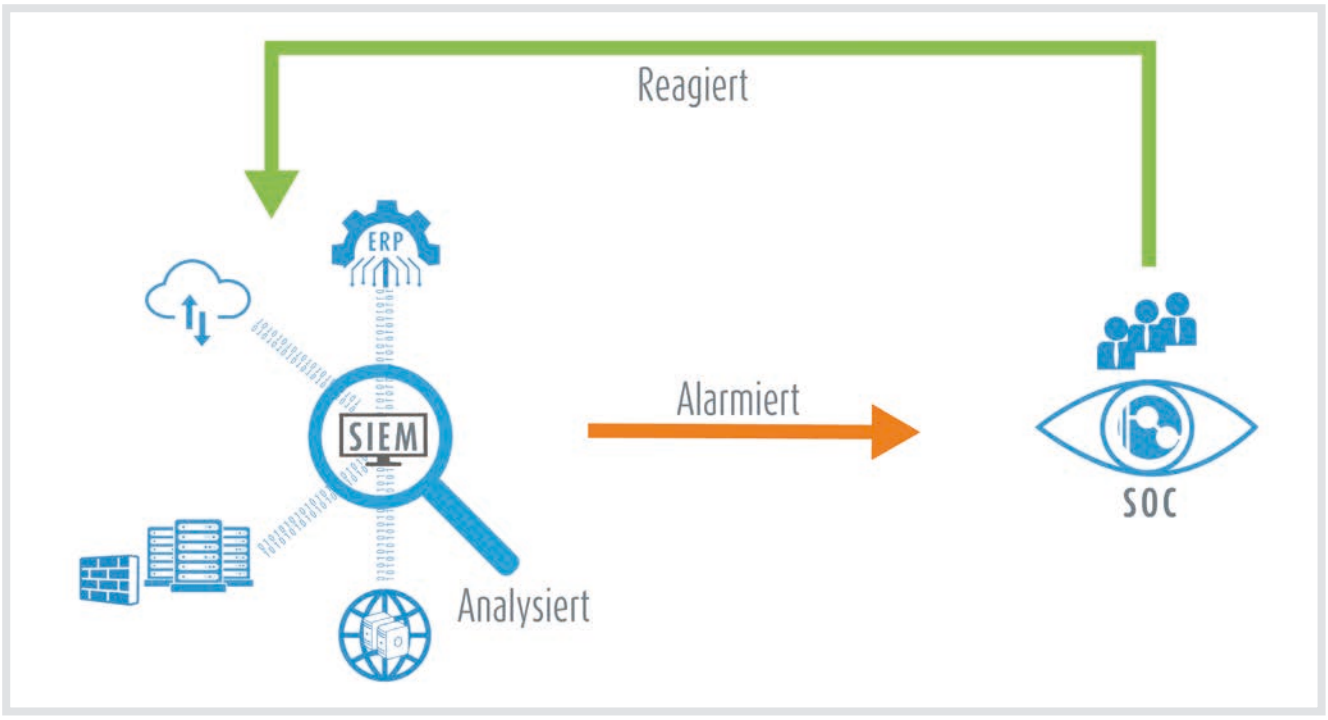

Foto: Koramis

Das Managed-Security-Portfolio von Koramis und Telent beinhaltet üblicherweise die 24/7-Netzwerküberwachung mit Echtzeit-Alarmierung.

Angriffe aus den Tiefen des Internets abwehren

Wie SIEM und Managed Security Services im Zusammenspiel für mehr Cybersecurity sorgen

DANIEL WEBER & JAKOB SCHMIDT

Emotet, Not-Petya, Triton, Industroyer, Havex, WannaCry - die Liste ließe sich fast endlos fortsetzen; die Namen stehen aber vor allem für eins: die wachsende Bedrohung von Unternehmen, Organisationen, Behörden und Privatpersonen durch immer ausgefeiltere Cyberattacken-Angriffe aus den Tiefen des Internets können jeden treffen. Sie legen Produktionen lahm oder sabotieren, stehlen unbemerkt Know-how, machen Behörden handlungsunfähig und hindern Betreiber Kritischer Infrastrukturen (Kritis) daran, ihrem Versorgungsauftrag nachzukommen – über Stunden, Tage oder gar Wochen.

Verschärft wird die Lage derzeit noch durch die coronabedingt vermehrt geleistete Arbeit aus dem Homeoffice, die Hackern und Cyberkriminellen neue Angriffsmöglichkeiten eröffnet.

Problem erkannt...

Der Gesetzgeber und andere handelnden Akteure haben das Problem längst erkannt und darauf reagiert. Kritis-Betreiber werden mit dem zweiten Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (ITSiG 2.0) dazu verpflichtet werden, ihre Maßnahmen zur Sicherstellung der Cybersecurity weiter zu erhöhen. Zu den obligatorischen Maßnahmen gehören das wirksame Betreiben von Systemen zur Angriffserkennung und -bewältigung (Security Incident & Event Management; SIEM) und eines Informationssicherheits-Managementsystems (ISMS). Auch einschlägige Security-Normen und -Richtlinien und Branchenstandards, wie die ISO2700x-Reihe oder IEC 62443 gehen in diese Richtung.

Foto: Koramis

„Mittelständler sind durch ihr Branchenwissen und oft niedrigen Security-Standards ein Ziel für Angreifer."

Jakob Schmidt, Coordinator Awareness, Koramis GmbH

... Gefahr gebannt?

Richtig implementiert und betrieben verbessern ISMS und SIEM die Prozesse und damit die Cybersecurity enorm. Genau hier liegt, insbesondere für KMUs, das Problem. Es mangelt diesen Unternehmen häufig am benötigten Know-how, an qualifizierten Mitarbeitern und internen Ressourcen, um solch hochspezialisierte Systeme effizient zu betreiben. Gleichzeitig sind Mittelständler durch ihr Branchenwissen bei gleichzeitig oftmals niedrigen Security-Standards ein lukratives Ziel für Angreifer. Ein Beispiel ist die erfolgreiche

Attacke auf die Pilz GmbH, einen Spezialisten für Sicherheits- und Steuerungstechnik. Im Herbst 2019 verschafften sich Hacker Zugriff auf sämtliche Unternehmensserver, verschlüsselten die dort gelagerten Daten und forderten ein Lösegeld.

Lösungsansatz: Managed Security Services

Hier kommen auf Cybersecurity spezialisierte Dienstleister, wie die Koramis GmbH – Ein Tochterunternehmen der Telent GmbH, ins Spiel. Sie übernehmen das komplexe Security-Thema für ihre Kunden. Ihre Lösungen für Managed Security umfassen SIEM-Tools, skalierbare Supportleistungen für den Schutz von IT-/OT-Umgebungen und individuelle Lösungen für Multi-Vendor-Umgebungen. Dafür wählen sie einen Technologiemix aus Hard- und Software, maschinellem Lernen und Künstlicher Intelligenz (KI) sowie Anomaly Detection, um den Datenfluss lückenlos zu überwachen.

Netzwerkplattformen, die solche Analytics-Funktionen bereits in ihrer Architektur implementiert haben, sind zum Beispiel Cisco DNA (Distributed Network Architecture) und Cisco ISE (Identify Service Engine). Auf der Basis von KI und maschinellem Lernen ermöglicht Cisco DNA eine einfache Verwaltung aller Geräte und Dienste, priorisiert und löst Netzwerkprobleme. Mit einer umfangreichen Umbrella-Funktion erlaubt Cisco ISE unter anderem 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. Integrierten Schutz vor Bedrohungen während eines Angriffs bietet Cisco Firepower, eine vollständig integrierte Next-Generation-Firewall (NGFW) mit Unified Management. Firepower-Geräte unterstützen die Integration mit SIEM-Tools von Drittanbietern.

SOC für mehr Sicherheit

Die technischen Lösungen erkennen Bedrohungen und schützen die Infrastruktur. Zusätzlich empfiehlt sich der Einsatz eines Security Operation Centers (SOC), eines Expertenteams, das Netzwerke kontinuierlich überwacht, nach Bedrohungen sucht und diese entfernt. Der Aufbau eines effektiven SOCs ist ressourcen- und zeitaufwendig. Daher entscheiden sich zahlreiche Unternehmen, unabhängig von ihrer Größe, gegen den Aufbau eines eigenen SOC und wählen stattdessen eine andere Option der Sicherheitsüberwachung: Sie sourcen diese Dienstleistung an einen Anbieter von Managed Security Services aus.

Das Managed-Security-Portfolio von Koramis und Telent beinhaltet üblicherweise die 24/7-Netzwerküberwachung mit Echtzeit-Alarmierung. Der integrierte Incident-Management-Workflow sorgt für die umgehende Behebung von Angriffen und Ausfällen. Telent als Systemintegrator und Koramis als Sicherheitsexperte verfügen über langjährige Praxiserfahrung bei der Planung, dem Aufbau und Betrieb sicherer Netze und Systeme und dazu passenden Managed Security Services.

„Kritis-Betreiber werden mit dem zweiten Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (ITSiG 2.0) dazu verpflichtet werden, ihre Maßnahmen zur Sicherstellung der Cybersecurity weiter zu erhöhen."

Daniel Weber,
Senior Security Operation Engineer der Koramis GmbH

Foto: Koramis

Den Faktor Mensch nicht vergessen

Zu guter Letzt sollten Unternehmen – ganz im Sinne eines ganzheitlichen Security-Ansatzes, wie ihn Telent und Koramis verfolgen – die organisatorische Sicherheit bezüglich des Faktors Mensch erhöhen. Denn im Normalfall sind die Menschen jene „Komponente", die am leichtesten zu hacken ist und die in ihrer täglichen Arbeit die definierten Prozesse leben und die (Security-)Technologie kontrollieren müssen. Oder um es mit dem Security-Experten Bruce Schneier zu sagen: „Nur Amateure greifen die Technologie an, Profis nehmen den Menschen ins Visier." ■

KORAMIS GmbH:
www.koramis.de

telent GmbH:
www.telent.de

Was ist ein SIEM?

Das Akronym SIEM steht für Security Information und Event Management. Das System, das die zwei Konzepte Security Information Management (SIM) und Security Event Management (SEM) vereint, ermöglicht einen ganzheitlichen Blick auf die eigene IT-Security zu erlangen. Dazu werden Meldungen, Logfiles und andere Daten aus allen relevanten Teilen der Infrastruktur gesammelt und ausgewertet. Dadurch lassen sich verdächtige Ereignisse, Angriffe und andere Bedrohungen in Echtzeit erkennen und ermöglicht die Einleitung von angemessenen Gegenmaßnahmen.

Die Vorteile sind:

- schnelle Identifizierung von potenziellen Bedrohungen,
- schnelle Reaktion auf security-relevante Events,
- Nachweis der Einhaltung von Compliance-Vorgaben,
- Entlastung der IT,
- Möglichkeit von nachträglichen forensische Analysen durch gesammelte Daten.