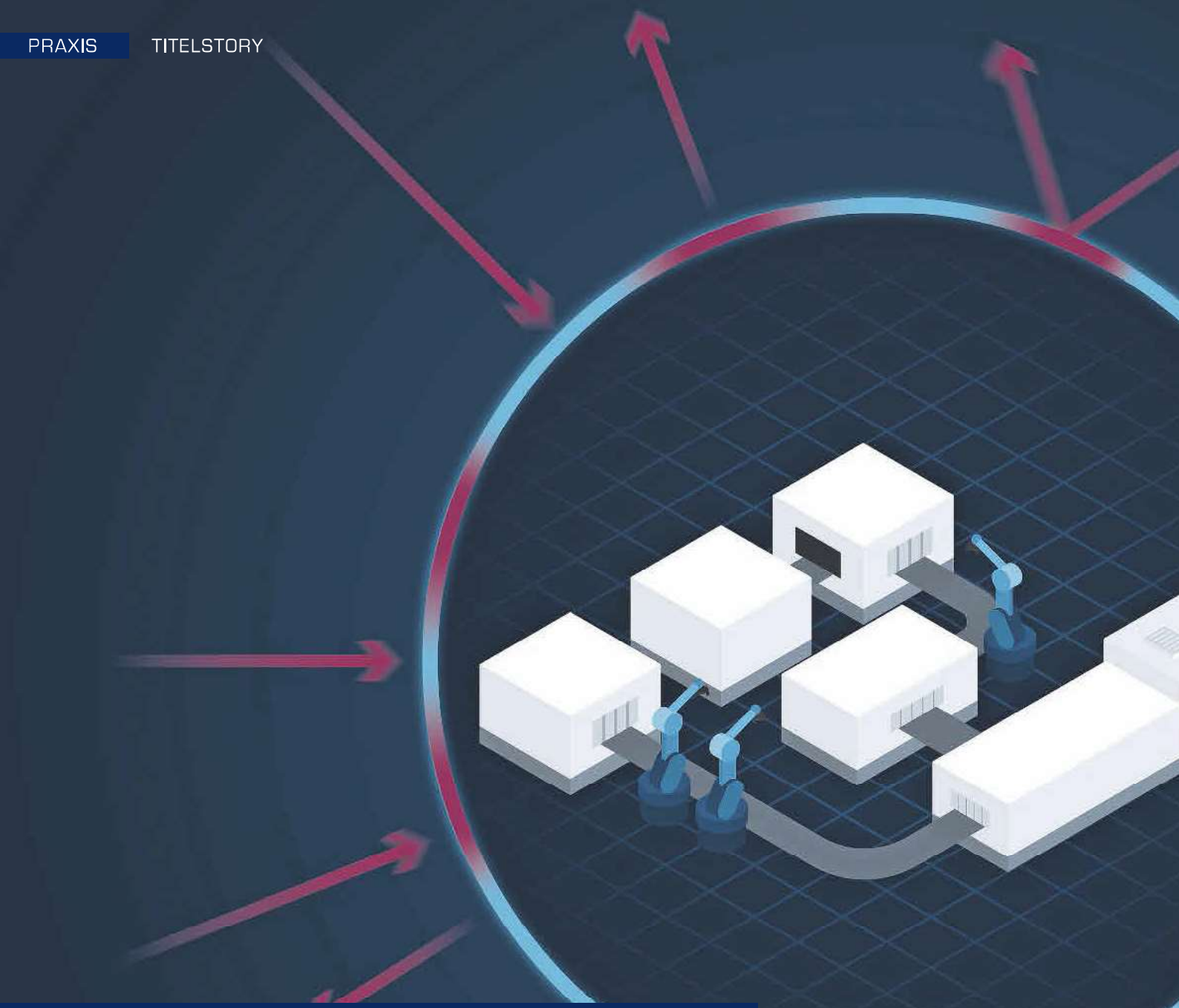
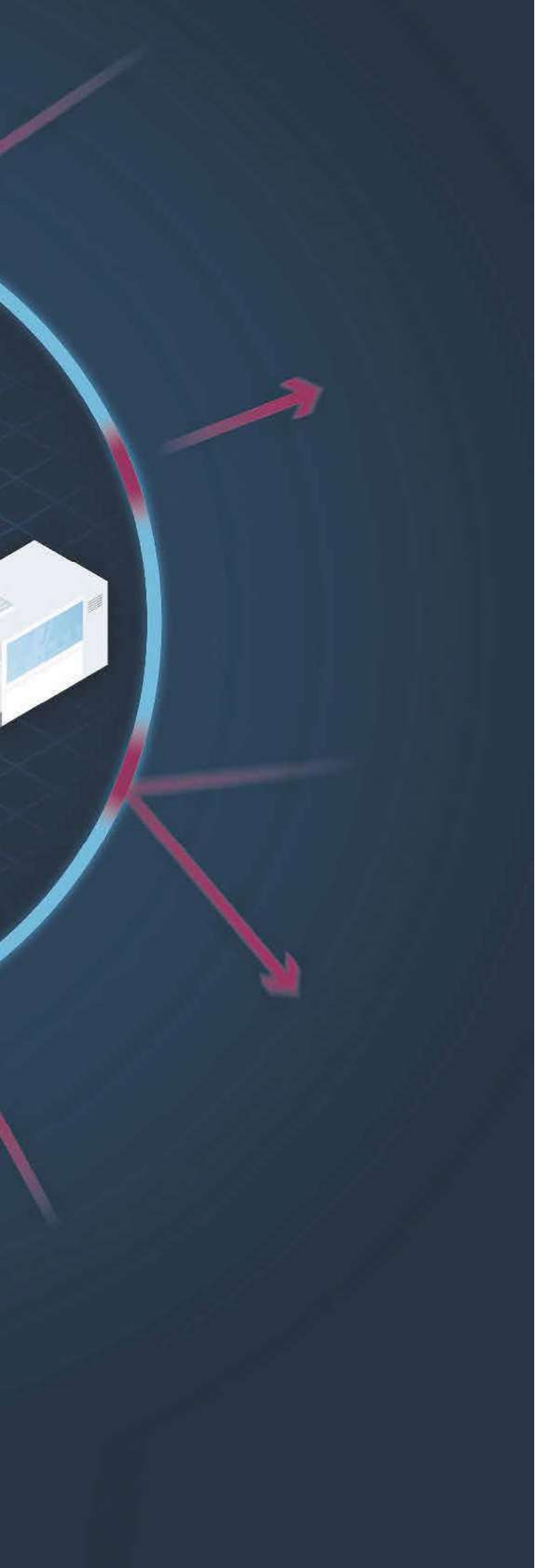


Cybersecurity: Mehrschichtig per Defense-in-Depth-Prinzip verteidigen

Industrieanlagen im Fadenkreuz der Hacker

Cybersecurity ist und bleibt für Industrie- und Produktionsanlagen eine Herausforderung – aber eine lösbare. Um den zunehmenden Bedrohungen gerecht zu werden und die Vorzüge der Digitalisierung mit steigender Vernetzung unbeschadet nutzen zu können, ist allerdings ein Umdenken und das Aufrüsten der Automatisierungstechnik (Operational Technology – OT) mit innovativen Schutzkonzepten und Security-Maßnahmen erforderlich. Nie war es für cyberkriminelle Angreifer leichter, sich Zugang zu Unternehmens- und Produktionsnetzwerken zu verschaffen und an wertvolle Daten zu gelangen. Trotzdem wird in der Industrie die Gefahr von Cyberangriffen zum Teil nach wie vor massiv unterschätzt.

Franz Köbinger, Marketing Manager Industrial Security,
Division Digital Industries, Factory Automation, Siemens AG



Bezüglich des Themas Cybersecurity war mindestens jedes zweite Unternehmen in Deutschland innerhalb von 2 Jahren von Datendiebstahl, Industriespionage oder Sabotage betroffen, wie Studien etwa des Verbandes der Informations- und Telekommunikationsbranche Bitcom bereits 2017 zeigten. Vermutlich liegt die Dunkelziffer sogar deutlich höher, da nicht jeder Angriff als solcher erkannt wird. Die Schäden liegen jährlich jedenfalls im hohen zweistelligen Milliardenbereich.

Doch trotz dieser beeindruckenden und erschreckenden Zahlen erlangen zumeist nur Angriffe auf kritische Infrastrukturen sowie auf staatliche Einrichtungen größere öffentliche Aufmerksamkeit oder Schadsoftware-Infektionen mit weltweiter Verbreitung wie etwa die Erpresser-Software „WannaCry", die 2017 Furore machte. Sie verschlüsselt Daten, die man nur gegen Bezahlung mit Bitcoins wieder entschlüsseln kann – wenn überhaupt. Auch hier zeigte sich, dass davon nicht nur klassische IT-Systeme betroffen waren, sondern auch Industrie- und Produktionsanlagen. Schadsoftware und Hackerangriffe unterscheiden schon längst nicht mehr zwischen IT und OT (Operational Technology), also der klassischen Automatisierungstechnik.

Nachholbedarf in der Automatisierungstechnik

„WannaCry" hat aber noch mehr aufgezeigt: Es gibt noch gewaltigen Nachholbedarf bei der OT, was Cybersecurity anbelangt. Denn selbst Jahre nachdem es wirksame Sicherheitsupdates und Patches gegen diese Schadsoftware gibt, tauchen immer noch weitere Fälle in diesem Umfeld auf. Während bei IT-Systemen schon lange Prozesse etabliert sind, um schnellstmöglich Sicherheitslücken zu schließen, scheint das bei der OT noch keine Selbstverständlichkeit zu sein und Schutzmaßnahmen werden nur punktuell eingesetzt. Dabei ist in der Industrie das Schadenspotenzial sicher nicht geringer einzuschätzen. Jeder Betreiber weiß, was eine Stunde oder ein Tag Produktionsausfall bedeuten können oder Image-Schäden durch sabotierte Produkte und nicht zuletzt der Diebstahl geistigen Eigentums durch direkte Konkurrenten kosten können.

Wo sind aber die Gründe für diese offensichtliche Diskrepanz zu suchen? Ein Grund mag der Historie geschuldet sein, denn für OT ist das Thema Cybersecurity viel neuer verglichen mit der IT. Auch die Lebenszyklen der Automatisierungskomponenten und Systeme sind deutlich länger als bei den IT-Systemen. Erst bei der neuesten Generation von Automatisierungssystemen werden konsequent Security-by-Design-Ansätze berücksichtigt. Vorher war das schlichtweg keine Anforderung und nach wie vor sind noch viele Automatisierungssysteme im Einsatz, die vor über 10 Jahren oder vor noch längerer Zeit entwickelt worden sind.

Steigende Risiken durch neue Angriffsmethoden

In den letzten Jahren nahmen die Risiken stetig zu und es tauchten neue Bedrohungen auf, die insbesondere für kleinere Unternehmen existenzbedrohend sein können: Erpressung mit sogenannter

Für Maschinenbauer und Betreiber industrieller Anlagen ist Cybersecurity eine Herausforderung – glücklicherweise aber eine lösbare. Mittels eines mehrstufigen Defense-in-Depth-Konzepts für Anlagensicherheit, Netzwerksicherheit und Systemintegrität lassen sich die Vorzüge der Digitalisierung unbeschadet nutzen

Bild: Siemens

Die digitale Transformation sichern – Digitalisierung erfordert eine Anpassung und Erweiterung der Security-Konzepte

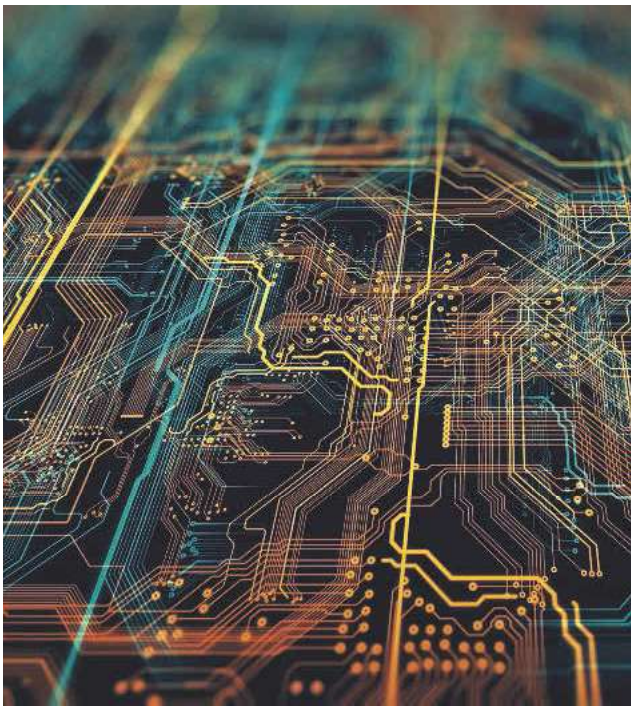


Bild: Siemens

Cybersecurity bietet Schutz vor Industriespionage und Angriffen durch Schadsoftware als größte Bedrohungen

Ransomware. Anders als bei der Industriespionage, bei der sich Hacker Zugriff auf das Unternehmensnetzwerk verschaffen, um dort möglichst lange unerkannt Daten abzugreifen, werden bei Ransomware-Angriffen Daten verschlüsselt und damit unbrauchbar gemacht.
Diese Angriffe sind leichter auszuführen und nicht so zielgerichtet wie bei der Spionage. Die Schadprogramme werden wahllos verschickt. Die Hacker versuchen dann mit vergleichsweise niedrigen Forderungen Lösegeld zu erpressen. Solche Angriffe sind für Unternehmen trotzdem hochgefährlich, weil sich die Systemsperrung auf den gesamten Betrieb auswirkt – nichts geht mehr. Keine Zugriffe mehr auf Kunden- oder Logistikdaten, keine Zugriffe mehr auf Maschinen, Programme, Applikationen oder Systeme, da alle Daten verschlüsselt und damit unbrauchbar gemacht wurden. Falls das Unternehmen den Fehler gemacht hat, dass die Back-up-Systeme auch über Netzwerke zugänglich sind, werden diese als erste verschlüsselt und der Schaden wird maximal. Auch bei Zahlung gibt es keine Gewähr, dass man den Entschlüsselungscode bekommt oder dass er funktioniert. Oft geht die Erpressung dann noch weiter. Das BSI (Bundesamt für Sicherheit in der Informationstechnik) rät daher, keine Zahlungen zu leisten.
Aber auch die Fähigkeiten und Möglichkeiten von Cyberangreifern entwickeln sich stetig weiter. Ihnen kommt zugute, dass der Trend zur Digitalisierung für immer weitergehende Vernetzung und mehr Daten sorgt. Die Vernetzung macht es Angreifern prinzipiell einfacher, auf Daten oder Komponenten zuzugreifen und Daten werden schon als das „neue Öl" oder auch das „neue Gold" bezeichnet. Auch wenn die Vergleiche hinken: Daten treiben die digitalisierte Industrie an und werden immer umfangreicher und wertvoller. Cyberkriminalität wird damit einfacher und zugleich lukrativer. Kein Wunder, dass die Bedrohungen insgesamt stark zugenommen haben und weiter zunehmen werden. Es ist ein regelrechter „Goldrausch" bei der Cyberkriminalität zu verzeichnen. Auch Unternehmen, die bislang verschont wurden, geraten nun unvermittelt ins Visier von Angreifern. Niemand kann sich mehr in Sicherheit wiegen.

Gegenmaßnahmen zur Abwehr von Cyberangriffen

Glücklicherweise gibt es bereits bewährte und effektive Konzepte zur Abwehr von Cyberangriffen, die speziell auf die Bedürfnisse und Anforderungen der OT zugeschnitten sind. In vielen Fällen müssen diese nur zur Anwendung gebracht werden, um Cybersecurity zu erreichen. Die Siemens AG, Nürnberg, empfiehlt hier nachdrücklich ein mehrschichtiges Verteidigungskonzept, das alle Ebenen mit einbezieht und nach dem sogenannten Defense-in-Depth-Prinzip eine tiefengestaffelte Verteidigung erlaubt. Diese mehrschichtige Verteidigung kombiniert mehrere Security-Maßnahmen auf drei Ebenen:

- **Anlagensicherheit:**
  Zur Sicherheit der Gesamtanlage gehören neben technischen Maßnahmen auch organisatorische wie Richtlinien und Prozesse sowie die Überwachung der Automatisierungsanlagen auf Anomalien, um Angriffe möglichst frühzeitig entdecken und größere Schäden vermeiden zu können.
- **Netzwerksicherheit:**
  Diese beinhaltet alle Maßnahmen, um unbefugte Zugriffe auf Automatisierungsnetze und das Mitlesen oder Verfälschen industrieller Kommunikation zu unterbinden, etwa über Firewalls oder die Nutzung verschlüsselter Protokolle.

Bild: Siemens

Bild: Siemens

Ein wesentlicher Faktor für den Erfolg der digitalen Wirtschaft ist die Reduzierung des Geschäftsrisikos durch Minimierung der Cyberrisiken

„Daten treiben die digitalisierte Industrie an und werden immer umfangreicher und wertvoller. Cyberkriminalität wird damit einfacher und zugleich lukrativer."

- **Systemintegrität:**
  Hierzu zählen alle Security-Maßnahmen, die dem Schutz der Automatisierungssysteme und Endgeräte wie Controller, Industrie-PCs und SCADA-Systeme dienen.

Der Nutzen liegt auf der Hand: Der Aufwand für Angreifer, mehrere aufeinander abgestimmte Verteidigungsebenen zu überwinden, steigt immens. Damit sinkt auch die Wahrscheinlichkeit, dass Angriffe erfolgreich durchgeführt werden können. Aber auch ein anderes Problem wird damit gelöst: Schwachstellen in Software und Produkten. Diese werden sich nie gänzlich vermeiden lassen, wie die ständigen Sicherheitsupdates zeigen. Auch dauert es immer eine gewisse Zeit vom Bekanntwerden über das Bereitstellen der Patches bis zur tatsächlichen Behebung beim Anwender. Es kann auch vorkommen, dass einige Schwachstellen nicht behoben werden, weil beispielsweise bei älteren Geräten deren Support eingestellt wurde oder der Anwender die Sicherheitsupdates nicht ausführt, weil kein Wartungsfenster verfügbar ist. Hier sorgt das Defense-in-Depth-Konzept dafür, dass einzelne Schwachstellen dennoch nicht ausgenutzt werden können oder deren Ausnutzung keine Schäden nach sich zieht, da andere Security-Maßnahmen weiterhin wirksam schützen. Wenn Angreifer sich Zugang zum Netz verschafft haben, können sie immer noch nicht auf die Endgeräte zugreifen und umgekehrt können Schwachstellen bei Endgeräten nicht ausgenutzt werden, wenn der Angreifer keinen Netzzugriff hat. Innentäter stellen natürlich eine besondere Herausforderung dar, aber auch hier können Maßnahmen wie beispielsweise physische Zugangskontrollen oder das 4-Augen-Prinzip für Abhilfe sorgen.

Fazit: Krise oder Chance?

Cybersecurity für die Industrie, kurz Industrial Security, ist und bleibt eine Herausforderung – aber eine lösbare. Solange Hersteller von industriellen Automatisierungs-, Netzwerk- und Softwarekomponenten dafür sorgen, dass die Cybersecurity-Eigenschaften und Funktionen sich den stetig wachsenden Bedrohungen anpassen und darüber hinaus mit entsprechenden Services auch dafür sorgen, dass dies während des Betriebes so bleibt, können auch Maschinenbauer und Betreiber industrieller Anlagen ihre Assets in angemessener Art und Weise schützen und die Vorzüge der Digitalisierung unbeschadet nutzen.

www.siemens.com

INFO

Mehr zum Defense-in-Depth-Konzept der Siemens AG: hier.pro/g3abl

elektro AUTOMATION