SICHERE KOMMUNIKATION – MIT DEM SENTRON PRODUKTPORTFOLIO

Die Energieverteilung in Infrastrukturen und Gebäuden **cybersicher digitalisieren**

Die Herausforderung

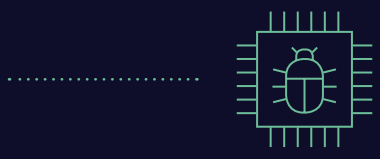
Die Sicherheit ist ein entscheidender Faktor für die Art und Weise, wie die Energieverteilung in Infrastrukturen und Gebäuden in einer digitalisierten Welt betrieben werden.

Cybersecurity, die Sicherheit der Kommunikations- und IT-Systeme, der Stromnetze sowie anderer digitaler Infrastrukturen, wird immer wichtiger – ein hochsensibler Bereich, in dem man zuverlässige Partner und ebenso sichere und zuverlässige Hard- und Software braucht. Denn das Internet der Dinge (IoT) und neue, digitale Geschäftsmodelle bieten zwar viele Vorteile, bergen aber auch Risiken. Je mehr Geräte in Ihren Infrastrukturen vernetzt und mit der Cloud verbunden sind, desto mehr Möglichkeiten für potenzielle Angriffe gibt es.

Cybersicherheitsexperten von Siemens haben in den letzten Jahren einen kontinuierlichen Anstieg von Malware und Exploits verzeichnet, die ihre Angriffe auf unterschiedlichste Anwendungen und Geräte richten.

Malware ändert zum Beispiel Geräte- und Softwarekonfigurationen oder lädt manipulierte Firmware auf IoT-Geräte. Letztere sorgt dafür, dass die eigentliche Funktion des Geräts verloren geht oder für andere Zwecke missbraucht wird. Siemens ist mit einem ganzheitlichen Ansatz zum Schutz und sicheren Betrieb solcher IoT-Landschaften ein Vorreiter auf dem Gebiet der Cybersicherheit.
siemens.de/sentron-digital

Malware:
ein Computerschadcode, der die eigentliche Funktion der Anwendung oder des Produkts stört.



Exploits:
nutzen Schwachstellen, um Software anzugreifen und Malware nachzuladen.

SIEMENS

Cybersicherheit **strategisch geplant**

Weil dieses Thema sich nicht nur auf die Grenzen des eigenen Einflussbereichs beschränkt, sondern auch bei Geschäftspartnern und Lieferanten im unmittelbaren Umfeld eine wichtige Rolle spielt, hat Siemens schon früh begonnen, auch dieses Umfeld möglichst cybersicher zu gestalten.

Ein wichtiger Schritt dazu ist die von Siemens initiierte Charter of Trust, ein stetig wachsender Verbund von zurzeit 15 Großkonzernen aus unterschiedlichsten Märkten (IBM, Mitsubishi oder Total).

Als eine der ersten Maßnahmen der Charter of Trust erarbeiteten die Partner im Oktober 2018 unter der Schirmherrschaft des Vorstandvorsitzenden der Siemens AG, Joe Kaeser, grundlegende Anforderungen an die Cybersicherheit digitaler Lieferketten. Diese werden sie unter Berücksichtigung ihrer Lieferanten in ihren eigenen globalen Lieferketten einbinden.

Charter of Trust

In der Charter of Trust wird die vertrauensvolle Zusammenarbeit führender Unternehmen aus der ganzen Welt für Cybersecurity über die Grenzen einzelner Unternehmen hinaus im globalen Maßstab organisiert. Die zehn Schlüsselprinzipien der Charter geben die Leitlinien für die Gestaltung einer digitalen Welt vor.

01 Verantwortung für Cyber- und IT-Sicherheit verankern

02 Verantwortung in der digitalen Lieferkette übernehmen

03 Cybersicherheit als Werkseinstellung konfigurieren

04 Bedürfnisse der Nutzer in den Mittelpunkt stellen

05 Innovation und Co-Creation vertiefen

06 Cybersicherheit zum festen Teil der Ausbildung machen

07 Kritische Infrastrukturen und IoT-Lösungen zertifizieren

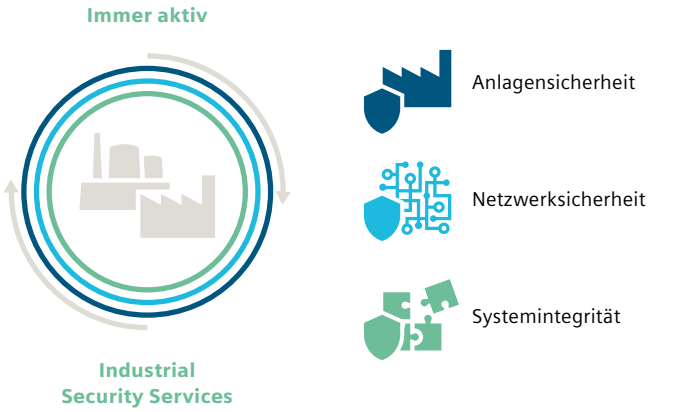
08 Transparenz und Reaktionskraft steigern

09 Regulatorischen Rahmen schaffen

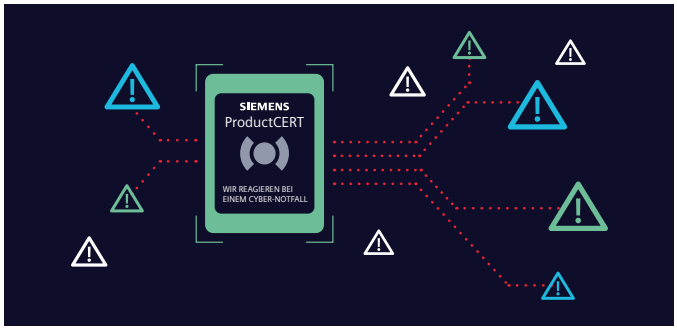
10 Gemeinsame Initiativen vorantreiben

Ganzheitlicher Lösungsansatz bei Siemens

Um den vielgestaltigen Bedrohungen für die Datensicherheit im IoT zu begegnen, ist ein strategisches Vorgehen auf vielen Ebenen ratsam.



Defense-in-Depth:
eine Strategie sich überlagernder, gestaffelter Abwehrmechanismen, mit der wertvolle Informationen und Daten geschützt werden. Versagt ein Abwehrmechanismus, tritt sogleich der nächste in Kraft.



Siemens verfolgt dazu einen ganzheitlichen Schutzansatz. Unter dem Defense-in-Depth-Konzept wird ein vielschichtiges Informationssicherungskonzept auf allen Ebenen gleichzeitig aufgebaut – von der Betriebs- bis zur Feldebene, von der Zutrittskontrolle bis zum Kopierschutz.

Maßgeblich verantwortlich für all diese Prozesse, Anwendungen und Lösungen ist das Siemens ProductCERT. CERT steht dabei für „Computer Emergency Response Team". Ein Cybersicherheitsexpertenteam informiert und berät die Kunden und sucht weltweit nach neuen Hinweisen zu Schwachstellen bei Siemens-Produkten, um sofort entsprechende Gegenmaßnahmen zu erarbeiten.

Wichtig ist Siemens auch die proaktive Kommunikation bekannt gewordener Angriffe und der passenden Gegenmaßnahmen wie Patches und Updates. Darüber informiert Siemens zum Beispiel über die frei zugängliche Webseite Siemens Security Advisories (SSA) sowie den kostenlosen Twitter-Account @ProductCERT und die ebenfalls kostenfreien Advisory-Mailings für registrierte Empfänger.

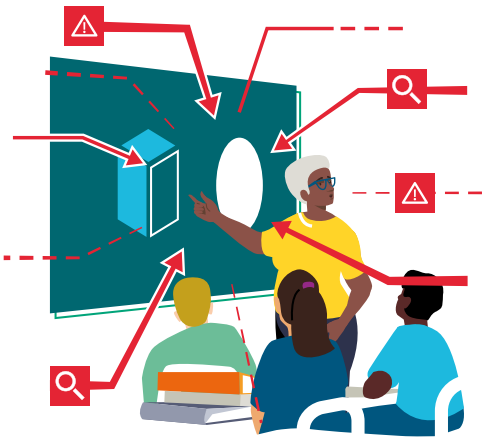
Kenne die Probleme. Kenne die Gegenmaßnahmen. Abboniere Siemens Security Advisories.

Geschulte Mitarbeiter

Der Ansatz einer ganzheitlichen cybersicheren Lösung umfasst bei Siemens auch die Schulung der Mitarbeiter.

Siemens führt jährlich eine für jeden Mitarbeiter verpflichtende interne Cybersicherheitsbewusstseinsschulung durch. Dabei werden unter anderem Angriffsszenarien wie Social Engineering erklärt.

Siemens verfügt außerdem über eine Cybersicherheitsorganisation, die über alle operativen und strategischen Firmenteile ausgerollt ist: Unter dem Kurznamen PSS (Product and Solution Security) kann sich jeder Mitarbeiter und jedes interne Projektteam zum Thema Cybersicherheit beraten und weiterbilden lassen. Das ermöglicht ihnen, den Kunden Lösungen und Produkte zu liefern, die diese cybersicher konfigurieren, einbauen und betreiben können.



Social Engineering:
das Ausspähen von persönlichen Daten über unterschiedlichste Wege.

Schwachstellenanalyse **in der Tiefe**

Basierend auf der PSS-Strategie erfolgt darüber hinaus auch eine Bedrohungs- und Risikoanalyse, welche dazu dient, Geräte und Applikationen bereits vor und während der Entwicklung unterschiedlichen Cybersicherheitstests zu unterziehen.

Einer dieser Tests ist der sogenannte Schwachstellen-Scan, mit dem bekannte Schwachpunkte im Sinne der Cybersicherheit sofort erkannt und umgehend behoben werden können. Parallel dazu wird die Robustheit der Kommunikationsschnittstelle in einem automatisierten Test geprüft. Dabei wird die Stabilität des Geräts unter Veränderung bestimmter Parameter der IP-Kommunikation getestet.

Schutzmechanismen für das **SENTRON Produktportfolio**

Die Cybersecurity-Maßnahmen bilden die Basis zum sicheren Betrieb kommunikationsfähiger Produkte:

- Nur von Siemens signierte Firmware wird in diesen Produkten eingesetzt. So kann ausschließlich authentische, von Siemens hergestellte Software auf dem jeweiligen IoT-Gerät installiert und betrieben werden. Das verhindert die Veränderung der Firmware durch Dritte.
- Bei vielen Siemens-Geräten kann ein Passwortschutz gesetzt werden, der die Konfiguration des Geräts vor unautorisierten Schreibzugriffen schützt.
- Durch Konfiguration eines IP-Adressenfilters werden nur bestimmte, vom Kunden anerkannte IP-Adressen zur Kommunikation mit dem Gerät freigegeben.
- Die Konfiguration lässt sich durch einen Hardware-Schreibschutzschalter gegen Änderungen an der Konfiguration aus der Ferne verriegeln.

Mit all diesen Maßnahmen hat Siemens die Weichen für eine cybersichere SENTRON Produktreihe gestellt. Da sich die Bedrohung ständig verändert und weiterentwickelt, passt auch Siemens seine SENTRON Produkte dem gestiegenen Sicherheitsbedürfnis an und entwickelt neue Sicherheitstechniken, die stetig Risiken reduzieren. Mit SENTRON Produkten investieren die Kunden in den neuesten Stand der Technik und damit in eine sichere Zukunft.

Herausgeber
Siemens AG

Smart Infrastructure
Electrical Products
Siemensstraße 10
93055 Regensburg
Deutschland

Artikel-Nr. SIEP-B10239-00
Dispo 25600 TH S22-220144 WS 0622

SIEMENS