# Was Betreibende Kritischer Infrastrukturen beim Einsatz von Systemen zur Angriffserkennung in der Netzleit- und Fernwirktechnik beachten müssen

## SO ERREICHEN SIE MIT RHEBO UND SEINEN PARTNERN INNERHALB DER GESETZLICHEN FRIST UMSETZUNGSGRAD 3 FÜR DEN SCHUTZ IHRER KRITISCHEN INFRASTRUKTUR

Die Orientierungshilfe »Einsatz von Systemen zur Angriffserkennung« des BSI definiert klare Anforderungen an ein Angriffserkennungssystem in Kritischen Infrastrukturen nach dem novellierten IT-Sicherheitsgesetz. Rhebo und seine Partner unterstützen Sie vollumfänglich bei der Planung und Umsetzung des Sicherheitssystems, damit Sie fristgerecht bis 1. Mai 2023 Ihre Cyberresilienz nachweisen und mindestens Umsetzungsgrad 3 für Ihr System zur Angriffserkennung erreichen.

Mit Rhebo OT Security, Rhebo AMI Security und Rhebo IIoT Security bietet Rhebo einfache und effektive Cybersicherheitslösungen für die Netzleit-, Fernwirk- und Steuerungstechnik sowie verteilte industrielle Anlagen in Energieunternehmen und Kritischen Infrastrukturen. Wir unterstützen Sie auf dem gesamten Weg der OT-Sicherheit von der initialen Risikoanalyse bis zum betreuten OT-Monitoring mit Anomalie- und Angriffserkennung.

**ECHTZEIT-SICHTBARKEIT IN DER NETZLEITTECHNIK**
durch Asset Discovery und ICS-Kommunikationsmonitoring

**FRÜHZEITIGE ANGRIFFSERKENNUNG**
durch OT-Anomalieerkennung für schnelle Gefahrenabwehr.

**OT-SICHERHEITS-SERVICES**
von der Infrastruktur-Risikoanalyse über kontinuierliches OT-Monitoring bis zur forensischen Analyse.

| GRUNDFUNKTIONEN | PROTOKOLLIERUNG | | DETEKTION | | | REAKTION |
|---|---|---|---|---|---|---|
| | PLANUNGSZIELE | UMSETZUNGSANFORDERUNGEN | PLANUNGSZIELE | UMSETZUNGSANFORDERUNGEN | | |
| Kontinuierliches Monitoring geeigneter Parameter | Schrittweise Vorgehensweise zur Umsetzung basierend auf Risikoanalyse | SzA erfüllt Basisanforderungen von OPS.1.1.5 »Protokollierung« | umfassende und effiziente Abdeckung der Bedrohungslandschaft | SzA erfüllt Basisanforderungen von »DER.1 – Detektion von sicherheitsrelevanten Ereignissen« | Auswertung ist priorisierte Aufgabe des zuständigen Personals | Automatischer Alarm bei Schwellenwertüberschreitung** |
| Fortwährende Identifikation und Vermeidung von Bedrohungen (§ 8a Absatz 1a Satz 3 BSIG) | Angemessene Sichtbarkeit in angemessener Zeit | Zentrale Speicherung der sicherheitsrelevanten Protokollierungsdaten | Berücksichtigung der Risikoanalyse sowie Unternehmensgröße und -struktur | Kontinuierliche Überwachung und Auswertung von Protokolldaten | Personal ist speziell geschult und qualifiziert | Einleitung qualifizierter Reaktion nach Alarm** |
| Bereitstellen geeigneter Beseitigungsmaßnahmen von Störungen (§ 8a Absatz 1a Satz 3 BSIG) | Erheben, Speichern und Auswerten von Protokollierungsdaten auf System- und Netzebene. Ggf. zusätzliche SzA integrieren, um Verfügbarkeit der Produktivsysteme nicht zu gefährden. | Anzahl zentraler Speicherstellen minimieren (mindestens an funktionalen Einheiten orientieren). | Standardisierte Bestimmung der Abdeckung (z. B. MITRE ATT&CK und MITRE ATT&CK for ICS) | Automatisierte Risikobewertung mit unmittelbarer Alarmierung der Verantwortlichen bei SRE | Angriffserkennung:<br>• wird zentral eingesetzt<br>• erkennt und bewertet alle SRE<br>• erlaubt lückenlose Einsicht und Auswertung aller Daten | Automatische Meldung sicherheitsrelevanter Ereignisse |
| Detektion von SRE (Missbrauchserkennung, Anomalieerkennung) | Berücksichtigung von Speichersystemen für Protokollierungsdaten und deren IT-Sicherheitsvorkehrungen | Ausreichende Dimensionierung (Skalierbarkeit) | Separate Betrachtung von Detektionsmaßnahmen für die IT- und OT-Umgebung | Ereignisprüfung und ggf. Reaktion innerhalb einer der Risikoanalyse entsprechend geringen Zeitspanne | Angriffserkennung setzt aufgezeichnete Ereignisse in Bezug | Automatische Reaktion und automatischer Datenstromeingriff in Netzen, wo Reaktion kritische Dienstleistung nicht gefährdet (i.d.R. IT) |
| Maßnahmen, um Störungen infolge von Angriffen zu verhindern oder auf sie zu reagieren (technisch, organisatorisch) | DSGVO-Compliance | Funktionen zur Filterung, Normalisierung, Aggregation, Korrelierung und Analyse | Benennung von Verantwortlichen | Kontinuierliche Auswertung der Daten | Prozess für manuelle Unterbindung eines Sicherheitsvorfalls, wo automatische Reaktion nicht möglich ist | |
| Abdecken der sicherheitsrelevanten Systeme | Identifikation aller relevanten OT-Systeme für das SzA | Protokoll- und Protokollierungsdaten zur Auswertung geeignet verfügbar machen | Verfahrensanleitung für aktive Suche nach sicherheitsrelevanten Ereignissen durch Mitarbeiter | Regelmäßiges Audit und bei Bedarf Anpassen der Analyseparameter | Begründung eines Ausschlusses von Netzen oder Netzsegmenten von automatischer Reaktion | |
| organisatorische Rahmenbedingungen zur Protokollierung, Detektion und Reaktion sicherstellen | Detektion und Reaktion entsprechend der Risikoanalyse ermöglichen, auch wenn Infrastruktur keine auskömmlichen Protokollierungsereignisse bereitstellt. Ggf. zusätzliche Systeme integieren. | Zeitliche Befristung zur Bearbeitung der Protokolldaten definieren | Ausreichend Personal für Detektion | Regelmäßige, automatische Untersuchung bereits überprüfter Protokollierungsdaten auf SRE | Auslösen von Reaktionen nur bei qualifizierten SRE** | |
| technische Rahmenbedingungen zur Protokollierung, Detektion und Reaktion sicherstellen | Abschätzung des Protokoll- und Protokollierungsdatenaufkommens pro Systemgruppe | Protokollierungsdatenquellen auf Netzebene von außen (Netzgrenzen) nach innen (Netzbereiche) erschließen | Detektion von Schadcode | Informationen zu aktuellen Angriffsmustern und Schwachstellen der eingesetzten Systeme fortlaufend einholen (von Herstellern, Behörden, Medien, etc.) und berücksichtigen | Erfüllt alle Basisanforderungen von DER.2.1 »Behandlung von Sicherheitsvorfällen« | |
| personelle Rahmenbedingungen zur Protokollierung, Detektion und Reaktion sicherstellen | Dokumentation der Planungsphase | Kritische Anwendungen und Applikationen ausgehend von zentralen, kritischen Systemen (z. B. Prozessleittechnik, Leitsystemen) erschließen. Priorisierung nach Kritikalität der Systeme. | Identifikation von Netzsegmenten, die zusätzliche Detektionssysteme benötigen | Kalibrierung der Detektionsmechanismen zur Feststellung von SRE im Normalzustand (Baselining) initial und nach Änderungen innerhalb des Anwendungsbereichs oder der Bedrohungslage | Umsetzung der Standardanforderungen aus DER.2.1 »Behandlung von Sicherheitsvorfällen« für alle Sicherheitsvorfälle, die im Zusammenhang mit Angriffen stehen bzw. stehen könnten. | |
| Informationen zu aktuellen Angriffsmustern für technische Vulnerabilitäten einholen | Dokumentation aller Netzbereiche, Protokollierungsquellen, Beziehungen untereinander und des Datenflusses der Protokollierungsereignisse im Anwendungsbereich | Prozess zur Prüfung der korrekten, vollständigen Umsetzung der Planung | Netzbasierte Intrusion Detection Systeme (NIDS) zwischen internen und externen Netzen | Bewertung des Normalzustandes bzgl. falsch positiver Meldungen & ggf. Änderungen vornehmen | Behandlung von Sicherheitsvorfällen im vermeintlichen Zusammenhang mit Angriffen | |
| Fortlaufende Aktualisierung des SzA | Gruppierung gleicher Systemgruppen innerhalb der Dokumentation | Berücksichtigung weitergehender gesetzlicher oder regulatorischer Anforderungen an die Protokollierung | Zentrale Protokollierungsinfrastruktur für Auswertung von SRE | SRE auf Sicherheitsvorfall (qualifiziertes SRE) überprüfen | Prüfung von Störungen und kritischen Sicherheitsvorfälle auf Meldepflicht nach § 8b Absatz 3 BSIG bzw. §11 Absatz 1c EnWG | |
| Fortlaufende Aktualisierung der Signaturen des SzA | Dokumentation der zu protokollierenden Ereignisse für jedes System bzw. für jede Systemgruppe | | zeitliche Synchronisation der Protokollierungsdaten | Automatisierte Qualifizierung der SRE in eindeutig zuordenbaren Fällen durch SzA | Automatisierte Vermeidung und Beseitigung angriffsbedingter Störungen durch SzA (bei eindeutig qualifizierbaren SRE) | |
| Konfiguration der relevanten Systeme ermöglicht Schwachstellenerkennung | Prozess zur Anpassung der Protokollierung bei Veränderungen | | regelmäßige Kontrolle der Ereignismeldungen auf Auffälligkeiten | Qualifizierung der SRE in nicht eindeutig zuordenbaren Fällen (Anomalien) durch festgelegte Verantwortliche im Unternehmen | keine Beeinträchtigung der kritischen Dienstleistung durch automatisiert ergriffene Maßnahmen | |
| | | | regelmäßige Aktualisierung der Signaturen der Detektionssysteme | Nachjustierung der Detektionsmechanismen basierend auf qualifizierter SRE | Unterstützung auch einer nicht-automatisierten Qualifizierung und Behandlung von Ereignissen | |
| | | | Berücksichtigung externer Quellen zu neuen Erkenntnissen über SRE | Berücksichtigung weitergehender gesetzlicher oder regulatorischer Anforderungen an die Detektion | | |
| | | | Prozesse zur internen:<br>• Verteilung neuer Erkenntnisse an relevante Stellen<br>• Bewertung und Eskalierung sicherheitsrelevanter Erkenntnisse und Informationen aus externen Quellen | | | |
| | | | Personal zur Auswertung der Protokolldaten:<br>• sind beauftragt (intern oder extern)<br>• ausschließlich für diese Aufgabe zuständig | | | |

### LEGENDE

erfüllt Rhebo*

unterstützt Rhebo*

interner Kundenprozess (kann durch Rhebo-Partner unterstützt werden)

Muss Anforderung

Sollte- / Kann-Anforderung

**SzA** System zur Angriffserkennung
**SRE** sicherheitsrelevante Ereignisse

* Die Kategorien »erfüllt Rhebo« und »unterstützt Rhebo« beziehen sich ausschließlich auf die Anforderungen für ein System zur Angriffserkennung in der Operational Technology (OT, Netzleittechnik, Fernwirktechnik)

** in der Orientierungshilfe unter dem Kapitel »Detektion« gelistet

**MATRIX ZUR BSI-ORIENTIERUNGSHILFE SZA 10-2022 V2**
Alle Angaben ohne Gewähr.
Änderungen vorbehalten.
© Rhebo GmbH

Spinnereistr. 7 | 04179 Leipzig | Germany

**rhebo.com**