PRESSECLIPPING

Sonderdruck aus dem DIGITAL BUSINESS CLOUD 4/2022

Angriff(e erkennen) ist die beste Verteidigung

Jedes Unternehmen muss Schäden durch Cyberattacken vermeiden. Die Anforderungen zur Umsetzung einer wirksamen Sicherheitsstrategie sind enorm, denn die Zeiten, als der IT-Administrator die Sicherheitsüberwachung parallel zur System-Verfügbarkeitsprüfung übernehmen konnte, sind lange vorbei. Wie lassen sich Risiken also minimieren? VON SIEGO KREITER

IT-INFRASTRUKTUREN werden immer komplexer und damit anfälliger für Angriffe. Moderne Technologien wie das Internet der Dinge (IoT) sind dank unzähliger Sensoren und Messstationen gefährliche Einfallstore ins Netzwerk. Gleiches gilt für den Bereich der Operation Technology (OT), welcher die Steuerung von Produktionsanlagen umfasst.

Hacker halten sich nicht an klassische Bürozeiten, in der die IT-Abteilung persönlich besetzt ist. Angriffe erfolgen zu jedem denkbaren Zeitpunkt. Ob mitten in der Nacht, sonn- oder feiertags: Die Überwachung rund um die Uhr, muss stehen. Dadurch lassen sich die meisten Angriffe rechtzeitig feststellen und abwehren. Speziell im KRITIS-Umfeld zwingt der Gesetzgeber die Unternehmen daher zur Etablierung entsprechender Systeme. Auch für Firmen mit hoher Internetpräsenz und Betreiber von Online-Shops oder hochgradig vernetzten IT-Landschaften mit vielen unterschiedlichen Endgeräten werden diese Systeme zur Minimierung der Cyberrisiken unverzichtbar.

Angriffserkennung mit System

Verschiedene Angriffsszenarien führen zu unterschiedlichen Indikatoren, die eine Angriffserkennung ermöglichen. Diese Indikatoren findet man, wenn man die kompletten Log-Dateien des Netzwerks und der IT-Systeme überwacht – eine Aufgabenstellung, die manuell nicht leistbar ist. Security-Information-&-Event-Management-(SIEM)-Lösungen unterstützen die automatisierte Echtzeitanalyse sämtlicher Ereignisse im Netzwerk und den Systemen. Dabei werden nicht nur die Daten selbst analysiert, sondern auch Informationen aus allen Systemen korreliert, um aus dem Zusammenspiel verdächtige Aktivitäten zu erkennen. So werden Muster identifiziert, die vom gewohnten Verhalten der Infrastruktur abweichen und Hinweise auf mögliche Sicherheitsprobleme geben. Hinzu kommt die Überwachung des Netzwerkverkehrs, dessen Datenpakete auf Viren, Angriffsmuster, Protokollfehler und sonstige Abweichungen analysiert werden. Aber selbst die Ergebnisse aus dem SIEM müssen in den Kontext des Unternehmens gesetzt und interpretiert werden, was ein hohes Maß an Security-Expertise voraussetzt.

24x7-Überwachung im SOC

Gerade Mittelständler stellt das vor erhebliche Probleme: Weder finden sie am Markt nicht ausreichend Mitarbeiter mit den notwendigen fachlichen Kompetenzen noch sind diese innerhalb eines Betriebes ausgelastet. Daher setzen immer mehr Unternehmen auf Partner, die SIEM-Services im Rahmen eines externen Security Operations Center (SOC) bereitstellen. Das SOC ist das Zentrum für jegliche sicherheitsrelevanten IT-Services, die für den Schutz eines Unternehmens erforderlich sind. Im SOC der IS4IT-Gruppe laufen sämtliche Informationen der schutzbedürftigen IT-Systeme der Kunden zusammen. Wird ein Angriff erkannt, erhalten die Kunden sofortige Empfehlungen, um diesen durch entsprechende Verteidigungsmaßnahmen zu unterbinden. Bei der Wahl eines externen SOC-Anbieters ist ein zentrales Entscheidungskriterium, dass dieser sein SOC auf mehrere Tier-3-Rechenzentren – bevorzugt mit Standort in Deutschland – verteilt hat. Damit wird die Ausfallsicherheit im Fall von lokalen Störungen sowie die Einhaltung der strengen deutschen Gesetzgebung gewährleistet. Mit einem SOC auf Basis von Managed Services lässt sich eine maximale Sicherheitsstrategie auch für mittelständische Unternehmen wirtschaftlich umsetzen. •

Der AUTOR
Siego Kreiter
ist Geschäftsführer der IS4IT KRITIS GmbH.