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 REIFEGRAD 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 Reifegrad 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 überwiegende Aufgabe des 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	Ausreichende Dimensionierung (Skalierbarkeit)	Standardisierte Bestimmung der Abdeckung (z. B. MITRE ATT&CK)	Automatisierte Risikobewertung mit unmittelbarer Alarmierung der Verantwortlichen bei SRE	Angriffserkennung: • wird zentral eingesetzt • erkennt und bewertet alle SRE • 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	Funktionen zur Filterung, Normalisierung, Aggregation, Korrelierung und Analyse	Separate Betrachtung von Detektionsmaßnahmen für die IT- und OT-Umgebung	Benennung von Verantwortlichen	Angriffserkennung setzt aufgezeichnete Ereignisse in Bezug (in einem SIEM)	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	Protokollierungsquellen auf Netzebene von außen (Netzgrenzen) nach innen (Netzbereiche) erschließen		Verfahrensanleitung für aktive Suche nach sicherheitsrelevanten Ereignissen durch Mitarbeiter	Permanente Auswertung der Daten	Begründung eines Ausschlusses von Netzen oder Netzsegmenten von automatischer Reaktion**
Abdecken der sicherheitsrelevanten Systeme	Identifikation aller relevanten OT-Systeme für das SzA	Kritische Anwendungen und Applikationen ausgehend von zentralen, kritischen Systemen (z. B. Prozessleittechnik, Leitsystemen) erschließen. Priorisierung nach Kritikalität der Systeme.		Ausreichend Personal für Detektion	Regelmäßiges Audit und bei Bedarf Anpassen der Analyseparameter	Auslösen von Reaktionen nur bei qualifizierten SRE**
organisatorische Rahmenbedingungen zur Protokollierung, Detektion und Reaktion sicherstellen	Detektion und Reaktion im sinnvollen Rahmen ermöglichen, auch wenn Infrastruktur keine auskömmlichen Protokollierungsereignisse bereitstellen kann	Maximale Protokollierung eingebetteter Systeme, ohne Funktionsfähigkeit des Systems zu beeinträchtigen		Detektion von Schadcode	Regelmäßige, automatische Untersuchung bereits überprüfter Protokollierungsdaten auf SRE	Erfüllt alle Basisanforderungen von DER.2.1 »Behandlung von Sicherheitsvorfällen«
technische Rahmenbedingungen zur Protokollierung, Detektion und Reaktion sicherstellen	Abschätzung des Protokollierungsdatenaufkommens pro Systemgruppe	Prozess zur Prüfung der korrekten, vollständigen Umsetzung der Planung		Identifikation von Netzsegmenten, die zusätzliche Detektionssysteme benötigen	Informationen zu aktuellen Angriffsmustern und Schwachstellen der eingesetzten Systeme fortlaufend einholen (von Herstellern, Behörden, Medien, etc.) und berücksichtigen	Umsetzung der Standardanforderungen aus DER.2.1 »Behandlung von Sicherheitsvorfällen« für alle Sicherheitsvorfälle, die im Zusammenhang mit Angriffen stehen bzw. stehen könnten.
personelle Rahmenbedingungen zur Protokollierung, Detektion und Reaktion sicherstellen	Dokumentation der Planungsphase	Berücksichtigung weitergehender gesetzlicher oder regulatorischer Anforderungen an die Protokollierung		Netzbasierte Intrusion Detection Systeme (NIDS) zwischen internen und externen Netzen	Kalibrierung der Detektionsmechanismen zur Feststellung von SRE im Normalzustand (Baselining) initial und nach Änderungen innerhalb des Anwendungsbereichs oder der Bedrohungslage	Behandlung von Sicherheitsvorfällen im vermeintlichen Zusammenhang mit Angriffen
Informationen zu aktuellen Angriffsmustern für technische Vulnerabilitäten einholen	Dokumentation aller Netzbereiche, Protokollierungsquellen, Beziehungen untereinander und des Datenflusses der Protokollierungsereignisse im Anwendungsbereich			Zentrale Protokollierungsinfrastruktur für Auswertung von SRE	Bewertung des Normalzustandes bzgl. falsch positiver Meldungen & ggf. Änderungen vornehmen	Meldung kritischer Sicherheitsvorfälle (inkl. Angriffe) an zuständige Behörde
Fortlaufende Aktualisierung des SzA	Gruppierung gleicher Systemgruppen innerhalb der Dokumentation			zeitliche Synchronisation der Protokollierungsdaten	SRE auf Sicherheitsvorfall (qualifiziertes SRE) überprüfen	Automatisierte Vermeidung und Beseitigung angriffsbedingter Störungen durch SzA (bei eindeutig qualifizierbaren SRE)
Fortlaufende Aktualisierung der Signaturen des SzA	Dokumentation der zu protokollierenden Ereignisse für jedes System bzw. für jede Systemgruppe			regelmäßige Kontrolle der Ereignismeldungen auf Auffälligkeiten	Automatisierte Qualifizierung der SRE in eindeutig zuordenbaren Fällen durch SzA	keine Beeinträchtigung der kritischen Dienstleistung durch automatisiert ergriffene Maßnahmen
Konfiguration der relevanten Systeme ermöglicht Schwachstellenerkennung	Prozess zur Anpassung der Protokollierung bei Veränderungen			regelmäßige Aktualisierung der Signaturen der Detektionssysteme	Qualifizierung der SRE in nicht eindeutig zuordenbaren Fällen (Anomalien) durch festgelegte Aufgabenbereich im Unternehmen	Unterstützung auch einer nicht-automatisierten Qualifizierung und Behandlung von Ereignissen
				Berücksichtigung externer Quellen zu neuen Erkenntnissen über SRE	Nachjustierung der Detektionsmechanismen basierend auf qualifizierter SRE	
				Prozesse zur internen: • Verteilung neuer Erkenntnisse an relevante Stellen • Bewertung und Eskalierung sicherheitsrelevanter Erkenntnisse und Informationen aus externen Quellen	Einbindung des SzA in SIEM-Lösung	
				Personal zur Auswertung der Protokolldaten: • sind beauftragt (intern oder extern) • ausschließlich für diese Aufgabe zuständig	Berücksichtigung weitergehender gesetzlicher oder regulatorischer Anforderungen an die Detektion	

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 09-2022

Spinnereistr. 7 | 04179 Leipzig | Germany

rhebo.com