# 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. Im Falle von Abweichungen zu den erwarteten Konfigurationen (u.a. dem erwarteten Patch-Level) werden die Gründe hierzu zeitnah analysiert und die Abweichungen behoben oder gemäß dem Ausnahmeprozess dokumentiert. | 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. Die Protokollierung umfasst definierte Ereignisse, welche die Sicherheit und Verfügbarkeit der kritischen Dienstleistung beeinträchtigen können, einschließlich einer Protokollierung des Aktivierens, Stoppens und Pausierens der verschiedenen Protokollierungen. Die Protokolle werden bei unerwarteten oder auffälligen Ereignissen durch autorisiertes Personal anlassbezogen überprüft, um eine zeitnahe Untersu-chung von Störungen und Sicherheitsvorfällen sowie das Einleiten geeigne-ter Maßnahmen zu ermöglichen. Ergänzende Informationen zur Basisanforderung Sicherheitsrelevante Ereignisse sind u. a. e An- und Abmeldevorgänge e Erstellung, Änderung oder Löschung von Benutzern und Erweiterung der Berechtigungen e Verwendung, Erweiterung und Änderungen von privilegierten Zugriffs-berechtigungen e Nutzung von temporären Berechtigungen. Da es sich bei den protokollierten Daten i. d. R. um personenbezogene Daten handelt, sind in dem Fall datenschutzrechtliche Anforderungen an die Auf-bewahrung zu beachten und zu überprüfen. Erfahrungsgemäß sollte eine Frist von einem Jahr nicht überschritten werden. | 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. Für diese kritischen Assets wurden Protokollierungs- und Überwachungsmaßnahmen definiert. | UG5 |  |
| 92 | **Systematische Log-Auswertung - Aufbewahrung** Die erstellten Protokolle werden auf zentralen Protokollierungsservern aufbewahrt, wo sie vor unautorisierten Zugriffen und Veränderungen geschützt sind. Protokolldaten sind unverzüglich zu löschen, wenn sie zur Erreichung des Zwecks nicht mehr erforderlich sind. Zwischen den Protokollierungsservern und den protokollierten Assets erfolgt eine Authentifizierung, um die Integrität und Authentizität der übertragenen und gespeicherten Informationen zu schützen. Die Übertragung erfolgt nach einer dem Stand der Technik entsprechenden Verschlüsselung oder über ein eigenes Administrationsnetz (Out-of-Band-Management). | 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. Änderungen der Protokollierungen und Überwachungen werden vorab durch unabhängige und autorisierte Mitarbeiter überprüft und freigegeben. Der Zugriff und die Verwaltung der Protokollierungs- und Überwachungsfunktionen erfordern eine Multi-Faktor-Authentifizierung. | UG5 |  |
| 94 | **Systematische Log-Auswertung - Verfügbarkeit** Die Verfügbarkeit der Protokollierungs- und Überwachungssoftware wird unabhängig überwacht. Bei einem Ausfall der Protokollierungs- und Überwachungssoftware werden die verantwortlichen Mitarbeiter umgehend informiert. Die Protokollierungs- und Überwachungssoftware ist redundant vorhanden, um auch bei Ausfällen die Sicherheit und Verfügbarkeit der Systeme der kritischen Dienstleistung zu überwachen. | UG5 |  |
| 95 | **Penetrationstest** Der KRITIS-Betreiber lässt mindestens jährlich Penetrationstests durch qualifiziertes internes Personal oder externe Dienstleister durchführen. Die Penetrationstests erfolgen nach einer dokumentierten Testmethodik und umfassen die für den sicheren Betrieb der kritischen Dienstleistung als kritisch definierten Infrastruktur-Komponenten, die im Rahmen einer Risiko-Analyse als solche identifiziert wurden. Art, Umfang, Zeitpunkt/Zeitraum und Ergebnisse werden für einen sachverständigen Dritten nachvollziehbar dokumentiert. Feststellungen aus den Penetrationstests werden bewertet und mindestens bei mittlerer bis sehr hoher Kritikalität in Bezug auf die Vertraulichkeit, Integrität oder Verfügbarkeit der kritischen Dienstleistung nachverfolgt und behoben. Die Einschätzung der Kritikalität und der mitigierenden Maßnahmen zu den einzelnen Feststellungen werden dokumentiert. | 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. Die Maßnahmen sind mit den Aktivitäten des Änderungsverfahrens (Change Management) und der Störungs- und Fehlerbehebung (Incident Management) abgestimmt. | 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. B. MITRE ATT&CK bzw. ATT&CK for ICS). In Abhängigkeit der Unternehmensgröße und der Bedrohungslandschaft KANN eine separate Betrachtung von Detektionsmaßnahmen für die IT- und OT-Umgebung erforderlich sein. | 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 |  |