INDUSTRIAL SECURITY IN DER ENERGIEWIRTSCHAFT

Ein ganzheitlicher Ansatz für OT Security.
Chancen im Energiesektor.

Inhaltsverzeichnis

Industrial Security in der Energiewirtschaft Evolution. Evolution der IT- und OT-Sicherheit im Energiesektor

Einleitung: Versorgung braucht Sicherheit

Cyber-Attacken, die Pipelines, Kraftwerke und andere Strukturen des Energiesektors gezielt ins Visier nehmen, nehmen an Häufigkeit und Präzision zu. Soweit „The Bad News“. Die guten Neuigkeiten:

Wer seine Sicherheitsstrategie an die veränderten Rahmenbedingungen anpassen kann, kann das Risiko eines Ausfalls, gezielte Sabotage oder den Abfluss vertraulicher Daten minimieren. Der notwendige Aufwand und die Komplexität, unter diesen Voraussetzungen noch erfolgreich zu attackieren, lassen die meisten Attacken dann schon in der Anfangsphase „auffliegen“ und/oder scheitern. Wir möchten Ihnen auf den nächsten Seiten einen Überblick verschaffen, welche Rahmenbedingungen für Sicherheit im Energiesektor gelten und wie Ihre Möglichkeiten aussehen, den zunehmenden Bedrohungen effektiv zu begegnen, denn: Die Evolution des Energiesektors hat in den letzten Jahrzehnten an Geschwindigkeit zugenommen und durch die immer stärkere Digitalisierung, Vernetzung, steigende Anzahl der Fernzugriffe und Cloud-Nutzung sind auch die Cyber-Sicherheitsrisiken gewachsen.

Unsere Gesellschaft ist heute mehr denn je abhängig von Elektrizität, verlangt immer mehr nach zusätzlichen, digitalen Dienstleistungen und der Klimawandel erfordert den Wechsel hin zu erneuerbaren Energiequellen, die mitunter dezentral ins Netz gespeist werden. Der Ersatz von Verbrennern durch E-Autos schreitet voran.

Die Folge: Das Stromnetz wird zu Microgrids mit hohem Vernetzungsgrad und komplexer Echtzeit-Steuerung umstrukturiert, Cloud-Dienste werden eingesetzt und das Internet-of-Things-(IoT) ist zu einem Wirtschaftsfaktor geworden, der auch IT und OT immer stärker zusammenwachsen lässt.

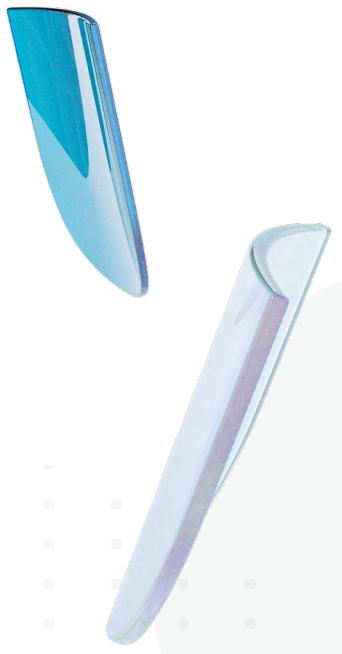
So hat parallel zum Rest der Gesellschaft auch die Digitalisierung der Energiewirtschaft Fahrt aufgenommen und setzt vermehrt auf „intelligente“ Geräte, um die Lieferung elektrischer Energie zu optimieren.

Wer in den letzten Monaten die Presse verfolgt hat, hat eine neue Aggressivität und Häufigkeit von Cyberattacken auf Versorgungsunternehmen wahrnehmen können. Kritische Infrastruktur steht immer häufiger im Fokus teils vermutlich staatlich unterstützter Hackergruppen.

ABER - Meine Botschaft an Sie: Sie haben als Verteidiger die besseren Karten. Allerdings müssen sie diese auch ausspielen.
Wie das geht, möchte ich auf den folgenden Seiten kurz skizzieren.

Es wünscht Ihnen eine informative Lektüre

Bernd Jäger | Olaf Reimann | Andreas Velten
Telekom Security



1. Die Evolution des Energiesektors

Laut Sektorendefinition des BSI ist die Energieversorgung „ein zentraler Bereich Kritischer Infrastrukturen, der sich im Fall von Ausfällen oder Störungen extrem und unmittelbar auch auf die anderen Sektoren und somit auf Staat, Wirtschaft und Gesellschaft auswirkt." Gleichzeitig entwickelt sich der Energiesektor wie jeder andere Wirtschaftszweig weiter und setzt zunehmend auf Vernetzung und Digitalisierung – nicht nur infrastrukturell, sondern auch im Kontakt mit den Endabnehmern. Je tiefer die Vernetzung der verschiedenen Untersysteme jedoch reicht, desto verwundbarer wird auch das Gesamtsystem.

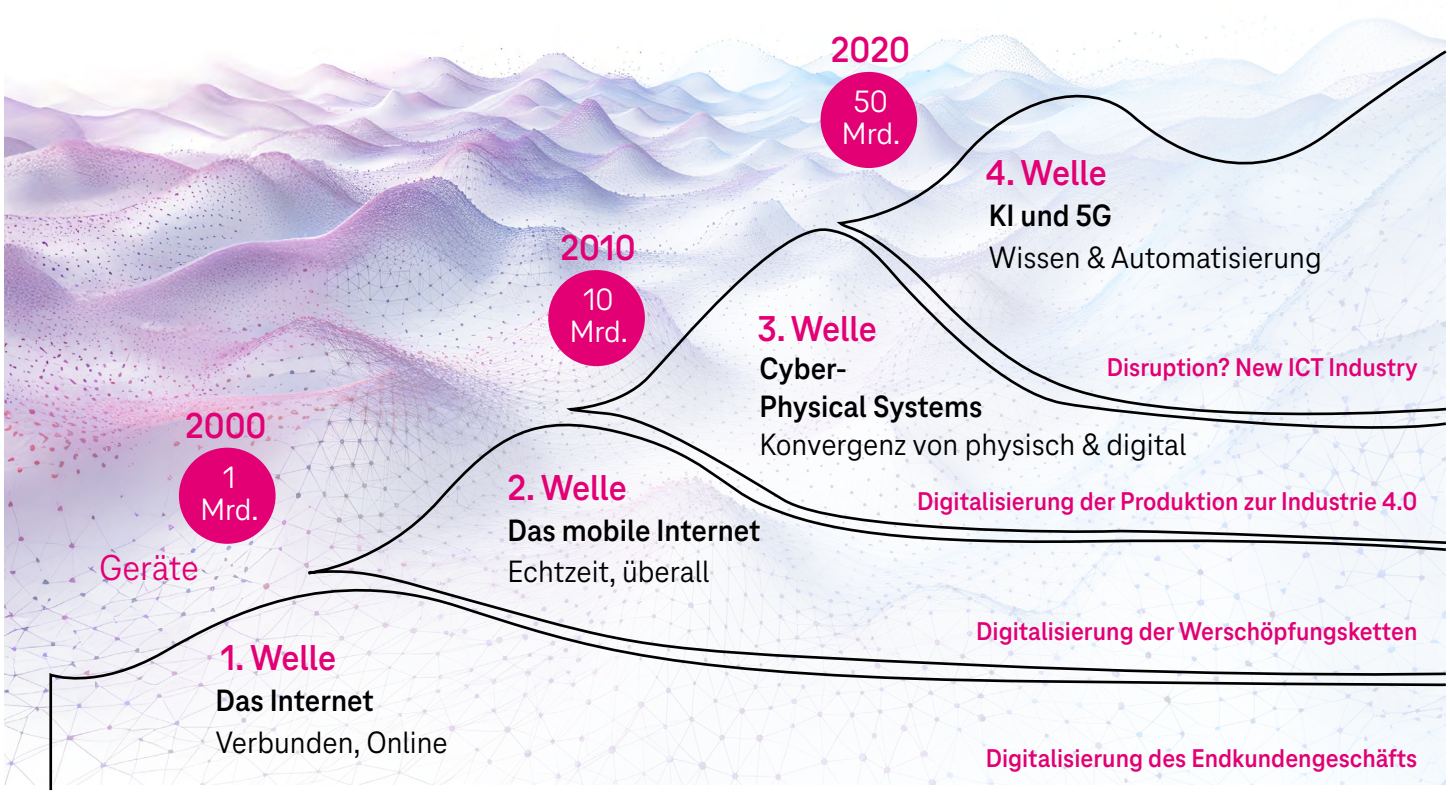
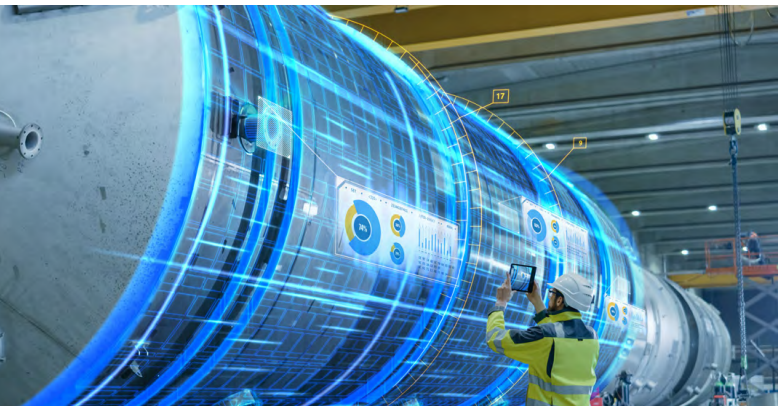


Abbildung 1: Die Entwicklung der Digitalisierung des Energiesektors[1]

[1] https://cps-hub-nrw.de/blog/2018-11-23-ki-der-energiewirtschaft-die-4-welle-der-digitalen-transformation-greift-um-sich

2. Die Evolution der Bedrohung für den Energiesektor



Digitalisierung und Vernetzung verändern viele Aspekte des OT-Prozesses, wie zum Beispiel Architektur, Kommunikationsbedarf, Kerntechnologien und Skills, Betriebsabläufe sowie Risikoprofile und Notfallpläne. Insbesondere die Integration digitaler Lösungen in alte Anlagen kann sie verwundbar für Cyberangriffe machen. Allerdings sind nicht alle alten Industrieanlagen, die vernetzt wurden, automatisch leicht angreifbar. Der „Schwierigkeitsgrad" eines Angriffes hängt auch stark vom Ziel des Angreifers ab: Eine einfache, opportunistische Betriebsstörung gelingt unter Umständen leicht, die gezielte, reproduzierbare Manipulation eines OT-Prozesses hingegen ist oft ein langwieriger Prozess.

Allerdings sind in den letzten Monaten Trends zu beobachten, auf die wir reagieren sollten:

Angreifer entwickeln ein tieferes Verständnis für den OT-Prozess

In den letzten Jahren haben sowohl die Verteidiger als auch die Angreifer gelernt, OT-Prozesse zu analysieren und, zumindest „im Groben", zu verstehen [1]. Hieraus lassen sich kritische Funktionsgruppen wie „Kühlung" oder „Dosierung Chemikalie X" identifizieren und ggf. auch im OT-Netzwerk (nachdem man sich erst einmal Zugang verschafft hat) einer IP-Adresse zuordnen. Das hilft den Verteidigern, von den kritischen Assets ausgehend, gezielte Schutzkonzepte zu entwickeln, aber leider auch den potenziellen Angreifern, genau diese Komponenten zu manipulieren.

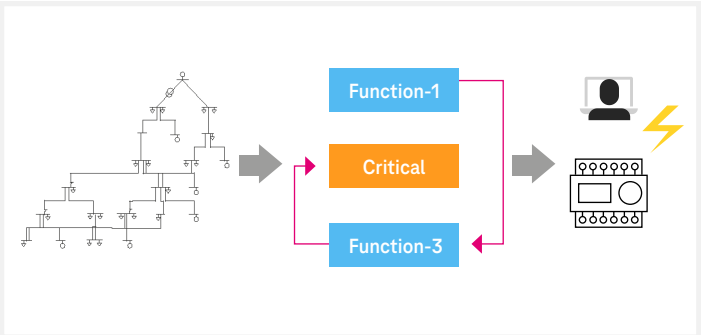


Abbildung 2: Angreifer identifiziert die kritische Komponente im Prozess

Angriffe dringen „leiser" und „tiefer" in OT-Netze vor

Derzeit konzentrieren sich die Cyber-Sicherheitsmaßnamen meist auf die IT-/OT-Übergangszone und den SCADA Layer (Purdue Level 5–2) [2]. Das hat bisher gut funktioniert, weil einerseits viele Angriffsvektoren (veraltete Windows-Systeme und Fremdnetz-Zugänge) hier angesiedelt sind und andererseits Funktionseinschränkungen, die durch die Sicherheitsmaßnamen evtl. ungewollt auftreten, den eigentlichen OT-Prozess typischerweise nicht beeinträchtigen.

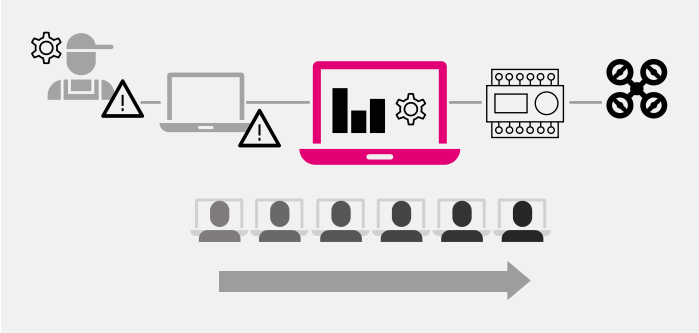


Abbildung 3: Angreifer dringen tiefer in das OT-Netz ein[1]

Hinzu kommt, dass auch für die meisten Angreifer auf diesem Level (Angriff von Windowssystemen mit Standard Windows-Malware und anschließende Manipulation des Prozesses auf einer graphischen Benutzeroberfläche [HMI]) Endstation war. Angriffe, wie der auf dem CISS Event [3] gezeigte „Bit-in-the-Middle" Angriff, zeigen jedoch, dass sich die Angriffe weiterentwickelt haben und Angreifer mit weniger auffälligen und eventuell schon vorhandenen Werkzeugen direkt mit dem „Control-Level" (Purdue Level 1) oder sogar mit Purdue Level 0 Assets (z.B. dem Prozess Zeitgeber [4]) interagieren. Das erweitert einerseits die Möglichkeiten, den OT-Prozess „unauffälliger" zu manipulieren, da es Möglichkeiten gibt, Änderungen auf dieser Ebene vor der Supervisory Application „geheim" zu halten, und andererseits ist die „bösartige" Verwendung von „normale" Werkzeuge wie eine PowerShell auf einem Windows System oder eine Python Library, deutlich schwieriger zu detektieren.

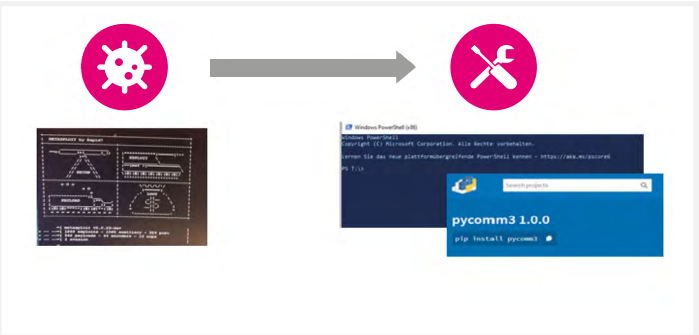
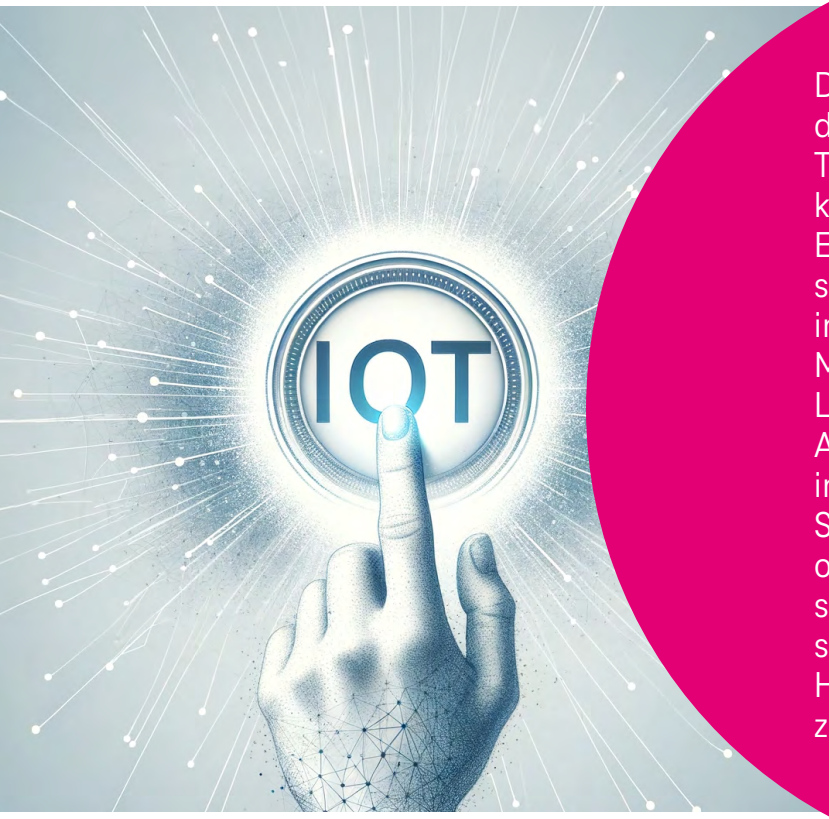


Abbildung 4: Auch im OT Bereich wechseln Angreifer zu weniger verdächtigen Werkzeugen

Angriffe auf die Lieferantenkette und den Energiesektor nehmen rapide zu

Abbildung 5: Sammlung von Meldungen des Telekom Security Cyber Threat Intelligence Teams



Das obige Bild ist nur eine kleine Auswahl an dCERT [5]/CTI Meldungen des Teams der Telekom Security zum Thema Verwundbarkeiten der Lieferkette und Bedrohungen des Energiesektors. Hierbei handelt es sich einerseits um direkte technische Schwachstellen in Software-Komponenten von OT Prozess/Management Technik (Netzwerk-Treiber Library eines Kontrollers), andererseits um die Ausnutzung von Vertrauensstellungen mittels indirektem Angriff der Zielumgebung über Schwachstellen in Dienstleister-Prozessen oder Technologien (zum Beispiel: Schwachstelle in der Management Software für Infrastruktur). Was aber deutlich wird ist, dass die Häufigkeit und Tragweite der Bedrohungen zunehmen

3. Die Evolution der Regulierung

Das im Mai 2021 in Deutschland in Kraft getretene „KRITIS 2.0“-Gesetz (IT-Sig. 2.0) enthielt bereits einige Neuerungen, die helfen konnten, den oben beschriebenen Trends entgegenzuwirken. Dies waren insbesondere:

- **§8a (1a) Angriffserkennung**
- **§2 (9b) Identifikation (und Anzeige) von „Kritischen Komponenten“**
- **§9b Asset Inventarisierung**
- **Kontinuierlich Bedrohungen im laufenden Betrieb mittels Muster erkennen und vermeiden**
- **„Technische Werkzeuge“ wie SIEM – Security Information and Event Management[3]**
- **„Unterstützende Prozesse“ in einem SOC – Security Operations Centre**

Das IT-SiG 3.0, das auf seinem Vorgänger IT-SiG 2.0 aufbaut, nimmt nun mehrere Änderungen und Ergänzungen vor:

Erweiterung des KRITIS Scopes:
Als KRITIS werden nun all jene Unternehmen betrachtet, deren Ausfall **„weitreichende Auswirkungen“** auf die öffentliche Versorgung hätte: das können damit auch kleinere Energieversorger und Stadtwerke sein, aber auch größere Lebensmittelhersteller oder Transportunternehmen.

Erhöhung der Bußgelder:
Strafen für Unternehmen, die beispielsweise wiederholt gegen Meldepflichten verstoßen, können nun mit höheren Bußgeldern (in Höhe von bis zu mehreren Millionen Euro) belangt werden.

Detailliertere Meldepflichten:
Security-Vorfälle wie z.B. ein Ransomware-Angriff müssen nun detaillierter und schneller gemeldet werden. Neben der Art eines Angriffs müssen z.B. auch die vermutete Herkunft und der Schadensumfang angegeben werden.

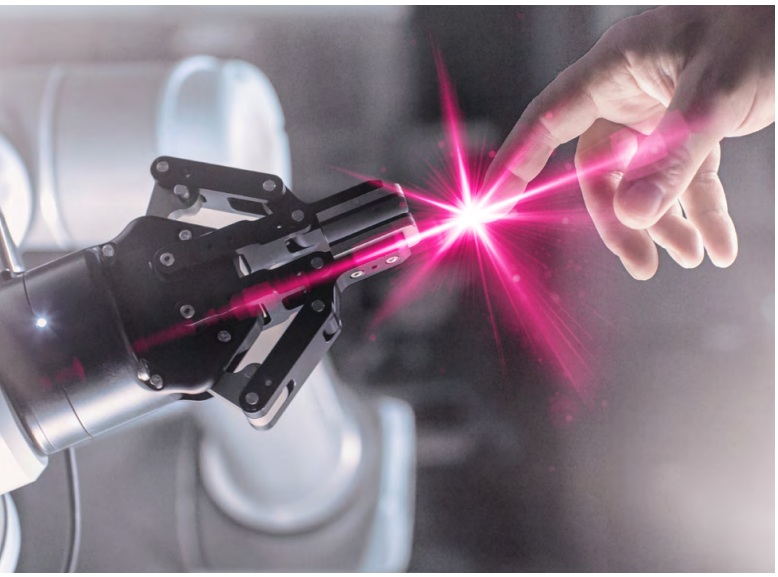
Erweiterte BSI-Befugnisse:
Das IT-SiG 3.0 räumt dem BSI weitreichendere Befugnisse ein, darunter auch unangekündigte Sicherheitsprüfungen oder Audits, um die Compliance der Unternehmen sicherzustellen.

4. Die Evolution der Schutzmaßnahmen

Nicht nur Angriffsmethoden und -werkzeuge haben sich weiterentwickelt. Betrachtet man die Evolution der Threat Detection, also das Erkennen von Bedrohungen und Angriffen, so bringt die zunehmende Nutzung von Methoden wie Machine Learning (ML) insbesondere für die Anomalie-Erkennung in OT-Netzen Vorteile. Unregelmäßigkeiten lassen sich in „traditionellen" Anlagen meist einfach erkennen, da die vorwiegende Machine-to-Machine-Kommunikation dieser Netze strengen, statischen Regeln folgt. In der modernen „Industrie 4.0" gilt dies nicht mehr uneingeschränkt.

Schutzlevel 1: Intrusion Detection Systems – signaturbasiert

Wer lange genug im IT-Security-Umfeld tätig ist, erinnert sich noch an Intrusion Detection Systems (IDS) der ersten Generation, deren Angriffserkennung ausschließlich auf statischen Signaturen basierte. Und wer einmal vor der zentralen Managementkonsole eines solchen Systems gesessen hat, das die Alarme vieler im Unternehmen verteilten Sensoren zusammenführt, erinnert sich vielleicht an den konstanten Strom von Meldungen, der dort an einem normalen Arbeitstag zu sehen war. Aufmerksam wurde man nur, wenn der Eventstrom plötzlich stockte, weil ein Sensor defekt war. Oder wenn sich der Strom beschleunigte und unregelmäßig wurde und sich beispielsweise eine Malware-Infektion im LAN ausbreitete. Es war nahezu unmöglich, aus der Flut von detaillierten Alarmen sinnvolle Informationen für das Ergreifen von konkreten Gegenmaßnahmen, also für die Incident Response, zu gewinnen. Da die rein signaturbasierte Erkennung derzeit nur noch geringe Erkennungsraten hätte, nutzen moderne IDS mittlerweile eine Vielfalt von Detection Engines, die unter anderem auch Machine Learning und Sandboxing beinhalten.



Schutzlevel 2: SIEM-Systeme

Aufgrund der Probleme der ersten Generation entwickelte sich eine zweite Generation von Threat Detection – das Security Information and Event Management (SIEM). Die primäre Aufgabe hierbei ist die Korrelation zahlreicher Security Events aus unterschiedlichen Quellen und die Extraktion von Informationen, aus denen sich konkrete Handlungen ableiten lassen. Die Systeme arbeiten regelbasiert, wobei das Erstellen dieser Regeln Expertenwissen erfordert. Dabei hängt die Qualität der Informationen, die Security-Analysten aus dem System ziehen, stark von der Qualität der Regeln ab. SIEM-Systeme sind heute noch wichtige Bausteine in einer gemeinsamen IT- und OT-Verteidigungsstrategie, da sie die sicherheitsrelevanten Daten aus beiden Welten zusammenführen können.

Schutzlevel 3: Verhaltensmuster analysieren[4]

Die dritte Generation von Threat Detection umfasst Verhaltensmusteranalysen mit Big Data und mathematischen Verfahren wie Machine Learning oder neuronalen Netzen. Hierbei beobachtet und lernt das System das gewöhnliche Verhalten der Anlage und erkennt Abweichungen von den Grundeinstellungen. Während SIEMs aufgrund der hohen Datenmenge die Rohdaten typischerweise für einen Zeitraum von 30 bis 90 Tagen speichern, erlauben die auf Verhaltensmuster basierenden Threat-Detection-Systeme vor allem im OT-Bereich – aufgrund der niedrigen Datenmenge in OT-Netzen – eine Langzeitbetrachtung. Diese kann sogar ein Jahr oder länger dauern, da detaillierte Rohdaten nur zu gewissen Anlässen gespeichert werden.

Schutzlevel 4: Den OT-Prozess verstehen

Die nächste Generation geht einen Schritt weiter und sorgt für OT Process Awareness. Dabei werten Algorithmen die Parameter nicht nur aus, sondern berücksichtigen auch die Zusammenhänge innerhalb der Produktionsabläufe – verfügen also über ein tiefes Verständnis der OT-Prozesse. *Ein Beispiel: Ein Ventil fährt auf einen gültigen Wert, aber diese Einstellung ergibt zu diesem Zeitpunkt im Prozess keinen Sinn.* Wie ausgereift aktuelle Lösungen auf Basis künstlicher Intelligenz (KI) schon sind, wird sich jedoch erst in Zukunft zeigen.

Schutzlevel 5: Die Fernwartung unter Kontrolle bringen

Vor einigen Jahren, als alle Anwendungen und Dienste im eigenen Rechenzentrum untergebracht waren, konnten sich produzierende Betriebe leisten, Themen wie Cloud-Migration oder eine verteilte arbeitende Belegschaft erstmal „hintenanzustellen". Heute ist das nicht mehr möglich. Die Pandemie hat die Unternehmen

[4] Ref to NIST BAD-Paper

gezwungen, Fernarbeit anzubieten, damit die Geschäftsoperationen weiterlaufen und immer smartere Maschinen benötigen immer tiefere Cloud Integration. Unternehmen mit SCADA und ICS System-monitoring prüfen, wie Schlüssel-Assets im Bedarfsfall remote zu erreichen sind.

Für Organisationen ist es unerlässlich geworden, die Business-Kontinuität zu allen Zeiten zu gewährleisten, was bedeutet, dass Remote-Mitarbeiter auch Zugang zu Geschäftsapplikationen und Daten haben müssen. Daher ist es für Energieunternehmen wichtig, den weltweit agierenden Spezialisten (Interne und Externe) häufig oder sogar ständig einen sicheren Zugang zur komplexen und immer smarteren Infrastruktur zu ermöglichen.

Sicherer Remote Access ermöglicht standortunabhängige, tägliche Operationen und Wartung. Bei Störungen des Betriebes verläuft die Fehlerbehebung leichter und schneller. Durch das rechtzeitige Eingreifen können Ausfälle vermieden werden, Spezialisten als knappe Ressource können effektiver eingesetzt werden und auch die Reisekosten sinken. Einige Kollaborations-plattformen vereinfachen außerdem die Zusammenarbeit zwischen Teams und Einzelpersonen.

Aber wie leicht ist es, Remote Access bereitzustellen? Was sollten Organisationen für diese Bereitstellung berücksichtigen?

Angriffe auf Produktionsanlagen erfolgen typischerweise in zwei Phasen:

- In der ersten Phase verschaffen sich die Angreifer Zugang zum Produktionsnetz
- In der zweiten Phase werden dann Systeme infiziert und bspw. verschlüsselt oder sensible Daten entwendet.

Sicherheitslücken bei Remote-Zugängen erkennen und schließen

Gerade in der ersten Phase werden häufig schlecht abgesicherte oder verwundbare Remote- bzw. Fernwartungszugänge ausge-nutzt. Zur gleichen Zeit erfordert die zunehmende Digitalisierung eine stärkere Vernetzung der Produktion mit externen Netzwerken, zum Beispiel für die Integration von Produktionsprozessen in cloudbasierte Anwendungen oder virtualisierte Control-Center.

Sicherheitsrisiken bei Fernwartung: Identifizierung und Überwachung optimieren

Für eine Fernwartungslösung wird üblicherweise das IT-Netz des Unternehmens, in dessen Produktionsumgebung das Fern-wartungsobjekt steht, zum Teil geöffnet. Identifizierung und Authentisierung des zugreifenden Mitarbeiters oder Wartungs-dienstleisters sind meist historisch gewachsen, wenig standardisiert, oft mangelhaft gewartet (Patchen, alte Accounts löschen, sichere Konfiguration ...) und unzureichend überwacht. Fehlende Kontrollmöglichkeiten darüber, welche Arbeiten ein Wartungsdienstleister am Fernwartungsobjekt wann durchführt, stellen einen weiteren kritischen Punkt dar.

Die moderne Lösung mit Proxy-System und End-to-End-Verschlüsselung

Moderne Fernwartungslösungen setzen deshalb auf ein Proxy-System (Rendezvousserver): Ein sicherer Tunnel gewährleistet eine zuverlässige Verschlüsselung, Authentisierung und Autorisierung nach dem AAA-Prinzip (authentication, authorization und accounting). Das ermöglicht, die Gefahr einer unerwünschten Kopplung verschiedener Netze zu vermeiden. Ein Operator kann hierbei Fernwartungen gezielt zulassen und über den Rendezvous-Server einen Ende-zu-Ende Tunnel etablieren, über den ein durch-gängiger und verschlüsselter Fernwartungszugriff stattfinden kann.

Dadurch wird der Fernzugriff nicht nur abgesichert, das Unternehmen wird auch in die Lage versetzt, seiner gesetzlichen bzw. regulatorischen Auskunfts- und Nachweispflicht (bspw. gegenüber dem BSI, Aufsichtsbehörden etc.) nachzukommen und Zugriffe, die über die Plattform getätigt werden, datenschutzkon-form zu überwachen und bei Bedarf aufzuzeichnen.

Bei entsprechender Konzeptionierung der Plattform kann während des Fernwartungsvorgangs zudem das Fernwartungsziel oder Netzwerk isoliert werden, damit ein Wartungsdienstleister von hier aus nicht unerwünscht auf ein anderes Ziel zugreifen kann oder sich potenzielle Malware Infektionen nicht ausbreiten können

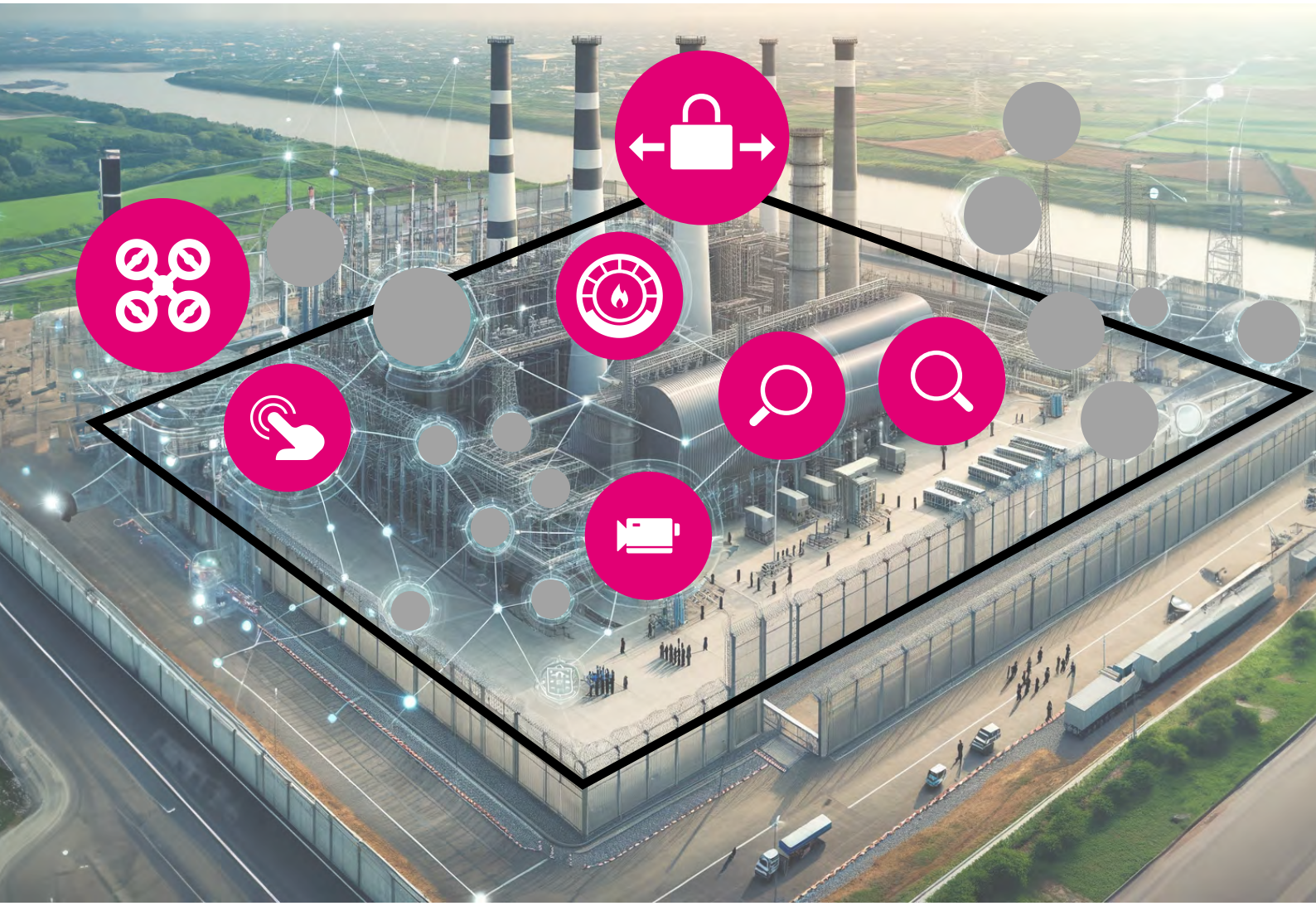
Je mehr Systeme und Anwendungen in naher Zukunft in die Cloud verlagert werden, desto wichtiger werden zudem Techniken, die hier für eine klare Identifizierung und Rechtezuteilung des Zugreifenden sorgen. Zwei-Faktor-Authentifizierung und Zero-Trust-Technologien wie z.B. Privileged Access Management sind Schutzmechanismen, die im IT-Umfeld bereits etabliert sind, durch die Digitale Transformation der Energiewirtschaft aber kurzfristig Einzug in die OT-Landschaft halten werden.

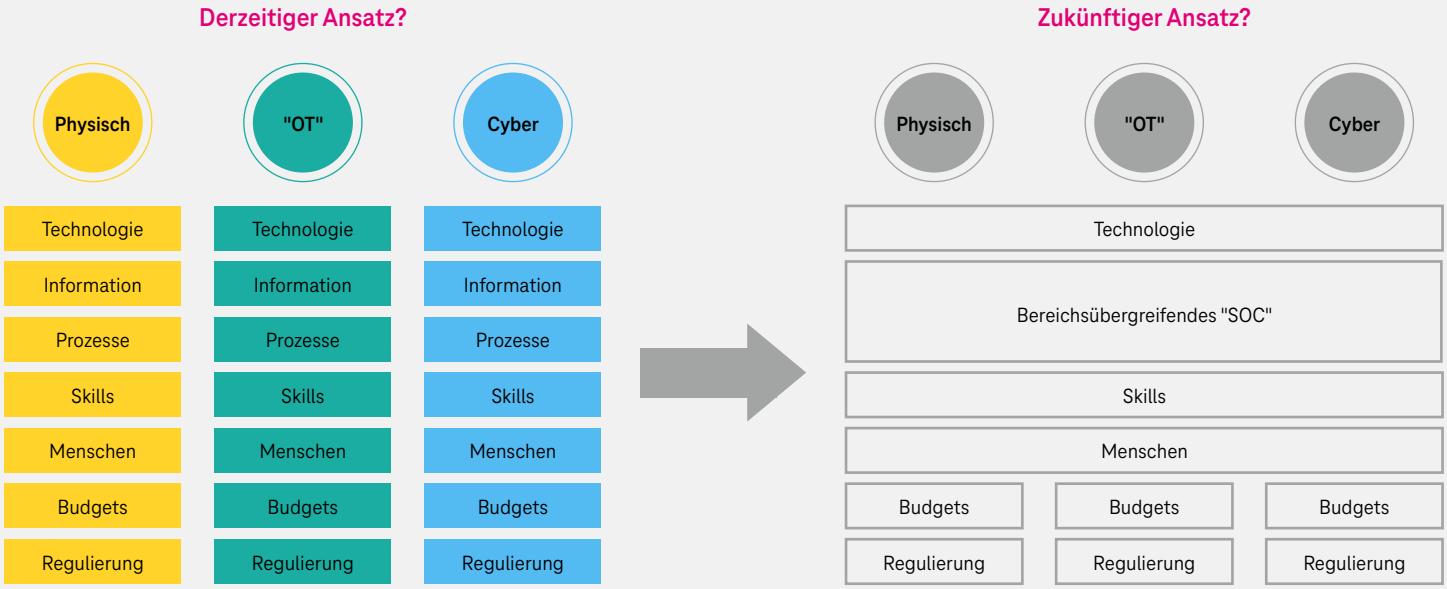
Aufgrund der steigenden Nachfrage nach sicheren Fernwartungs-lösungen und begleitenden Managed Services setzt die Deutsche Telekom in diesem Bereich auf den Magenta Secure Industrial Remote Access Service – kurz MSIRAS – für die sichere Fernwartung in der Industrie (Industrial RAS).

5. Ein ganzheitlicher Ansatz zum Anlagenschutz in der Energiewirtschaft

Der ganzheitliche, wirksame Schutz von kritischer Infrastruktur erfordert koordinierte Konzepte, bei denen Maßnahmen aus verschiedenen „Domänen“ übergreifend umgesetzt werden. So wird kaum jemand die Notwendigkeit, IT- und OT-Security in einem integrierten Ansatz gemeinsam zu betrachten, in Frage stellen. Aber gerade bei Anlagen im Energiesektor, wie zum Beispiel kleineren, abgelegenen Verteilerstationen oder Pumpwerken, darf der Aspekt der physischen Sicherheit nicht „übersehen“ werden. Sie stellt oft das Fundament für Cyber- oder OT-Security dar: Die beste Firewall im Netzwerk nützt mir nichts, wenn der Angreifer sich an einem abgelegenen Ort „einfach“ physikalischen Zugriff auf sein Zielgerät, eine bestimme Leitung, einen Schaltschrank, die Funkstrecke, oder den Signalverstärker in der Glasfaserleitung am Hochspannungsmast verschaffen kann. Jedes verbindende Element in der Prozesskette ist ein potenzieller Angriffspunkt.

Die Grundidee eines ganzheitlichen Ansatzes zum Anlagenschutz in der Energiewirtschaft lautet: „Physische Sicherheit“, „OT-Health“ und „Cyber-Security“ werden nicht länger in Silos betrachtet, sondern in einem Security Operation Center (SOC) zusammengeführt, um Informationen in ihrem Kontext betrachten und bewerten zu können:





Derzeit beauftragen Betreiber einer Anlage zum Beispiel eine Security Firma für die Überwachung des Geländes und der Gebäude. Die Kameras „sprechen“ aber nicht mit dem Cyber-Intrusion-Detection-System und auch die Prozesse, Menschen und ihre Skills zur Alarmbehandlung „berühren“ sich nicht.

Bricht man diese Silos auf und führt die Informationen und Prozesse aller drei Bereiche zusammen, erweitert sich sofort der Blick auf einen größeren Kontext. Das erlaubt es, die Gesamtsituation schneller und besser zu beurteilen:

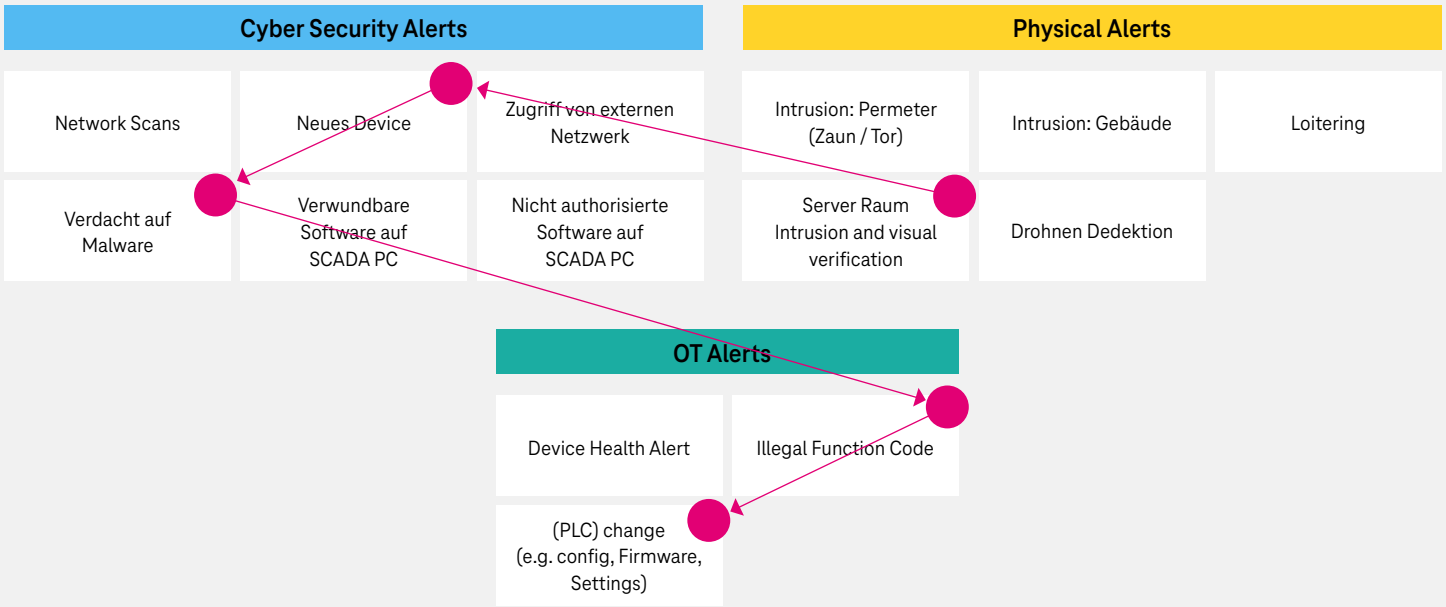


Abbildung 6: Die Ereignisse aus den drei Domänen werden kausal verknüpft

Die Abbildung oben zeigt eine solche Verknüpfung. Ein Physical-Security Sensor (Kamera) detektiert eine Person in einem Serverraum. Anschließend meldet ein Cyber-Security-Sensor ein neues Device im OT-Netz, das sich „verdächtig" verhält (falsche IP, viele SMB Requests, etc.). Als nächstes wird aus der OT-Domäne gemeldet, dass ein ungültiger Parameter in einem Steuerkommando aufgetreten ist und dass sich die Firmware eines Steuergerätes geändert hat. Mit Hilfe der Informationen aus allen drei Domänen lässt sich in kürzester Zeit klären, dass hier ein Techniker eine ungeplante Wartung mit seinem Notebook durchgeführt hat.

In **domänübergreifenden Incident/Response-Modellen** werden die verschiedenen Domänen, von der Technologie-Ebene bis hin zu den IncidentResponse Teams, als Einheit betrachtet. Das heißt, die Informationen von Sensoren wie Video-Überwachungskameras, SCADA-Management-Systemen und Cyber-Security-Sensoren führen ihre Informationen in einem SOAR-System zusammen. In diesem System sind sogenannte Playbooks (Ablaufanweisungen zur Handhabung von Alarmen und Incidents) für übergreifenden Angriffs- oder Störungsszenarien hinterlegt. In den ersten Sekunden nach einem Alarm analysiert ein SOAR System automatisiert diverse Parameter und Daten zur Einschätzung der Kritikalität und des Kontextes der Situation. Das ermöglicht dem eigentlichen Analysten eine schnellstmögliche Einschätzung der Situation und der besten Maßnahmen. Wird zum Beispiel eine Veränderung an der Firmware eines Device im OT-Netzwerk gemeldet, greift die SOAR über APIs in den ersten Sekunden automatisch auf eine Asset-Datenbank zu, um die Kritikalität der betroffenen Komponente und des Prozesses zu bestimmen. Gleichzeitig wird geprüft, ob im entsprechenden Planungssystem ein Wartungsfenster eingetragen ist und ob die Videoüberwachung ggf. eine Person am Standort oder in der Nähe der betreffenden Komponente identifiziert hat. Des Weiteren versuchen die Cyber-Sensoren die Art und das Verhalten der veränderten Komponente zu beurteilen und ggf. Verhaltensmusterabweichungen anzuzeigen. Falls es im Kontext Sinn macht, kann an den SCADA Systemen der „Gesundheitszustand" des OT-Prozesses erfragt werden. All diese Informationen werden zur Beurteilung der Gesamtsituation, soweit möglich automatisiert, zusammengezogen. Dies ermöglicht es schneller und präziser wirklich kritische Situationen zu identifizieren und Entscheidungen auf einer breiteren Datenbasis zu treffen.

6. Ausblick: Was sich im Energiesektor verändern wird

Neue Modelle: Purdue 4.0?

Die „klassischen“ Architektur-Referenzmodelle [2], anhand derer derzeit Risiken und Cyber-Sicherheitskonzepte diskutieren werden, passen noch gut zu den Verteilerstationen, Kraftwerken und Kontrollzentren, die zurzeit in Betrieb sind. Betrachtet man die Entwicklung aus Abbildung 1 im Kontext der Energiewende und der weiteren Digitalisierung unserer „cyber-physischen“ Welt, in der Anlagen, Netzwerke und Smartgrid-Teilnehmer auf 5G-Basis vernetzt und virtuelle Control-Center als eine Instanz in der Cloud implementiert sind, könnte die Erweiterung der Modelle um einen „IoT-Anteil“ sinnvoll sein (Abbildung 8). In diesen Modellen ist zum Beispiel der „Device“-Layer besonders interessant und zukünftige Sicherheitskonzepte könnten unter anderem auf „Schwarmintelligenz“-Mechanismen und einem dynamischen „Vertrauens-Rating“ der Devices untereinander basieren, so dass „kritische“ Operationen nur mit Nachbar-Devices mit einem hohen „Trust-Rating“ durchgeführt werden.

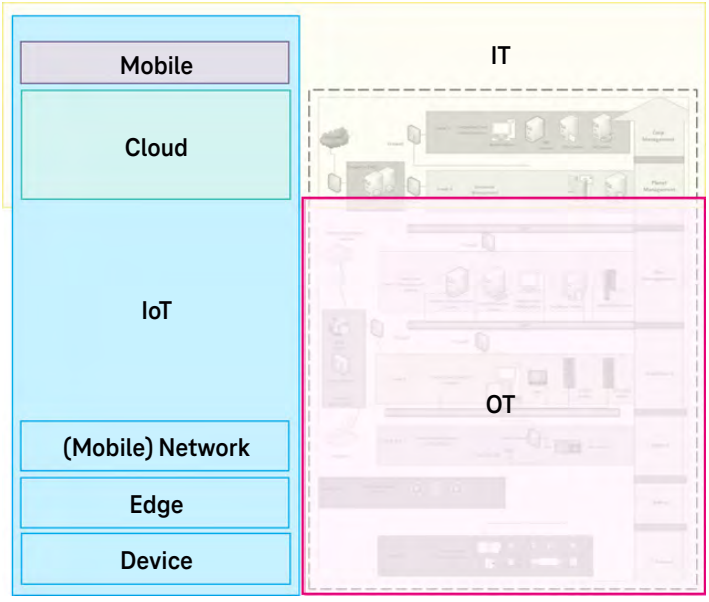


Abbildung 8: Erweiterung des klassischen Purdue Models um einen "IoT Anteil"

Cloud-Nutzung
Laut einer SANS-Studie [6] nutzten bereits in 2021 schon 49,2% der Betreiber die Cloud für „Monitoring, Konfiguration und Analyse“. Diese massive Nutzung auch jenseits der reinen Analyse dürfte die meisten Security-Experten überrascht haben. Da es unwahrscheinlich ist, dass sich dieser Trend kurzfristig ändert, muss Cloud-Security zu einem integralen Bestandteil von OT-Sicherheitskonzepten werden. Es muss also mit der „OT-Brille“ auf das Thema Cloud-Security geschaut werden. In den Risikoprofilen müssen beispielsweise die Auswirkungen eines modifizieren Konfigurationsfiles am Standort der Anlage betrachtet werden oder die Auswirkungen einer „relativ simplen“ (D)DoS-Attacke und der aus ihr resultierenden „Nicht- Verfügbarkeit“ einer Cloud-Komponente.

[5] DDoS: Distributed Denial of Service

7. Fazit

Mit der noch tiefergehenden Digitalisierung der Energieindustrie geht zwangsläufig eine Vergrößerung der Angriffsflächen von Organisationen einher – aber welche Maßnahmen können gewährleisten, dass der Zugang zu sensiblen Netzwerken und Systemen beschränkt bleibt? Daher ist SASE ein sinnvoller Baustein bei der Implementierung eines Schutzprogramms in der modernen Produktion.

Diese Lösungen hindern Cyberkriminelle daran, in das Netzwerk einzudringen und die Kontrolle über kritische Assets zu erlangen. Der gesamte OT-spezifische Datenverkehr kann durch kontinuierliche Überwachung gesichert werden und Bedrohungen lassen sich erkennen. Mit einer SASE-basierten Lösung erreichen OT-Organisationen operative Effizienz durch die Konsolidierung der Administration und des Managements über OT und IT hinweg. Daraus ergibt sich eine Reduzierung der operativen Kosten.

Die Security-Dynamik ist in vielen Bereichen des Energiesektors hoch. Neue Prozess-Technologien, Angriffstaktiken und Verteidigungsmaßnahmen sind ebenso Treiber einer stetigen Evolution wie die Veränderungen der rechtlichen Rahmenbedingungen und die Entstehung neuer Businessmodelle. Sie alle steigern die gegenseitigen Abhängigkeiten und führen zu einer größeren und wachsenden Komplexität der Gesamtsysteme.

Trotzdem sind viele Verteidiger ausreichend mit wirkungsvollen Konzepten, Prozessen, Technologien und Know-how ausgerüstet, um den OT-Security-Herausforderungen zu begegnen. Schon mit ein paar Basis-Elementen wie etwa Sensoren für die Transparenz und Sichtbarkeit der Vorgänge in der Anlage (Physical, Cyber und OT), einer smarten (Netzwerk-)Segmentierung rund um den OT-Prozess, einem gepflegten Asset-Register und einem Prozess zur Reaktion auf Alarme lassen sich die Risiken in diesem dynamischen Umfeld deutlich reduzieren.

Und nicht zuletzt besitzen die Verteidiger den „Heimvorteil“! Sie kennen sich in ihren Anlagen besser aus als die Angreifer und sind (unter anderem mit Unterstützung durch externe Dienstleister) daher oft einen Schritt voraus.

Quellen

[1] **O. J. Delgado, „Unit Operations for ICS security professionals (one big and expensive Lego),“ [Online].** Available: https://www.sans.org/presentations/unit-operations-for-ics-security-professionals-one-big-and-expensive-lego/

[2] **P. Uni, „Purdue Ref. Architecture Model,“ [Online].**
Available: http://www.pera.net/Pera/PurdueReferenceModel/ReferenceModel.html

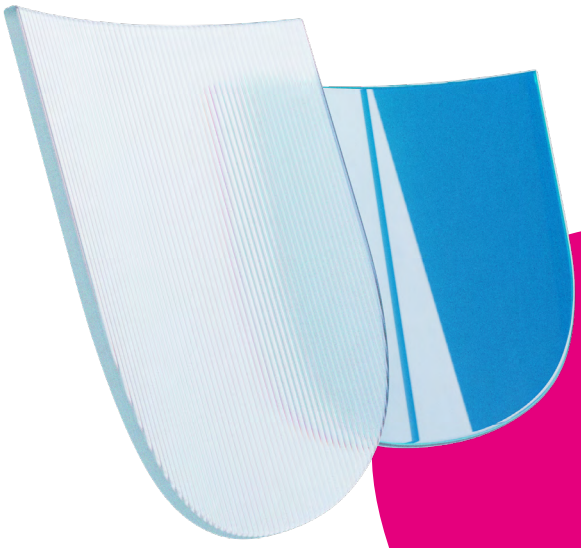
[3] **CISS, „Critical Infrastructure Security Showdown 2020,“ [Online].**
Available: https://itrust.sutd.edu.sg/ciss/ciss-2020-ol/

[4] **J. S. Tim Conway, „Killing Time,“ [Online].**
Available: https://www.youtube.com/watch?v=2iV-KuGQtgU

[5] **dCERT, „dCERT Telekom Security,“ [Online].**
Available: https://www.dcert.de/

[6] **SANS, „A SANS 2021 Survey: OT/ICS Cybersecurity,“ [Online].**
Available: https://www.sans.org/white-papers/SANS-2021-Survey-OTICS-Cybersecurity/

Deutsche Telekom Security GmbH | 02/2024



Kontakt
E-Mail: security@telekom.de
Web: security.telekom.de

Herausgeber
Deutsche Telekom Security GmbH
Office Port 1
Friedrich-Ebert-Allee 71–77
53113 Bonn

Connecting your world.