issa | INTERNATIONAL SOCIAL SECURITY ASSOCIATION

Section on Machine and System Safety

Carry out updates safely

Indispensable even in small businesses!

Factsheet Nº 4

issa INTERNATIONAL SOCIAL SECURITY ASSOCIATION

Section on Machine and System Safety

Carry out updates safely

Indispensable even in small businesses!

Factsheet
Nº 4

A real-life example

The toolmaker „Hammer and Chisel“ is a medium-sized enterprise with 20 employees at two production sites. In two-shift operation, they produce prototype and series tools, among other things. Its machinery includes various machines, mostly connected to the company's own network. The machines can even be monitored across locations via the internet. For each of the machines, there is a master agreement with the respective machine manufacturer or supplier, which regulates, among other things, in which cases a software update of the integrated components must be carried out. It also specifies who is responsible for the new update, how exactly a software update may be installed on the machine and which final release tests ensure the safe use of the machine after the update is installed.

In the present example, the toolmaker was informed by a supplier that a security vulnerability had been discovered on a machine that would allow an attacker to operate the lathe outside the maximum permissible speed range without shutting down the machine. The toolmaker's impact analysis showed that as an initial measure, the affected machine could continue to be operated without any network connection, as this meant that there was no possibility for an attacker to exploit the security vulnerability. After testing and release of the new software by the machine manufacturer, the software update could be transferred to the affected machine in close coordination with the toolmaker. Before the machine was put into operation again, a complete function test was carried out. This ensures that all functionalities and safety functions work correctly. Of course, an approval protocol was prepared and signed on the course of the new installation and commissioning. Since there was a defined process for installing a software update in the company, everyone who was involved knew what to do in such a case. Furthermore, the downtime of the machine could be reduced to a minimum.

Using an internal process makes a software update easy and safe in your company too.

Why are software updates so important?

Nowadays, almost every machine has integrated software. The number of code lines within the programs used is constantly increasing. For this reason, it is not surprising that as a rule, every software delivered contains undiscovered errors that only become known after it has been placed on the market.

Furthermore, more and more machines have digital interfaces and communicate with other participants. Often, communication is shifted beyond the internal networks to the internet. This happens especially when production is located at several sites or when remote maintenance is to be carried out.

If an error is discovered in the software used that can lead to an unauthorised person being able to access the machine, this is called a security vulnerability. Depending on the criticality, such a vulnerability must be closed very quickly, which can usually only be guaranteed by a new software version, the update.

What should be considered when a security vulnerability becomes known?

Every company should have an internal process for dealing with newly discovered software errors. As a rule, this starts with an impact analysis to determine the criticality of the effect of the error.

Then, depending on the classification made, measures should be taken to ensure the safe continued operation of the machine until a software update is available.

What should be considered when updating the software?

Software updates for your machines may only be installed if they have been approved by the respective machine manufacturer. If the release is available, it should be clearly regulated who in your company may initiate the installation and who will carry it out.

After installation is complete, check that all machine functions are being carried out correctly. To avoid unintended effects of the update, it is recommended to also test those functions that were not the subject of the update.

Further information

1 **Software updates – a cornerstone for IT-security:** https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Updates-Browser-Open-Source-Software/Wichtige-Softwareupdates/wichtige-softwareupdates_node.html

2 **Federal Office for Information Security:** www.bsi.bund.de/EN

3 **Government of Canada: Cyber security for small businesses: Why software updates are essential:** https://www.getcybersafe.gc.ca/en/blogs/cyber-security-small-businesses-why-software-updates-are-essential

4 **Trusted Computing Group:** https://trustedcomputinggroup.org/resource/tcg-guidance-for-secure-update-of-software-and-firmware-on-embedded-systems/

10 tips for safe and secure updates in your company

1. Create an internal process for software update management in your company

2. Carry out an risk analysis when a vulnerability becomes known

3. Define measures to ensure safe operation of the machine as long as software updates are not yet available

4. Determine by contract who is responsible for software updates and when they are to be delivered or installed

5. Only install software updates that have been tested and approved by the manufacturer

6. Make a backup of the machine software before installing the update

7. After installing the software update, carry out a complete start-up test of the machine

8. After each update, check that all connections to other machines and software continue to work

9. Instruct and sensitise your employees in the correct handling of security vulnerabilities and software updates

10. When purchasing machines and devices with digital interfaces, make sure that the components used are update-capable

issa | INTERNATIONAL SOCIAL SECURITY ASSOCIATION

Section on Machine and System Safety

ISSA-Section
Machine and System Safety

Dynamostrasse 7–11
D-68165 Mannheim
Germany
Phone: +49 (0) 621 4456 2213
Fax: +49 (0) 621 4456 2190

www.safe-machines-at-work.org

AUVA

BGN
Berufsgenossenschaft
Nahrungsmittel und Gastgewerbe

IFA
Institut für Arbeitsschutz der
Deutschen Gesetzlichen Unfallversicherung

INAIL
ISTITUTO NAZIONALE PER L'ASSICURAZIONE
CONTRO GLI INFORTUNI SUL LAVORO

suva

TECHNICAL UNIVERSITY
OF KOŠICE

UNIVERSITY of
GREENWICH