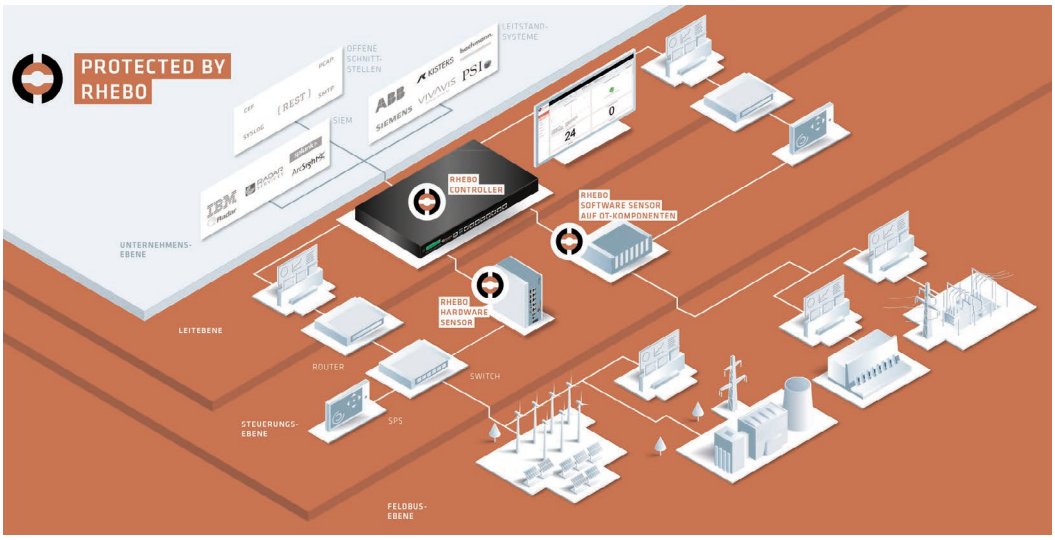
Ein System zur Angriffserkennung auch in der OT?

Ein System zur Angriffserkennung benötigen nach NIS2 offiziell nur kritische Anlagen. Doch ohne können auch andere betroffene Unternehmen den Anforderungen nicht nachkommen. Was genau braucht es und warum?



Das NIDS Rhebo Industrial Protector analysiert die gesamte Kommunikation innerhalb des OT-Netzwerkes und meldet diese in Echtzeit. Alle Bilder © Rhebo

Gesetze haben ihre Tücken. Folgt man dem genauen Wortlaut der bisherigen Entwürfe des NIS2-Umsetzungsgesetzes (Stand Juli 2025), besteht die Pflicht, ein System zur Angriffserkennung (SzA) in den kritischen Prozessen zu betreiben, nur für kritische Anlagen. Wie so immer steckt der Teufel im Detail. Denn betrachtet man auch die anderen Anforderungen an alle rund 30.000 in Deutschland von der NIS2 betroffenen Unternehmen, kommt eigentlich niemand an einem System zur Angriffserkennung (SzA) vorbei. Viele Wege führen nach Rom.

Autor:
Uwe Dietzmann
Sales Manager
Rhebo
www.rhebo.com

Die NIS2 fordert beispielsweise:

- eine regelmäßige Bewertung der (inneren und äußeren) Cyberrisiken,
- Fähigkeit zur Bewältigung von Sicherheitsvorfällen,
- die Berücksichtigung der Cybersicherheit der Lieferkette,
- Verfahren zur Bewertung der eingesetzten Sicherheitsmechanismen.

Alle vier Anforderungen benötigen a) Sichtbarkeit auf und in die eigenen Netzwerke und Systeme sowie b) Wege, um mit dem nicht abstellbaren Restrisikos umzugehen.

Restrisiko

Das Restrisiko ist in der OT, den industriellen Kommunikationsnetzen, ein relevanter Aspekt bei der Cybersicherheit. Denn die Risikolandschaft industrieller Systeme ist aufgrund der Historie, steigenden Vernetzung und Digitalisierung nach wie vor unüberschaubar:

- Die Anzahl der von der Cybersecurity & Infrastructure Security Agency (CISA) gemeldeten Schwachstellen steigt seit Jahren stetig an [1]. Nicht nur muss davon ausgegangen werden, dass die gemeldeten Schwachstellen nur die Spitze des Eisberges bilden, denn OT-Systeme sind historisch für Verfügbarkeit und Funktionalität und nicht Cybersicherheit entwickelt worden. In OT-Umgebungen ist das Ausrollen von Sicherheitspatches in der Regel auch meist stark zeitverzögert und kompliziert – in Teilen sogar unmöglich.
- In OT-Umgebungen haben Dienstleister für die Konfiguration und Wartung der Systeme häufig umfassende Befugnisse. Kompromittierte Wartungslaptops, Updates und Fernzugänge (Stichwort: Lieferkettenangriff bzw. Supply Chain Compromise) können somit leicht Bedrohungen in die OT bringen, ohne die Firewall zu alarmieren. Gerade VPN-Zugänge, RDP und Edge Geräte rücken zusehends ins Visier der Angreifenden.
- Das Lieferkettenproblem ist weitreichender: Software-Entwickler greifen seit langem auf externe Bibliotheken und Softwarebausteine zurück. Auch in der Hardware befinden sich häufig Einzelteile von dutzenden vorgelagerten Lieferanten, über die man selbst keine Übersicht hat. Der Fall SolarWinds hat 2020 einen Vorgeschmack geliefert, wie die Kompromittierung eines Softwareunternehmens auf seine Kunden durchschlagen kann. Die Konsequenzen, die sich aus der Kompromittierung des Open Source npm Packet Managers Mitte 2025 ergeben, können bislang nur erahnt werden.
- OT-Netzwerke werden durch die Konvergenz von IT und OT auch bei Vorfällen in der IT häufiger in Mitleidenschaft gezogen und sei es nur, um die OT vorsorglich zu schützen. Das zeigten nicht zuletzt die Ransomware-Angriffe auf deutsche Flughäfen. Resilienz bedeutet in diesem Zusammenhang auch, bei IT-Vorfällen in der OT handlungsfähig zu bleiben und die Anlagenausfälle zu minimieren.
- In jeder OT gibt es mindestens ein Legacy-System oder werden Legacy-Protokolle verwendet, deren Sicherheitslücken nicht mehr gepatcht werden können (Bild 1). Mit dem Ende des Supports von Windows 10 wird sich die Zahl weiter erhöhen.

Kurz gesagt:

Das größte Cyberrisiko für Industrieunternehmen verbirgt sich innerhalb der eigenen (ohnehin niedrigen) Mauern der OT. Aus diesem Grund reicht es nicht aus, sich nur auf seine Firewalls zu verlassen, wenn OT-Sicherheit diskutiert wird. Dass Angreifende langsam auf den Geschmack kommen, zeigt nicht zuletzt der Anstieg der Angriffe auf Industrieunternehmen, was auch von Cyberversicherungsfirmen bestätigt wird.

Das Dreierteam der OT-Sicherheit

Somit wird offensichtlich, dass Firewalls allein keine adäquate Sicherheitslösung darstellen. Firewalls sichern die industrielle Infrastruktur als erste Abwehrlinie an den Netzwerk- und Segmentgrenzen.

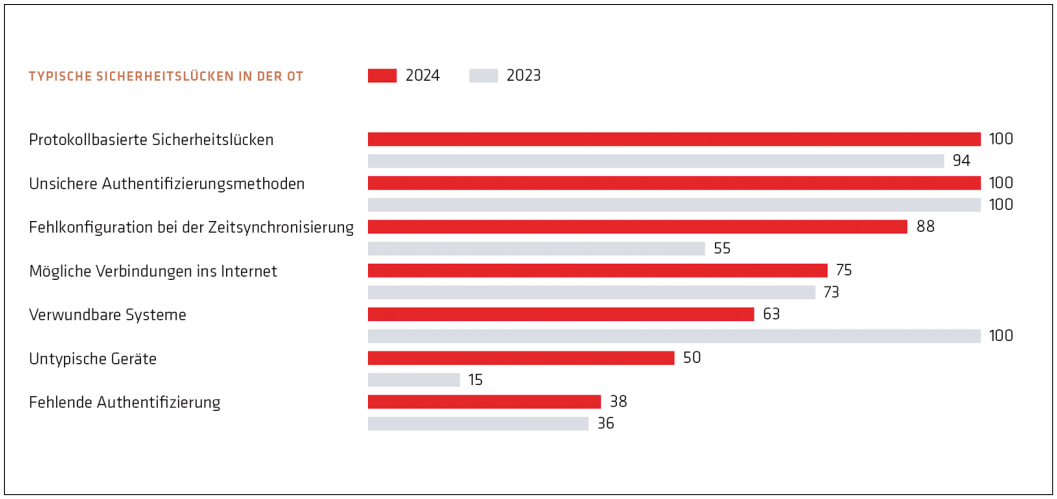


Bild 1: Die am häufigsten während Rhebo Industrial Security Assessments in OT-Netzwerken identifizierten Sicherheitsrisiken

Ihr Blick ist nach Außen gerichtet. Die Aufgabe von Firewalls ist, von außen auf ein Netzwerk eindringende Bedrohungen zu erkennen und zu stoppen. In der Regel erfolgt die Erkennung von Bedrohungen signaturbasiert und auf IT- und Internetprotokolle beschränkt. Firewalls fehlen somit drei Fähigkeiten:

1. Der Blick ins OT-Netzwerk.
2. Das Verständnis für industrielle Protokolle.
3. Die Identifikation von anomalen, nicht über Signaturen definierte sicherheitsrelevanten Vorgängen.

Netzbasiertes Angriffserkennungssystem

Diese Lücken schließt ein netzbasiertes Angriffserkennungssystem (NIDS für Network Intrusion Detection System) wie Rhebo Industrial Protector. Das NIDS ist innerhalb der OT-Netzwerke positioniert und behält die Innenansicht (Bild 2). Integriert wird es wahlweise über Mirrorport Switches, Netzwerk-Taps oder als Software-Agent auf bestehenden Gateways (Aufmacherbild). An diesen Stellen liest es passiv und rückwirkungsfrei jegliche Kommunikation und analysiert sie auf Anomalien und Auffälligkeiten.

Erkennung schadhafter Aktivitäten

Das NIDS identifiziert dabei Systeme mit bekannten Schwachstellen und erkennt mehrstufige, komplexe Angriffe durch verhaltensbasierte Kommunikationsanalyse. Diese schadhaften Aktivitäten reichen von ausgenutzten Schwachstellen sowie Netzwerkzugriffen mittels gestohlener Zugangsdaten, über den Eintrag von Malware über die Lieferkette (Hersteller, Dienstleister), bis zu lateralen Bewegungen erfolgreicher Eindringlinge und Konfigurationsveränderungen. Für diese Angriffstaktiken liegen selten Signaturen vor. Das NIDS bildet damit die zweite Linie der Abwehr, indem es Aktivitäten innerhalb der Netzwerke erkennt, welchen Firewalls gegenüber blind sind.

Mastermind der Cybersicherheit

Das SIEM wiederum bildet das Mastermind der Cybersicherheit, indem es alle Datenquellen für Cybersicherheitsmeldungen intelligent zusammenführt und auswertet. Ein SIEM ist deshalb ohne Datenquellen in den jeweiligen zu schützenden Bereichen machtlos. NIDS, Firewalls und verfügbare Logs der OT-Systeme bilden hierbei wichtige Datenquellen.

Den Kopf über Wasser halten

Das kann im ersten Moment überwältigen. Um trotzdem handlungsfähig zu bleiben und sowohl Compliance als auch Cybersicherheit zu gewährleisten, empfiehlt es sich, auf zwei Punkte beim Einsatz von Systemen zur Angriffserkennung zu achten:

1. Die eingesetzten Systeme – insbesondere das häufig für Industrieunternehmen neue NIDS – müssen einfach und zeiteffizient betrieben werden können. Intuitive, aufgeräumte Oberflächen, Fokus auf relevante Funktionen, effektive Filterfunktionen, Schnittstellen zu gängigen SIEM-Systemen wie Splunk und IBM QRadar und eine saubere, sinngebende Darstellung der Anomaliemeldungen sind ein Muss.
2. Der Aufbau und Betrieb der Systeme können schrittweise erfolgen. So ist es durchaus sinnvoll, den Betrieb im Rahmen eines Service Level Agreements gemeinsam mit dem Hersteller zu starten. Diese Form des "Co-Piloting" entlastet die Verantwortlichen im Unternehmen und baut Schritt für Schritt das eigene Knowhow im Bereich der OT-Cybersicherheit auf.

OT-Sicherheit richtig angehen

Ein System zur Angriffserkennung ist mehr als ein paar Firewalls an den Netzwerkgrenzen. Mit der besonders breiten Palette an Cyberrisiken in OT-Netzen müssen dabei sowohl bekannte als auch neuartige Angriffstaktiken detektiert werden können. Die Lösung für ein effektives System zur Angriffserkennung liegt deshalb im Zusammenspiel von Firewalls, einem netzbasierten System zur Angriffserkennung (NIDS) und einem optionalen SIEM. ◄

Referenz

[1] https://www.first.org/blog/20250106-Vulnerability-Forecast-Year-in-Review

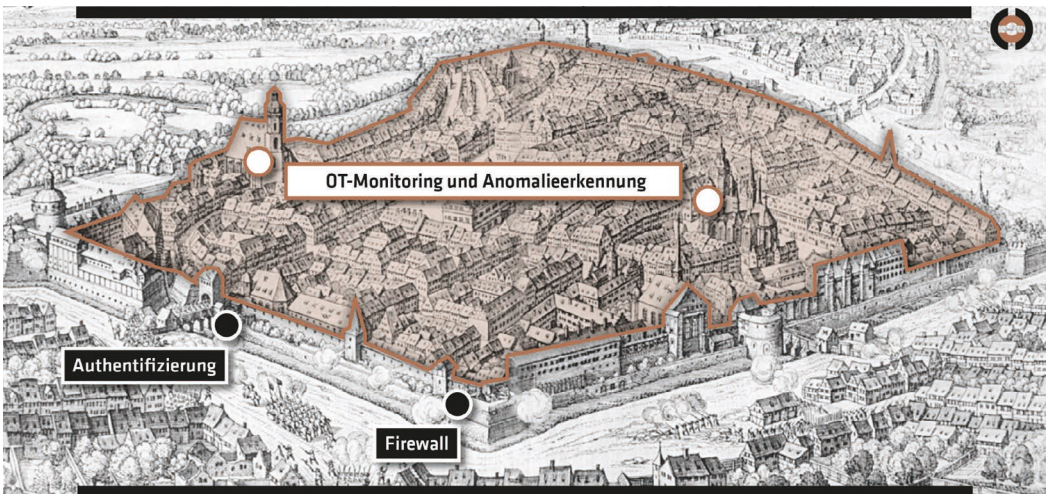


Bild 2: Ein OT-Monitoring bildet die Innere Sicherheit in der OT-Sicherheitsstrategie