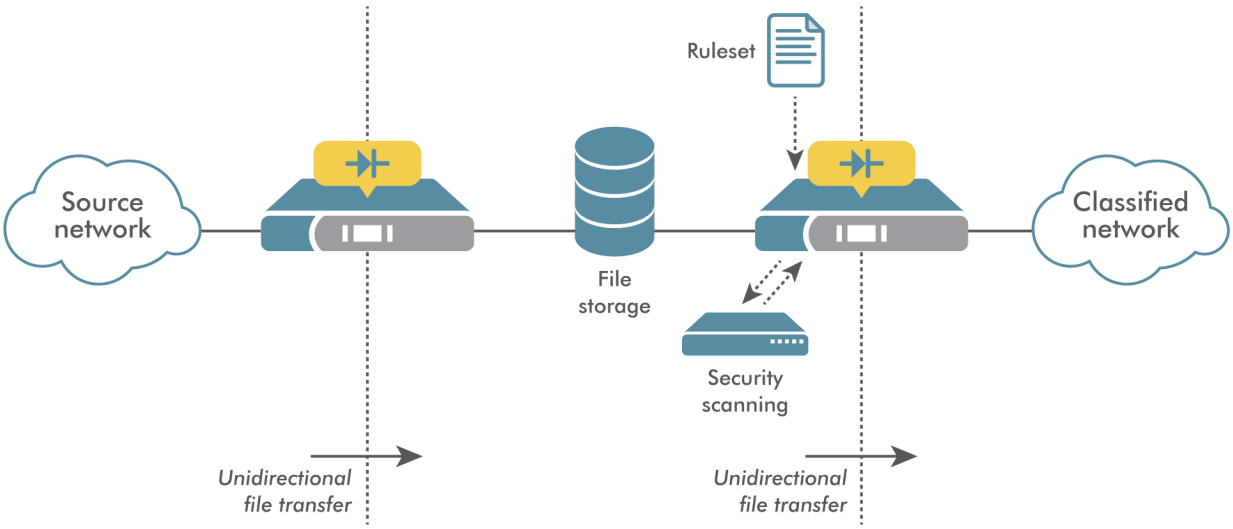


Solution 2

File Sanitation Ensures that the Update is Free of Malicious Code

To further ensure that the update has not been manipulated, the import of update packages can be conducted through file sanitation consisting of two data diodes and a server for antivirus scanning. The file sanitation conducts an independent control making sure that the update is valid. However, even in this case it is best to let the receiving WSUS Import Server verify the signature and thereby get another control of the accuracy of the update.

File santitation can also be used for importing other types of files, e.g. signature files for antivirus software, update packages for Linux-based systems and import of completely arbitrary files. Control and steering of which update packages that are installed is managed in the WSUS Export Server - the same solution as for importing a data diode (see solution 1).



Advantages

Maintained Integrity and Full Control

This solution enables the import of update packages without risking information leakage. Since the integrity of the update packages is controlled in a protected environment, the risk of getting unwanted malware in the systems is minimised. If you choose to import through file sanitation, the integrity of the update is checked by two independent security mechanisms which provide a good defense-in-depth.

As only the updates that have been tested and approved are let into the system, you have complete control over which updates that are allowed. By doing this, updates that otherwise risk interfering the availability of the system are avoided.

advenica

Advenica provides expertise and world-class high assurance cybersecurity solutions for critical data in motion up to Top Secret classification. We enable countries, authorities and companies to raise information security and digitalise responsibly. Founded in 1993, we are EU approved to the highest level of security. Our unique products are designed, developed and manufactured in Sweden.

Read more at advenica.com

ISO 9001 CERTIFIED
ISO 14001 CERTIFIED