Lösungen

Aufzeichnen, auswerten, abwehren

[14.08.2025] Kritische Infrastrukturen sind gefordert, Schutzmechanismen zu errichten, die den Betrieb essenzieller Systeme bei Cyberangriffen, Naturereignissen oder menschlichem Versagen aufrechterhalten. Ein empfehlenswerter Ansatz ist hier das Security Information and Event Management.

Städtische Krankenhäuser, Energieversorger, Wasserwerke oder Notruf-Leitstände erfüllen wichtige gesellschaftliche Funktionen. Gerade deshalb geraten sie zunehmend ins Visier von Angreifern. Deren Augenmerk liegt auf der Betriebstechnologie (Operational Technology, OT), also auf Soft- und Hardware, mit der sich physische Prozesse, Geräte und Infrastrukturen abhören, steuern und überwachen lassen. Ist die OT-Sicherheit ausgehebelt, ist es möglich, Gas- und Stromnetze zu kapern, die Trinkwasserversorgung und Abwasserbeseitigung zu sabotieren oder Ampelanlagen zu manipulieren.

Durch das konsequente Sammeln, Korrelieren und Analysieren von Daten soll OT Security Information and Event Management (OT-SIEM) solche Angriffe verhindern. iQSol, Hersteller verschiedener Security-Appliances sowie Anbieter für Business-Continuity-Lösungen aus Österreich, hat dafür bereits 2015 die LogApp entwickelt. Die Lösung wird an die zu überwachenden IT- und OT-Systeme angeschlossen und zeichnet – auch On-Premise – Logs auf. Sie dokumentiert also alle Vorkommnisse (Events). Liegen Abweichungen vor, wird alarmiert. Bei Brute-Force-Attacken, unberechtigten Zugriffen auf Geräte und Sensoren in Wasser- oder Kraftwerken reagiert die LogApp sofort. Ihre Informationen übergibt sie an ein Alarmierungssystem wie den iQSol AMS, das Administratoren und andere im System hinterlegte Personen via E-Mail, Sprachnachricht oder SMS benachrichtigt. Da für eine forensische Analyse Log-Sammlungen unabkömmlich sind, werden diese von Standards wie etwa NIS2 vorgeschrieben.

Verbindendes Element

Auch für den Betrieb eines Security Operations Centers (SOC), der auf XDR oder SOAR setzt, ist diese Datendrehscheibe das verbindende Element. Klassischerweise werden bewährte Playbooks eingeplant, bespielt und abgebildet. Use Cases helfen, gängige Gefahren wie Ransomware einzuschätzen, Angriffsparameter zu überwachen und zu alarmieren, um möglichst schnell die Attacke erkennen zu können. Eine Windows-File-Monitoring-Funktion ist ebenso hilfreich wie die Interaktion mit spezifischen Industrieprotokollen, eine Härtung des Active Directory oder die Integration von IT-Security-Lösungen, die ihren Fokus auf Maschinen, Energieanlagen und so genannte Fabrics legen. Die Stärke eines OT-SIEM besteht darin, dass hier viele Datenquellen angebunden werden können und so Weitergaben in übergeordnete SOC-Systeme möglich werden.

Isolierte Infrastrukturen

In der OT-Welt begegnet man oft stark isolierten Infrastrukturen, die nicht nur hoch abgesichert sein müssen, sondern auch den Kontakt zur Internet-Außenwelt scheuen. Deshalb kommen nur Sicherheitslösungen in Betracht, die vor Ort eingesetzt werden können und die möglichst wenige Updates benötigen – nur einer von vielen Aspekten, der gegen teure und aufwendige Cloudlösungen von US-

Anbietern spricht. Angesichts der geopolitischen Lage ist es darüber hinaus ratsam, eine datenschutzkonforme Software aus dem EU-Raum vorzuziehen.

Im Vordergrund stehen außerdem Einbindungsmöglichkeiten in die OT-Systempartnerlandschaft wie zum Beispiel mit Siemens oder namhaften Anbietern aus der Automatisierungs- und Leitstellentechnik. Da zudem Compliance eine große Rolle spielt, ist eine kostengünstige OT-SIEM-Lösung mittlerweile das naheliegendste Tool. Im Sinne einer gesamtheitlichen Security ist es sinnvoll, den ganzen Prozess von Beginn an zu betrachten, eine Entscheidung für ein Informationssicherheits-Managementsystem (ISMS) zu treffen, Reifegradanalysen einzuplanen und Notfallhandbücher anzulegen.

Gebot der Stunde

Immer wichtiger werden auch Maßnahmen am Ende eines Notfallmanagements, nämlich die Alarmierung und das Business Continuity Management unter technologischen Gesichtspunkten. Denn Formulare, Papiere und Handbücher sind zwar notwendig, in der Krise helfen sie technisch aber nur wenig. Automatisierung lautet also das Gebot der Stunde.

Viele Unternehmen verfügen mittlerweile über einen Notfallplan, der die nächsten Schritte exakt definiert. Königsklasse ist, wenn auch eine so genannte Power-Management-Lösung bedacht und somit die Business Continuity, die durchgängige Geschäftsfähigkeit, unterstützt wird. Sie schaltet geplant ab, bevor es andere tun. Dafür kann sie Betriebstechnologien und gefährdete Systeme nach fest definierter Reihenfolge mittels Knopfdruck herunterfahren, bevor Eindringlinge oder mangelnde Stromversorgung Hardware-Schäden und in der Folge Datenverluste verursachen können. Ist die Gefahr gebannt, ist auch der geordnete Wiederanlauf über die zentrale Appliance hocheffizient möglich. iQSol bietet für solche Fälle die PowerApp an, die Unternehmen entweder selbst steuern oder in ein bewährtes SOC auslagern.

Bewährte und umfassende OT-Security

Nicht nur die Kritischen Infrastrukturen haben ein Interesse daran, sich gegen Angriffe zu schützen. Dies fordert auch die europäische Gesetzgebung. Verschärft wurde das durch die 2022 verabschiedete NIS2-Richtlinie, die 2024 in deutsches Recht überführt wurde – und auf viele Kommunalbetriebe Druck ausübt. Mit den Appliances und Services von iQSol kann den Anforderungen von NIS2 – etwa den Maßnahmen zum Business Continuity Management, Melde- und Unterrichtungspflichten – einfach entsprochen werden. Am erfolgreichsten sind Projekte, in denen namhafte Hersteller von Energie- und Leitstellentechnik sowie Infrastrukturlösungen technisch integriert werden. Dort gibt es keine Widrigkeiten, da die Betreiber die OT-Security direkt anbieten. Das Ziel ist es, eine bewährte und umfassende OT-Security – von der Firewall über OT-SIEM/SOC bis hin zur Shutdown-Appliance – aufzubauen, die über viele Jahre einsetzbar, auditierbar und zuverlässig läuft. Für ein städtisches Krankenhaus, den Abwasserbetrieb oder Stadtwerke ist das realistisch umsetzbar.

()

Der Beitrag ist im Schwerpunkt Cybersicherheit der Ausgabe Juli/August 2025 von stadt+werk erschienen. Hier können Sie ein Exemplar bestellen oder die Zeitschrift abonnieren.

Stichwörter: Informationstechnik, Cybersicherheit, iQSol, Kritische Infrastrukturen (KRITIS), Security Information and Event Management (SIEM)