So sichert Rhebo die Stationsautomatisierung in Umspannwerken nach der BSI-Empfehlung

PASSIVES SICHERHEITS-MONITORING

RÜCKWIRKUNGSFREIE ANGRIFFSERKENNUNG

KONTINUIERLICHE NETZWERKÜBERWACHUNG

Umspannwerke bilden ein besonders attraktives Ziel für die Akteure hybrider Kriegsführung. Die Anlagen sind meist über weite Flächen verteilt, nicht leicht erreichbar und ohne Cybersicherheitspersonal vor Ort. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) identifiziert eine Vielzahl an Angriffsvektoren, die Firewalls nur ungenügend (bis nicht) erkennen und überwachen können:

- Engineering Workstations (EWS) von internen und externen Mitarbeitenden
- Angriffe über die Lieferkette (Hersteller, Integratoren, Dienstleister)
- exponierte Netzwerkkomponenten
- Schwachstellen in den Fernzugriffstechnologien
- lokale WAN-Verbindungen
- mangelhafter physischer Perimeterschutz.

Hinzu kommen Sicherheitsrisiken aktueller OT-Protokollen wie GOOSE, SV, MMS, IEC-104 oder IEC 61850.

In seiner Veröffentlichung CS 153 »Monitoring in der Stationsautomatisierung« vom März 2025 weist das BSI deshalb Verteilnetzbetreiber darauf hin, auch die lokalen Fernwirktechnik-Netzwerke (OT) zu überwachen. Dies folgt der Pflicht nach einem System zur Angriffserkennung nach dem IT-SiG 2.0 und NIS2.

Das BSI empfiehlt dafür das Zusammenspiel aus drei Monitoring-Ansätzen, die in aufsteigender Reihenfolge an Effektivität und Handhabbarkeit gewinnen:

1. Hostbasiertes Intrusion Detection System (HIDS)
2. Allgemeine Log-Daten
3. Netz(werk)basiertes Intrusion Detection System (NIDS).

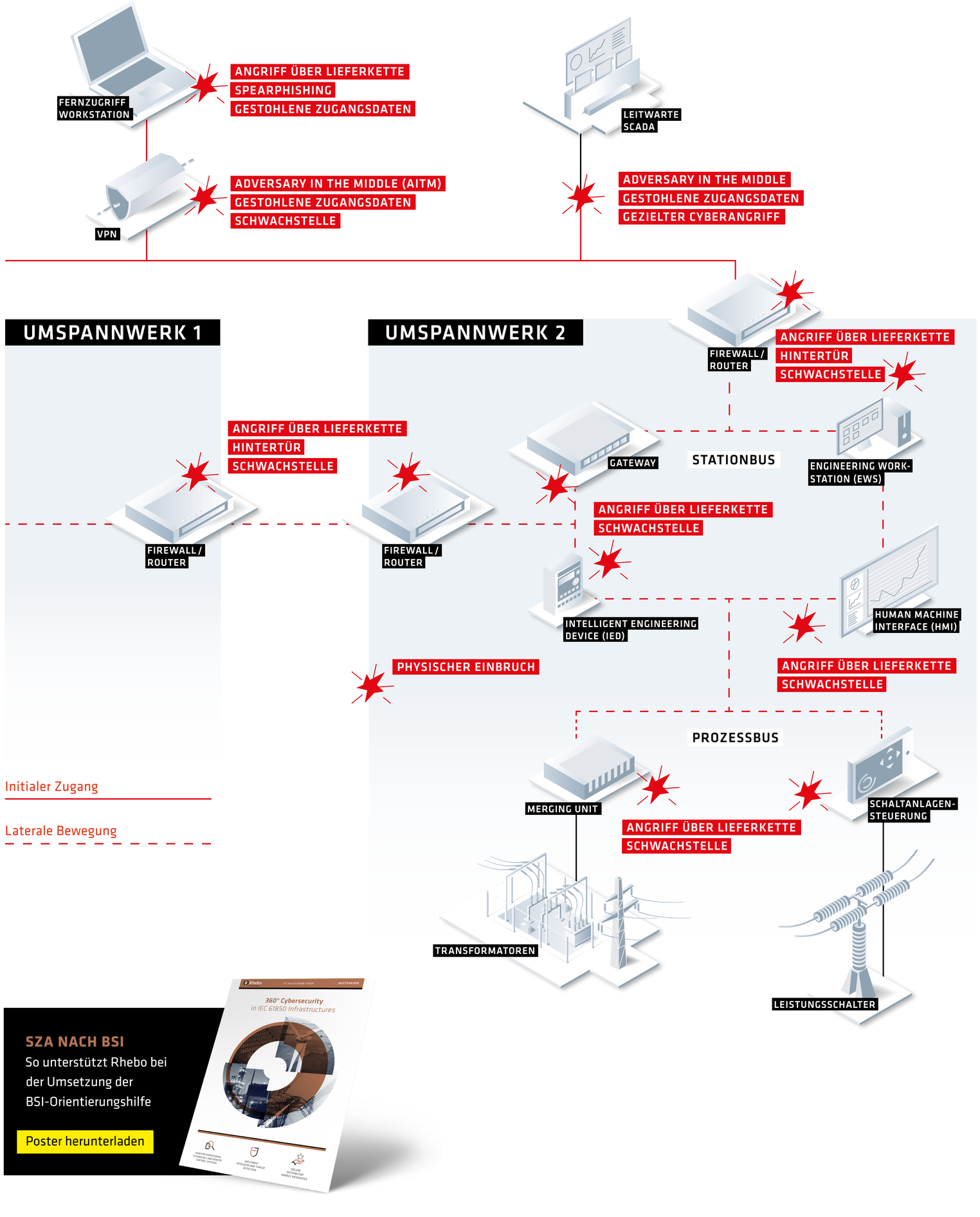
Hostbasierte IDS können aufgrund der Ressourcenknappheit der OT-Komponenten und Limitierungen bei der Dekodierung industrieller Protokolle in der Regel nur auf den IT-Systemen (wie Windows-Server) eingesetzt werden. Die eigentliche OT bleibt damit ein blinder Fleck.

Log-Daten der Komponenten geben Aufschluss über Zugriffe, können die Verantwortlichen jedoch aufgrund der Datenflut und unterschiedlichen Log-Formate überfordern. Weiterhin liefern sie in der Regel keine cybersicherheits-relevanten Informationen.

Ein netzbasiertes IDS dagegen analysiert kontinuierlich die gesamte Kommunikation sowohl des Stationbus als auch des Prozessbus. Anomalien und sicherheitsrelevante Vorgänge werden in Echtzeit gemeldet. Die Integration erfolgt einfach über Mirror Switch Ports oder Netzwerktaps. Die rückwirkungsfreie, rein passive Analyse verhindert ungewollte Eingriffe in die Steuerungsprozesse und Überlastung der überwachten Komponenten.

PUNKTE DER VOM BSI PRIORISIERTEN CYBERRISIKEN IN UMSPANNWERKEN

UND WIE DIESE ANGRIFFE DURCH DAS
NIDS RHEBO INDUSTRIAL PROTECTOR FRÜHZEITIG ERKANNT WERDEN KÖNNEN.



Das Rhebo Industrial Protector NIDS unterstützt die DOKUMENTATION durch

- eine Netzwerkkarte mit aktiven OT-Geräte innerhalb der Umspannwerke
- Informationen zu Verbindungen, Protokollen und Verhaltensmustern der Kommunikation zwischen den Geräten
- Informationen zur Firmware-Version und bekannten Schwachstellen (CVE)

Das Rhebo Industrial Protector NIDS ermöglicht die Echtzeit-ERKENNUNG von

Hintertüren, zum Beispiel durch
- Downloads und Uploads
- versuchte Internetverbindungen

Direkte Cyberangriffe, zum Beispiel durch
- neue Geräte, die innerhalb oder mit der OT kommunizieren
- neue Verbindungen, Protokolle zwischen Geräten
- Internetverbindungen
- Netzwerkscans
- fehlgeschlagene Anmeldeversuche (zum Beispiel durch Brute-Force oder Password Spraying)
- Downloads und Uploads

Physische Einbrüche, zum Beispiel durch
- neue Geräte, die innerhalb oder mit der OT kommunizieren
- neue Verbindungen, Protokolle zwischen Geräten

Gestohlene Anmeldedaten/AitM, zum Beispiel durch
- geändertes Kommunikationsverhalten
- neue Verbindungen, Protokolle zwischen Geräten

Angriff über Lieferkette, zum Beispiel durch
- geändertes Kommunikationsverhalten
- Downloads und Uploads

Technische Fehlerzustände, zum Beispiel durch
- ICMP nicht erreichbar
- TCP-Wiederholungsversuche
- Prüfsummenfehler
- Zeitsynchronisationsfehler

Sicherheitslücken, zum Beispiel durch
- Firmware-Version und bekannte Schwachstellen (CVE-Einträge)

Rhebo Industrial Protector NIDS unterstützt die REAKTION AUF VORFÄLLE mit

- Informationen zu CVE-Risiken für Systeme
- Input für SIEM über Syslog und Warnmeldungen über SNMP
- forensischen Daten zu Sicherheitsvorfällen

NIDS NACH BSI-CS 153 06-2025