PMeV NETZWERK SICHERE KOMMUNIKATION
KOMPAKT Nr. 1/2021

Mehr Cybersecurity durch das Zusammenwirken von SIEM und Managed Security Services

Von Nico Werner*

Bekannte Namen wie Emotet, Not-Petya, Triton, Industroyer, Havex, WannaCry stehen als Synonyme für die wachsenden Bedrohungen durch immer ausgefeiltere Cyberattacken auf Unternehmen, Organisationen, Behörden und Privatpersonen. Gezielte, aber auch breit angelegte Angriffe aus dem Internet können jeden treffen. Besonders schwer wiegt, wenn die Angriffe Produktionen lahmlegen oder sabotieren, Know-how unbemerkt stehlen, Behörden handlungsunfähig machen und Betreiber Kritischer Infrastrukturen (KRITIS) daran hindern, ihrem Versorgungsauftrag nachzukommen – teilweise über Stunden, Tage oder gar Wochen hinweg. Der derzeitige enorme Anstieg der Arbeit aus dem Homeoffice verschärft die Situation zusätzlich; er eröffnet Hackern und Cyberkriminellen neue Möglichkeiten zu Angriffen.

Problem erkannt

Das Beispiel der Homeoffice-Arbeit steht für eine generelle Herausforderung: Die zunehmende Digitalisierung eröffnet Hackern und kriminellen Netzwerken nie dagewesene Möglichkeiten, auf die angemessen reagiert werden muss. Sowohl der Gesetzgeber als auch andere handelnde Akteure haben das Problem längst erkannt und entsprechend 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 der Betrieb eines Informationssicherheits-Managementsystems (ISMS). Einschlägige Security-Normen und -Richtlinien sowie Branchenstandards, wie die ISO2700x-Reihe oder IEC 62443, zielen ebenfalls in diese Richtung.

Gefahr gebannt?

SIEM und ISMS verbessern die Prozesse und damit die Cybersecurity enorm. Allerdings müssen diese richtig implementiert und betrieben werden. Aber genau hier liegt – insbesondere für KMU – das Problem. Es mangelt diesen Unternehmen häufig am benötigten Know-how, an qualifizierten Mitarbeitern und internen Ressourcen, um solch hochspezialisierte Systeme effizient zu betreiben. Mittelständler sind aber wegen ihres spezifischen Branchenwissens, bei gleichzeitig häufig ungenügend umgesetzten Security-Standards, ein lukratives Ziel für Angreifer. Ein Beispiel ist die erfolgreiche Attacke auf die Pilz GmbH, einen Spezialisten für Sicherheits- und Steuerungstechnik. Hacker verschafften sich im Herbst 2019 Zugriff auf sämtliche Unternehmensserver, verschlüsselten die dort gelagerten Daten und forderten ein Lösegeld.

Lösungsansatz: Managed Security Services

Um die mit den Anforderungen aus dem ITSiG konfrontierten Firmen sachgerecht in Sachen Cybersecurity zu unterstützen, kommen auf Cybersecurity spezialisierte und nach ISI/IEC 27001 zertifizierte Dienstleister 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. Sie setzen einen Technologiemix aus Hard- und Software, maschinellem Lernen, Künstlicher Intelligenz (KI) sowie Anomaly Detection ein, um den Datenfluss lückenlos zu überwachen.

PMeV - Netzwerk sichere Kommunikation
Professioneller Mobilfunk e. V. • Schönhauser Allee 10-11 • 10119 Berlin
Vorsitzender: Hytera Mobilfunk GmbH • Bernhard Klinger
Redaktion: Jochen Müller • Kommunikation & Public Affairs • Hobsweg 78 • 53125 Bonn
www.pmev.de • mueller@pmev.de

Netzwerkplattformen, die solche Analytics-Funktionen bereits in ihrer Architektur implementiert haben, sind beispielsweise Cisco DNA (Distributed Network Architecture) und Cisco ISE (Identify Service Engine). Auf der Basis von KI und maschinellem Lernen ermöglicht z. B. 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. Das sorgt für maximale Sicherheit für das gesamte Netzwerk. Das zentrale Management bietet 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

Das Erkennen von Bedrohungen und das Schützen der Infrastruktur werden durch technische Lösungen unterstützt. Dennoch empfiehlt sich zusätzlich der Einsatz eines Security Operation Centers (SOC) – also ein Expertenteam, das Netzwerke kontinuierlich überwacht, nach Bedrohungen sucht und sie entfernt. Allerdings ist der Aufbau eines effektiven SOC ressourcen- und zeitaufwendig. Daher entscheiden sich zahlreiche Unternehmen, unabhängig von ihrer Größe, gegen den Aufbau eines eigenen SOC. Stattdessen wählen Sie eine andere Option der Sicherheitsüberwachung: Sie ziehen erfahrene Anbieter von Managed Security Services zu Rate und beauftragen diese, die SOC-Funktion für sie wahrzunehmen.

Das KORAMIS Managed Security Portfolio der Firma des Autors beinhaltet üblicherweise die 24/7-Netzwerküberwachung mit Echtzeit-Alarmierung. Der integrierte Incident-Management-Workflow sorgt für die umgehende Behebung von Angriffen und Ausfällen.

Faktor Mensch nicht vergessen

Im Sinne eines ganzheitlichen Security-Ansatzes sollten Unternehmen die organisatorische Sicherheit im Hinblick auf den Faktor Mensch erhöhen. Ein gutes Sicherheitskonzept umfasst neben der technologischen Komponente die Prozesse und die Organisation sowie den Menschen. Denn im Normalfall sind die Menschen jene Komponente im Sicherheitsgeschehen, die am leichtesten zu „hacken“ ist. Sie müssen die definierten Prozesse leben und im Rahmen ihrer Aufgaben die (Security)-Technologie kontrollieren und beurteilen. Um es mit dem Security-Experten Bruce Schneier zu sagen: „Nur Amateure greifen die Technologie an, Profis nehmen den Menschen ins Visier.“

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. 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. Somit wird die Einleitung von angemessenen Gegenmaßnahmen möglich. Die Vorteile sind:

- Schnelle Identifizierung von potentiellen Bedrohungen
- Schnelle Reaktion auf Security-relevante Events
- Nachweis der Einhaltung von Compliance-Vorgaben
- Entlastung der IT
- Nachträgliche forensische Analysen durch gesammelte Daten sind möglich

*Der Autor:
Nico Werner ist Leiter des Fachbereichs Cybersecurity im PMeV und Head of Cybersecurity der telent GmbH, ein Mitgliedsunternehmen des PMeV. cybersecurity@pmev.de