TECHNISCHE VERÖFFENTLICHUNG

Cybersicherheit

When **energy** matters

socomec
Innovative Power Solutions

Cybersicherheit - Fragen und Antworten

Dieses Dokument liefert Antworten auf wichtige Fragen zur Cybersicherheit.

Methodik

Zuerst werden grundlegende Prinzipien erläutert und dann die häufigsten Anwendungsfälle für unsere Kunden vorgestellt.

Obwohl wir bei unseren Produkten für größtmögliche Sicherheit sorgen, hängt die Robustheit einer Installation auch von ihrer Gesamtkonzeption ab, da jeder einzelne Aspekt Auswirkungen auf die Gesamtsicherheit haben kann.
Die Sicherheit einer elektrischen Installation kann mit einem Kettenhemd verglichen werden. Genau wie bei den Komponenten einer Installation bietet jeder einzelne Metallring des Kettenhemds einen lokalen Schutz. Was aber den Gesamtschutz so wirksam macht, ist das kohärente Ineinandergreifen der Einzelteile.
Eine unzureichende Abdeckung oder ein Loch im Kettenhemd stellt eine Schwachstelle dar und erhöht das Risiko eines gezielten Angriffs um das Zehnfache.
Wir haben hier für Sie die Informationen zusammengestellt, die Ihnen bei der Entscheidungsfindung für Ihr Sicherheitskonzept helfen werden.

Viel Spaß beim Lesen!

€ 800,000

kostet eine Sicherheitsverletzung
im Durchschnitt*

Jedes Unternehmen ist

29 Cyberangriffen

pro Jahr ausgesetzt**

** Quelle: https://experiences.microsoft.fr/articles/cybersecurite/cybersecurite-chiffres-cles/*

*** Quelle: https://www.silicon.fr/hub/malwarebytes-hub/cybersecurite-les-10-chiffres-qui-font-peur*

Inhalt

Cybersicherheit: Definition

„Der Zweck aller Gesetze, Richtlinien, Tools, Systeme, Sicherheitskonzepte und -mechanismen, Risikomanagementmethoden, Maßnahmen, Schulungen, bewährten Praktiken und Technologien, die zum Schutz von Personen und der materiellen und immateriellen IT-Vermögenswerte von Staaten und Organisationen eingesetzt werden können“.

Quelle: Wikipedia

Laut Wikipedia stellt die **Cybersicherheit** eine Reihe von wirtschaftlichen, strategischen und politischen Herausforderungen dar, die weit über die Sicherheit von Informationssystemen (SIS) hinausgehen. Es geht um Management-IT, industrielle IT, eingebettete IT und vernetzte Geräte. Cybersicherheit muss als Teil eines ganzheitlichen Ansatzes betrachtet werden, wobei wirtschaftliche, soziale, bildungspolitische, rechtliche, technische, diplomatische, militärische und nachrichtendienstliche Aspekte berücksichtigt werden müssen.

Der Begriff **Cyber-Resilienz** ist eng mit dem Management der Cybersicherheit verbunden. Er bezieht sich **auf die Fähigkeit des Systems oder der Netzarchitektur, den Betrieb im Falle eines Ausfalls oder eines Angriffs fortzusetzen.**

In diesem Dokument wird erläutert, wie ein allumfassender Ansatz für die Informationssicherheit entwickelt werden kann. Der Fokus liegt dabei auf unserer Hardware, es werden aber auch viele weitere Parameter betrachtet.

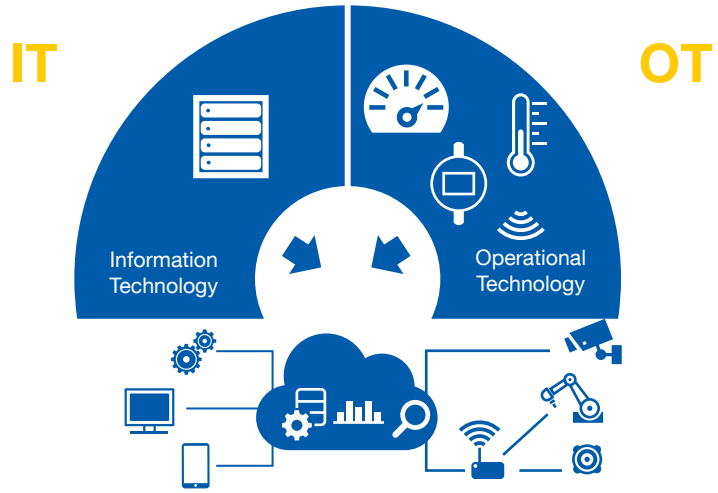
Ziel ist es, unseren Kunden ein umfassendes, an ihre Bedürfnisse angepasstes Angebot zu unterbreiten, das eine **kohärente, sichere und widerstandsfähige Lösung** garantiert.

Cybersicherheit: Warum ist sie notwendig?

Warum ist es so wichtig, sich mit dem Thema Cybersicherheit zu befassen?

Konvergenz von IT und OT

Definition von IT und OT



Historisch gesehen gab es in Industrieunternehmen zwei **getrennte Umgebungen.**

IT (Information Technology)

IT (Information Technology)

- **Definition**
Infrastruktur für die Büroautomation.

- **Angeschlossene Komponenten**
PCs und Server.

- **Sicherheitsstufe** Alles,
was mit diesem Netz verbunden ist, ist **standardisiert** und **gesichert** (normalerweise Windows oder Linux).
Den Administratoren dieses Netzes stehen eine **Reihe von Tools und Diensten zur** Verfügung, **um die Sicherheit** des gesamten Systems **wirksam zu gewährleisten** (Virenschutz, Firewall, massiver Patch-Deployment-Service, regelmäßige Updates, Alarmüberwachung usw.).
Sie können **schnell Patches bereitstellen,** die dann an alle Geräte im Netzwerk verteilt werden.
Außerdem wird die installierte IT-Basis häufig erneuert **(kurzer Lebenszyklus von 3 bis 5 Jahren**), wodurch die Beibehaltung veralteter oder elektronisch unzuverlässiger Produkte vermieden wird.

OT (Operational Technology)

OT (Operational Technology)

- **Definition**
Umgebung der industriellen Prozesse.

- **Angeschlossene Komponenten**
Von kommunizierenden Sensoren über Industriesteuerungen bis hin zu Zählern, Motoren mit Positionsmeldern usw. sowie allen Komponenten einer Produktionslinie.

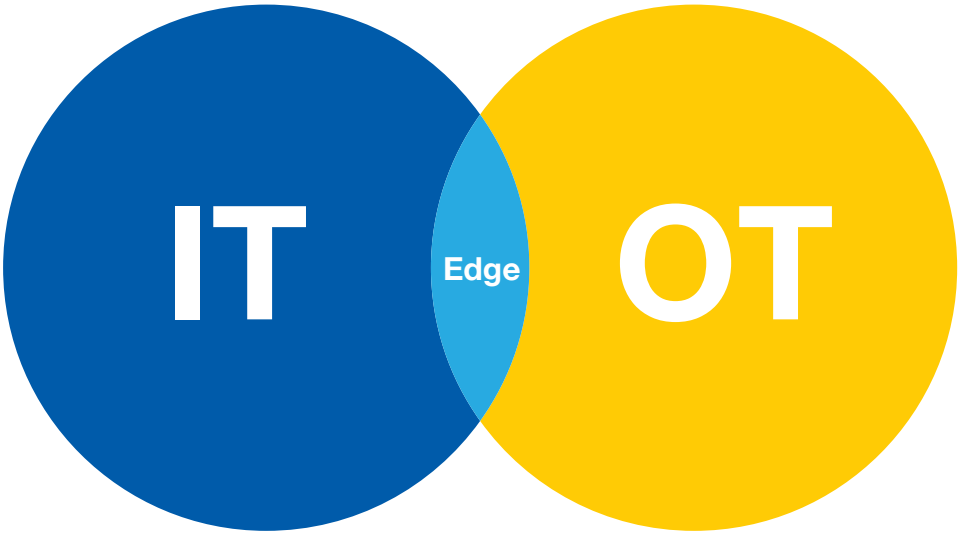
- **Sicherheitsstufe**
Alle diese Komponenten können aufgrund ihrer **Heterogenität** nicht miteinander kommunizieren.
Das Gesamtsystem bzw. die Installation verfügt über **keine „eingebaute Sicherheit“**, da dies bisher als zu teuer angesehen wurde und von den üblichen Wartungsmaßnahmen wie z. B. Updates nicht berührt wird.
Außerdem sind die entsprechenden Produkte teuer und auf Langlebigkeit ausgelegt, oft mit Lebenszyklen von **10 bis 20 Jahren** oder mehr. Dementsprechend verbleiben anfällige Geräte häufig sehr lange Zeit im Unternehmen, so dass Sicherheitslücken lange genug offen bleiben, um ausgenutzt zu werden.

Rückmeldung von Betriebsdaten zur Optimierung von Prozessen und Verbräuchen.

OT: zunehmend offen und vernetzt

Lange Zeit war die OT sehr verletzlich und unsicher. Die einzig sinnvolle und zuverlässige Form des Schutzes bestand darin, diese Umgebung als einen innerhalb des Unternehmens isolierten Bereich zu betreiben, um ihre Schwachstellen nicht preiszugeben.
Seit einigen Jahren erleben wir schon das rasante Fortschreiten des **IoT** (Internet der Dinge) und der **Industrie 4.0**.
Was ist der Grund dafür? Die Notwendigkeit der Rückmeldung von Betriebsdaten zur Optimierung von Prozessen und Verbrauch.
Die Überwachung, Steuerung und Optimierung des industriellen Prozesses (OT) aus dem Büro oder der **Cloud**, d.h. der IT-Umgebung, ist eine Notwendigkeit geworden. Ein isolierter Betrieb der OT-Netzwerke ist deshalb nicht mehr möglich.
Wir erleben also ein Zusammenwachsen – eine Konvergenz – dieser vormals getrennten Umgebungen, die trotz ihrer inhärenten Unterschiede miteinander kommunizieren müssen.

Edge: ein sensibler Konvergenzbereich



Um die Konvergenz von IT und OT zu erleichtern, gibt es eine Kommunikationszone, die als **Edge** bezeichnet wird und den Übergang zwischen der Industrie- und der Büroautomatisierungsumgebung markiert.
In dieser Zone finden wir Geräte, die Sprachumwandlungen vornehmen, um Nachrichten von einer Umgebung in die andere zu übertragen.
Hier handelt es sich in der Regel um **Gateways**, die gleichzeitig mit OT und IT verbunden sind. Sie nehmen Nachrichten aus der IT-Umgebung entgegen, wandeln sie in eine verständliche Form um und leiten sie dann an die OT-Umgebung weiter – und umgekehrt.

Diese Geräte sind dabei sehr exponiert:
- Sind befinden sich in große Nähe zum Internet als wesentliche Quelle von Hackerangriffen,
- oder sie sind mit der IT-Umgebung verbunden, wodurch die OT angreifbar wird.

Da diese Zone besonders sensibel ist, muss ein Höchstmaß an Sicherheit gewährleistet werden, insbesondere bei den Gateways und ihrer Umgebung.

Heutzutage erfolgt die Einrichtung der Edge oft ohne Schutz und ohne Berücksichtigung der Schwachstellen und Sicherheitslücken, was die zunehmende Zahl von Angriffen auf Unternehmen erklärt!
Ein Hacker dringt bevorzugt über die am wenigsten geschützte Seite in ein Unternehmen ein – und hier eignet sich die OT meist besonders!

Ein Hacker dringt bevorzugt über die am wenigsten geschützte Seite in ein Unternehmen ein – und hier eignet sich die OT meist besonders!

Zunehmende Häufigkeit der Angriffe

Zahlen und Statistiken

Ein kurzer Rückblick auf die Geschichte der Datenverarbeitung zeigt, dass die ersten Angriffe auf Unternehmen im November 2007 stattfanden. Der berühmte **Stuxnet-Virus** ebnete den Weg für eine Welle von Angriffen in diesem Sektor. Deren Häufigkeit nimmt seitdem stetig zu.
Stuxnet wurde angeblich von den Regierungen der USA und Israels entwickelt, um die iranischen Atomanlagen anzugreifen und das iranische Atomprogramm einzubremsen. Obwohl diese Systeme damals nicht mit dem Internet verbunden waren, wurden die Anlagen durch die Einschleppung des Virus über USB-Sticks manipuliert!
Fünf Unternehmen, die mit dem Atomprogramm in Verbindung stehen, wurden gehackt. Zentrifugen und Ventile wurden sabotiert, um ihre physische Zerstörung herbeizuführen, wobei die Überwachungsorgane mit Falschinformationen versorgt wurden, um keinen Verdacht zu erregen.

Seitdem wurde diese Methode für das Hacken von Unternehmensumgebungen oft wiederholt. Diese Angriffe sind schwerwiegend, da sie Prozesse mit erheblichen finanziellen Auswirkungen beeinträchtigen, Hardwareausfälle verursachen und/oder eine Gefahr für Menschen darstellen können.

Gesundheits- und IT-Branche: Umgang mit Cyber-Bedrohungen
(Von Stéphane Astier und Claire Lefebvre)
Seit einigen Jahren nehmen Cyberangriffe auf die IT-Systeme von Gesundheitseinrichtungen zu: 2020 entfielen fast 11 % der in Frankreich registrierten Cyberangriffe auf Krankenhäuser. Dieser Trend setzte sich 2021 fort, unter anderem mit dem am 12. September bestätigten Cyberangriff auf die Pariser Krankenhausbehörde.

Quelle: Haas Avocats

Mehr als die Hälfte der französischen Unternehmen bereits Opfer von Cyberangriffen
CESIN – Expertengruppe für digitale und Informationssicherheit
Die Expertengruppe CESIN hat gerade ihre siebte jährliche Barometer-Umfrage veröffentlicht, die von OpinionWay erstellt wurde. Als erstes fällt auf, dass 2021 für Cyberkriminelle ein erfolgreiches Jahr war: Mehr als jedes zweite Unternehmen gibt an, zwischen einem und drei erfolgreiche Angriffe erlebt zu haben.
60 % der Unternehmen berichten, dass diese Angriffe ihren Geschäftsbetrieb unterbrochen hatten.

Quelle: L1FO – CESIN – CESIN – CESIN – GlobalSecurityMag – UD – IT Social

Cyberangriff unterbricht Kraftstoffversorgung im Iran
Im Iran herrschte mehr als 24 Stunden ein landesweiter Kraftstoffmangel. Ein Cyberangriff hatte landesweit Tankstellen lahmgelegt, den Zugang zu Zapfsäulen mit elektronischen Karten blockiert und den Alltag erheblich gestört.

Quelle: LMI – SN – Siecle Digital

Annecy zum zweiten Mal innerhalb eines Jahres Opfer eines Cyberangriffs
Die IT-Abteilungen von Annecy im Departement Haute-Savoie waren seit heute Vormittag nach einem Hackerangriff erneut ausgefallen. Online-Angebote und E-Mail waren nicht verfügbar.

Quelle: UD

Cyberangriff auf den Hafen von Houston: Cyberkriminelle greifen kritische Infrastrukturen an
Houston, einer der größten Häfen der USA, hat soeben bekannt gegeben, dass er im vergangenen Monat Ziel eines mutmaßlichen Hackerangriffs durch einen Nationalstaat war. Die Cyberkriminellen sollen Malware implantiert und versucht haben, Microsoft-Anmeldedaten zu stehlen. Die IT-Teams der Hafenbehörde gaben jedoch an, dass sie diesen Hackversuch abwehren konnten und bestätigten, dass keine betrieblichen Daten oder Systeme betroffen waren.

Quelle: UnderNews

159 lokale Behörden
wurden im Jahr 2020 gehackt*

Im Jahr 2022 erlebte Malware einen rasanten Wiederanstieg von ihrem Siebenjahrestief im Jahr 2021 und **kletterte auf erstaunliche 2,8 Milliarden Angriffe****

Im Jahr 2022 war der Energiesektor mindestens **4 % der Betriebszeit Ransomware-Angriffen ausgesetzt.**
Cyber-Angriffe kosten den **Energiesektor durchschnittlich 4,72 Millionen pro Vorfall** (2022)***.

** Nach Angaben von IPTF Acyma (Anssi).*

*** https://www.sonicwall.com/medialibrary/en/infographic/mid-year-update-2022-sonicwall-cyber-threat-report.pdf*

**** https://www.ibm.com/downloads/cas/3R8N1DZJ*
https://docs.apwg.org/reports/apwg_trends_report_q3_2022.pdf

Auf Daten abzielende Cyberangriffe

Angriffe auf Unternehmen zielen in der Regel auf Daten ab. Dabei sind mehrere Szenarien denkbar.

- **Böswillige Überwachung:** Die Daten werden zu böswilligen Überwachungszwecken missbraucht. Dabei kann es sich um wirtschaftliche oder strategische Daten handeln, die über den Schwarzmarkt an Konkurrenten weiterverkauft werden. Es kann sich auch um technische Daten handeln, mit denen die Hacker einen Angriff vorbereiten.

- **Manipulierte Daten:** Ziel dieses Angriffs ist die Beeinflussung eines Abrechnungs- oder Industrieprozesses durch Manipulation der Daten.

- **Datenlöschung:** Löschung von Daten oder Informationen, z.B. aus einem CRM-System, um dem Zielunternehmen Schwierigkeiten zu bereiten.

Angriffe auf industrielle Prozesse

Diese Angriffe können auf industrielle Prozesse abzielen, durch:

- **eine Manipulation der Daten,** z.B. Änderung des Produktionssollwerts oder der Kalkulationswerte, Änderung oder Löschung der Zugangsdaten des Wartungspersonals, Änderung der Zugangsrechte usw.

- **direkte Steuerung** von Aktoren, um einen Prozess zu stören oder zu zerstören, oder sogar Menschen zu gefährden.

85 %
Finanzielles Risiko

45 %
Datenrisiko

30 %
Risiko einer Unterbrechung der Geschäftstätigkeit/des Betriebs

29 %
Risiko der Rufschädigung

Auswirkungen von Angriffen

Die finanziellen Auswirkungen sind kumulativ: Produktionsausfall und Umsatzeinbußen, Vertragsstrafen wegen mangelnder Lieferfähigkeit oder sogar der Verlust unzufriedener Kunden. Die Folgen eines Angriffs auf das Image des Unternehmens sind ebenfalls beträchtlich und spiegeln ein Versagen beim Schutz des Unternehmens und seiner Kunden wider, insbesondere wenn das Unternehmen nicht mit einem Kommunikationsplan und entsprechenden Maßnahmen reagiert.

Was ist zu schützen?

Systemsicherheit bietet Schutz vor Bedienungsfehlern und/oder Missbrauch.
In der Regel wird eine Analyse durchgeführt, um festzustellen, welche Ressourcen geschützt werden müssen (sensible Daten oder Geräte wie Gateways).
Ein anderer Ansatz ist die Betrachtung der verschiedenen potenziellen Bedrohungen, um die zu ergreifenden Schutzmaßnahmen zu bestimmen.
In allen Fällen muss ein wirksames Sicherheitskonzept den Schutz und die Integrität der Daten, die Verfügbarkeit der Prozesse und die Rückverfolgbarkeit der dort durchgeführten Maßnahmen gewährleisten.

Datenschutz

Unter Datenschutz versteht man die Sicherheit, dass die ausgetauschten Daten für Unbefugte nicht zugänglich sind und sensible Daten nicht in die Hände unbefugter Dritte gelangen.
Hierbei geht es um Passwörter, persönliche Daten, aber auch um sensible Betriebsdaten, Verwaltungs- oder Wartungsdaten usw.

Beispiel: Ein Unbefugter fängt die an den Remote-FTP-Server gesendete Index-csv-Datei ab.
Ein gefälschter FTP-Server gibt sich als der echte Server aus, um die gesendeten Dateien abzufangen.

Prozessverfügbarkeit

Verfügbarkeit bedeutet, dass die Daten zuverlässig jedem autorisierten Benutzer zur Verfügung stehen.

Beispiel: Ein Angriff durch Überfluten des Gateways mit Anfragen, bis es zusammenbricht und den Datenzugang unterbricht.

Datenintegrität

Integrität bedeutet, dass Gewissheit besteht, dass das System, seine Konfiguration und seine Daten zuverlässig sind und nicht manipuliert wurden.

Dies beinhaltet Maßnahmen, die sicherzustellen, dass das System intakt bleibt und sein Betrieb nicht durch unkontrollierten Datenverkehr beeinträchtigt wird.

Rückverfolgbarkeit von Maßnahmen

Rückverfolgbarkeit gewährleistet die Authentifizierung von Benutzern und weist die Verantwortlichkeit für durchgeführte Maßnahmen nach.

Dies ist ein wesentliches Merkmal der Cybersicherheit, da damit protokolliert wird, wer was wann getan hat.

Wie können Sie sich schützen?

Schritt # 1: Audit durchführen

Schritt 1: Audit durchführen

Verfolgen Sie den Weg der Daten und identifizieren Sie alle potenziellen Angriffspunkte für Hacker (physisch, drahtgebunden, drahtlos usw.).

Vernetzte Produkte und lokale Anwendungen > *Kommunikations-netzwerk* > *Cloud-Plattform und Webdienste* > *Web-Apps und mobile Apps* > *Qualifizierte Dienstleistungen*

Datenerzeugung > Datenübertragung > Datenzentralisierung und -speicherung > Datenverarbeitung

Schritt # 2: Sensible Punkte identifizieren

Schritt 2: Sensible Punkte identifizieren

Sobald der Datenpfad bestimmt ist, müssen die sensiblen Punkte entlang des Pfades identifiziert werden, damit entsprechende Sicherheitsmaßnahmen umgesetzt werden können.
Der Schutzgrad richtet sich **nach der Sensibilität der Daten und der Anfälligkeit des Übertragungspunkts, ohne dabei die Risikobewertung zu übertreiben.**

Schritt # 3: Maßnahmenplan umsetzen

Schritt 3: Maßnahmenplan umsetzen

A

Aufbau oder Anpassung der Architektur zur **Sicherung der gesamten Kette**

B

Auswahl von Systemen, die ein angemessenes Sicherheitsniveau aufweisen

C

Aufbau einer **cybersicheren Organisation**

A Aufbau oder Anpassung der Architektur zur Sicherung der gesamten Kette

Es gibt viele Möglichkeiten, sich zu schützen: Backups, Verschlüsselung von Informationen, verschlüsselte Kommunikationskanäle usw.
Wichtig ist dabei, dass **diese Maßnahmen über die gesamte Kette verteilt werden, um eine umfassende und ausreichende Abdeckung zu gewährleisten.**
Es bringt wenig, nur ein Glied der Kette maximal zu verstärken, da bekanntlich das schwächste Glied der Kette die Belastbarkeit des Gesamtsystems bestimmt.
Erst wenn alle Glieder der Wertschöpfungskette gleichermaßen gesichert sind, können Daten ausgetauscht werden, ohne dass die Gefahr besteht, dass sie böswillig abgefangen oder manipuliert werden.

Weitere Informationen finden Sie im Abschnitt „Das Angebot von Socomec – Schutz der Architektur“.

Weitere Informationen über Normen und Standards finden Sie auf Seite 12.

Mit diesem Ansatz der kontinuierlichen Verbesserung wird Cybersicherheit fest in der DNA des Unternehmens verankert.

B Auswahl von Systemen, die ein angemessenes Sicherheitsniveau aufweisen

Die Sicherung der gesamten Kette erfordert natürlich eine sorgfältige Auswahl ihrer Subsysteme. Im Folgenden sind einige Prüfkriterien aufgeführt, die sicherstellen, dass das ausgewählte System ein ausreichendes Sicherheitsniveau aufweist.

Kriterium 1: Produktgestaltung unter Berücksichtigung der „eingebauten Sicherheit“

Zur Gewährleistung eines hohen Sicherheitsniveaus muss Cybersicherheit bereits in der Produktgestaltungsphase für bestimmte Verwendungszwecke berücksichtigt werden, indem es in seiner endgültigen Umgebung platziert wird.
Beim Ansatz „eingebaute Sicherheit“ ist es von entscheidender Bedeutung, nicht nur die Sicherheit des Produkts selbst zu berücksichtigen, sondern auch die Architekturen, in die es integriert werden soll.

Kriterium 2: Normen und Standards

Die Frage der Cybersicherheit in Unternehmen steht heute an einem Wendepunkt.
Die Verschärfung der Gesetzgebung in Europa und Frankreich führt hier zu einem Paradigmenwechsel. Mit der Einführung gesetzlicher Verpflichtungen entwickelt sich das aktuelle Denken über die Cybersicherheit von Unternehmen weiter. Ein Produkt oder System, das die Anforderungen einer Norm erfüllt, gilt als Qualitätsgarantie.

C Aufbau einer cybersicheren Organisation

Um effizient zu sein, muss der Ansatz von der auf Cybersicherheit ausgerichteten Organisation **vorgelagert durch die Produktgestaltung abgesichert** und **nachgelagert durch Unterstützung des Kunden** gewährleistet werden.

Organisatorischer Ansatz und Risikomanagement

Sobald die Risiken ermittelt sind, muss das Verhältnis bestimmt werden zwischen:
- der Wahrscheinlichkeit eines Ereignisses und
- den Auswirkungen eines solchen Ereignisses.

Anhand dieses Verhältnisses werden dann die anzuwendenden Schutzmaßnahmen bestimmt:
- Senkung des Risikos durch Eingrenzung seiner möglichen Auswirkungen,
- Senkung des Risikos durch Verringerung der Eintrittswahrscheinlichkeit,
- Teilen des Risikos mit einem Dienstleister,
- Akzeptanz des Risikos, z.B. wenn die zu treffende Maßnahme im Verhältnis zum Risiko zu teuer ist.

Ständige Verbesserung

Der Risikomanagementplan wird dann in einen Maßnahmenplan überführt.
Diese Maßnahmen können sehr vielfältig sein, von der Implementierung einer Firewall bis hin zur Schulung von Teams und der Definition von Kommunikations- und Informationsübertragungsprozessen.
Der Maßnahmenplan soll natürlich langfristig entwickelt werden, einschließlich operativer Kontrollmaßnahmen, um sicherzustellen, dass er innerhalb der neugestalteten Organisation ordnungsgemäß funktioniert.
Regelmäßig analysierte Schlüsselindikatoren ermöglichen die fortlaufende Ermittlung verbesserungswürdiger Bereiche und folglich die Anpassung des Maßnahmenplans.

Compliance

Dieser Ansatz ist sehr pragmatisch und für jedes Unternehmen geeignet. Um sicherzustellen, dass alle Aspekte der Cyber-Umgebung abgedeckt sind, sollten international anerkannte und bewährte Leitlinien befolgt werden.
Eine Reihe von Normen untermauert diesen Ansatz und verleiht dem Prozess, seiner Anerkennung und dem Vertrauen, das in die gem. ISO 27001 neu gestaltete Organisation gesetzt wird, zusätzliches Gewicht.

Normen im Blickpunkt

Auswirkungen des MPA auf Unternehmen

Das 2013 in Kraft getretene Gesetz zur Programmierung für das Militär, der „Military Programming Act (MPA)“ ermöglicht die Identifizierung und Klassifizierung von mehr als 200 Organisationen, die als „öffentliche und private Betreiber von wesentlicher Bedeutung“ (Operators of Vital Importance (OIV)) Einrichtungen betreiben oder nutzen, die als wesentlich für das Bestehen der Nation gelten.
Die mit der Einhaltung der Vorschriften verbundenen Verpflichtungen werden die Kontakte zwischen den OIV und den Akteuren in Bereichen, die auf digitales Vertrauen angewiesen sind, beschleunigen und intensivieren und die Entwicklung einer dauerhaften Cybersicherheitsbranche fördern.

Umsetzung der europäischen NIS-Richtlinie

Die im Dezember 2018 in Kraft getretene Richtlinie zur Netz- und Informationssicherheit (NIS) legt einen europäischen Rahmen fest, der mit dem MPA vereinbar ist und für dessen Anwendung jedes Land in seinem Hoheitsgebiet verantwortlich sein wird. Die Richtlinie beschreibt Maßnahmen, die ein hohes Maß an Sicherheit für die Netze und Informationssysteme der 27 Mitgliedstaaten der Europäischen Union gewährleisten sollen.
In Frankreich wurde ein Rechtsrahmen geschaffen, um die Cybersicherheit der Dienstanbieter, die als wesentlich für das Funktionieren von Wirtschaft und Gesellschaft gelten (OES), zu verbessern. Ende 2019 gab es 600 solcher Dienstanbieter.

Sektorspezifische Regulierung

Zusätzlich zu den Verpflichtungen, die im Rahmen des MPA eingeführt wurden, gibt es zahlreiche Gesetze und Verordnungen für private und öffentliche Einrichtungen. Die zwei nachfolgenden sind für Unternehmen besonders erwähnenswert und international bekannt.

Norm ISO 27001

Diese Norm gilt für alle Arten von Organisationen (Unternehmen, Nichtregierungsorganisationen, Regierungsbehörden usw.) und legt die Anforderungen für die Einführung eines Managementsystems für die Informationssicherheit (ISMS) fest. Das ISMS definiert die Sicherheitsmaßnahmen für bestimmte Umgebungen, um den Schutz der Vermögenswerte der Organisation zu gewährleisten.

Ziel ist es, Funktionen und Informationen vor Verlust, Diebstahl und Manipulation sowie IT-Systeme vor Eindringlingen und Großschäden zu schützen. Dies schafft zusätzliches Vertrauen bei den Beteiligten.

Die ISO/IEC 27001 führt eine Reihe von Kontrollpunkten auf, die beachtet werden müssen, um die Wirksamkeit des ISMS zu gewährleisten und dessen Funktion und Weiterentwicklung zu ermöglichen. Im Einzelnen besteht Anhang A der Norm ISO/IEC 27002 aus 14 Abschnitten mit 114 Sicherheitsmaßnahmen. Wie bei der ISO 9001 und der ISO 14001 ist auch eine Zertifizierung gemäß ISO/IEC 27001 möglich.

Norm IEC 62443 *(„Industrielle Kommunikationsnetze – IT-Sicherheit für Netze und Systeme“)*

Die IEC 62443 ist eine internationale, branchenübergreifende Norm. Sie enthält eine Reihe von Normen, technischen Berichten und Informationen über sichere industrielle Anwendungen.
Dieses Maßnahmen- und Inhaltspaket ist in **vier allgemeine Kategorien** gegliedert: in vier allgemeine Kategorien gegliedert.

- General: Diese Kategorie umfasst grundlegende Informationen wie Konzepte, Modelle und Terminologien.
- Policies and Procedures: Diese Kategorie betrifft den Produkteigentümer. Hier wird vor allem ein System zum Management industrieller IT-Sicherheit beschrieben.
- System: Diese Kategorie beschreibt verschiedene verschiedene Vorgaben für Sicherheitsfunktionen von Steuerungs- und Automatisierungssystemen. Die Kernaspekte beruhen auf dem Grundprinzip der „Zones & Conduits“.
- Components and Requirements: Diese Kategorie beschreibt spezifische Anforderungen an die Produktentwicklung und Technologie.

Weitere Informationen

ENISA
Agentur der Europäischen Union für Cybersicherheit

Die Agentur der Europäischen Union für Cybersicherheit (European Union Agency for Cybersecurity (ENISA) hat am 1. September 2005 ihren Betrieb aufgenommen.

Die Agentur arbeitet eng mit den EU-Mitgliedstaaten und anderen Interessengruppen zusammen, um Ratschläge und Lösungen zu liefern und deren Fähigkeiten im Bereich der Cybersicherheit zu verbessern. Sie unterstützt auch die Entwicklung einer kooperativen Reaktion auf groß angelegte grenzüberschreitende Cybersicherheitsvorfälle oder -krisen und arbeitet seit 2019 an Zertifizierungssystemen für Cybersicherheit.

Die ENISA unterstützt die Kommission, die Mitgliedstaaten und folglich auch die Wirtschaft bei der Erfüllung der Anforderungen an die Netz- und Informationssicherheit, einschließlich der derzeitigen und künftigen EU-Rechtsvorschriften. Die ENISA ist letztlich bestrebt, sowohl für die Mitgliedstaaten als auch für die EU-Institutionen als Zentrum für Fachwissen zu dienen und sie in Fragen der Netz- und Informationssicherheit zu beraten.

Das Angebot von Socomec

Für Socomec ist Sicherheit seit jeher ein integraler Bestandteil seiner Produkte, um die Sicherheit der Anlagen oder Installationen zu gewährleisten und ihre Benutzer zu schützen. Die Produkte entwickeln sich weiter, und ihre Technologie wird komplexer, wenn neue Funktionen aus Bereichen wie Elektronik oder IT hinzukommen. Außerdem decken die Funktionen und Merkmale, die unseren Kunden angeboten werden, immer mehr Bereiche ab, da sie nicht mehr nur auf einem einzigen, eigenständigen Produkt basieren, sondern auf kompletten „Ökosystemen". Diese umfassen eine Reihe von Produkten, Kommunikationsnetze und virtuelle Server in der Cloud sowie die damit verbundenen Anwendungen.

Socomec und Cybersicherheit

Wie im vorangegangenen Kapitel erläutert, reicht es nicht aus, nur die Produkte zu sichern: Um ein ausreichendes Sicherheitsniveau zu gewährleisten, muss die gesamte Wertschöpfungskette betrachtet werden.
Die Glieder dieser Kette sind natürlich die Geräte, aber auch die Kommunikationsmittel und die dort zirkulierenden Daten usw.
Vor diesem Hintergrund bietet Socomec **integrierte Lösungen** an, um die Kontrolle über die gesamte Kette und ein ausreichendes Sicherheitsniveau für alle Einzelglieder der Kette zu gewährleisten.
Obwohl viele Tests auf allen Ebenen (Entwicklung, Labor, Integration) durchgeführt werden, ist Sicherheit bei Socomec ein so wesentliches Thema, dass wir **alle unsere Angebote durch externe Stellen validieren** lassen**.**
Die von diesen unabhängigen Stellen gemäß **ISO 27002** ausgestellten Zertifikate garantieren somit die Sicherheit und Homogenität der gesamten Wertschöpfungskette. Das Unternehmen arbeitet in diesem Sinne an empfindlichen Produkten (z.B. Gateways), an den Architekturen, in denen sie installiert werden, aber auch an der Optimierung der Organisation, die das Management des Gesamtsystems ermöglicht.

Schutz der Socomec-Produkte

In einer technischen Architektur sind die empfindlichsten Produkte die **Kommunikationsgateways.**

Warum sind Gateways besonders empfindlich?

Ein Gateway stellt die Verbindungen her, durch die alle Informationen fließen. Diese Informationsdrehscheibe ist deshalb der ideale Angriffspunkt für alle, die Daten löschen oder manipulieren wollen. Darüber hinaus stellen Gateways die erste Verbindung zu Ethernet-Medien dar und ermöglichen einen einfachen Zugriff von außen.
Dies ermöglicht es Hackern, aus der Ferne und diskret auf einem Hochgeschwindigkeitskanal zu operieren und mehrere Hacking-Methoden gleichzeitig zu versuchen.

Wie sind die Socomec-Gateways gesichert?

Sichere Ethernet-Produkte

Die Ethernet-Produkte von Socomec weisen ein erhöhtes Sicherheitsniveau auf und entsprechen der internationalen Norm ISO/IEC 62443-4-2. Diese international für ihre hohen Anforderungen anerkannte Norm gewährleistet eine vollständige Abdeckung der zu behandelnden Sicherheitsbereiche.

Strenge Passwortrichtlinie

Für den Zugriff auf die Profile „Advanced User", „Admin" oder „Cyber Security", mit denen die Konfiguration geändert werden kann, wurde auf dem Webserver eine sehr strenge Passwortrichtlinie eingeführt:
- **Standardpasswörter müssen bei der ersten Anmeldung geändert werden**. Dadurch wird verhindert, dass Unbefugte, die Kenntnis von den Standardpasswörtern erlangen, auf das Konfigurationsmenü zugreifen können.
- **Neue Passwörter müssen bestimmte Kriterien der Komplexität erfüllen** (mindestens 10 Zeichen, darunter Klein- und Großbuchstaben, Zahlen und Sonderzeichen).
- **Passwörter müssen mindestens einmal im Jahr geändert werden**, um weiterhin Zugriff auf das Konfigurationsmenü zu erhalten.
- **Schutz vor versuchtem Identitätsdiebstahl:** Nach drei fehlgeschlagenen Anmeldeversuchen wird der Benutzer für eine Stunde gesperrt. Dies verhindert, dass bösartige Programme auf das System zugreifen können.

Außerdem **werden die Passwörter verschlüsselt**, so dass ein Hacker sie nicht verwenden kann, falls es ihm gelingt, sie abzufangen.

Die Vorteile einer Zusammenarbeit mit Socomec

Integration von Sicherheitsfunktionen bereits bei Konstruktion und Herstellung der Produkte (Zertifizierung nach ISO 27001)

Sichere Ethernet-Produkte gemäß der internationalen Norm ISO/IEC 62443

Regelmäßige Audits der Produkte und ihrer Verwendung in den Zielarchitekturen durch zertifizierte Dritte

Sovereign Cloud von Socomec

Betroffene Produkte

Kommunikationsgateways DIRIS Digiware M-xx

DIRIS Digiware D-xx (ab Version 2.2)

DATALOG H80 (ab Version 2.5)

NetVision-Karte (ab Version 7.2)

Personalisierte Sicherheitsrichtlinien

Cybersecurity-Nutzer können **ihre Sicherheitsrichtlinien an die jeweilige Anwendung anpassen**, um die Anfälligkeit des Gateways/Displays für mögliche Cyberangriffe zu verringern. Dafür stehen folgende Optionen zur Verfügung:

- Deaktivieren des USB- und des RS485-Anschlusses bei Nichtgebrauch,
- Deaktivieren nicht verwendeter Kommunikationsprotokolle (BACnet, SNMP),
- Deaktivieren bestimmter Dienste (Modbus-Skript, um Konfigurationsänderungen zu verhindern).

Verschlüsselte Kommunikationsprotokolle

Gateways und Displays sind mit sicheren Versionen von Kommunikationsprotokollen mit **digitalen SSL/TLS-Zertifikaten** kompatibel. Das Zertifikat hat einen doppelten Zweck: Es verschlüsselt den Datenaustausch zwischen Client und Server und prüft die Identifikation des Remote-Servers durch den Client.

- **HTTPS für das Surfen im Internet**. Die zwischen dem Gateway (Server) und dem Webbrowser (Client) ausgetauschten Skripte werden verschlüsselt. Dies soll verhindern, dass Hacker sie analysieren, interpretieren und schließlich für cyberkriminelle Zwecke wiederverwenden.
- **FTPS** (csv-Export) und **SMTPS** (E-Mail) zum Senden von Daten vom Gateway (Client) an einen Remote-Server.

Firewall

Der Nutzer kann **eine maximale Anzahl von Anfragen pro Sekunde und eine maximale Bitrate in bit/s** festlegen. Wenn ein Angreifer einen dieser Parameter überschreitet, wird er für eine Minute gesperrt.

Weitere Sicherheitsfunktionen

- Sichere Updates (zertifizierte Original-Firmware).
- Sichere Speicherung persönlicher Daten (AES 256-Verschlüsselung).
- Überprüfung der Integrität der Sicherheitsfunktionen beim Start.

Unser allgemeines Ziel ist es, unseren Kunden ein System zur Verfügung zu stellen, das Cyberangriffen so wenig wie möglich ausgesetzt ist. Außerdem wollen wir sicherzustellen, dass die Konfiguration, Hierarchie und die historischen Daten von Gateways im Falle eines Cyberangriffs nicht verloren gehen.

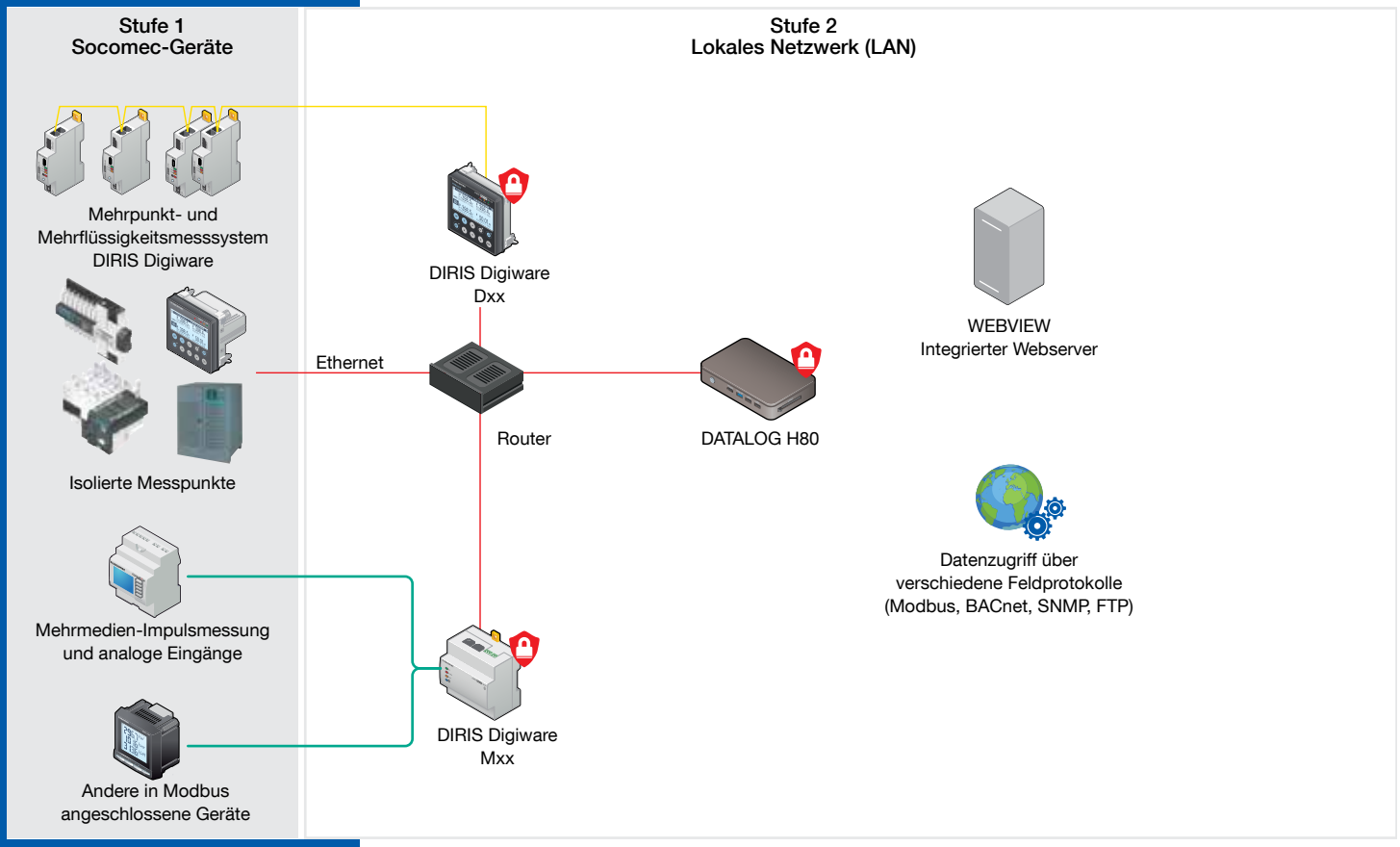
Schutz von Architekturen

Die unten dargestellten Referenzarchitekturen decken die häufigsten Anwendungsfälle ab. Unsere Produkte sind so konzipiert, dass sie die entsprechenden Anforderungen erfüllen und sich nahtlos in diese Umgebung integrieren lassen. Unsere Tests und Qualifizierungsprüfungen bestätigen diese Kompatibilität und die Widerstandsfähigkeit der Installation bei Angriffsversuchen.

Lokaler Zugang

Funktionsprinzip

Diese Installation ermöglicht die lokale und zentrale Überwachung von Produktdaten. Die Daten werden über lokale Displays oder eine WEBVIEW-Anwendung angezeigt, die in den Kommunikationsgateways DIRIS Digiware M, Displays DIRIS Digiware D, dem Datenlogger DATALOG H80 oder den Multifunktionsmessgeräten DIRIS A-40 eingebettet ist.
Je höher ein Gerät in der Hierarchie angesiedelt ist, desto umfangreicher kann es alle mit ihm verbundenen Produkte überwachen.



Empfehlungen

- Isolieren Sie Messgeräte in einem eigenen Netzwerk (separate Netzwerkgeräte oder spezielles VLAN).
- Deaktivieren Sie nicht genutzte Funktionen.
- Ändern Sie Standardpasswörter.
- Ändern Sie Passwörter regelmäßig.

Integration von Sicherheitsfunktionen und Prüfung durch unabhängige, zertifizierte Cybersicherheits-spezialisten.

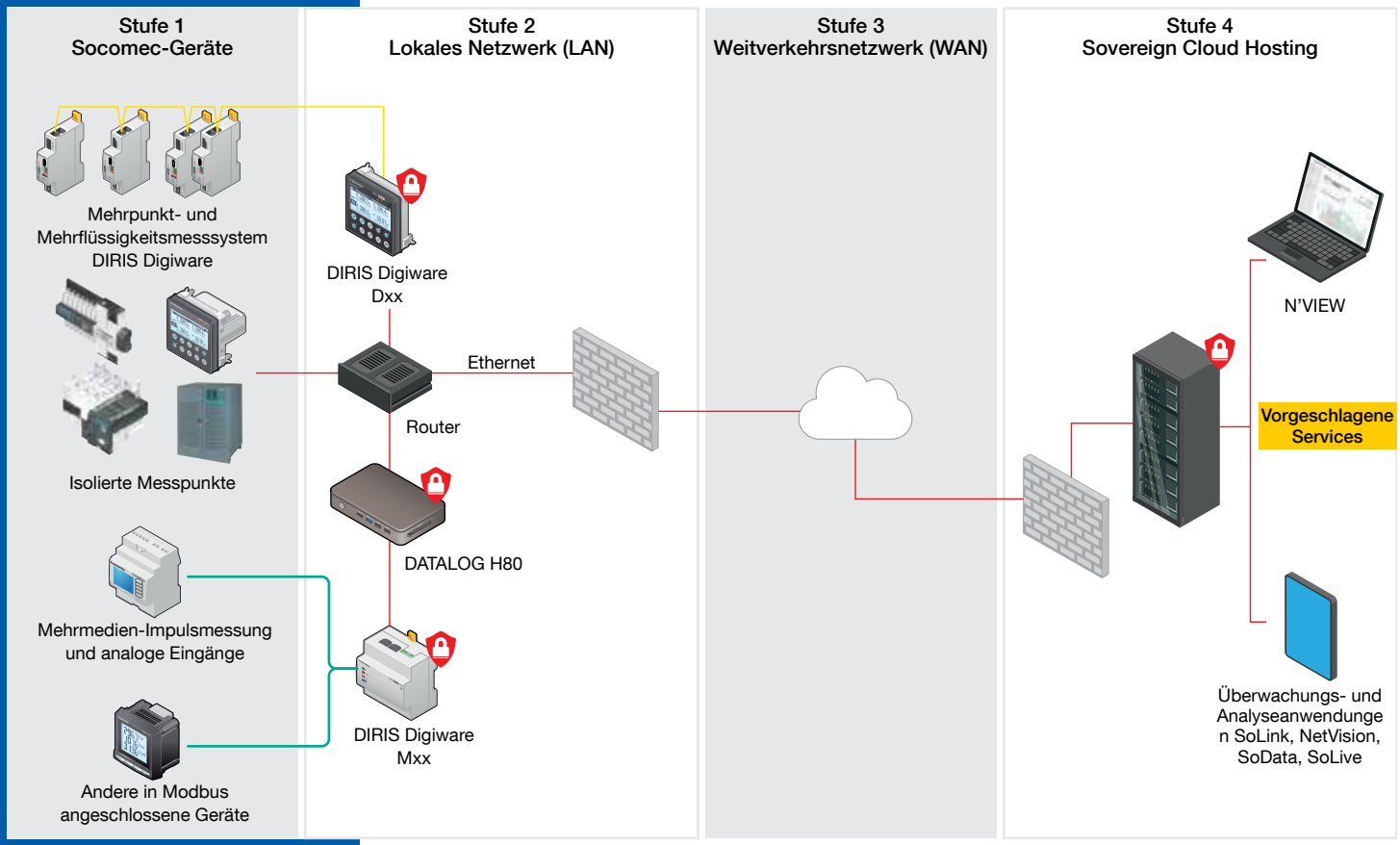
Das Angebot von Socomec

- Eine strenge Passwortrichtlinie.
- Zugang zu passwortgeschützten Produkten mit Passwörtern, die nur von autorisierten Personen geändert werden können.
- Kontrolle der Sicherheitsfunktionen über eine geschützte Website, auf die nur autorisierte Personen Zugriff haben.

Cloud

Funktionsprinzip

Dieser Anwendungsfall bietet die Möglichkeit, Unternehmensdaten (ein oder mehrere Standorte) über das Internet zu überwachen.
Dazu werden die von den Produkten gemessenen lokalen Daten zentral und sicher in die Cloud ins Internet zurückgespielt. Dedizierte und sichere Cloud-Anwendungen nutzen diese Daten dann, um Informationen über die Installation bereitzustellen.
Die Daten werden über verschlüsselte Protokolle (FTP, HTTP, MQTT) sicher außerhalb des Unternehmens versendet.



Empfehlungen

- Erlauben Sie den Fernzugriff auf das Gerät nur über authentifizierte Verbindungen (VPN auf der Firewall zwischen dem Gerät und dem Internet).
- Filtern Sie die Quell-IP-Adressen, die über den Internet-Router Zugang zum Gerät haben.
- Aktivieren Sie die Datenlogger-Funktion (Daten pushen/Daten auf einen entfernten Server exportieren) auf dem Gerät (Mxx, Dxx, Datalog H8x), um die Rückmeldung von Daten an die Cloud zu ermöglichen.
- Öffnen Sie die Proxy/FW-Ports Ihres Unternehmens entsprechend dem gewählten Protokoll (HTTPS: TCP 8080; FTPS: TCP 990...), dies wird in der Regel von der IT-Abteilung verwaltet.

Das Angebot von Socomec

- Zugang zu passwortgeschützten Produkten mit Passwörtern, die nur von autorisierten Personen geändert werden können.
- Kontrolle der Sicherheitsfunktionen über eine geschützte Website, auf die nur autorisierte Personen Zugriff haben.
- Sovereign Cloud von Socomec zertifiziert nach ISO 27001 und HDS: Datenspeicherung in der Zone Frankreich, Sicherheit und Datenkontrolle, Skalierbarkeit.
- Sicherheit für die gesamte Kette mit Zertifizierung durch eine unabhängige externe Organisation, die auf Cybersicherheit spezialisiert ist.
- Dedizierte Anwendungen für die Cloud-Nutzung (Robustheit, Skalierbarkeit, Lastbeständigkeit, Schutz für diese Art von Umgebung usw.).

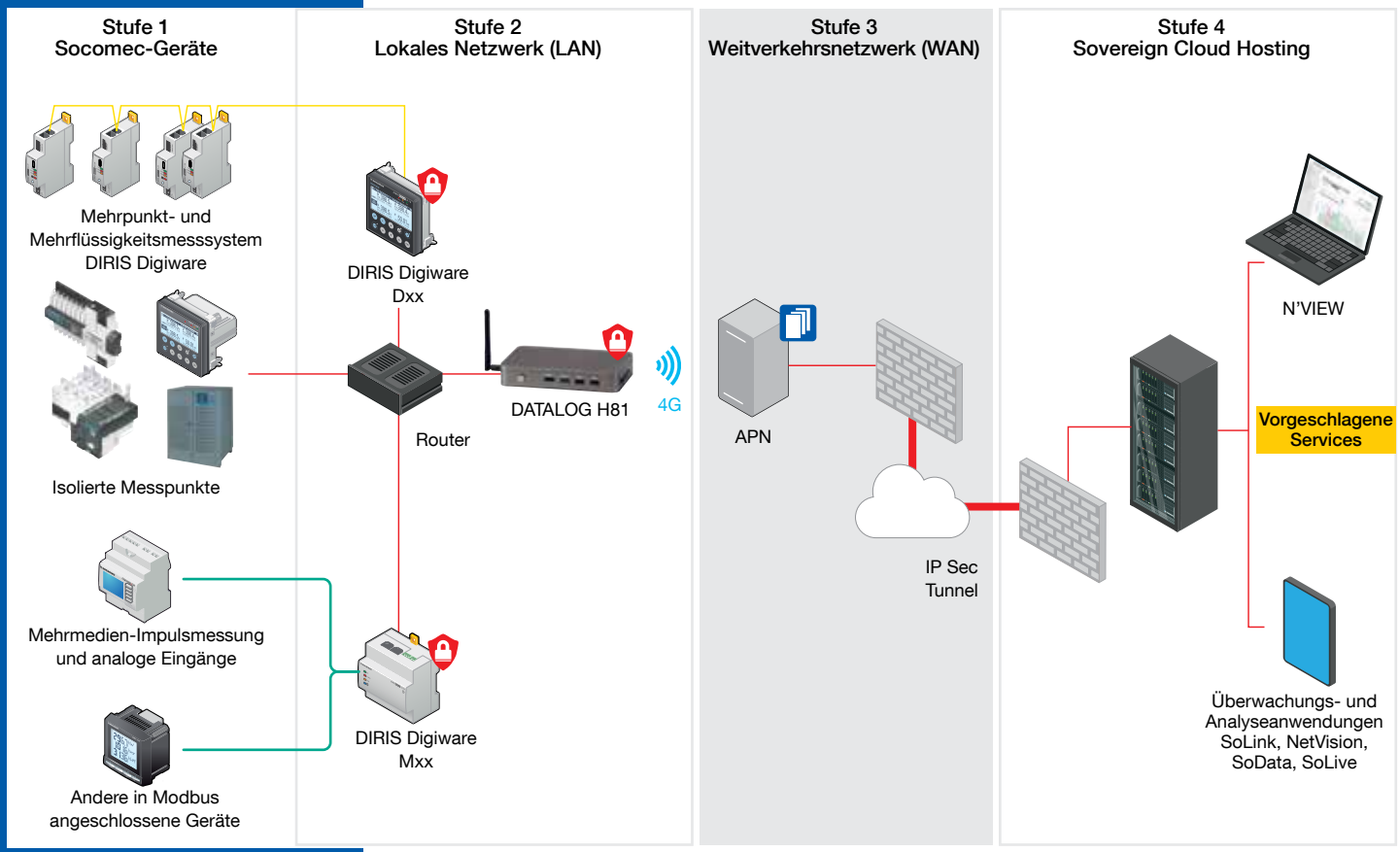
Funkübertragung

Funktionsprinzip

Zu wenig oder keine Infrastruktur? Dann hilft die drahtlose Übertragung!
Die Nutzung von Mobilfunknetzen ermöglicht es, vor Ort bestehende Beschränkungen (IT-Zwänge, starre oder nicht vorhandene Infrastrukturen usw.) zu überwinden.

4G-Architektur

Die drahtlose Verbindung wird über ein von Socomec bereitgestelltes Gateway (H81) in Verbindung mit einem Mobilfunkvertrag (4G) hergestellt.
Die Sicherheit der Datenströme und ihrer Speicherung wird durch unsere in Frankreich gehosteten Einrichtungen (Sovereign Cloud) gewährleistet.



Empfehlungen

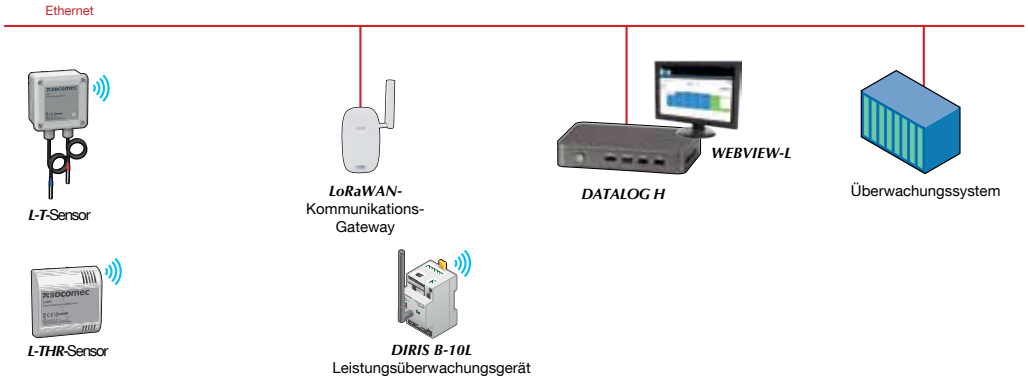
- Isolieren Sie Messgeräte in einem eigenen Netzwerk (separate Netzwerkgeräte oder spezielles VLAN).
- Aktivieren Sie nur tatsächlich erforderliche Dienste.

Das Angebot von Socomec

- 4G-Zugang weltweit dank der von Socomec bereitgestellten eSim.
- Vereinfachte Konfiguration für eine schnelle und sichere Installation.
- Sovereign Cloud von Socomec: Datenspeicherung in der Zone Frankreich, Sicherheit und Datenkontrolle, Skalierbarkeit.
- Dedizierte Anwendungen für die Cloud-Nutzung (Robustheit, Skalierbarkeit, Lastbeständigkeit, Schutz für diese Art von Umgebung usw.).

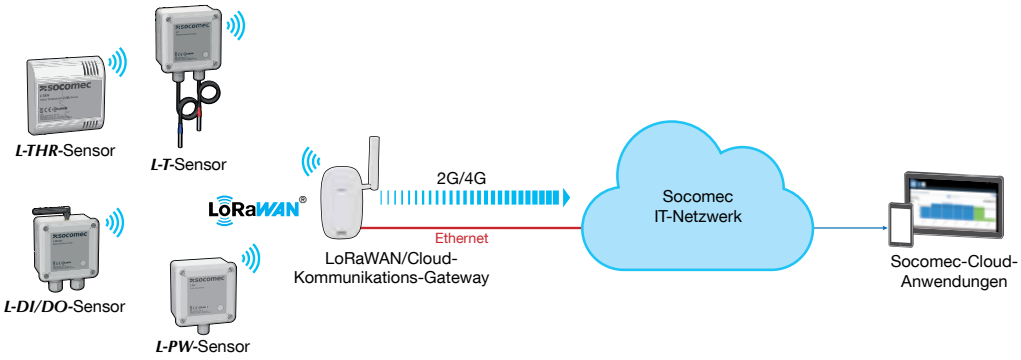
Lokale Architektur

Privates Netz mit lokaler Verarbeitung der Messdaten.



Cloud-Architektur

Privates Netzwerk mit Messdatenübertragung an eine Cloud-Plattform.



Schutz durch Organisation

Socomec hat beschlossen, den Datenschutz, die Integrität und die Verfügbarkeit von Informationen schon bei der Entwicklung eines neuen Produkts/einer neuen Dienstleistung noch umfangreicher als bisher auszubauen.
Dies ermöglicht die Kontrolle über die Verbreitung von Informationen und gewährleistet, dass diese nicht zur Verfälschung eines Produkts während der Entwicklung verwendet werden können.

ISO/IEC 27001 ist eine internationale Norm für die Sicherheit von Informationssystemen.
Sie gilt für alle Arten von Organisationen (Unternehmen, Nichtregierungsorganisationen, Regierungsbehörden usw.) und legt die Anforderungen für die Einführung eines Managementsystems für die Informationssicherheit (ISMS) fest.

Das ISMS definiert die Sicherheitsmaßnahmen für bestimmte Umgebungen, um den Schutz der Vermögenswerte der Organisation zu gewährleisten. Ziel ist es, Funktionen und Informationen vor Verlust, Diebstahl und Manipulation sowie IT-Systeme vor Eindringlingen und Großschäden zu schützen. Dies schafft zusätzliches Vertrauen bei den Beteiligten.

Um unseren Kunden diese Sicherheit bieten zu können, ist unsere Organisation nach ISO 27001 für die IoT-Umgebung zertifiziert.

Entdecken Sie unsere ISO-Zertifikate.

Glossar

APN

Access Point Name oder APN, auch Netzzugangspunkt-Kennung genannt, ist eine Kennung, die es einem Mobiltelefonbenutzer eines 2G- oder 4G-Netzzugangspunkts ermöglicht, sich mit dem Internet zu verbinden, indem er den zu verwendenden Gateway GPRS Support Node (GGSN für 2G) oder den Packet Data Network Gateway (PGW für 4G) identifiziert. Der APN besteht in der Regel aus einer alphanumerischen Kennung sowie MCC- und MNC-Codes zur Identifizierung des Mobilfunknetzbetreibers. Das Telefon selbst ergänzt die alphanumerische Kennung mit dem MCC- und MNC-Code, den es aus der IMSI der SIM-Karte des Telefons ableitet.

Architektur-Audit

Eine Studie über die Übereinstimmung eines Informationssystems mit den Anforderungen des Unternehmensumfelds.

Cloud

Der Prozess der Nutzung von IT-Servern aus der Ferne über das Internet. In der Cloud können Unternehmen ihre Daten auf externen Servern speichern und aus der Ferne darauf zugreifen. Es gibt 3 Arten von Clouds: Public Cloud, Private Cloud und Hybrid Cloud. Im Laufe der Jahre hat sich die Cloud zu einem unverzichtbaren Instrument für alle Unternehmen entwickelt, die sich weiterentwickeln und wettbewerbsfähig bleiben wollen.

Sovereign Cloud

Laut einem Rundschreiben des französischen Innen- und des Kulturministeriums vom April 2016 ist die Sovereign Cloud „ein Bereitstellungsmodell, bei dem das Hosting und die gesamte von einem Cloud-Dienst durchgeführte Datenverarbeitung physisch innerhalb der Grenzen des Staatsgebiets von einer Einrichtung durchgeführt werden, die nach französischem Recht und in Übereinstimmung mit den französischen Gesetzen und Normen tätig ist“. Mit anderen Worten, die Sovereign Cloud ist ein ergänzendes Konzept zu einem Datenspeicherdienst, das darauf abzielt, die gehosteten Daten so weit wie nach französischem Recht möglich zu schützen. Die wichtigsten Merkmale dieser Cloud sind, dass sie von einem französischen Dienstleister gehostet und verwaltet wird, der nicht mit einem ausländischen Unternehmen verbunden ist, dessen Infrastruktur sich in Frankreich befindet und der die dort geltenden Gesetze und Normen einhält. Diese Zertifizierung garantiert also, dass die gespeicherten Daten der Kontrolle durch die französischen Behörden unterliegen und dass die Hosts den Gesetzen Frankreichs entsprechen.

Network Core

Der Network Core gilt als das Herzstück des IT-Netzes. Konkreter ausgedrückt: Wenn Informationen von Standort A an Standort B gesendet werden, werden diese von Standort A gesendeten Informationen vom Network Core empfangen und dann an Standort B übertragen. Der Network Core ist also der Konzentrations- und Verteilungspunkt für Informationen. In der Praxis besteht dieser Network Core aus einem Switch, auch Netzwerkswitch genannt, und einem elektrischen Schutz.

Cybersicherheit

Alle Gesetze, Richtlinien, Tools, Systeme, Sicherheitskonzepte und -mechanismen, Risikomanagementmethoden, Maßnahmen, Schulungen, bewährten Praktiken und Technologien, die zum Schutz von Personen und der materiellen und immateriellen IT Vermögenswerte (ob direkt oder indirekt an ein Netz angeschlossen) von Staaten und Organisationen eingesetzt werden können (mit dem Ziel der Sicherstellung der Verfügbarkeit, Integrität und Authentizität, Vertraulichkeit, Nachweisbarkeit und Nichtabstreitbarkeit).

Cyber-Resilienz

Die Fähigkeit, sich auf ständig wechselnde Bedingungen vorzubereiten und sich an diese anzupassen und die eigenen Fähigkeiten nach vorsätzlichen Angriffen, Unfällen, Naturkatastrophen oder Zwischenfällen bei der Nutzung von IT- und Kommunikationsressourcen schnell wiederherzustellen. (Quelle: http://www.ab-consulting.fr/blog/non-classified/cyber-securite-vs-cyber-resilience).

Cyberkriminalität

Umfasst Straftaten, die an einem oder über ein Computersystem begangen werden, das in der Regel an ein Netzwerk angeschlossen ist.

Edge

Edge Computing (oder Network Edge Computing) ist eine Optimierungsmethode im Cloud Computing, bei der Daten am Rande des Netzes, in der Nähe der Datenquelle, verarbeitet werden. Durch diese Nähe kann bei der Analyse der Daten die zwischen Sensoren und Datenverarbeitungszentren erforderliche Bandbreite minimiert werden. Bei diesem Ansatz werden möglicherweise Ressourcen genutzt, die nicht ständig mit einem Netzwerk verbunden sind wie Laptops, Smartphones, Tablets oder Sensoren. Mit Edge Computing lässt sich auch die Übertragung umfangreicher und irrelevanter Daten an Datenzentren oder die Cloud vermeiden, was die Fluidität und Reaktionszeit verbessert.

Industrie 4.0

Das Konzept der Industrie 4.0 oder der Industrie der Zukunft bezieht sich auf eine neue Art der Organisation der Produktionsmittel. Dieses neue Industriemodell etabliert sich als Konvergenz der virtuellen Welt, der digitalen Produktgestaltung und des digitalen Managements (Betrieb, Finanzen und Marketing) mit Produkten und Objekten der realen Welt. Die großen Versprechungen dieser vierten industriellen Revolution sind die Möglichkeit, Verbraucher mit einzigartigen und personalisierten Produkten anzulocken und trotz geringer Produktionsmengen Gewinne zu erzielen.

IoT

IoT ist die Kurzbezeichnung für das „Internet der Dinge“ oder das „Internet der vernetzten Dinge“. Die Kurzbezeichnung IoT bezieht sich im Allgemeinen auf das Ökosystem der vernetzten Objekte, einschließlich des Marktes für diese Objekte, aber auch auf alle Geschäfts- und Marketingmodelle, die sich aus ihrer Entwicklung ergeben.

Local Area Network (LAN)

Kommunikationssystem für den Anschluss von einigen hundert Computern und Peripheriegeräten in einem Umkreis von wenigen Kilometern. Das in den 1970er Jahren entstandene Lokale Netzwerk erfuhr mit der Entwicklung von Mikrocomputern in den 1980er Jahren und der Einführung des Ethernet-Kommunikationsstandards ein beträchtliches Wachstum. Im Gegensatz dazu kann das Wide Area Network (WAN) Tausende von Computern zusammenbringen, die Hunderte oder sogar Tausende von Kilometern voneinander entfernt sind.

LoRaWAN

LoRaWAN ist ein Funkkommunikationsprotokoll, das auf der LoRa-Technologie basiert.
Im Zusammenhang mit dem Internet der Dinge ermöglicht es die Organisation eines Niedrigenergieweitverkehrnetzes (Low Power Wide Area Network (LPWAN)), in das Endgeräte mit geringem Stromverbrauch über Gateways eingebunden werden.
(Quelle: Wikipedia).

Firewall

Eine Lösung zum Schutz eines oder mehrerer an ein Netz angeschlossener Rechner vor Angriffen von außen (eingehende Filterung) und zum Blockieren unzulässiger Verbindungen nach außen (ausgehende Filterung), die von Programmen oder Personen initiiert werden (Quelle: ANSSI).

Gateway

System zur Verbindung zweier Computernetze unterschiedlicher Art, z. B. eines lokalen Netzes und des Internets. Meistens dienen Gateways auch als Firewall und Proxy sowie zur Umsetzung von dienstbezogenen Richtlinien usw. (Quelle: Wikipedia).

Sicherheit von Informationssystemen (SIS)

Alle technischen, organisatorischen, rechtlichen und personellen Mittel, die eingesetzt werden, um die unbefugte Nutzung, den Missbrauch, die Manipulation oder die Unterschlagung eines Informationssystems zu verhindern.

Security by Design

Eine Methode zur Vorhersage der Sicherheit eines Produkts (oder Systems) zum Zeitpunkt seiner Auslegung oder Konstruktion, wobei davon ausgegangen wird, dass es im Laufe seines normalen Betriebs zwangsläufig einer Reihe potenzieller oder tatsächlicher Bedrohungen ausgesetzt sein wird.

Virtuelles Privates Netzwerk (VPN)

Ein System zur Herstellung einer direkten Verbindung zwischen entfernten Rechnern durch die Trennung des spezifischen Datenverkehrs vom übrigen Informationssystem. Die Verwendung eines VPN wird dringend empfohlen, wenn Unternehmensressourcen von außerhalb genutzt werden sollen.

Wide Area Network (WAN)

Eine Art von Telekommunikationsnetz (oder IT-Netz), das ein sehr großes geografisches Gebiet abdecken kann, z. B. die Fläche eines oder mehrerer Länder oder sogar den gesamten Planeten. Der Betrieb eines WAN basiert auf der Punkt-zu-Punkt-Verbindungstechnik, bei der eine Verbindung zwischen einem Telekommunikationsbetreiber (Free, SFR oder Bouygues Telecom für Frankreich) und dem Netz eines Kunden über eine Mietleitung (Kupferleitungen wie bei der herkömmlichen Telefonie oder Glasfaser) hergestellt wird.

Socomec: Unsere Innovationen im Dienste Ihrer Energieleistung

1 unabhängiger Hersteller

4.200 Mitarbeiter weltweit

8 % der Umsätze für Forschung und Entwicklung

400 Experten für Serviceleistungen

Ihr Experte für Leistungsmanagement

SCHALTGERÄTE

MESSEN UND ZÄHLEN

STROMWANDLUNG

ENERGIESPEICHERLÖSUNG

QUALIFIZIERTE DIENSTLEISTUNGEN

Ihr Spezialist für kritische Anwendungen

- Regelung und Überwachung von Niederspannungsanlagen
- Sicherheit von Personen und Eigentum
- Messung von elektrischen Parametern
- Energiemanagement
- Energiequalität
- Energieverfügbarkeit
- Energiespeicherung
- Prävention und Reparaturen
- Messung und Analyse
- Optimierungen
- Beratung, Inbetriebnahme und Schulung

Weltweite Präsenz

12 Produktionsstandorte
- Frankreich (3x)
- Italien (2x)
- Tunesien
- Indien
- China (2x)
- USA (2x)
- Kanada

30 Niederlassungen und Handelsstandorte
- Algerien • Australien • Belgien • China • Deutschland
- Dubai (Vereinigte Arabische Emirate) • Elfenbeinküste
- Frankreich • Indien • Indonesien • Italien • Kanada
- Malaysia • Niederlande • Österreich • Polen • Portugal
- Rumänien • Schweden • Schweiz • Serbien • Singapur
- Slovenien • Spanien • Südafrika • Thailand • Tunesien
- Türkei • USA • Vereinigtes Königreich

80 Länder
in denen unsere Marke vertreten ist

SOCOMEC GmbH
Deutschland
Erzbergerstraße 10
68165 Mannheim
Tel.: +49 621 716840
Fax: +49 621 71684-44
info.de@socomec.com

SOCOMEC SOLUTIONS GmbH
Österreich
Kolpingstraße 14
1230 Wien
Tel.: +43 1 6152560
Fax: +43 1 6152560-80
office.at@socomec.com

IHR HÄNDLER / PARTNER

www.socomec.de

100 years OF SHARED ENERGY

socomec Innovative Power Solutions

DOT 01031 01 de - 09 / 24 - Photo: Martin Bernhart – Erstellt von: Socomec – Gyss Imprimeur Obernai