ENGINSIGHT

BSI-Orientierungshilfe:
Enginsight erfüllt fast 60 % der Anforderungen*

So gelingt die automatische Angriffserkennung in kritischen Infrastrukturen

GRUNDLAGEN

- Kontinierliche und automatische Erfassung und Auswertung geeigneter Parameter
- Fortwährende Identifikation und Vermeiden von Bedrohungen (§ 8a Absatz 1a Satz 3 BSIG)
- Sicherheitsrelevante Ereignisse erkennen (Detektion)
- Technische und organisatorische Maßnahmen, um Störungen infolge von Angriffen zu verhindern oder auf sie zu reagieren
- Alle für die Funktionsfähigkeit relevanten Systeme, Komponenten oder Prozesse, abdecken
- Die notwendigen technischen, organisatorischen und personellen Rahmenbedingungen schaffen
- Fortlaufende Informationen zu aktuellen Angriffsmustern für technische Vulnerabilitäten einholen
- Alle zur effektiven Angriffserkennung erforderliche Hard- u. Software durchweg aktuell halten
- Die Signaturen von Detektionssystemen immer aktuell halten
- Alle relevanten Systeme so konfigurieren, dass Versuche, bekannte Schwachstellen auszunutzen, erkannt werden können

PROTOKOLLIERUNG

PLANUNG

- Schrittweises Vorgehen für die Umsetzung der Protokollierung basierend auf der Risikoanalyse
- Schrittwahl nach angemessener Sichtbarkeit innerhalb angemessener Zeit
- Erheben, Speichern und Bereitstellen der notwendigen Protokoll- und Protokollierungsdaten auf System- bzw. Netzebene
- Zusätzliche Speichersysteme zur Protokollierung
- Die zur Speicherung notwendigen Systeme u. deren IT-Sicherheitsvorkehrungen bedenken
- Umgang mit Protokollierungsdaten entspr. der DSGVO (Anonymisierung bzw. Pseudonymisierung)
- Alle maßgeblichen Systeme identifizieren,damit deren Protokollierungsdaten später erfasst werden können
- Protokollierungsinfrastruktur so anpassen und/oder. ergänzen, um Detektion und Reaktion entsprechend der Risikoanalyse notwendigen Rahmen zu ermöglichen
- Protokollierungsdatenaufkommen anhand eines repräsentativen Systems pro Systemgruppe abschätzen
- Die Ergebnisse der Planungsphase in einer geeigneten Form dokumentieren
- Dokumentation aller Netzbereiche, Protokollierungsdatenquellen, deren Beziehungen u. Datenfluss der Protokoll- u. Protokollierungsdaten im Anwendungsbereich in angemessenem Abstraktions-/Detailgrad
- Gruppierung gleicher Systemgruppen innerhalb der Dokumentation
- Gleiche bzw. sehr ähnliche Netze zusammenfassen
- Für jedes System bzw. jede Systemgruppe dokumentieren, welche Ereignisse dieses bzw. diese protokolliert
- Prozess einrichten, der sicherstellt, dass die Protokollierung bei Changes angepasst wird

UMSETZUNG

- Alle Basisanforderungen von OPS.1.1.5 Protokollierung erfüllen
- Alle gesammelten sicherheitsrelevanten Protokoll- und Protokollierungsdaten an für den jeweiligen Netzbereich zentralen Stellen speichern
- Die Anzahl zentraler Speicherstellen möglichst geringhalten und an funktionalen Einheiten orientieren, damit der Zugriff einfach erfolgen kann
- Protokollierungsinfrastruktur ausreichend dimensionieren
- Genügend technische, finanzielle und personelle Ressourcen
- Protokoll- und Protokollierungsdaten filtern, normalisieren, aggregieren
- Protokoll- und Protokollierungsdaten geeignet verfügbar machen, damit sie ausgewertet werden können
- Zeitlich befristete Speicherung unbearbeiteter Protokolldaten kann den Detektionsprozess zusätzlich unterstützen
- Protokollierungsdatenquellen auf Netzebene von außen (Netzgrenzen) nach innen (Netzbereiche) erschließen
- Systemebene (kritische Anwendungen und Applikationen) ausgehend von den zentralen, kritischen Systemen erschließen (z. B. Prozessleit- u. Automatisierungstechnik u. Leitsysteme)
- Priorisierung zur Auswahl der Protokollierungsdatenquellen von der Kritikalität der Systeme ableiten
- Nach erfolgreicher Umsetzung prüfen, ob alle Protokollierungsdatenquellen gemäß der Planung umgesetzt wurden
- Branchenspezifisch weitergehende gesetzliche oder regulatorische Anforderungen an die Protokollierung, ebenfalls entsprechend umsetzen

DETEKTION

PLANUNG

- Auswahl und Einsatz von Detektionsmaßnahmen für eine umfassende und effiziente Abdeckung der Bedrohungslandschaft
- Ggf. separate Betrachtung von Detektionsmaßnahmen für die IT- und OT-Umgebung
- Ergebnisse der Risikoanalyse sowie die Größe und Struktur des Unternehmens einbeziehen
- Zur Bestimmung der Abdeckung eine standardisierte Methode anwenden (z. B. MITRE ATT&CK bzw. ATT&CK for ICS)

UMSETZUNG

- Kontinuierliche Überwachung und Auswertung aller Protokolldaten
- Automatisierung durch unmittelbare Alarmierung der Verantwortlichen bei relevanten Ereignissen
- Ereignisprüfung und ggf. die -reaktion einer der Risikoanalyse entsprechend geringen Zeitspanne
- Zuständige Mitarbeitende von Dienstleistern benennen
- Verfahrensanleitungen für die Verantwortlichen, die aktiv nach sicherheitsrelevanten Ereignissen suchen
- Genügend technische, finanzielle und personelle Ressourcen bereitstellen
- Schadcodedetektionssysteme einsetzen und zentral verwalten
- Anhand des Netzplans festlegen, welche Netzsegmente durch zusätzliche Detektionssysteme geschützt werden müssen
- Die im Netzplan definierten Übergänge zwischen internen u. externen Netzen um netzbasierte Intrusion Detection Systeme (NIDS) ergänzen
- Zeitliche Synchronisation der Protokollierungsdaten
- Protokollierungsdaten regelmäßig nach Auffälligkeiten kontrollieren
- Signaturen der Detektionssysteme regelmäßig aktualisieren
- Externe Quellen für neue Erkenntnisse zu sicherheitsrelevanten Ereignissen heranziehen
- Sicherstellen, dass Meldungen als relevant erkannt und an die richtige Stelle weitergeleitet werden
- Informationen aus zuverlässigen Quellen grundsätzlich auswerten
- Alle gelieferten Informationen nach Relevanz bewerten, ggf. entsprechend der Sicherheitsvorfallbehandlung eskalieren
- Personal (intern oder extern) zur Auswertung der Protokollierungdaten beauftragen
- Die Auswertung ist prisorierte Aufgabe der Auswertenden
- Weiterführende Schulungen und Qualifikationen für die Auswertenden
- Zentrale Komponenten zur Erkennung und Auswertung einsetzen
- Zentrale automatisierte Analysen mit Softwaremitteln einsetzen (aufzeichnen, in Bezug setzen und sicherheitsrelevante Vorgänge sichtbar machen)
- Alle eingelieferten Protokoll- und Protokollierungsdaten lückenlos in der Protokollverwaltung einsehbar und auswertbar
- Daten kontinuierlich auswerten
- Automatisch Alarmierung beim Überschreiten definierter Schwellenwerte
- Verantwortlichen Personenkreis für die Auswertung der Protokoll- und Protokollierungsdaten benennen
- Im Alarmfall (nach fachlicher Bewertung und innerhalb einer der Risikoanalyse entsprechend geringen Zeitspanne) eine qualifizierte und bedarfsentsprechende Reaktion einleiten
- Analyseparameter regelmäßig auditieren und anpassen, falls erforderlich
- Protokoll- und Protokollierungsdaten regelmäßig automatisch untersuchen hinsichtlich sicherheitsrel. Ereignisse
- Meldungen zu aktuellen Angriffsmustern aus versch. Quellen berücksichten und in dokumentierte Prozesse des Schwachstellenmanagements einfließen lassen
- Initiale Kalibrierung, um festzustellen, welche sicherheitsrel. Ereignisse im Normalzustand auftreten (Baselining)
- Normalzustand der falsch positiven Meldungen bewerten, ggf. anpassen
- Kalibrierung bei Änderungen innerhalb des Anwendungsbereichs oder der Bedrohungslage erneut durchführen
- SRE auf Sicherheitsvorfall überprüfen und bewerten
- Die zur Angriffserkennung eingesetzten Systeme sollten, in eindeutig zuordenbaren Fällen, eine automatisierte Qualifizierung der SRE ermöglichen
- Nur qualifizierte SRE lösen den Prozess der Reaktion aus
- Qualifizierung in automatisiert nicht eindeutig zuordenbaren Fällen manuell durch festgelegte Verantwortliche
- Detektionsmechanismen basierend auf den gewonnenen Erkenntnissen der Qualifizierung nachjustieren

REAKTION

- Mindestanforderung für die Reaktion: alle Basisanforderungen von DER.2.1. Behandlung von Sicherheitsvorfällen, die im Zusammenhang mit Angriffen stehen bzw. stehen könnten.
- Alle Standardanforderungen aus DER.2.1
- Automatische Meldung bei einem SRE durch die eingesetzten Detektionssysteme
- Automatische Reaktion und Datenstromeingriff in Netzen muss möglich sein
- Ggf. manuelle Reaktion zum Unterbinden eines möglichen Sicherheitsvorfall
- Ausschluss von Netzen oder Netzsegmenten von einer automatischen Reaktion, bzw. dem Eingriff in den Datenstrom begründen
- Festgestellte Sicherheitsvorfälle im vermeintlichen Zusammenhang mit Angriffen müssen behandelt werden
- Bei Störungen und Sicherheitsvorfällen prüfen, ob diese den Kriterien der Meldepflicht nach § 8b Absatz 3 BSIG bzw. §11 Absatz 1c EnWG entsprechen und eine Meldung an das BSI notwendig ist
- Automatisiert Maßnahmen zum Vermeiden und Beseitigen von angriffsbedingten Störungen, sofern das zu Grunde liegende SRE eindeutig qualifizierbar ist
- Gewährleisten, dass ausschließlich automatisiert ergriffene Maßnahmen nicht zu einer relevanten Beeinträchtigung der kritischen Dienstleistung des Betreibers führen können
- Die eingesetzten SzA sollten auch eine nicht-automatisierte Qualifizierung und Behandlung von Ereignissen unterstützen

LEGENDE

*Zusammen mit den Services der Enginsight-Partner gelingen fast 85 % Abdeckung. Die restlichen 15 % sind organisatorischer Art.

erfüllt	unterstützt	organisatorisch
muss	sollte	kann

REIFEGRADE

Stufe 3: Alle Muss-Anforderungen erfüllt
Stufe 4: Alle Muss- und Sollte-Anforderungen erfüllt
Stufe 5: Alle Anforderungen erfüllt

Matrix zur BSI-Orientierungshilfe SZA, Stand 11-2023.
Alle Angaben ohne Gewähr. Änderungen vorbehalten.

Enginsight GmbH
Leutragraben 1
07745 Jena
enginsight.com

Mit Enginsight Ihre IT-Sicherheit optimieren und Compliance-Anforderungen effizient erfüllen.

Jetzt Termin vereinbaren