# Checkliste

|  |  |  |  |
| --- | --- | --- | --- |
| Anforderungsnr. | Name | Umsetzungsgrad | Status |
| 84 | **Umgang mit Schwachstellen, Störungen und Fehlern - Prüfung offener Schwachstellen** Die IT-Systeme, welche der KRITIS-Betreiber für die Entwicklung und Erbringung der kritischen Dienstleistung verwendet, werden mindestens monatlich automatisiert auf bekannte Schwachstellen (Vulnerabilities) geprüft. | UG5 |  |
| 90 | **Systematische Log-Auswertung - Konzept** Richtlinien und Anweisungen mit technischen und organisatorischen Maßnahmen sind gemäß SA-01 dokumentiert, kommuniziert und bereitgestellt, um Ereignisse auf allen Assets, die zur Entwicklung oder zum Betrieb der kritischen Dienstleistung verwendet werden, zu protokollieren und an zentraler Stelle aufzubewahren. | UG5 |  |
| 91 | **Systematische Log-Auswertung - kritische Assets** Der KRITIS-Betreiber führt eine Liste aller protokollierungs- und überwachungskritischen Assets und überprüft diese Liste regelmäßig auf deren Aktualität und Korrektheit. | UG5 |  |
| 92 | **Systematische Log-Auswertung - Aufbewahrung** Die erstellten Protokolle werden auf zentralen Protokollierungsservern aufbewahrt, wo sie vor unautorisierten Zugriffen und Veränderungen geschützt sind. | UG5 |  |
| 93 | **Systematische Log-Auswertung - Konfiguration** Der Zugriff und die Verwaltung der Protokollierungs- und Überwachungsfunktionen sind beschränkt auf ausgewählte und autorisierte Mitarbeiter des KRITIS-Betreibers. | UG5 |  |
| 94 | **Systematische Log-Auswertung - Verfügbarkeit** Die Verfügbarkeit der Protokollierungs- und Überwachungssoftware wird unabhängig überwacht. | UG5 |  |
| 95 | **Penetrationstest** Der KRITIS-Betreiber lässt mindestens jährlich Penetrationstests durch qualifiziertes internes Personal oder externe Dienstleister durchführen. | UG5 |  |
| 96 | **Umgang mit Schwachstellen, Störungen und Fehlern - Integration mit Änderungs- und Incident-Management** Richtlinien und Anweisungen mit technischen und organisatorischen Maßnahmen für den Umgang mit kritischen Schwachstellen sind gemäß SA-01 dokumentiert, kommuniziert und bereitgestellt. | UG5 |  |
| 101 | **Planung der Protokollierung** |  |  |
| 101.3 | Hierzu KÖNNEN zusätzliche Systeme eingesetzt werden, sodass zur wirksamen Angriffserkennung nicht jedes einzelne Gerät Protokollierungs-daten aufzeichnen muss und damit die Verfügbarkeit der Produktivsysteme und damit der kritischen Dienstleistung gewährleistet werden kann. | UG5 |  |
| 101.6 | Das anfallende Protokoll- und Protokollierungsdatenaufkommen KANN (und wird dringend empfohlen) anhand eines repräsentativen Systems pro Systemgruppe bestimmt werden. | UG5 |  |
| 103 | **Protokollierung auf System- und Netzebene** |  |  |
| 103.8 | Eine zeitlich befristete Speicherung der unbearbeiteten Protokolldaten KANN den Detektionsprozess zusätzlich unterstützen. | UG5 |  |
| 104 | **Planung der Detektion** |  |  |
| 104.2 | Zur Bestimmung der Abdeckung KANN (und es wird empfohlen) eine standardisierte Methode angewendet werden (z. | UG5 |  |
| 110 | **Kontinuierliche Überwachung und Auswertung von Protokoll- und Protokollierungsdaten** |  |  |
| 110.2 | Dies KANN automatisiert werden, wenn bei relevanten Ereignissen eine unmittelbare Alarmierung der Verantwortlichen gewährleistet ist. | UG5 |  |