OT-Sicherheit in Stationsautomatisierung und Umspannwerken

Sinnvolle Angriffserkennung in der Praxis

Frank Stummer

1 Einleitung

Umspannwerke und Systeme für die Stationsautomatisierung gelten seit Jahrzehnten als robust, langlebig und zuverlässig. Genau das macht sie heute zur Schwachstelle. Geräte mit Lebenszyklen von 20 bis 30 Jahren kommunizieren über Protokolle aus einer Zeit, als diese Systeme physisch isoliert betrieben wurden und Cybersicherheit kein Thema war. Heute sind dieselben Systeme über Fernwartungszugänge, Leittechnikschnittstellen und Smart-Grid-Anbindungen mit der Außenwelt verbunden. Das Ergebnis: eine wachsende Angriffsfläche, die vielen Betreibern noch nicht vollständig bewusst ist. Energieversorger stehen dabei unter besonderem Druck. Ein Ausfall der Stationsautomatisierung oder eines Umspannwerks kann unmittelbare Konsequenzen für die Versorgungssicherheit ganzer Regionen haben. Kein Wunder, dass kritische Energieinfrastruktur zunehmend in den Fokus staatlicher und krimineller Angreifer gerät. Dieser Beitrag zeigt auf der Grundlage realer Betriebsdaten und Angriffsszenarien, welche Sicherheitslücken in der Praxis bestehen, wie eine sinnvolle netzbasierte Angriffserkennung in diesem Umfeld funktioniert und was passiert, wenn sie fehlt – oder wenn sie rechtzeitig greift. Die dargestellten Erkenntnisse basieren auf Einsatzerfahrungen aus dem OT-Monitoring bei Energieversorgern und -erzeugern in Europa.

2 Monitoring in OT-Netzen

2.1 Was in OT-Netzen wirklich vorzufinden ist

Wer regelmäßig OT-Sicherheitsassessments in Energieversorgungsunternehmen durchführt, entwickelt ein ziemlich klares Bild davon, was in diesen Netzen tatsächlich los ist. Die Erkenntnis ist ernüchternd: Es sind selten spektakuläre Zero-Day-Exploits, die Angreifern den Weg ebnen. Es sind die Basics, die nicht stimmen. Bild 1 zeigt die häufigsten Sicherheitslücken in OT-Netzen, die wir in den letzten Jahren bei Sicherheitsassessments bei unseren Kunden sehen.

Protokolldesign und Authentifizierung aus einer anderen Zeit

An erster Stelle stehen protokollbasierte Sicherheitslücken. OT-Protokolle wie IEC 60870-5-104, IEC 61850 oder Modbus wurden ohne Authentifizierung und Verschlüsselung konzipiert – weil beides im ursprünglichen Einsatzszenario nicht nötig war. Sobald diese Systeme aber über Schnittstellen mit anderen Netzwerkbereichen verbunden werden, entstehen inhärente Risiken, die sich protokollseitig kaum beheben lassen. Man muss damit umgehen, nicht sie wegdefinieren. Oft unmittelbar damit verknüpft: unsichere Authentifizierungsmethoden. Passwörter werden im Klartext übertragen, Standardzugangsdaten bleiben unverändert, veraltete Authentifizierungsverfahren ohne Verschlüsselung sind die Norm.

Betriebliche Schwächen: Fehlkonfiguration, Patches, unbekannte Geräte

Fehler bei der Zeitsynchronisierung erscheinen zunächst harmlos. Im Ernstfall aber erschweren falsch synchronisierte Systemuhren die Korrelation von Ereignissen erheblich und können auch forensische Auf-

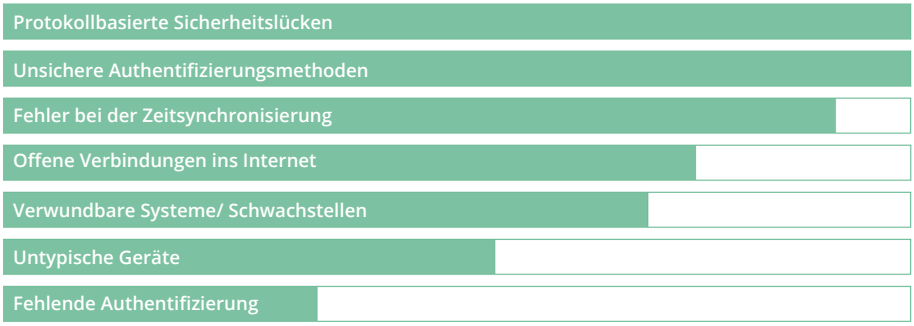

Bild 1. Häufigkeit der Top-OT-Sicherheitslücken in der Praxis (Quelle: Rhebo).

Autor

Dr. Frank Stummer
Business Development Manager
Rhebo GmbH
Leipzig, Deutschland

arbeitungen von Vorfällen faktisch unmöglich machen. Offene Verbindungen ins Internet sind oft tatsächlich notwendig, aber nicht gut dokumentiert oder sind ein Überbleibsel aus einer Wartungssitzung („mal eben schnell einen Zugang geben“). Verwundbare Systeme mit (meist eigentlich bekannten) Schwachstellen sind in OT-Umgebungen die Regel. Patches werden nicht eingespielt, weil Stabilitäts- und Verfügbarkeitsanforderungen Vorrang haben. Das ist in gewissem Maße nachvollziehbar – aber es bedeutet: Wer nicht patcht, muss umso mehr überwachen. Besonders beunruhigend ist das weitverbreitete Phänomen untypischer oder unbekannter Geräte im OT-Netz. In vielen Assessments tauchten Geräte auf, die in keinem Asset-Register erfasst waren: private Laptops von Mitarbeitern, nicht autorisierte Netzwerkkomponenten, Systeme, die von externen Dienstleistern zurückgelassen wurden, aber auch Geräte, die eigentlich nicht OT-tauglich sind, aber aus Mangel an besseren Alternativen (oder aus Preisgründen) trotzdem verbaut sind. Was man nicht kennt oder was nicht geeignet ist, kann man nicht schützen.

Fernzugänge: Das unterschätzte Einfallstor in Unterstationen

Für Umspannwerke und Unterstationen gibt es ein besonders relevantes Muster: Zugriffe über kompromittierte Fernzugänge. Fernwartung durch Gerätehersteller, Lieferanten und externe Dienstleister ist in diesem Umfeld Standard. Wenn diese Zugänge kompromittiert oder schlicht nicht dokumentiert sind, bleiben Zugriffe – übrigens auch physische – über lange Zeiträume unbemerkt. Das ist keine Theorie; das ist gelebte Praxis in vielen Netzen.

2.2 Der Ansatz: Drei Säulen, die zusammenwirken müssen

Aus der Erfahrung mit zahlreichen Energieversorgern hat sich ein strukturierter Drei-Säulen-Ansatz für OT-Sicherheit bewährt. Er ist kein Wunschdenken, sondern ein pragmatisches Vorgehen, das die Realität von OT-Betriebsumgebungen berücksichtigt.

Säule 1: Erst sehen, dann handeln – das Assessment

Am Anfang steht immer die Frage: Was ist überhaupt in meinem Netz? Ohne vollständige Sichtbarkeit auf alle OT-Assets, deren Kommunikationsverhalten und bekannte Schwachstellen ist jede weitere Sicherheitsmaßnahme ein Schuss ins Dunkle. Ein OT-Sicherheitsassessment identifiziert alle aktiven Geräte, gleicht sie mit der CVE-Datenbank (Common Vulnerabilities and Exposures) ab und prüft das Netz auf Gefährdungen, Sicherheitslücken und technische Fehlerzustände. Das Ergebnis ist ein priorisierter Maßnahmenplan mit konkreten Handlungsempfehlungen – kein Papier, das in der Schublade landet, sondern die Arbeitsgrundlage für alles Weitere.

Säule 2: Passiv, aber wachsam – das NIDS

Im laufenden Betrieb übernimmt ein netzbasiertes Intrusion Detection System (NIDS) die Kernaufgabe. Es liest den gesamten Netzverkehr passiv mit – ohne aktive Abfragen, ohne Eingriff in den Betriebsprozess, ohne Ausfallrisiko. Das System lernt das normale Kommunikationsverhalten aller OT- und IIoT-Assets und meldet in Echtzeit jede Abweichung: neue Geräte, unbekannte Protokollnutzungen, ungewöhnliche Verbindungsaufbauten, auffällige Befehlssequenzen und vieles mehr. Das ist der entscheidende Punkt: Ein NIDS erkennt Angriffe, die Firewalls und Segmentierung bereits überwunden haben. Backdoors über kompromittierte Fernzugänge, Innentäter, Zero-Day-Exploits – sie alle hinterlassen Spuren im Netzverkehr. Wer diese Spuren nicht liest, wird sie nicht finden. NIDS-Lösungen lassen sich sowohl als dedizierte Hardware-Sensoren als auch als Softwarelösung auf bereits vorhandenen Industrieswitches betreiben. Die Integration in bestehende Architekturen der Stationsautomatisierung ist damit relativ einfach. Ebenso einfach ist die Einbindung in die gesamthafte Sicherheitsinfrastruktur eines Unternehmens und es ist eine sehr wertvolle Informationsquelle für zentrale Lösungen der Sicherheitsüberwachungen. Die Stärke des Ansatzes liegt in der Integration: Über standardisierte Schnittstellen (wie CEF, SYSLOG, SNMP, SMTP u.a.) werden NIDS-Meldungen direkt in ein zentrales SIEM (Security Information and Event Management) eingespeist. Dort werden sie mit IT-Ereignissen korreliert und u.a. nach dem Framework „MITRE ATT&CK“ und deren Erweiterung „for ICS“ klassifiziert. Das zentrale SOC (Security Operation Center) erhält ein einheitliches und v.a. gesamthaftes Lagebild über IT und OT. Es ist ein grundlegendes Prinzip, durch das Zusammenspiel von verschiedenen Maßnahmen das Sicherheitslevel auf das gewünschte Maß zu bringen.

Säule 3: Expertise, die im Betrieb oft fehlt – externe Unterstützung

OT-Sicherheitsmonitoring läuft nicht von selbst. Es braucht Expertise, um Meldungen richtig zu bewerten, echte Bedrohungen von Fehlalarmen zu unterscheiden und forensische Spuren im Ernstfall zu sichern. Diese Expertise fehlt in den meisten OT-Betriebsteams – und der Arbeitsmarkt gibt sie auf absehbare Zeit auch nicht her. Externe Experten können diese Lücke schließen: Sie unterstützen beim laufenden Betrieb des Monitorings, führen schnelle forensische Analysen durch und liefern regelmäßige Risiko- und Schwachstellenberichte.

2.3 Was das Monitoring wirklich aufdeckt: Drei Fälle aus der Praxis

Fall 1: Klartext-Passwörter im Leitnetz

Im Leitnetz eines Energieerzeugers meldete das NIDS Verbindungen, bei denen Authentifizierungsinformationen unverschlüsselt übertragen wurden – konkret Passwörter über FTP (File Transfer Protocol) im Klartext. Gleichzeitig wurden öffentliche IP-Adressen im internen OT-Netz sichtbar, die zumindest auf den ersten Blick unbekannt waren (Bild 2).

Das ist das eigentliche Problem: Nicht die einzelne Schwachstelle, sondern die Kumulation von Unaufmerksamkeiten, die jahrelang unbemerkt bleiben – bis jemand anfängt hinzuschauen. Es hat dann keine zwei Stunden Arbeit beansprucht, um auf die Variante SFTP (Secure FTP) mit einem höheren Sicherheitslevel umzustellen. Außerdm hat sich schnell herausgestellt, dass die öffentlichen Verbindungen tatsächlich gewollt waren und auch notwendig sind. Wenn man solche Sachverhalte kennt, lassen sich diese dann auch an einer Firewall bewusst und sicher konfigurieren.

Fall 2: Backdoor durch eine Schwachstelle, die seit Jahren bekannt war

Eine Schadsoftware hatte in einem OT-Netz bereits eine Backdoor geöffnet. Die zugrundeliegende ausgenutzte Schwachstelle war ein Buffer Overflow in der PCT-Protokollimplementierung der Microsoft SSL-Bibliothek und übrigens bereits seit langem öffentlich dokumentiert (Bild 3).

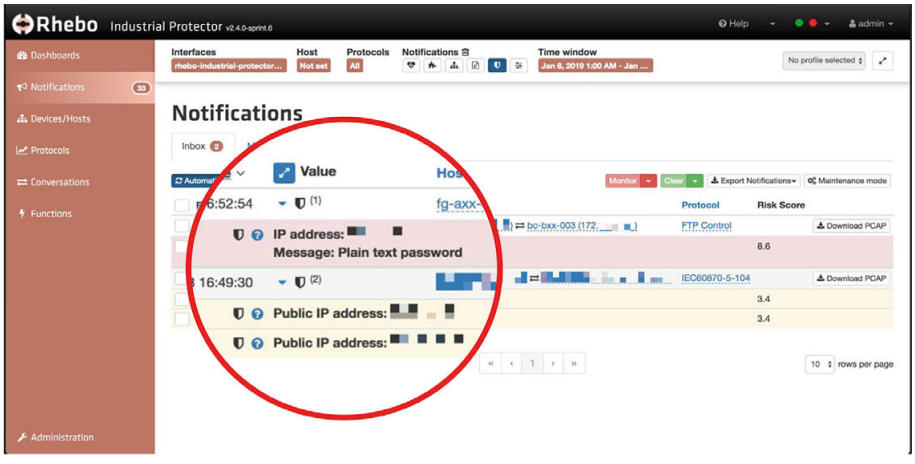

Bild 2. Meldung unsicherer Klartext-Passwörter und öffentliche Verbindungen (Quelle: Rhebo).

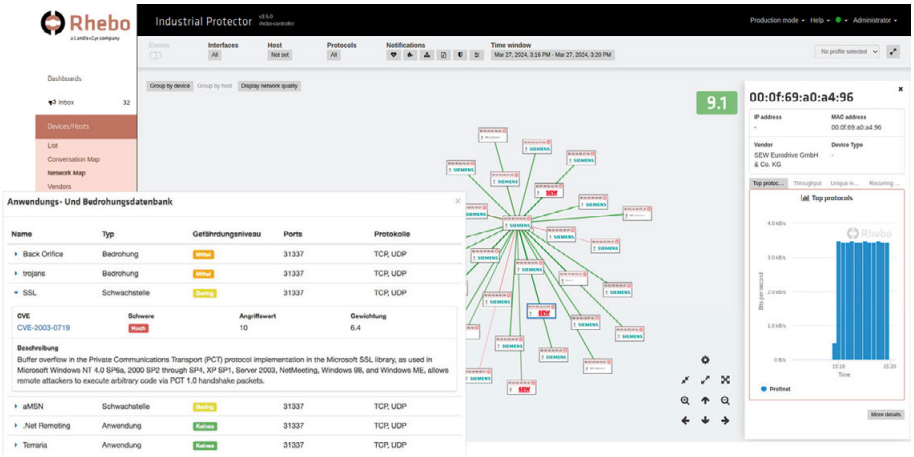

Bild 3. Identifikation einer CVE-Schwachstelle (Quelle: Rhebo).

Das NIDS hat sowohl die Schwachstelle des Gerätes als auch die Backdoor-Kommunikation erkannt. Das erste ist letztlich ein simpler Abgleich des im Netzwerk beobachteten Gerätes und seines Versionsstandes mit den verfügbaren CVE-Datenbanken und eine einfache, aber wichtige Alarmmeldung. Das zweite erfordert sicherlich etwas mehr Expertise und fällt ggf. erst an einer zentraleren Beobachtungsstelle auf. Ein früher Patch hätte den Fall verhindert. Aber für OT-Umgebungen gilt: Wer aus Stabilitätsgründen nicht (sofort) patchen kann oder will, muss zwingend überwachen. Eines von beidem. Nicht keines.

Fall 3: Fehlkonfiguration beeinträchtigt die Anbindung der Unterstationen

Nicht immer geht es um Cybersicherheit. Sogar viel häufiger geht es schlicht um die verlässliche Kommunikation an sich. Ein zentrales Gerät in der Netzleittechnik eines Energieversorgers war unregelmäßig, aber häufig nicht erreichbar. Die Ursache: eine fehlerhafte Konfiguration, die die Kommunikationsstabilität von und zu den Unterstationen erheblich beeinträchtigte. Das Monitoring visualisierte die ICMP-Unreachable-Meldungen – es handelt sich um ein weitverbreitetes Protokoll für die Diagnose und Fehlermeldung in Netzwerken – im Zeitverlauf und ermöglichte die schnelle Lokalisierung der Fehlerquelle (Bild 4), ohne wochenlange manuelle Fehlersuche.

Dieser Fall zeigt: Ein NIDS ist nicht nur ein Sicherheitswerkzeug. Es ist auch ein Stabilitäts-Monitoring. In OT-Netzen ist die Grenze zwischen Sicherheitsvorfall und Betriebsstörung fließend – und ein System, das beides sichtbar macht, hat natürlich doppelten Nutzen.

2.4 MITRE ATT&CK for ICS: Angriffsmuster kennen, bevor sie auftreten

Wer Angriffe erkennen will, muss Angriffsmuster kennen. Das MITRE ATT&CK Framework und seine Erweiterung für ICS, also industrielle Steuersysteme, liefert genau das: eine systematische Übersicht aller dokumentierten Taktiken, Techniken und Prozeduren, die Angreifer in industriellen Steuerungssystemen einsetzen – von Initial Access über Lateral Movement bis hin zum Impact. Auch ein für die OT geeignetes passives NIDS kann einen erheblichen Teil dieser Taktiken und Techniken direkt im Netzverkehr erkennen: Netzwerk-Sniffing, Remote System Discovery, Lateral Tool Transfer, Spoof Reporting Messages, Default Credentials, Command-and-Control-Kommunikation usw. Andere Techniken, die beispielsweise ausschließlich auf lokaler Codeausführung oder Dateisystemmanipulation beruhen, sind durch das Netzmonitoring allein nicht sichtbar – ein NIDS ist kein Allheilmittel, sondern ein zentrales Element in einer gestaffelten Sicherheitsarchitektur. Was das Framework vor allem lehrt: Angriffe auf kritische Infrastruktur sind keine Zufallsereignisse. Sie sind geplant, geschehen phasenweise und oftmals sehr geduldig. Wer das nicht verinnerlicht hat, unterschätzt die Bedrohung systematisch.

2.5 Was passiert, wenn der Angriff zu spät auffällt: Der Fall Ukrenergo

Im Jahr 2016 bereiteten Angreifer – mutmaßlich die staatlich gesteuerte Gruppe Sandworm – ein volles Jahr lang den gezielten Angriff auf den ukrainischen Netzbetreiber Ukrenergo vor. Am 17. Dezember 2016 brachten sie die Netzleittechnik zum Absturz und legten die Stromversorgung in Teilen von Kyjiw lahm. Der Einsatz des ICS-Schadcodes Industroyer über das Protokoll IEC 60870-5-104 markierte dabei eine neue Qualitätsstufe in Angriffen auf Energieinfrastruktur. Die Kill-Chain-Analyse dieses Angriffs (Tabelle 1) ist bis heute Pflichtlektüre für jeden, der OT-Sicherheit in Umspannwerken verantwortet.

Zwölf Monate. So lang bewegten sich die Angreifer im Netz, ohne entdeckt zu werden. Ein NIDS in der OT hätte in mehreren Phasen anschlagen können: bei den ungewöhnlichen lateralen Bewegungen, beim erstmaligen Einsatz von IEC-60870-5-104-Befehlen außerhalb des normalen Betriebsmusters, bei der Kommunikation mit dem

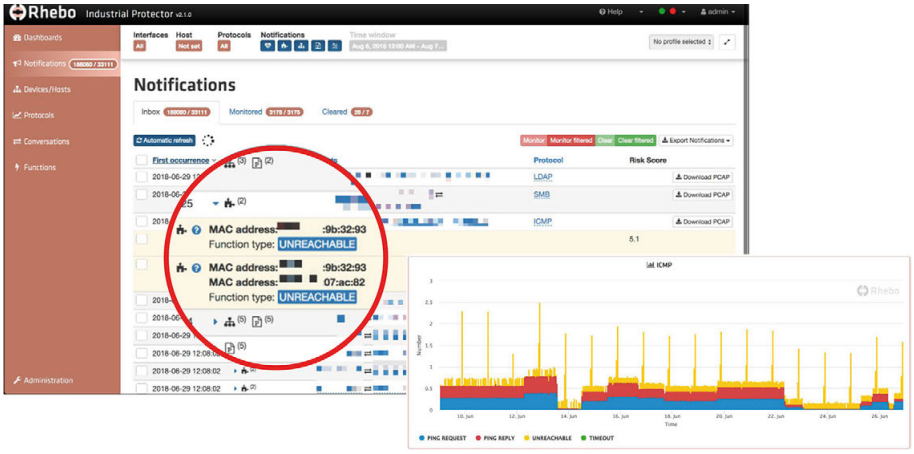

Bild 4. ICMP-Unreachable-Zeitverlauf als Indikator einer Fehlkonfiguration (Quelle: Rhebo).

Tab. 1. Angriffsphasen des Ukrenergo-Angriffs 2016.

Zeitraum	Kill-Chain-Phase	Was passierte
Januar 2016	Reconnaissance / Delivery	Spearphishing-Angriff auf die IT-Infrastruktur des Unternehmens
Feb. bis Nov. 2016	Exploitation / Lateral Movement	Schrittweise Ausbreitung im IT-Netz, unentdeckt über zehn Monate
Anfang Dez. 2016	Lateral Movement	Übergang in die Netzleittechnik, weitere Ausbreitung im OT-Bereich
Mitte Dez. 2016	Persistence	Übernahme von drei zentralen Servern als Angriffs-Beachheads
16. Dez. 2016	Weaponization	Hochladen des Industroyer-Schadcodes auf die kompromittierten Server
17. Dez. 2016	Actions on Objectives	Ausführung über IEC 60870-5-104, Löschen der Konfigurationen, Absturz der Netzleittechnik, Stromausfall in Kyjiw

Command-and-Control-Server. Stattdessen: Stille. Bis es zu spät war. Nur mit viel Arbeit und einer gehörigen Portion Glück – die Angreifer selbst hatten einige Fehler gemacht, die den Schaden letztlich abgemildert haben – waren die Auswirkungen zeitlich und räumlich noch relativ begrenzt.

2.6 Wenn das Monitoring greift: Ein Angriff, der keinen Schaden anrichtete

Nicht jeder Angriff endet mit einem Schaden. Im Produktionsnetz eines großen Getränkeabfüllers wurde ein gezielter Angriff in allen Phasen durch das eingesetzte NIDS in Echtzeit sichtbar gemacht, forensisch aufgeklärt und ohne Produktionsunterbrechung abgewehrt. Der Angriff lief über vier klar erkennbare Phasen:

- **Phase 1:** Reconnaissance – u.a. UDP-Portscans und DNS-Diensteabfragen, um das Netz zu kartieren, hier wurden Basisfunktionen in der Kommunikation (User Datagram Protocol und Domain Name System) ausgespäht
- **Phase 2:** ARP-Spoofing – Abhören des internen Kommunikationsflusses, hier des Address Resolution Protocols zur Übersetzung von IP-Adressen in lokale MAC-Adressen der einzelnen Geräte
- **Phase 3:** Manipulation des Log-Servers, Umleitung auf den Angreifer, Ausspähen von Firewall-Zugangsdaten
- **Phase 4:** Mehrere Versuche, die Firewall zu übernehmen – Bruteforce mit Default-Passwörtern (erfolglos), SQL-Injection (erfolglos), schließlich Öffnen einer Reverse Shell über eine bekannte Firewall-Schwachstelle (erfolgreich) und Umkonfiguration der Firewall-Regeln

An diesem Punkt wurde der Angriff gestoppt. Alle Schadsoftware beseitigt, forensische Spuren gesichert. Möglich war das, weil das System jede einzelne Phase sichtbar gemacht hatte – vom ersten Portscan bis zum Firewall-Übernahmeversuch. Dabei handelt es sich sowohl um relativ einfache Angriffsmethoden und deren Erkennung wie die Änderung der Kombination aus MAC- und IP-Adresse als auch tiefergehende Angriffsmethoden und deren detaillierte Auswertung von Spuren durch Experten wie bei den Übernahmeversuchen der Firewall (siehe die Bilder 5 und 6).

3 Zusammenfassung

OT-Netze in Stationsautomatisierung und Umspannwerken sind real bedroht. Nicht hypothetisch. Nicht irgendwann. Jetzt. Die Sicherheitslücken, die in Assessments immer wieder auftauchen – unsichere Protokolle, Klartext-Authentifizierung, ungepatchte Schwachstellen, unbekannte Geräte, unkontrollierte Fernzugänge – sind keine Ausnahme. Sie sind der Normalzustand in vielen Netzen. Die gute Nachricht: Die Lücke zwischen Bedrohung und Schutz lässt sich schließen. Passives Netzmonitoring in der OT

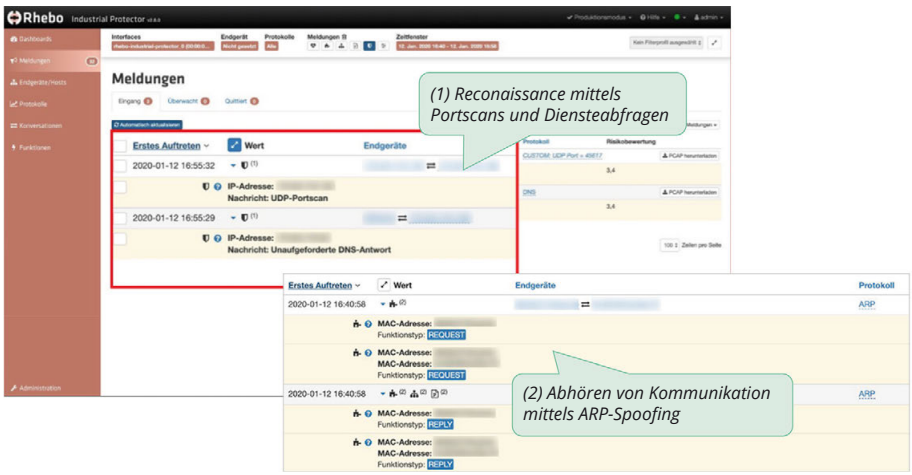

Bild 5. Aufklärung verschiedener Angriffsmethoden (Quelle: Rhebo).

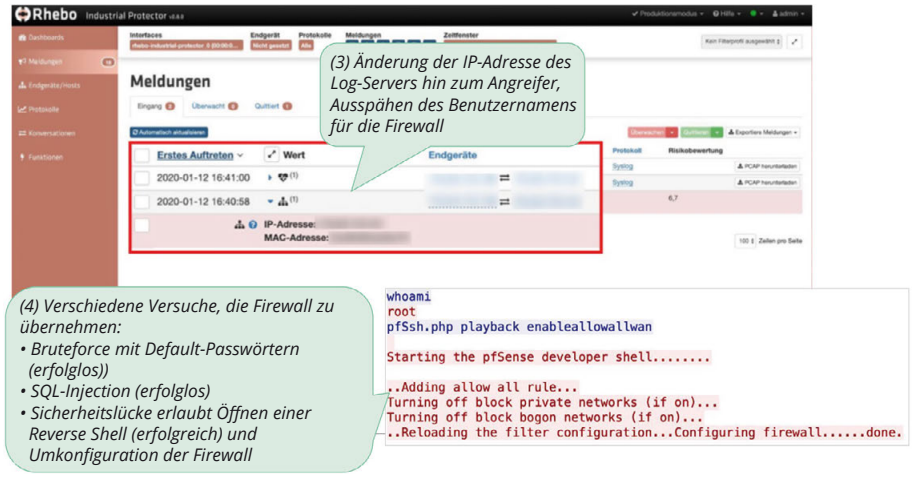

Bild 6. Aufklärung verschiedener Angriffsmethoden (Quelle: Rhebo).

ist nicht-invasiv, betriebsunterbrechungsfrei und in bestehende Architekturen der Stationsautomatisierung integrierbar. Es schafft die Sichtbarkeit, ohne die jede Sicherheitsmaßnahme im Dunkeln tappt. Und es wirkt: Der abgewehrte Angriff auf den Getränkeabfüller zeigt, was möglich ist, wenn das Monitoring greift. Was der Ukrenergo-Fall zeigt, ist die andere Seite: Zwölf Monate unentdeckte Angriffsvorbereitungen in einem Netz, das als sicher galt. Das kann jedes Übertragungsnetz, jedes Umspannwerk, jede Stationsautomatisierung betreffen, die keine Sichtbarkeit in den eigenen Datenverkehr hat.

Zwei Schlussfolgerungen für Betreiber:

- **Sichtbarkeit ist die Voraussetzung, nicht das Ziel.** Ohne vollständiges Asset-Inventar und Netzmonitoring fehlt die Grundlage jeder weiteren Sicherheitsmaßnahme.
- **OT-Sicherheit ist Betriebsaufgabe, nicht IT-Aufgabe.** Lösungen, die OT-Prozesse stören oder gefährden, werden nicht akzeptiert. Passives Monitoring ist deshalb der richtige Ansatz für dieses Umfeld.

Eine sinnvolle erste Maßnahme für Betreiber, die noch nicht begonnen haben: ein OT-Sicherheitsassessment. Es dauert wenige Wochen, liefert vollständige Sichtbarkeit über den eigenen Netzbestand und ist die Basis, auf der alles andere aufbaut.

Abstract

OT-Security in substation automation: Effective attack detection

Substations and substation automation systems are regarded as robust and durable. It is precisely this that makes them a vulnerability today: devices with lifecycles of 20 to 30 years communicate via protocols that were designed without authentication or encryption – and are now connected to the outside world via remote maintenance access points and control system interfaces. Practical experience shows that it is rarely spectacular zero-day exploits that pave the way for attackers. It is the basics that are lacking – plaintext passwords, unpatched vulnerabilities, unknown devices on the network, uncontrolled remote access. The 2016 attack on the Ukrainian grid operator Ukrenergo illustrates what this means: twelve months of undetected preparation, followed by the collapse of the grid control system. Using real-world cases, this article demonstrates how a structured three-pillar approach closes this gap: an OT security assessment as a foundation, a passive network-based intrusion detection system (NIDS) for detecting attacks during live operations, and external expertise for analysis and forensics. Passive monitoring is non-invasive, causes no disruption to operations and detects attacks that have already bypassed firewalls and segmentation.