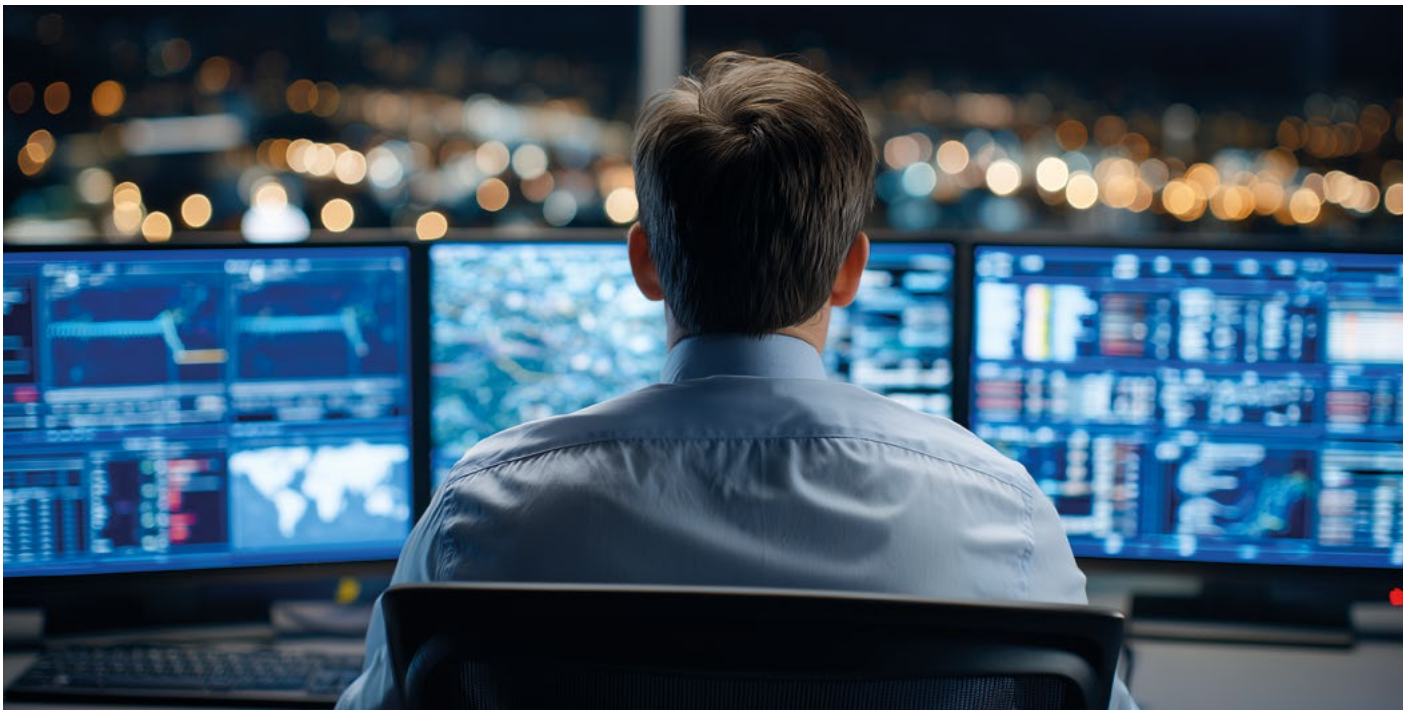


Quelle: AdobeStock 1541392573

OT-Security in der Energieversorgung

Vom Perimeterschutz zum kontinuierlichen Exposure Management

Energieanlagen werden digitaler, vernetzter und damit angreifbarer. Gleichzeitig bleiben Verfügbarkeit und Betriebssicherheit unverzichtbar. Klassische Schutzkonzepte, die auf Perimetersicherheit setzen, stoßen an ihre Grenzen. Entscheidend ist ein kontinuierlicher Blick auf Assets, Kommunikationsbeziehungen und reale Angriffspfade bis hin zu Continuous Threat Exposure Management.

Umspannwerke, Leitstellen und Schaltanlagen sind auf Stabilität ausgelegt. Die Betriebstechnik (OT) in der Energieversorgung ist historisch gewachsen. Viele Komponenten sind auf lange Lebenszyklen ausgelegt, Änderungen erfolgen kontrolliert, Wartungsfenster sind knapp. Der Betrieb ist auf Stabilität optimiert. Lange galt das als Sicherheitsvorteil: Wer nicht am Netz hängt, ist schwer angreifbar – so die Logik.

Doch diese Zeiten sind vorbei. IT/OT-Konvergenz, Fernwartung, externe Dienstleister, Smart Grids und Datenschnittstellen erhöhen die Vernetzung – und damit die Angriffsflächen. Gleichzeitig steigen die Anforderungen an Cyberhygiene und Nachweise, zum Beispiel durch BSI-Vorgaben oder NIS 2. Für Kritis-Betreiber bedeutet das: Sicherheit ist kein Projekt mit Enddatum, sondern ein fortlaufender Prozess.

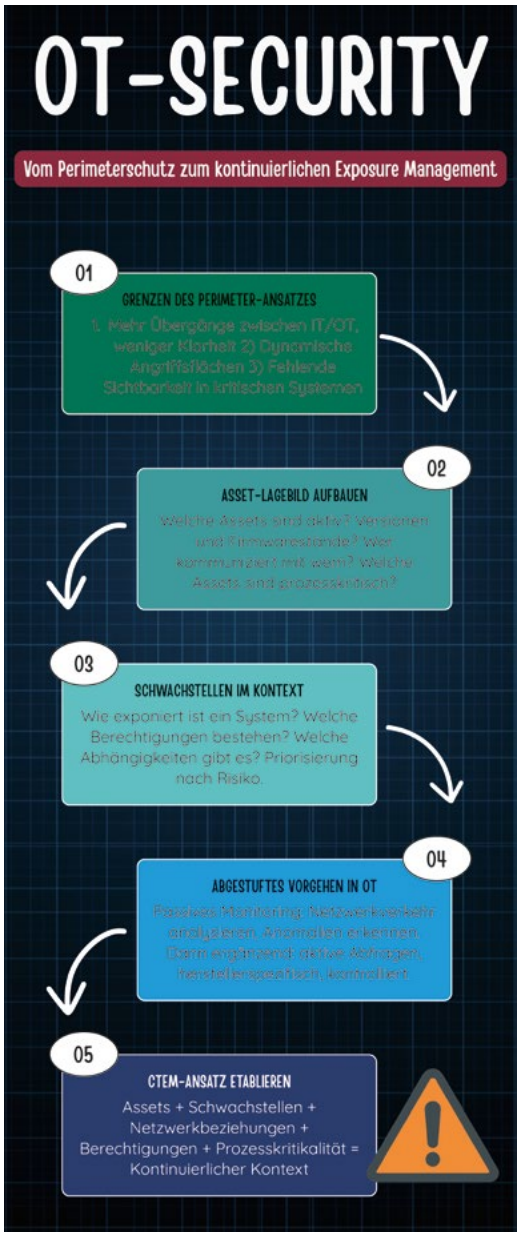
Perimeterschutz bleibt Pflicht – reicht aber nicht mehr aus

Zwar bleiben Firewalls, Endpoint Protection, physische Sicherheit und Segmentierung entscheidend. Sie mindern Standardrisiken und bilden die Basis jeder Sicherheitsarchitektur. Die entscheidenden Fragen moderner OT-Sicherheit beantworten sie indes nicht: Was passiert im Inneren? Wo liegen Schwachstellen? Welche Kombinationen eröffnen Angriffspfade?

Drei Entwicklungen zeigen die Grenzen des Perimeter-Ansatzes:

1. Mehr Übergänge, weniger Klarheit
Übergänge zwischen IT und OT entstehen durch Fernzugänge, Datenabflüsse, Reporting-Schnittstellen oder gewachsene Strukturen. Der Perimeter wird dadurch »porös« – oft ohne vollständige Transparenz im Betrieb.

2. Dynamische Angriffsflächen
Neue Komponenten, geänderte Regelwerke, zusätzliche Dienstleisterzugänge:



Quelle: telent

Fünf Schritte zum kontinuierlichen Exposure Measurement

Selbst kleine Änderungen verschieben Risiken. In der heterogenen OT mit ihren langen Lebenszyklen bleibt das schwer zu überblicken.

3. Fehlende Sichtbarkeit
Betreiber kennen oft ihre Netzübergänge, aber nicht das vollständige Bild ihrer OT-Assets und deren Kommunikationsbeziehungen. Doch genau diese Transparenz ist nötig, um Risiken sinnvoll zu priorisieren.

Audit-Listen sind keine Sicherheitsstrategie: Der Kampf um das Asset-Lagebild

Admins erstellen ihre Asset-Inventare oft manuell. Typisch sind Excel-Listen, die für Audits aktualisiert werden, aber kein kontinuierlich gepflegtes Lagebild liefern. Für Kritis-Umgebungen ist das riskant, da Betrieb und Sicherheit immer enger verknüpft sind.

Wer ein belastbares Lagebild haben will, muss klären, welche Assets aktiv sind, einschließlich »vergessener« Legacy-Komponenten. Er braucht einen Überblick über Versionen und Firmwarestände. Genauso muss er wissen, wer mit wem im Netz – und warum – kommuniziert. Ebenfalls wichtig: Welche Assets sind prozesskritisch (zum Beispiel Schutz- und Leittechnik)?

Ohne dieses Wissen bleibt der Betrieb im »Blindflug«: Einzelne Events am Perimeter werden sichtbar, der Kontext, in dem Risiken entstehen, bleibt jedoch verborgen. Man reagiert auf Ereignisse, statt Risiken planbar zu reduzieren.

Schwachstellenmanagement: Ohne Kontext oft nutzlos

Klassisches Vulnerability Management priorisiert Schwachstellen nach CVE- oder CVSS-Werten. Dies liefert wichtige Signale, reicht in der OT aber nicht aus. Entscheidend ist, wie sich eine Schwachstelle in der realen Umgebung auswirkt. Dafür müssen zentrale Fragen geklärt werden: Wie gefährdet ist ein System? Ein exponiertes System ist anfälliger als eines in segmentierten Bereichen. Welche Berechtigungen bestehen? Wer hat Zugriff, und welche Rolle spielt das Asset im Prozess?

Wer die Abhängigkeiten kennt, zum Beispiel zu zentralen Steuerungsknoten, kann besser einschätzen, welche Kombinationen Angreifern effektive Angriffspfade eröffnen. Und wo der Schutz besonders stark sein muss.

Ein weiteres Problem sind die Silos in arbeitsteiligen Organisationen. Netzwerk, OT, Server und Web-Anwendungen haben oft getrennte Zuständigkeiten. Angreifer nutzen genau diese Schnittstellen zwischen Domänen: Nicht »eine« Lücke führt zum Durchbruch, sondern eine Kette aus ungepatchten Systemen, ungünstigen Berechtigungen und unsauberem Regelwerk.

Warum »einfach scannen« in der OT keine Option ist

In der IT ist aktives Scannen etabliert. In der OT ist es heikler: Viele Legacy Komponenten sind empfindlich, und aktive Abfragen können im schlimmsten Fall zu Störungen oder Ausfällen führen. Im Kritis-Kontext ist das inakzeptabel.

Bewährt hat sich ein abgestuftes Vorgehen: zunächst passiv beobachten, dann gezielt aktiv ergänzen. Praktisch bedeutet das, passives Monitoring zu etablieren und im Zuge dessen kontinuierlich den Netzwerkverkehr zu analysieren, Kommunikationsbeziehungen zu prüfen und Anomalien zu erkennen. Ergänzende aktive Abfragen erfolgen nur dort, wo es vertretbar ist, herstellerspezifisch, kontrolliert und schrittweise. So entsteht eine verlässliche Datenbasis. Entscheidend ist dabei die Erfahrung in der OT: Der Administrator muss einschätzen können, welche Komponenten sich gefahrlos abfragen lassen und wo Vorsicht geboten ist. Telent unterstützt Betreiber dabei, solche Ansätze in bestehende Netzarchitekturen und Abläufe zu integrieren.

Durch dieses Vorgehen gewinnen Betreiber Transparenz, ohne den Betrieb zu gefährden, und können fundierter entscheiden, welche Systeme wie bewertet werden müssen.

Vor allem im Kritis-Umfeld zeigt sich der Nutzen schnell. Betreiber erhalten nicht nur eine Momentaufnahme, sondern einen kontinuierlichen Überblick. Sie erkennen, welche Systeme extern erreichbar sind, welche Dienste sichtbar werden und wo Schwachstellen oder Fehlkonfigurationen lauern. Das erleichtert die Priorisierung. Statt Maßnahmen nach Alarmpegeln abzuarbeiten, lässt sich gezielt entscheiden, was wirklich gefährlich ist. Ein moderates Problem an einer exponierten Schnittstelle kann so schneller in den Fokus rücken als eine formell hoch bewertete Schwachstelle tief im segmentierten Netz. Frühzeitige Maßnahmen senken das Risiko erfolgreicher Angriffe, indem Schwachstellen geschlossen oder durch andere Schritte entschärft werden.

Bedrohungsbild: Mehr Erkundung, mehr Automatisierung, mehr Social Engineering

Immer häufiger tasten Angreifer Systeme von außen ab. Sie wollen herausfinden, welche Produkte sichtbar sind, welche Dienste reagieren, und welche Fehlkonfigurationen auffallen. Oft handelt es sich dabei noch nicht um Angriffe, sondern um systematisches »Information Gathering«.

KI verstärkt diesen Trend: Sie senkt die Einstiegshürden für einfache Angriffe. Spear-Phishing wird überzeugender, Identitäten und Materialien lassen sich leichter erzeugen, und einfache Tools

sind schneller verfügbar. Hochkomplexe Angriffe bleiben Spezialisten vorbehalten, doch die Zahl opportunistischer Versuche steigt.

CTEM: Vom Befund zur Risikologik – kontinuierlich und kontextbasiert

Hier setzt Continuous Threat Exposure Management (CTEM) an. CTEM ist kein Einzelsystem, sondern ein methodischer Rahmen, der technische und organisatorische Informationen zusammenführt. Es erweitert den Blick über klassisches Schwachstellenmanagement hinaus: Assets, Schwachstellen, Netzwerkbeziehungen, Berechtigungen und Prozesskritikalität werden in einen gemeinsamen Kontext gesetzt. Das geschieht kontinuierlich, nicht nur punktuell.

Ziel ist es, Risiken entlang realer Angriffspfade zu priorisieren. Welche Kombinationen ermöglichen einen plausiblen Angriffspfad? Wo lohnt sich eine Maßnahme am meisten?

Für Kritis-Betreiber ist das besonders wichtig, da »Patchen« oft nicht schnell genug oder gar nicht möglich ist. Gründe dafür können Legacy-Systeme, Freigabeprozesse oder Wartungsfenster sein. CTEM unterstützt daher auch alternative Maßnahmen wie Härtung, angepasste Segmentierung, bereinigte Regelwerke, reduzierte Berechtigungen oder auch verbessertes Monitoring.

Der Mehrwert liegt nicht in der Masse gefundener Schwachstellen, sondern in einer betriebsnahen Risikologik: CTEM hilft, plausible Angriffspfade zu erkennen und Maßnahmen so zu bündeln, dass sie das Risiko messbar senken. Das kann bedeuten, Exponiertheit zu reduzieren, Segmentierung nachzuschärfen, Rechte zu minimieren oder die Detektion zu verbessern, je nachdem, welche Abfolge im konkreten Umfeld am wahrscheinlichsten ist.

Wo Patches nicht sofort möglich sind, schafft CTEM Handlungsfähigkeit: Risiken lassen sich durch gezielte Schritte verringern, statt reflexartig auf jede neue Meldung zu reagieren.

Typische Stolpersteine – und wie man sie vermeidet

CTEM scheitert oft an praktischen Hürden: Häufig beginnt man zu früh mit aktiven Scans. Besser ist es, passiv zu starten, Systeme zu klassifizieren und dann gezielt aktiv vorzugehen. Ein Tool ohne Betriebsmodell führt schnell ins Chaos. Ergebnisse müssen in Tickets, Change-Prozesse und klare Verantwortlichkeiten überführt werden. Oft entdeckt man viele Schwachstellen, priorisiert sie aber kaum. Hier hilft es, den Kontext nach Wichtigkeit zu ordnen – zum Beispiel nach Prozesskritikalität, Angriffspfaden und Exponiertheit. Silo-Strukturen bleiben bestehen, wenn man die Organisation nicht durchdacht oder unvollständig anpasst. CTEM funktioniert nur, wenn IT, OT, Netz und Anwendungen gemeinsam betrachtet werden. Besonders heikel wird es, wenn die Nachweisführung vernachlässigt wird. Gerade im Kritis-Umfeld ist Auditierbarkeit entscheidend: Was wurde erkannt? Wie priorisiert? Welche Maßnahmen wurden umgesetzt, und wie ist der aktuelle Status?

Damit das im Alltag funktioniert, muss es in bestehende Prozesse integriert werden. Das reicht vom Ticketing über Change- und Freigabeabläufe bis hin zur Audit-Dokumentation. In vielen Projekten wird daher ein Partner eingebunden, der von der Analyse über die Umsetzung bis zum Betrieb begleitet. Telent bringt hier langjährige Erfahrung und Branchen-Know-how mit, vor allem in der Energiewirtschaft, und unterstützt kompetent in allen Phasen.

Fazit: Resilienz durch Transparenz und Priorisierung

Perimeterschutz bleibt wichtig, reicht aber in vernetzten OT-Umgebungen nicht mehr. Der Schlüssel liegt in der Transparenz: Nur wer Assets, Kommunikationsbeziehungen und realistische Angriffspfade kennt, kann Risiken sinnvoll priorisieren. CTEM bietet dafür den passenden Rahmen: kontinuierlich, kontextbasiert und praxistauglich. Das Ergebnis sind nicht »mehr Alarme«, sondern eine bessere Steuerbarkeit: Maßnahmen werden planbarer, Nachweise belastbarer – und die Resilienz gegenüber Bedrohungen wächst.

Daniel Weber,
Senior Manager Security Solutions,
telent, Saarbrücken

>> info.germany@telent.de

>> www.telent.de