dacoso

Die KRITIS-Checkliste: alle Muss-Anforderungen des IT-SiG 2.0 auf einen Blick

Mit dieser Checkliste erhalten Sie den Überblick darüber, welche Anforderungen KRITIS-Organisationen ab 01.05.2023 erfüllen müssen. Dabei haben wir neben den Gesetzestexten des IT-Sicherheitsgesetz 2.0 auch die BSI-Orientierungshilfe und weitere wichtige Dokumente wie BS3-Standards berücksichtigt. Überprüfen Sie Schritt für Schritt, wie es aktuell um Ihre Compliance steht.

Sie haben mindestens einmal „Nicht erfüllt“ angekreuzt? Unser KRITIS-Experte David Haas bespricht gerne mit Ihnen Ihre Situation und klärt offene Fragen im direkten Gespräch.

Vereinbaren Sie einen Termin unter **kritis@dacoso.com**!

Muss-Anforderungen	Erfüllt	Nicht erfüllt
Grundfunktionen		
Kontinuierliches Monitoring geeigneter Parameter		
Detektion von sicherheitsrelevanten Ereignissen (SRE) zur Missbrauchs- oder Anomalieerkennung		
Abdeckung der sicherheitsrelevanten IT/OT-Systeme		
Technische Rahmenbedingungen zur Protokollierung, Detektion und Reaktion sicherstellen		
Informationen zu aktuellen Angriffsmustern für technische Vulnerabilitäten einholen		
Fortlaufende Aktualisierung der Systeme zur Angriffserkennung (SzA)		
Fortlaufende Aktualisierung der Signaturen der Systeme zur Angriffserkennung (SzA)		
Konfiguration der relevanten Systeme zur Ermöglichung der Schwachstellenerkennung		
Kontinuierliches Monitoring geeigneter Parameter		
Detektion von sicherheitsrelevanten Ereignissen (SRE) zur Missbrauchs- oder Anomalieerkennung		
Organisatorische Rahmenbedingungen zur Protokollierung, Detektion und Reaktion sicherstellen (ISMS, BCM, etc.)		
Personelle Rahmenbedingungen zur Protokollierung, Detektion und Reaktion sicherstellen (z.B. 24/7-Hotline)		
Protokollierung		
Herbeiführung einer angemessenen Sichtbarkeit in angemessener Zeit		
Erhebung, Speicherung und Auswertung von Protokollierungsdaten auf System- und Netzebene		
Berücksichtigung von Speichersystemen für Protokollierungsdaten und deren IT-Sicherheitsvorkehrungen		
Identifikation aller relevanten IT/OT-Systeme für die Berücksichtigung in den Systemen zur Angriffserkennung		
Dokumentation der Planungsphase		
Dokumentation der zu protokollierenden Ereignisse für jedes System bzw. für jede Systemgruppe		
Prozess zur Anpassung der Protokollierung bei Veränderungen		
Systeme zur Angriffserkennung erfüllen die Basisanforderungen von OPS.1.1.5 "Protokollierung" vollumfänglich		
Zentrale Speicherung der sicherheitsrelevanten Protokollierungsdaten		
Ausreichende Dimensionierung zur Skalierbarkeit		
Funktionen zur Filterung, Normalisierung, Aggregation, Korrelierung und Analyse		

Muss-Anforderungen	Erfüllt	Nicht erfüllt
Protokoll- und Protokollierungsdaten zur Auswertung geeignet verfügbar machen		
Definition der zeitlichen Befristung zur Bearbeitung der Protokolldaten		
Prozess zur Prüfung der korrekten, vollständigen Umsetzung gemäß der Planung		
Berücksichtigung weitergehender gesetzlicher oder regulatorischer Anforderungen an die Protokollierung (wenn vorhanden, z.B. bei erhöhtem Schutzbedarf)		
Detektion		
Umfassende und effiziente Abdeckung der gesamten Bedrohungslandschaft in IT und OT		
Berücksichtigung der Risikoanalyse sowie Unternehmensgröße, Struktur, Kritikalität der Dienstleistung		
Systeme zur Angriffserkennung erfüllen die Basisanforderungen von "DER.1 - Detektion von sicherheitsrelevanten Ereignissen"		
Kontinuierliche Überwachung und Auswertung von Protokolldaten		
Ereignisprüfung und ggf. Reaktion innerhalb einer der Risikoanalyse entsprechend geringen Zeitspanne		
Vorsehen einer ausreichenden Anzahl an Personal für die Detektion		
Detektion von schadhaftem Code		
Identifikation von Netzsegmenten, die zusätzliche Detektionssysteme benötigen, anhand eines Netzplans		
Sicherung der im Netzplan definierten Übergänge zwischen internen und externen Netzen		
Angriffserkennung wird zentral eingesetzt, erkennt und bewertet alle sicherheitsrelevanten Ereignisse und erlaubt lückenlose Einsicht und Auswertung aller Daten		
Angriffserkennung setzt aufgezeichnete Ereignisse in Bezug		
Kontinuierliche Auswertung der Daten		
Sicherstellung der Aus- und Bewertung von Informationen aus zuverlässigen Quellen		
Regelmäßige Auditierung und bei Bedarf Anpassung der Analyseparameter		
Regelmäßige und automatische Untersuchung bereits überprüfter Protokollierungsdaten auf sicherheitsrelevante Ereignisse		
Regelmäßige Aktualisierung der Signaturen der eingesetzten Detektionssysteme		
Fortlaufendes Einholen und Berücksichtigung von Information zu aktuellen Angriffsmustern und Schwachstellen der eingesetzten Systeme (Hersteller, Behörden, TI-Feeds, Darknet etc.)		
Bewertung des Normalzustandes bzgl. false-positive Meldungen und ggf. notwendiger Änderungen		
Berücksichtigung externer Quellen zu neuen Erkenntnissen über sicherheitsrelevante Ereignisse		
Überprüfung von sicherheitsrelevanten Ereignissen auf Sicherheitsvorfälle und ggf. Eskalation		
Kontinuierliche Nachjustierung der Detektionsmechanismen basierend auf qualifizierten sicherheitsrelevanten Ereignissen		
Benennung von Verantwortlichen Mitarbeitenden bzw. Mitarbeitenden von Dienstleistern		

Muss-Anforderungen	Erfüllt	Nicht erfüllt
Verfahrensanleitung für die aktive Suche nach sicherheitsrelevanten Ereignissen durch Mitarbeitende		
Einrichtung einer zentralen Protokollierungsinfrastruktur für die Auswertung von sicherheitsrelevanten Ereignissen		
Berücksichtigung weitergehender gesetzlicher und regulatorischer Anforderungen an die Detektion		
Reaktion		
Erfüllung der Basisanforderungen aus DER.2.1 "Behandlung von Sicherheitsvorfällen", für alle Sicherheitsvorfälle, die im Zusammenhang mit Angriffen stehen bzw. stehen könnten		
Automatischer Alarm bei Schwellwertüberschreitung (s. Orientierungshilfe "Detektion")		
Einleitung qualifizierter Reaktion nach Alarm		
Automatische Meldung sicherheitsrelevanter Ereignisse		
Automatische Reaktion und Eingriff in Netze, bei denen die Reaktion die kritische Dienstleistung nicht gefährdet		
Behandlung von Sicherheitsvorfällen im vermeintlichen Zusammenhang mit Angriffen		
Prozess zur manuellen Unterbindung eines Sicherheitsvorfalls, bei dem die automatische Reaktion nicht möglich ist		
Begründung eines Ausschlusses von Netzen, oder Segmenten von einer automatischen Reaktion		
Prüfung von Störungen und kritischen Sicherheitsvorfällen auf die Meldepflicht nach §8b Abs. 3 BSIG bzw. §11 Abs. 1c EnWG (BSI-Kontaktstelle)		

Über dacoso

dacoso ist ein führender IT-Dienstleister für Netzwerkperformance und Datensicherheit in Deutschland, Österreich und der Schweiz. Der Fokus liegt auf Managed Services für Optical Networks, Intelligent Networks und Cyber Security, die dacoso für seine Geschäftskunden im eigenen Security Operations Center (SOC) in Deutschland betreibt. Ergänzt werden diese durch Mehrwertdienste wie Beratung, Beschaffung und Installation. Viele KRITIS-Organisationen vertrauen schon heute auf dacoso. Das Fundament ist das starke dacoso-Team: kompetent, zuverlässig, flexibel - und immer nah am Kunden. Die dacoso GmbH ist ein inhabergeführtes Unternehmen mit Hauptsitz in Langen bei Frankfurt a.M. und 11 weiteren Standorten in Deutschland, Österreich und der Schweiz.