Cyber-Sicherheit

Mindeststandard zur Protokollierung und Detektion 2.0

[11.08.2023] Neu strukturiert hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) den Mindeststandard zur Protokollierung und Detektion von Cyber-Angriffen. Version 2.0 steht auf der BSI-Website zur Verfügung.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat jetzt den Mindeststandard zur Protokollierung und Detektion von Cyber-Angriffen in der Version 2.0 veröffentlicht. Er beinhaltet organisatorische und technische Anforderungen rund um die Erfassung von Protokoll- und Protokollierungsdaten, um Cyber-Angriffe auf die Bundesverwaltung frühzeitig zu erkennen. Wie das BSI mitteilt, wurde der Mindeststandard neu strukturiert. Eine wesentliche Neuerung im aktuellen Entwurf sei die weitgehende Integration der Protokollierungsrichtlinie Bund (PR-B), die bislang als Anlage zum Mindeststandard vorlag. Somit wurden die Sicherheitsanforderungen sowohl zur Protokollierung als auch zur Detektion erweitert, erklärt das BSI. Aufgrund der geänderten Rechtsgrundlage (§§ 5 und 5a BSIG) sowie des Angebots der datenschutzkonformen, zentralen Protokollierungs- und Detektionsinfrastruktur (Detection as a Service, DaaS) des BSI werde das Rahmendatenschutzkonzept (RDSK) nicht länger als Anlage zum Mindeststandard mitgeführt.
Die Version 2.0 des Mindeststandards, die Änderungsübersicht sowie die Referenztabelle stehen auf der BSI-Website zur Verfügung.

(ve)

Zur Änderungsübersicht
Mindeststandard und Referenztabelle zum Download

Stichwörter: IT-Sicherheit, BSI