konradin Industrie | Das Kompetenznetzwerk der Industrie

Ausgabe 03 (Juni) | 2022 wirautomatisierer.de

elektro AUTOMATION

Konzepte Systemlösungen Komponenten

Intelligente Automation und Robotiktrends
Messe Automatica
» Seite 14

SPS als Smart Service in der Cloud
Cloudtechnologie
» Seite 21

SPS liefert Daten zur Analyse
Steuerungstechnik
» Seite 30

„Nur eine ‚sehende' Maschine kann sich anpassen"
Andreas Waldl, Product Manager Integrated Machine Vision, B&R
» Seite 48

TITELSTORY

Leitfaden zur Modellierung von Schnittstellen mittels OPC UA
» Seite 24

Schlüsseltechnologien für die Smart Factory

Security-Tools von Prosoft sorgen für stabile OT-Systeme

Sicheres Datenhandling in der OT

Der Grad von Vernetzung und Digitalisierung in der Produktion bietet in Deutschland gerade im KMU-Umfeld noch viel Potenzial. Im Jahr 2018 lag die Digitalisierungsquote erst bei 30 % respektive 20 % bei kleineren Unternehmen. Durch die konsequente Digitalisierung kann laut McKinsey der Wirtschaftsstandort Deutschland bis 2025 insgesamt 126 Mrd. Euro zusätzlich an Wertschöpfung erreichen und Standortnachteile abfedern. Immerhin 25 % der Wertschöpfung entfallen in Deutschland auf das produzierende Gewerbe.

Robert Korherr, Geschäftsführer der Prosoft GmbH in Geretsried

IM ÜBERBLICK

Werden Produktionsumgebungen nicht gegen mobile Speichergeräte abgeschottet, helfen sogenannte Datenschleusen, um die Sicherheit zu gewährleisten.

Das Thema Cybersecurity gehört aber zu den Hemmnissen, die Unternehmen davon abhalten, Digitalisierung und Vernetzung weiter voranzutreiben. Kein Wunder, sind doch die Hidden Champions der deutschen Industrie Experten auf ihrem Gebiet, aber längst nicht in jedem Fall auch noch für den Bereich Cybersecurity in der Operational Technology (OT). Physisch getrennte (air-gapped) Produktionsumgebungen werden seltener, sind jedoch immer noch ein Garant für hohe Verfügbarkeit und Schutz vor Angriffen und Manipulationen. IT und OT nutzen immer häufiger dieselben Standards und Infrastrukturen. Trotzdem hängt die OT bei der IT-Sicherheit allgemein noch hinterher.

Defense-in-Depth-Ansatz

Eine Studie das SANS-Instituts aus 2018 zeigt, dass 25 % der Angriffe auf Unternehmen auf Beschäftigte zurückzuführen sind. Weitere 16 % auf Service-Provider. Insgesamt passieren also 41 % aller Attacken innerhalb der Firewall. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) empfiehlt mit dem amerikanischen Defense-in-Depth-Ansatz sowohl einen Perimeterschutz (Abschottung nach Außen) als auch eine interne Unterteilung in Bereichen durch Bildung von abgeschotteten Zonen in der Produktion. Gerade Innentätern und Service-Providern ist mit den üblichen Maßnahmen zur Cybersicherheit nicht beizukommen. Hier empfiehlt das BSI spezielle technische und organisatorische Maßnahmen (TOM).
Neben all den verfügbaren und möglichen Vektoren für Cyberangriffe darf man analoge Wege nicht unberücksichtigt lassen. Malware kann über infizierte USB-Sticks von Mitarbeitern, Servicetechnikern und Besuchern problemlos die Firewall umgehen. Auch isolierte Produktionsumgebungen werden aus verständlichen Gründen nicht gegen mobile Speichergeräte abgeschottet. Hier helfen, ähnlich wie bei den Security-Checks am Flughafen, sogenannte Datenschleusen, auch als Wechseldatenträgerschleusen bezeichnet.

Bild: Prosoft

Cybersecurity gehört zu den Hemmnissen, die Unternehmen bislang davon abhalten, die Digitalisierung einzuführen.

Datenschleusen

Dabei handelt es sich um Kiosk-Systeme, die, am besten unter Aufsicht, die von Besuchern mitgebrachten Speichergeräte durchleuchten, d. h. auf Malware überprüfen. Hierbei verwenden alle wichtigen Hersteller von Datenschleusen sogenannte Anti-Malware-Multiscanner. In einem Malware-Multiscanner werden mehrere Anti-Viren-Engines gebündelt. Das bedeutet, dass ein mitgebrachtes Speichergerät nicht nur mit einer Anti-Viren-Engine überprüft wird, sondern je nach Hersteller mit mindestens zwei bis maximal rund 30 AV-Lösungen. Das ist notwendig, da laut BSI täglich über 300.000 neue Malware-Varianten entwickelt werden. Um die Wartezeit der Besucher während des Scan-Vorgangs mit dem Anti-Malware-Multiscanner so gering wie möglich zu halten, ist die parallele, also gleichzeitige Überprüfung mit allen integrierten Scannern sinnvoll, besonders wenn es sich um die Überprüfung mit bis zu 30 AV-Engines handelt.

Besucher, die einen sensiblen IT- oder OT-Bereich betreten wollen, müssen also mitgebrachte Datenträger überprüfen lassen. Vor der Prüfung fragt das System nach den Daten des Besuchers und des Mitarbeiters im Unternehmen und protokolliert alle Angaben. Sind alle Daten auf dem Datenträger ohne Beanstandung, ist mit einer Wahrscheinlichkeit von über 99,5 % keine Malware mehr auf dem Datenträger.

Datei-Desinfektion

Die Restrisiken sind sogenannte Zero-Day-Exploits. Darunter versteht man bisher unbekannte Sicherheitslücken, die von Angreifern bereits erfolgreich ausgenutzt werden. Erkennt die Heuristik in den Malware-Scannern nicht ausführbaren Programmcode oder Befehlsaufrufe, ist für die Zero-Day-Exploits der Weg frei. Die Option Datei-Desinfektion in Datenschleusen schützt auch wirksam gegen diese Restrisiken. Eine Datei-Desinfektion arbeitet nach der Regel, dass alle Dateitypen, die Schadcode enthalten können, auch mit Schadcode infiziert sind. Riskante Dateitypen wie Audio- und Videodateien und Office-Dokumente, die eingebettete Malware enthalten können, werden deshalb ausnahmslos in harmlose Dateien umgewandelt und eventuelle Links wie sie auch in PDFs noch enthalten sein können, werden unschädlich gemacht.

Sichere Datenübertragung ins Produktionsnetzwerk

Wurde ein mobiler Datenträger mit der Datenschleuse überprüft, kann der Besucher entweder sein Speichergerät mitnehmen oder auf einen vom besuchten Unternehmen zur Verfügung gestellten mobilen Datenträger kopieren und nur damit den sensiblen IT-Bereich betreten. Eine andere Option ist es, die Daten auf dem mitgebrachten Speichergerät nur in die Datenschleuse zu kopieren und dort auf Malware überprüfen zu lassen. Diese Funktion eröffnet auch die Möglichkeit, dass Besucher nicht auf das Scan-Ergebnis warten müssen. Die gescannten Dateien werden dann über Secure File Transfer in eine Art Tresor übertragen, der sich noch im IT-Netzwerk befindet und gespeichert. Dabei werden nur virenfreie Daten über eine sichere Verbindung in den Datentresor transferiert. Alle Dateien im Datentresor werden immer mit den neuesten Anti-Malware Signaturen überprüft.

Bild: Prosoft

Scanner für mobile Datenträger.

Produktionsnetzwerk bleibt weiterhin abgeschottet

Da der Datentresor (Vault) sich außerhalb der OT befindet, bleibt ein isoliertes Produktionsnetzwerk weiterhin abgeschottet. Die über die Datenschleuse gescannten Dateien werden mithilfe von individuellen Codes aus dem Datentresor angefordert und sicher übertragen. Falls gewünscht, kann der Dateizugriff erst nach einem voreingestellten Zeitraum erlaubt werden. Damit verhält sich der Datentresor wie eine Art interne Sandbox, die ebenfalls neue Dateien über eine Zeitspanne testet. Eine granulare Benutzerverwaltung legt die Art der Authentifizierung und der Dateitypen fest, auf die zugegriffen werden kann. Wichtig dabei ist, dass Gäste und Mitarbeiter immer nur auf ihre Dateien zugreifen können. Verlassen die Gäste das Unternehmen, werden auch ihre Dateien gelöscht.

Anti-Malware-Multiscanner

Der amerikanische Hersteller OPSWAT bietet mit MetaDefender Kiosk eine Datenschleuse, die auf Basis eines Anti-Malware-Multiscanners mit mind. 8 bis 30+ AV-Engines und Datentresor eine Komplettlösung anbietet. Der Hersteller Presense liefert mit Provaia für Industriekunden ebenfalls eine Datenschleuse, die als Version Janus im Auftrag des BSI auch für Bundesbehörden empfohlen wird. (ge)

www.prosoft.de

INFO

Weitere Informationen über die Metascanner:

hier.pro/1P1b0