Beitrag <kes>-Homepage Schlaglicht - <kes> online

Angriffserkennung für KRITIS: Wie Unternehmen die Umsetzung angehen können

KRITIS-Betreiber sind ab Mai 2023 gesetzlich verpflichtet, ihre IT/OT-Umgebung mit einer wirksamen Angriffserkennung gegen Cyberkriminalität zu schützen. Die Zeit drängt und somit die Frage, welche Maßnahmen geschäftskritische Systeme effektiv und zulässig schützen.

Von René Odermann

Die Zahl der Angriffe steigt so rasant wie sich die Art der Methoden verändert: 553.000 neue Schadprogramm-Varianten an einem einzigen Tag – dieser im vergangenen Jahr gemessene Wert war der bis dato höchste. Nicht zuletzt angesichts der geopolitischen Konflikte, wird das Gefahrenpotenzial weiter zunehmen. Um die IT-Sicherheit in Deutschland signifikant zu verbessern, verschärfte die Bundesregierung bei der Neufassung des IT-Sicherheitsgesetzes (IT-SiG 2.0) die Spielregeln: Zum einen erweiterte sie den Kreis der Adressaten um die Branchen Abfallwirtschaft und Rüstungsindustrie sowie zusätzlich um Betriebe, die allein durch ihre Größe volkswirtschaftlich relevant sind, und deren wichtige Zulieferer. Außerdem wurden Schwellenwerte gesenkt, so dass beispielsweise für die Einstufung als Stromerzeugungsanlagen 36 Megawatt ausreichen anstelle der bisherigen 420 Megawatt. Zum anderen sind alle betroffenen Unternehmen verpflichtet, ab dem 1. Mai 2023 Systeme zur Angriffserkennung, die dem „geltenden Stand der Technik“ entsprechen, ordnungsgemäß einzusetzen und gegenüber dem BSI nachzuweisen.

Immer mehr Angriffsflächen

Die neuen Anforderungen konzentrieren sich gleichermaßen auf die IT und die Betriebstechnik (Operational Technology, OT). Denn die OT 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, die umso erfolgreicher sind, wenn die eingedrungene Malware lange unentdeckt bleibt und sich im Netzwerk weit verbreitet. Deswegen ist schnelles Gegensteuern so wichtig – mithilfe einer Angriffserkennung setzt man auf frühzeitige Intervention, um Schäden zu begrenzen oder zu vermeiden.

Doch wie sollen Unternehmen die Umsetzung angehen? Anfang Juni 2022 veröffentlichte das BSI einen Entwurf zur Orientierungshilfe, der Anforderungen für die Umsetzung der Angriffserkennung definiert, Nachweisformulare enthält und

…2

das Reifegradmodell erläutert, über das die implementierten Maßnahmen bewertet werden. Eine ganzheitliche Angriffserkennung erfasst grundsätzlich alle Systeme, Komponenten und Prozesse, die funktionskritisch sind. Um sie sichtbar zu machen, sollte jede Cybersecurity-Maßnahme mit der Inventarisierung aller IT/OT-Assets beginnen. Das beinhaltet auch deren Eigenschaften wie Firmware-Versionen, Protokolle und Kommunikationsverbindungen. Eine derart umfassende Erhebung schafft die erforderliche Transparenz, um das am besten geeignete Angriffssystem auswählen zu können.

Technische Möglichkeiten

Die Orientierungshilfe nennt neben allgemeinen Anforderungen an ein System zur Angriffserkennung auch die drei wesentlichen Aufgaben Protokollierung, Detektion und Reaktion. Um sicherheitsrelevante Ereignisse überhaupt erkennen zu können, müssen Protokollierungsdaten fortlaufend auf System- und Netzebene erhoben, gespeichert und bereitgestellt werden. Zusammen mit einer Anomalieerkennung kann das System Abweichungen von der üblichen Kommunikation analysieren und melden. Den Vorgaben des IT-SiG 2.0 entspricht auch ein System aus Intrusion-Detection (IDS) und Intrusion-Prevention (IPS). Darüber hinaus können Unternehmen auch ein auf die OT spezialisiertes IDS/IPS einsetzen, das mit den proprietären Protokollen der Anlagen und Steuerungen umgehen kann. Solche Systeme sind somit in der Lage, sowohl Angriffe als auch Fehlkonfigurationen, die auf menschlichem Versagen basieren, zu 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 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 zu sammeln.

Ihre Monitoring-Pflicht können KRITIS-Betreiber über ein Security-Incident-Event-Management-(SIEM)-System erfüllen, das sowohl die IT als auch die OT im Blick hat. Ein SIEM erhält von zahlreichen Datenkollektoren eine Fülle an Informationen, bereinigt diese zu einem sogenannten normalisierten Stream und alarmiert bei Auffälligkeiten. Die Fehlermeldungen müssen dann an einer zentralen Stelle, wie beispielsweise einem Security-Operation-Center (SOC), ausgewertet und verifiziert werden. In der Praxis ist gerade das eine Herausforderung für die Security-Teams oder KMUs, da oft Personal fehlt, um die zahlreichen Alarme dezidiert zu prüfen. Das ist aber zwingend erforderlich, um zielgerichtet reagieren zu können. Ein Ausweg bietet hierfür ein SOC als Service. Diese werden von spezialisierten Dienstleistern betrieben, die über erfahrene Security-Teams verfügen, die von einem SIEM und anderen Systemen gesammelte Daten auswerten, die Netzwerke ihrer KRITIS-Kunden rund um die Uhr überwachen, aktiv nach Bedrohungen suchen, diese entfernen und weitergehende Handlungsempfehlungen aussprechen.

…3

kes
Die Zeitschrift für Informations-Sicherheit

Fazit

Die Orientierungshilfe des BSI versteht sich nur als Richtschnur, lässt KRITIS-Unternehmen aber freie Hand für ein individuelles Konzept zur Angriffserkennung, das exakt zu den geschäftskritischen Prozessen und Komponenten passt und sich in die individuelle Cybersecuritiy-Strategie einfügt. Ein SOC vereint dafür Prozesse, Technik und Experten als integriertes Angbot für mehr IT- und OT-Sicherheit.

René Odermann ist Head of Sales & Business Development CyberSecurity bei der telent GmbH.