www.pwc.de/KRITIS

Systeme zur Angriffserkennung

Ab Mai 2023 verpflichtend für Betreiber kritischer Infrastruktur und Energieversorgungsnetzen

pwc

Unsere umfassende Expertise für die neuen Anforderungen des BSI

Die Betreiber Kritischer Infrastrukturen aller Sektoren sowie Betreiber von Energieversorgungsnetzen sind in Deutschland dazu verpflichtet, Angriffserkennung zu leisten, um ihre Informationssysteme zu schützen. Nach einer Neuerung im BSIG und im EnWG müssen Systeme zur Angriffserkennung (SzA) Bestandteil der Nachweise gegenüber dem BSI sein.

Welche Neuerung ergeben sich für Betreiber ab Mai 2023?

Systeme zur Angriffserkennung sind nach der regulatorischen Definition Prozesse, die durch technische Werkzeuge und organisatorische Einbindung unterstützt werden. Dies bedeutet, dass die Systeme explizit neben technischen Maßnahmen auch organisatorische Maßnahmen erfordern und diese deshalb bei Planung der Ressourcenverteilung ausreichend berücksichtigt werden müssen.

Daraus ergeben sich für Systeme zur Angriffserkennung im Hinblick auf deren Funktionalität die wesentlichen Aufgabenbereiche der Protokollierung, Detektion und Reaktion. Nachweise, die dem BSI ab dem 1. Mai 2023 vorgelegt werden, müssen auch Aussagen zur Umsetzung von Angriffserkennungssystemen, enthalten. Betreiber von Energieversorgungsnetzen und solchen Energieanlagen, die als kritische Infrastruktur gelten, haben dem BSI erstmalig am 1. Mai 2023 und danach alle zwei Jahre die Erfüllung der Anforderungen nachzuweisen.

Nachweis von Systemen zur Angriffserkennung

Die Qualität der eingesetzten Systeme gemäß § 8a Absatz 1a BSIG bzw. nach § 11 Absatz 1e EnWG lässt sich von unseren erfahrenen Kritis-Auditoren mit Hilfe eines Umsetzungsgradmodells bewerten und in einer durch uns durchgeführten Nachweisprüfung zertifizieren.

Der Qualität von Systemen zur Angriffserkennung steht häufig entgegen, dass sich Betreiber allein auf Techniklösungen verlassen, indem ein ungeeigneter Umgang mit Sicherheitsvorfällen erfolgt und deren Auswertung ausbleibt; Mitarbeitende nicht ausreichend sensibilisiert sind, SOC/SIEM-Lösungen in OT-Umgebung als ausreichend erachtet werden oder die personellen Ressourcen fehlen, um kompetent auf zeitkritische Vorfälle zu reagieren.

Wie wir Sie unterstützen können − für eine sichere, digitale Lösung zur Angriffserkennung

✓ Erfolgreiche Qualitätsbewertung nach dem BSI Umsetzungsgradmodel

Ziel der Anwendung eines Umsetzungsgradmodells ist es, die Qualität von Systemen zur Angriffserkennung zu erhöhen. Durch regelmäßige Analysen kann überprüft werden, welche Teilbereiche noch unzureichend gesteuert sind. Ein niedriger Umsetzungsgrad begründet einen besonderen Handlungsbedarf. Umsetzungsgradmodelle können folglich dabei unterstützen, Schwerpunkte für die Weiterentwicklung von Systemen zur Angriffserkennung zu setzen. Wenn das Auditoren-Team bei den Muss-Anforderungen in den Bereichen Protokollierung, Detektion und Reaktion feststellt, dass die Anforderung noch in Planung oder Umsetzung befinden, ist eine ausreichende Qualität des Systems für Angriffserkennung nicht festzustellen und es besteht Handlungsbedarf aufseiten des Betreibers.

✓ Bedarfsgerechte Lösungen für Ihre Systeme

Der erste Schritt ist die Findung der richtigen Systemlösung. Durch eine Markterhebung sprechen wir eine maßgeschneiderte Empfehlung für das richtige Produkt in Ihrer Umgebung aus. Dabei kann sich die richtige Produktauswahl für SIEM (Security Information and Event Management) und ein SOC (Security Operations Center) für Ihre IT schwierig gestalten, beispielsweise bei Netzwerk vs. Host basierter Sensorik und Signatur vs. Anomaly basierter Erkennung. Bei PwC evaluieren wir die Optionen Hands-on in unserem Cyber Security Experience Center, einem integrierten Modell-Ökosystem mit realen Komponenten kritischer Infrastrukturen. Unsere Fachteams unterstützen Sie bei der Integration des OT-Monitorings in Ihr bestehendes SOC oder der Berücksichtigung von OT Security spezifischen Aspekten während des Incident Detection & Incident Response Prozesses.

✓ Internes Upskilling

Sicherheit ist nie allein eine Frage der Technik. Daher können wir Ihre Mitarbeitenden mit zielgerichteten Schulungen zum Thema Behandlung von Sicherheitsvorfällen befähigen, die Umsetzung der Detektionsanforderungen zu erfüllen.

✓ Managed Service

Verhindert die gegebenen Personallage den genannten Befähigungsansatz, können wir Ihnen eine Vielzahl von Dienstleistungen auch als Managed Service anbieten:

- 24x7 Überwachung Ihrer Infrastruktur durch unser SOC
- Zeitnahe Eskalation von Alarmen aus der Überwachung
- Eine schnelle und effektive Reaktion auf Cyber-Sicherheitsvorfälle durch die Kollaboration von SOC und Incident Response Teams
- Individuell anpassbare Servicevereinbarungen, um Ihren spezifischen Geschäftsanforderungen gerecht zu werden
- Verfügbarkeit relevanter Berichte und Daten
- Ausführliche und wirksame Unterstützung bei der Meldung von Verstößen, in Übereinstimmung mit DSGVO und StGB
- Zugang zu einem breiten Spektrum von Expert:innen für Cybersicherheit, Forensik, Unternehmensberatung

Ihre Ansprechpersonen

Bei Interesse an einem individuellen Angebot, kommen Sie auf unsere kompetenten Ansprechpartner zu. Wir unterstützen Sie gerne dabei, eine den BSI-Anforderungen zugeschnittene Lösung zu erhalten − inklusive schneller Bereitstellung!

Leiter KRITIS Center of Excellence

André Glenzer
Partner
Mobile: +49 160 94470376
andre.glenzer@pwc.com

Cyber Security & Privacy

Moritz Anders
Partner
Mobile: +49 1515 5455621
moritz.anders@pwc.com

Cyber Security Architect, Digital Utilities

Daniel Hanner
Senior Manager
Mobile: +49 15152360004
daniel.hanner@pwc.com

Die PricewaterhouseCoopers GmbH Wirtschaftsprüfungsgesellschaft bekennt sich zu den PwC-Ethikgrundsätzen (zugänglich in deutscher Sprache über www.pwc.de/de/ethikcode) und zu den Zehn Prinzipien des UN Global Compact (zugänglich in deutscher und englischer Sprache über www.globalcompact.de).

www.pwc.de