Log-Management zur Einhaltung von IT-SiG und B3S

Was KRITIS-Betreiber jetzt beachten müssen

Mit dem IT-Sicherheitsgesetz 2.0 (IT-SiG) haben sich die Pflichten für KRITIS-Betreiber nochmals verschärft. So müssen sie nun technische und organisatorische Maßnahmen einführen, die der Prävention gegen IT-Vorfälle, deren Detektion oder Mitigation dienen und dem Stand der Technik entsprechen. Logfiles, also Protokolldateien, die Ereignisse dokumentieren, spielen dabei eine zentrale Rolle.

Von Sanjo Franz, SYSTEMA Gesellschaft für angewandte Datentechnik mbH

Zur Einhaltung zahlreicher Gesetzgebungen und Regulatorien im Bereich Datenschutz und Datensicherheit sind die Verfügbarkeit, Integrität und Vertraulichkeit der eingesetzten IT-Systeme sowie die Authentizität der Informationen heute eine bedingungslose Grundvoraussetzung. Gemäß BSI-Gesetz und IT-Sicherheitsgesetz (IT-SiG) sind hier die Betreiber kritischer Infrastrukturen seit 2015 verpflichtet, angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen und zur Erhöhung der IT-Sicherheit zu treffen. Dabei müssen zentrale Vorgaben aus der Regulatorik (DSGVO, BSIG, BDSG …) erfüllt und bestehende Standards (ITIL, ISO 27001, BSI IT-Grundschutz, B3S …) eingehalten werden. Mit der Erweiterung des im Mai 2021 in Kraft getretenen IT-Sicherheitsgesetzes 2.0 haben sich die Pflichten (Meldepflicht, Registrierung) für KRITIS-Betreiber nochmals verschärft. Zudem fallen nach neuer KRITIS-Verordnung nun auch Unternehmen im besonderen öffentlichen Interesse (UBI/UNBÖFI) und deren Zulieferer unter die Regulierung.

Log-Management ist keine Kür, sondern Pflicht

Tagtäglich verarbeiten IT-gestützte Systeme personenbezogene Daten und vertrauliche Geschäftsinformationen. Um gesetzliche Anforderungen an den Datenschutz zu erfüllen und die Nachvollziehbarkeit von sicherheitsrelevanten Ereignissen zu gewährleisten, müssen KRITIS-Betreiber technische und organisatorische Maßnahmen im Sinne der Kritikalität (Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der Daten) entwickeln. Diese Anforderungen setzen den Einsatz einer Log-Management-Lösung zur Protokollierung von Störungen, Informationssicherheitsvorfällen, Datenzugriffen von Benutzern und Administratoren sowie von Veränderungen entsprechender Benutzerrechte voraus. Die ordentliche Erfassung und Auswertung dieser Protokolldaten – neben dem Backup und der Firewall die dritte Säule der IT- und Datensicherheit in Unternehmen – dient also nicht nur der Erfüllung gesetzlicher Vorgaben. Sie unterstützt Unternehmen auch maßgeblich dabei, nahezu in Echtzeit auf Datenmissbrauch oder -verlust zu reagieren.

Verbesserung der IT- und Cybersicherheit

KRITIS-Betreiber müssen technische und organisatorische Maßnahmen (TOM) im Bereich IT-Sicherheit einführen, die der Prävention gegen IT-Vorfälle, deren Detektion oder Mitigation dienen und dem Stand der Technik entsprechen. Dies ist spätestens bis zum 1. Mai 2023 gegenüber dem BSI nachzuweisen. Mit Prävention sind Abwehrmaßnahmen wie die

Neben der Verbesserung der IT-Sicherheit lassen sich durch geeignete Log-Management-Tools geforderte Regularien einhalten und somit eine umfassende Auditsicherheit nachweisen.

sichere Authentifizierung, IPS und NAC gemeint. Ein professionelles Sicherheitsmanagement (ISMS) definiert die Standards und kontrolliert kontinuierlich deren Einhaltung. Detektion von IT-Sicherheitsvorfällen kann durch einzelne Maßnahmen wie IDS, SIEM oder durch eine IT-Sicherheitszentrale (SOC), in der alle Informationen zur IT-Sicherheit zusammenlaufen, erreicht werden. Logfiles, also kleine Protokolldateien, die Ereignisse dokumentieren, spielen bei der Prävention und Detektion eine zentrale Rolle. Von professionellem Log-Management spricht man, wenn Logfiles manipulationssicher, pseudonymisiert und mit eindeutigem Zeitstempel abgespeichert werden. Da die meisten Logdateien für die Detektion von IT-Sicherheitsvorfällen nicht entscheidend sind, müssen Filter wichtige Ereignisse sichtbar machen und bei Anomalien die Verantwortlichen alarmieren.

Fazit

Es gibt viele Gründe, die für den notwendigen Einsatz von Log-Management in kritischen Infrastrukturen sprechen. Das sind zum einen zu erfüllende Regulatorien und Compliance-Vorschriften, aber auch der fortlaufend zu gewährleistende störungsfreie IT-Betrieb und die damit zusammenhängende IT-Sicherheit. Für diese Felder ist die Logfile-Analyse eine wichtige und vielfach auch vorgeschriebene Informationsquelle. Bei der Unmenge an Logfiles, die täglich bereits in kleinen IT-Infrastrukturen anfallen, gleicht die Filterung von relevanten Logdateien der Suche nach der „Nadel im Heuhaufen“. Aber professionelles Log-Management kann aus Big Data nützliche Informationen für die Verfügbarkeit der IT und deren Absicherung erkennen. Bedenkt man alle Vorgaben, ist der Einsatz einer Log-Management-Lösung alternativlos für den sicheren Betrieb von Anlagen und IT/OT-Systemen in kritischen Infrastrukturen. ■