genua.

IT/OT-Konvergenz in der Brownfield-Fabrik

Leitfaden für die sichere Vernetzung von Produktionsanlagen in der Fertigungs- und Prozessautomatisierung

Die wenigsten industriellen Digitalisierungsprojekte werden auf der grünen Wiese geplant. Häufig gilt es, Bestandsanlagen (Brownfield) in der Fertigungs- und Prozessautomation zu erweitern. Die gute Nachricht ist: Mit einem ganzheitlichen Ansatz können solche Umgebungen effizient gegen Cyberangriffe geschützt werden. Dieses Whitepaper beschreibt die wesentlichen Herausforderungen, gibt einen Überblick über die Norm IEC 62443 als wichtige Strukturierungshilfe und liefert wertvolle Hinweise für eine zukunftssichere IT/OT-Strategie.

SecurITy made in Germany

Inhalt

1. Konvergenz von OT und IT – Herausforderung für Safety und Security 3

2. IT/OT-Referenzarchitektur 5

3. Schutzziele: OT vs. IT 6

4. Die Normenreihe IEC 62443 7

5. Wirkungsvolle Strategien für Defense in Depth 9

6. Chancen der Anomalie-Erkennung in einem OT-Netz 10

7. Zero-Trust-Architekturen für die Industrie 12

7.1 Zero Trust Networking nach Forrester 14

7.2 Software-Defined Perimeter 15

7.3. Software-Defined Perimeter am Beispiel Fernwartung 16

8. Sicherheitsrisiko Mensch 18

9. Hochsichere Datenausleitung 19

10. Fazit: Handlungsempfehlungen im Überblick 20

11. Quellenverzeichnis und weiterführende Informationen 21

1. Konvergenz von OT und IT – Herausforderung für Safety und Security

Wenn im Zuge von Industrie 4.0 klassische Datenverarbeitung (IT, Informationsverarbeitung) und Produktionsumgebung (OT, Operational Technology, Betriebstechnologie) vernetzt werden sollen, liegt die Herausforderung für Sicherheitsverantwortliche darin, die unterschiedlichen Rahmenbedingungen und Zielsetzungen der beiden Domänen in einem gemeinsamen Sicherheitskonzept zu erfüllen. Während Cybersicherheit in der IT seit Jahrzehnten eine Selbstverständlichkeit darstellt, werden in der OT viele Produktionsanlagen nach wie vor mit unzureichendem oder fehlendem Schutz gegen Cyberangriffe betrieben.

Dabei handelt es sich vielfach um alte, oft proprietäre, teilweise isolierte (stand-alone) Systeme, die über Feldbusse mit anderen Rechnern innerhalb derselben Maschine oder mit externen Sensoren und Aktoren vernetzt sind. Diese Produktionsanlagen müssen zuverlässig vor Angriffen von außen und innen geschützt werden können, ohne dass die Leistungsfähigkeit (Performance) oder die funktionale Betriebssicherheit (Safety) beeinträchtigt werden.

Insbesondere durch die Öffnung eines internen OT-Netzwerks für Fernwartungszugänge oder durch für Predictive Maintenance genutzte, nachträglich aufgesetzte Datenschnittstellen entstehen potenzielle Einfallstore für Angreifer.

Laut Umfragen des Branchenverbandes Bitkom in den Jahren 2021 und 2022 für die jeweils zurückliegenden zwölf Monate erlitten deutsche Unternehmen pro Jahr über 200 Milliarden Euro Schaden durch Datendiebstahl, Industriespionage und Sabotage. Ein Großteil der Schadenssumme entfiel dabei auf Ausfall, Diebstahl oder Schädigung von Informations- und Produktionssystemen oder Betriebsabläufen. 45 Prozent der befragten Unternehmen stimmten der Aussage zu, dass Cyberangriffe ihre geschäftliche Existenz bedrohen.

Mit einer ganzheitlichen, mehrstufigen Sicherheitsstrategie lässt sich auch in Brownfield-Anlagen hohe Sicherheit mit überschaubarem Aufwand realisieren. Sie ist letztendlich die Voraussetzung, um von den Chancen der Digitalisierung und Industrie 4.0 wie höherer Wettbewerbsfähigkeit, verbesserter Prozesseffizienz oder OEE-Optimierung langfristig zu profitieren.

Eine gute IT-OT-Security-Strategie legt nicht nur den Grundstein, um Security Incidents frühzeitig zu identifizieren. Sie hilft auch, Fehlkonfigurationen zu erkennen sowie die Verfügbarkeit und Effizienz zu steigern.

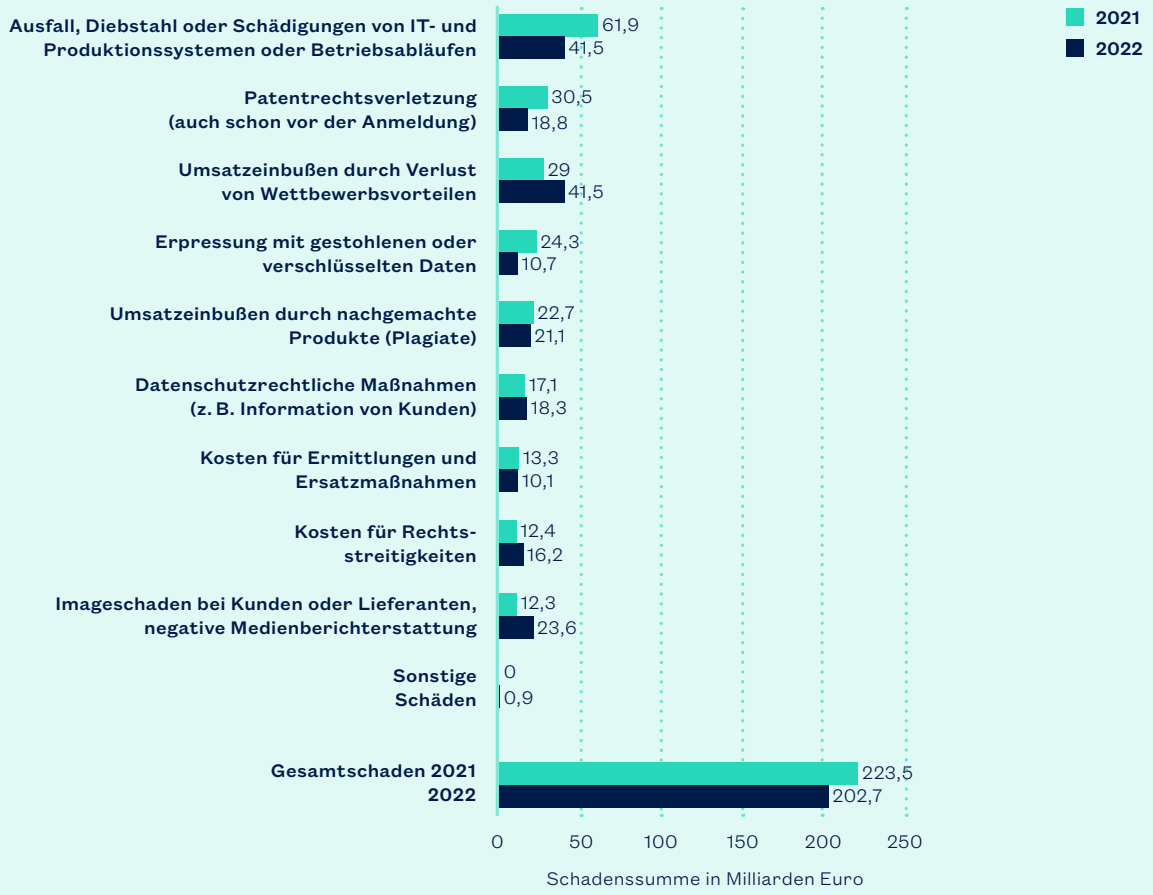


Bild 1: Schadenssummen durch Datendiebstahl, Industriespionage oder Sabotage in Unternehmen in Deutschland in den Jahren 2021 und 2022 (Quelle: Bitkom Research 2022 [1])

Dieses Whitepaper beschäftigt sich vorwiegend mit den Herausforderungen einer Brownfield-Situation und ist wie folgt aufgebaut:
In Kapitel 2 wird zur Einführung in das Thema eine sichere IT-OT-Architektur dargestellt. Nach einer kurzen Betrachtung der unterschiedlichen Schutzziele von IT und OT (Kapitel 3) folgt in Kapitel 4 ein Überblick zur Normenreihe IEC 62443. Diese stellt eine Strukturierungshilfe zur Einrichtung von Cybersicherheitsmaßnahmen in der Automatisierungsindustrie dar. Kapitel 5 beschreibt Ansätze für eine wirkungsvolle Defense-in-Depth-Strategie.

In Kapitel 6 werden Chancen und Möglichkeiten durch den Einsatz moderner Machine-Learning-basierter Anomalie-Erkennung in einem OT-Netz aufgezeigt. Kapitel 7 befasst sich mit dem Security-Paradigma Zero Trust Networking und dessen Implementierungsmöglichkeiten für OT-Netze. Es folgen Hinweise zum Umgang mit dem „Sicherheitsrisiko Mensch“ (Kapitel 8). Einen Lösungsvorschlag für die hochsichere Datenausleitung aus kritischen Infrastrukturen beschreibt schließlich Kapitel 9. Das Whitepaper schließt mit einem Fazit sowie Hinweisen zu weiterführenden Informationen.

[1] Achim Berg: Wirtschaftsschutz 2022, Bitkom e.V.
www.bitkom.org/sites/main/files/2022-08/Bitkom-Charts_Wirtschaftsschutz_Cybercrime_31.08.2022.pdf

2. IT/OT-Referenzarchitektur

Um eine nachhaltig wirksame Sicherheitsstrategie aufzubauen, empfehlen sich folgende Bestandteile (vgl. Bild), die in den folgenden Kapiteln dieses Leitfadens genauer beschrieben werden.

- Umsetzung von Defense in Depth und Zero Trust
- Netzwerksegmentierung gemäß Zones & Conduits
- Netzwerküberwachung mittels intelligenter Anomalie-Erkennung
- Sicherer Fernzugriff durch eine geeignete Fernwartungsarchitektur
- Hochsicheres Edge Computing für die Prozessoptimierung
- Hochsichere Datenausleitung mittels Datendioden

Bild 2: IT/OT-Referenzarchitektur für eine digitalisierte Brownfield-Fabrik. Implementierte Anwendungsszenarien sind hier u. a. die sichere Fernwartung, die Prozessoptimierung auf Basis von Edge Computing sowie die hochsichere Datenausleitung mittels Datendiode.

3. Schutzziele: OT vs. IT

Die Steuerung der meisten industriellen Anwendungen ist zeitkritisch; bei einigen Industriesteuerungen (Industrial Automation Control Systems, IACS) darf die Latenz (maximale Verzögerungszeit bei der Bearbeitung) nur wenige Millisekunden oder weniger betragen (Echtzeitanforderungen). Sicherheitsmaßnahmen in der OT dürfen daher niemals dazu führen, dass es in der Anwendung zu kritischen Verzögerungen in der Bearbeitung kommt.

Für jede Situation und Konfiguration muss das „richtige“ Maß an Sicherheit gefunden werden, bei dem einerseits das Schutzniveau ausreichend hoch ist und andererseits noch alles schnell genug abläuft. Keinesfalls darf es durch Sicherheitsmaßnahmen zu Störungen, Ausfällen oder gar Schäden in der Produktion kommen.

Diese bei Industrieanlagen und Steuerungen gebräuchliche Priorität der Anlagen- und Betriebssicherheit (Safety first) zeigt sich auch in der Reihenfolge der Schutzprioritäten in der OT: Während bei der IT Vertraulichkeit und Integrität der Daten deutlich vor der Verfügbarkeit rangieren, ist es in der OT gerade umgekehrt. Für den Betrieb der Anlagen haben Verfügbarkeit und Daten- bzw. Systemintegrität die höchste Priorität; die Vertraulichkeit der Daten spielt für die Funktions- und Betriebsfähigkeit einer Anlage nur eine untergeordnete Rolle.

Die Unterschiedlichkeit der Zielsetzungen zeigt sich auch in den Sicherheitsstandards bzw. Normen für die beiden Bereiche, die jeweils die Grundlage für die entsprechenden Zertifizierungen bilden. Während die ISO/IEC-27001-Familie die Datensicherheit in IT-Managementsystemen (Information Security Management Systems, ISMS) beschreibt, befasst sich die IEC-62443-Familie ausdrücklich mit industriellen Automatisierungssystemen (Industrial Automation and Control Systems, IACS).

Die Normenreihe IEC 62443 definiert und beschreibt nicht nur die Vorgaben für eine mögliche spätere Zertifizierung. Sie liefert auch eine wichtige Strukturierungshilfe zur Einrichtung von Cybersicherheitsmaßnahmen in der Automatisierungsindustrie. Sie wird daher im Folgenden näher beschrieben.

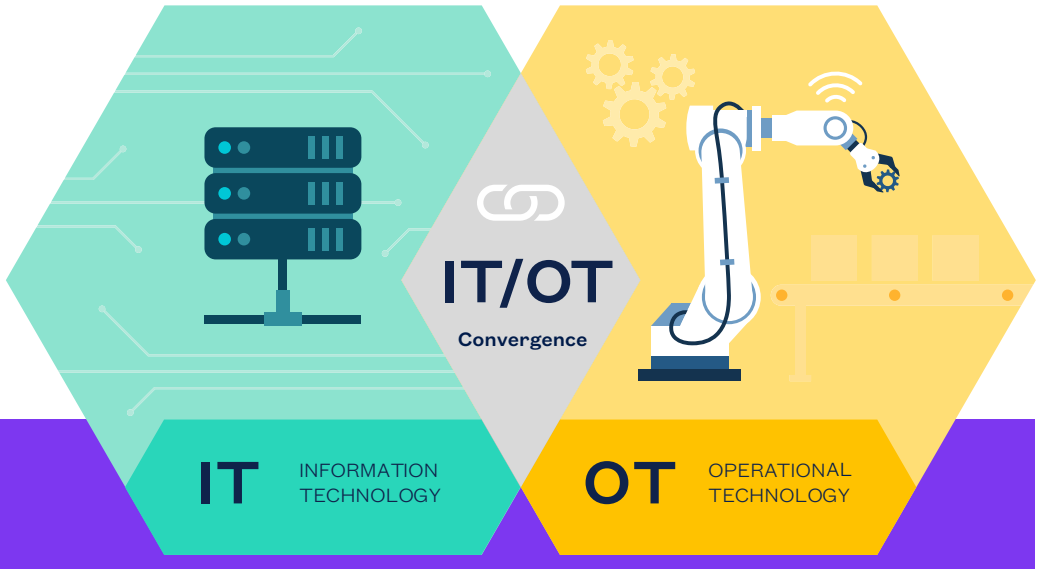


Bild 3: IT/OT-Konvergenz bedeutet, die unterschiedlichen Schutzziele von IT und OT sinnvoll auszubalancieren. Dabei müssen Produktionsanlagen zuverlässig vor Angriffen von außen und innen geschützt werden können, ohne dass die Leistungsfähigkeit (Performance) oder die funktionale Betriebssicherheit (Safety) eingeschränkt werden.

4. Die Normenreihe IEC 62443

Die grundlegende Struktur der Normenreihe IEC 62443 gliedert sich derzeit in vier Bereiche zum Thema „Cybersicherheit von Anlagen in der Automatisierungstechnik“, die jeweils mehrere Dokumente zu Einzelthemen enthalten:

„Grundkonzepte“ (General) beschreibt Grundlagen und Begriffe.

„Richtlinien und Verfahren“ (Policies and Procedures) richtet sich primär an die Betreiber von Anlagen und definiert Anforderungen und Bewertungskriterien für deren cybersicheren Betrieb.

„Automatisierungssysteme“ (Systems) beschreibt hauptsächlich für Systemintegratoren die technischen Anforderungen sowie Möglichkeiten für Risikoklassifizierung und -bewertung.

„Komponenten von Automatisierungssystemen“ (Components) fokussiert sich auf die Hersteller der einzelnen Komponenten, vorwiegend bezüglich technischer Anforderungen und Lebensdauerzyklen.

Darüber hinaus sind für die Zukunft zwei weitere Bereiche für Applikations- bzw. branchenspezifische Profile (Profiles) und Evaluationsmethodik (Security Evaluation Methodology) geplant.

Aufbau der Normenreihe IEC 62443

* noch nicht veröffentlicht

Bild 4: Aktuelle und geplante Dokumente zur Normenreihe IEC 62443 nach Angaben der IEC

Die IEC 62443 und Defense in Depth

In der IEC 62443-1-1 „Concepts and Models“ wird das Defense-in-Depth-Konzept näher beschrieben, das die Hauptziele Verfügbarkeit und Systemintegrität sichern soll. Dafür werden die einzelnen Schutzebenen drei Grundschichten zugeordnet. Von außen nach innen gesehen sind dies:

- **Anlagensicherheit**
- **Netzwerksicherheit**
- **Systemintegrität**

Dazu passend definiert die IEC 62433-1-1 die drei grundlegenden Rollen bzw. Verantwortlichkeiten für das Gesamtsystem:

- **Betreiber (Owner)**
- **Integrator (Integrator)**
- **Hersteller (Manufacturer)**

Letzterer liefert die Komponenten, aus denen das Automatisierungssystem zusammengesetzt ist.

Sicherheitslevel und ihre Bedeutung

Um die Gefahr eines Cyberangriffes angemessen und nachhaltig abwehren zu können, muss festgelegt werden, wie mögliche Gefährdungsszenarien klassifiziert werden können bzw. vor welcher Art von Angreifer und Bedrohungen ein Schutz aufgebaut werden muss. Dabei ist zu beachten, dass der investierte Aufwand in einem vernünftigen Verhältnis zu den zu schützenden Zielen steht. Hierzu werden in IEC 62443-3-3 folgende Sicherheitslevel (SL) beschrieben

- **SL-0:** keine Gefährdung durch ungewollte oder fahrlässige Eingriffe (Idealfall, kommt in der Praxis nicht vor)
- **SL-1:** Gefährdung durch zufällige oder fahrlässige ungewollte Eingriffe
- **SL-2:** Gefährdung durch einfache vorsätzliche Angriffe mit begrenzten Mitteln und allgemeinen Kenntnissen
- **SL-3:** Gefährdung durch gezielte vorsätzliche Angriffe mit erweiterten Mitteln durch erfahrene Spezialisten
- **SL-4:** Gefährdung durch gezielte vorsätzliche Angriffe mit umfangreichen Mitteln und Ressourcen durch erfahrene Spezialisten mit hoher Motivation

Entsprechend dieser Klassifizierung kann die gewählte Sicherheitslösung bewertet und ggf. auch später zertifiziert werden. Hierfür werden drei Arten der Sicherheitsstufen festgelegt:

- **SL-T:** die Zielsicherheitsstufe (Target Level), die der Betreiber erreichen will
- **SL-A:** die tatsächlich erreichte Sicherheitsstufe (Achievement Level), die mit den implementierten Maßnahmen aktuell erreicht wird
- **SL-C:** die potenziell erreichbare Sicherheitsstufe (Capability Level), die maximal ohne Einleitung zusätzlicher Maßnahmen mit den vorhandenen Komponenten erreicht werden kann

Wie die einzelnen Schichten konkret implementiert werden, spielt dabei nur eine untergeordnete Rolle. So kann für jede Schicht und jedes Szenario jeweils die am besten passende Strategie bzw. Methode ausgewählt werden.

5. Wirkungsvolle Strategien für Defense in Depth

In Brownfield-Produktionsumgebungen erfolgen Vernetzung und Kommunikation je nach Einsatzzweck und Anwendung über eine Vielzahl an unterschiedlichen Feldbussen und eigenen Protokollen. Während aktuelle Standards wie etwa TSN (Time-Sensitive Networking; Echtzeitfähigkeit) und OPC UA Sicherheitsmechanismen (Security) bereits in ihrem grundlegenden Konzept enthalten, verfügen ältere Protokolle wie etwa Modbus oder BACnet über keinerlei derartige Mechanismen. Es können allenfalls Sicherheitsmechanismen in der Anwendung selbst oder spezielle, ganzheitliche Schutzkonzepte für die benötigte Sicherheit sorgen.

Um einen Angreifer an der Fortbewegung im internen Netzwerk zu hindern, ist die statische Netzsegmentierung (Zones) ein klassisches und bewährtes Konzept. Solche Segmentierungen können physikalisch, logisch (Software, Protokoll) oder gemischt erfolgen. Mit entsprechenden „Wächtern“ an den wenigen Übergängen (Conduits) lassen sich die einzelnen Zonen entsprechend den jeweiligen Anforderungen gezielt absichern. Hierfür können unterschiedliche Methoden wie Filter oder Firewalls zum Einsatz kommen. Solch ein Sicherheitskonzept mit ineinander verschachtelten Zonen mit nur wenigen, exakt definierten Übergängen bezeichnet man in der Cybersicherheit als Zones & Conduits.

Die Kombination mehrerer dieser Sicherheitstechniken in einer Defense-in-Depth-Strategie bietet eine robuste mehrstufige Verteidigung. So können z. B. an den Zonengrenzen verschiedene Arten von Firewalls zum Einsatz kommen (Applikation, Inhalte, Adressen) und innerhalb einer sicher abgeschirmten Zone auch problemlos unsichere alte, aber echtzeitfähige Feldbusse genutzt werden. In einem Brownfield-Szenario lassen sich auf diese Weise komplette Altsysteme als Ganzes sicherheitstechnisch kapseln bzw. nach außen isolieren. Auch kann während einer Fernwartung die Kommunikation zusätzlich eingeschränkt werden, um die mit dem Fremdzugriff verbundenen zusätzlichen Risiken im Griff zu haben. So können die unterschiedlichen Belange der einzelnen Stakeholder (Betreiber, Integrator, Maschinenhersteller) und die verschiedenen Sicherheitsaspekte des konkreten Anlagenbetriebs (Anlagensicherheit, Netzwerksicherheit und Systemsicherheit) jeweils optimal berücksichtigt werden.

Moderne Zero-Trust-Konzepte gehen über statische Netzsegmentierung hinaus und bieten eine granulare und dynamische Absicherung einzelner Dienste, Systeme oder Netzsegmente. Dabei werden Zugriffe kontinuierlich verifiziert und nur die gerade nötigen minimalen Zugriffsrechte durchgesetzt.

6. Chancen der Anomalie-Erkennung in einem OT-Netz

In der IT sind das Beobachten (Monitoring) und Überprüfen des Netzwerkverkehrs auf verdächtige Veränderungen (Anomalie-Erkennung) probate Mittel, um die interne Netzwerksicherheit zu erhöhen. Diese Methoden spielen auch in der OT eine zunehmend wichtige Rolle. Herkömmliche Geräte zur Erkennung von Auffälligkeiten (Intrusion Detection Systems) und zum Schutz vor Angreifern (Intrusion Prevention Systems) können aber nur Auffälligkeiten im Datenstrom selbst feststellen. Bei anscheinend normalen Datenströmen wie etwa Steuer- und Regelbefehlen in der OT können diese Systeme nicht überprüfen, ob diese Befehle von einem berechtigten Benutzer oder einem unbefugten Angreifer abgeschickt wurden.

Insbesondere bei der Absicherung von gewachsenen OT-Netzen empfiehlt sich daher folgendes schrittweises Fünf-Phasen-Vorgehen[2]

Phase 1: Assets katalogisieren

Phase 2: Assets identifizieren

Phase 3: Kommunikationspfade abbilden

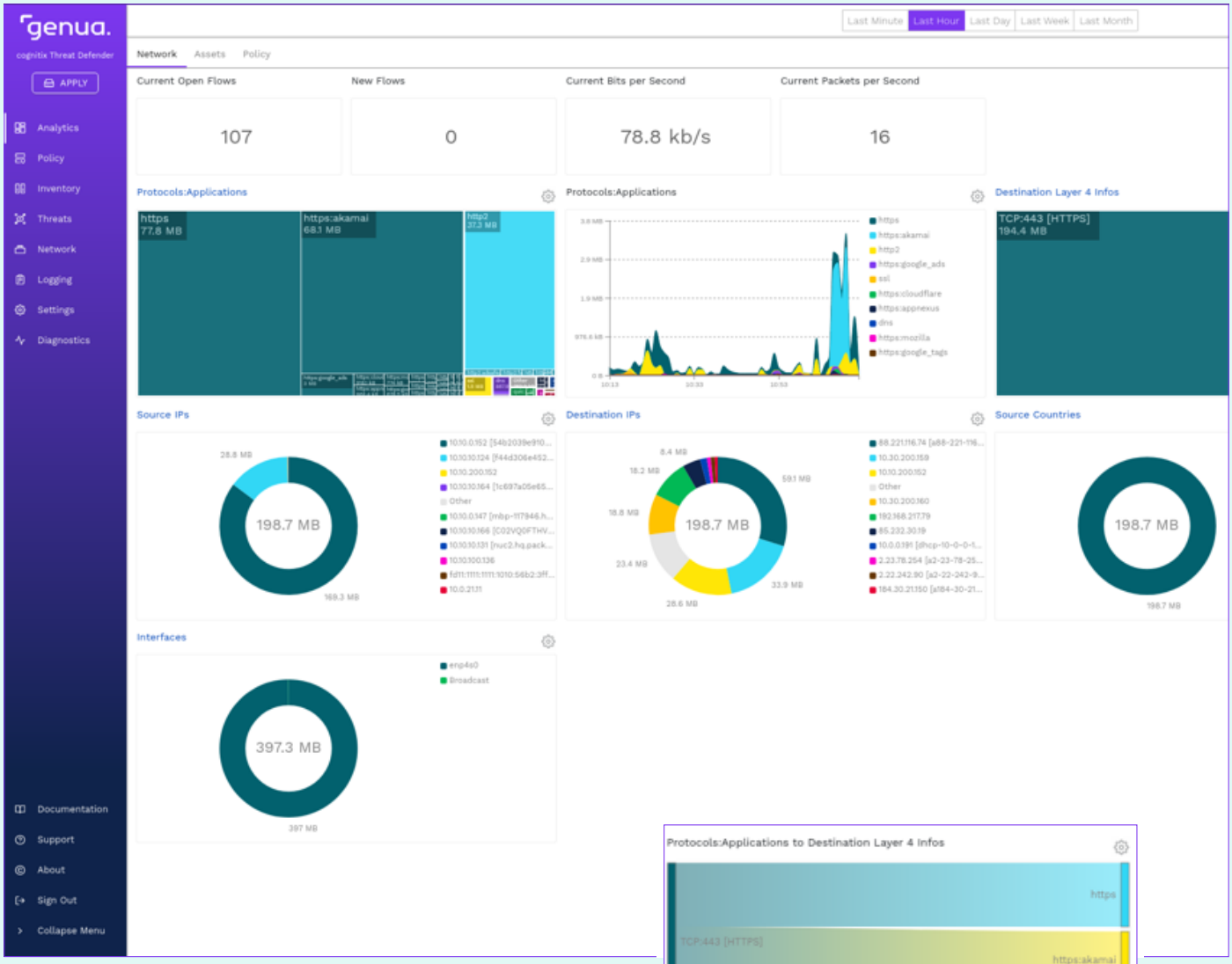
Phase 4: Stabilisierung

Phase 5: Aktives Blocking

Erklärt sei dies an cognitix Threat Defender von genua (Bild 5). Dieser führt zunächst eine Bestandsaufnahme (Asset Detection) durch, welche Geräte im Netzwerk vorhanden sind. Anschließend erfolgt eine Traffic-Analyse, wer im Normalfall mit wem wie viel kommuniziert. Dank Machine-Learning-Algorithmen kann das Gerät nach einer kurzen Anlernzeit selbstständig zwischen Standardereignissen, spontanen, aber legitimen Ereignissen und Bedrohungen unterscheiden und den Datenverkehr in Echtzeit klassifizieren, Anomalien und potenzielle Brüche melden und, wenn gewünscht, automatisiert auf das jeweilige Ereignis reagieren. Das heißt in der Praxis, dass jeglicher Kommunikation definierte Regeln zugeordnet werden können. Der Threat Defender liefert iterativ eine Grundlage für IT-OT-Verantwortliche, auf deren Basis sie ein fein granuliertes Regelwerk (Network Policy) erstellen können, in dem unerwünschte oder unnötige Kommunikation und Dienste unterbunden werden. Zum Beispiel können unerwünschte Protokolle wie Multicast von Anfang an verboten bzw. deaktiviert werden.

In einer nachfolgenden Stabilisierungsphase, in der das System noch nicht oder noch nicht vollständig „scharf“ geschaltet ist, werden das System bzw. dessen Policies praxisgerecht nachjustiert (Finetuning). Sinnvollerweise werden diese ersten Phasen anhand eines gespiegelten Datenverkehrs durchgeführt, um sicherzustellen, dass die Funktion des OT-Netzes nicht durch Latenzen oder Datenverluste durch fehlerhafte Blockierungen gefährdet wird. In einer optionalen letzten Phase legt der Nutzer fest, ob das System bei aktiv erkannten Bedrohungen oder bereits bei unbekannter Kommunikation nur Warnungen bzw. Alarme ausgibt oder den Datenverkehr tatsächlich unterbrechen darf. Wird dieses aktive Blocking des Datenverkehrs tatsächlich erlaubt, ist vorher OT-seitig zu gewährleisten, dass dadurch die Betriebssicherheit der Produktionsanlagen (Safety) zu keinem Zeitpunkt gefährdet ist.

[2] s. a. das Whitepaper „Ein neuer Ansatz für die IT-Sicherheit in Produktionsnetzen“ www.genua.de/fileadmin/campaigns/landingpage-lead-ctd/200820-Whitepaper-cTD-final.pdf



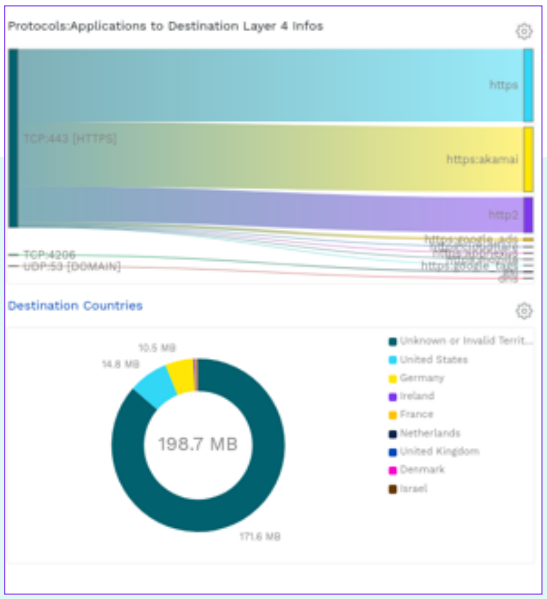


Bild 5: Benutzeroberfläche von cognitix Threat Defender. Sie zeigt, welche Assets im gewählten Zeitraum wie viel Datenverkehr initiiert (Source Assets) bzw. beantwortet (Destination Assets) haben sowie den Datenverkehr zwischen den Assets. Falls zutreffend, werden auch Zwischenfälle nach Assets angezeigt. Basierend auf diesen Analysen können Policies festgelegt, überwacht und durchgesetzt werden.

7. Zero-Trust-Architekturen für die Industrie

Ein typisches Charakteristikum der Industrie 4.0 ist, dass Industrieanlagen häufig durch externe Maschinenhersteller gemanagt werden oder Verbindungen zu fremd verwalteten Diensten haben, z. B. für Cloud Computing. Für die Industrie bedeutet dies einen zunehmenden Kontrollverlust. Die in der IT seit Längerem etablierten Zero-Trust-Architekturen helfen Betreibern, die Netzwerkhoheit über ihre OT zu behalten.

Im Paradigma des Zero Trust Networking wird das Vertrauen in die Sicherheit des Gesamtnetzes durch das Vertrauen in die Sicherheit spezifischer Kommunikationsendpunkte ersetzt, d. h. in Geräte, Dienste und Anwendungen. Eine Kompromittierung einzelner Endpunkte ist damit auf die erlaubten Kommunikationsbeziehungen beschränkt und gefährdet nicht mehr das Gesamtnetz.

Dieses Vorgehen gibt dem Betreiber die Kontrolle über seine Anlagen zurück und senkt proaktiv die Angriffsfläche. Es erlaubt reaktiv auch eine schnellere Detektion und Begrenzung von Schäden sowie eine rasche und gezielte Recovery. Das Resultat sind robustere und resiliente Netze, passend zur höheren Kritikalität und den damit einhergehenden Anforderungen an Zuverlässigkeit und Kontrolle.

Warum Zero Trust?

Der traditionelle Ansatz für das Management digitaler Infrastrukturen bestand bis dato in zentral verwalteten Netzen mit einem einheitlich hohen Sicherheitsniveau. Um die Sicherheit des ganzen Netzes nicht zu gefährden, musste eine Kompromittierung einzelner Teile z. B. durch starke Separation von anderen Netzen unbedingt vermieden werden.

In heutigen Netzen sind jedoch mehr und mehr Systeme durch externe Hersteller und Dienstleister fremd gemanagt bzw. haben notwendige Verbindungen zu fremd verwalteten Netzen etwa für Edge oder Cloud Computing. Dies führt zu einem zunehmenden Kontrollverlust über das eigene Netz: Der traditionelle Ansatz skaliert nicht mit der Realität der Netze und den gestiegenen Anforderungen an Verfügbarkeit und Zuverlässigkeit.

Es gibt mehrere Ansätze, Zero Trust Networking zu implementieren. Die im Folgenden beschriebenen Architekturen sind für die Industrie besonders interessant. Alle Zero-Trust-Ansätze unterscheiden sich primär durch den Ort der Durchsetzung in der Netzwerkinfrastruktur und die damit einhergehenden Möglichkeiten bzw. Limitierungen. Ihnen ist gemein, dass die Entscheidungen basierend auf den Identitäten von Geräten, Anwendungen, Nutzern bzw. Diensten erfolgen, die nicht notwendigerweise an eine spezifische physische Ausprägung gekoppelt sind. Dadurch vereinfacht sich das Management gerade in dynamischen Umgebungen, wie z. B. bei der Anbindung an Cloud-Dienste oder auch bei der Fernwartung von Systemen durch (mobile) externe Dienstleister. Typische Identitäten sind in diesem Umfeld z. B. kryptografische Zertifikate oder Nutzer-Accounts. In eher statischen, kontrollierten Netzen können aber auch klar zugeordnete physische Merkmale wie die MAC- oder IP-Adresse als Identitäten in den Entscheidungen genutzt werden.

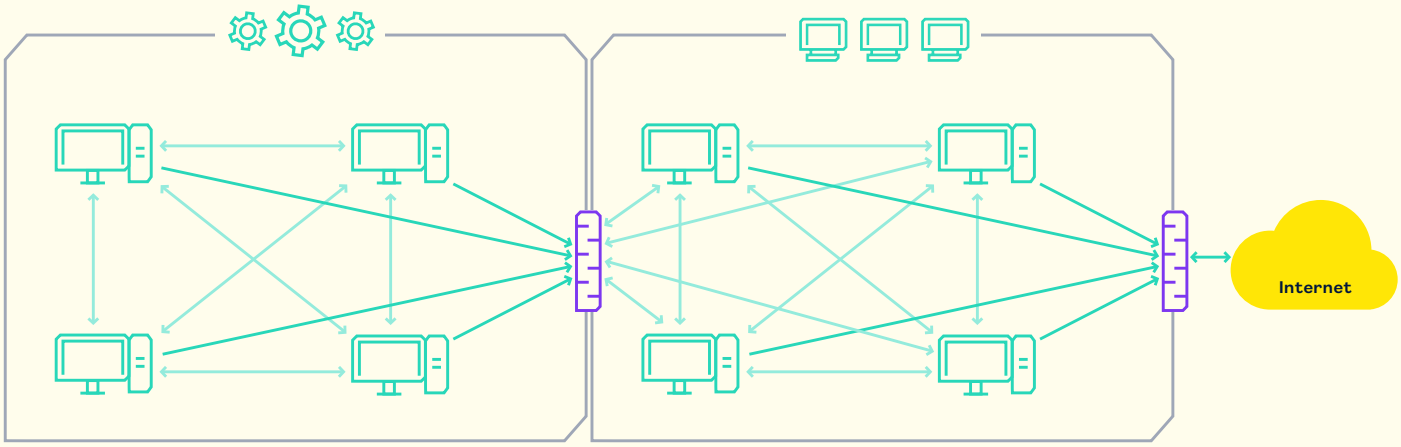


Bild 6: Klassische Koppelung von OT (links) und IT (rechts). Beide Netzwerke werden am Netzwerk-Perimeter bzw. -Übergang durch eine Firewall getrennt, die die mögliche Kommunikation einschränkt. Man kann hier jedoch nicht von einem perfekten Schutz ausgehen, d. h., eine Kompromittierung in der IT kann zu einer Kompromittierung des kompletten OT-Netzwerks führen.

7.1 Zero Trust Networking nach Forrester

Beim Zero Trust Networking nach Forrester wird ein bestehendes Netz in sich selbst durch den Einsatz von Firewalls an strategischen Stellen in Mikrosegmente unterteilt, zwischen denen die Kommunikation reguliert wird. Im Extremfall befindet sich jedes Gerät im Netz in einem eigenen Mikrosegment. Dieser Ansatz eignet sich besonders für eine nachträgliche Härtung bestehender Netze und arbeitet gut mit Legacy-Anwendungen zusammen. Es wird jedoch ein eventuell dynamisches Mapping zwischen Identitäten und IP-Adressen benötigt, da nur diese zuverlässig als Entscheidungskriterium im Datenverkehr sichtbar sind.

Eine zuverlässige Umsetzung der netzbasierten Mikrosegmentierung kann mit dem bereits erwähnten cognitix Threat Defender erreicht werden. Dieser integriert sich transparent wie ein Switch in das Netzwerk, erlaubt dabei aber eine granulare, dynamische und kontextübergreifende Regulierung der Datenströme. Im Gegensatz zu Switches mit Network Access Control (NAC) oder vielen Firewalls finden dabei die Kontrolle und die Restriktion nicht nur auf Netzebene, sondern auch auf Applikationsebene statt. Diese Fähigkeiten werden ergänzt um ein integriertes Intrusion Detection System (IDS) und die Nutzung von Indicators of Compromise (IoC), also Artefakten, die auf eine Kompromittierung hinweisen. Die Ergebnisse können wiederum in die Zugriffsregeln einfließen. Dies ermöglicht es z. B. potenziell infizierte Systeme in Echtzeit zu isolieren oder in ihrer Kommunikation zu beschränken, um Angriffe frühzeitig zu erkennen und angemessen reagieren zu können.

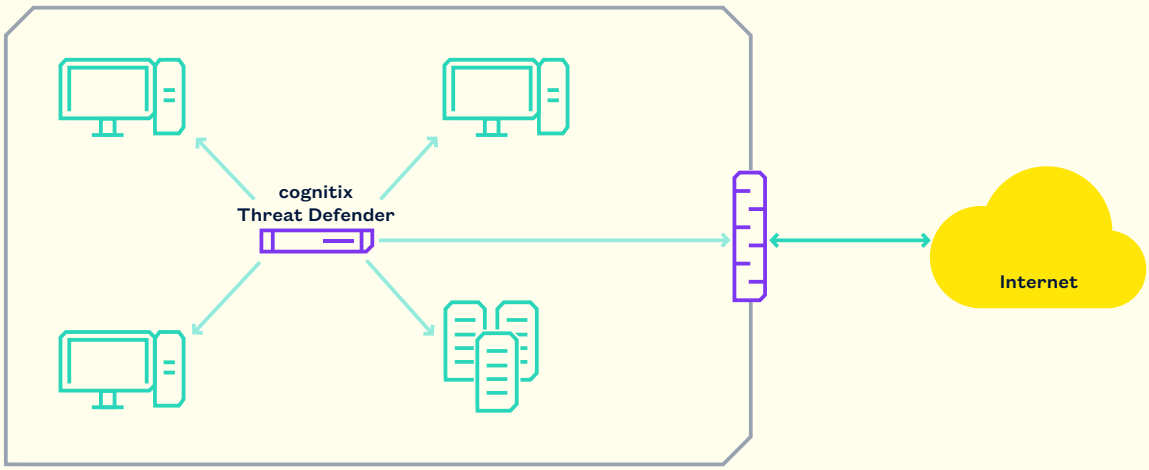


Bild 7: Mikrosegmentierung nach Forrester. Einzelne Dienste oder Geräte werden voneinander abgetrennt und die Kommunikation zwischen ihnen reguliert und überwacht.

7.2 Software-Defined Perimeter

Das Zero-Trust-Networking-Konzept der Cloud Security Alliance (CSA) wiederum ist ein Software-Defined Perimeter (SDP), der externen Clients nach einer Authentisierung Zugriff in eine interne Infrastruktur erlaubt. Im Gegensatz zu einem klassischen Virtual Private Network (VPN) findet hier jedoch keine komplette Netzkopplung statt, sondern der Zugriff ist auf einzelne Dienste beschränkt. Der ursprüngliche Vorschlag der CSA definiert ein spezielles Tunnel-Protokoll zur Verschlüsselung und Übertragung der Identitäten, das die Clients implementieren müssen. Dies erschwert die Anbindung von Legacy-Anwendungen. Alternative Umsetzungen über VPN-Technologien vereinfachen dies, da hier der Tunnel transparent auf Netzebene und nicht auf Applikationsebene realisiert wird.

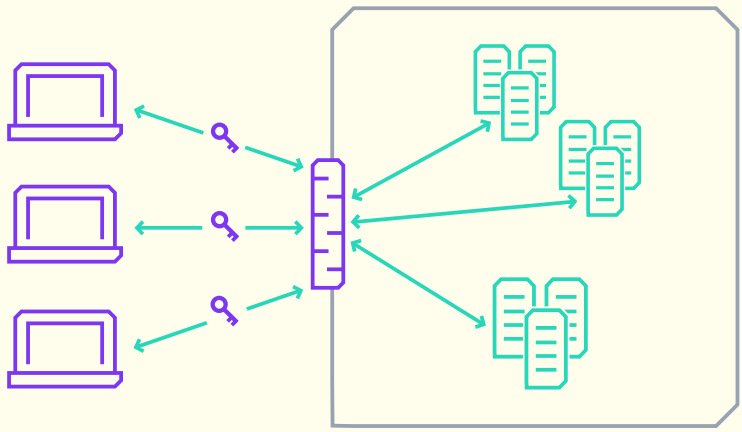


Bild 8: Implementierung eines Software-Defined Perimeters, der externen Clients nach einer Authentisierung Zugriff auf bestimmte Dienste in einer internen Infrastruktur erlaubt.

7.3 Software-Defined Perimeter am Beispiel Fernwartung

Eine an das Konzept des Software-Defined Perimeters angelehnte Lösung ist die Fernwartungslösung genubox von genua. Dabei übernimmt ein Rendezvous Server die Rolle des Software-Defined Perimeters und erlaubt authentisierten externen Anwendern den Zugriff nur auf spezifische Dienste. Hierhin verbindet sich das Zielsystem von innen.

Der Fernwarter wiederum baut ebenfalls eine verschlüsselte Kommunikation zu diesem Perimeter auf. Nach erfolgreicher Authentisierung wird ein Zugriff ausschließlich auf spezifisch benötigte Dienste ermöglicht, wie z. B. auf den Desktop der zu wartenden Maschine, das Terminal oder auf ausgewählte Ports.

Das geschieht nach dem Principle of Least Privilege: Nur das gewünschte Protokoll der Software bestimmt also die Verbindung. Alle anderen Anwendungen oder gar beide Netze werden nicht gekoppelt. Eine Schnittstelle zu Identitäts- und Zugriffsmanagementsystemen ermöglicht die flexible Anbindung der Fernwartung an eine zentrale Benutzer- und Rechteverwaltung.

Entsprechend den erhöhten Anforderungen an Sicherheit und Compliance im Industrieumfeld findet bei der genua-Fernwartung zusätzlich eine Videoaufzeichnung des Desktops bzw. der SSH-Verbindung statt sowie eine Überprüfung übertragener Dateien auf Malware. Diese Aufzeichnungen sind auch nachträglich abrufbar.

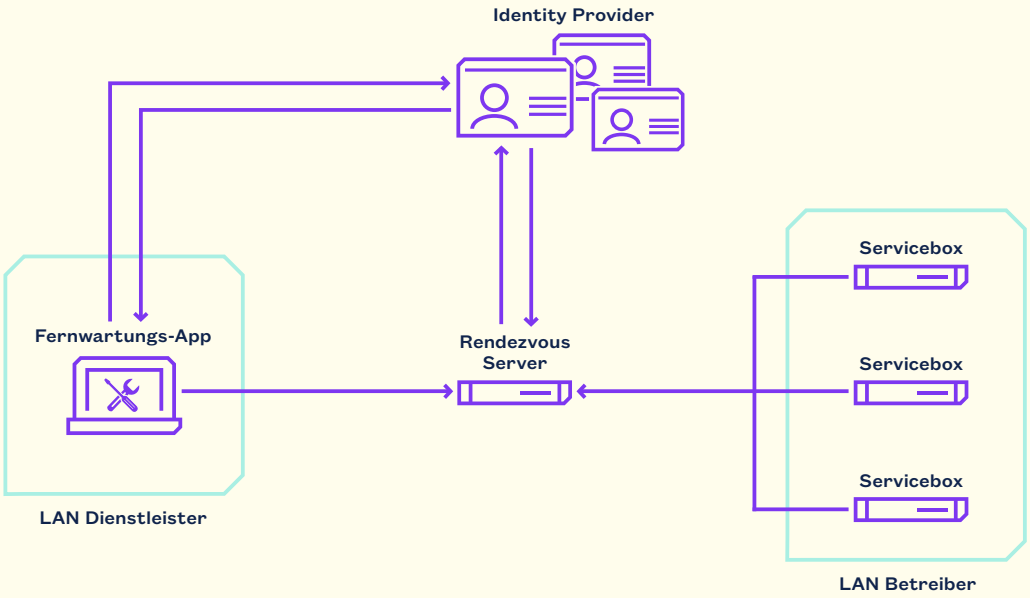


Bild 9: Die Fernwartungslösung von genua unterstützt die Implementierung von Zero-Trust-Konzepten. genubox erlaubt die Anbindung an Identitäts- und Zugriffsmanagementsysteme.

Expertentipp

Sichere Fernwartungsarchitekturen – darauf kommt es an

Markus Maier, Product Owner Industrieprodukte, genua

„Fernwartungszugänge sind beliebte und lohnende Angriffsziele. Die Hauptursachen liegen in ihrer Mehrfachnutzung durch verschiedene Personen bzw. Firmen einerseits sowie fehlender Grundsicherheit und zu reichhaltigen (unspezifischen) Zugriffsmöglichkeiten andererseits. Allgemein sind dabei die folgenden grundlegenden Anforderungen an die IT- und OT-Sicherheit immer zu berücksichtigen.

Aus Perspektive der IT-Sicherheit sollte man unbedingt darauf achten, dass Fernwarter nur Zugriff auf die benötigten Zielsystem-Applikationen erhalten – über sichere und speziell gehärtete Komponenten und nach Multi-Faktor-Authentifizierung. Zusätzlich sollten Applikationsfilter oder auch Application Level Gateways zur weiteren Trennung vorhanden sein. Alle Zugriffe müssen protokollierbar sein und am besten durch ein SIEM-System automatisiert überwacht werden. Im Betrieb ist aus Effizienz- und Sicherheitsgründen ein zentrales Management der erlaubten Fernwartungszugriffe unverzichtbar. Und zur nahtlosen Integration sollten gängige Authentifizierungsdienste unterstützt werden.“

8. Sicherheitsrisiko Mensch

Die besten Sicherheitsmaßnahmen nützen nichts, wenn sie vom Anwender „Mensch“ nicht leicht und benutzerfreundlich gehandhabt werden können. Gelbe Zettel mit dem Passwort oder die Chipkarte für die Zwei-Faktor-Autorisierung unter der Tastatur sind nach wie vor keine Seltenheit. In der OT ist die Ausgangssituation nicht ganz so kritisch, da hier viele Systeme im wörtlichen Sinne „eingebettet“ sind, vielfach auch „headless“, d. h. ohne ständige eigene Benutzerschnittstelle betrieben werden oder eine Bedienung nur über einen Konsolenzugriff vor Ort möglich ist. Hier ist es bei nachträglicher Vernetzung z. B. über Programmierschnittstellen (Application Programming Interface, API) sinnvoll, nach dem Zero-Trust-Prinzip vorzugehen und Zugriffsmöglichkeiten nur solange wie benötigt, nur so privilegiert wie nötig und entsprechend überwacht zu vergeben. An dieser Stelle hilft es nicht nur, durch Schulungen das Problembewusstsein (Awareness) bei den Anwender zu schärfen, sondern konkret auch passende Regeln (Policies) und Prozesse (Procedures) zu etablieren. Auch die Normenreihe IEC 62443 hilft sinnvoll weiter; speziell mit den Normen des Bereichs 2 „Policies and Procedures“ (62443-2-x).

Bild 10: Ein angemessenes Problembewusstsein (Awareness) bei den Mitarbeitern zu schaffen ist wichtiger Bestandteil einer ganzheitlichen und nachhaltigen Cyber-Security-Strategie.

9. Hochsichere Datenausleitung

Besondere Anwendungen mit höchster Schutzklasse stellen Industrieanlagen im Bereich kritischer Infrastruktur (KRITIS) dar. Hierzu gehören bspw. viele teils jahrzehntealte IACS-Systeme in der Energie- und Wasserversorgung sowie in Kernkraftwerken. Diese basieren oft noch auf veralteten Betriebssystemen wie etwa DOS, die schon seit vielen Jahren nicht mehr aktualisiert und gepatcht werden können. Da deren Schwachstellen aber schon sehr lange öffentlich bekannt sind, stellt ein externer Zugriff auf diese Systeme ein vollkommen unkalkulierbares, nicht vertretbares Risiko dar. Trotzdem wird auch hier für eine effiziente Überwachung und Steuerung oftmals ein (Fern-)Zugriff auf die Daten des laufenden Betriebs benötigt. Abhilfe für dieses Dilemma schaffen sichere Datendioden[3]. Sie stellen eine besonders sichere und performante Lösung dar, bei der Daten nur in eine Richtung fließen können. Dabei sind die jeweiligen Netzwerke auch physikalisch völlig entkoppelt, was quasi eine unüberwindbare, absolut sichere Einbahnstraße in Richtung Außenwelt darstellt.

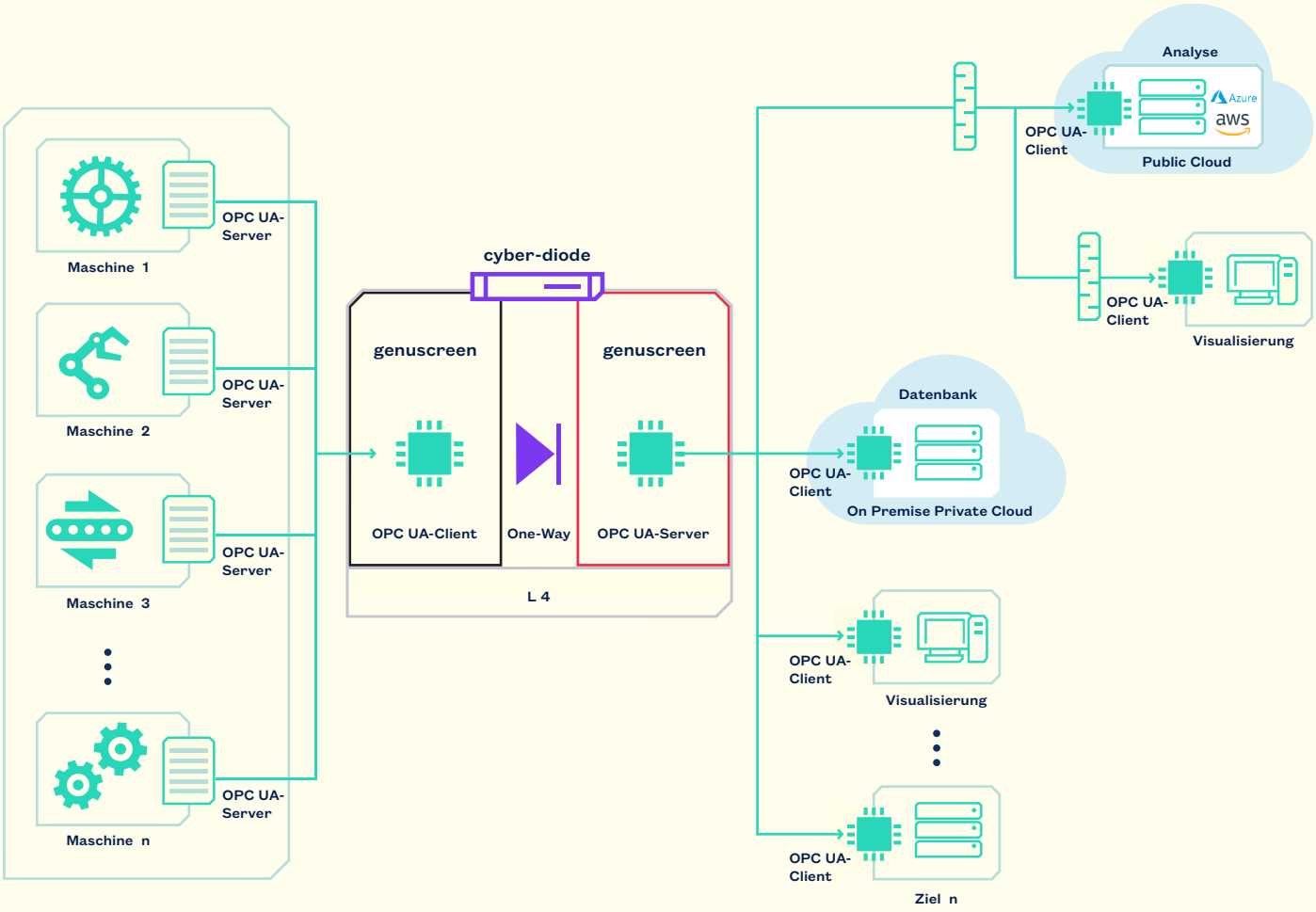


Bild 11: Schaubild für den Einsatz von genua cyber-diode unter Nutzung von OPC UA für die Datenausleitung

[3] s. a. das Whitepaper „Eine industrielle Datendiode für besonders kritische Anlagen und Prozesse“ www.genua.de/knowledgebase/eine-industrielle-datendiode-fuer-besonders-kritische-anlagen-und-prozesse

10. Fazit: Handlungsempfehlungen im Überblick

Mit den richtigen Sicherheitskonzepten und Lösungen lassen sich bestehende Produktionsanlagen in der Automation (Brownfield) gut und effizient gegen Cyberangriffe nachrüsten.

1. Um ausreichende Sicherheit auch bei nachgerüsteten Lösungen zu gewährleisten, ist ein ganzheitliches, typischerweise mehrschichtiges Sicherheitskonzept wie Defense in Depth zwingend erforderlich. Dies beginnt mit einer passenden Segmentierung der jeweiligen Netze und den passenden Geräten an den jeweiligen Übergangspunkten.

2. Der Datenverkehr im Netzwerk muss strengen Regeln folgen, die transparent, bei Bedarf anpassbar und jederzeit auf ihre Einhaltung überprüfbar sind. Zugänge müssen immer verifiziert, auf die jeweils minimal notwendige Funktionalität beschränkt, protokolliert und zentral und benutzerfreundlich verwaltet werden können. Diese Prinzipien stellen auch die Basis für weiterführende Sicherheitskonzepte wie Zero Trust Network Access (ZTNA) dar.

3. Für optimale Sicherheit müssen Netzwerksegmente mit Legacy-Systemen, bei denen eine moderne und vollständige Absicherung z. B. wegen Echtzeitanforderungen nicht oder nur eingeschränkt machbar ist, fein segmentiert und möglichst sicher gekapselt werden. Hierzu sollten modernste Komponenten mit höchstmöglicher Schutzklasse eingesetzt werden. Die Normenreihe IEC 62443 bietet hierzu passende Standards und Strukturierungshilfen an, deren Einhaltung dann auch quantitativ gemessen werden kann.

4. Auch der Mensch bleibt nach wie vor einer der größten Risikofaktoren, kann aber durch geeignete Maßnahmen wie Schulungen und moderne Hilfsmittel wie AI-basierende Systeme und Rendezvous Server wirksam unterstützt werden.

5. Weil die Komplexität der Netzwerke immer höher und die möglichen Angriffsszenarien immer ausgefeilter werden, sind einschlägige Erfahrungen bei der Planung und Realisierung von sicheren Netzwerken unabdingbar. Dies gilt umso mehr, wenn man nicht auf der grünen Wiese (Greenfield) vollkommen neu anfangen kann, sondern aus der vorhandenen Infrastruktur (Brownfield) mit den passenden Erweiterungen das Optimum herausholen muss.

6. Bei neuen Projekten (Greenfield) muss konsequent auf eine sicherheitsorientierte Architektur (Design by Security) und Netzwerke mit Protokollen mit integrierten Sicherheitsfunktionen wie etwa bei OPC UA geachtet werden.

Die Firma genua verfügt über jahrelange Erfahrungen aus Projekten in der Industrie, Prozessautomatisierung und kritischer öffentlicher Infrastruktur (KRITIS). Der IT-Security-Spezialist bietet dafür modernste Sicherheitskomponenten mit höchstmöglichem Sicherheitslevel an.

11. Quellenverzeichnis und weiterführende Informationen

Weiterführende Informationen der genua GmbH

Ein neuer Ansatz für die IT-Sicherheit in Produktionsnetzen
www.genua.de/fileadmin/campaigns/landingpage-lead-ctd/200820-Whitepaper-cTD-final.pdf

Eine industrielle Datendiode für besonders kritische Anlagen und Prozesse
www.genua.de/knowledgebase/eine-industrielle-datendiode-fuer-besonders-kritische-anlagen-und-prozesse

Zero-Trust-Architekturen in der Industrie
www.genua.de/knowledgebase/zero-trust-fuer-die-industrie

cognitix Threat Defender: Moderner Netzwerkschutz mit Artificial Intelligence, Data Analytics und Anomalie-Erkennung im Netzwerk
www.genua.de/it-sicherheitsloesungen/cognitix-threat-defender

Fernwartungslösung genubox: Sichere und komfortable Fernwartung
www.genua.de/it-sicherheitsloesungen/fernwartungs-appliance-genubox

IT-Sicherheitslösungen von genua für die Industrie
www.genua.de/einsatzfelder/industrie

Quellenverzeichnis

Achim Berg: Wirtschaftsschutz 2022, Bitkom e.V.
www.bitkom.org/sites/main/files/2022-08/Bitkom-Charts_Wirtschaftsschutz_Cybercrime_31.08.2022.pdf

Steffen Zimmermann: Leitfaden IEC 62443 für den Maschinen- und Anlagenbau,
überarbeitete Ausgabe 2021, VDMA Verlag
www.vdma.org/cybersecurity (deutsch)

John Nye: Quick Start Guide: An Overview of the ISA/IEC 62443 Standards, 2020
www.isa.org/ISAGCA (englisch)

genua.

Weitere Informationen:

www.genua.de/digitale-industrie

Über genua

Die genua GmbH ist ein Enabler der digitalen Transformation. Wir sichern sensible IT-Netzwerke im Public- und Enterprise-Sektor, bei KRITIS-Organisationen und in der geheimschutzbetreuten Industrie mit hochsicheren und skalierbaren Cyber-Security-Lösungen. Dabei fokussiert sich die genua GmbH auf den umfassenden Schutz von Netzwerken, Kommunikation und interner Netzwerksicherheit für IT und OT. Das Lösungsspektrum umfasst Firewalls & Gateways, VPNs, Fernwartungssysteme, interne Netzwerksicherheit und Cloud Security sowie Remote-Access-Lösungen für mobile Mitarbeiter und Home Offices.

Die genua GmbH ist eine Tochtergesellschaft der Bundesdruckerei-Gruppe. Mit mehr als 350 Mitarbeitern entwickelt und produziert sie IT-Security-Lösungen ausschließlich in Deutschland. Seit der Unternehmensgründung 1992 belegen regelmäßige Zertifizierungen und Zulassungen durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) den hohen Sicherheits- und Qualitätsanspruch der Produkte. Zu den Kunden zählen u. a. Arvato Systems, BMW, die Bundeswehr, das THW sowie die Würth-Gruppe.

genua GmbH
Domagkstraße 7 | 85551 Kirchheim bei München
T +49 89 991950-0 | E info@genua.de | www.genua.de