WHITEPAPER

Cybersecurity in der Milch- und Softdrinkindustrie

Risikominimierung nach KRITIS
siemens.de/industrialsecurity

SIEMENS

Mit der zunehmenden Digitalisierung von Unternehmen und der damit einhergehenden Vernetzung praktisch aller Bereiche werden große ökonomische Potenziale eröffnet. Schon heute sind über 20 Milliarden Geräte und Maschinen über das Internet vernetzt – bis 2030 werden es rund eine halbe Billion sein.
Digitalisierung und Vernetzung können ein Motor für Wachstum und Wohlstand sein. Gleichzeitig entstehen durch die zunehmende Vernetzung aber auch neue Gefährdungslagen, auf die schnell und konsequent reagiert werden muss.

Das betrifft auch die Unternehmen der Nahrungsmittel- und Getränkeindustrie
2017 wurde einer der großen Lebensmittelkonzerne Opfer eines so genannten Ransomware-Trojaners. Die Malware-Variante »Petya« befiel damals Computersysteme in aller Welt und sperrte ihre Benutzer aus – um ein Lösegeld zu erpressen.

Nach eigenen Angaben entgingen dem Unternehmen durch die Cyberattacke Umsätze in Höhe von rund 140 Millionen US-Dollar. Es dauerte mehrere Tage, bis die wichtigsten Systeme wieder einsatzfähig waren, und ein paar Wochen für die restlichen Systeme.

Dieser und ähnliche Vorfälle in den vergangenen Jahren haben die Gesetzgeber zahlreicher Staaten dazu veranlasst, entsprechende Vorschriften und Regelungen für Cybersecurity zu erlassen. Durch diese Vorgaben sollen kritische Infrastrukturen geschützt werden, um die Versorgungssicherheit der Bürger und die Stabilität des Landes zu gewährleisten.

In Deutschland beispielsweise ist im Juli 2015 das Gesetz zur »Erhöhung der Sicherheit informationstechnischer Systeme« (IT-Sicherheitsgesetz) in Kraft getreten, das Betreiber kritischer Infrastrukturen (KRITIS) zu bestimmten Maßnahmen verpflichtet. Zu den Betreibern kritischer Infrastrukturen gehören auch Unternehmen im Sektor Ernährung. Cyberangriffe können hier nicht nur die Produktion stören und wirtschaftliche Schäden zur Folge haben, sondern auch gesundheitliche Risiken bedeuten.

Oberstes Ziel ist die Vermeidung von Produktionsfehlern und Produktionsmanipulation und somit insbesondere die Vermeidung von Reputationsverlust. Entsprechende Schutzmaßnahmen sind kein Luxus, sondern Pflicht.

Inhaltsverzeichnis

Gesetzgeber schreiben weltweit IT-Sicherheit vor

In Deutschland schreibt seit Juli 2015 das IT-Sicherheitsgesetz für bestimmte kritische Infrastrukturen eine Meldepflicht für sicherheitsrelevante Vorfälle vor. Zeitlich versetzt kommt für die KRITIS-Betreiber die Einhaltung von Mindeststandards bei Cybersecurity hinzu. Die Umsetzung der Standards basiert insbesondere auf der IEC 27001 und der IEC 62443. Sowohl die Hersteller von Automatisierungsund Netzwerkkomponenten als auch die Anlagenbetreiber haben sich bei den Maßnahmen für Cybersecurity an den aktuellen Stand der Technik zu halten. Der juristische Begriff »Stand der Technik« wird verwendet, weil die technische Entwicklung erfahrungsgemäß schneller ist als die Gesetzgebung. Was zu einem bestimmten Zeitpunkt Stand der Technik ist, lässt sich anhand existierender nationaler oder internationaler Standards und Normen wie beispielsweise DIN oder IEC bzw. anhand erfolgreich in der Praxis erprobter Vorbilder – so genannter Best Practices – für den jeweiligen Bereich ermitteln.

Stand der Technik laut IEC 62443

Die Dokumente der IEC 62443 sind wie folgt aufgeteilt:

- IEC 62443-1 umfasst Terminologien, Konzepte, Anwendungsfälle und Modelle
- IEC 62443-2 richtet sich an Anlagenbetreiber; es beschreibt die Umsetzung eines Security Management System, Patch Management etc.
- IEC 62443-3 beschreibt Sicherheitstechnologien für Steuerungen und Netzwerkkomponenten
- IEC 62443-4 richtet sich an die Hersteller und formuliert, wie z. B. der Entwicklungsprozess sicherzustellen ist

Bereits diese Aufteilung zeigt, dass Cybersecurity ein umfassender Prozess ist und Sicherheitsstandards schon in der Entwicklung der Komponenten einzuhalten sind.

Ähnliche Vorgaben umfasst der FDA Food Safety Modernization Act (FSMA), der in den USA unter anderem auf eine Kombination aus Überwachung, Eingriffsmöglichkeiten und Überprüfung von Cybersecurity-Maßnahmen setzt. In Großbritannien regelt der PAS 96:2017 die Schutz- und Abwehrmaßnahmen gegen Angriffe auf die Nahrungsmittel-und Getränkeindustrie.

Im Kern haben alle Gesetze und Vorgaben gemeinsam, dass sie auf eine Mischung aus technischen Standards und Meldepflichten bei Vorfällen setzen sowie die Einhaltung der Vorgaben überwachen.

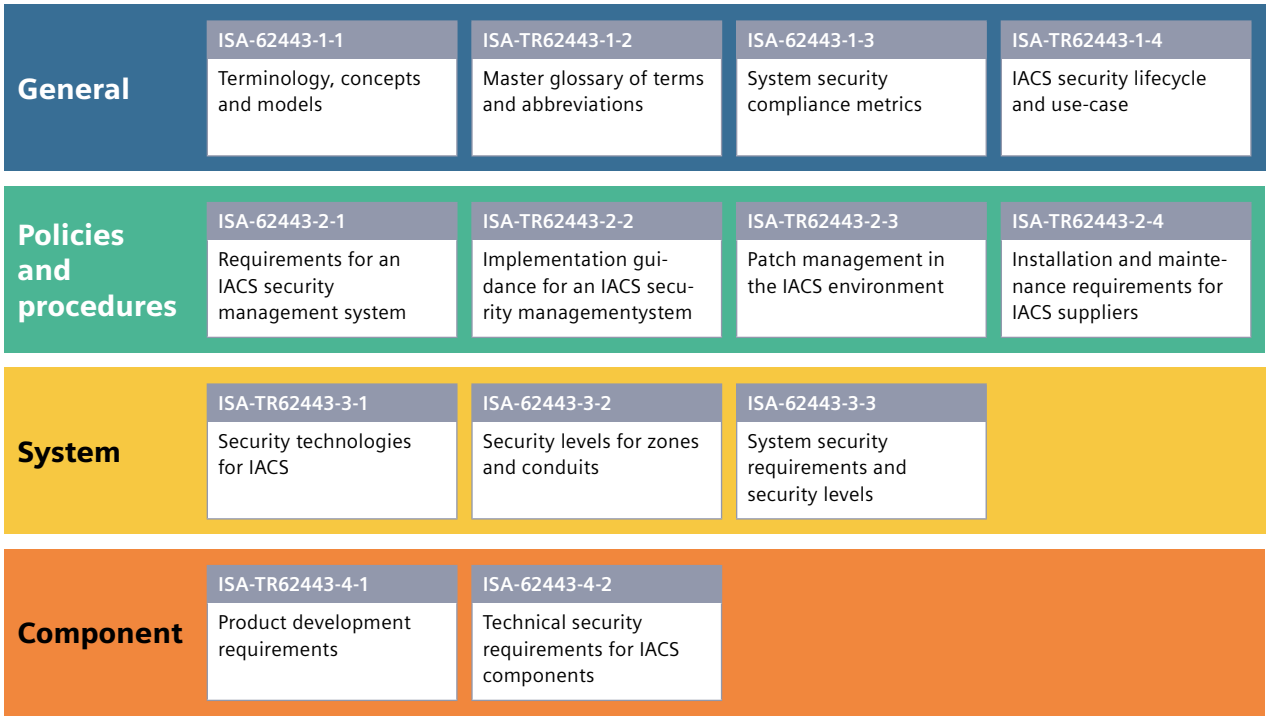

Abbildung 1: Dokumente der Norm IEC 62443

Cybersecurity – ein fortlaufender Prozess

Der effektive Schutz gegen Cyberangriffe wird nicht durch eine einmalige Umsetzung von Maßnahmen erreicht, sondern durch einen fortlaufenden Prozess.

Im Anschluss an eine Bewertung der Risiken (Assessment) für den automatisierten Prozess müssen Maßnahmen umgesetzt werden (Implementation), um diese Risiken zu minimieren. Diese Maßnahmen müssen überwacht werden und es muss kontinuierlich geprüft werden, ob aufgrund einer geänderten Gefährdungslage eine Überarbeitung der Maßnahmen erforderlich ist (Management). Die nötigen Maßnahmen sind dabei so unterschiedlich wie die Bewertung der Risiken. Abhängig vom Automatisierungsgrad, von der verwendeten Technologie und der Vernetzung von OT (Operational Technologies) und IT (Informationstechnik) erstellen Security-Experten geeignete Schutzmechanismen, die auf das jeweilige Unternehmen und seine Prozesse abgestimmt sind.

Die Verantwortung für IT-Sicherheit liegt stets beim Anlagenbetreiber. Auch wenn Teile des Betriebs oder der komplette Betrieb durch Outsourcing nicht mehr von eigenem Personal betreut werden, steht der Anlagenbetreiber in der Verantwortung. Gefährdungen durch das Outsourcing sind dann zusätzlich zu bewerten. Generell sind Schulungen des Personals empfehlenswert, um das Bewusstsein für Cyberangriffe zu schärfen und im Notfall schnell und zielgerichtet reagieren zu können.

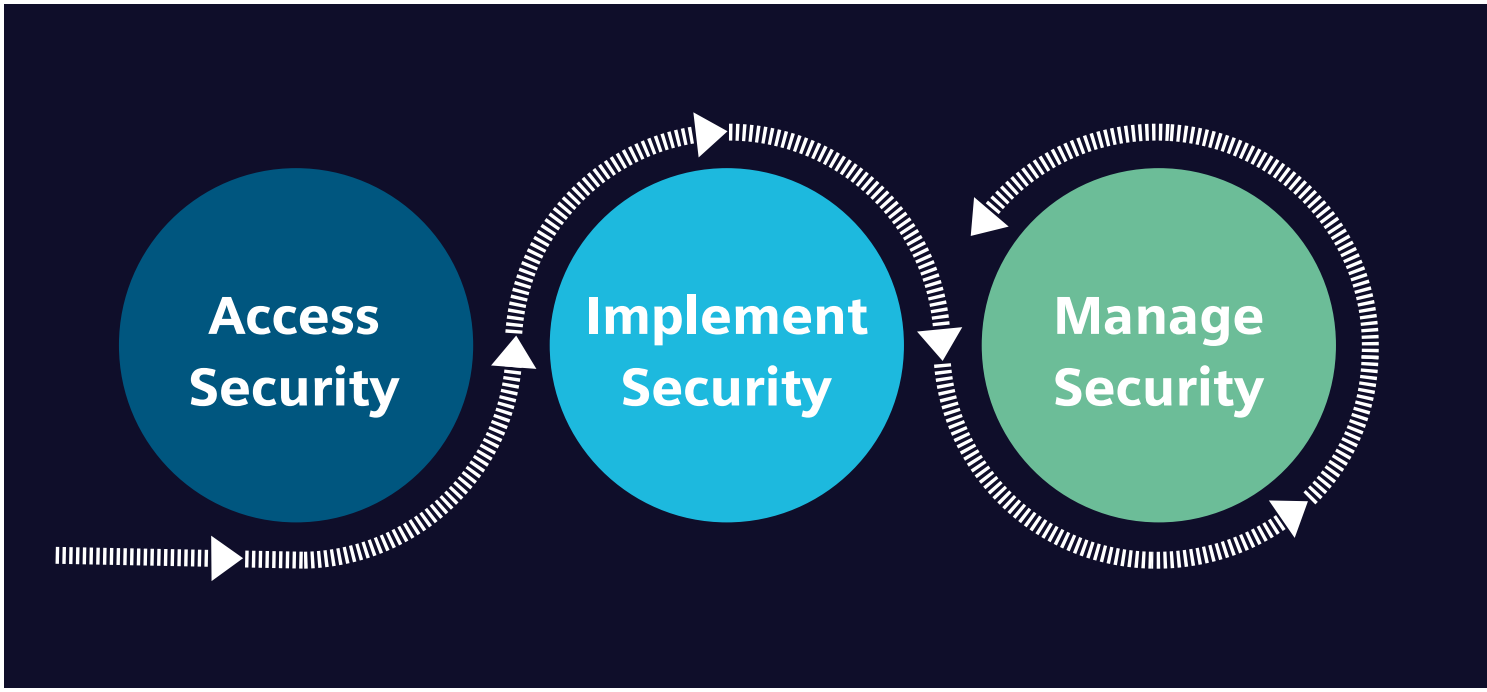

Abbildung 2: Die drei Phasen der IT/OT-Sicherheit oder industriellen Sicherheit

Bedrohungen – Ziele der Angriffe und Arten von Angreifern

Welches Interesse verfolgen Angreifer, die versuchen, die Sicherheitsmaßnahmen zu überwinden? Sie lassen sich in vier Typen unterteilen.

Ungebildete Angreifer (»Script Kiddies«) nutzen fertige Skripte aus dem Internet, um aus Spielerei mit einfachen Mitteln bekannte Schwachstellen anzugreifen.

Gebildete Angreifer (»Hacker«) wollen durch ihre komplexeren Attacken Vorteile für sich erzielen und zum Beispiel Lösegeld für verschlüsselte Daten erpressen.

Betriebsspionage wird meist von Insidern ausgeführt, die ihr spezielles Wissen nutzen, um Daten zu stehlen oder dem Unternehmen zu schaden – hierbei gehen (ehemalige) Mitarbeiter gezielt gegen ein bestimmtes Unternehmen vor.

Technisch sind **staatlich getriebene Attacken** am gefährlichsten. Diese Attacken nutzen in der Regel zuvor unbekannte Schwachstellen, und die Ziele sind vielfältig: Zugriff auf sensible Daten, Datenmanipulation, Störung der Fertigungsprozesse oder sogar die Zerstörung ganzer Anlagenteile. Die Motivation dahinter kann neben wirtschaftlichen Interessen auch die Destabilisierung eines Staates sein – z. B. durch Angriffe auf die Versorgung mit Lebensmitteln.

Gefährdungen

Folgende Arten von Angriffen wurden vom deutschen Bundesamt für Sicherheit in der Informationstechnik (BSI) als die zehn häufigsten Angriffe auf industrielle Anlagen identifiziert (Stand: BSI-CS 029 | Version 2.0 vom 11.07.2018):

1. Unberechtigte Nutzung von Fernwartungszugängen, die Industrial Control Systems (ICS) für den Zugriff von außen öffnen, aber oft nicht ausreichend geschützt sind.
2. Online-Angriffe über die Office-IT, die in der Regel mit dem Internet verbunden ist und auch eine Verbindung ins ICS-Netz herstellen kann.
3. Angriffe auf verwendete Standardkomponenten wie Betriebssysteme, Application-Server oder Datenbanken, die oft Fehler oder Schwachstellen enthalten können, die Angreifer ausnutzen. Solche Komponenten können auch in ICS-Systemen eingesetzt werden und so das Risiko erhöhen.
4. (D)DoS-Angriffe auf Netzwerkverbindungen können Systeme überlasten und so die Funktionsfähigkeit des ICS-Netzes oder das ICS selbst beeinträchtigen.
5. Menschliches Fehlverhalten und Sabotage von internen oder externen Tätern stellen eine große Gefahr dar. Fahrlässigkeit und menschliches Versagen bedrohen auch Vertraulichkeit und Verfügbarkeit.
6. Das Einschleusen von Malware geschieht häufig über Wechseldatenträger oder mobile IT-Komponenten von externen Mitarbeitern (Beispiel: Stuxnet).
7. Das Mitlesen und Einspielen von Steuerbefehlen ist einfach möglich, da die meisten Steuerungskomponenten über Klartextprotokolle und daher ungeschützt kommunizieren.
8. Der unberechtigte Zugriff auf Netzwerkkomponenten wird möglich, wenn Innentäter – oder nach Durchbrechen der Schutzmaßnahmen auch Externe – nicht durch sichere Methoden zur Authentifizierung und Autorisierung der Komponenten abgefangen werden können.
9. Angreifer können Netzwerkkomponenten manipulieren, um Man-in-the-Middle-Angriffe durchzuführen oder Sniffing zu erleichtern.
10. Ausfälle durch extreme Umwelteinflüsse oder technische Defekte sind nie völlig auszuschließen, mit entsprechenden Komponenten und Schutzmaßnahmen lassen sich aber Risiko und Folgeschäden minimieren.

Cybersecurity – Vorgehensweise in mehreren Schritten

Die Liste der Gefährdungen zeigt, dass Angriffe sehr unterschiedlich erfolgen können. Der Prozess muss gegen diese Vielfalt an Bedrohungen geschützt werden. Für die Umsetzung von Cybersecurity definieren der deutsche Branchenstandard wie auch die IEC 62443 einen mehrschrittigen Prozess.

1. Die Objektauswahl erfasst und dokumentiert alle Systeme der Anlage, inklusive der Subsysteme und eines Netzplans.
2. Aus der Anwendungsfallauswahl ergeben sich die Gefährdungen, zum Beispiel, dass auf ein System per Fernwartungszugang zugegriffen wird.
3. Die Gefährdungsbestimmung legt die Gefährdungen pro Anwendungsfall fest, beispielsweise, dass ein Fernwartungszugang von einer unberechtigten Person benutzt wird.
4. Die Risikobewertung basiert auf der Identifikation von möglichen Gefährdungen anhand einer Risikomatrix.

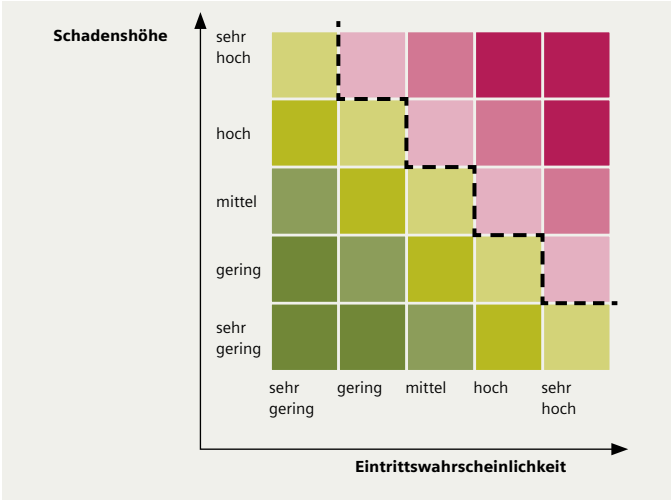

Abbildung 3: Risikomatrix nach BSI-Standard 200-3

Eine Gefährdung mit hoher Eintrittswahrscheinlichkeit und hohem potenziellen Schaden landet in der Risikomatrix rechts oben im roten Bereich (hohes Risiko). Geringe Schadenshöhe und Eintrittswahrscheinlichkeit bedeuten ein geringes Risiko – in der Matrix links unten grün dargestellt. Die genaue Aufschlüsselung von Schadenshöhe (Grad der Einschränkung des Anlagenbetriebs), Eintrittswahrscheinlichkeit und Risiko ist im BSI-Standard 200-3 festgelegt.

5. Durch die Maßnahmenermittlung werden konkrete Möglichkeiten definiert, die im folgenden Kapitel detailliert beschrieben werden.
6. Zur Maßnahmenumsetzung gehört bereits die terminliche und organisatorische Umsetzungsplanung. Hierzu gehört auch, die Verantwortung für die Maßnahmenumsetzung zu definieren und das Budget dafür klar zuzuordnen.
7. Für das Audit müssen die Maßnahmen nachgewiesen werden, die Dokumentation der Anlage muss vollständig sein und Checklisten müssen ausgefüllt sein. In regelmäßigen Abständen muss die Wirksamkeit der Maßnahmen geprüft werden. Wenn Mängel erkannt werden, sei es durch geänderte Risiken, sei es durch neue Arten von Schadsoftware o. Ä., muss der Prozess, beginnend mit der Gefährdungsbestimmung, neu gestartet werden.

Schutzkonzept

Da die Gefährdungen unterschiedlichster Natur sind, von außen wie von innen erfolgen können und die Angreifer unterschiedlich gut gerüstet sind, ist es wichtig, ein vielschichtiges Schutzkonzept zu erstellen, um den Prozess bestmöglich zu schützen. Auch wenn beispielsweise die Firewall überwunden wurde, weil der Angreifer die Anlage physisch betreten hat, müssen weitere Schutzmechanismen auf den Endgeräten greifen.

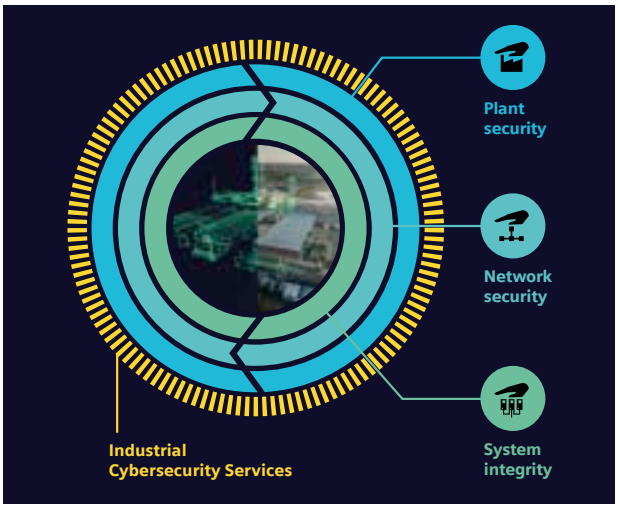

Abbildung 4: Schutzkonzept »Defense in Depth«

Die Abbildung zeigt das mehrstufige Schutzkonzept, das Anlagenschutz, Netzwerkschutz und System integrität als die drei wesentlichen Schichten für effektive Sicherheit definiert.

Maßnahmen zum Anlagenschutz

Mit organisatorischen Maßnahmen sind alle Maßnahmen zum physischen Schutz der Anlage gemeint. Betrachtet werden müssen neben Einbruchsschutz auch Maßnahmen gegen Umwelteinflüsse.

Schutzkonzept

- Einbruch/Vandalismus
- Unbefugter Zutritt
- Hochwasser/Überschwemmungen
- Feuer
- Rauch/Staub/Schadgase
- Blitz/Überspannung/EMV

Organisatorische Maßnahmen

Entsprechend den Gefährdungen müssen Maßnahmen getroffen werden, um die Anlage zu schützen. Besonders muss hier noch der Fall betrachtet werden, wenn Außenstationen (z. B. Lager) in der Regel unbesetzt sind und nur von der Leitwarte aus per Fernzugriff überwacht werden. Außenstationen sind einbruchssicher aufzubauen, Fenster und Türen geeignet zu sichern. Mittels Tür-/Fensterkontakten kann die Steuerung erkennen, wenn Türen und Fenster geöffnet werden, und dies an die Leitwarte weitermelden.

Eine IP-Kamera hilft, Angreifer zu erkennen und von der Leitwarte aus das Gebäude zu überwachen.

Unterschiedliche Produktionsbereiche sind auch physisch mittels differenzierter Zutrittsberechtigungen zu trennen. Kritische Komponenten sind z. B. in einem verschlossenen Schaltschrank zu sichern (siehe hierzu auch Seite 14).

Die Richtlinien für physische Zugangsschutzmaßnahmen haben auch Einfluss darauf, welche Cybersecurity-Maßnahmen in welcher Stärke erforderlich sind. Wenn beispielsweise zu einem Bereich von vornherein nur ausgesuchte berechtigte Personen Zugang haben, müssen die Netzzugangsschnittstellen oder Automatisierungssysteme nicht im gleichen Maß abgesichert werden, wie es bei öffentlich zugänglichen Bereichen der Fall wäre.

Mit einer Zertifizierung nach IEC 27001 können Unternehmen Risiken im Bereich Informationssicherheit senken, relevante Sicherheitsvorschriften und -anforderungen besser erfüllen und die Entwicklung einer internen Sicherheitskultur fördern.

Maßnahmen zum Netzwerkschutz

Das Netzwerk muss so strukturiert werden, dass es potenziellen Angriffen bestmöglich widersteht. Dabei muss der Zugriffsmöglichkeit, der Verfügbarkeit und dem Schutz Rechnung getragen werden.

Zugriffsmöglichkeit

Netzwerke sind meist keine abgeschlossenen Systeme ohne Anbindung ans Internet. Für Anlagenbetreiber ist es zunehmend notwendig geworden, dass Zugriffe von außen für Wartung, Diagnose, Optimierung, Patches, Updates etc. möglich sind.

Verfügbarkeit

Der automatisierte Prozess, der beispielsweise mittels PROFINET Kommunikation über das Netzwerk geregelt wird, soll unabhängig von einzelnen Leitungsunterbrechungen ausgeführt werden. Die Überwachungssysteme in der Leitwarte sollen den Prozess weiterhin beobachten können, auch wenn vereinzelte Router ausfallen.

Schutz

Der Prozess soll vor allen möglichen Risiken geschützt werden, die das Netzwerk bedrohen können, wie unberechtigter Zugriff, Schadsoftware, (D)DoS-Attacken etc. Alle Kommunikationsarten außer den zulässigen und gewünschten Zugriffen sollen durch geeignete Maßnahmen geblockt werden.

Die IEC 62443 fordert für den Netzwerkschutz folgende Elemente:

- Segmentierung der Netzwerkarchitektur
- Isolierung oder Segmentierung für Hochrisikokomponenten
- Blockieren nicht notwendiger Kommunikation und
- Zugriffe durch Firewalls

Netzwerksegmentierung

Die Netzwerksegmentierung durch Firewalls schützt gegen netzwerkseitige Angriffe. Das Netzwerk wird in funktionelle Gruppen aufgeteilt, wie beispielsweise Produktionsnetzwerke, Anlagennetzwerk und Büronetzwerk, und der Zugriff wird detailliert durch Firewalls geregelt.

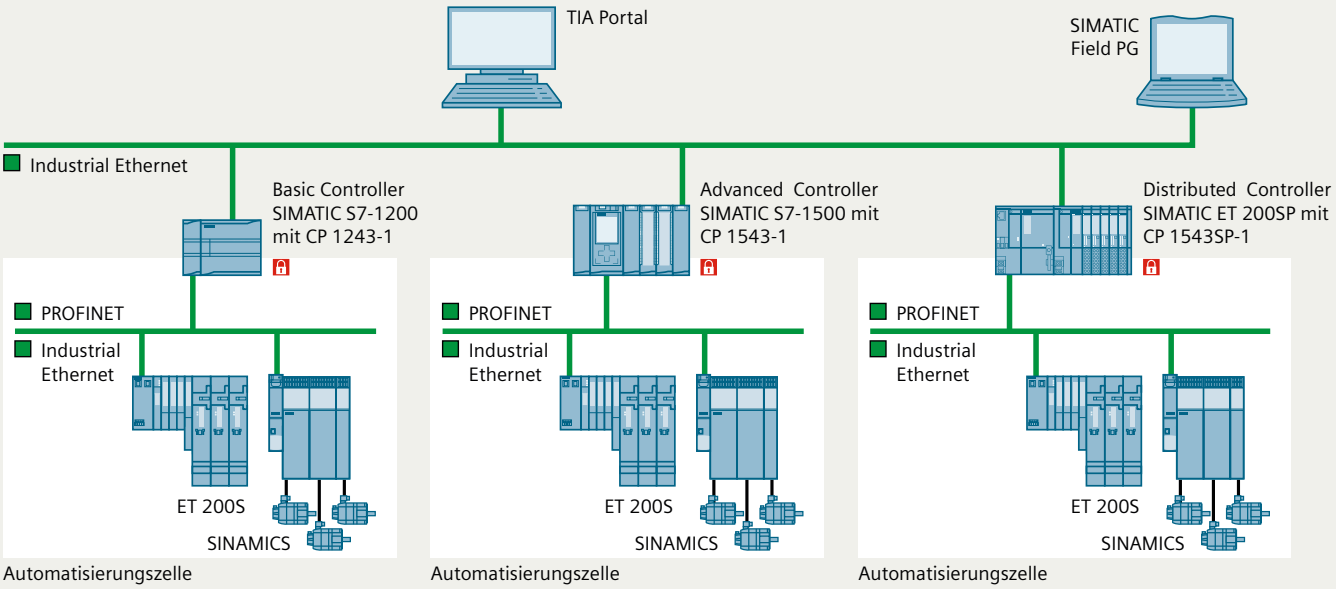

Abbildung 5: Netzwerksegmentierung entsprechend IEC 62443-2-1

Demilitarisierte Zone (DMZ)

Das Bild zeigt einen in der IEC 62443-2 empfohlenen Netzwerkaufbau. Die Automatisierungszellen unten sind als funktionelle Einheiten zusammengefasst und jeweils mit einer Firewall vom anlagenübergreifenden Netzwerk getrennt. Im darüberliegenden Anlagennetz hängen alle Geräte, die übergeordnet für den Betrieb der Anlage wichtig sind, wie ein Leitsystem, Server und Ähnliches. Der Übergang vom Anlagennetz zum Büronetzwerk ist nochmals durch eine Firewall getrennt. Hier können eine oder mehrere demilitarisierte Zonen (kurz DMZ) eingerichtet werden. In einer DMZ kommunizieren die Geräte aus dem über- und unterlagerten Netzwerk nicht direkt miteinander, sondern über einen Server, der beispielsweise den Anlagenzustand aus den Automatisierungszellen abfragt und diese Informationen dem überlagerten Netzwerk zur Verfügung stellt. Das Büronetzwerk ist ebenfalls mit einer oder mehreren Firewalls gegenüber dem Internet gesichert.

Durch diesen Aufbau ergeben sich in diesem Beispiel drei Schutzmauern für die jeweiligen Automatisierungszellen, die den Prozess steuern. Das Büronetzwerk, das potenziell häufiger von eingeschleuster Malware (z. B. USB-Sticks) betroffen ist, ist durch zwei Firewalls von der Automatisierungszelle getrennt. Je näher ein Mitarbeiter an der Automatisierungszelle arbeitet, desto wichtiger ist die konstante Sensibilisierung für das Thema Cybersecurity.

Fernzugriff und verteilte Außenstationen

Eine spezielle Herausforderung ist die Anbindung von externen, verteilten Stationen. Diese müssen autark arbeiten können, wobei dennoch die Überwachung aus der Leitwarte heraus möglich sein soll. Das Netzwerk einer Außenstelle muss geschützt und der Zugriff zur Außenstelle muss gesichert werden, auch wenn diese über ein eigenes Netzwerk oder eine firmeneigene Verbindung angebunden ist. Die Außenstation kann per Kabel (z. B. ADSL, SHDSL) oder über Funk (z. B. LTE, UMTS) angebunden sein. Das Modem muss eine Firewall enthalten und VPN-fähig sein.

Um die Sicherheit zu erhöhen, kann gemäß IEC 62443 die VPN-Verbindung für Fernzugriffe so eingerichtet werden, dass der Tunnel nur aufgebaut wird, wenn ein Techniker vor Ort aktiv den VPN-Aufbau an der Baugruppe aktiviert.

Drahtlose Verbindungen per WLAN

Die Funkübertragung mittels WLAN oder anderer Technologien muss besonders betrachtet werden. Bei der kabelgebundenen Kommunikation muss ein Angreifer physischen Zugang zu den Kabeln oder den Netzkomponenten haben, um den Datenverkehr mitlesen oder verfälschen zu können. Bei drahtloser Kommunikation verbreiten sich die Funkwellen hingegen über einen größeren Bereich, was einen Angriff einfacher macht.

Wenn WLAN in der Automatisierungszelle benötigt wird, ist ein eigenes WLAN für die Automatisierung einzurichten. Das Büro-WLAN muss über andere WLAN Access Points betrieben werden, um so die Netzwerksegmentierung aufrechtzuerhalten.

Organisatorische Maßnahmen für WLAN

Der Access Point ist unzugänglich oder in einem abgeschlossenen Schaltschrank gesichert zu installieren, wobei die WLAN-Antennen abgesetzt montiert werden. Damit kann kein Angreifer physisch auf den Access Point zugreifen. Darüber hinaus ist die WLAN-Frequenz mit Bedacht zu wählen, da andere Applikationen, die dieselbe Frequenz nutzen, die Übertragung ähnlich Störsendern einschränken oder sogar ganz unterbrechen können.

Technische Schutzmechanismen für WLAN

Der aktuelle Stand der Technik ist die WPA2-Verschlüsselung. Ältere Verschlüsselungen (WEP und WPA) dürfen nicht mehr verwendet werden, da diese Methoden unsicher sind und leicht überwunden werden können. Das Standardpasswort und die SSID müssen geändert werden und die SSID sollte verborgen werden.

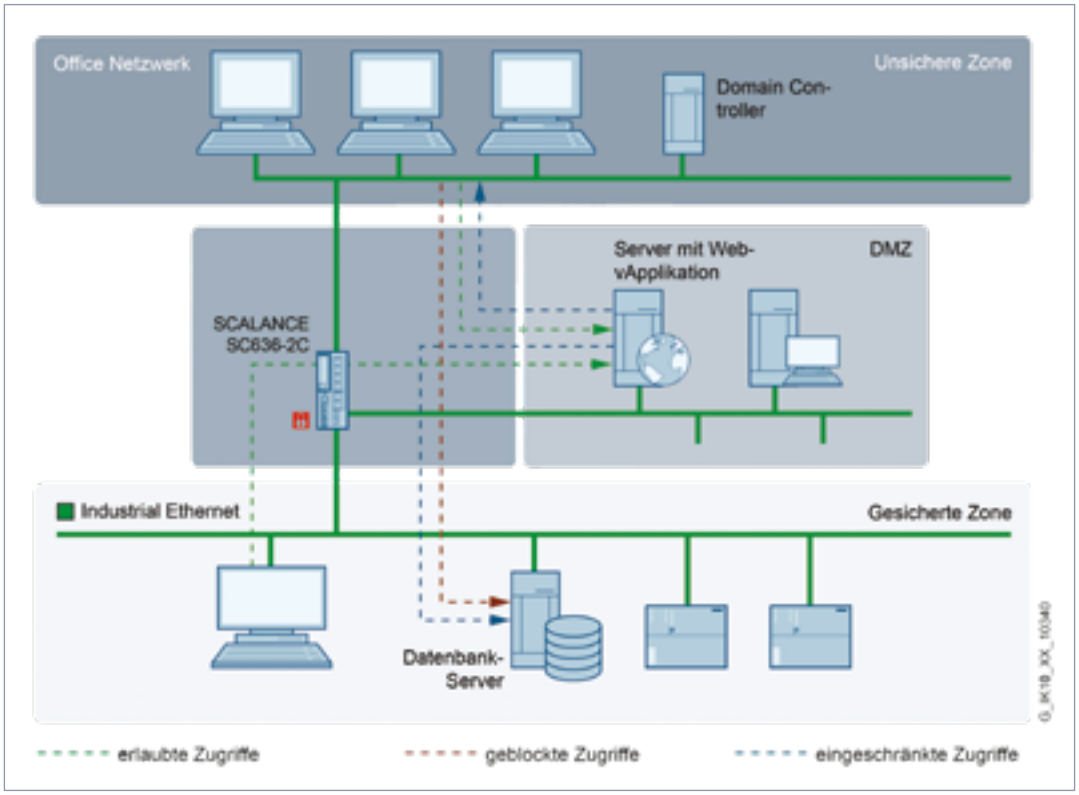

Abbildung 6: Verbindung eines lokalen Service PC via DMZ port der SCALANCE S615

Allgemeine Anforderungen an Netzwerkelemente

Der internationale Standard für sichere Konfiguration und Verwaltung von Netzkomponenten in der Norm IEC 62443 empfiehlt die folgenden Eigenschaften und Schutzmechanismen für die Konfiguration und Absicherung der Geräte.

Zugriffsschutz und Account-Verwaltung
Um Netzwerkkomponenten gegen unberechtigten Zugriff zu schützen, müssen für den Zugriff freigegebene Accounts verwaltet und ggfs. gesperrt werden können. Die folgenden Eigenschaften sollen unterstützt werden:

- Zugriffsmöglichkeit einrichten
- Nutzer identifizieren/identifizierbar machen durch Accounts
- Accounts einstellen/ändern/beenden durch einen zentralen Manager
- Dokumentation von Accounts und Accountnutzern
- Ungenutzte Accounts werden gelöscht oder gesperrt regelmäßige Prüfung des Zugriffsrechts
- Default-Passwörter müssen geändert werden

Die Anforderungen an den Zugriffsschutz lassen sich durch User Management Components (UMC) realisieren.
Bei UMC werden verschiedene Benutzer-Accounts auf einem zentralen Server, dem UMC-Ring-Server, angelegt. TIA Portal Projekte können diese Benutzer verwenden und es können ihnen Zugriffsrechte für die Netzwerkkomponenten und -teilnehmer erteilt werden.

Zugriffskontrolle: Authentifizierung
Bei Zugriff auf eine Komponente soll der zugreifende Nutzer identifiziert werden können. Die Authentifizierung soll die folgenden Mechanismen bieten:

- Zugriff nur möglich, wenn Nutzer authentifiziert wurde (oder eine ausreichende Zutrittskontrolle existiert)
- starke Schutzmechanismen für administrativen Zugang
- Aufzeichnen aller Zugriffe auf kritische Systeme
- Alle Fernzugriff-Nutzer identifizieren
- Richtlinien für den Fernzugriff, automatisches Log-out bei Inaktivität
- Fernzugriffe sperren nach wiederholt fehlgeschlagenem Log-in
- Re-Authentifizierung nach Inaktivität bei Fernzugriff
- Auch für Task-to-Task-Kommunikation muss ein Authentifizierungsmechanismus eingerichtet sein

Diese Forderungen betreffen unterschiedliche Systeme und müssen deshalb für die gesamte Anlage betrachtet werden. Für den Fernzugriff können die Forderungen zum Beispiel durch SINEMA Remote Connect abgedeckt werden, da unter anderem der automatische Log-out bei Inaktivität und das Sperren einer IP nach mehreren fehlgeschlagenen Log-in-Versuchen bereits implementiert sind. Es wird zudem stets mitprotokolliert, wenn ein Fernzugriff erfolgt. Im TIA Portal kann verschiedenen Benutzern das Zugriffsrecht auf das Projekt und nochmals gesondert für die Security-Konfiguration erteilt werden. Da die Security-Konfiguration nochmals als eigenes Recht geführt wird, wird auch die Forderung für den zusätzlichen Schutz des administrativen Zugangs gesichert.

Zugriffskontrolle: Autorisierung

Autorisierung bedeutet, einem zuvor authentifizierten Nutzer bestimmte Rechte einzuräumen, beispielsweise den Zugriff auf eine Komponente. Für die Autorisierung benennt die IEC 62443 die folgenden Punkte:

- Logische oder physische Methode für Zugriffserlaubnis
- Rollenbasierte Zugriffsrechte auf das System oder auf Informationen
- Zugriffsrecht auf Safety-Funktionen muss ein separates Recht sein
- Für kritische Systeme müssen mehrere Zugriffsstufen eingerichtet werden

Netzwerkmanagement

Für das Netzwerkmanagement kann das Standardprotokoll SNMP eingesetzt werden, das mittlerweile von allen Netzwerkschnittstellen unterstützt wird. Mit dem SINEMA Server lassen sich das Netzwerk und über VPN angebundene Anlagenteile durch Nutzung von SNMP überwachen. So können alle Netzwerkteile verwaltet und Ausfälle schneller erkannt werden.

Netzwerkplan

Für die Dokumentation der Anlage ist ein physikalischer Netzwerkplan, also eine Topologie-Ansicht, erforderlich. Die Topologie zeigt, wie die Teilnehmer miteinander verschaltet sind. Aus diesem Netzwerkplan müssen Adressen (IP und MAC), Port-Verschaltung und Installationsort ersichtlich sein. Einen solchen Netzwerkplan könnte man beispielsweise aus TIA Portal heraus drucken oder man nutzt dafür das Netzwerkplanungstool SINETPLAN.

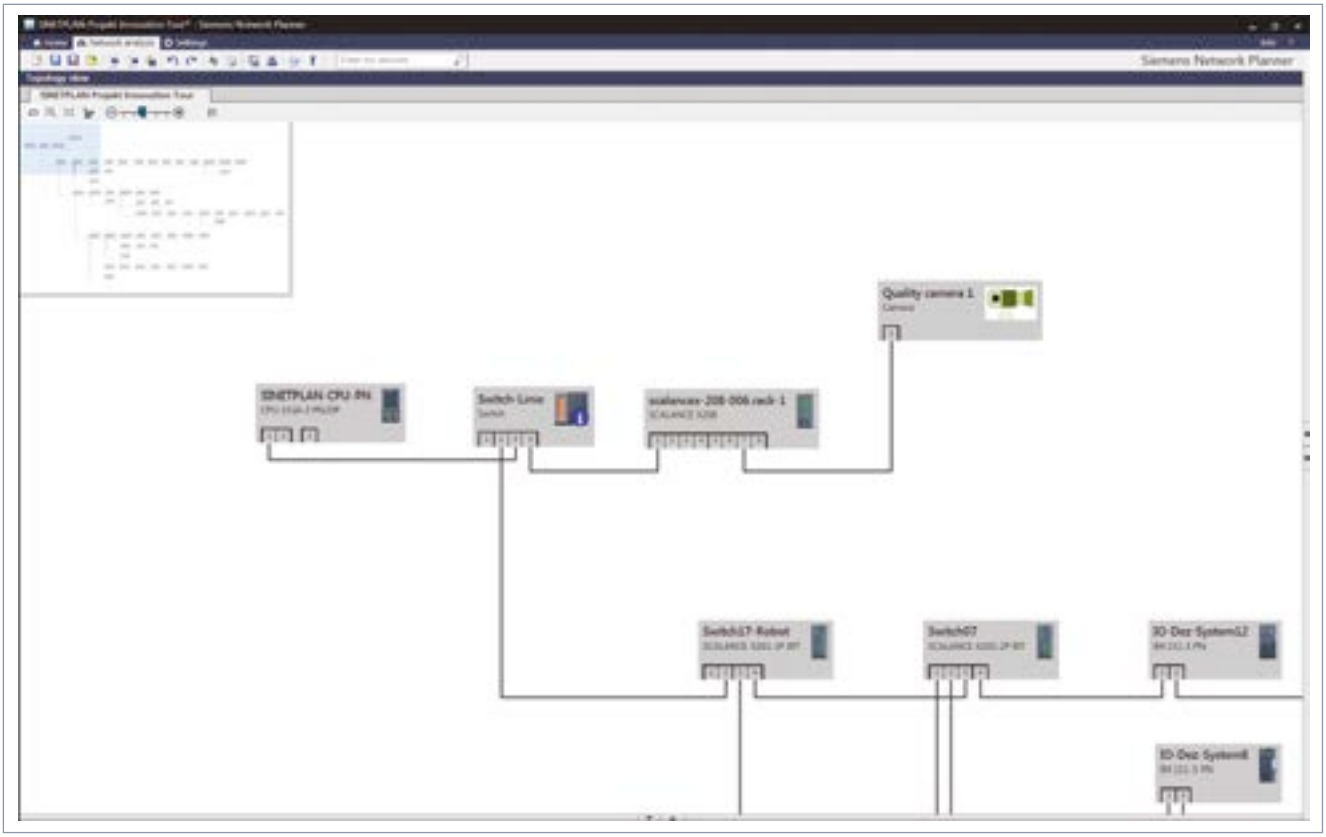

Abbildung 7: Topologisches Netzwerk in SINETPLAN

Maßnahmen zur Systemintegrität

Unter Systemintegrität versteht man das Sicherstellen der Echtheit und Unverfälschtheit von Daten und Programmen innerhalb eines Systems. Niemand darf unbefugt das Programm verändern oder Daten verfälschen (weder auf dem Kommunikationsweg noch im System) oder das Programm oder die Daten umkopieren. Das Know-how für die Regelung des Prozesses ist ebenfalls schützenswert.

Programmzugang
Bereits die Programmierung der Steuerungen (SPS) ist Bestandteil der Cybersecurity. Der Zugang zum Projekt und zu den Büroräumen ist daher zu schützen. Durch das Windows-Log-in wird generell der Schutz für das Projekt erreicht. Ab TIA Portal V15 kann das gesamte Projekt verschlüsselt werden. Somit ist das Öffnen des Projekts nur über einen zusätzlichen Benutzernamen und ein zusätzliches Passwort möglich, was die parallele Arbeit mehrerer Personen am gleichen Projekt sicher macht.

CPU-Zugriffsschutz
Mit den verschiedenen Zugriffsstufen der CPU können verschiedene Passwörter eingerichtet werden, damit der Vollzugriff nur qualifiziertem Personal zur Verfügung steht.

Webserver
Immer mehr Steuerungslösungen verwenden Zugriffe über Webserver, die oft auch für Fernzugriffe verwendet werden. Dafür muss auch der Webserver gut geschützt werden. HTTPS ist die sichere Variante von HTTP und bevorzugt einzusetzen. Durch Einrichten verschiedener Benutzer und Zugriffsstufen kann man die vom Branchenstandard geforderte Authentifizierung und Autorisierung erreichen.

Sichere Kommunikation
Kommuniziert die Steuerung aus ihrer sicheren Zelle nach außen, muss diese Kommunikation verschlüsselt werden. Der heutige Stand der Technik ist TLS-Verschlüsselung. Diese kann in der S7-1500 über OPC UA oder über eine TCP-Verbindung genutzt werden.

Eine weitere Möglichkeit für die Verschlüsselung ist die Nutzung der eingebauten Firewalls, um eine VPN-Verbindung aufzubauen. Die Firewalls bauen zueinander den VPN-Tunnel auf, die Kommunikation zwischen den Automatisierungszellen wird verschlüsselt über das überlagerte Netz übertragen und beim Zielnetzwerk wieder entschlüsselt.

Sicherheitsmaßnahmen auf industriellen PCs
Im Industrieumfeld eingesetzte PCs (IPCs) erfordern spezielle Maßnahmen, da hier einige Bedrohungen – wie infizierte Datenträger – direkt wirken können, während bei einer Steuerung USB-Datenträger nicht direkt angeschlossen werden können. Die folgenden Maßnahmen dienen der Härtung eines IPC gegen Cybersecurity-Attacken.

Benutzerkonten
Es ist sinnvoll, Administrator- und Benutzerkonten anzulegen. Nur der Administrator ist berechtigt, Änderungen an Sicher heitseinstellungen zu tätigen oder Software zu (de-)installieren. Der normale Benutzer kann dies nicht, sodass keine Schadsoftware im normalen Betrieb installiert werden kann.

Richtlinien konfigurieren
Über die Microsoft Management Console können Richtlinien für die Verwendung von Datenträgern, der Systemsteuerung etc. eingestellt werden. Sie finden online ein Dokument, das darüber informiert, welche Richtlinien genutzt werden können und wie diese einzustellen sind:
support.industry.siemens.com/cs/ww/de/view/109475014

Enhanced Write Filter (EWF)
Diese Funktion steht auf SIMATIC IPCs zur Verfügung und sichert einen Teil des Dateisystems gegen Abänderung von Daten, indem Schreibzugriffe in den RAM umgeleitet werden. Nach einem Neustart des IPC ist das Dateisystem unverändert. Schadprogramme, die im Betrieb Zugriff erhalten haben, sind nach dem Neustart nicht mehr vorhanden.

Firewall
Bereits Standard-Firewalls (Windows-Firewall) bringen einen sinnvollen Basisschutz; sie sollten dringend aktiviert bleiben. Mit geeigneten Regeln ist die Firewall so zu konfigurieren, dass ausschließlich Nutzdatenkommunikation möglich ist und andere Kommunikation geblockt wird.

Virenschutz
Mittels einer geeigneten Antivirus-Software können Viren und Schadprogramme erkannt werden. Bei Siemens setzen wir für die Automatisierung auf eine McAfee-Installation. Ein Management Server verwaltet die Antivirus-Clients auf den PC-Systemen und stellt die aktuellen Virensignaturen bereit. Der Management Server kann auch Alarme per E-Mail versenden, um das Servicepersonal zu benachrichtigen.

IEC-62443-zertifizierte Produkte
Bei der Wahl der eingesetzten Steuerungen, PCs und sonstigen Systeme ist darauf zu achten, dass sie Schutzmechanismen enthalten und auf Schwachstellen getestet wurden. Solche Tests sind standardisiert; beispielsweise zeigt ein Achilles-Zertifikat an, dass das System durch Belastungs- und Schwachstellentests geprüft wurde. Außerdem kann der Hersteller bereits seine Produktentwicklung sicher durchführen, um so ein hohes Maß an Qualität für seine Produkte sicherzustellen. Der Entwicklungsprozess von Siemens wurde geprüft und hielt der Prüfung nach IEC 62443-4 stand:
siemens.com/press/PR2016080373DFDE

Personelle Maßnahmen

Da die besten technischen und organisatorischen Schutzmechanismen wirkungslos sind, wenn die eigenen Mitarbeiter fahrlässig handeln, sind auch Trainings zu Cybersecurity und klare Definitionen der Verantwortungsbereiche ein integraler Bestandteil von Cybersecurity. Die IEC 62443 empfiehlt, neues Personal bereits durch ein Screening auf Zuverlässigkeit zu prüfen und zu testen, inwiefern es der Verantwortung gerecht wird. Bestandspersonal ist ebenso auf Zuverlässigkeit zu prüfen. Fremdpersonal kann ebenfalls durch Trainings unterwiesen werden, sollte jedoch stets durch eigenes geschultes Personal begleitet und beaufsichtigt werden.

Verantwortung
Der Branchenstandard verlangt, dass Betreiber kritischer Infrastrukturen (KRITIS) gegenüber der Organisation UP KRITIS ihren Ansprechpartner für Cybersecurity benennen. Generell ist es empfehlenswert, die Verantwortung für Cybersecurity im Unternehmen auf eine Person oder Gruppe zu übertragen.

Trainings
Regelmäßige Schulungen müssen den korrekten Umgang mit installierten Systemen, Wechseldatenträgern und Software sowie ein Training der Reaktion auf Vorfälle und alle weiteren möglichen Gefährdungen enthalten. Für Administratoren fordert der Branchenstandard explizit, dass diese für den richtigen Umgang mit Netzwerkkomponenten geschult werden, damit die Konfigurationen korrekt durchgeführt werden.

Notfallplan und Wiederherstellung

Der Branchenstandard fordert ein Konzept für den Notfall, wenn eine Gefährdung eingetreten ist und der Prozess unterbrochen wurde. Dieses Konzept wird auch Business Continuity Management genannt. Folgende Fragen sind zu klären:

- Welche Ausfallzeit ist tolerierbar?
- Wie kann der Prozess unabhängig von Steuerung/Office weiterarbeiten?
- Wie gut können andere Anlagenteile die Versorgung kompensieren?
- Wie wird das betroffene System wieder bereinigt?
  - Durch Redundanzen
  - Durch Wiederherstellung auf Basis eines Backups
- Wie wird ein weiteres Eintreten dieses Ausfalls verhindert?
  - Meldung
  - Optimierung

Siemens ProductCERT
Siemens verfügt über ein Team von Sicherheitsexperten, das als Anlaufstelle für Kunden und deren Sicherheitsexperten dient, falls diese eine Sicherheitslücke erkannt haben. Dieses Team heißt Product Computer Emergency Response Team (ProductCERT). Gemeldete Sicherheitslücken werden sofort bewertet und analysiert.

Siemens Security Advisories
Das Siemens ProductCERT untersucht alle Meldungen zu Sicherheitsproblemen und veröffentlicht sogenannte Security Advisories zu validierten Sicherheitsschwachstellen, die Siemens Produkte direkt betreffen und ein Softwareupdate bzw. -upgrade oder eine andere Aktion des Anlagenbetreibers erfordern. Nutzen Sie diese Informationsquelle für die Bewertung der Auswirkungen einer Sicherheitsschwachstelle. Der offene Umgang mit eigenen Schwachstellen wird von Siemens betrieben, damit Sie reagieren können, bevor die Schwachstellen bei Ihnen ausgenutzt werden. Bleiben Sie informiert mit unseren RSS Feeds:
siemens.com/global/de/home/produkte/services/cert.html#Benachrichtigungen

Gesamtüberblick

Für eine umfassende Industrial Security müssen alle Schutzstufen berücksichtigt werden. Sicherheitsmaßnahmen müssen so vielfältig sein wie die potenziellen Risiken. Ein Ende-zu-Ende-Ansatz und mehrere Verteidigungslinien werden Industrieanlagen zuverlässig schützen. Um dieses komplizierte Thema für die Industrie einfacher zu gestalten, bietet Siemens ein abgestimmtes Lösungsportfolio speziell für die Sicherheit von Industrieanlagen und Betriebstechnologien.

Eine repräsentative Netzarchitektur einer Softdrinkanlage ist in der folgenden Abbildung dargestellt. Sie zeigt die Ebenen, in denen die in diesem Dokument beschriebenen Sicherheitsmaßnahmen gemäß den Empfehlungen der Norm IEC-62443 implementiert wurden.

Warum Siemens?
Siemens bietet eine zuverlässige Basis für sichere und innovative Automatisierungslösungen.

Wir bei Siemens:

- verstehen Digitalisierung,
- verstehen die Nahrungsmittel- und Getränkeindustrie,
- verstehen industrielle Kommunikation,
- verstehen industrielle Sicherheit und
- haben bewährte und zertifizierte Security-Prozesse und -Produkte.

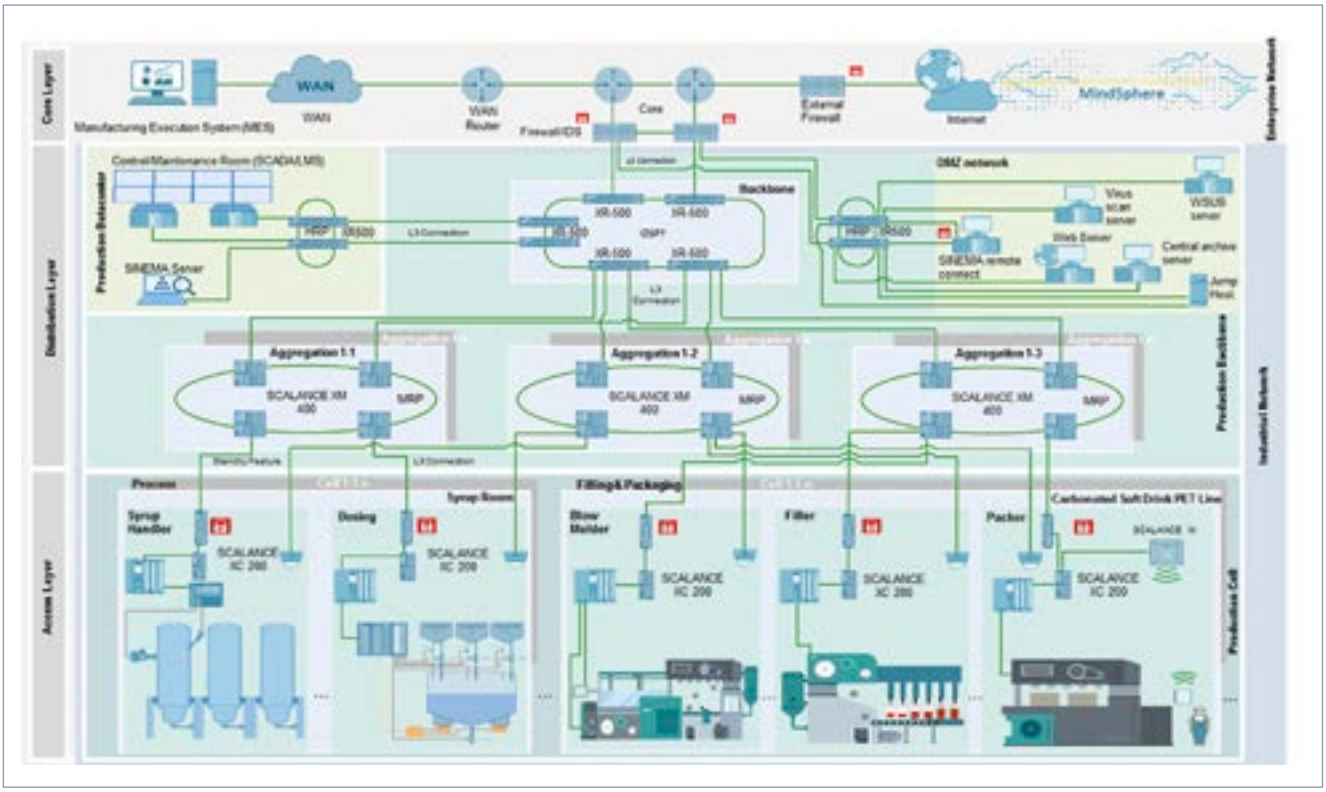

Abbildung 8: Netzarchitektur einer Softdrinkanlage.

Begriffe und Abkürzungen

Authentifizierung
Die Erkennung und Identifizierung eines Benutzers oder (bei vernetzten Anlagen) eines anderen Systems.

Autorisierung
Die Berechtigung für den Zugriff auf ein System bzw. einen (Software-)Teil eines Systems oder auf ein Programm.

Cybersecurity
Alle technischen Maßnahmen für die Sicherheit einer Anlage wie Netzwerkschutz, Systemhärtung der Komponenten und Monitoring von Vorfällen.

Prozess
Der eigentliche Fertigungsprozess, z. B. die Käseproduktion oder das Abfüllen in Flaschen, unabhängig davon, ob es sich um einen diskreten oder einen kontinuierlichen Prozess handelt.

Virtual Private Network (VPN)
Mit VPN wird eine verschlüsselte Verbindung zwischen den VPN-Teilnehmern aufgebaut; man spricht auch von einer VPN-Gruppe. Ein VPN ähnelt einem Tunnel, Datenverkehr kann aus jeder Richtung geschickt werden. Im Tunnel wird der Datenverkehr verschlüsselt übertragen und am Tunnelende – also am anderen VPN-Gerät – wieder entschlüsselt weitergeleitet. Die Endgeräte müssen somit keine Verschlüsselung unterstützen, die VPN-Geräte übernehmen die Verschlüsselung.

Herausgeber
Siemens AG

Digital Industries
Factory Automation
Vertical Sales Food & Beverage
Lindenplatz 2
20099 Hamburg
Deutschland

Für weitere Informationen wenden Sie sich an
E-Mail: fb.communications@siemens.com

Artikel-Nr. VRFB-B10060-00