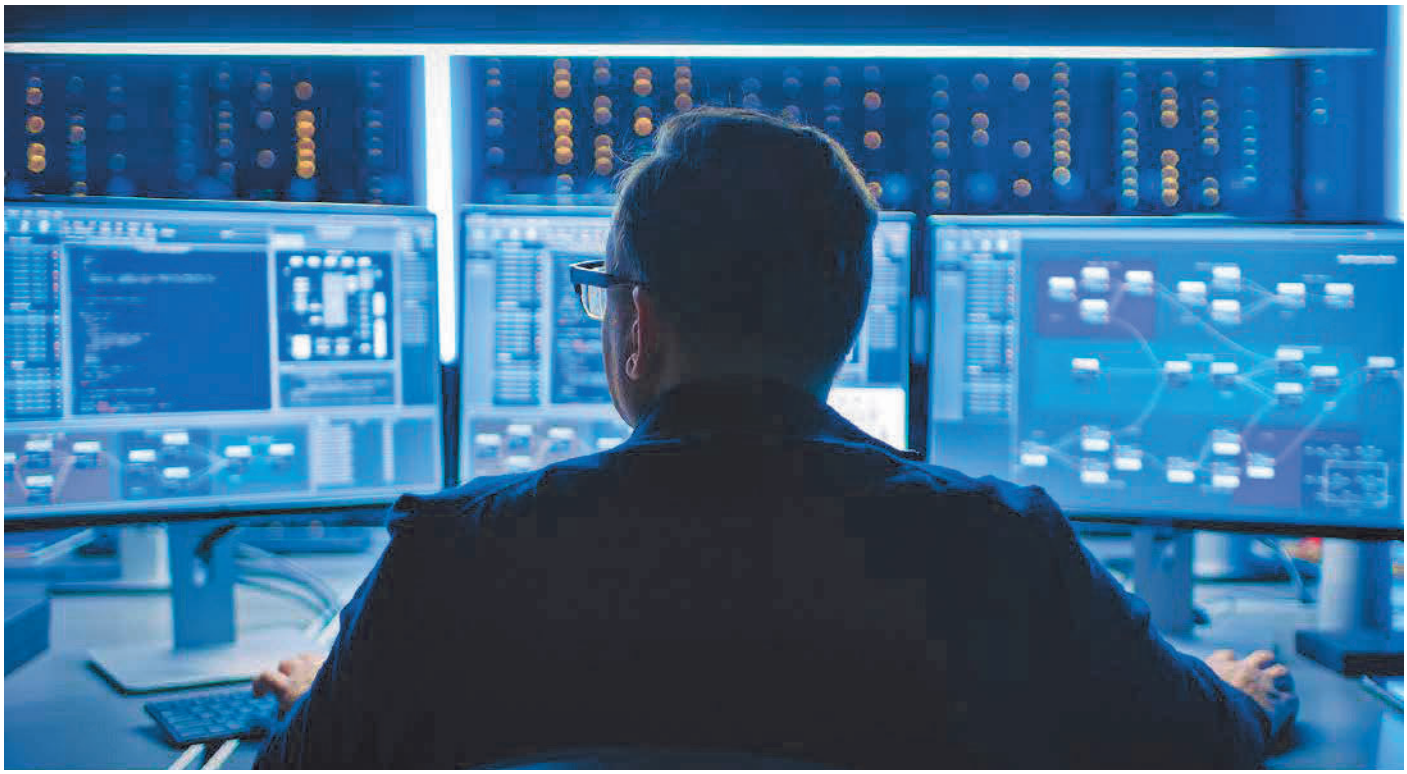
CYBERSICHERHEIT

Kommandozentrale für mehr Cybersecurity

Angriffserkennung für KRITIS: Security Operation Center (SOC) as a Service

IT/OT-Infrastrukturen wirksam vor Cyberkriminalität zu schützen – dafür reicht Technik allein nicht. Um das komplexe Thema in den Griff zu bekommen, braucht es zusätzlich hochspezialisiertes Personal. Daran mangelt es vielen kleinen und mittelgroßen KRITIS-Betreibern. Diese Lücke können externe Security Operation Center füllen, die auch kostenmäßig eine interessante Alternative sind. Ein Beitrag von René Odermann, Account Director Development Cybersecurity bei Telent.



Datendiebstahl, Industriespionage oder Sabotage: Es ist keine Frage mehr, ob ein Unternehmen Opfer eines Cyberangriffs wird, sondern wann. 46 Prozent der von der Business Data Plattform Statista befragten deutschen Unternehmen haben im vergangenen Jahr mindestens einmal eine Cyberattacke erlebt. Die dadurch entstandenen Schäden summierten sich für die Gesamtwirtschaft auf mehr als 202 Milliarden Euro. Auch zukünftig wird das Gefahrenpotenzial – nicht zuletzt angesichts der geopolitischen Konflikte – weiter steigen. Security-Risiken zu verhindern, aufzudecken, zu bewerten, zu kontrollieren und im Fall der Fälle eine forensische Analyse einzuleiten sind die zentralen Aufgaben eines Security Operation Center (SOC). Es kombiniert technische Tools, strukturierte Prozesse sowie erfahrenen Experten und ist vergleichbar mit einer Kommandozentrale, in der innerhalb eines Unternehmens alle Fäden zum Thema Security zusammenlaufen.

IT-SiG 2.0 verschärft Pflichten für KRITIS-Betreiber

Die Bundesregierung will deutschlandweit die IT-Sicherheit erhöhen. Mit dem novellierten IT-Sicherheitsgesetz (IT-SiG 2.0) erweiterte sie deshalb den Kreis der KRITIS um die Branchen Abfallwirtschaft und Rüstungsindustrie sowie um Betriebe, die aufgrund ihrer Größe volkswirtschaftlich relevant sind, und deren wichtige Zulieferer. Sie alle verpflichtet das IT-SiG 2.0, ihre IT/OT-Umgebung besser gegen Cyberkrimi-

◄◄ zurück zum Inhaltsverzeichnis

nalität zu schützen, indem sie vom 1. Mai 2023 an Systeme zur Angriffserkennung, die dem „geltenden Stand der Technik“ entsprechen, ordnungsgemäß einsetzen und das gegenüber dem BSI nachweisen. Das IT-SiG 2.0 zielt gleichermaßen auf die IT und die Betriebstechnik (Operational Technology, OT). Denn sie steuert – ob bei der Stromversorgung, der Wasseraufbereitung oder in anderen kritischen Infrastrukturen – Prozesse, die sich bei Ausfall oder Manipulation duch einen Cyberangriff enorm auf die Versorgung und Sicherheit der Bevölkerung auswirken können. Im Zuge der Digitalisierung öffnet sich die ursprünglich von der Außenwelt abgeschottete OT und arbeitet immer enger mit der IT zusammen. Das schafft viele Angriffsflächen für Cyberattacken.

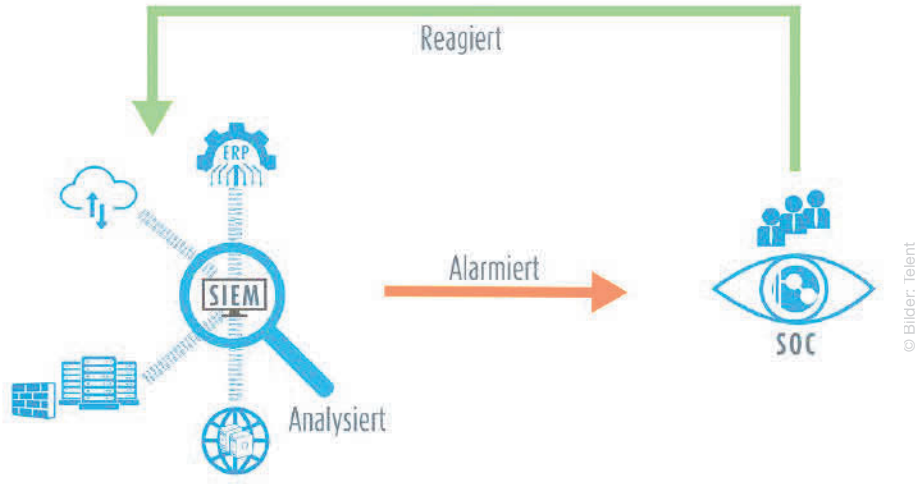
Das IT-SiG 2.0 lässt KRITIS-Unternehmen freie Hand für ein individuelles Konzept zur Angriffserkennung. Den Vorgaben entspricht u. a. ein System aus Intrusion Detection System (IDS) und Intrusion Prevention System

> „Die ursprünglich von der Außenwelt abgeschottete OT öffnet sich.“

(IPS). Ein auf die OT spezialisiertes IDS/IPS versteht die Sprache der proprietären Protokolle der Anlagen und Steuerungen und kann dadurch sowohl Angriffe als auch Fehlkonfigurationen, die auf menschlichem Versagen basieren, erkennen, im Verdachtsfall zu alarmieren oder nicht autorisierte Datenpakete zu blockieren. Eine Ergänzung hierzu sind Honeypots, die als virtuelle Maschinen bewusst mit Sicherheitslücken konfiguriert werden, um Hacker gezielt anzulocken und sie bewusst in die Irre zu leiten. Über die permanent überwachten Honeypots lassen sich IP-Adressen von Eindringlingen identifizieren, um sie dann für das gesamte System zu blockieren, und Informationen zur Vorgehensweise von Angreifern sammeln.

Echtzeit-Alarmierungen müssen qualifiziert bewertet werden

Die drei wichtigsten Funktionen einer Angriffserkennung sind Protokollierung, Detektion und Reaktion. Ein wichtiges Handwerkszeug, auch für das Team in einem SOC, ist ein SIEM. Die Abkürzung steht für Security Incident and Event Management und bezeichnet ein System, dass Meldungen, Logfiles und eine Vielzahl anderer



© Bilder: Telent

Bei einer 24/7-Netzwerküberwachung werten Experten im SOC die Alarmierungen des SIEM aus

Daten aus allen relevanten Bereichen der IT/OT-Infrastruktur sammelt, aggregiert und auf Auffälligkeiten hinweist. Um bei einer Alarmierung richtig zu reagieren, müssen die bereitgestellten Daten qualifiziert gesichtet und mit Blick auf die betriebliche Infrastruktur, etwa die verwendeten Softwareversionen, bewertet werden. In der Praxis kommen Fehlalarme häufig vor. Doch wer kann diese Aufgaben übernehmen? Angesichts begrenzter personeller und fachlicher Ressourcen stellt das viele Unternehmen vor große Herausforderungen; für die Umsetzung des IT-SiG 2.0 müssen sie noch höhere Hürde nehmen. Statt interne Kapzitäten aufzubauen, was auf dem leergefegten Arbeitsmarkt für Cybersecurity-Spezialisten kein einfaches Unterfangen ist, bieten sich externe Anbieter von Managed Security Services als Alternative an.

René Odermann, Account Director Development Cyber Security bei Telent

Unternehmen können mithilfe externer Dienstleister nur dann ein optimales Schutzniveau erreichen, wenn diese die richtigen Spezialisten an Bord haben. Dabei geht es nicht allein um die Zertifizierungen. Insbesondere bei komplexen IT/OT-Umgebung muss der Wissenshorizont passen, wie ihn Telent durch die langjährige Erfahrung in Industrial Security und industrieller Automatisation für KRITIS-Betreiber, Industrieunternehmen und öffentliche Auftraggeber besitzt. Dazu gehört für Telent auch, alle gesetzlichen Vorgaben mit ihren Muss-, Soll- und Kann-Kriterien detailliert zu betrachten, um konkret zu ermitteln, welche Punkte als Dienstleistungen erbracht werden können. Ein umfassender Sachverstand ist die Voraussetzung, um technisch hochwertige, verlässliche IT- und OT-Sicherheitsstrategien mit einem ganzheitlichen Cybersecurity-Ansatz umzusetzen.

Bei allem liegt der Fokus darauf, Technik in einen individuell für jeden Kunden sinnvollen Service zu überführen. Dabei nutzt das Telent-Team sein tiefgehendes OT-Verständnis, um außergewöhnlich flexible Lösungen zu finden, etwa vorhandene OT-Risikoerkennungsmodule von Unternehmen in die Dienstleistungen des SOC einzubinden. Als erfahrener Anbieter von Managed Security Services überwacht telent die Netzwerke seiner KRITS-Kunden rund um die Uhr, sucht aktiv nach Bedrohungen, entfernt diese und spricht weitergehende Handlungsempfehlungen aus. Somit füllt das externe SOC nicht nur Lücken bei knappen Personalressourcen, sondern stärkt die Cyberabwehr, ohne dass Unternehmen selbst hohe Investitionen in Securitysoftware, Hardware, Sicherheitsexperten, Schulungen und vieles mehr tätigen müssen, die beim Aufbau eines eigenen SOC entstehen. ●

Telent GmbH
Backnang
Tel.: +49 7191 900 0
Info.germany@telent.de
www.telent.de

◄◄ zurück zum Inhaltsverzeichnis