IT&Production
AKTUELLES UND FUNDIERTES FACHWISSEN FÜR IHRE BRANCHE

DOSSIER

IT-SICHERHEIT

IT-Sicherheit: Mission Critical

Patrick C. Prather
pprather@it-production.com

Meldungen zu den teils dramatischen Folgen `erfolgreicher' Hacks auf industrielle Infrastrukturen erreichen uns Redakteure beinahe täglich. Viele dieser Schreiben sollen mit bedrohlichen Statistiken oder konkreten Beispielen anregen, sich mit der IT-Sicherheit auseinanderzusetzen – und natürlich zu investieren. Jedenfalls: Die Bedrohungslage ist ernst, die Folgen eines Cyberangriffs sind manchmal gravierend – und können Unternehmen etwa nach einem Datendiebstahl ins Taumeln oder gar zu Fall bringen. Warum ich Ihnen an dieser Stelle Schilderungen über die jüngsten Vorfälle dennoch erspare? Erstens werden diese Nachrichten mittlerweile schneller von neuen verdrängt, als Sie diese Zeilen lesen dürften. Und zweitens befassen Sie sich ja bereits mit dem Thema IT-Sicherheit, sonst würden Sie nicht gerade durch unser Dossier scrollen.

In industrielle IT-Infrastrukturen gehören Hacker allenfalls auf Einladung, etwa für Penetrationstests. Klingt logisch, ist aber in Wirklichkeit bockschwer zu erreichen. Für hundertprozentigen Schutz eines Netzwerkes müssten Mensch und Technik stets perfekt funktionieren. Doch an beidem hakt es oft genug. Insofern bleibt den Firmen nur, ein Niveau an IT-Sicherheit anzupeilen, das dem (bestenfalls gut kalkulierten) Risiko entspricht – und planvoll darauf hinzuarbeiten. Dazu braucht es die passenden Technologien wie Managementsysteme, Verschlüsselung und Firewalls. Es braucht aber auch IT-Spezialisten, die diese Systeme einrichten und pflegen, intern oder extern. Doch das reicht nicht. Jeder Mitarbeiter muss die Regeln kennen und sie einhalten. Das fängt beim sagenhaften USB-Stick auf dem Parkplatz an und hört beim Zuschieben einer Tür im Werk, R&D und Rechenzentrum noch lange nicht auf. All das macht es so schwierig, sich als Firma wirkungsvoll gegen Hacker abzusichern.

Die Arbeit derjenigen, die diese missionskritische Aufgabe übernommen haben, wollen wir mit diesem Online-Dossier ein wenig erleichtern. Im Grunde sollten das zwar alle Mitarbeiter sein. Aber bis diese so weit sind, unterstützen wir diese Weichensteller mit einem breit gefächerten Informationsangebot von der Prävention über Normen und Standards bis hin zur IT-Forensik.

Informative Lektüre wünscht Ihnen

Patrick C. Prather
Leitender Redakteur, IT&Production

Inhalt

IT&Production – DOSSIER

In unserem Format **IT&Production Dossier** fokussieren wir auf die zentralen Themen aus der Welt der industriellen IT und Fertigungstechnik. Mit diesem Informationsangebot wollen wir es Ihnen so leicht wie möglich machen, sich schnell einen umfassenden Überblick über jeweils einen Toptrend der Branche zu verschaffen. Dazu liefern wir kürzlich veröffentlichte und exklusive Inhalte nicht nur aus der IT&Production, sondern ggf. dem gesamtem Industriemedien-Portfolio des TeDo Verlages. Der Vorteil für Sie: Auf einen Blick sehen sie den Toptrend aus der Perspektive der industriellen IT, der Automatisierer und IoT-Designer, der Gebäudeautomation und der industriellen Bildverarbeitung. Zwei Tipps, wenn Sie mögen: Schicken Sie unser Dossier an Ihre Kolleginnen und Kollegen – und schauen Sie gelegentlich wieder hinein. Wir aktualisieren in regelmäßigen Abständen. ■

Bild: ©scanrail/iStockphoto.com

IT-Sicherheit: Cloud vs. Firmennetz

Noch immer fürchten einige Unternehmen, dass der Betrieb einer ERP- oder CRM-Lösung in der Cloud unsicher ist. Doch die Cloud-Rechenzentren haben als wahre Spezialisten der Datenverarbeitung einige grundlegende Vorteile gegenüber firmeneigenen Infrastrukturen, ein umfassendes Sicherheitskonzept aufzustellen und zu erhalten.

Für eine umfassende Sicherheits-Strategie müssen Unternehmen mehrere Aspekte berücksichtigen - gleich ob sie Daten lokal speichern oder mit einer Cloud-Lösung arbeiten. Diese sind:

- Objektsicherheit (Intrusion Protection)
- Ausfallsicherheit (High Availability)
- Backup-Strategie (Disaster Recovery)
- Sicherheit vor verschiedenen digitalen Angriffen (Security)

Zusätzlich zu den hier genannten Aspekten gehören auch das Rechte-Management (Access Control) sowie ein Datenschutzkonzept in die Betrachtung eines vollständigen Sicherheitskonzeptes. Da es sich hierbei aber um konzeptionelle Fragen handelt, bei denen es keinen signifikanten Unterschied macht, wo Software und Daten gehostet werden, sind Rechte-Management und Datenschutz nicht Thema der nun folgenden Gegenüberstellung.

Objektsicherheit

Laut polizeilicher Kriminalstatistik wird in Deutschland durchschnittlich alle fünf Minuten ein Einbruch verübt. Der Schutz der eigenen IT-Infrastruktur schließt daher physikalischen Objektschutz mit ein - sei es vor Diebstahl, Vandalismus oder Sabotage. Denn gelangt ein Angreifer erst einmal in einen Serverraum - und somit hinter die Firewall - sind Angriffe auf die IT-Infrastruk-

Bild: ©matejmo/iStockphoto.com

Die Werkzeuge zur IT-Sicherheit entfalten nur bei sachkundigem Betrieb ihre bestmögliche Wirkung. Diese Pflege auszulagern, kann dringend benötigte IT-Ressourcen für andere Projekte freisetzen.

tur einer Firma wesentlich einfacher zu bewerkstelligen, etwa durch Einspielen von Schadsoftware oder dem Mitschneiden von Netzwerk-Traffic. Moderne Cloud Rechenzentren haben für ihre Serverräume ein Sicherheitskonzept in puncto Zutrittskontrolle und Einbruchschutz. Mechanischer Schutz, Videoüberwachung, Vier-Augen-Prinzip, Sicherheitspersonal rund um die Uhr, Kontrolle an neuralgischen Zugängen: All das ist in den großen Rechenzentren in der Regel umgesetzt. Hinzu kommen eine permanente Kontrolle der Raumtemperatur in Serverräumen, Überspannungsschutz der Hardwarekomponenten, Schutz vor Schäden durch Feuer, Wasser, CO2 und so weiter. Hier kann jede Firma für sich selbst beantworten, ob der Schutz des eigenen Rechenzentrum den genannten Maßnahmen ebenbürtig ist.

Ausfallsicherheit

Stromausfall, Netzausfall, Hardwarecrashs oder Feuer: Die Gefahr, dass eines dieser Ereignisse ein Unternehmen irgendwann einmal trifft, ist nicht zu unterschätzen. Sicherheit bedeutet deshalb auch, auf diese Szenarien vorbereitet zu sein. Was passiert, wenn an einem Montagmorgen nach einem Stromausfall oder einem Hardwareausfall das ERP-System eines Unternehmens wegbricht? Der Webshop ist offline, die Produktion steht still und mit jeder Stunde Downtime wird sowohl der finanzielle als auch der Image-Schaden größer. Beeinflusst solch ein Szenario den laufenden Betrieb nicht, spricht man von einem hochverfügbaren, ausfallsicheren System. In der Praxis müssen dafür alle Komponenten sowie die gesamte IT-Infrastruktur mindestens doppelt vorhanden sein. Das heißt: sämtliche Hardware gibt es zwei Mal und sie ist räumlich voneinander getrennt aufgebaut, zwei Stromleitungen zu unterschiedlichen Trassen sind verlegt und es gibt zwei Verbindungen ans Netz. Aktuelle Rechenzentren sind so geplant, dass Sie dem Grundsatz von hochverfügbarer IT-Infrastruktur Rechnung tragen. Redundanzen gehören zum Standard und zudem stehen Administratoren für den Fall einer Panne rund um die Uhr zur Verfügung. Darüber hinaus sind solche Rechenzentren in Brandabschnitte unterteilt, um selbst bei einem Feuer noch verfügbar zu bleiben. Einen Schritt weiter gehen Betreiber, wenn sie die IT-Infrastruktur an zwei komplett unterschiedlichen Standorten betreiben. Geo-Redundanz sichert Verfügbarkeit auch dann, wenn ein Cloud-Rechenzentrum einmal komplett ausfallen sollte. Für die meisten Unternehmen ist Hochverfügbarkeit folglich über die Cloud wesentlich einfacher und günstiger zu realisieren, als im eigenen Haus. Alleine das notwendige Know-How für Konzeption und Betrieb ist enorm anspruchsvoll. Spätestens die Umsetzung von Geo-Redundanz ist definitiv zu aufwändig und zu teuer.

Backup-Strategie

Wenn im Produktivsystem plötzlich Daten korrumpieren, etwa nach einem Virus, einem falsch eingespielten Update oder einem Hardware-Fehler, hilft eine gespiegelte IT-Infrastruktur nicht weiter. In diesem Szenario sollte die IT-Administration möglichst schnell ein vollständiges Backup zurückspielen. Das Backup kommt dabei wahlweise aus der Cloud oder - heute immer noch üblich - über Bandlaufwerke und Magnetbänder, die etwa in Bankschließfächern gelagert werden. Je nach entstandenem Schaden lässt sich ein Restore für Unternehmen kaum innerhalb von ein bis zwei Tagen bewerkstelligen, wie es wünschenswert wäre. Bei Schäden an wichtiger Hardware muss sogar oft erst nachbestellt werden. Viele Komponenten haben sehr lange Lieferzeiten oder benötigen teure Wartungsverträge mit Ersatzteilgarantien und entsprechenden Reaktionszeiten. Außerdem ist auch hier umfangreiches technisches Know-How notwendig. Eine Disaster Recovery in unter 48 Stunden im eigenen Rechenzentrum ist für Unternehmen eine enorme Herausforderung. In Cloud-Rechenzentren gibt es Hardware-Redundanz ohnehin, sowie auf Disaster Recovery spezialisierte Systemadministratoren. Daten werden hier aktuell und Geo-Redundant synchronisiert. So ist es im Schadensfall oft nur ein Routine-Eingriff, ein

Backup von dem Zeitpunkt vor besagtem kritischen Ereignis einzuspielen. Spezialisierte Rechenzentren sichern ihren Nutzern eine Wiederherstellungszeit von rund zehn Stunden zu - mithilfe weiterer Cloud-Services noch weniger.

Schutz vor digitalen Angriffen

Anders als bei den ersten drei Szenarien, die sich eher selten ereignen, erfolgen digitale Angriffe auf Unternehmen und deren IT-Infrastruktur mehrmals pro Tag. Schutz vor dieser Gefahr bieten:

- Ein sicheres Netzwerk und eine Firewall
- Schnelles Schließen von Sicherheitslücken via Updates
- Maßnahmen gegen Social Engineering

Entscheidend ist bei einer Firewall die richtige Konfiguration. Dies setzt viel Erfahrung voraus, besonders wenn Mitarbeiter eines Unternehmens auch von unterwegs oder von zu Hause aus per VPN arbeiten. In Cloud-Rechenzentren sind Netzwerktechniker und System-Administratoren rund um die Uhr zur Stelle. So kann ein Cloud-Provider ungewöhnliche Datenströme oft schneller erkennen und unterbinden. Zugriffe per VPN von externen Netzwerken werden in Rechenzentren eher restriktiv gehandhabt - oder es werden User-spezifische Firewalls eingerichtet und gepflegt. Zwar können Unternehmen, die eine On-Premise Lösung bevorzugen, diesen Schutz auch mit anderen Dienstleistern erreichen. Die Erfolgsaussicht eines digitalen Angriffes auf die Firewall eines Cloud-Rechenzentrum dürfte jedoch geringer ausfallen.

Sicherheitsupdates und Social Engineering

Um Gefahren zu vermeiden, müssen Unternehmen sehr diszipliniert sein und sämtliche Updates für alle Programme regelmäßig einspielen. In Rechenzentren geschieht dies automatisch. Die Zero-Day-Gap für Cloud-Anwendungen ist somit gering. Social Engineering sind Angriffe, die einen PC-Anwender als Einfallstor identifiziert und ausnutzt. Etwa vermeintliche Handwerker, die sich Zugang beispielsweise zu Serverräumen verschaffen. Bei Unternehmen, die Ihre Mitarbeiter nicht kontinuierlich sensibilisieren, sind die Erfolgsaussichten von Social Engineering-Angriffen extrem hoch. Experimente zeigen immer wieder, dass Schadcode auf einem herumliegenden USB-Stick erschreckend oft den Weg ins Firmen-Netzwerk findet. In Cloud-Rechenzentren ist dieses Szenario möglich, aber unwahrscheinlicher: Das Wissen um die gängigen Social-Engineering-Tricks und sonstige Angriffsvektoren wird in Schulungen und Trainings vermittelt. Nimmt man alle hier genannten Sicherheitsaspekte zusammen, ist die Sicherheit in Cloud-Rechenzentren überdurchschnittlich hoch. Hier schlägt der N-Vorteil zu buche, denn Cloud-Rechenzentren schützen nicht nur die eigenen Daten, sondern die einer sehr großen Zahl an Unternehmen. So profitieren alle Anwender von einmalig hohen Anschaffungskosten für Sicherheitstechnik und sämtlichen erforderlichen Redundanzen. ■

Die Autoren: Torben Nehmer ist Entwicklungsleiter und Marco Niecke ist Technischer Redakteur bei Inway Systems.

www.inway.de

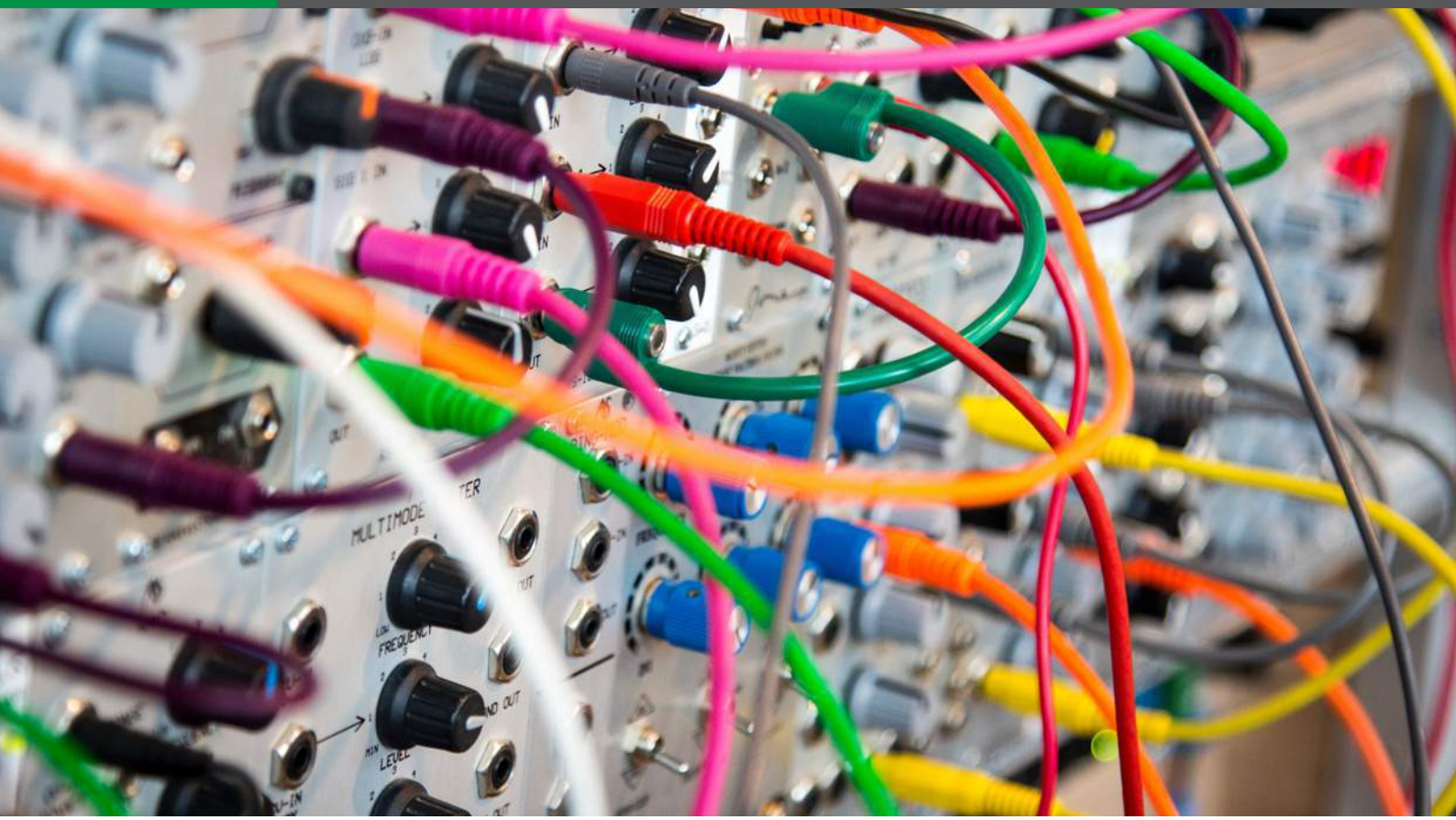


Bild: ©John Carlisle / unsplash.com

Die geringeren Latenzzeiten sind einer der größten Vorteile des Edge Computings gegenüber dem Cloud Computing.

IIoT-Dienste überwachen und absichern

Rechnen ‘on the Edge’

IT-Infrastruktur, Plattformdienste und Software flexibel und bedarfsgerecht beziehen – auf diese Vorteile setzt bereits jedes fünfte Unternehmen aus dem produzierenden Gewerbe. Die Rede ist von cloudbasierten Anwendungen und Diensten. Müssen Daten jedoch quasi in Echtzeit und mit einer geringen Bandbreite übertragen werden, wird der Cloud per Edge Computing eine dezentrale Infrastruktur vorgeschaltet. Um den Betrieb dieser sensiblen IT-Ebene im Werk abzusichern, gibt es spezialisierte Service-Assurance-Lösungen.

Für Anwendungen, die verschiedene Daten aus unterschiedlichen Quellen benötigten und vergleichsweise wenig Bandbreite brauchen, können Cloudlösungen sinnvoll sein. Müssen Datenmengen jedoch schnell oder gar in Echtzeit, mit geringer Latenzzeit und bei wenig Bandbreite, verarbeitet werden, ist Cloud-Computing nicht die optimale Lösung. Dies gilt besonders dann, wenn Informationen aus dem industriellen internet of Things (IIoT) – sei es im Rahmen von Machine-to-Machine-Kommunikation (M2M) oder bei Prozessen in der Smart Factory – übertragen und analysiert werden müssen. Geht es etwa um Maschinen, die schnell und selbstständig Entscheidungen treffen müssen, erweist sich die Verarbeitung ihrer Daten in der Cloud oft als Flaschenhals oder Nadelöhr. Beispielsweise darf es bei autonomen Fahrzeugen nur zu äußerst geringen Latenzzeiten kommen, damit das Auto jederzeit auf unvorhergesehene Ereignisse reagieren kann. Die Zeit, um die Fahrzeugdaten zur Verarbeitung in die Cloud und wieder zurück zu übertragen, ist oft schlicht nicht vorhanden.

Edge- oder Cloudlösung?

Wenn Daten also nahezu in Echtzeit oder bei geringer Bandbreite übertragen werden müssen, ist Edge Computing das Mittel der Wahl. Im Gegensatz zur Cloud zeichnet sich Edge Computing dadurch aus, dass Informationen für ihre Verarbeitung nicht erst von der intelligenten Maschine oder dem Netzwerk in die Wolke und wieder zurück transferiert werden müssen. Die Daten werden dezentral und damit direkt am Entstehungsort, also am Rande des Netzwerks (Edge), verarbeitet. Auf diese Weise verrin-

gern sich Übertragungsstrecke und damit Übertragungszeit. Auch mögliche Fehlerquellen, die während der Übertragung zur Cloud auftauchen können, können durch Edge Computing reduziert werden.

Nicht nur Vorteile

Doch auch Edge Computing hat gewisse Nachteile. So benötigt das Konzept zahlreiche Technologien wie Sensornetze, mobile Datenerfassung, mobile Signaturanalyse, Peer-to-Peer- und Ad-hoc-Vernetzung. Dies macht es für Unternehmen schwierig, die komplette Anwendungs- und Servicekette im IIoT zu überwachen. Doch dies ist wichtig, damit Unternehmen jederzeit Einblick haben, ob Daten von Maschinen und Sensoren im IIoT von Produktions- und Steuerungssystemen korrekt verarbeitet und fristgerecht für weitere Anwendungen und Maschinen bereitgestellt werden. Außerdem benötigen Maschinen und Endgeräte beim Edge Computing einen höheren Schutz vor möglichen Ausfällen und Missbrauch. Denn sie verarbeiten Daten eben direkt und erfordern oft eine hohe Verfügbarkeit für weitere systemabhängige Komponenten. Darüber hinaus erschweren hybride Strukturen, also die gleichzeitige Nutzung von Cloud und Edge Computing, die Überwachung der Datenverarbeitung. Experten gehen allerdings davon aus, dass beide Formen in Unternehmen auch mittelfristig koexistieren werden. Dem Edge Computing wird dann die Aufgabe zukommen, Daten zu bündeln und zumindest ausgewählte Datenteile zur Weiterverarbeitung an die Cloud weiterzuleiten. Laut Analystenhaus IDC könnten die IT-Ausgaben für Edge-Infrastrukturen bis 2020 fast 18 Prozent der Gesamtausgaben für IoT-Infrastrukturen ausmachen.

Belastung für die IT-Struktur

Doch mit jeder Veränderung – egal ob Update, eine neue Verbindung oder eine zu integrierende Drittanwendung – erhöht sich die Komplexität eines hybriden Systems. Zugleich bedeutet die hohe Abhängigkeit einzelner Prozesse im IIoT voneinander, dass ein Ausfall einer Komponente weitaus gravierendere Auswirkungen zur Folge hat. Dadurch steigt der Druck, jederzeit die ungestörte Übertragung und Verarbeitung von Daten zu gewährleisten. Die Bedeutung von Service Assurance, also der Absicherung von IIoT-Diensten durch genaue Überwachung der Servicebereitstellungsinfrastruktur, kann so zu einem erfolgskritischen Faktor werden. Doch gängige Tools zur Netzwerküberwachung reichen oft nicht mehr aus: Monitoring-Tools für einzelne Infrastruktur-Komponenten bieten meist zu wenig Informationen über das gesamte Edge- und Cloud-Computing-System und die Abhängigkeiten zwischen den einzelnen Elementen sowie zwischen internen und externen Ressourcen. Genau dort setzt Service Assurance an. Das Konzept soll einen ganzheitlichen Blick auf die gesamte Servicebereitstellungsinfrastruktur ermöglichen – vom Rand des Netzwerks über das Kernnetz bis in die Cloud. Über Monitoring-Daten und Analysen von Traffic-Daten aus dem hybriden Netzwerk können Unternehmen zudem in Echtzeit sehen, ob Dienste und Maschinen einwandfrei funktionieren und die Datenübertragung gewährleistet ist. Unternehmen sind somit in der Lage, ein besseres Verständnis dafür zu entwickeln, wie IIoT-Geräte und Verbindungen mit dem Netzwerk interagieren. Mögliche Anomalien wie Stör- und Fehlerquellen, die den Geschäftsbetrieb beeinträchtigen, können schneller identifiziert und isoliert werden.

Latenzzeit erfolgskritisch

Die deutlich verkürzte Latenzzeit ist der größte Vorteil des Edge Computings gegenüber Cloud Computing. Doch um diese Potenziale voll nutzen zu können, müssen IT- und Netzwerk-Experten einen transparenten Einblick in die Datenverarbeitung am Rande des Netzwerkes sicherstellen. Durch den Einsatz einer Service-Assurance-Lösung können Unternehmen ihre hybriden Systeme aus Cloud- und Edge-Komponenten vollständig überwachen und potenzielle Störquellen identifizieren. ■

Der Autor Martin Klapdor ist
Senior Solutions Architect
bei Netscout.

www.netscout.com

Vorbereitet auf den IT-Angriff

Notfallplan in Software gießen

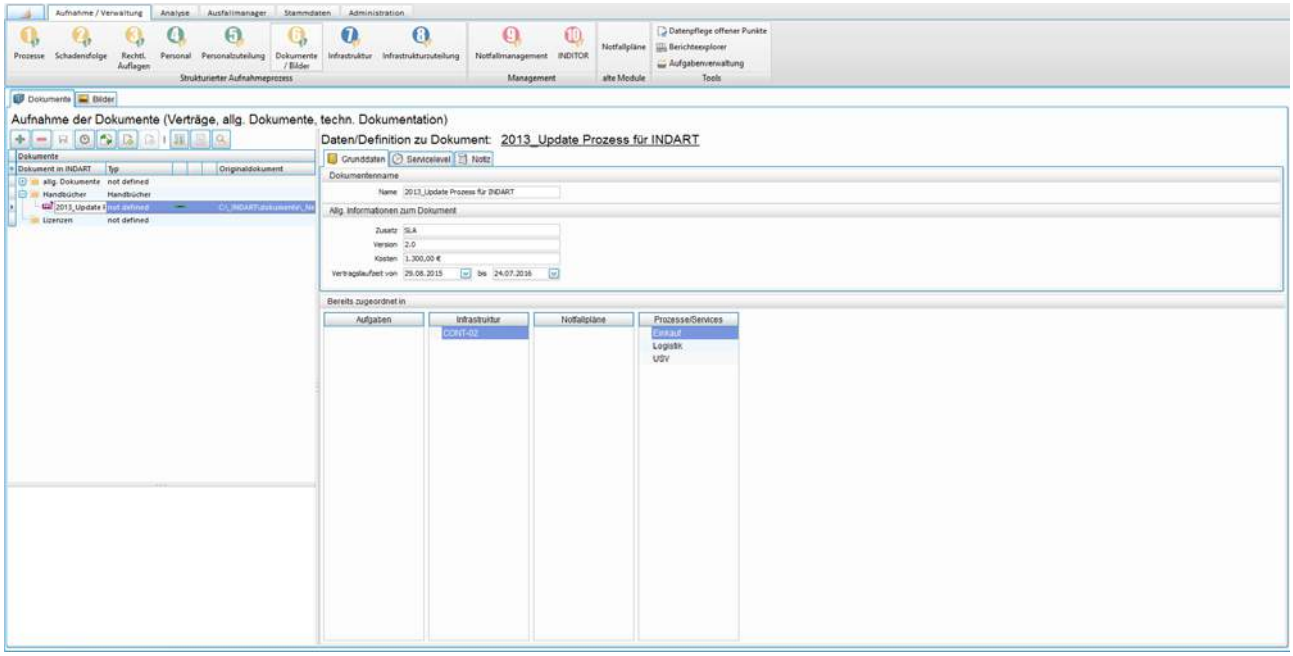


Bild: Contechnet Ltd.

Was passiert, wenn die IT-Systeme eines Unternehmens einem Hackerangriff zum Opfer fallen? Es gilt, den Überblick zu behalten und so die Folgen möglichst gering zu halten – also den Notfallplan zu befolgen. Die Regeln für diesen Plan hält die Firma Oetinger Aluminium in einer softwarebasierten Notfallplanung fest.

Die Firma Oetinger produziert und transportiert pro Jahr rund 180.000 Tonnen Aluminiumgusslegierungen in fester und flüssiger Form. Insbesondere die Just-in-Time-Belieferung mit Flüssigmetall erfordert eine genaue Einhaltung der Termin- und Temperaturvorgaben.

Mehr Angriffsfläche

Im Zuge der Digitalisierung der Industrie spielen auch bei Oetinger Aluminium IT-Systeme eine immer größere Rolle: Maschinen sind vernetzt, Produktionsprozesse laufen automatisiert, und geschäftskritische Daten sind vor Ort oder in der Cloud gespeichert. Da die notwendigen IT-Strukturen immer komplexer werden, steigt gleichzeitig die Anfälligkeit von Fehlern oder Systemausfällen. Auch die Anzahl der Cyberangriffe nimmt zu – 2016 wurden bereits 69 Prozent der Industrieunternehmen in Deutschland Opfer von Cyberattacken. „Inzwischen häufen sich insbesondere die Meldungen über digitale Angriffe auf Industrieunternehmen. Auch wenn wir bis jetzt verschont wurden, haben wir es zum Anlass genommen, uns intensiver mit unserem IT-Notfallmanagement auseinanderzusetzen. Dabei ist uns bewusst geworden, dass wir im Ernstfall weder auf eine zweckmäßige Dokumentation noch auf eine geeignete Notfallplanung zurückgreifen konnten“, sagt Ralf Vögeli, IT-Leiter bei Oetinger Aluminium WH GmbH.

Kein Plan für den Notfall

Anderen Industrieunternehmen geht es ähnlich, denn noch immer hat die Hälfte von ihnen keine betriebliche IT-Notfallplanung zur Hand. Neben Cyberangriffen ist eine solche Notfallplanung auch für den Datenschutz relevant. Im Zuge der Datenschutz-Grundverordnung (DSGVO) sind Unternehmen dazu verpflichtet, personenbezogene Daten angemessen zu schützen. Dazu müssen die Verantwortlichen wissen, welche Daten gespeichert werden, wie diese verarbeitet werden und wo sich die Daten befinden. Vorran-

gig geht es bei einem Notfallplan selbstverständlich darum, sich auf den Ernstfall einer Cyberattacke vorzubereiten. Die IT-Abteilung von Oetinger Aluminium verschaffte sich dazu einen Überblick über die unterschiedlichen Möglichkeiten der Notfallplanung und entschied sich am Ende für eine softwarebasierte Lösung. Die Wahl fiel auf die Lösung Indart Professional von Contechnet: „Letztendlich hat uns das Preis-Leistungs-Verhältnis und die kompetente Beratung überzeugt“, beschreibt der IT-Leiter das Auswahlverfahren.

Nicht bei Null beginnen

Obwohl Oetinger vorher über kein Notfallhandbuch verfügte, musste das Unternehmen nicht ganz von vorn beginnen, da die meisten Daten bereits vorhanden waren. Es mussten jedoch die Kernprozesse definiert werden. Nachdem sich Oetinger Aluminium für die Lösung entschieden hatte, wurde R. Bücker EDV-Beratung Datentechnik GmbH als Partner für die Umsetzung mit ins Boot geholt. Die Herausforderung bestand zunächst darin, alle notfallkritischen Elemente der zwei Standorte Weißenhorn und Neu-Ulm zu identifizieren. Nach der Einteilung in Prozesse, Services, Basisservices sowie Ausfallszenarien wurden das Schadensausmaß sowie mögliche Folgeschäden betrachtet. Nachdem Oetinger mithilfe des Dienstleisters wichtige Dokumente wie Lizenzen, Verträge und Handbücher in die Software aufgenommen und auch das Personal bestimmten Rollen zugewiesen hatte, war die IT an der Reihe. Die IT-Infrastruktur des Unternehmens wurde aufgenommen, ihrem Standort zugeordnet und anschließend mit den unternehmenskritischen Prozessen verknüpft. An diesem Punkt erkannte das Team von Oetinger erst im Detail die Vielschichtigkeit der IT-Infrastruktur des Unternehmens, und es wurde deutlich, welche Rolle die einzelnen Systeme für die Geschäftsprozesse spielen.

In Arbeitsabläufe integrieren

Nachdem die IT-Abteilung mit R. Bücker EDV die acht Planungsschritte durchlaufen hatte, war die betriebliche IT-Notfallplanung von Oetinger Aluminium einsatzbereit. Um den Notfallplan auf dem aktuellen Stand zu halten, muss das Tool zur regelmäßigen Dokumentation in die Unternehmenskultur und die täglichen Arbeitsabläufe integriert werden. Um die IT-Abteilung dabei zu entlasten, entschied sich Oetinger zusätzlich für das Scan- und Importer-Tool Iscan aus der Contechnet-Suite. Die Lösung ermöglicht das Auslesen von Informationen der eingesetzten Hard- und Software im Unternehmen. Außerdem liefert es eine detaillierte Übersicht über die genaue Anzahl der PCs, Server und Netzwerksysteme. Da die Daten vollständig in die Indart-Software übertragen werden, unterstützt das Tool die Mitarbeiter gleichzeitig bei der fortlaufenden Datenpflege ihrer Notfallplanung.

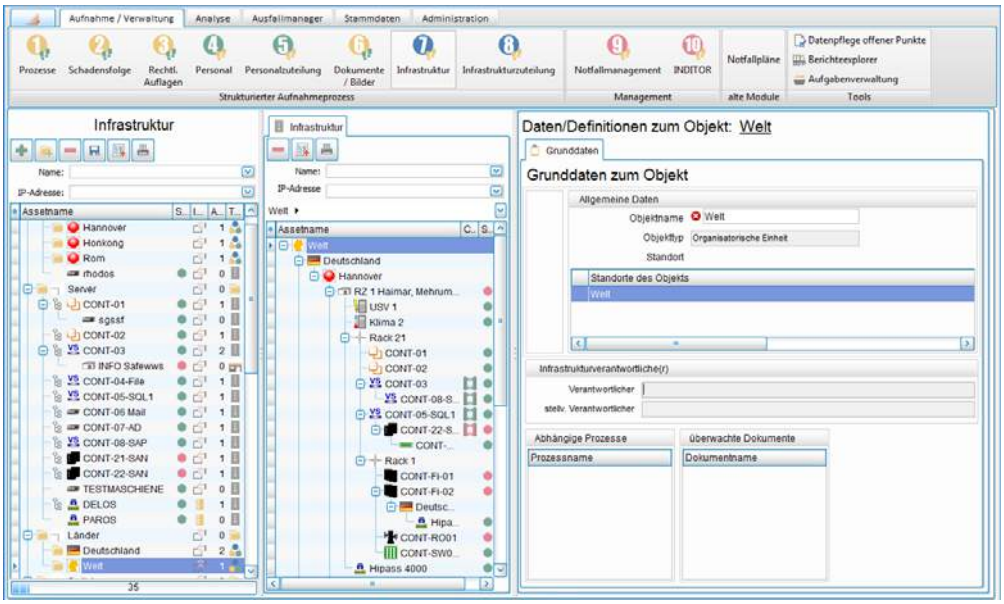


Bild: Contechnet Ltd.

Oetinger musste bei dem Projekt nicht bei Null beginnen, da viele Daten bereits vorlagen.

Schulungsaufwand minimieren

Um den Schulungsaufwand zu minimieren und jedem Mitarbeiter seine entsprechenden Aufgaben ohne direkten Zugriff auf die Software anzeigen zu lassen, wurde zusätzlich das Webmodul Inforweb eingeführt. Damit können sich die Mitarbeiter mit persönlichen Zugangsdaten einloggen und sehen nur die für sie hinterlegten Aufgaben bzw. die Unternehmenswerte wie Prozesse, Personal oder Infrastruktur, für die sie verantwortlich sind. Um die Sinne der Mitarbeiter zu schärfen, führt Oetinger zudem ein- bis zweimal jährlich eine Notfallübung durch. Dabei wird gleichzeitig auch das Notfallhandbuch auf seine Alltagstauglichkeit geprüft.

Einsatz ausweiten

Die softwarebasierte IT-Notfallplanung bietet Oetinger Aluminium die nötige Dokumentation und Handlungssicherheit im Ernstfall. Insbesondere für die IT-Mitarbeiter ist diese Lösung ein Hilfsmittel, um den Anforderungen eines kontinuierlichen, stabilen und performanten IT-Betriebs gerecht zu werden. „Das Projekt hat uns viel gebracht, da der Mehrwert nicht nur darin besteht, dass am Ende ein fertiges Notfallhandbuch zur Verfügung steht. Auch die gesamten Vorarbeiten, wie die Dokumentation und das Befassen mit den installierten Systemen, Wiederherstellungszeiten etc., haben uns dazu bewogen, unsere Prozesse im Detail auf den Prüfstand zu stellen“, fasst Ralf Vögeli das Projekt zusammen. Zukünftig soll das Notfallhandbuch auf weitere fertigungskritische Prozesse ausgeweitet werden. ■

Die Autorin Samira Liebscher
ist freie Journalistin.

www.contechnet.de

Mikrosegmentierung in der Produktion

Gekapselt bis zur Maschinenebene

Mit der Vernetzung der Produktion entstehen neue Angriffsflächen für Cyberkriminelle. Ein vielversprechender Ansatz zur Risikobegrenzung ist die Trennung der Office-IT von der Produktionsumgebung per Mikrosegmentierung.

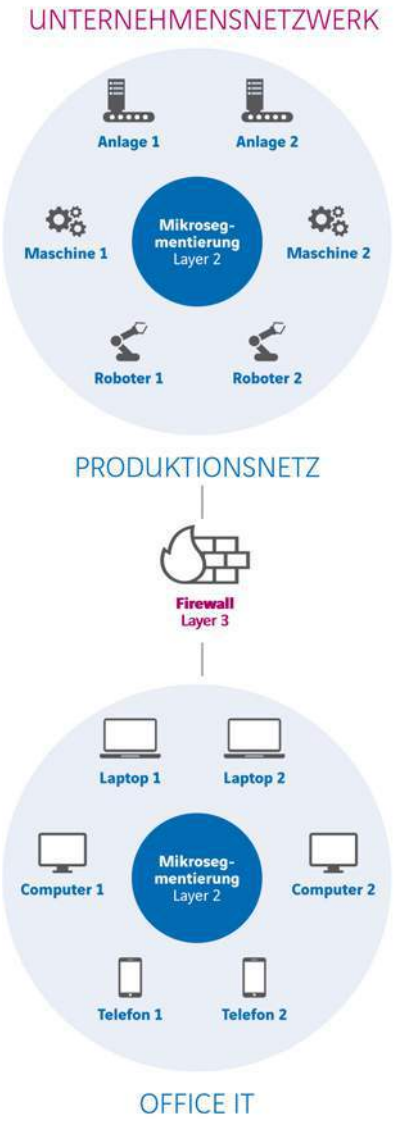
IT-Systeme wachen über die automatisierten Abläufe in der vernetzten Produktion und greifen beim Unter- oder Überschreiten bestimmter Parameter ein, um die Qualität und Effizienz zu wahren oder Wartungsarbeiten anzustoßen. Doch was passiert, wenn sich Malware über das Unternehmensnetzwerk verbreitet, mit dem die Produktion verbunden ist? In diesem Fall ist es die Aufgabe der IT, Automatismen zur Abwehr des Angriffs zu starten, denn die Fertigungstechnik ist durch die Vernetzung ähnlichen Bedrohungen ausgesetzt wie die Office-IT. Zu dieser Einschätzung kommt das Bundesamt für Sicherheit in der Informationstechnik (BSI) in seinem Ranking über die Top-Bedrohungen für Industrieanlagen. Demnach führen Social Engineering und Phishing die Liste der potenziellen Angriffsszenarien an. Idealerweise sind die Mitarbeiter so sensibilisiert und geschult, dass sie nicht auf verdächtige E-Mail-Anhänge klicken, welche den Angreifern Zutritt verschaffen könnten. Dennoch muss die Fertigungsbranche ihre Produktionsstraßen auch technologisch vor Cyber-Attacken schützen. Ziel muss eine Lösung sein, die automatisiert handelt, wenig kostet und gleichzeitig effektiv schützt.

Sicherheit im Netz

Diese Anforderungen erfüllt auch für virtuelle Netzwerke die Mikrosegmentierung, die direkt an der Netzwerkkarte einer virtuellen Maschine (VM) ansetzt. Die VMs sorgen für das Einhalten detaillierter Richtlinien und führen Netzwerkkontrollen durch. Auf diese Weise lässt sich die Workload absichern, wobei eine attackierte VM nicht die nächste VM infizieren kann. Die Mikrosegmentierung setzt die Sicherheitsregeln auch innerhalb eines virtuellen Netzwerks durch, was in traditionellen Umgebungen meist nicht effektiv gelingt. Dort trennen Firewalls meist bloß das öffentliche vom internen Netz, ohne dass innerhalb der beiden Teilnetze eine Reglementierung stattfindet. Im Gegensatz zu einem konventionellen Firewall-Regelwerk bietet die Mikrosegmentierung nun die Möglichkeit, Identitäten über IP-Adressen oder Hostnamen hinaus zu definieren. Die Technologie sichert die Netzwerke im Rechenzentrum daher wesentlich effektiver ab. Dieser Sicherheitsgewinn lässt sich vom Rechenzentrum auf die Produktionsstraßen übertragen. Im Alarmfall greift dann ein Automatismus, der Datenpakete blockiert oder die Verbindung unterbricht. Die Maschinen laufen derweil weiter.

Die passende Architektur

Wie sich der Ansatz in die Praxis überführen lässt, verdeutlicht das Beispiel eines weltweit agierenden Zulieferbetriebes für die Automobilindustrie. Dieser suchte nach einer Lösung, um im Fall einer Cyberattacke einen Produktionsstopp zu vermeiden. Axians bekam den Auftrag, die Mikrosegmentierung für ihn zu konzipieren und umzusetzen. Das Unternehmen befand sich in einer Ausgangssituation, die anderen Vertretern der Fertigungsbranche vertraut vorkommen dürfte. So wird in der Produktionsstraße über das Protokoll TCP/IP kommuniziert. Nach dem Identifizieren über die IP-Adresse erfolgt der Transport der Datenpakete. Den Anlagen- und Maschinenpark fasst ein Subnetz zusammen. Aufgabe der Mikrosegmentierung ist es, dieses Produktionsnetz von der Office-IT zu trennen. Zusätzlich muss es möglich sein, jede Maschine einzeln abzusichern und im Bedarfsfall zu isolieren. Eine große Herausforderung ist hierbei die Beibehaltung der bestehenden IP-Adress-Struktur. Da Änderungen der IP-Adressen im Produktionsumfeld zum Teil unvorhergesehenen Folgeaufwand nach sich ziehen, sollten sie nach Möglichkeit beibehalten werden. Zudem sollte die Lösung skalieren, um sie auch an anderen Standorten weltweit ausrol-



Mit Mikrosegmentierung lässt sich jede Maschine einzeln absichern.

Bild: Axians IT Solutions GmbH

len zu können. Dieses Anforderungsprofil lässt sich mit einer integrierten Cisco-Security-Architektur erfüllen – mit Cisco Identity Services Engine (ISE) für die Administration, der Cisco Firepower NGFW (Next Generation Firewall) sowie den Cisco Catalyst Switchen der neuesten Generation. Die Segmentierung findet in diesem Fall auf Layer 2 statt und minimiert somit den administrativen Aufwand bei der Migration. Die Identity Services Engine stellt in diesem Szenario die Plattform für das Richtlinienmanagement zur Verfügung und liefert Benutzer- und Gerätetransparenz. Zudem bietet sie uneingeschränkte Mobilität bei kontrolliertem Zugriff. Die verwendete Lösung hatte zudem ein Intrusion Prevention System (IPS) sowie eine Advanced Malware Protection mit an Bord.

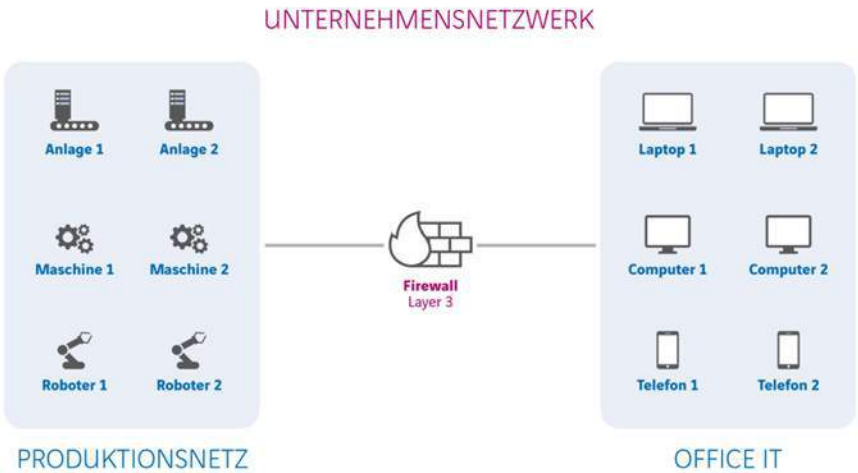


Bild: Axians IT Solutions GmbH

Ohne Mikrosegmentierung trennt meist nur eine Firewall Office IT und Produktionsnetz voneinander.

Mechanismen und ihre Effekte

Rein Software-definiert erfolgt die Mikrosegmentierung innerhalb eines Subnetzes. Die Cisco-Technologie Trustsec, vereinfacht über Secure Group Tagging (SGT) den Netzwerkzugriff, beschleunigt Sicherheitsvorgänge und stellt sicher, dass Sicherheitsaktionen konsistent angewendet werden – und zwar im gesamten Netzwerk. Dessen Datenverkehr wird über den Endpunkt identifiziert – und nicht anhand der IP-Adresse oder bestimmter Zugriffskontrolllisten. Die Sicherheitsarchitektur wird so installiert und remote freigeschaltet, dass die Produktion auch während der Migration weiterlaufen kann. Für den Betrieb definiert ein Administrator über die Identity Services Engine die Security-Regeln. Mit den Security Group Tags legt er fest, wer innerhalb einzelner Netzwerksegmente Regeln einführen und ändern darf. Unter den Voraussetzungen leitet der Cisco Catalyst 3650X-Switch die Datenpakete so weiter, wie es die Security-Regeln vorsehen. Die Segmentierung zur Office-IT und eine allgemeine Layer-3-Segmentierung übernimmt die Firewall. Im Betrieb äußert sich der Sicherheitsgewinn in mehrfacher Hinsicht. So sichert der Authentifizierungs-Standard 802.1x im Zusammenspiel mit den Secure Group Tag Access Control Lists (ACL) der Cisco ISE den Netzwerkzugang ab. Bei einer Bedrohung reagiert das Netzwerk selbständig. Z.B. wird ein infizierter Rechner automatisch vom Netz getrennt und in einen Quarantäne-Cluster verschoben. Als Konsequenz verringert sich die Angriffsfläche. Außerdem läuft nun vieles im Netzwerk transparenter ab als vorher. Ein Administrator kann leichter nachvollziehen, wie eine Malware ins Netz gelangt ist. Das Reporting-Feature dokumentiert zusätzlich Sicherheitsvorfälle.

Eine große Sorge weniger

Über eine Mikrosegmentierung lässt sich ein Unternehmensnetzwerk einschließlich der Produktion detailliert absichern. Diese Technologie lässt sich lokal oder an allen Standorten einer Unternehmensgruppe implementieren. Ein weltweites Ausrollen stellt jedoch hohe Anforderungen an den ausführenden Netzwerkspezialisten. Denn Planung, Installation und Betrieb der Lösungen müssen aufeinander abgestimmt sein. Wer sich jedoch für diesen Weg entscheidet, muss sich kaum noch Sorgen machen, dass ein unbeabsichtigter Klick eine komplette Produktionsstraße lahmlegt, denn in diesem Bereich verbreiten sich Schadsoftware und andere Gefahren nicht mehr. ■

Der Autor Frank Greisiger ist Vertriebsleiter Südwest bei Axians Networks & Solutions.

Public Key Infrastructure

Sichere Protokolle auch für kleine IoT-Geräte

Die Zahl der Geräte im Internet of Things wächst stetig, doch noch immer mangelt es an verbindlichen Standards für die Sicherheit bei der Datenübertragung. Eine der größten Herausforderungen des IoT ist die Bereitstellung vertrauenswürdiger Identitäten für Geräte mit begrenzten Ressourcen. Mit Public-Key-Factor-basierten Protokollen ließe sich das lösen.

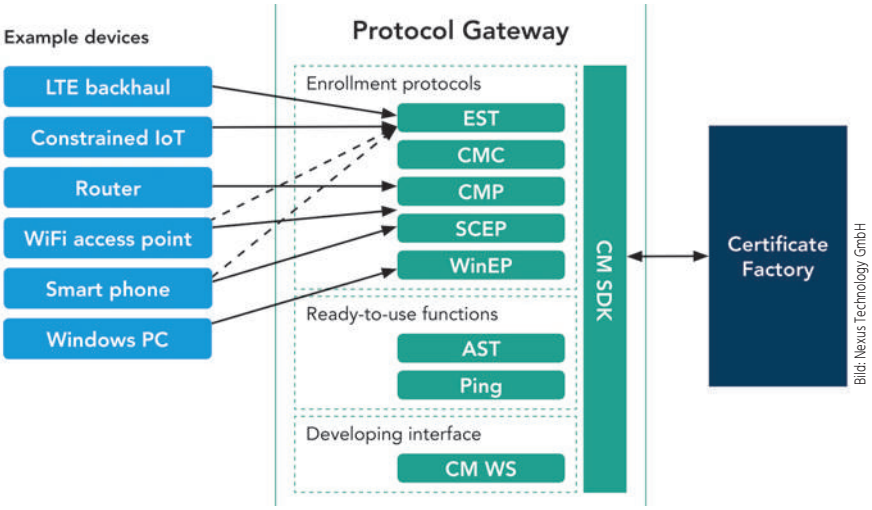


Bild: Nexus Technology GmbH

Der Branchenverband Cloud Security Alliance hat in seinem Report 'Future Proofing the Connected World' einen Katalog konkreter Maßnahmen veröffentlicht, um die Sicherheit vernetzter Geräte zu verbessern. Eine zentrale Rolle spielt dabei die Implementierung von Funktionen für die starke Authentifizierung, Autorisierung sowie für die Zugriffskontrolle. Für die Authentifizierung benötigt jedes Gerät eine vertrauenswürdige Identität. Im Bereich Netzwerkkommunikation ist dabei eine Public Key Infrastructure (PKI) der De-Facto-Standard, um vertrauenswürdige Identitäten in Form von digitalen Zertifikaten bereitzustellen. Die Zertifikate werden von einem vertrauenswürdigen Dritten (in der Regel eine sogenannte Certificate Authority) ausgestellt und sorgen dafür, dass Geräte oder auch Menschen, die bislang nichts voneinander wussten, sicher miteinander kommunizieren können. Die Herausforderung dabei ist die Zertifikatsverteilung.

Automatisierte Zertifikate

Möchte man auf einem Smartphone ein digitales Zertifikat nutzen, beispielsweise für die E-Mail-Verschlüsselung oder für das digitale Signieren von Dokumenten, so wird das Zertifikat zunächst auf einem sicheren Weg auf das Telefon übertragen bzw. direkt auf dem Smartphone erzeugt. Um die Identität des Zertifikats zu schützen, wird es mit einem PIN versehen. Dieser muss bei jeder Verwendung angegeben werden. Alternativ zum PIN ist die Bestätigung des Zertifikats auch per Fingerabdruck möglich. Bei einem Sensor funktioniert dies nicht, da keine Benutzeroberfläche vorhanden ist. Daher muss die Zertifikatsverteilung auf diese Geräte automatisiert werden. Zwar existieren bereits Protokolle, die dafür genutzt werden. Allerdings sind sie zu komplex, um auch für Geräte mit begrenzten Ressourcen, wie beispielsweise batteriebetriebene Geräte, geeignet zu sein. Häufig verwenden Hersteller anstelle der PKI-Technologie geteilte Schlüssel (symmetrische Verschlüsselung) oder PINs und Passwörter für die Kommunikation zwischen vernetzten Geräten.

Was ist ein gutes IoT-Protokoll?

Ein gutes IoT-Protokoll sollte folgende drei Anforderungen erfüllen:

- PKI-basiert: Im Netzwerk ausgetauschte Information wird mittels asymmetrischer Kryptographie verschlüsselt
- Automatisierte Zertifikatsverteilung: Zertifikate können in Sekundenschnelle an Tausende Geräte verteilt werden, ohne dass sie manuell bestätigt werden müssen
- Leichtgewichtig: Das Protokoll funktioniert auch für Geräte mit geringer Rechenleistung und begrenzter Energie

Das EST-Protokoll

Das sogenannte Enrollment over Secure Transport (EST)-Protokoll wurde 2013 standardisiert und von Cisco in Zusammenarbeit mit der Internet Engineering Taskforce entwickelt. Mit dem Protokoll können Zertifikatsverteilungsprozesse beschleunigt und automatisiert werden – ein großer Vorteil in komplexen IoT-Umgebungen. Das ältere SCEP-Protokoll (Simple Certificate Enrollment Protocol) wiederum unterstützt

keine Erstellung und Verteilung von Schlüsseln auf Server-Seite und ist daher nur bedingt geeignet, Zertifikate für Clients und Certificate Authorities (CA) zu erneuern. Außerdem ist SCEP nicht standardisiert und erzeugt daher oft Probleme beim Zusammenspiel verschiedener Implementierungen. Auch CMP (Certificate Management Protocol) und CMS (Certificate Management over CMS) sind weit verbreitete Protokolle, die zwar standardisiert sind, bei denen es aber schwieriger ist, sie auf Clients zu implementieren. Für Geräte mit begrenzten Ressourcen sind sie daher ungeeignet. Als als Anbieter von Identity- und Security-Lösungen war Nexus Anfang 2017 unter den ersten Unternehmen, die das EST-Protokoll in einem kommerziellen Produkt unterstützen. Allerdings fehlt dem EST-Protokoll die Funktionalität für die automatische Zertifikatserneuerung. Dies wurde mittels einer REST API (Representational State Transfer, Application Programming Interface) für die Nexus PKI gelöst, die es für Kunden und Entwickler einfacher machen soll, entsprechende Funktionen für die Zertifikatserneuerung zu implementieren.

Das Cebot Protokoll

Das EST-Protokoll ist zwar besser geeignet als seine Vorgänger, dennoch bietet es keine wirklich praktikable Lösung für das erstmalige Verteilen und Widerrufen von Zertifikaten auf vielen verteilten Geräten. Ein wichtiger Schritt in diese Richtung ist das Cebot-Protokoll (Certificate Enrollment for Billions of Things). Cebot ist ein Projekt des schwedischen Forschungsinstituts Rise SICS und Nexus, das mit den Unternehmen Ericsson, Saab, Intel und Scypho bereits einige Unterstützer hat. Das Protokoll wurde speziell für die Anforderungen des IoT entwickelt. Die Funktionsweise ist einfach: Beim Kauf einer smarten LED-Lampe hat der Hersteller beispielsweise bereits ein Zertifikat auf der Lampe installiert. Sobald diese angeschlossen wird, verbindet sie sich automatisch mit der Certificate Authority, um das Zertifikat bestätigen zu lassen. Für diese Kommunikation sorgt Cebot. Das Protokoll löst damit das Problem, Zertifikate auch für Geräte mit begrenzten Ressourcen automatisch bereitzustellen. Cebot soll in einem nächsten Schritt der Internet Engineering Task Force (IETF) vorgelegt werden, um als Standardprotokoll anerkannt zu werden.

EU investiert in IoT-Sicherheit

Um PKI noch skalierbarer und leichtgewichtiger für das IoT zu machen, hat sich Nexus mit verschiedenen Partnern aus Forschung und Wirtschaft zusammengetan. Das Secure IoT-Projekt wird von Eurostars gefördert, einem gemeinsamen Programm der europäischen Forschungsinitiative Eureka und der Europäischen Kommission. Ziele des Projekts sind u.a. eine Lösung für das automatische erstmalige Verteilen und Widerrufen von Zertifikaten für batteriebetriebene IoT-Geräte zu finden sowie die Entwicklung eines IoT-Gateways, das sowohl moderne Protokolle für die IoT-Sicherheit als auch ältere Protokolle unterstützt. Das Projekt wurde im September 2016 gestartet und ist auf 36 Monate ausgelegt.

Datenschutz autonomer Fahrzeuge

Secredas steht für 'Product Security for Cross Domain Reliable Dependable Automated Systems' und ist ein von der EU im Rahmen von Horizon 2020 gefördertes Projekt. Das Ziel ist, eine Lösung für die Sichereit und den Datenschutz vernetzter und automatisierter Fahrzeuge sowie anderer automatisierter Systeme zu finden. Im Rahmen des Projekts soll eine Softwarelösung zur Validierung von Architekturmethoden, Referenzarchitekturen, Komponenten und Integrationen entwickelt, die auch die sichere Kommunikation zwischen verschiedenen automatisierten Systemen ermöglicht. Secredas soll damit Vertrauenswürdigkeit in IoT-Netzwerke bringen, insbesondere um die europäische Auto- und Medizinindustrie in dieser Hinsicht zu stärken. Das Forschungsprojekt bringt ein Konsortium von Partnern aus 15 Ländern zusammen, das die gesamte Wertschöpfungskette der Automobilindustrie, Schlüsselakteure im medizinischen Bereich, eine Reihe von Akteuren in anderen Verkehrsbereichen (Eisenbahnen, Luft- und Raumfahrt) und Forschungsinstitute umfasst. ■

Identitäten verwalten seit 20 Jahren

Der IT-Sicherheitsspezialist hat bereits seit 20 Jahren eine eigene PKI-Identitätsplattform auf dem Markt, die für IoT-Anwendungen genutzt wird. Mit 10.000 Zertifikaten pro Sekunde ist das System nach Angaben des Anbieters sogar dazu geeignet, die nächste Generation der vernetzten Fahrzeugkommunikation V2X (auch als Car2X bezeichnet) zu unterstützen.

Der Autor Thorsten Gahrmann ist Head of Software Sales bei Nexus.

www.nexusgroup.com

Verzahnte Entwicklung bei Elwema Automotive

Anlagensoftware versioniert und protokolliert

Bild: Auvesy GmbH

SPS-Programmierung, Human Machine Interfaces, Konnektivität – die Softwareentwicklung für moderne Anlagen wird immer aufwendiger. Um diese Arbeiten zu unterstützen und abzusichern, nutzt der Zulieferer Elwema Automotive speziell angepasste Versionierungsanwendungen von Auvesy. Bei der Produktion behalten die Mitarbeiter so alle Arbeitsfortschritte und Änderungen im Blick. Doch auch nach der Inbetriebnahme protokollieren die Programme Anlagenänderungen sicher und nachvollziehbar.

Die Elwema Automotive GmbH aus Ellwangen und Monschau realisiert Fertigungslösungen in der Reinigungs-, Prüf- und Montagetechnik, insbesondere für die Bereiche Motoren, Lenkung und Getriebe vornehmlich für die Automobilindustrie. Entsprechend anspruchsvoll sind die gefertigten Anlagen und die Anforderungen an das Daten- und Programmmanagement für Steuerungen, Human Machine Interfaces, Robotik und Konfigurationsdaten. Die Versions- und Datenmanagementlösung Versiondog des IT-Herstellers Auvesy hilft dem Maschinenbauer Elwema im Engineering und in der Anlagenfertigung dabei, die Programme im Blick zu behalten.

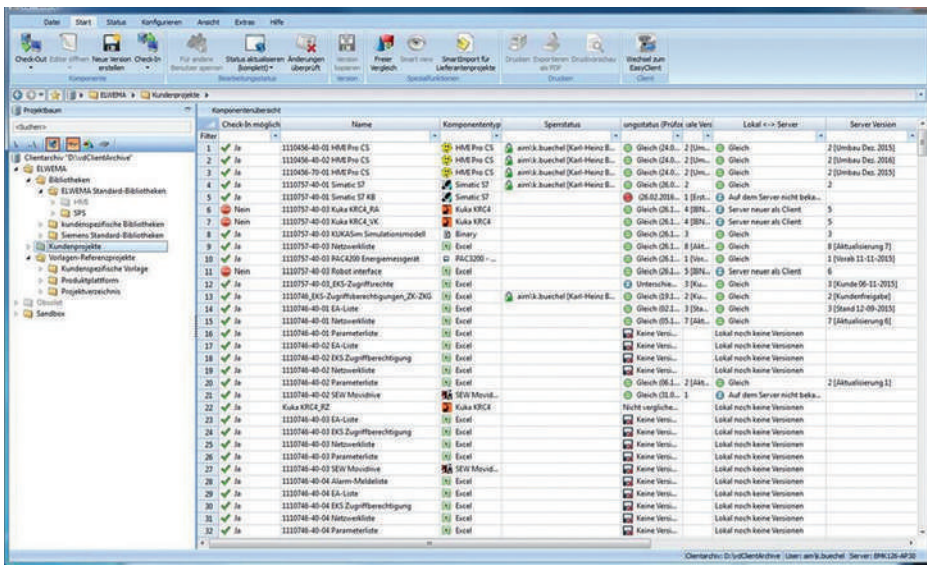
Auf Projektarbeit ausgelegt

Vor dem Einsatz des Tools kam es immer wieder zu Missverständnissen beim Umgang mit Daten. „Es war keine klare Filestruktur vorhanden. Simple Dinge wie die Namensgebung von Files wurden unterschiedlich gehandhabt, oder Modifikationen wurden nicht abgeglichen. Das alles führte zu Suchvorgängen und verursachte unnötigen Zeitaufwand“, berichtet Karl-Heinz Büchel, Leiter der Steuerungstechnik und der Automatisierung bei Elwema. Auf der Suche nach einer Lösung stieß man auf Versiondog, das in einer dreimonatigen Testphase überzeugen konnte. Seit rund drei Jahren setzt der Maschinenbauer projektspezifische Versionen der Anwendung für die Anlagensteuerung ein. Diese beinhalten beispielsweise Netzwerk- oder EA-Listen. Etwa 35 Mitarbeiter haben Zugriff auf diese Daten. Die Lösung versioniert und dokumentiert Änderungen und verwaltet Projektdaten im Sinn eines Lifecycle Managements. Das aktuell geladene Programm, die verwendeten Parameter und Sollwerte, wie auch die eindeutige Versionszuordnung sind stets aktuell abrufbar. „Durch das Arbeiten mit Versiondog haben wir uns weiterentwickelt und Prozesse standardisiert“, sagt Büchel. „Wir haben jetzt eine zentrale Stelle für die Datenablage, eine klare Rechtestruktur, die Änderungsgründe sind ersichtlich, die Transparenz wer, wo, wann, was geändert hat, die Source-Code-Verwaltung ist möglich und der Versionsvergleich nützt der Standardisierung. Änderungen folgen einem einheitlichen Muster: Datei auschecken, Sperrstatus setzen, ändern, einchecken. Alles ist dokumentiert und jederzeit nachvollziehbar.“

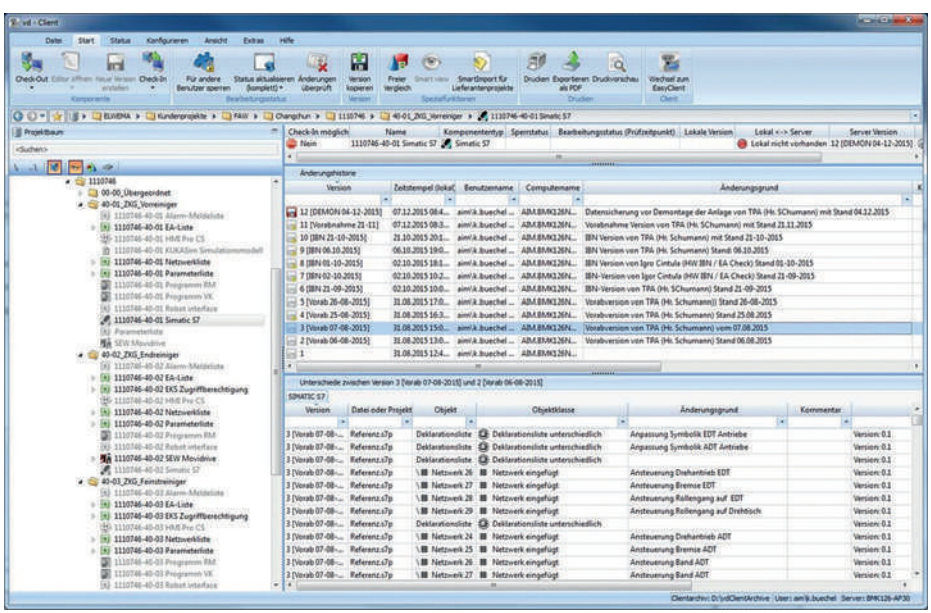
Die Anlage lebt weiter

Der Versionierungsprozess ist jedoch nicht mit der Fertigstellung einer Anlage beendet. Nach der Montage und Inbetriebnahme erfolgt vor Auslieferung zunächst die Vorabnahme durch den Kunden. Dann wird sie demontiert und vor Ort beim Kunden wieder aufgebaut. Dabei ist die Integration der Komponenten nach einer CNC-Maschine keine Seltenheit. Denn nach der Bearbeitung (z.B. eines Kurbelwellengehäuses) erfolgen die Reinigung der gefertigten Teile, die Montage und anschließend die Prüfung auf Dichtheit, z.B. der Öl- und Wasserräume. Damit diese Integration funktioniert, müssen die jeweiligen Daten- Und Programmstände versioniert werden. Dieser Auslieferungsstand

Bilder: Auvesy GmbH



Übersicht der Komponentenstatus in einem Elwema-Projektverzeichnis



Versiondog-Versionshistorie einer S7-Softwarekomponente mit Änderungsdarstellung in Version 3 im Fenster rechts unten

wird auch an den Kunden übermittelt. Nach der Auslieferung kann die Anlage weiter überarbeitet, umgebaut oder erweitert werden. Bei allem muss die aktuelle Daten- und Software-Version festgehalten und abgeglichen werden, was mit Versiondog recht einfach fällt. Es ist unter technischen sowie Sicherheits- und Gewährleistungsaspekten wichtig, dass alle Beteiligten auf dem gleichen Informationsstand sind und mit gleichen Programmversionen arbeiten. Deshalb wird der Prozess über den gesamten Lebenszyklus einer Anlage hindurch geführt. So ist dokumentiert, was der Kunde nach der Übergabe der Anlage mit ihr gemacht hat. Durch den Zeitstempel ist auch festgehalten, wann etwas verändert wurde.

Mitarbeiter geschult

Um das Bewusstsein bei den Mitarbeitern zu verankern, dass Anlass, Zeitpunkt und Verantwortlichkeit für jede Anpassung von Programmen und Daten dokumentiert werden muss, setzte der Maschinenbauer Schulungen für die rund 35 Nutzer an. Denn wie so häufig steht und fällt der Nutzen leistungsfähiger Anwendungen mit der Bereitschaft der Belegschaft, die Programme konsequent und wie vorgesehen zu benutzen. ■

Die Autoren sind Karl-Heinz Büchel, Leiter Steuerungstechnik & Automatisierung bei Elwema sowie Silke Glasstetter, Head of Marketing bei Auvesy GmbH.

Lernen aus WannaCry und Co.

Das IT-Sicherheitsgesetz als starkes Argument

Bild: © Peter Eggermann / Fotolia.de

Trotz der aufsehenerregenden Cyberangriffe wie mit der Ransomware WannaCry im letzten Jahr ist die IT-Sicherheit auf der Prioritätenliste vieler Unternehmen noch immer nicht weit genug oben. Doch zumindest bei versorgungskritischen Infrastrukturen fordert der Gesetzgeber mittlerweile ein Bündel von Sicherheitsmaßnahmen. Diese könnten künftig auch Produzenten umsetzen müssen, die Kritis-Betreiber mit wichtigen Komponenten versorgen.

In der Transformation hin zur Industrie 4.0, beziehungsweise zur Integrated Industry, nimmt die IT eine tragende Rolle innerhalb der Produktions- und Wertschöpfungskette ein. Denn die Vernetzung aller Gegenstände und Systeme sowie deren Ausstattung mit zusätzlicher Intelligenz zur besseren Nutzung und Überwachung ermöglichen innovative Anwendungen und Geschäftsmodelle. So lassen sich Effizienzsteigerungen unter anderem realisieren, indem Produktionsabläufe digital simuliert oder Stillstände in der Fertigung durch vorausschauende Wartung minimiert werden. Zunehmend kommen mobile Endgeräte und Apps zum Einsatz. Meist werden diese zum Monitoring der Produktionsanlagen genutzt, doch einige davon gestatten bereits weiterführende Eingriffsoptionen: Werks- und Produktionsleiter können zu jeder Zeit von jedem Standort die Produktionsprozesse kontrollieren und Einfluss auf Steuerungspa-

rameter nehmen. Nachweislich bringt die hochgradige Vernetzung viele Vorteile für den Betriebsablauf, andererseits jedoch ebenso viele Angriffspunkte, die ausgenutzt werden können. Dies basiert zum einen auf den immer komplexer werdenden IT-Landschaften sowie den immanenten Schwachstellen von Komponenten der OT und zum anderen auf dem Fehlen adäquater Schutzkonzepte.

Genug offene Flanken

Die fortschreitende Digitalisierung und die daraus resultierende Entwicklung neuer Geschäftsmodelle wie Predictive Maintenance auf Basis von Internettechnologien bringen einen massiven Anstieg der Gefahrenpotentiale mit sich. Ungeachtet dieses Fakts finden jedoch die unsicheren Basistechnologien wie Web-Sprachen, Kommunikationsprotokolle, Datenbanken oder Betriebssysteme im Produktionsumfeld Verwendung und stoßen auf Produktionsnetze und -komponenten, die hochsensibel sind und meist für solche Szenerien nicht konzipiert wurden. Aufgrund der langen Lebenszyklen der Systeme im Produktionsumfeld sind sehr häufig noch IT-Komponenten ohne spezifische IT-Wartung wie Upgrades im Einsatz, für die es zudem teilweise bereits seit längerem keine Sicherheitspatches mehr gibt, weil der Hersteller die Wartung eingestellt hat. Mittlerweile haben sich bestimmte Angreifer darauf spezialisiert, direkt nach Sicherheitslücken zu suchen, sobald Produktionsanlagen mit dem Internet – also in einem TCP/IP Netz – verbunden sind. Dass dies keine theoretische Gefahr ist, belegen diverse Studien – bereits im Jahr 2016 erfolgte jeder vierte Cyberangriff auf industrielle Systeme. Dafür gibt es verschiedene Gründe: Der Datentransfer zwischen den Systemen der Produktion läuft vermehrt über offene Standards – zur Absicherung der OT sind jedoch teils völlig andere Konzepte und Lösungen notwendig, als im klassischen IT-Umfeld, die dort vorherrschenden Ansätze sind nur sehr bedingt übertragbar. Zudem erfordert jede weitere Anbindung von Applikationen sowie Vernetzung von Geräten und Systemen neue Schnittstellen, die per se ein Risiko darstellen – hier werden ständig neue Schwachstellen entdeckt. Die Ausführung der zumeist systematischen Attacken erfolgt mit regelmäßig aktualisierten Angriffsmethoden; hierfür gibt es unter anderem Standardwerkzeuge, die inzwischen auf speziellen Plattformen im Internet frei zur Verfügung stehen.

IT-Sicherheitsgesetz für die Industrie gefordert

Mit Inkrafttreten des IT-Sicherheitsgesetzes in 2015 müssen die Betreiber kritischer Infrastrukturen (Kritis) im wesentlichen zwei Vorgaben erfüllen: Die definierten Organisationen und Institutionen mit relevanter Bedeutung für das Gemeinwesen sind fortan verpflichtet binnen zwei Jahren nachzuweisen, dass sie wirksame Vorkehrungen zum Schutz der Daten getroffen haben, um deren Verfügbarkeit, Integrität, Vertraulichkeit und Authentizität zu wahren. Zudem stehen sie in der Pflicht, die qua Definition kritischen Sicherheitsvorfälle unverzüglich zu melden sowie eine Kontaktstelle für das Bundesamt für Sicherheit in der Informationstechnik (BSI) anzugeben. Relevante Bedeutung haben dem Gesetz zufolge Organisationen in den Bereichen Staat und Verwaltung, Energie, Gesundheitswesen, Finanz- und Versicherungswesen, Transport und Verkehr, IT und TK, Medien und Kultur sowie Wasser und Ernährung.

Schlecht programmierte Apps

Auch schlecht programmierte Apps und ohnehin unsichere Endgeräte bieten eine große Angriffsfläche, beispielsweise bei deren Einsatz zur Maschinensteuerung: Die Eingriffsmöglichkeiten reichen hier von Manipulation der Produktionsprozesse, was unter Umständen die Produktions- und Produktqualität stark beeinträchtigen kann, bis hin zum Abschalten einer kompletten Produktionslinie.

Kritis auch für Zulieferer

Mittlerweile ist erkennbar, dass Zulieferer von Anlagen und Komponenten, die wesentlich für eine Kritis-Umgebung sind, zumindest für die gelieferten Komponenten Kritis-Anforderungen standhalten müssen. Heute steht zur Diskussion, dass das IT-Sicherheitsgesetz analog im Kontext von Industrie 4.0 Anwendung finden soll. Dies erscheint aus dem Grund akut, da oftmals schlecht gewartete, veraltete und ungesicherte, aber dennoch innerhalb einer Wertschöpfungskette hochgradig vernetzte OT-Systeme für Angriffe leicht nutzbar sind. Das derzeitig vorzufindende IT-Sicherheitsniveau der OT entspricht bei weitem nicht den gestiegenen Anforderungen. Von daher ist es an der Zeit, Sicherheitsstrategien im industriellen Umfeld zu entwickeln.

Rat liefert der Gesetzestext

Im Grunde geht es bei der Diskussion bezüglich der erweiterten Einführung des IT-Sicherheitsgesetzes darum, Unternehmen dahingehend zu sensibilisieren, dass sie die bestehenden Probleme aktiv angehen. Dazu gehört ein Verständnis dafür zu schaffen, dass IT-Sicherheit ein kontinuierlicher Prozess ist. Hilfreich bei der Ausgestaltung einer effizienten Vorgehensweise ist das gemeinsame Thesenpapier von Teletrust und dem Bundesverband der IT-Anwender (VOICE) aus dem Jahr 2017. In diesem Leitliniendokument werden Defizite und Problembereiche im IT-Sicherheitsumfeld dargestellt, die es dringend zu beheben gilt. Dazu haben Teletrust und Voice gemeinsam sechs Thesen erarbeitet, „die jeweils spezifische 'Gemeinsame Aufgaben' innerhalb jeder These skizzieren, wie vorhandene Herausforderungen erfolgreich bewältigt werden können", etwa in der ersten These 'Ohne IT-Sicherheit gelingt keine nachhaltige Digitalisierung' oder der vierten: 'Security-by-Design, Privacy-by-Design und nachvollziehbare Qualitätssicherung sind unabdingbar'. Mit zunehmender Digitalisierung sollten auch mittelständische Unternehmen nicht mehr den Standpunkt vertreten, dass sich kein Angreifer für sie interessieren wird. Was aber andererseits nicht zu der fatalistischen Einstellung führen sollte, dass aufgrund der hohen Komplexität ein Absichern der eigenen Infrastruktur per se unmöglich sei. ■

Der Autor Wolfgang Straßer ist Gründer und Geschäftsführer der @-yet GmbH.

www.add-yet.de

Zugriffsrechte verwalten

Für jeden Mitarbeiter ein eigenes Netz

Bild: Wallix Deutschland

Die Bedrohung durch Cyberattacken ist greifbar, das erkennen auch die Unternehmen. Jedoch haben verschiedene Abteilungen unterschiedliche Anforderungen an die IT-Sicherheit. Mit Privileged-Access-Lösungen kann man diesen Unterschieden Rechnung tragen.

In seinem aktuellen Bericht zur Lage der IT-Sicherheit warnt das Bundesamt für Sicherheit in der Informationstechnik (BSI) davor, dass ungezielte Angriffe auf Produktionssysteme oft erfolgreich sind, weil Unternehmen häufig Altsysteme einsetzen und keine geeigneten Prozesse und kaum Knowhow zur IT-Sicherheit für den Produktionsbereich vorhanden sind. Hersteller und Maschinenbauer würden zudem von den Betreibern keine ausreichenden Informationen über die notwendigen Sicherheitsanforderungen erhalten, so das BSI. Diese würden von den Betreibern weder eingefordert noch seien entsprechende Ressourcen vorgesehen. Zudem fehle es bei den Herstellern vielfach an Prozessen, um mit Schwachstellen in eigenen Produkten umzugehen, diese zu kommunizieren und für eine Fehlerbeseitigung Sorge zu tragen. Eine deutliche Kritik. Allerdings sollte man verstehen, dass die Herausforderung durch die digitale Integration für IT-Abteilungen und Betriebsleiter in der Produktion ungleich schwieriger ist als in anderen Branchen. Die Lebenszyklen von Maschinen und die Größe der Assets sind in keiner anderen Branche so groß. Zudem werden Anlagen und Fertigungsstraßen der Industrie über Jahrzehnte abgeschrieben und sind nur schwer komplett auswechselbar. Zugleich steigen aber die Anforderungen an die Produktivität. Durch Modernisierungsprojekte dürfen operationale Abläufe daher nicht zu beeinträchtigt werden – längere Wartungsfenster sind aus Sicht der Wettbewerbsfähigkeit nicht möglich, ein Komplettstillstand zur Neuaufsetzung der Netzwerke ist undenkbar. Die Legacy-Herausforderung und die hohen Anforderungen an die Produktivität müssen auch von IT-Abteilungen beachtet werden. Die neue Konkurrenzsituation ist besonders kritisch, da die Digitalisierung den Markt für neue Anbieter öffnet, die ohne Fertigungsmittel Lösungen in digitaler Form anbieten. Etablierten Unternehmen droht dabei der Abstieg in das Commodity-Geschäft, falls sie es nicht schaffen, ihr Knowhow digital zu vermarkten.

Umsetzung ist schwierig

In den Führungsebenen stehen die Themen Digitalisierung und die Gefahr durch Cyberattacken auf der Tagesordnung. Die Umsetzung und die Abwehr gestalten sich jedoch nicht einfach. IT-Verantwortliche verlangen häufig mehr Einfluss in die Prozesssteuerung und möchten, dass smarte Produktionsanlagen ebenfalls unter ihre Verwaltungsgewalt fallen. Betriebsverantwortliche wollen dagegen das volle Potenzial von vernetzten Geräten nutzen, fürchten aber, dass durch Umstellungen die Anlagen nicht richtig funktionieren könnten. Hinzu kommt, dass sich durch die Modernisierung auch die Bezugsmodelle für Maschinen und Anlagen ändern. Geräte werden geleast oder durch On-Demand-Services ersetzt. Dies erfordert auch immer mehr gesicherte Fernwartungszugänge. Ursprüngliche geschlossene Netzwerke und Insellösungen sind somit online, wodurch der Verwaltungsaufwand steigt. IT-Verantwortliche müssen Lösungen finden, wie sie trotz der wachsenden Anzahl an Aufgaben die Compliance-Vorgaben erfüllen und Auditsicherheit gewährleisten können. Neben der Endpunktsicherheit geht es dabei vor allem um den Faktor Mensch und die Frage, wer zu welcher Zeit über welche Plattform auf welche Systeme zugreifen darf. Zeitgleich sollten aber Betriebsleiter die Möglichkeit haben, Probleme im operativen Bereich ohne lange Bürokratieprozesse zu beseitigen. Sie benötigen Mittel, die es ihnen erlauben, Dienstleistern und externen Experten im Fall der Fälle schnell Zugriff auf die nötigen Bereiche zu gewähren. Die Schwierigkeit bestand dabei bisher darin, die Bedürfnisse beider Seiten in Einklang zu bringen. Durch IoT- und Cloudtechnologie funktionieren Wirtschaft und Gesellschaft als 'Always-on-Modell'. Die Industrie braucht neben entsprechenden IT-Sicherheitsmechanismen vor allem flexible Wege, um die Verwaltung von unterschiedlichen Administrationsaccounts zu erleichtern.

Die Brücke zwischen IT und OT

Ein Wartungszugriff kann viel Aufwand bedeuten: Das Fernzugriffsfenster eines Technikers darf nicht gegen IT-Sicherheitsrichtlinien verstoßen und der gesamte Vorgang muss trotzdem protokolliert werden. Gleichzeitig muss sichergestellt werden, dass es sich nicht um einen geschickt getarnten Angriff handelt. Ein solcher Konflikt zwischen OT und IT kann in der Praxis durch Privileged-Access-Lösungen (PAM) beseitigt werden. Diese lassen sich genau auf die Vorgaben der IT-Abteilungen abstimmen und können dann von der Betriebsverantwortlichen genutzt werden, um Rechte von Nutzern granular zu erweitern. Die Lösung übernimmt dabei die Protokollierung und die Absicherung der Accounts. Für besonders kritische Bereiche können zudem Sessions aufgezeichnet oder das Vier-Augen-Prinzip festgelegt werden. Im Betriebsalltag ist PAM ein einfaches Tool zur Verwaltung von Nutzer mit erhöhten Zugriffsrechten, dass sich agentenlos in jede Umgebung integrieren lässt. Die User brauchen keine umfassenden IT-Kenntnisse und die Freigaben können im Umfang und Zeitraum auf das Nötigste begrenzt werden. Dadurch werden keine Konten mehr vergessen – beispielsweise, wenn ein Angestellter das Unternehmen verlässt. Auch das ungewollte Teilen von Zugängen wird unterbunden. IT-Verantwortliche können zudem Sicherheitsvorgaben einfacher umsetzen: Alle Aktionen werden aufgenommen und bei Problemen ist nachvollziehbar, wie es zu einem Vorfall kommen konnte. Cyberangriffen kann zudem durch Passwortmanagement und Segmentierung vorbeugt werden. Gerade bei Ransomware wird die Bedrohung deutlich abgemildert. Zudem können Angriffe aus dem Inneren einer Firma leichter enttarnt und gesperrt werden.

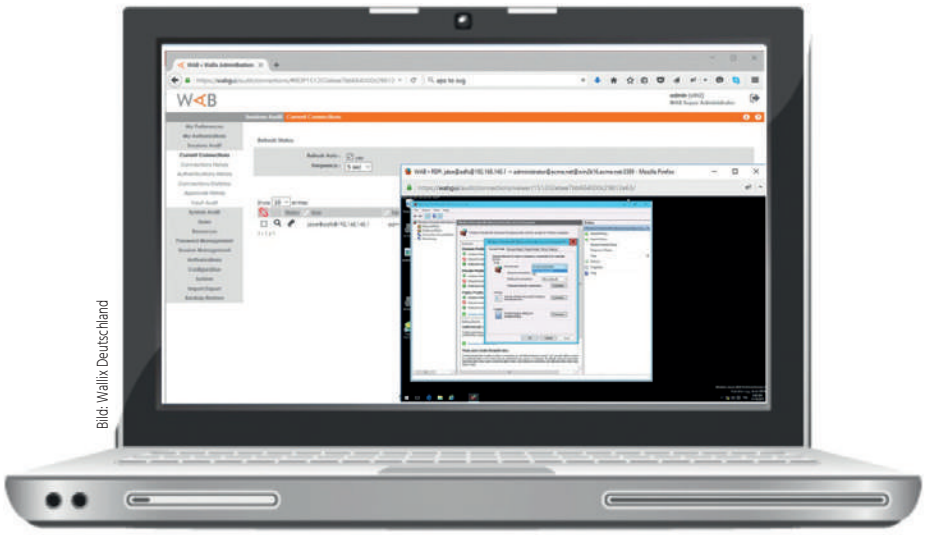


Bild: Wallix Deutschland

Um Konflikte zwischen OT und IT zu beseitigen, kann eine PAM-Lösung die richtige Wahl sein. Diese kann auf die Anforderungen beider Seiten abgestimmt werden.

Jeder hat Sicherheitsbedenken

Für jedes Produktionsunternehmen liegt die Zukunft in der Digitalisierung, und in fast jeder Organisation gibt es dabei Sicherheitsbedenken. Die Anmerkung des BSI ist dabei keine neue Erkenntnis, den entsprechenden Abteilungen in den Firmen fehlt es jedoch oft an praktischen Mitteln, um die Gesamtherausforderung umzusetzen. Durch eine gemeinsame Management-Plattform für Accounts mit erhöhten Zugriffsrechten können Unternehmen eine Grundlage schaffen, um die unterschiedlichen Anforderungen von IT-Security und Betriebsabläufen abzudecken. PAM bietet daher die Möglichkeit, die kontrastreichen Anforderungen von Produktivität und IT-Sicherheit unter einen Hut zu bringen. Besonders Accounts mit erhöhter Sicherheitsfreigabe sind hier im Visier der Cyberkriminellen, da sie den Angreifern eine breite Palette zur deren Bereicherung eröffnen. Mikromanagement allein ist schon zeitaufwendig und unwirtschaftlich. Durch die speziellen Anforderungen potenziert sich diese Problematik – falls sich eine Organisation nicht entsprechend aufstellt. ■

Der Autor Markus Westphal ist Director Central Europe & DACH bei Wallix.

www.wallix.com

Gefahren frühzeitig erkennen

Lösung zur Anomalieerkennung

Im Zuge der Digitalisierung müssen Industrieunternehmen beim Management ihrer Industrial Control Systems (ICS) umdenken, um sowohl Cybersicherheit als auch Produktivität zu gewährleisten. Die Netzwerkmonitoring-Ergebnisse bei einem Stahlunternehmen zeigen, wie intransparent und unsicher die Netzwerke noch sein können.

Die zunehmende Vernetzung der Fertigung stellt Unternehmen vor neue Herausforderungen: Zum einen erhöht sich die Anzahl und Heterogenität der Komponenten, was die Komplexität steigert und Risiken von Netzwerkstörungen birgt. Zum anderen werden Industrial Control Systems (ICS) durch die Anbindung an die Office-IT anfällig für externe Störungen wie Schadprogramme, Cyberattacken oder Manipulation. Laut einer Bitkom-Studie kosten Angriffe auf die IT-Infrastruktur allein Unternehmen in Deutschland jährlich rund 55 Milliarden Euro. Dieser Wert berücksichtigt noch nicht die Stillstände, die sich aus technischen Fehlerzuständen und Netzwerkproblemen ergeben. Das US-amerikanische Analystenhaus Gartner beziffert die ungeplante Stillstandzeit auf jährlich durchschnittlich 87 Stunden

Bild: ©skeeze / Pixabay.com

pro Unternehmen. Bei Kosten und Verlusten zwischen mehreren Tausend bis hin zu Hunderttausend US-Dollar je Stunde entstehen somit noch weitere Schäden. Das Analystenhaus Forrester Consulting fand zudem heraus, dass nur 18 Prozent aller Verantwortlichen zuverlässig alle Komponenten und Vorgänge in ihrem Industrial Control System kennen.

Kleine Störung, große Wirkung

Die Transparenz und das vollständige Wissen über die Kommunikationsvorgänge und Teilnehmer innerhalb der ICS ist jedoch Grundlage, um diese effizient zu betreiben. Gerade in automatisierten Fertigungen können bereits kleine Störungen zu Qualitätseinbußen und Produktionsunterbrechungen führen. Das gilt umso mehr, wenn Echtzeitprozesse im Spiel sind. Im Rahmen von langfristigen Netzwerkmonitoring-Projekten sowie Stabilitäts- und Sicherheitsaudits in Industrie-4.0-Unternehmen tauchen immer wieder Sicherheitslücken und technische Fehlerzustände auf. Davon sind selbst gut gepflegte ICS nicht ausgenommen. Um derartige Anomalien zu erkennen eignet sich beispielsweise die Anomalieerkennung Rhebo Industrial Protector. Diese überwacht die Kommunikation innerhalb eines ICS.

Schnell erste Ergebnisse

Die Anomalieerkennung setzte 2017 auch ein deutsches Stahlunternehmen ein, um eine Bestandsaufnahme seines ICS vorzunehmen. Die Lösung wurde dazu passiv und rückwirkungsfrei in das zu überwachende ICS integriert. Erste Ergebnisse lagen bereits direkt nach der Inbetriebnahme vor. Eine Detailanalyse der Kommunikationsmuster im ICS machte weitere Anomalien sichtbar, welche die Cybersicherheit oder sogar die Produktivität der Fertigung hätten beeinträchtigen können.

Technische Fehlerzustände nicht vernachlässigen

Auch wenn der Fokus vieler Netzwerkmanagement-Strategien auf der IT-Sicherheit liegt, sollten technische Fehlerzustände nicht vernachlässigt werden. Fehlerhafte Einstellungen bei Routern oder Firewalls,

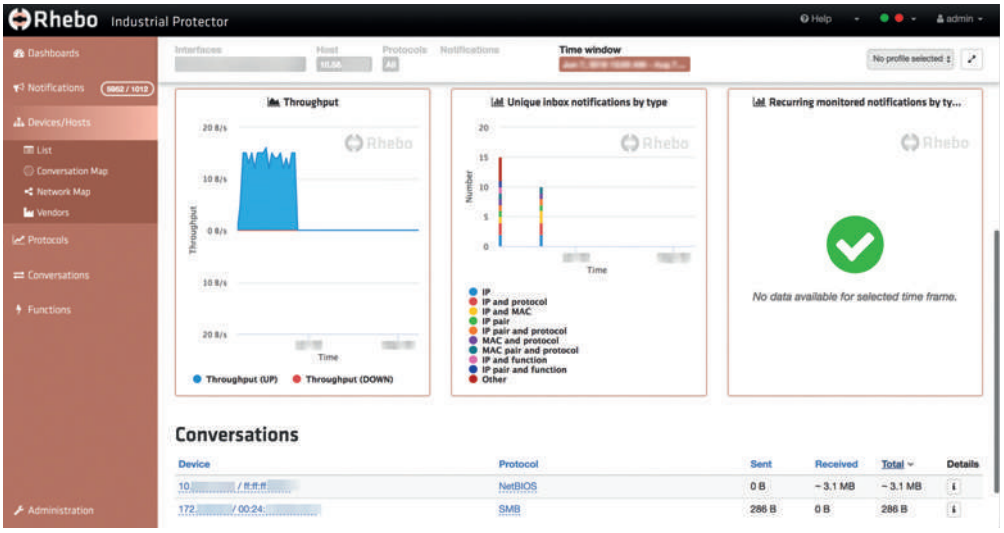


Bild: Rhebo GmbH

Die frei konfigurierbare Bedienoberfläche des Rhebo Industrial Protector zeigt gebündelt Ereignisse und Parameter im ICS an.

widersprüchliche Gerätekonfigurationen, falsch ausgelegte Kapazitäten oder beschädigte Komponenten beeinflussen die Funktionalität des ICS. Im Fall des Stahlunternehmens identifizierte die Anomalieerkennung unter anderem verschiedene Fehlermeldungen und TCP-Prüfsummenfehler. Die Prüfsumme gibt Aufschluss über die Datenintegrität der Kommunikation. Prüfsummenfehler deuten daher auf Daten- oder Übertragungsfehler hin, die häufig durch fehlerhaftes Netzwerkequipment entstehen. Diese können dann zu Verzögerungen oder Ausfällen bei Echtzeitprozessen führen, was die Produktivität beeinträchtigt. Bei einer SPS wurde beispielsweise eine bislang unentdeckte Fehlermeldung innerhalb des S7-Protokolls, das zur Programmierung von SPSen eingesetzt wird, entdeckt. Diese wies auf einen möglichen Programmierfehler hin, der mittelfristig die Funktionalität der SPS hätte gefährden können.

Unentdecktes aufgedeckt

Wie eine Studie des SANS Institutes zeigt, verbinden sich 32 Prozent aller IIoT-Geräte automatisch mit dem Internet. Dabei werden traditionelle IT-Sicherheitsschichten regelmäßig umgangen. Auch im Stahlunternehmen fanden sich mehrere, zuvor unentdeckte Sicherheitslücken: Dazu gehörte u.a. ein vermutliches ARP(Address Resolution Protocol)-Spoofing über einen nicht registrierten Einplatinenrechner sowie sowie der unregulierte Versand sicherheitsgefährdender Dateien. Mittels des ARP-Spoofings gibt sich der Hacker beispielsweise gegenüber dem Kontrollraum als Steuerung aus, während er in Richtung des Production Floors vorgibt, der Controller zu sein. Damit kann er in beide Richtungen die Prozesse manipulieren. Im vorliegenden Fall wurde das nicht autorisierte Gerät umgehend entfernt. Des Weiteren empfing ein Windowsrechner, der für die Entwicklung von Siemens-Programmen (Simatic) genutzt wird, eine nicht benötigte ini-Datei, ein Dateityp, der häufig zur Verbreitung von Schadsoftware genutzt wird. Die beteiligten Geräte wurden identifiziert und die Kommunikation unterbunden.

Gefahren erkannt, Gefahren gebannt

Das Stahlunternehmen erlangte durch den Einsatz der industriellen Anomalieerkennung Klarheit aller Vorgänge in seinem Industrial Control System. Fehlkonfigurationen und potentielle Sicherheitsrisiken wurden eindeutig identifiziert und beseitigt. Die Grundlage für eine störungsfreie, stabile und sichere vernetzte Produktion ist somit gelegt. ■

Der Autor Martin Menschner ist CTO bei der Rhebo GmbH.

www.rhebo.com

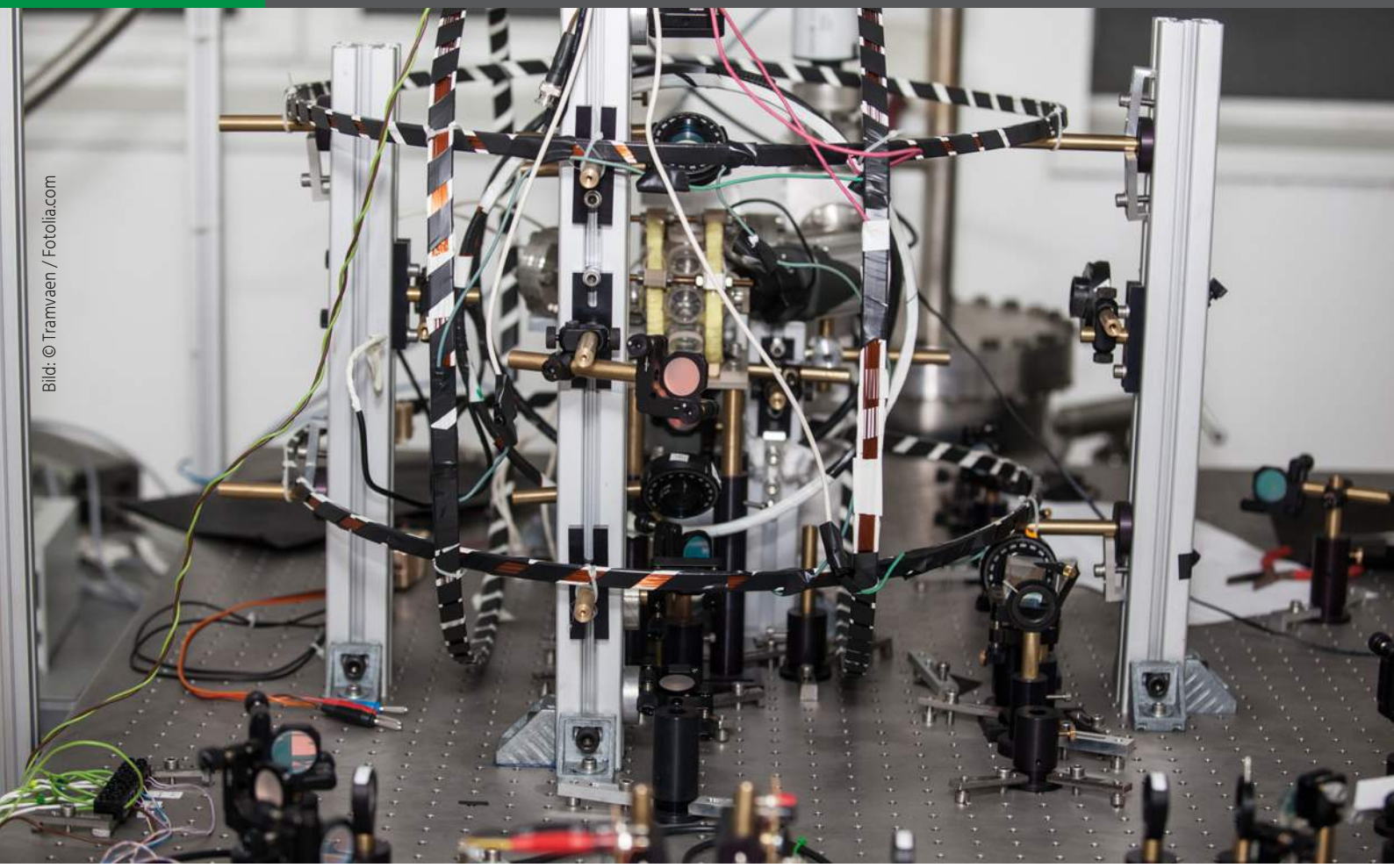


Bild: © Tramvaen / Fotolia.com

Quanten-Computing

Götterdämmerung für die moderne Krypthographie?

Die superschnellen Quantensysteme sind dafür prädestiniert, die Datenströme in Industrie-4.0-Umgebungen und für Anwendungen des Internet of Things zu verarbeiten. Das findet so noch nicht statt, aber Simulationsplattformen stehen bereit, um etwa IoT-Anwendungsfälle zu programmieren. Bei allen Vorteilen dieser Technologie ist es dringend angeraten, neue Sicherheitsstandards für eine quantensichere Verschlüsselung zu prüfen.

Die Plattformökonomie ist eine Herausforderung für die Fertigungsbranche: Damit Unternehmen dabei von einem möglichst großen Nutzen profitieren, müssen Serviceplattformen aufgebaut und das Domänenwissen verbunden werden. Gelingt das nicht, drohen branchenfremde Drittanbieter, Nischen zu erobern. Ihnen mag das Fachwissen über die Maschinen- und Anlagenwelt fehlen, aber sie wissen, wie man Daten-Services entwickelt. Eine Anwendungsmöglichkeit für Industrie 4.0 und Internet of Things (IoT) stellt die vorausschauende Wartung (Predictive Maintenance) dar. Sensoren produzieren dabei Datenströme, die von einer Streaming-Analytics-Software in einer bestimmten Reihen- und Zeitfolge bearbeitet wird. Aus den Sensordaten lassen sich mittels integriertem maschinellem Lernen und den statistischen Wartungsinformationen Erkenntnisse extrahieren und in Echtzeit anwenden sowie Vorhersagen treffen. Der Anwendungsfokus der Plattformökonomie wird sich jedoch in dem Maße weiten müssen, wie die Vernetzung fortschreitet, da dadurch noch größere und variablere Datenströme entstehen. Durch die Weiterentwicklung der Plattformökonomie müssen zukünftig noch mehr Daten verarbeitet und neue Anwendungsfälle entwickelt werden. Die Quantentechnologie scheint prädestiniert zu sein, beim Lösen dieser beiden Herausforderungen entscheidend mitzuhelfen.

Parallele Datenverarbeitung

Im Gegensatz zu herkömmlichen Superrechnern können Quantenrechner Unmengen an Daten parallel verarbeiten. Diese Fähigkeit wird sich gerade in einer Industrie-4.0-Umgebung und bei diversen Anwendungsszenarien für das IoT als großer Vorteil erweisen. Für das Analysieren und Optimieren von Produktionsprozessen und vernetzten Fertigungsumgebungen eröffnen sich endlose Möglichkeiten, die gewaltigen Datenmengen mit Quantencomputern in Echtzeit zu beherrschen und nutzbar zu machen. Je mehr Variablen eine Berechnung aufweist, desto mehr kommt die Überlegenheit der Quantenrechner zum Tragen. Den Grundstein für das parallele Durchrechnen der verschiedenen Lösungswege in Sekunden oder Millisekunden legt ein Quantengatter, das die sogenannten Quantenbits, kurz Qubits, verschränkt und ihre Zustände von Null, Eins oder irgendwo dazwischen manipuliert. Diese Zustandsänderungen der Qubits lassen sich messen und für das Ergebnis in Null- oder Eins-Werte 'einfrieren'. Es bedarf jedoch besonderer Quantenalgorithmen, um ein Quantengatter nutzen zu können.

Supraleiter und die Alternativen

Viele der möglichen Anwendungsfelder wie Verkehrssimulationen, Finanztransaktionen oder eben IoT-Szenarien setzen allerdings eine Rechenleistung voraus, die nicht auf 50 bis 100Qubits beruht, sondern bis zu 1.000Qubits verlangt. Der Blick auf den aktuellen Entwicklungsstand offenbart, dass trotz großer Fortschritte noch einiges zu tun bleibt, bis Quantensysteme diese Ansprüche erfüllen und in großen Stückzahlen am Markt verfügbar sind. Das wird jedoch erst in zehn bis 20 Jahren soweit sein. Momentan setzt Googles Quantenprozessor Bristlecone mit 72Qubit den Maßstab, gefolgt von IBM, dessen Quantenrechner 50Qubit leisten soll. Hauchdünn dahinter rangiert Intel: Der Halbleiterhersteller hat seinen Chip Tangle Lake mit 49Qubit ausgestattet. Am weitesten gediehen ist der Ansatz, der auf Supraleiter setzt. Doch der Aufbau dieser Systeme beispielsweise von Google und Intel sind überaus komplex, um sie für den Supraleitungseffekt bis fast auf den absoluten Nullpunkt – also -273,15°C oder 0°K – herunter zu kühlen. Diese aufwendige Ausstattung schlägt sich im Anschaffungspreis nieder, der bei einer zweistelligen Millionensumme beginnt. An technologischen Alternativen wird geforscht, hauptsächlich um den Aufbau eines Quantensystems zu vereinfachen. In die Richtung weisen Spin-Qubits, mit denen sich Intel und das niederländische Forschungszentrum Qutech beschäftigen. Die Fachleute erzeugen die Spin-Qubits mit Mikrowellenimpulsen, welche die Drehung eines Elektrons auf Siliziumsubstrat steuern. Diese Technologie funktio-

Bild: Atos Information Technology GmbH

Spezialisten ohne die finanziellen Mittel für einen eigenen Quantencomputer können mit dem Quantensimulator von Atos experimentieren.

niert bereits bei 1°K – eine scheinbar geringe Temperaturveränderung, die eine deutliche Systemvereinfachung erlaubt. In eine ganz andere Richtung blickt das Institut für Quantenoptik und Quanteninformation (IQOQI) der Universität Innsbruck – es forscht an Qubits in Ionenfallen. Eine Vielzahl von Experten sieht im Noisy Intermediate-Scale Quantum (NISQ) einen vielversprechenden Ansatz. Dieser kommt ohne die üblichen komplexen Fehlerkorrekturverfahren aus. Auch das führt zu einem einfacheren Quantensystem, geht aber mit einem höheren Rauschen, also einer höheren Fehlerrate, einher. Das Manko lässt sich durch spezielle Quantenalgorithmen wieder ausgleichen, die auf flachen Schaltkreisen (Shallow Circuits) laufen.

Forscher simulieren erst einmal

Einsatzfähige Systeme existieren zwar, aber die hohen Anschaffungskosten halten die Anwendergemeinde klein. Cloud-Plattformen stellen in der Hinsicht einen preiswerten Zugang dar. So können Interessenten über eine Cloud-Plattform auf einen Quantencomputer der Reihe IBM Q zugreifen, der in einem Forschungslabor von IBM steht. Ebenso sind Quantensimulatoren mit deutlich weniger Anschaffungskosten verbunden. Unter diesen Rahmenbedingungen kristallisieren sich derzeit vor allem zwei Anwendergruppen heraus. Zum einen sind es Forschungseinrichtungen, die Quantenalgorithmen entwickeln und testen. Die andere Anwendergruppe bilden Universitäten, die Studenten in Programmiersprachen für Quantencomputer ausbilden. Die erste Gruppe repräsentiert das Oak Ridge National Laboratory (ORNL) in Oak Ridge (US-Bundesstaat Tennessee). Das ORNL setzt einen Quantensimulator von Atos ein, um Algorithmen zu entwickeln, zu optimieren und mithilfe von Emulation zu testen. Auf der Atos Quantum Learning Machine (QLM) lassen sich bis zu 41Qubit simulieren. Das ORNL nutzt diese Möglichkeit, um Algorithmen ausgiebig zu testen. Danach führen die Forscher ihre erstellten Algorithmen auf einem echten Quantencomputer von IBM aus. Dieses Vorgehen ist deutlich effizienter; als ausschließlich die teure Hardware zu verwenden.

Sicherheit wichtiger denn je

Ein weiterer Kunde von Atos, die FH Oberösterreich in Hagenberg, nimmt noch aus einem anderen Grund eine Vorreiterolle ein: Informationssicherheit. Warum ist das nötig? Die Rechenleistung von Quantensystemen kann mithilfe des Shor-Algorithmus gegen asymmetrische Kryptosysteme wie RSA oder ECC (Elliptic Curve Cryptography) gerichtet werden. Mit einem Beschleuniger von 1.000 logischen Qubits werden sich diese Kryptosysteme, die derzeit zur Sicherung des Internets verwendet werden, in jedem Fall brechen lassen. Zudem lässt sich die Rechenleistung der Quantensysteme auch gegen symmetrische Verfahren wie AES (Advanced Encryption Standard) und SHA (Secure Hash Algorithm) richten. Auf lange Sicht droht nicht das gänzliche Entschlüsseln, aber ein Halbieren der eingesetzten Schlüssellängen. Das National Institute of Standards and Technology (NIST) in den USA hat aufgrund dieses Bedrohungspotenzials eine Initiative mit dem Ziel gestartet, neue standardisierte Verschlüsselungsverfahren zu entwickeln. Der Evaluierungsprozess wird etwa drei bis fünf Jahre dauern. Anschließend werden auf Basis der Ergebnisse neue Post-Quanten-Verschlüsselungsstandards erstellt. Das Unterfangen ist zwar aufwendig und kostet viel Zeit, auf der anderen Seite ist dieselbe Verschlüsselungstechnologie in bestimmten Systemen bis zu 20 Jahre im Einsatz. Je früher Kraftwerke, Industrieanlagen, Maschinen oder IoT-Komponenten mit einer zukunftssicheren Datenverschlüsselung ausgestattet werden, desto geringer fällt später der Aufwand für die Nachrüstung aus. Somit gewinnt die Entwicklung neuer Sicherheitsstandards auch für die Fertigungsbranche an Bedeutung, um beispielsweise den Datentransport zwischen IoT-Endpunkten und Gateway in einem IoT-System oder 5G-Protokolle abzusichern. An dieser Stelle kommen die Quantenrechner wieder ins Spiel: Mit ihnen lassen sich auch solche Datentransfers schützen, etwa durch eine starke Verschlüsselung und sichere Verfahren für den Austausch von Schlüsseln.

Pflicht oder Kür?

Nur wenige Akteure investieren bisher in die extrem teure Hardware für Quantensysteme. Simulationsplattformen bieten hingegen eine wichtige Alternative, um in die Nutzung der Quantentechnik einzusteigen. Die fortschreitende Vernetzung liefert der Fertigungsbranche gleich zwei wesentliche Motive, sich mit Quantensimulatoren zu beschäftigen: Solch eine Plattform ließe sich ideal für das Programmieren von IoT-Anwendungsfällen nutzen. Auch könnten mit der Rechenleistung der Simulatoren noch fehlende Anwendungen für Big Data und künstliche Intelligenz geschaffen werden. Wer zeitig in die nötige Entwicklungsarbeit einsteigt, stärkt seine Wettbewerbsfähigkeit. Wenn Industrie- und Fertigungsunternehmen ihre Prioritäten jedoch in anderen Bereichen sehen, sollten sie sich den Sicherheitsaspekt vor Augen halten: Quantensimulatoren helfen, ihr künftiges Industrie 4.0- und IoT-Geschäft abzusichern. Zunächst könnte mit dem Simulator die Stärke von Quantencomputer-gestützten Entschlüsselungstechniken überprüft werden. Der nächste logische Schritt wäre das Entwickeln von Lösungen, die vor Entschlüsselungsversuchen schützen. Ohne solche Algorithmen lassen sich in Zukunft persönliche sowie Kunden- und Geschäftsdaten nicht mehr ausreichend vor dem Zugriff Unbefugter sichern. ■

Der Autor Philippe Duluc ist CTO Big Data und Security bei Atos Information Technology GmbH.

www.atos.net

Schutz vor Distributed-Denial-of-Service-Attacken

Waschstraße für den Internet-Traffic

Bild: PlusServer GmbH

Sind der Online-Shop oder Unternehmensanwendungen nicht erreichbar, könnte dahinter eine Distributed-Denial-of-Service-Attacke stehen. Bei dieser Art von Cyberangriff wird das Ziel durch eine große Anzahl gleichzeitiger Anfragen überlastet. Um sich davor zu schützen, lassen sich verschiedene Security-Lösungen kombinieren.

Durch die Digitalisierung werden die Infrastrukturen im Unternehmen nach außen geöffnet und mit Schnittstellen an das Internet angebunden. So können Unternehmen schnell und flexibel mit Kunden und Dienstleistern kommunizieren, unmittelbar auf Anforderungen reagieren, just-in-time produzieren und so die Lagerhaltungskosten verringern. Doch trotz aller Vorteile birgt diese Öffnung auch Gefahren: Je mehr Schnittstellen nach außen bestehen, desto anfälliger werden die Infrastrukturen für Angriffe über das Netz wie beispielsweise DDoS-Attacken (Distributed Denial of Service). Aus diesem Grunde sollte zu jeder Digitalisierungsstrategie auch die entsprechende Securitystrategie inklusive DDoS-Schutz gehören.

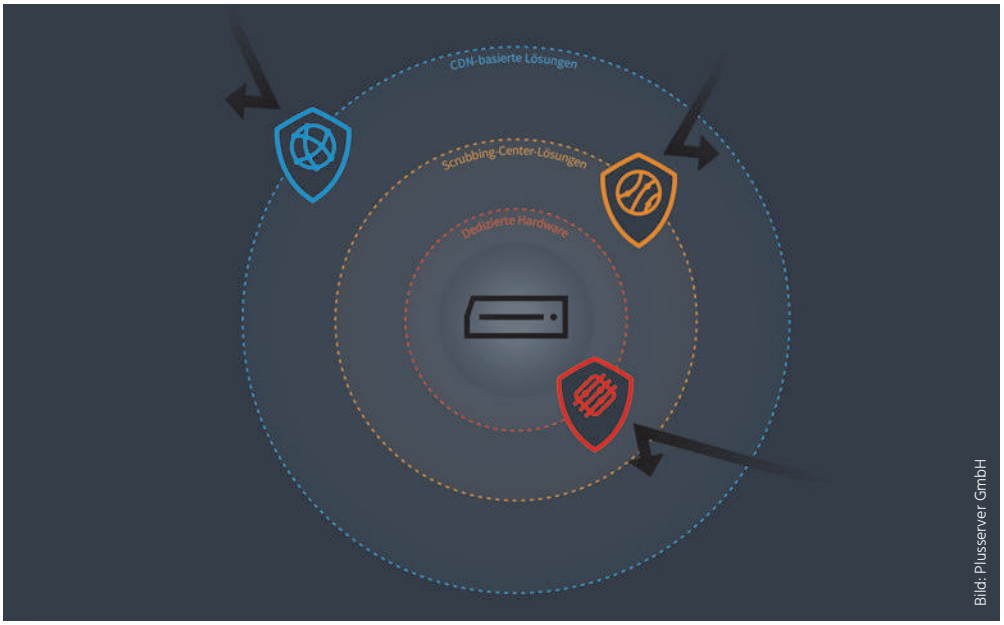
Angriff oder Ablenkungsmanöver?

Cyberattacken können geschäftskritische Unternehmensanwendungen vorübergehend außer Gefecht setzen oder auch dauerhaft schädigen. Die Angriffsmethoden reichen von volumetrischen DDoS-Angriffen, die Zielsysteme durch eine hohe Anzahl gleichzeitiger Anfragen überlasten, bis hin zum Ausnutzen von Sicherheitslücken in Webanwendungen. Oft werden auch mehrere Angriffsarten kombiniert, um beispielsweise durch einen DDoS-Angriff von einem Angriff auf Webanwendungen abzulenken. So kann sich ein Angreifer Zugriff auf Datenbanken verschaffen, um Daten zu stehlen oder zu manipulieren. Im schlimmsten Fall können dann auch Entwicklungs- oder Produktionsdaten, die unternehmensinterne Kommunikation sowie vertraulichen Informationen über neue Produkte betroffen sein.

Betriebliche Vorgänge geraten ins Stocken

Wenn Systeme und die darauf betriebenen Anwendungen infolge eines DDoS-

Angriffs nicht erreichbar sind, können betriebliche Vorgänge ins Stocken geraten: Kunden sind nicht in der Lage, neue Bestellungen aufzugeben, Lieferanten werden nicht rechtzeitig über benötigte Werkstoffe informiert und die Produktion gerät in Verzug. Unter Umständen können auch Vertragsstrafen drohen, wenn die Auslieferung von Waren nicht wie geplant stattfindet, weil beispielsweise die Lkw-Flotte nicht mehr koordiniert werden kann. Hinzu kommen wirtschaftliche Verluste aufgrund unproduktiver Mitarbeiter, wenn diese nicht auf ihre Daten zugreifen können oder die Kommunikation extern sowie intern ausgefallen ist. Imageverluste drohen beispielsweise, wenn Kundendaten entwendet wurden. Um die Wahrscheinlichkeit eines erfolgreichen Angriffs aus dem Netz zu reduzieren, stehen eine Reihe von Mitteln zur Verfügung.



Je nach Lösungstyp findet die Mitigation an weltweit verteilten Knotenpunkten, in einem Scrubbing Center oder direkt im Rechenzentrum statt.

DDoS-Schutz für Unternehmen

Die Auslagerung von Diensten in externe Rechenzentren oder Cloudlösungen kann ein erster Schritt sein, um die Sicherheit der Daten und Anwendungen zu steigern – sofern der Anbieter eine Rund-um-die-Uhr-Betreuung der Infrastruktur im Rahmen eines Managed Hostings zur Verfügung stellt. Dazu gehören die Überwachung der Systeme sowie regelmäßige Back-ups oder ein Patch-Management. Auch sollte ein Anbieter verschiedene DDoS-Schutzlösungen im Portfolio aufweisen. Managed-Hosting-Provider arbeiten dabei meist mit Security-Lösungsanbietern zusammen. Zertifizierungen wie ISO27001 oder IT-Grundschutz nach den Vorgaben des Bundesministeriums für Sicherheit in der Informationstechnik bieten darüber hinaus Orientierung, um die Datensicherheit beim Managed-Hosting-Anbieter einzuschätzen. Für den DDoS-Schutz bietet sich für produzierenden Unternehmen vor allem eine Lösung an, die die gesamte IT-Infrastruktur berücksichtigt. Das bedeutet, dass neben der Website oder dem Webshop auch Mailsysteme, Datenbanken oder ERP-Anwendungen vor Attacken geschützt werden. Diese Lösungen arbeiten mit sogenannten Scrubbing-Centern – einer Art Waschstraße für den Internet-Traffic – in Kombination mit einer Web Application Firewall (WAF). Da der eingehende Datenverkehr mithilfe des Border Gateway Protocols auf die Scrubbing Center umgeleitet bzw. geroutet wird, spricht man auch von BGP-basierten Lösungen. Die Abwehr von Schadtraffic erfolgt bei dieser Methode bereits am Rande des Netzwerks, bevor er das Rechenzentrum erreicht. So sorgt die Lösung auch dafür, dass während eines Angriffsversuchs die Leitungen ins Rechenzentrum für den gewollten Verkehr frei bleiben. Eine WAF bietet in dieser Konstellation Schutz gegen Angriffe, die direkt auf Schwachstellen in Webanwendungen abzielen. Sie unterscheidet sich von herkömmlichen Firewall-Lösungen insofern, als dass sie die ein- und ausgehende Kommunikation direkt auf der Anwendungsebene überwacht. Klassische Firewalls arbeiten hingegen auf der Netzwerkebene und stellen daher keinen Schutz gegen Angriffe dar, die auf dem Hypertext Transfer Protocol (HTTP) basieren. Die Arbeit der WAF sollte zusätzlich mit regelmäßigen Vulnerability-Scans unterstützt werden. So können Sicherheitslücken in den Anwendungen von vorneherein aufgedeckt und beseitigt werden, sofern bereits ein entsprechender Sicherheitspatch zur Verfügung steht.

Angiffe nehmen zu

Wie in vielen anderen Bereichen sind auch in der Cyberkriminalität bestimmte Trends identifizierbar, auf welche die Security-Firmen umgehend reagieren und ihre Lösungen entsprechend optimieren. In der jüngsten Ausgabe seines State of the Internet Security Reports (Sommer 2018) verzeichnet Akamai, ein Anbieter von DDoS-Schutzlösungen, einen weltweiten Anstieg der DDoS-Angriffe um insgesamt 16 Prozent. Webanwendungen wurden zudem um 38 Prozent häufiger angegriffen als im Sommer des Vorjahres. Die Security-Experten von Link11 konzentrieren ihre Auswertung auf die DACH-Region und registrierten im ersten Quartal 2018 durchschnittlich täglich 160 Attacken auf verschiedene Ziele. Der Spitzenwert bei der Angriffsbandbreite betrug 212GBit/s. Solche großvolumigen Angriffe traten in jüngerer Vergangenheit vermehrt auf, was u.a. auf die Kaperung ungeschützter IoT-Geräte durch Cyberkriminelle zurückgeführt wird. Da deren Zahl in Zukunft weiter ansteigen dürfte, vermuten Security-Experten weitere großangelegte Attacken in der nächsten Zeit. Die Vorsorge durch geeignete Schutzmaßnahmen sollte somit auf der Agenda aller IT-Verantwortlichen in Unternehmen stehen. ■

Der Autor Patrick Czech ist Head of Cloud Product Manager bei PlusServer GmbH.

www.plusserver.com

Bild: © Sashkin - Fotolia.com

Blockchain und Datensicherheit

Branchenriesen wie Airbus, Siemens und Daimler beschäftigen sich aktuell damit, wie sich Blockchain-Technologie sinnvoll einsetzen lässt. Die Fachleute sollten jedoch eine gewisse Skepsis bewahren und sich zunächst mit der Vertraulichkeit von Daten beschäftigen. Die entscheidende Frage dazu lautet: Welche Daten können in einer Blockchain überhaupt gespeichert werden?

Die Daten, die in eine Blockchain geschrieben werden, sind in der Regel öffentlich. Sogar 'private', zentral verwaltete, Blockchains können von den Teilnehmern eingesehen werden. Darüber hinaus werden die in die Blockchain geschriebenen Daten nicht selbst verwaltet. Stattdessen befinden sie sich in einem geteilten Ledger, das in einem dezentralen System gespeichert wird. Ohne ein umfassendes Verständnis davon, welche Daten in eine Blockchain gehören und welche nicht, können erhebliche Datenschutz- und Sicherheitsrisiken entstehen. Unternehmen müssen die Risiken einschätzen können, für den Fall, dass die Blockchain ihr volles Potenzial entfaltet. Gelegentlich werden diese Risiken mit denen in der Frühphase des Internets verglichen. Damals bestand die Gefahr, dass Unternehmen aus dem Gesundheitswesen, der Produktion und vor allem dem Finanzwesen lahmgelegt werden könnten.

Kein herkömmliches Datenbankverwaltungssystem

Außerdem muss berücksichtigt werden, dass die Blockchain kein Datenbankverwaltungssystem im herkömmlichen Sinne ist. Sie eignet sich für unveränderliche Aufzeichnungen und einen Vertrauenskonsens. Datenbankverwaltungssysteme sind im Gegensatz zu Blockchains für hohe Lese- und Schreibraten sowie komplexe Abfragen und Datensuchen entwickelt. Deswegen werden Blockchain-Bereitstellungen durch ein Datenbankmanagementsystem (DBMS) erweitert, das wichtige operative und datenintensive Funktionen ausführt. Betriebsdaten sind die Grundlage für ein erfolgreiches Geschäft, indem sie Echtzeitanwendungen und Analysen im gesamten Unternehmen ermöglichen. Leider haben viele Unternehmen Schwierigkeiten, die erfolgskritische Datenintegration, erweiterte Suche und Priorisierung von Betriebsdaten effizient und dauerhaft bereitzustellen. Mit einem Operational Data Hub (ODH)-Ansatz können diese Herausforderungen gemeistert und die Grundlagen für Fortschritte mit der Blockchain geschaffen werden. Anhand dieser Methode können Unternehmen einfach Daten aus verschiedenen Quellen oder Silos an einem Ort zusammenführen und somit Datensu-

che und -harmonisierung, Sicherheit und Governance sowie operationale Funktionen in Echtzeit verbessern.

Achtung Datenschutz

Ob eine private Blockchain erstellt wird oder Architekturen implementiert werden, die sich eine öffentliche Blockchain zunutze machen – es muss zunächst entschieden werden, welche Plattform für die Bereitstellung am besten geeignet ist. Obwohl die Blockchain über inhärente Sicherheitseigenschaften verfügt, können Schwachstellen manipuliert werden, besonders in Zusammenhang mit Technologien, die mit einer Blockchain kommunizieren. Die meisten Fälle, in denen Sicherheitslücken im Zusammenhang mit Blockchains – zum Beispiel Bitcoin-Umwandlungen – ausgenutzt wurden, waren das Ergebnis von Schwachstellen in verwendeten Zusatztechnologien, schlecht durchdachten Datenarchitekturen oder beidem. Idealerweise besteht jede Technologie, die in einer Blockchain-Architektur eingesetzt wird, aus einer Infrastruktur mit integrierten Sicherheitsmechanismen, die nachfolgend erläutert werden.

Den Datenzugriff beschränken

Es gibt Daten, die Unternehmen niemals in eine öffentliche Blockchain laden würden, etwa elektronische Krankenakten oder Sozialversicherungsnummern. Mit einer privaten Blockchain müssen Sicherheitsfunktionen stark genug sein, um den Zugriff durch unautorisierte Personen auf ähnlich vertrauliche Informationen zu verhindern. Gemeint ist hier der Bedarf, vertrauliche Daten wie personenbezogene Daten verfassen zu können. Dadurch können Unternehmen Leseberechtigungen für ihre Daten an autorisierte Personen vergeben, indem sie vertrauliche Informationen entfernen, ersetzen oder ausblenden, um Datenverletzungen oder Verstöße gegen Gesetze oder Vorschriften zu vermeiden. Die Sicherheit auf Elementebene ermöglicht zudem, bestimmte Teile in Dokumenten für ausgewählte Benutzer auszublenden. Nicht zuletzt kann die vollständige Verschlüsselung vertraulicher Daten sicherstellen, dass diese nicht von unbefugten Parteien aufgerufen werden können. Das gilt vor allem für Daten, die gerade übermittelt oder durch nicht vertrauenswürdige Netzwerke übertragen werden.

Validierung der Datenqualität

Blockchains können erst dann Verantwortung für die Genauigkeit und Qualität von Daten übernehmen, wenn sie in die Blockchain eingegeben wurden. „Man muss auf die Qualität der Daten vertrauen können, die aus den bestehenden Quellsystemen der Unternehmen gewonnen werden“, schreibt Deloitte in seinem Bericht ‘Blockchain & Cyber Risk’. Darin wird auch Prakash Santhana, Advisory Managing Director bei Deloitte U.S, zitiert: „Die größte Schwachstelle in der Blockchain-Architektur liegt jenseits der Architektur, in sogenannten Oracles, die vertrauenswürdig sein müssen. Ein beschädigtes Oracle kann einen Dominoeffekt im gesamten Netzwerk verursachen.“ Oracles sind im Kontext von Blockchain eine Art von Agent, der Geschehnisse aus der Realwelt verifiziert und diese Smart Contracts bereitstellt. Daten sollten also unbedingt vor der Blockchain validiert werden.

Richtlinien zu Data Governance

Es ist wichtig, Richtlinien zu Data Governance aufzustellen und an bewährten Verfahren festzuhalten, wie die Wahrung der Zugriffskontrollen, Metadaten, Datenqualität und Sicherheitsfunktionen innerhalb und außerhalb der Blockchain. Eine der wahrscheinlichsten Schwachstellen mit Distributed-Ledger-Technologie entsteht außerhalb der Blockchain. Das sind Orte, an denen Blockchains auf andere Computer treffen, die Mitarbeiter und Organisationen für den Zugriff auf Blockchain-Dienste verwenden. Während des Zugriffs auf die Blockchain sind die Daten in der Kette am anfälligsten.

Die Rolle der Daten

Bisher hat sich Blockchain-Technologie vor allem bei digitalen Währungen bewährt. Und es gibt viele weitere, vielversprechende Anwendungsbereiche der Blockchain, die erst noch den Absprung schaffen müssen. Intelligente Verträge etwa bieten die Möglichkeit, eine Art Vertrag ohne menschliche Interaktion abzuschließen – sie sind nur einer von vielen Bereichen, die auf großes Interesse stoßen. Intelligente Verträge können jedoch nur solange von der Technologie profitieren, wie die Intelligenz in der Blockchain auf korrekten Daten basiert. Damit das möglich wird, müssen die Daten, die zu Beginn in den intelligenten Vertrag einfließen, vollständig korrekt sein. Dies trifft auf eine Vielzahl von Branchen zu. Tatsächlich verspricht Blockchain-Technologie auch in der Produktion Unternehmen, die sich auf ihre Aufzeichnungen verlassen können, geringere Risiken und größeres Vertrauen, sofern der durchgängige Datenfluss wohl durchdacht ist. Smart Contracts sind ein weiteres Beispiel dafür, wie die Produktion von Blockchain profitieren könnte. Diese Programmcodes legen nach dem Wenn-dann-Prinzip fest, unter welchen Bedingungen, welche Entscheidung oder Aktion herbeigeführt wird. Meldet eine Anlage zum Beispiel eine Störung, wird automatisch ein Servicetechniker bestellt, der den Fehler behebt. Anschließend wird die Reparatur dokumentiert und die Produktion wieder aufgenommen – alles ohne manuellen Eingriff.

Datenbank als Fundament

Wird eine Blockchain-Technologie mit einer Datenbank aufgewertet, lassen sich die Daten validieren, deren Konsistenz absichern und ein anonymisierter Datenspeicher bereitstellen. Die Datenbank hilft auch beim Umgang mit Risiken sowie der Einhaltung der Compliance, wenn Daten mit anderen Quellen verwoben werden. Das gleiche gilt für die Analyse von Daten, mit denen Unternehmen handlungsorientierte Erkenntnisse gewinnen wollen. Ungeachtet dessen, wie Daten gespeichert oder übertragen werden, liegt ihr Wert letztendlich in den Erkenntnissen, die sich aus ihnen gewinnen lassen. Nur wenn die eingegebenen Daten korrekt sind, kann die Blockchain-Technologie eine wichtige Rolle bei der Umwandlung der resultierenden Datenausgabe spielen. Blockchains können betriebliche Abläufe verbessern und sind laut Deloitte in der Lage, „Transaktionsdaten schneller als jedes andere System zu überprüfen.“ Jetzt ist es Sache der Unternehmen, sich dieses Werkzeug für eine höhere Effizienz und somit Wettbewerbsfähigkeit zunutze zu machen. ■

Der Autor Stefano Marmonti ist
DACH Director bei Marklogic.

www.marklogic.de

Entlastung durch Local Breakouts

Sicherer Datentransfer rund um den Globus

Bild: Leitz GmbH & Co. KG

Die Leitz GmbH & Co. KG, ein Hersteller von Holzbearbeitungswerkzeugen, setzt beim Schutz der Kunden- und Produktivdaten auf eine IT-Sicherheitsstruktur, die vom Hauptsitz in Oberkochen aus administriert wird. Auf Basis der Unified-Threat-Management-Lösungen von Watchguard und zusammen mit dem IT-Dienstleister Fornax, wurden die Produktionsanlagen und die elektronische Abwicklung von Zollanmeldungen sorgfältig gegen ungewollte Zugriffe abgesichert.

Jeder Standort der Leitz GmbH & Co. KG – 36 Vertriebesgesellschaften, sechs Produktionsstandorte und 120 Servicestationen – ist an das zentrale Rechenzentrum des Unternehmens in Oberkochen angeschlossen. Von dort aus stellt ein 15-köpfiges Team alle erforderlichen Services über eine virtualisierte Server-Umgebung bereit. Für den Schutz des Netzwerks ist seit 2006 ein UTM(Unified Threat Management)-Cluster von Watchguard im Einsatz. Hinsichtlich der Anbindung der Standorte gab es bei Leitz bisher unterschiedliche Ansätze: Bei der Mehrzahl der Außenstellen erfolgte der Zugriff von Beginn an über abgesicherte VPN-Tunnel. Bei den größeren Niederlassungen kommt eine MPLS-Umgebung der British Telekom zum Einsatz.. Dieser Status quo wurde jedoch überdacht.

Das Rechenzentrum entlasten

Ein wichtiges Kriterium war dabei die Bandbreite: „Bei unseren VPN-Standorten lief der Datenverkehr vollständig über unser Rechenzentrum in der Zentrale, inklusive des externen Internet-Traffics der einzelnen Lokationen“, berichtet Roland Berndt, Abteilung technische EDV bei Leitz. Um für Entlastung zu sorgen, wurde ein Local-Breakout-Konzept geprüft: „Der Servicequalität unseres zentralen Netzwerks kommt es deutlich zugute, wenn der allgemeine Internetverkehr direkt vor Ort erfolgen kann, ohne den Schritt über das Rechenzentrum in Oberkochen.“

Nur relevante Anwedungen

Zukünftig sollen ausschließlich unmittelbar relevante, interne Prozesse auf der Basis von VPN-Tunneln über die Zentrale laufen – beispielsweise der ERP-Zugriff. Weniger geschäftskritische Anwendungen via Internet sollen parallel dazu über lokale Provider ermöglicht werden – mit den entsprechenden Sicherheitsvorkehrungen

und Multi-WAN-Möglichkeit für zusätzlichen Ausfallschutz. „Im Rahmen der Breakouts ist es wichtig, dass alle Unternehmensvorgaben jederzeit erfüllt werden“, sagt Marko Bauer, Geschäftsführer der Fornax EDV-Service GmbH. Sein Unternehmen unterstützt Leitz seit 2008 im Bereich der IT-Sicherheit.

Alte Plattformen ausgetauscht

Insbesondere die Möglichkeiten der zentralen Verwaltung und Konfiguration über Templates spielten bei der Neuausrichtung der Sicherheitslandschaft eine entscheidende Rolle. Im Zuge dessen wurde auch der bisherige Hersteller auf Herz und Nieren geprüft und die allgemeine Anbieterlandschaft näher betrachtet. „Einen Schnitt brauchten wir in jedem Fall. Es stellte sich jedoch die Frage, ob wir auf die jüngste Modell-Generation von Watchguard bauen oder komplett wechseln“, sagt Berndt. Am Ende entschied man sich für die Hardware des Herstellers und hat mittlerweile fast alle alten 120 Plattformen ausgetauscht. Je nach Größe und Anforderung der Niederlassungen kommen unterschiedliche Hardware-Modelle zum Einsatz. Diese lassen sich jedoch über den System Manager zentral von Oberkochen aus bedienen. Der Rollout erfolgte innerhalb kurzer

Bild: Leitz GmbH & Co. KG

Zukünftig sollen ausschließlich relevante, interne Prozesse per VPN-Tunnel über die Zentrale laufen.

Leitz liefert seine Produkte weltweit aus. Die Security Appliances sind daher Atlas-zertifitiert, um Zollanmeldungen zu erleichern.

Zeit. Die Hardware musste lediglich an den jeweiligen Standort verschickt und dort verbunden werden. Die Konfiguration erfolgt automatisch entsprechend der zentral hinterlegten, individuell anpassbaren Einstellungsvorgaben. Ein IT-Mitarbeier muss nicht vor Ort sein.

Aus für MPLS-Verbindungen

Im Zuge der Umstellung sollen nach und nach auch die kostenintensiven MPLS-Verbindungen abgelöst werden. Zu diesem Zweck wurde im Frühjahr 2017 in der österreichischen Vertriebszentrale in Riedau das erste UTM-Hochverfügbarkeitscluster jenseits des zentralen Rechenzentrums in Oberkochen in Betrieb genommen. Die darüber erzeugte VPN-Verbindung mit dem zentralen Rechenzentrum inklusive der Option lokaler Breakouts soll das MPLS-Konstrukt mittelfristig ersetzen. Nach erfolgreicher Pilotphase sollen so bis 2019 alle bestehenden MPLS-Anbindungen weltweit abgelöst werden. Marko Bauer verdeutlicht den Einspareffekt des Umstiegs: „Unsere Kalkulation hat gezeigt, dass der Return-on-Invest bei diesem Wechsel bereits nach knapp einem Jahr erreicht ist. Dafür haben wir dann die Hardware inklusive der Lizenz für die eingesetzten Security-Services für drei Jahre."

Verschiedene UTM-Dienste

Neben der reinen Firewall-Funktionalität setzt das Unternehmen verschiedene UTM-Dienste wie Intrusion Prevention, Gateway Antivirus, Application Control, Spamblocker, Webblocker oder/und Reputation Enabled Defense ein. An ausgewählten Standorten greift darüber hinaus ein APT-Blocker als Sandbox-Technologie zum Erkennen und Blockieren von Malware und Zero-Day-Angriffen. Ein weiterer MPLS-Standort des Unternehmens befindet sich im holländischen Elst. Auch dort wird inzwischen ein UTM-Cluster eingesetzt. Aufgrund von Sicherheitsbedenken kommt dabei ein Segmentierungsansatz für das Netzwerk zum Tragen: „Bisher war in Elst nur die Verwaltung ansässig, jetzt kommt jedoch die Produktion hinzu", erläutert Roland Berndt. „Da vernetzte Fertigungsanlagen immer öfter als Ziel für Übergriffe auserkoren werden, wollten wir hier eine zusätzliche Sicherheitsschicht einziehen." Der Datenverkehr der CNC-Maschinen wird mit der Watchguard-Plattform über separate VLAN-Strukturen isoliert, zudem ist das Maschinennetz über Switches von anderen Bereichen abgetrennt. Der gesamte Netzwerkverkehr in Richtung Produktivdaten muss erst die Firewall und weitere Scan-Module passieren. An den Übergabepunkten können zudem Benutzerberechtigungen auf Basis von Active Directory kontrolliert werden. So kann nicht nur der Datenzugriff durch unautorisierte Nutzer unterbunden, sondern auch verhindert werden, dass sich von Produktionsanlagen ausgehende Gefahren im ganzen Netzwerk ausbreiten. Zudem wird durch unterteilte Netzwerkbereiche eine schnellere Identifizierung von Schwachstellen möglich. Nach Test der Netzwerk-segmentierung soll das Konzept in allen weiteren Produktionsstandorten Einzug halten und sukzessive verfeinert werden.

Zertifiziert für Atlas

Leitz konnte mit seinem IT-Security-System ein weiteres Problem lösen und die Kommunikation im Rahmen von Zollanmeldungen absichern: „Leitz liefert seine Produkte in nahezu jeden Winkel der Erde, entsprechend hoch ist der Aufwand der Zollabfertigung", sagt Berndt. Um die damit einhergehenden Prozesse zu verschlanken, sollte Atlas (Automatisiertes Tarif- und Lokales Zollabwicklungssystem) genutzt werden. Dabei handelt es sich um eine vom Informationstechnikzentrum Bund bereitgestellte Lösung zur elektronischen Abwicklung und Überwachung des grenzüberschreitenden Warenverkehrs. Die Übermittlung der Daten erfolgt via VPN-Tunnel – jedoch nur, wenn der dafür verantwortliche Hersteller entsprechend zertifiziert ist. Diese Zertfizierung erhielt der Hersteller der Security-Appliances im Juni 2017 und liefert für die VPN-Anbindung an das Atlas-Zollverfahren auch eine vollständige Dokumentation. „Natürlich lässt sich hier und da immer noch weiter optimieren, aber da arbeiten wir ja gemeinsam mit Fornax konsequent dran. Mit den Möglichkeiten, die uns Watchguard in dem Zusammenhang bietet, sehen wir uns auch langfristig auf der sicheren Seite", sagt Berndt. ■

Die Autorin Rebecca Hasert ist Redakteurin bei Press'n'Relations in Ulm.

www.watchguard.de

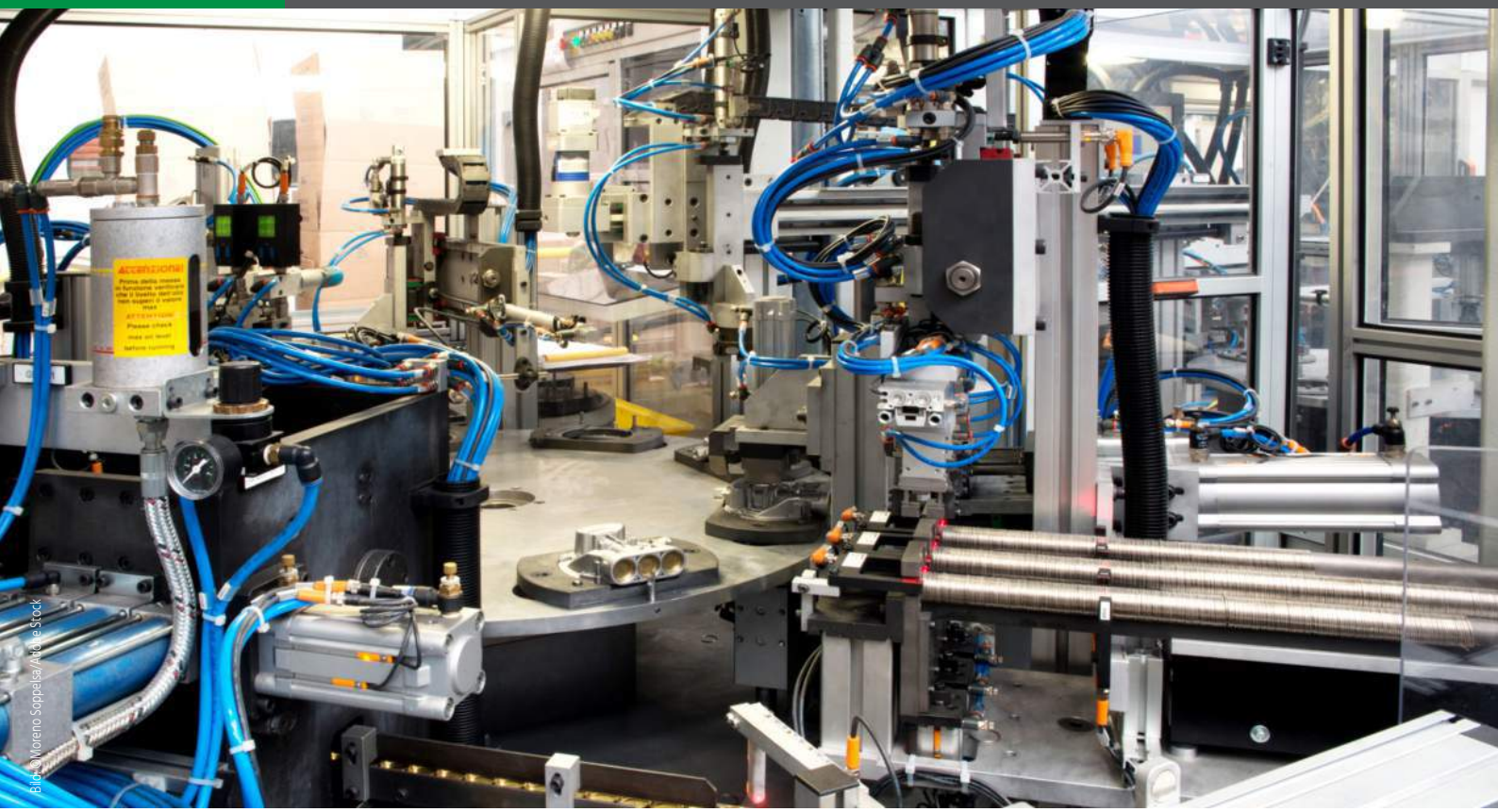


Bild: Moreno Soppelsa/Adobe Stock

Machine-2-Machine-Kommunikation

Maschinendaten in der Kapsel

Ohne Machine-to-Machine- beziehungsweise Sensor-Aktor-Kommunikation kommen Produzenten auf ihrem Weg zur Industrie 4.0 an Grenzen. Ohne IT-Sicherheit im Netzwerk aber auch. Zwar lässt sich der Transfer von Produktionsdaten auch vertikal absichern, aber eine sinnvolle Abgrenzung von Anlagen, Zellen und Linien spart unnötigen Aufwand und verringert Risiken.

Die Vernetzung der Komponenten im Fertigungsnetz sowie die Öffnung des Produktionsnetzes in Richtung Office-IT führen dazu, dass vermehrt auch Datenverkehr in die Produktion fließen kann, der dafür nicht vorgesehen ist. Andersherum kommt es vor, dass direkt von einem Steuerungs-PC im Produktionsnetz ein Zugriff auf das Internet möglich ist. Dadurch kann es zu unerwünschten Kommunikationsbeziehungen kommen, für die nur unzureichende Sicherungsmaßnahmen bestehen.

Status Quo Anlagenschutz

Um Anlagenerweiterungen zu schützen, werden häufig neuere Protokolle entwickelt. Diese können sich aber als ungeeignet erweisen, da sie auf die vorhandene Technik nicht anwendbar sind. Eine Möglichkeit, Altsysteme vor Missbrauch zu schützen ist wiederum, sie weitestgehend vom restlichen Netzwerkverkehr zu isolieren. Daraus ergeben sich jedoch Anforderungen hinsichtlich der Gewährleistung der Authentizität als auch von Integrität der Steuerungsdaten. Eine besondere Herausforderung im üblichen Mischbetrieb von Bestandsanlagen und neuer Technik stellen die neuen Anlagen dar: Auch wenn diese den aktuellen Stand der Technik aufweisen sollten, liefern Anlagenbauer oft teils veraltete oder nicht mehr vom Hersteller unterstütze Systeme mit aus und untersagen dem Betreiber zudem, diese Bestandteile der Anlage während der Garantiezeit zu verändern. Dadurch kann es passieren, dass der Altbestand besser abgesichert ist als neue Anlagen. Dies resultiert unter anderem daraus, dass versucht wird, bestehende Systeme im stabilen Betrieb abzusichern, während neuen Anlagen im fragilen Anlauf-Prozess keinerlei Änderungen zuzumuten sind.

Abschottung ist keine Lösung

Eine Schutzmöglichkeit wäre die Rückkehr zu einem geschlossenen Produktionssystem und sowohl alte als auch neue Systeme mit zusätzlichen Gateways oder Firewalls so voneinander abzuschotten, dass keine problematischen Netzwerkzugriffe möglich sind. Dies widerspricht jedoch dem Industrie-4.0-Ansatz, der einen weitreichenden Datenaustausch beschreibt – sogar über die Grenzen der Organisation hinweg. Dabei hat sich eine vollständige Kontext- und Datenflussana-

lyse für die Kommunikation innerhalb der Produktion und über deren Grenzen hinweg sowie die Erarbeitung entsprechender Maßnahmen zur sicheren Bereitstellung der Daten etabliert.

Offen oder proprietär

Beim internen Einsatz von kabellosen Technologien muss zwischen proprietären, also eigenen, und offenen Standards unterschieden werden, wobei sich dabei die Frage nach den übergeordneten Protokollen und angeschlossenen Endgeräten ergibt. Wird auf WLAN gesetzt, sollte auch eine entsprechende Absicherung (IT-Sicherheit) erfolgen. Sind andere Standards der Maschinenkommunikation oder proprietäre Technologien geplant, können diese häufig nur durch ebenso proprietäre Mechanismen abgesichert werden. Bei der Bereitstellung von Daten für Kooperationspartner wurde bisher oft auf Standards wie EDI /EDIFACT gesetzt, was aber häufig zu hohem Aufwand bei der Änderung oder Anpassung der Schnittstellen auf allen Seiten geführt hat. Bei offeneren und flexibleren Anbindungen mit mehr Sicherheitsoptionen können sogenannte APIs (Application Programming Interfaces) helfen. Diese lassen sich oft schneller anpassen und Betreiber sind in der Lage, mehrere Versionen parallel laufen zu lassen, um die Kommunikationspartner bei der Migration nicht unter Druck setzen zu müssen. Der Vorteil der Nutzung von APIs nach außen (published API) liegt also darin, die eher langsamen Entwicklungszyklen in der eigenen Infrastruktur und Produktions-IT von den sich schneller ändernden Anforderungen der Lieferanten oder Kunden abzukoppeln. Intern kann somit weiterhin mit langsameren Verfahren zur SAP-Anbindung gearbeitet werden, während man nach außen auch moderne Apps für Smartphones anbieten kann.

Authentizität durch Zertifikate

Neben der Vertraulichkeit von Informationen spielt auch die Authentizität von Sender und Empfänger eine Rolle. Je nach Leistungsfähigkeit der Kommunikationspartner (in diesem Fall ein Ausschlusskriterium für einfache Sensornetze) können Zertifikate bei der Sicherung der Authentizität helfen. Diese haben sich im privaten Bereich bereits etabliert – etwa beim Onlinebanking. Diese Art der Absicherung kann auch auf Maschinen übertragen werden. Eine entsprechende Speicherausstattung und grundlegende Verschlüsselungsfunktion der Hardware vorausgesetzt, sind Zertifikate derzeit ein sehr sicheres Verfahren zur Absicherung der Maschinenkommunikation. Eine klare Abgrenzung muss jedoch bei Betrachtung der Kommunikation auf Busebene erfolgen: Die dort angewendete Signalisierung kann nicht durch gängige Mittel der IT-Sicherheit geschützt werden, da die Übermittlung der Informationen proprietär erfolgt. Ein Nachteil von Zertifikaten ist jedoch die begrenzte Lebensdauer von etwa ein bis drei Jahren. Zudem basiert die Sicherheit des Gesamtsystems darauf, dass alle beteiligten Partner einer Dritten Partei vertrauen (in dem Fall der die Zertifikate ausgebenden Public-Key-Infrastruktur). Zudem kann im schlimmsten Fall die Kommunikation zusammenbrechen, wenn die jeweiligen Knoten den Ursprung der Zertifikate oder deren Gültigkeit nicht prüfen können. Dies kann insbesondere dann passieren, wenn die Zertifikate der jeweiligen Knoten in der Kette ablaufen oder die Lebensdauer des Vertrauensankers erreicht wird. Kommerzielle Anbieter von Zertifikaten sind daher bereits dazu übergegangen, für solche Einsatzszenarien nur Zertifikate mit erweiterter Lebensdauer von bis zu 30 Jahren einzusetzen.

Absicherung unumgänglich

Eine wirksame Absicherung der M2M-Kommunikation ist unumgänglich. Dazu gilt es, lokale Daten und lokale Kommunikation von dem zu trennen, was den Einflussbereich der Organisation verlassen darf. Als erste Schutzmaßnahme steht also die Abgrenzung der jeweiligen Anlagen, Zellen, Linien und Maschinen untereinander auf dem Plan, damit nur noch der gewünschte Datenverkehr aus der Anlage herauskommen und nur noch validierte Steuerungsinformationen in die Anlage hineingelangen. Zunächst kann dies nur auf Basis einfacher Firewalls und Netzwerkfilter erfolgen, da die zur tieferen Analyse des Verkehrs notwendigen Kenntnisse der Protokolle erst in die Sicherheitstechnik einfließen müssen. Dabei besteht Nachholbedarf, da sich die Stabilität der angeschlossenen Maschinen hinsichtlich Angriffen aus dem Netz bislang als eher unterdurchschnittlich erweist. ■

Die Autoren sind Sebastian Rohr, technischer Geschäftsführer der Accessec GmbH, und Markus Soppa, Research Consultant der Accessec GmbH.

Im Bereich der vernetzten Autos könnte es zu Konflikten zwischen Datenschutz und neuen Services wie dem automatischen Notrufsystem eCall kommen.

Bild: ©chombosan/iStockphoto.com

Dateneigentum im Internet der Dinge

Sichere Daten im digitalen Zeitalter

Die EU-Datenschutzgrundverordnung DSGVO tritt im Mai 2018 in Kraft. Ein Aspekt betrifft den Schutz personenbezogener Daten und damit auch das Thema, wem Daten eigentlich gehören. Im Kern geht es um den Schutz von Verbraucherdaten. Produzierende Unternehmen sollten sich damit ebenfalls beschäftigen, wenn sie das Internet der Dinge für sich nutzen wollen.

Jüngste Analysetechnologien wandeln Maschinen- und Nutzerdaten in wertvolle Informationsquellen. Gleichzeitig wird die Frage, wem solche Daten eigentlich gehören, zum Gegenstand komplexer Diskussionen. Wenn Konsumenten beispielsweise eine Fitness-App von Strava nutzen, um ihren Workout-Erfolg nach dem Training zu prüfen, sollten die Daten dann nur ihnen selbst zur Verfügung stehen oder hat auch der Gerätehersteller ein Nutzungsrecht? Ähnliches gilt für Produktionsumgebungen, in denen Daten rund um die Instandhaltung oder die Leistungsfähigkeit von Geräten und Maschinen entstehen. Die neuesten IoT-Technologien und Anwendungen zur Geräteüberwachung erlauben es Herstellern von Autos, Flugzeugen oder Zügen, ihre Systeme mithilfe von Sensoren zu überwachen. Solche Maßnahmen helfen den Herstellern dabei, die Ausfallzeiten zu minimieren, indem sie vorzeitig auf Wartungszyklen hinweisen, sodass ein Fahrzeug bei Bedarf aus dem Verkehr gezogen, schnell repariert und wieder eingesetzt werden kann – Stichwort Predictive Maintenance.

Wem gehören aber die Daten?

Die Reduzierung von ungeplanten Ausfall- oder Stillstandzeiten bringt Fluggesellschaften und allen anderen Transportunternehmen enorme Kostenvorteile. Die von den Sensoren erzeugten Daten können daher ein sehr kostbares Wirtschaftsgut darstellen. Beispielsweise mag eine Fluggesellschaft glauben, dass sie Anspruch auf die Daten hat, weil ihr das Flugzeug gehört. Ebenso könnte der Flugzeugteilehersteller Ansprüche auf die gespeicherten Daten erheben, weil er etwa

entsprechende Bestimmungen im Vertrag mit der Airline vereinbart hat, die dem Hersteller die Rechte auf alle im Flugzeug gespeicherten Daten einräumen. Ein solcher Fall kann besonders kompliziert werden, wenn Teile unterschiedlicher Hersteller in einem Milliardenprojekt verbaut und später von Dienstleistern gewartet werden. An diesem Punkt wird das Eigentum der Daten nämlich erfolgsentscheidend. In diesem Szenario kann es dazu kommen, dass derjenige, der den Anspruch auf die Daten erhebt (beispielsweise die Airline), die gespeicherten Informationen für die eigene Wartungsfirma nutzt. Das kann zu Interessenkonflikten führen, wenn die Fluggesellschaft ihren Wartungsdienst anderen Wettbewerbern anbietet und als 'Center of Excellence' agiert. Je mehr Parteien also in ein Projekt involviert sind, desto mehr könnten theoretisch auch Anspruch auf gespeicherte IoT-Daten erheben.

Da immer mehr Endgeräte internetfähig sind, sollten Kunden die allgemeinen Geschäftsbedingungen von Geräte- und Maschinenherstellern auch wirklich verstehen, um die eigenen Daten zu schützen.

Notrufsystem mit Fallstrick

Vernetzte Autos sind ein weiterer Bereich, wo es zu Konflikten kommen kann: So fordert das geplante automatische Notrufsystem der EU eCall, dass alle Kraftfahrzeuge, die ab April 2018 gebaut werden, mit einer eCall-Technologie ausgestattet sind. Im Falle eines schweren Unfalls wählt die eCall-Technik automatisch Europas übergreifende Notrufnummer 112. Was aber geschieht, wenn ein Auto gleichzeitig auch den jeweiligen Standort des Fahrers kontinuierlich an den Autohändler übermittelt? Was wäre, wenn die Daten auch an Dritte, beispielsweise Versicherungsgesellschaften weitergeleitet würden? Und infolgedessen die Versicherungsprämie des Fahrers hochgestuft würde, weil etwa die Daten darauf hinweisen, dass er sich besonders risikofreudig verhält? Bei diesem Beispiel bekommt das Recht auf personenbezogene Daten und die Möglichkeit, die Übermittlung der Daten abzustellen, schon eine ganz andere Bedeutung.

Datennutzung besser verstehen

Ein Audit der personenbezogenen Daten, die in einer Organisation verfügbar sind, hilft in diesem Fall zu ermitteln, welche Daten gespeichert sind, woher sie stammen und an wen sie weitergegeben werden. Im Rahmen von Initiativen zu Connected Cars bitten OEMs ihre Kunden, eine Connected Car Privacy Policy als Teil ihrer Kontoeinrichtung zu unterzeichnen. Dieses Richtlinien müssen daraufhin überprüft werden, ob sie mit den Anforderungen der DSGVO in Einklang stehen, wobei besonderes Augenmerk auf die Rechte des Einzelnen gelegt werden muss. Bieten Richtlinien Einzelpersonen die Möglichkeit, die über sie gespeicherten Daten abzufragen? Können sie ihre Daten korrigieren oder löschen? Die Löschung von Daten ist ein besonders heikles Thema. Damit Hersteller Services auf Basis von Connected Car-Technologien anbieten können, müssen sie häufig Daten über mehrere Plattformen hinweg übertragen und speichern sowie Daten mit Zulieferern austauschen. Darüber hinaus müssen solche Löschanfragen mit den Anforderungen an die Datenarchivierung abgeglichen werden, um die Hersteller vor Rechtsstreitigkeiten zu schützen. Ein weiterer wichtiger Gesichtspunkt ist, ob die Hersteller ihre Kunden im Rahmen der aktuellen Prozesse um ihre Einwilligung bitten, direkt auf der Grundlage von Fahrzeugdiagnoseinformationen kontaktiert zu werden, und ob sie damit einverstanden sind, dass diese Daten mit dem Händlernetz geteilt und aktiv kommuniziert werden.

Das Kleingedruckte lesen

Was können also Anwender und Unternehmen tun, um sich selbst zu schützen und sich in einer immer komplexer werdenden Welt der Eigentumsrechte von Daten zurechtzufinden? In Zeiten, da die meisten Endgeräte internetfähig sind, wird es immer wichtiger, die allgemeinen Geschäftsbedingungen von Geräte- und Maschinenherstellern genauer zu lesen und auch wirklich zu verstehen. Das berühmte Häkchen im Kästchen wird künftig stärkere Auswirkungen für beide Seiten und für die jeweiligen Daten haben. Die europäische Datenschutzgrundverordnung DSGVO ist sicherlich ein Schritt in die richtige Richtung, um den Datenschutz der Kunden zu verbessern. Jeder sollte sich künftig selbst fragen, wenn er ein vernetztes Auto, Fitbit oder Smartphone kauft, ob er die allgemeinen Geschäftsbedingungen genau gelesen hat und welche Informationen er tatsächlich weitergeben möchte. Gleiches gilt für die produzierende Industrie, die mit ihren Systemlieferanten das Thema Dateneigentum diskutieren sollten, um zukünftigen Konflikten aus dem Weg zu gehen. ■

Der Autor Otto Neuer ist Vice President Sales EMEA Central bei Talend.

de.talend.com

Mehr als Zeit erfassen und Zutritt kontrollieren

Individuell, sicher und vernetzt

Bild: Datafox GmbH

Manche erinneren sich noch an die alten Stempeluhren und den Pförtner am Schlagbaum. Vereinzelt gibt es das noch. Doch meistens arbeiten Zeiterfassung und Zutrittskontrolle heute digital und vernetzt. Dass diese Systeme mehr Funktionen als früher mitbringen, liegt auf der Hand. Beschäftigen sich Unternehmen mit der Einführung einer Zutrittskontrolle, sollten sie daher genau wissen, was sie brauchen und an wen sie sich wenden.

In der Zeiterfassung hat insbesondere die Einführung des Mindestlohns im Jahr 2015 bei vielen Firmen zum Umdenken geführt. So werden heute auch in kleinen und kleinsten Unternehmen Arbeitszeiten elektronisch erfasst, um zum Beispiel den Dokumentationspflichten gerecht zu werden. Aber auch die einfachen Erfassungsprozesse, die Auswertbarkeit und natürlich die Übergabe der Daten an die Systeme zur Lohnabrechnung, Dienstplanung und das ERP-System sprechen für digitale Erfassungslösungen.

Erfasst wird am Terminal

Trotz immer mehr mobiler Lösungen, die Smartphones und Tablets einbeziehen, bleiben stationäre Zeiterfassungsterminals bei vielen Unternehmen die erste Wahl. Dies liegt vor allem daran, dass sich Arbeitgeber von den kurzlebigen Technologiezyklen der Smartphone-Hersteller unabhängig machen wollen und nicht erwarten können, dass jeder Mitarbeiter ein passendes Endgerät besitzt. Stationäre Zeiterfassungsterminals haben in der Regel eine Lebensdauer von mehr als zehn Jahren und sind leicht bedienbar. Gerade in anspruchsvollen Bereichen wie der Produktion, im Außeneinsatz oder an sehr warmen beziehungsweise kalten Orten sind Zeiterfassungsterminals meist die beste Wahl. Der Trend bei der Zeiterfassung, Zutrittskontrolle und anderen Anwendungen geht hierbei seit vielen Jahren zu RFID-Verfahren wie Mifare, bei denen ein meist passiver Transponder in Form eines Schlüsselanhängers, einer Karte oder eines Aufklebers in das magnetische Feld des Lesers gebracht wird. Dort können die eindeutige Seriennummer zur Identifikation oder programmierte Segmente und weitere gespeicherte Daten zum Beispiel über Zutrittsberechtigungen, Kantinenguthaben, Fingerprint-Templates et cetera übertragen werden.

Fingerabdruck recht sicher

Die Identifikation oder Verifikation der Mitarbeiter und weiterer berechtigter Personen findet immer öfter über biometrische Merkmale statt. Insbesondere Fingerabdrücke werden sehr oft verwendet, da die Erkennung recht sicher ist und die Abdrücke einfach zu erfassen sind. Die Nutzung von Gesichtserkennung, Iris-Scan sowie Handvenen-Erkennung spielen hingegen in den meisten Anwendungen eine Nebenrolle. Einerseits ist hier die Nutzerakzeptanz, andererseits der Kostenfaktor ein Ausschlusskriterium. Da die Nutzung biometrischer Daten für die Zeiterfassung und Zutrittskontrolle immer Zustimmungspflichtig ist, kann schon ein einzelner Mitarbeiter dem Arbeitgeber einen Strich durch die Rechnung machen. Methoden wie Barcode oder PIN-Eingabe sind ebenfalls noch weit verbreitet, auf Grund des sehr niedrigen Sicherheitsniveaus aber oft nicht empfehlenswert. So ist ein Barcode etwa für die Zeiterfassung mit Smartphones schnell fotografiert und an einen Kollegen geschickt, der dann Zeiten stempeln könnte. Immer mehr Anwender erwarten von den Systemen eine hohe Durchgängigkeit – also die Verwendung gleicher Identifikationsmedien von der Zeiterfas-

sung, Zutrittskontrolle über die Kantine, den Drucker bis in die Fertigung für die Betriebsdatenerfassung (BDE) und Werkzeugausgabe.

Alles aus einer Hand

Anbieter mit breitem Produktportfolio und vielen Optionen, haben in Verbindung mit den passenden Kommunikationsarten oft einen Vorteil am Markt. So wollen Unternehmen häufig die Zeiterfassung und Zutrittskontrolle, die Betriebs- und Maschinendatenerfassung, Kantinenlösungen sowie Workflow-Angebote aus einer Hand beziehen. Dies stellt einerseits die Softwareanbieter vor große Herausforderungen – andererseits aber auch die Hardwareanbieter, die ein möglichst breites Produktportfolio bieten müssen. Dabei sollen Geräte per LAN, WLAN oder Mobilfunk kommunizieren können. Auch die Datenübergabe und Anbindung an alle Arten von Software, Datenbanken und natürlich in die Cloud sind technisch machbar. Erste Hardwarehersteller bieten die Einbindung Ihrer Geräte über das abgesicherte Protokoll HTTPS. Dieses weltweit einheitliche und verbreitete Verfahren zur Datenübergabe erfordert kaum Programmieraufwand und funktioniert quasi in Echtzeit - sowohl im internen Netzwerk, als auch im Internet und Mobilfunknetz. Der Datenaustausch für Zeiterfassung, Saldenabfrage und Zutrittskontrolle ist damit online und abgesichert über das Internet möglich. Gerade der Betrieb von Terminals mit Mobilfunk und die Anbindung per HTTPS ermöglicht es, Geräte ohne großen Aufwand an jedem Ort in Betrieb nehmen zu können. Die M2M-Datenverträge der großen Netzbetreiber sind hierbei verhältnismäßig günstig.

Individuelle Lösungen gefragt

Auch auf dem Markt für Zeit und Zutritt ist mehr Individualisierung erkennbar. Ziel ist die Benutzerfreundlichkeit und Einbindung des Softwareanbieters als auch der Endkunden ins Corporate Design. Einzelne Hardwarehersteller bieten hier weitreichende Möglichkeiten für Zutrittsleser sowie Zeiterfassungs- und BDE-Terminals. Der Markt der Anbieter für die Zeiterfassung und Zutrittskontrolle umfasst allein in Deutschland mehr als 1000 Firmen. Der größte Teil sind Software- und Lösungsanbieter. Die Zahl der Hardwarehersteller ist eher überschaubar und wird vor allem von deutschen und europäischen Herstellern dominiert. Natürlich werden gerade am unteren Ende des Preisniveaus auch Geräte aus Fernost angeboten. Fehlender oder schlechter Support, oft wechselnde technische Spezifikationen und schwankende Qualität sorgen aber für einen stagnierenden oder gar fallenden Marktanteil. Neben den etablierten Anbietern komplexer Human Resources-Lösungen hat sich in den letzten Jahren eine Startup-Landschaft gebildet, die sich mit den Themen Dienstplanung, mobiler Zeiterfassung per App und Cloud-Lösungen beschäftigt. Es ist aber zu bemerken, dass auch äußerst innovative Anbieter nach kurzer Zeit oft auf stationäre Terminals setzen, um damit den Anforderungen des Marktes gerecht zu werden. Durch Venture-Capital und viele frische Ideen entstehen so schlagkräftige Unternehmen, die Modelle wie ‘Software as a Service’ und ‘pay as you use’ auf den Markt der Zeiterfasssung und Zutrittskontrolle zuschneiden.

Arbeitsteiliger Markt

Der Bereich der Zutrittskontrolle gliedert sich in Anbieter für Sicherheitstechnik – also Drehkreuze, Schranken, Kameras et cetera. Hinzu kommen Anbieter von elektronischen Zutrittscontrollern und Lesern, sowie Schließzylindern und Beschlägen. Viele Softwareanbieter aus dem Bereich Zeiterfassung und ERP bieten integrierte Zutrittskontroll-Module. Es gibt außerdem Spezialisten, die ausschließlich Zutritts- und Sicherheitslösungen verkaufen. Die überwältigende Mehrheit der Anwender arbeitet in diesem Bereich mit RFID-Technik zur Identifikation. Der Trend geht dabei klar zu Online-Systemen, auf Basis der bereits erwähnten Mifare-Technologie, bei denen Berechtigungen vergeben werden können und die flexibel einsetzbar sind. Eine einfache Installation und Umsetzung ist wichtig, damit die späteren Betreiber die Systeme durch lokale Ressourcen oder Elektrofachbetriebe einrichten lassen können. Für viele Unternehmen sind dezentrale Systeme interessanter, bei denen kostengünstige Controller nicht mehr im Server-Raum, sondern in der Nähe der Tür platziert und im Netzwerk integriert werden. In anderen Umgebungen können leistungsstarke Zentralen Vorteile ausspielen, wenn viele Türen abzusichern und dazu Alarmanlagen einzubinden sind. Auf jeden Fall sollten die Betreiber in spe ihren Anbieter sorgfältig auswählen, damit dieser flexibel genug auf die spezifische Aufgabe reagieren kann. ■

Der Autor Stefan Tanneberger
ist Mitarbeiter im Vertrieb bei Datafox GmbH.

Zutritt zu 18 Standorten zentral gesteuert

Bilder: PCS Systemtechnik GmbH

Während eine Schließanlage nur schließt und öffnet, kann eine intelligente, digitale Zutrittskontrolle als vielseitiges Sicherheitsinstrument dienen. Das Beispiel Zollner Elektronik aus dem bayerischen Zandt zeigt, wie eine Zutrittskontrolllösung zum Koordinatensystem eines internationalen Unternehmens wurde.

Das 50 Jahre alte Familienunternehmen Zollner Elektronik wächst seit Jahren kontinuierlich und hat sich als Zulieferer der Automotivebranche einen Namen gemacht. Aktuell betreibt Zollner 18 Standorte über die ganze Welt verteilt. Das Geschäftsmodell beruht auf nach Kundenanforderungen entwickelte und gefertigte Mechatronikteile, vom Einzelteil bis zur Serienfertigung. Kernkompetenz sind elektronische Bauteile. Werke in Rumänien, China, Costa Rica oder Tunesien produzieren für den jeweiligen Zielmarkt in regionaler Nähe.

Steuerung der Zutrittskontrolle

Die Hightech-Produkte von Zollner sind sowohl bezüglich der Fertigungsprozesse als auch des Technologie-Knowhows äußerst sensibel. Daher befasst sich das Unternehmen stets auch mit der Sicherheit im eigenen Haus und schrieb in diesem Zusammenhang im Jahr 2015 das Zutrittskontrollsystem neu aus. Als Ergebnis der Evaluation entstand ein langfristig angelegtes Konzept mit Hard- und Software für Zeiterfassung und Zutrittskontrolle von PCS. Die bislang noch autonom geführten Zutrittskontrollsysteme werden nach und nach angebunden und vom Server aus dem Hauptsitz in Zandt gesteuert. Über den Zeitraum von mehreren Jahren wird die Zutrittskontrolle an allen Standorten vereinheitlicht, Dexicon angebunden und ausgebaut. Notwendig sind dafür die Umstellung auf SAP als führendes System zur Nutzung der hier verwalteten Personal-Stammdaten sowie die Anpassung der Zutrittskontroll-Software Dexicon an die jeweiligen Standortbedingungen. Die Vorteile für diese Zentralisierung: Transparenz über alle Zutritte und Alarmereignisse, schlanke Administration, einheitliche Zutrittsgruppen und damit die gebündelte Sicherheitskompetenz für einen weltweiten Zutritt im eigenen Haus.

Langjähriger Partner

Den Zuschlag erhielt PCS in Verbindung mit der Zutrittskontrollsoftware Dexicon Enterprise und der Intus Hardware für Zeiterfassung und Zutritt. Die Realisierung des Projektes erfolgt nach intensiven Vorbereitungen des gesamten Projektteams auf Basis des gemeinsam erarbeiteten Konzepts, das auf Standardkomponenten setzt. Einige Beispiele aus dem Projekt zeigen, mit welchen Management-Aufgaben das Zutrittskontrollsystem zur Unternehmenssicherheit bei Zollner beiträgt.

Vorgeschaltete ESD-Prüfungen

Zollner befasste sich bei der Analyse der bisherigen Zutrittskontrolle auch mit den

altäglichen Abläufen. Kritisch war die vor elektrostatischer Entladung (ESD) geschützte Fertigung von elektronischen Baugruppen. Wenn Personen diesen Fertigungsbereich betreten, muss sichergestellt sein, dass sie nicht elektrostatisch aufgeladen sind, sonst könnten Bauteile schon im Produktionsprozess durch Aufladung geschädigt werden. Schutzkleidung, Schuhe oder Ableitungsarmbänder verhindern dies. Zollner hat die ESD-Überprüfung vor die Zutrittskontrolle geschaltet. Erst nach erfolgter ESD-Prüfung, kann die Zutrittskontrolle bedient werden. Dann aktiviert die Zutrittskontrolle den Zutrittsleser und der Zugang zur Vereinzelungsschleuse kann genutzt werden.

Sichere Handvenenerkennung

Besonders sensible Bereiche bei Zollner sind das zentrale Rechenzentrum inklusive Backup-Rechenzentrum sowie die Prototypen-Entwicklung. Für den Schutz der beiden Bereiche ist dem Unternehmen eine Zutrittskontrolle nur auf RFID-Basis zu wenig, schließlich können Mitarbeiterausweise leicht in unbefugte Hände gelangen. Für diese Anforderung stellte PCS dem Unternehmen die Handvenenerkennung Intus PS vor. Die biometrische Zutrittskontrolle kann die Identität eines Mitarbeiters zweifelsfrei feststellen und gilt als fälschungssicher. Das biometrische System erkennt Menschen, indem es mit Infrarotstrahlen die einmaligen Venenmuster im Inneren der Hand liest. Das Handvenenmuster wird dabei in ein Template umgewandelt und kann so auf einem Mitarbeiterausweis gespeichert werden. Die Zutrittskontrolle zum Rechenzentrum erfolgt bei Zollner mit zwei Faktoren: Nur der berechtigte Personenkreis wird am Handvenenscanner eingelernt und erhält eine Mitarbeiterkarte mit seinen biometrischen Merkmalen – den Handvenentemplates. Nach dem Einlernen kann der Mitarbeiter den Ausweis vor den RFID-Teil des Systems halten und sich anschließend mit der Hand beziehungsweise den Handvenen verifizieren. Die Handvenenerkennung ist zudem mit der Einbruchmeldeanlage (EMA) verknüpft, steuert diese, sowie berücksichtigt und signalisiert vor der Freigabe einer Zutrittsanfrage den Status der EMA.

Rechte nach Benutzergruppe

Eine ausgereifte Zutrittskontrolle beugt nicht nur dem Eindringen von Unbefugten vor. Sie wirkt präventiv, wenn festgestellt werden soll, welche Mitarbeiter sich auf dem Gelände befinden. Bei Unternehmensbereichen wie Warehouse und Lager dokumentieren inzwischen oft Ein- und Austrittsleser, welche Mitarbeiter wann und wie lange anwesend waren und ob alle Mitarbeiter am Feierabend das Werk verlassen haben. Verschiedene Zutrittsprofile für unterschiedliche Mitarbeitergruppen legen zudem schon im Vorfeld die Zutrittsrechte fest. So haben Gruppen auf ihre Arbeitsbereiche zugeschnittene Zutrittsrechte, das Sicherheitsteam sehr weitgehende Zutrittsrechte und Besucher sehr restriktive Zutrittsrechte.

Mit Schreib-und Lesefunktion

Die Handvenenerkennungssysteme von PCS nutzen die neue Generation von RFID-Ausweisen mit dem Leseverfahren Mifare Desfire EV1. Mit den Scheckkartengroßen Ausweisen bei Zollner lassen sich bis zu 32 unterschiedliche Applikationen ausführen. Mit Hilfe der neuen Ausweistechnologie wird im Gegensatz zum bisherigen System nicht nur gelesen, sondern kann auch beschrieben werden, zum Beispiel Zutrittsrechte oder Geldbeträge für die Kantinennutzung.

Universell lesbare Piktogramme

Zollner nutzt neben der Zutrittskontrolle auch die Zeiterfassung von PCS. Das Terminal Intus 5600 mit Farbdisplay und Touchoberfläche wurde mit Zollner-Logo versehen und für die internationalen Standorte werden landesspezifische Texte eingeblendet. Da weltweit alle Mitarbeiter auf einem Intus-Terminal buchen sollen, entschied man sich für eine selbsterklärende Oberfläche auf der Basis von international verständlichen Piktogrammen. Die Zutrittskontrolle und Zeiterfassung wird bei Zollner von 10.000 Mitarbeitern an 18 Standorten weltweit genutzt. In Zusammenarbeit mit dem PCS-Projektteam wurde das System so ausgelegt, dass der gewünschte Unternehmensschutz für alle Standorte realisiert wurde. Auch für Erweiterungen ist die Zutrittskontrolle offen. Weitere Module wie Besuchermanagement oder Zufahrtskontrolle prüft Zollner gerade. ■

Die Autorin Susanne Plank ist
in der Marketing Communication bei
PCS Systemtechnik.

www.pcs.de

Handeln zwischen Spectre und Watering-Hole

Sicher auf die Plattform

Bild: © Adrian_Ilie825/Fotolia.com

Die Diskussionen rund um das Thema Plattformökonomie beziehen sich zumeist auf die Geschäftsmodelle: Doch mittlerweile gibt es vermehrt Stimmen, die eine Betrachtung aus technologischer Sicht als bedeutender erachten. Auch bei der Beurteilung von Chancen und Risiken herrscht keine Einigkeit – während einige Experten in der Plattformökonomie ein probates Mittel im globalen Wettbewerb sehen, stehen bei anderen bislang ungelöste Probleme im Vordergrund.

Bezüglich des digitalen Durchdringungsgrades und der daraus resultierenden Effizienzsteigerung gibt es momentan bei deutschen Unternehmen kein einheitliches Bild. Die eher zögerliche Haltung liegt unter anderem daran, dass sich – basierend auf dem bestehenden Geschäftsmodell – noch kein strategischer Ansatz für ein neues, disruptives entwickeln ließ. Zudem ergeben sich aus den bisherigen Aktivitäten in Richtung digitale Transformation, gemäß den Ergebnissen einer aktuellen Lünendonk-Studie, momentan nur wenig Wettbewerbsvorteile. Gleichwohl werden aber weitere Schritte unternommen, digitale Plattformen im industriellen Umfeld zu etablieren. Eine erklärbare Entwicklung, denn zum einen ist eine gewisse Dringlichkeit geboten, weil sich noch keine Vormachtstellung internationaler Unternehmen herausgebildet hat. Zum anderen sind Grundprinzip und Erfolgsrezept bekannter Unternehmen wie

Amazon oder Airbnb relativ gut reproduzierbar – mehrseitige Plattformen erleichtern im erheblichen Maße Interaktion und Transaktion zwischen unterschiedlichen Parteien.

Erfolg durch Sicherheit

Doch über den Erfolg der industriellen Plattformen wird auch ihre Sicherheit entscheiden. Nicht zuletzt unter dem Aspekt, dass „Wirtschaftsspionage seit jeher einer der Schwerpunkte der Ausspähungsaktivitäten fremder Nachrichtendienste ist“, wie Michael George, Leiter des Cyber-Allianz-Zentrums am Bayerischen Landesamt für Verfassungsschutz, erklärt.

Zwei Betrachtungsweisen

Die grundsätzliche Betrachtung von Plattformen erfasst zwei Dimensionen: die wirtschaftliche sowie die technologische. Gemäß letzterer basiert die Plattformökonomie unter anderem im ersten Schritt auf dem Zusammenwachsen von Informationstechnologie (IT) mit der Operational-Technologie (OT) auf dem Shop Floor. Denn dies ermöglicht die Vernetzung sowohl intern als auch unternehmensübergreifend. Im Weiteren ergeben sich dann, aus der vertikalen und horizontalen Integration auf der einen Seite, in Verbindung mit Plattformtechnologien wie Infrastructure-as-a-Service (IaaS) auf der anderen Seite die Voraussetzungen für neue Geschäftsmodelle, da Interaktionen sowie Transaktionen mit vielen unterschiedlichen Marktteilnehmern möglich wird. Darin liegen aber auch Risiken: „Angriffe sind umso erfolgreicher, je zielgerichteter sie ausgeübt werden können“, erklärt George. Aus diesem Grund optimieren Angreifer ihre Methoden ständig.

Das Wasserloch infizieren

So beobachtet der Experte derzeit vermehrt sogenannte Watering-Hole-Attacken. Diese basieren auf der Annahme, dass es bestimmte Portale, Plattformen oder Systeme gibt, die viele Anwender mit hoher Wahrscheinlichkeit oft aufsuchen müssen (ähnlich einem Wasserloch im Tierreich). Die Anwender werden dieser Logik folgend nicht direkt angegriffen, sondern das ‘Wasserloch’ wird infiziert. In der Praxis wurden derartige Angriffe etwa auf Unternehmen aus dem Energiesektor verübt – unter anderem indem die Anbieter-Webseiten manipuliert wurden, um Rechner von Besuchern mit Schadsoftware zu infizieren.

Aufwand lohnt sich

Zudem werden permanent gravierende Schwachstellen publik gemacht, wie aktuell die Sicherheitslücken Spectre und Meltdown. Auch wenn sich nach Ansicht von Professor Lutz Becker, Leiter der Business School und Studiendekan Sustainable Marketing & Leadership an der Hochschule Fresenius, ein Angriff über Spectre keinesfalls leicht realisieren lässt, so geht er doch davon aus, dass diese Lücke ausgenutzt wird, da sich ein erhöhter Aufwand immer lohne, wenn mit einer einzigen Attacke viel erreicht werden kann. Zusätzlich gefährdet seien Unternehmen oft auch durch den Einsatz veralteter Hard- und Software. „Insgesamt gesehen stellt also Digitalisierung ohne IT-Sicherheit im Fokus klar erkennbar ein unkalkulierbares Risiko für Verbraucher und Unternehmen dar“, so Bernd Fuhlert Geschäftsführer der @-yet GmbH

Umdenken gefordert

Im Zuge von Industrie 4.0 nutzt es nach Ansicht von Michael George nur wenig, alle internen Schnittstellen wie USB-Ports und DVD-Laufwerke abzusichern, während zwangsläufig durchlässige Übergänge zum Internet bestehen. Aber da auch die herkömmliche Perimeter-Sicherheit, mit denen die Übergänge zwischen Unternehmensnetzwerk und Internet geschützt werden sollen, nicht mehr ausreichen, müssen Unternehmen generell umdenken. Nach Meinung von Fuhlert und George, sollte die Grundlage der Abwehrstrategie sein, dass ein Angreifer es schafft, bis ins interne Unternehmensnetzwerk vorzudringen. Gegenmaßnahmen müssten somit darauf basieren, den Angreifer möglichst zeitnah zu identifizieren. Zudem sind nach wie vor das Aufdecken und Absichern von Schwachstellen von Bedeutung.

Austausch zur Abwehr

Ein weiterer wesentlicher Ansatz – gerade beim Thema Plattformökonomie – ist laut George der Austausch von Angriffsmethoden und Erfahrungswerten zwischen den Unternehmen über eine neutrale Plattform. Dies sei sinnvoll, da somit schnellstmöglich und effizient nach Lösungsmöglichkeiten zur Ab- und Gegenwehr gesucht werden könne.

Fazit

Allein aufgrund der steigenden Komplexität sowie im Sinne der Widerstandskraft, oder Resilienz, müssen Maßnahmen und Methoden zum Schutz gegen Angriffe neu überdacht werden. Damit einhergehen muss unter anderem das Clustern in Sicherheitsbereiche, was ein ganzheitliches Risikomanagement erfordert. Für den Entwurf der weiteren Strategie zur Absicherung bedürfe es dann, das wertvolle unternehmensinterne Knowhow zu identifizieren und im nächsten Schritt zu definieren, wie sich dieses mit entsprechenden Lösungen schützen lässt, sagt Fuhlert. Dafür sollten die bekannten Maßnahmen wie Patch-Management oder Segmentierung der Netzwerkbereiche zum Einsatz kommen. Dies biete die Grundlage für ein gutes Schutzniveau. Entscheidend sei ferner, dass „die Politik für die Plattformökonomie einen Ordnungsrahmen setzen muss, damit Sicherheit endlich den richtigen Stellenwert bekommt und nicht blind digitalisiert wird“, erklärt Fuhlert. Zudem sollte darüber auch ermöglicht werden, global faire Spielregeln für alle – kleine nationale ebenso wie multinationale – Unternehmen zu gewährleisten, um eine Benachteiligung aufgrund individueller Gesetzgebungen auszuschließen. ■

Die Autorin Ulla Coester ist wissenschaftliche Mitarbeiterin am Institut für angewandte digitale Visualisierung e.V an der Hochschule Fresenius, Köln.

www.xethix.com

IMPRESSUM

VERLAG/POSTANSCHRIFT:
Technik-Dokumentations-Verlag
TeDo Verlag GmbH®
Postfach 2140
35009 Marburg
Tel.: +49 6421 3086-0
Fax: +49 6421 3086-380
E-Mail: info@it-production.com
Internet: www.it-production.com

LIEFERANSCHRIFT:
TeDo Verlag GmbH
Zu den Sandbeeten 2
35043 Marburg

VERLEGER & HERAUSGEBER:
Dipl.-Stat. B. Al-Scheikly (V.i.S.d.P.)

REDAKTION:
Patrick Prather (Redaktionsleiter, ppr)
Marco Steber (Redakteur, mst)

REDAKTIONSASSISTENZ:
Bastian Fitz, Tamara Gerlach, Pascal Jenke, Christina Jilg, Melanie Novak, Sarah-Lena Schmitt, Florian Streitenberger, Natalie Weigel, Sabrina Werking

MARKETING/ANZEIGEN:
Christoph Kirschenmann (Leitung)
Monika Zimmer (Assistenz)
Moritz Ernst (Mediaberatung)
Tel.: +49 6421 3086-0
Es gilt die Preisliste Nr. I/2019

GRAFIK & SATZ:
Julia-Marie Dietrich, Tobias Götze, Fabienne Heßler, Melissa Hoffmann, Kathrin Hoß, Ronja Kaledat, Patrick Kraicker, Timo Lange, Ann-Christin Lölkes, Nadin Rühl

BANKVERBINDUNG:
Sparkasse Marburg/Biedenkopf
BLZ: 53350000 Konto: 1037305320
IBAN: DE 83 5335 0000 1037 3053 20
SWIFT-BIC: HELADEF1MAR

GESCHÄFTSZEITEN:

Mo. - Do.	8.00 bis 18.00 Uhr
Fr.	8.00 bis 16.00 Uhr

ISSN **1439-7722**
Vertriebskennzeichen **52130**