Warum Cybersicherheit während der Corona-Pandemie wichtiger denn je ist

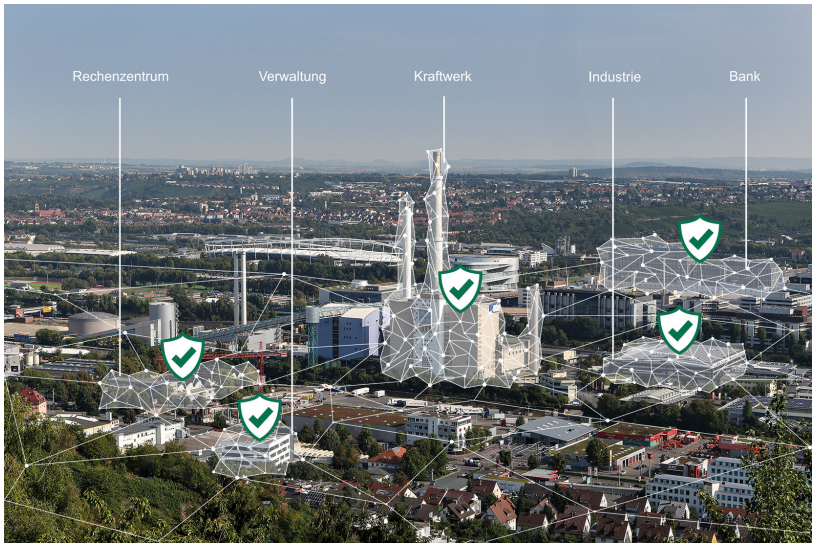
Mit „heißer Nadel" wurden seit Ausbruch der Corona-Pandemie Arbeitsabläufe digitalisiert, um ganze Belegschaften ins Homeoffice zu beordern. Innerhalb kürzester Zeit mussten belastbare IT-Infrastrukturen samt VPNs und einer Vielzahl neuer Endgeräte eingerichtet werden und funktionieren. Eine enorme Herausforderung, bei der eine schnelle IT-Verfügbarkeit häufig zulasten der Datensicherheit ging. Cyberkriminelle nutzen die neu entstandenen Angriffsflächen – mit teils dramatischen Auswirkungen auf Unternehmen, Organisation und Behörden.

Nico Werner, Head of Cybersecurity, telent GmbH
Daniel Weber, Senior Security Operation Engineer, telent GmbH

Hacker und Cyberkriminelle legen Produktionen lahm, stehlen unbemerkt Know-how, machen Behörden handlungsunfähig und hindern Betreiber Kritischer Infrastrukturen (KRITIS) daran, ihrem Versorgungsauftrag nachzukommen. Nach Einschätzung des Bundesamts für Sicherheit in der Informationstechnik (BSI) ist die IT-Sicherheitslage hierzulande angespannt. Neben den neuen Angriffsmethoden auf die immer komplexer werdenden IT-Landschaft kommt verschärfend hinzu, dass die Angreifer geschickt die COVID-19-Pandemie ausnutzen, indem sie z. B. Antragswebseiten für Soforthilfe-Maßnahmen täuschend echt nachahmen und missbrauchen.

Zur Sicherheit verpflichtet

Cyber-Angriffe beinhalten ein enormes Gefahrenpotenzial für Staat, Wirtschaft und Gesellschaft. Deswegen verpflichtet der Gesetzgeber KRITIS-Betreiber mit dem zweiten Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (ITSiG 2.0) dazu, 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 sowie Branchenstandards, wie die ISO2700x-Reihe oder IEC 62443 gehen in diese Richtung.



Lukratives Angriffsziel

ISMS und SIEM müssen richtig implementiert und betrieben werden. Nur dann können die hochspezialisierten Systeme, die durch IT verursachten Risiken identifizierbar und beherrschbar machen, um eine hohe IT-Sicherheit zu gewährleisten. Damit das gelingt, brauchen die Betreiber Know-how, ausreichend qualifizierte Mitarbeiter und interne Ressourcen. Daran mangelt es in vielen Betrieben – insbesondere bei KMU. Dadurch geraten sie in ein Dilemma, denn nicht nur Hidden Champions, sondern viele spezialisierte Firmen besitzen begehrtes Nischenwissen, das sie nur mit niedrigen Security-Standards schützen. Dadurch werden sie zum lukrativen 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.

Gebündelte Abwehrkraft

Sabotage, Datendiebstahl und Spionage: Mehr als 100 Milliarden Euro Schaden jährlich entsteht der deutschen Wirtschaft durch Cyberkriminalität laut einer Studie der Bitkom. Angesichts dieser Dimension lohnt es sich für Unternehmen, die ihre industrielle Umgebung und kritischen Infrastrukturen nicht selbst ausreichend sicher können, auf Dienstleister zuzugreifen, wie KORAMIS – Cybersecurity by telent. Dahinter steckt die gebündelte Kompetenz der Koramis GmbH, die sich im Februar 2021 mit der telent GmbH zusammenschloss. Gemeinsam übernehmen die Spezialisten 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.

KI und maschinelles Lernen

Netzwerkplattformen, die solche Analytics-Funktionen bereits in ihrer Architektur implementiert haben, sind z. B. Cisco DNA (Distributed Network Architecture) und Cisco ISE (Identify Service Engine). Cisco DNA setzt dabei auf KI und maschinelles Lernen, um alle Geräte und Dienste einfach zu verwalten, zu priorisieren und Netzwerkprobleme zu lösen. Für ein Maximum an Sicherheit vom Kabel- über das Wireless- bis hin zum VPN-Netzwerk sorgt die umfangreiche Umbrella-Funktion, über die Cisco ISE unter anderem richtliniengesteuerte Zugriffskontrolle in der gesamten Infrastruktur erlaubt. 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.

Sicherheit effektiv outsourcen

Bedrohungen erkennen und Infrastrukturen schützen – der erste Schritt dazu sind technischen Lösungen. Darüber hinaus empfiehlt sich der Einsatz eines Security Operation Centers (SOC). Damit ist ein Expertenteam gemeint, das Netzwerke kontinuierlich überwacht, gezielt nach Bedrohungen sucht und diese entfernt. Dieses Ziel effektiv zu erreichen, ist ressourcen- und zeitintensiv. Unabhängig von der Firmengröße etablieren deswegen viele Unternehmen kein eigenes SOC, sondern sourcen diese Dienstleistung an einen Anbieter von Managed Security Services aus.

Das Managed-Security-Portfolio von KORAMIS – Cybersecurity by telent beinhaltet üblicherweise die 24/7-Netzwerküberwachung mit Echtzeit-Alarmierung. Der integrierte Incident-Management-Workflow sorgt für die umgehende Behebung von Angriffen und Ausfällen. Die Spezialisten aus den Bereichen Systemintegration und IT-Sicherheit verfügen über langjährige Praxiserfahrung bei der Planung, dem Aufbau und Betrieb sicherer Netze und Systeme und dazu passenden Managed Security Services.

Der Mensch im Visier

„Nur Amateure greifen die Technologie an, Profis nehmen den Menschen ins Visier." Diese Erkenntnis des international anerkannten, US-amerikanischen Experten für Computersicherheit Bruce Schneier weist auf einen weiteren entscheidenden Faktor hin: den Nutzer der IT. Er ist im Normalfall jene „Komponente", die am leichtesten zu hacken ist und der in der täglichen Arbeit die definierten Prozesse leben und die (Security-)Technologie kontrollieren muss. Deswegen sollten Unternehmen – ganz im Sinne eines ganzheitlichen Security-Ansatzes, wie ihn KORAMIS – Cybersecurity by telent verfolgt – nicht zuletzt die organisatorische Sicherheit bezüglich des Faktors Mensch erhöhen.

Was ist ein SIEM

SIEM (Security Information und Event Management) vereint die Konzepte Security Information Management (SIM) und Security Event Management (SEM). Für einen ganzheitlichen Blick auf die eigene IT-Security werden Meldungen, Logfiles und andere Daten aus allen relevanten Teilen der Infrastruktur gesammelt und ausgewertet. So werden verdächtige Bedrohungen in Echtzeit erkannt und ermöglichen frühzeitige Gegenmaßnahmen.

Vorteile von SIEM:

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