issa | INTERNATIONALE VEREINIGUNG FÜR SOZIALE SICHERHEIT | IVSS

Sektion für Maschinen- und Systemsicherheit

Updates sicher durchführen

Unerlässlich auch in Kleinbetrieben!

Factsheet
№ 4

Ein Beispiel aus der Praxis

Der Werkzeugbauer „Hammer und Meißel“ ist ein mittelständisches Unternehmen mit 20 Mitarbeitenden an zwei Standorten. Im Zweischichtbetrieb werden unter anderem Prototypen- und Serienwerkzeuge hergestellt. Zu seinem Maschinenpark zählen unterschiedliche Maschinen, die meist ans firmeneigene Netzwerk angeschlossen sind. Über das Internet können die Maschinen sogar standortübergreifend überwacht werden. Für jede seiner Maschinen besteht ein Rahmenvertrag mit dem jeweiligen Maschinenbauer oder Zulieferer, in dem unter anderem geregelt ist, in welchen Fällen ein Software-Update der integrierten Komponenten durchgeführt werden muss. Weiterhin ist festgehalten, wer die Verantwortung für das neue Update trägt, wie ein Update durchzuführen ist und welche Freigabetests im Anschluss einen sicheren Weiterbetrieb der Maschine ermöglichen.

Im vorliegenden Fall wurde der Werkzeugbauer von einem Zulieferer informiert, dass an einer Maschine eine Sicherheitslücke entdeckt worden ist, die es einem Angreifer ermöglicht, die Drehmaschine außerhalb des zulässigen Bereichs der Drehgeschwindigkeit zu betreiben, ohne dass eine Abschaltung der Maschine erfolgt. Die Einflussanalyse des Werkzeugbauers ergab, dass als Erstmaßnahme die betroffene Maschine ohne jegliche Netzwerkverbindung weiter betrieben werden konnte, da so keine Möglichkeit für einen Angreifer besteht, die Sicherheitslücke auszunutzen. Nach erfolgter Testung und Freigabe der neuen Software durch den Maschinenhersteller konnte in enger zeitlicher Absprache mit dem Werkzeugbauer das Software-Update auf die betroffene Maschine übertragen werden. Vor der erneuten Inbetriebnahme der Maschine wurde ein kompletter Funktionstest durchgeführt. Dieser prüft, ob alle Funktionalitäten und Sicherheitsfunktionen korrekt arbeiten. Über den Ablauf der Neuinstallation und der Inbetriebnahme wurde ein Abnahmeprotokoll erstellt und unterzeichnet. Da ein definierter Prozess für das Aufspielen eines Software-Updates im Betrieb vorhanden war, wussten alle Beteiligten, was in solch einem Fall zu tun ist. Die Stillstandszeit der Maschine konnte auf ein Minimum reduziert werden.

Nach einem definierten internen Prozess zu handeln, macht ein Software-Update auch in Ihrem Betrieb einfach und sicher!

Warum sind Software-Updates so wichtig?

Heutzutage verfügt nahezu jede Maschine über integrierte Software. Die Anzahl an Codezeilen innerhalb der verwendeten Programme steigt stetig. Aus diesem Grund ist es nicht verwunderlich, dass in der Regel jede ausgelieferte Software unentdeckte Fehler enthält, die erst nach dem Inverkehrbringen bekannt werden.

Weiterhin verfügen immer mehr Maschinen über digitale Schnittstellen und kommunizieren mit anderen Teilnehmern. Oft wird dabei die Kommunikation über die internen Netzwerke hinaus auf das Internet verlagert. Dies geschieht besonders dann, wenn sich die Produktion an mehreren Standorten befindet oder eine Fernwartung durchgeführt werden soll.

Wird nun in einer verwendeten Software ein Fehler entdeckt, der dazu führen kann, dass eine unberechtigte Person auf die Maschine zugreifen kann, spricht man von einer Sicherheitslücke. Solch eine Schwachstelle muss – je kritischer, desto schneller – geschlossen werden. Dies kann in der Regel nur über eine neue Softwareversion, das Update, gewährleistet werden.

Was ist bei Bekanntwerden einer Sicherheitslücke zu beachten?

Jedes Unternehmen sollte einen internen Prozess haben, welcher den Umgang mit neu entdeckten Softwarefehlern festlegt. In der Regel startet dieser mit einer Einflussanalyse, um die Bedeutung der Auswirkung des Fehlers zu bestimmen.

Im Anschluss sollten dann, abhängig von der vorgenommenen Einstufung, Maßnahmen getroffen werden, die den sicheren Weiterbetrieb der Maschine bis zum Software-Update gewährleisten, so lange noch kein Software-Update vorhanden ist.

Was gilt es bei Software-Updates zu beachten?

Software-Updates für Ihre Maschinen dürfen erst dann installiert werden, wenn sie von dem betreffenden Hersteller der Maschine freigegeben sind. Liegt die Freigabe vor, sollte klar geregelt sein, wer in Ihrem Unternehmen die Installation veranlassen darf und wer sie durchführt.

Nach Abschluss der Installation ist zu prüfen, ob alle Maschinenfunktionen korrekt ausgeführt werden. Zur Vermeidung unbeabsichtigter Auswirkungen durch das Update wird empfohlen, auch solche Funktionen zu testen, die nicht Gegenstand des Updates waren.

Weitergehende Informationen

1 **Software-Updates – ein Grundpfeiler der IT-Sicherheit:**
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 **Bundesamt für Sicherheit in der Informationstechnik:**
www.bsi.bund.de/DE/

3 **Transferstelle IT-Sicherheit im Mittelstand (TISiM):**
https://www.sicher-im-netz.de/TISiM

10 Tipps für sichere Updates in Ihrem Unternehmen

1. Schaffen Sie einen internen Prozess für das Software-Update-Management in Ihrem Unternehmen
2. Führen Sie bei Bekanntwerden einer Sicherheitslücke eine Risikoanalyse durch
3. Legen Sie Maßnahmen fest, die einen sicheren Betrieb der Maschine gewährleisten, auch bevor es Software-Updates gibt
4. Legen Sie vertraglich fest, wer für Software-Updates zuständig ist und wann diese geliefert bzw. installiert werden sollen
5. Installieren Sie nur geprüfte und freigegebene Software-Updates
6. Erstellen Sie eine Sicherungskopie der Maschinensoftware, bevor Sie das Update installieren
7. Führen Sie nach der Installation des Software-Updates einen kompletten Inbetriebnahmetest der Maschine durch
8. Prüfen Sie nach jeder Aktualisierung, ob alle Verbindungen zu anderen Rechnern und Software weiterhin funktionieren
9. Unterweisen und sensibilisieren Sie Ihre Mitarbeitenden im richtigen Umgang mit Sicherheitslücken und Software-Updates
10. Achten Sie beim Kauf von Maschinen und Geräten mit digitalen Schnittstellen darauf, dass die verwendeten Komponenten updatefähig sind

issa | INTERNATIONALE VEREINIGUNG FÜR SOZIALE SICHERHEIT | IVSS

Sektion für Maschinen- und Systemsicherheit

IVSS Sektion
Maschinen- und Systemsicherheit

Projektgruppe Digital Manufacturing

Dynamostraße 7–11 · 68165 Mannheim
Deutschland
Telefon: +49 (0) 621 4456 2213
Fax: +49 (0) 3212 1419 443

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