TLP:WHITE

REPORT:

Recommended Practice: Updating Antivirus in an Industrial Control System

Irregular Issuance Report

IR-18-214 NUMBER

August 2, 2018 DATE

Recommended Practice: Updating Antivirus in an Industrial Control System

NCCIC

TLP:WHITE

REPORT:

Recommended Practice: Updating Antivirus in an Industrial Control System

Irregular Issuance Report

IR-18-214 NUMBER

August 2, 2018 DATE

Table of Contents

Figures

Acronyms

AV	antivirus
CRC	cyclic redundancy check
DMZ	demilitarized zone
DODIN APL	Department of Defense Information Network Approved Products List
HMI	human-machine interface
ICS	industrial control systems
IT	information technology
LAN	local area network
OT	operations technology
WSUS	Windows Server Update Services

Irregular Issuance Report

Recommended Practice: Updating Antivirus in an Industrial Control System

1. Overview

When properly deployed and up-to-date, antivirus software is an important part of a defense-in-depth strategy to guard against malicious software (malware) in industrial control systems (ICS)[1]. Antivirus is widely used in both ICS and information technology (IT) systems since it is an effective defensive measure against malware. The term "antivirus" covers anti-malware applications, which are not limited to defending only against viruses, but also other forms of malicious software.

In business IT environments, it is common practice to configure each antivirus client to update directly from the antivirus vendor or to update from the organization's servers, located in a secured subnet within the enterprise network (which get their updates from the antivirus vendor).

ICS and IT systems should be separated by an ICS demilitarized zone (DMZ), which should contain only the ICS servers that are accessible from the IT network[2]. Maintaining separation between general IT and ICS systems makes keeping antivirus software up to date more complicated and requires a different antivirus update method.

2. Antivirus Update Strategies

The recommended secure network architecture for ICS (Figure 1) places the antivirus, Windows Server Update Services, and patch server(s) in the control center LAN DMZ[3]. In this architecture, each level should only send or receive traffic to a directly adjacent level. This precludes the AV/WSUS/patch server from communicating directly with either the vendor antivirus servers (which are outside of the organization entirely) or the organizational antivirus servers (which are normally in the enterprise network).

Restricting the flow of data only to adjacent zones complicates the antivirus update process, so we need a better method. One method is to download the updates from the vendor antivirus servers to a dedicated host, write the updates to removable media, and use that media to update the AV/WSUS/patch server. Although at first glance this method appears to be time consuming, in practice, it is not. If the asset owner uses this method, it is important to take precautions to reduce the risk of introducing malware or otherwise compromising the ICS. This would include verifying that the update source is legitimate, that the hash values of the updates are correct, and that staff members handle distribution media securely. Asset owners should also ensure that staff members handle media in accordance with the organization's removable media policy and other guidance.

---

[1] Keith Stouffer, Victoria Pillitteri, Suzanne Lightman, Marshall Abrams, Adam Hahn, NIST Special Publication 800-82 Revision 2, Guide to Industrial Control Systems (ICS) Security: Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC): recommendations of the National Institute of Standards and Technology. (U.S. Dept. of Commerce, National Institute of Standards and Technology, 2015), 6-39.

[2] Ibid, 5-6

3 Industrial Control Systems Cyber Emergency Response Team, Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies, (U.S. Department of Homeland Security, 2016), 17.

Recommended Secure Network Architecture

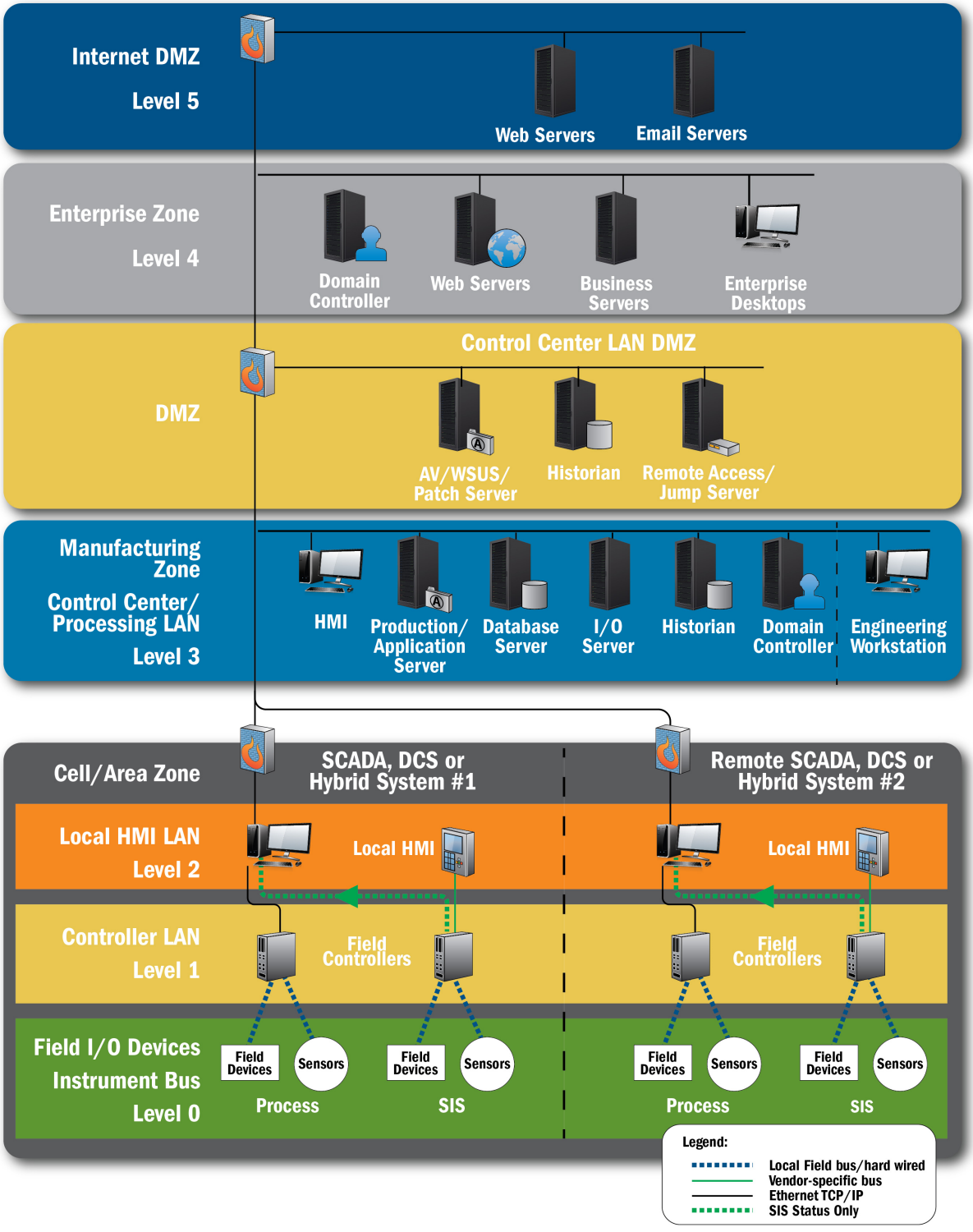

Figure 1. Recommended secure network architecture.

This method of transferring antivirus updates uses the following steps:

- Verify the source of the update.
- Download the update file(s) to a dedicated host (server or workstation).
- Scan the downloaded file(s) for malware.
- Verify the cryptographic hash of each downloaded file(s).
- Scan the removable media for malware or other unexpected data before use to verify its integrity. The safest options are to securely erase the removable media and reformat the drive with the appropriate file system (for flash or magnetic media) or to use a new CD or DVD (for optical media) for each update.
- Write the file(s) to the removable media. Dedicate this media exclusively for updates.
- Lock the media so others cannot write to it.
- Load the media into the test environment and verify that it has no adverse impact to the test system.
- Re-scan the media for malware or other unexpected data to verify that nothing transferred to the removable media from the test environment host.
- Install the update on a non-critical endpoint or segment of the system and verify that it has no adverse impact to the production system.
- Install the update on the remaining hosts.
- Monitor the system for any unusual behavior and verify proper operation of the ICS.

This method, informally known as “sneaker net,” is common in air-gapped networks. While this method is more labor intensive than an automatic chaining of updates, it is not prohibitively time-consuming.

Another method is to automatically “daisy chain” the updates. In this method, the update server in the control center LAN DMZ automatically takes its updates from another server in the enterprise zone, which, in turn, automatically gets it updates from the antivirus vendor’s servers.

3. Considerations

The verification of the update and its source, along with the testing of updates, is very important. Attackers have compromised update servers and “spoofed” update sources and placed malware on those servers disguised as updates; these malicious updates then compromised the systems of users who thought they were downloading legitimate updates. Verifying the update requires more than merely checking the URL or the source IP address of the vendor; asset owners must also verify that each file used in the update is legitimate by verifying that the cryptographic hash for the file is correct.

Automatic updates often have no means of integrity checking other than the cyclic redundancy check (CRC) in the application or the communication protocol. A check of the cryptographic hash of the update provides greater assurance that no one has tampered with the update file. Although it is possible for an attacker to compromise an antivirus vendor’s web site and replace both the update file and the cryptographic hash value, it would require more effort from the attacker, and the vendor would more likely catch and prevent the attempt. This may affect the choice of an antivirus solution. Asset owners should ensure that they can manually update the particular AV application.

Another issue that arises from chaining automatic updates is that staff might not follow the organization’s change management process. For many products, automatic updates are convenient and easy to configure, which makes ignoring change management procedures

very tempting for busy support personnel. Since ICS environments are very sensitive and the impacts of downtime can be serious, it is important for staff to follow strict change management procedures and update antivirus software when operations are minimally impacted. Asset owners should require this as part of a facility's regular maintenance.

Although antivirus software is not commonly thought of as being part of an organization's supply chain, it is. All software and firmware should be reviewed as part of the product evaluation because either one could be an attack vector. In 2014, a Chinese company installed malware on handheld scanning devices and in their updates in the ZombieZero campaign[4]. Preferably, an organization should have a program to evaluate vendors and their products to ensure that they meet operational and security criteria before adding them to an approved products list. Examples of this include the FIPS 201 Evaluation Program, GSA IT Schedule 70, and the Department of Defense Information Network Approved Products List (DODIN APL). The specific criteria and process of a product evaluation program should vary to meet the organization's needs and capabilities.

Although an antivirus client normally resides on the same host as other applications, this is not always the case. An antivirus scanner can be a designated computer that can "reach out" to other hosts and scan them remotely; however, the level of protection may vary and the scanning computer will need sufficient access to each scanned host. This also limits the effectiveness of antivirus. Since there is not a client always functioning on endpoints and because scans occur at intervals, the time between scans is a gap in protection.

The recommended secure network architecture diagram (Figure 1) depicts the AV/WSUS/patch server as a single server hosting three separate applications. This increases the risk of a compromise of either the server's operating system or the applications. If possible, these applications (AV/WSUS/patch) should reside on their own hosts, either physical or virtual, and the hosts hardened and traffic restricted.

In addition, many "next-generation" firewalls and intrusion prevention systems can inspect traffic and block detected malware from traversing a network, which prevents the malware from infecting endpoints. This, however, must be a configured capability of the device.

4. Test and Validation

Regardless of the configuration, there is always the possibility of an incompatibility or constraint having an adverse impact to the system, so testing is prudent. It is also important to back up any production endpoint (if possible) before updating it. If there is an adverse impact from the update, it will be easier and faster to recover from it with a backup. Asset owners should document the transfer and testing of updates as part of a comprehensive change management program. This should be a written procedure and staff tasked with performing updates.

Testing is a critical step since updates can adversely affect ICS environments; there have been cases where ICS applications have malfunctioned due to the installation or updating of antivirus software. Since antivirus scanning can significantly increase CPU and/or memory utilization, it can interfere with applications and processes on servers or workstations that have outdated or otherwise insufficient hardware. This is one reason why it is important to maintain test environments that closely approximate the production environments. Updates should be installed on a test system and the proper operation of the system checked for adverse impacts or anomalous behavior first. If there are no issues, deploy the update into operational systems in order of least criticality: first, the corporate IT network; next, the ICS DMZ; and finally, the ICS network. In each operational system, update non-critical assets first since any adverse impact would less likely interrupt or otherwise degrade operations. For example, update the backup HMI

4 Kelly Higgens, "Chinese Hackers Target Logistics & Shipping Firms With Poisoned Inventory Scanners." Dark Reading, UBM Technology Group, 2014.

server before the primary HMI. Some organizations forego having a test environment and roll out updates in the IT and OT production systems. Unfortunately, this increases the risk of an adverse impact because there are significant differences in the makeup of IT and OT systems. An IT system is simply not an accurate reflection of an OT system, so an accurate test environment is important.

The purpose of updating antivirus software is to ensure a higher level of protection. The resulting higher level of protection reduces downtime and other adverse impacts that are the consequences of a compromise of the ICS. The method should be tailored to the environment to support both the operational and security needs of the organization, but it should always include verification of the updates, maintain separation of levels to support defense in depth, and provide adequate testing of each update.