BWK ENERGIE.

SIEM-Sicherheitstools und das Security Operation Center (SOC) sind wirkungsvolle Werkzeuge für die Begrenzung von Sicherheitsrisiken bei Kritis-Betreibern. *Bild: Adobe Stock/telent*

Cybersecurity für Betreiber Kritischer Infrastrukturen

Sicherheitsrisiken bestmöglich vorbeugen

Kritische Infrastrukturen (Kritis) für die Energie- und Gesundheitsversorgung, Mobilität oder das Finanzwesen sind die Lebensadern moderner Gesellschaften. Um sie verstärkt zu schützen, legte Bundesinnenminister Horst Seehofer 2019 den Referentenentwurf für das zweite Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (ITSiG 2.0) vor. Kritis-Betreiber sind angehalten, den langfristigen Schutz ihrer sensiblen und oftmals komplexen Systeme zur obersten Priorität zu machen. Managed Security ist der Weg zur sicheren und zukunftsorientierten Infrastruktur.

Durch das ITSiG 2.0 soll das Bundesamt für Sicherheit in der Informationstechnik (BSI) nicht nur mehr Autorität erhalten, sondern auch zum Beispiel Hacker-Aktivitäten und den Betrieb verbotener Marktplätze im Darknet kriminalisieren. Zudem soll ein neues Kennzeichen die IT-Sicherheit von Produkten sichtbar machen. Der Fokus liegt künftig auf allgemein vernetzten Systemen oder Internet-of-Things (IoT)-Geräten.

Kritis-Betreiber wie Energieversorger, Verkehrsunternehmen oder Behörden müssen künftig strengere Sicherheitskriterien und Prozesse einhalten und sogenannte Systeme zur Angriffserkennung und -bewältigung („Security Incident & Event Management“ (SIEM)-Systeme) sowie Informationssicherheitsmanagementsysteme (ISMS) wirksam betreiben. Das BSI gibt dafür bestimmte Mindeststandards vor: Es dürfen nur Komponenten von Herstellern verbaut werden, die das Sicherheitskennzeichen tragen. Besonders in mittleren und

kleinen Unternehmen ist das einfacher gesagt, als getan, denn ihnen fehlen häufig die internen Ressourcen und das Know-how. Die Lösung ist Managed Security.

SIEM as a Service

Die steigende Komplexität von Technologien für Infrastrukturen, Anwendungen, virtuelle Maschinen, Clouds, Endgeräte und das IoT birgt ein verstärktes Risiko von Hackerangriffen und Ausfällen durch menschliches Versagen. Für IT-/OT-Infrastrukturen ist daher die kontinuierliche Kontrolle aller digitalen Prozesse, Netzkomponenten und eingebundenen Geräte erforderlich. Nur so ist Transparenz in der kompletten Infrastruktur gewährleistet. Gerade für mittelgroße und kleine Unternehmen bietet es sich an, mit Spezialisten zusammenzuarbeiten, die mit einem ganzheitlichen Ansatz und solider Erfahrung in den Bereichen Sicherheit, Netze und Prozesse zur Seite stehen.

Spezialisierte Systemintegratoren wie die telent GmbH bieten beispielsweise umfassende Sicherheitslösungen und Dienstleistungen aus einer Hand, die diese Kriterien erfüllen und Kunden in den Bereichen Kritis mit einem rechtssicheren Gesamtpaket unterstützen. Von der Schwachstellenanalyse über die Netzplanung mit Notfallkonzept bis zur Umsetzung von Managed-Security-Konzepten, inklusive Echtzeitüberwachung, erhalten Kunden eine jeweils bedarfsorientierte und schlüsselfertige Lösung.

Datenflüsse lückenlos überwachen können

Managed-Security-Lösungen beinhalten sowohl SIEM-Sicherheitstools als auch skalierbare Supportleistungen für den Schutz von IT-/OT-Umgebungen sowie maßgeschneiderte Lösungen für Multi-Vendor-Umgebungen. Dabei setzt telent auf fortschrittliche Hard- und Software, inklusive maschinellen Lernens und Künstlicher Intelligenz (KI), um den Datenfluss lückenlos zu überwachen. Umfangreiche Korrelationsinformationen und Algorithmen lösen Alarme aus und weisen auf verdächtige Bedrohungen hin.

Netzwerkplattformen, die solche Analytics-Funktionen bereits in ihrer Architektur implementiert haben, sind zum Beispiel Cisco DNA (Distributed Network Architecture) und Cisco ISE (Identify Services Engine). Auf der Basis von KI und maschinellem Lernen ermöglicht Cisco DNA eine einfache Verwaltung aller Geräte und Dienste, priorisiert und löst Netzwerkprobleme und sorgt für eine bessere Benutzerfreundlichkeit im gesamten Netzwerk. Mit einer umfangreichen Umbrella-Funktion erlaubt Cisco ISE unter anderem die richtliniengesteuerte Zugriffskontrolle in der gesamten Infrastruktur, was für maximale Sicherheit vom Kabel- über das Wireless- bis hin zum VPN-Netzwerk sorgt. Das zentrale Management bringt einen transparenten Überblick über Benutzer und Geräte im Netzwerk.

Die Gewährleistung von IT-Sicherheit bei kritischen Infrastrukturen wie beispielsweise Kraftwerken erfordert den Aufbau eines dicht geknüpften Maßnahmennetzes. *Bild: telent*

Einen integrierten Schutz vor Bedrohungen während und nach einem Angriff bietet Cisco Firepower, die erste vollständig integrierte Next-Generation-Firewall (NGFW) mit Unified Management. Firepower-Geräte unterstützen die Integration mit SIEM-Tools von Drittanbietern.

SOC as a Service

Die eingesetzten Lösungen erkennen Bedrohungen und schützen die Infrastruktur. Zusätzlich ist ein sogenanntes Security Operation Center (SOC) erforderlich, mit einem Team von ausgebildeten Experten, das Netzwerke kontinuierlich überwacht, proaktiv nach Bedrohungen sucht, sie erkennt und neutralisiert.

Der Aufbau eines SOC – oder die generelle Schaffung einer solchen Funktion im Unternehmen – ist eine kostspielige und zeitaufwendige Aufgabe, die ständige Anpassungsmaßnahmen erfordert, um effektiv zu sein. Tatsächlich entscheiden sich zahlreiche Unternehmen, darunter einige große, dafür, kein eigenes SOC aufzubauen. Stattdessen wählen sie andere Optionen zur Sicherheitsüberwachung, wie zum Beispiel die Beauftragung eines Managed-Security-Service von spezialisierten Sicherheitsfirmen – und sparen damit massive Investitionen.

Als Sicherheitsexperte hat telent ein komplettes Managed-Security-Portfolio. Dieses beinhaltet unter anderem:

- 24/7-Netzwerküberwachung, Bedrohungserkennung,
- Echtzeit-Alarme und schnelle Reaktion,
- integrierter Incident-Management-Workflow,
- Behebung von Angriffen und Ausfällen.

Durch die langjährige Praxiserfahrung bei der Planung, dem Aufbau und Betrieb sicherer Netze und Systeme profitieren Kunden von umfassendem Know-how im Bereich Kritis, Rund-um-die-Uhr-Service und dem ganzheitlichen Ansatz für ihre Sicherheitsanforderungen. ■

www.telent.de

Nico Werner

Head of Cybersecurity,
telent GmbH
Bild: telent

telent
service • commitment • value

cisco
Partner