OT-Netzwerksicherheit

BLIND IM EIGENEN HAUS

Der Bericht über den Cyberangriff auf die polnische Energieversorgung Ende Dezember 2025 zeigt erneut strukturelle Schwächen in der Cybersicherheit von OT-Netzen und kritischen Anlagen. Neben basaler Cyberhygiene fehlen Sichtbarkeit und grundlegende Prozesse der Detektionsauswertung. Auch deutsche Unternehmen sollten beide Aspekte berücksichtigen.

Kurz noch einmal zum Auffrischen: Am 29. Dezember 2025 versuchten vermutlich staatlich gestützte Cyberkriminelle die industrielle Steuerung von mindestens 30 Erneuerbare-Energie-Anlagen, einem Heizkraftwerk und (opportunistisch) einem Fertigungsunternehmen in Polen zu stören. Zumindest in den Fällen der Energieversorgung weiß man, dass direkte Auswirkungen verhindert werden konnten.

Wie spätere Analysen zeigten, hatten sich die Angreifer bereits seit mindestens März 2025 in den betroffenen Netzwerken eingenistet – also rund neun Monate vor dem eigentlichen Störversuch im Dezember. Die Angriffswege unterschieden sich dabei je nach Ziel: Während der Zugang zum Heizkraftwerk und zum Fertigungsunternehmen über klassische IT-Infrastruktur erfolgte, drangen die Akteure bei den Erneuerbare-Energie-Anlagen teils direkt über OT-Komponenten der lokalen Umspannwerke ein.

Die Timeline der Attacke verdeutlicht, dass die langfristige Präpositionierung staatlicher Akteure in kritischen Infrastrukturen offenbar Realität ist. Auffällig ist der Umfang der Aktivitäten, die über Monate hinweg unentdeckt blieben. Das deutet auf Defizite in der Erkennung und Reaktion innerhalb der Sicherheitsarchitektur der betroffenen Anlagen hin.

BASALE CYBER-SICHERHEIT FEHLT

Zugegeben, aus der Perspektive der IT-Sicherheit kann man nur die Hände über dem Kopf zusammenschlagen, wie nachlässig Cybersicher-

heit in den kritischen Anlagen behandelt wurde. Der Bericht des CERT Polska liest sich wie eine Bucketlist fehlender Cyberhygiene:

- Geräte liefen mit veralteter und verwundbarer Firmware.
- Über mehrere Geräte und Systeme hinweg wurden identische Passwörter und Accounts verwendet.
- Accounts nutzten Standardpasswörter aus den Werkseinstellungen.
- Benutzerkonten hatten Root-Privilegien.
- Sicherheitsfunktionen auf den Geräten waren deaktiviert.
- Eine Multi-Faktor-Authentifizierung war nicht implementiert.

Dieser Zustand der OT-Sicherheit ist dabei weder eine polnische Eigenart kritischer Infrastrukturen noch ein Einzelfall. In Deutschland sehen viele kritische Anlagen genauso aus. Elementare Regeln der Cyberhygiene bleiben unbeachtet, weil OT-Systeme lange Zeit nicht konsequent in die unternehmensweite Cybersicherheitsstrategie eingebunden waren – weder intern noch bei Dienstleistern, Systemintegratoren oder Zulieferern.

DIE OT IST UND BLEIBT EIN FLICKENTEPPICH

Das liegt zum einen an oftmals fehlenden Sicherheitsfunktionen vieler Komponenten und Systeme, aber auch an dem bislang fehlenden Sicherheitsverständnis in der Organisation. Ohne klare Verantwortung fallen die Priorisierung und technische Umsetzung schwer. Hinzu kommt ein anhaltender Mangel an qualifiziertem Fachpersonal im Bereich OT, während externe Servicedienstleistungen ungenutzt bleiben.

Betreiber von OT-Netzwerken sollten sich der bestehenden Risikolage bewusst sein: In vielen Infrastrukturen finden sich eine Vielzahl bekannter Schwachstellen und sicherheitstechnischer Defizite. Auch das Bundesamt für Sicherheit in der Informationstechnik (BSI) warnt regelmäßig in seinen Lageberichten zur IT-Sicherheit in Deutschland vor den Risiken in industriellen Netzen. Schwachstellenanalysen und Risikobewertungen in kritischer Infrastruktur und Industrie belegen seit Jahren die ausgeprägte Verwundbarkeit von OT-Umgebungen.

Abbildung 1: Die Angriffsflächen in OT-Netzwerken sind vielfältig und tief in den Systemen und Komponenten verankert, wie Schwachstellenbewertungen zwischen 2021 und 2025 herausfanden. (Bild: Rhebo)

In über 90 Prozent aller im Rahmen von Rhebo Industrial Security & Stability Assessments untersuchten OT-Netzwerke fanden sich veraltete und verwundbare Firmware, Software oder Betriebssysteme sowie Schwachstellen bei der Authentifizierung, Protokollsicherheit und Systemkonfiguration (siehe Abbildung 1). Diese Defizite sind in OT-Umgebungen nahezu überall anzutreffen.

Die detaillierte Analyse verdeutlicht die konkreten Angriffsvektoren in OT-Netzen weiter (siehe Abbildung 2). Passwörter wurden aufgrund veralteter, nicht gesicherter Protokolle fast flächendeckend als Klartext verschickt. Durch Werkeinstellungen, Fehlkonfigurationen und fehlende Segmentierung fanden sich in über 60 Prozent aller OT-Netze Systeme, die eine Verbindung zum Internet herstellen konnten oder dies aktiv (oft automatisiert) versuchten, obwohl dies weder notwendig noch gewollt war.

Doch nicht nur fehlende Zugangssicherung und Netztrennung erhöhen das Risiko. Auch grundlegende Betriebsparameter sind häufig fehlerhaft konfiguriert. So können Fehler in der Zeitsynchronisation (46 Prozent) nicht nur Probleme bei Echtzeitprozessen verursachen. Sie erschweren im Cybervorfall zudem die forensische Analyse erheblich, da ohne konsistente Zeitstempel keine verlässliche Korrelation von Log-Dateien möglich ist.

In knapp 44 Prozent aller Fälle wurden darüber hinaus während der Schwachstellenbewertungen neue und teilweise unbekannte Netzteilnehmer registriert. In der Regel liefen diese Neuregistrierungen an der Administration vorbei, denn die Systeme wuchsen „historisch" nach Bedarf.

BLINDE FLECKEN IN DER ERKENNUNG

Diese fehlende Sichtbarkeit beschränkt sich nicht nur auf die bestehenden Sicherheitslücken und -risiken der OT-Netzwerke. Der Vorfall in der polnischen Infrastruktur zeigte auch weitere blinde

Abbildung 2: Die am häufigsten in OT-Netzen identifizierten Anomalien der letzten fünf Jahre (Bild: Rhebo)

Flecken beim Erkennen maliziöser Aktivitäten im Netzwerk (siehe Abbildung 1), die frühzeitig die Alarmglocken hätten auslösen müssen:

- Kommunikation über SSL-, SMB- und RDP-Protokolle;
- Exfiltration sensibler Daten;
- neue Verbindungen zwischen bislang nicht gekoppelten Systemen;
- Nutzung zusätzlicher oder untypischer Protokolle innerhalb bestehender Verbindungen;
- Upload von Tools wie Reverse-SOCKS-Proxys, Impacket oder Wipern;
- Verbindungsaufbau zu öffentlichen IP-Adressen;
- aktive Netzwerkscans.

In OT-Netzwerken ist die Nutzung klassischer hostbasierter Angriffserkennungssysteme aufgrund limitierter CPU-Ressourcen häufig nur bedingt möglich und sinnvoll. Zudem lehnen Betreiber aktive, automatisierte Gegenmaßnahmen – etwa das Blockieren von Verbindungen oder das Isolieren von Geräten – bewusst ab, um die Stabilität kritischer Prozesse nicht zu gefährden.

Als Alternative empfiehlt das BSI in seinem Dokument BSI-CS 153 „Stationsautomatisierung" ein netzbasiertes Angriffserkennungssystem (Network Intrusion Detection System, NIDS). Solche Systeme spiegeln den Datenverkehr an definierten Abgriffspunkten – etwa Switches – rein passiv, analysieren ihn auf Anomalien und melden Abweichungen von einer zuvor definierten Baseline-Kommunikation an die Verantwortlichen.

Ein NIDS ermöglicht in OT-Umgebungen ein kontinuierliches, passives Monitoring des Netzwerkverkehrs, ohne Endgeräte zu belasten oder aktiv in kritische Prozesse einzugreifen. Durch die Anomalieerkennung lassen sich auch solche Aktivitäten identifizieren, die auf den ersten Blick legitim erscheinen – etwa bei Nutzung autorisierter Accounts.

FEHLENDE HANDLUNGSFÄHIGKEIT

Eine weitere Herausforderung in kritischen Infrastrukturen besteht auf personeller Ebene. Laut CERT Polska hatte ein hostbasiertes Angriffserkennungssystem bereits über ein halbes Jahr vor dem winterlichen Vorfall suspekte Aktivitäten auf einzelnen Systemen registriert. Diese Sicherheitslogs wurden jedoch anscheinend erst nach dem Vorfall, im Rahmen der forensischen Systemanalyse, ausgewertet. So ärgerlich das ist, so wenig verwundert es.

OT-Sicherheit ist in vielen Unternehmen noch immer Neuland. Oft fehlt qualifiziertes Personal mit klarer Verantwortung und ausreichender Zeit für OT-Sicherheit sowie ein belastbares Verständnis für den Umgang mit Angriffserkennungssystemen und deren Meldungen. Für den Einstieg kann es sinnvoll sein, externe Expertise einzubinden. Ein NIDS lässt sich in der Anfangsphase gemeinsam mit dem Anbieter betreiben, wobei Analyse und Bewertung von Anomalien unterstützt werden. Das erleichtert den Aufbau einer belastbaren OT Baseline, schafft Sicherheit bei der Einordnung von Vorfällen und beschleunigt den Kompetenzaufbau im eigenen Team. ■

JAN FISCHER
ist Head of Sales bei Rhebo.