IT-Sicherheitsgesetz 2.0

Schutz kritischer Infrastrukturen

[17.08.2022] Am 1. Mai 2023 tritt die Novelle zum IT-Sicherheitsgesetz 2.0 in Kraft. Mit Ablauf der Übergangsfrist müssen die Betreiber Kritischer Infrastrukturen (KRITIS) neue Auflagen erfüllen. Mit einem Cyber Defense Center (CDC) lassen die sich effektiv umsetzen.

Cyber-Kriminelle nehmen immer häufiger Betreiber Kritischer Infrastrukturen (KRITIS) und Unternehmen mit besonderer volkswirtschaftlicher Bedeutung ins Visier. Dies kann nicht nur zu millionenschweren Produktionsausfällen und Versorgungsengpässen führen, sondern hat im schlimmsten Fall die Gefährdung der öffentlichen Sicherheit zur Folge. Zudem müssen sich KRITIS-Betreiber vor monetär motivierten Erpressungsversuchen schützen. Auch politisch motivierte Angriffe als Teil einer hybriden Kriegsführung sind mittlerweile zu einer realen Bedrohung geworden.
Der deutsche Gesetzgeber hat bereits im Jahr 2021 mit dem Zweiten Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme – kurz: IT-Sicherheitsgesetz 2.0 – auf diese Gefahren reagiert. Hiermit wurde das bestehende BSI-Gesetz um weitere Punkte ergänzt.
So müssen neben den traditionellen KRITIS-Betreibern künftig auch Unternehmen im so genannten besonderen öffentlichen Interesse, etwa Rüstungshersteller oder Unternehmen mit besonders großer volkswirtschaftlicher Bedeutung, bestimmte IT-Sicherheitsmaßnahmen umsetzen. Damit einhergehend wurde der Kreis der kritischen Infrastrukturen um Sektoren wie die Abfallentsorgung und Rüstungsherstellung erweitert.

Die neuen Auflagen im Überblick

Betreiber kritischer Infrastrukturen müssen spätestens bis zum 1. Mai 2023 Systeme zur Angriffserkennung implementieren. Auch müssen KRITIS-Betreiber den geplanten erstmaligen Einsatz kritischer Komponenten dem Bundesministerium des Innern und für Heimat (BMI) anzeigen, etwa wenn der Hersteller von einem Drittstaat kontrolliert wird oder sicherheitspolitischen Zielen der deutschen Bundesregierung, EU oder NATO widerspricht. Die Unternehmen im besonderen öffentlichen Interesse werden außerdem zur regelmäßigen Abgabe einer Selbsterklärung verpflichtet. Hiermit müssen sie darlegen, welche Zertifizierungen im Bereich der IT-Sicherheit in den zurückliegenden zwei Jahren durchgeführt und wie ihre IT-Systeme abgesichert wurden.
KRITIS-Betreiber und Unternehmen, die ihre IT und Leittechnik vor Cyber-Angriffen schützen müssen, benötigen deshalb integrierte Lösungen, die im Einklang mit dem IT-Sicherheitsgesetz 2.0, dem BSI-Gesetz sowie der ISO-Norm 27001 zur Informationssicherheit stehen. Auf der Technologieseite sollten daher mehrere Detektionsmodule eingesetzt werden.

Maßnahmen zum Schutz kritischer Infrastrukturen

Zum einen braucht es eine Log-Daten-Analyse (LDA) oder ein Security Information and Event Management (SIEM). Hierunter ist das Sammeln, die Analyse und Korrelation von Logs aus verschiedensten Quellen zu verstehen. Dadurch wird die Alarmierung bei Sicherheitsproblemen oder potenziellen Risiken möglich. Um manipulierte Software schnell erkennen zu können, ist außerdem das so genannte Vulnerability Management samt Compliance (VMC) wichtig. Das Schwachstellen-Management sorgt mit kontinuierlichen, internen und externen Schwachstellen-Scans bei umfassender Erkennung,

Compliance Checks und Tests für eine komplette Abdeckung. Im Rahmen der Software Compliance wird die autorisierte Software-Verwendung für jeden Server und jede Server-Gruppe mithilfe eines Regelwerks und einer kontinuierlichen Analyse festgestellt.
Ebenfalls sollten KRITIS-Betreiber über ein Network Condition Monitoring (OT-Modul) verfügen. Dieses meldet in Echtzeit Kommunikationsvorgänge, die auf eine Störung im Betrieb hinweisen. Technische Überlastungszustände, physische Beschädigungen, Fehlkonfigurationen und eine Verschlechterung der Netzwerkleistung werden damit nicht nur umgehend erkannt. Auch die Fehlerquellen werden direkt ausgewiesen. Die Netzwerkverhaltensanalyse (Network Behavior Analytics) wiederum erkennt gefährliche Malware, Anomalien und anderen Risiken im Netzwerkverkehr auf Basis von signatur- und verhaltensbasierten Detection Engines. Um Anomalien auf Computerrechnern (Hosts) zu erkennen und zu überwachen, braucht es außerdem eine Endpoint-Detection-and-Response (EDR)-Lösung. Sie sorgt für aktive Schutzaktionen und eine sofortige Alarmierung.

Betrieb im Cyber Defense Center (CDC)

Die Weiterverarbeitung der sicherheitsrelevanten Informationen aus diesen Modulen ist komplex und wird von Sicherheitsspezialisten durchgeführt. Aus einer riesigen Datensammlung bewerten und priorisieren sie die automatisiert gewonnenen Erkenntnisse. Die Ergebnisse dieser Analyse sind die Basis, auf der das hausinterne Fachpersonal die richtigen Gegenmaßnahmen einleiten kann.
Für eine bestmögliche Datensicherheit ist die Einrichtung von On-Premise-Lösungen zu empfehlen. Sie gelten als die sicherste Form der Software-Verteilung. Zwar geht der Trend vermehrt Richtung Cloud. Hinsichtlich der hohen Datensensibilität im KRITIS-Bereich ist dies jedoch problematisch.
Mit einem Cyber Defense Center (CDC) – auch Security Operations Center (SOC) genannt – können KRITIS-Betreiber und Unternehmen alle oben genannten Punkte effektiv umsetzen. In solch einem CDC lässt sich ein durchgängiges, integriertes Sicherheitskonzept für die IT- und OT-Infrastruktur implementieren. Das Defence Center umfasst Technologien, Prozesse und Experten, die für die Überwachung, Analyse und Aufrechterhaltung der Informationssicherheit eines Unternehmens verantwortlich sind. Es sammelt in Echtzeit Daten aus den Netzwerken, Servern, Endpunkten und anderen digitalen Ressourcen des Unternehmens und nutzt die intelligente Automatisierung, um potenzielle Bedrohungen der Cyber-Sicherheit zu erkennen, zu priorisieren und darauf zu reagieren. Das alles leistet das CDC rund um die Uhr, sodass Bedrohungen schnell eingedämmt und neutralisiert werden können.

Europäische Sicherheitstechnologien nutzen

Um die Anforderungen etwa der EU-Datenschutzgrundverordnung (DSGVO) oder des BSI-Gesetzes einfacher umsetzen zu können, sollten die KRITIS-Betreiber und Unternehmen im besonderen öffentlichen Interesse außerdem auf europäische Sicherheitstechnologien setzen. Erleichtert wird so beispielsweise der laut BSI-Gesetz erforderliche Nachweis über die Vorsorgemaßnahmen zum Schutz der Funktionsfähigkeit der betriebenen kritischen Infrastrukturen. Andererseits wird die Prüfung kritischer Komponenten seitens des BSI erleichtert, die sicherstellen soll, dass der EU-datenschutzwidrige Zugriff auf sensible Informationen durch Drittstaaten-Akteure zu keiner Zeit gelingen kann. Das ist umso wichtiger in Zeiten des inaktiven Privacy Act zwischen der USA und Europa.
Es ist damit zu rechnen, dass Attacken auf Europas kritische Infrastrukturen weiter zunehmen werden. Auf der geopolitischen Bühne ist das vor allem jetzt während des Ukraine-Kriegs sichtbar. Mit einer ganzheitlichen Cyber-Defense-Center-Lösung können deutsche KRITIS-Betreiber ihre Cyber-Resilienz deutlich steigern, und sich so gegen Angriffe verteidigen.

()

Stichwörter: Informationstechnik, IT-SiG 2.0, KRITIS