IT- und OT-Security für Maschinen- und Anlagenbauer

Rechtssicher cybersicher

Cybersecurity-Techniken für IT und OT in der Industrie müssen nicht nur Angreifer und deren Malware draußen halten oder möglichst schnell aufspüren, sondern auch immer mehr Vorschriften erfüllen. Ralf Habermann, Geschäftsführer der TG alpha GmbH in Deggendorf, erläutert, worauf es ankommt.

Ralf Habermann, TG alpha

> *„Wenn jemand ein OT-System angreift, dann muss ich davon ausgehen, dass ich einen Profi vor mir habe, der in der Lage ist, herkömmliche Sicherheitsmaßnahmen zu umgehen."*

Markt&Technik: Maschinenverordnung, Cyber-Resilience-Act, NIS 2, ISO 13489 – auf Maschinen- und Anlagenbauer prasseln gerade zahlreiche neue oder runderneuerte regulative Anforderungen ein. Wie kann man da noch den Überblick behalten?

Ralf Habermann: Schauen wir zunächst auf die Datensicherheit, also die Cybersecurity. Viele der genannten Verordnungen zielen einheitlich auf ein angemessenes Schutzniveau, allerdings mit unterschiedlicher Fokussierung. In der Maschinenverordnung geht es darum, dass durch korrumpierte Daten oder böswillige Angriffe niemand zu Schaden kommt, während NIS 2 darauf abzielt, die (Volks-)Wirtschaft zu schützen, damit ein Cyberangriff nicht zu Stromausfällen oder zum Zusammenbruch der Trinkwasserversorgung führt. Dass gerade mittelständische Unternehmen in allen Bereichen, vom Maschinenbauer bis zum Stadtwerk, in der Umsetzung viel Luft nach oben haben, ist oft angesprochen worden, daher will ich darauf nicht weiter eingehen. Grundsätzlich ist aber IT- und OT-Sicherheit mit diesen Regelwerken keine Frage des »Ja« oder »Nein« mehr, sondern eine Frage dessen, mit welchen Schritten man anfängt, seinen Betrieb und seine Anlagen sicherer zu machen.

Mit welchen Schritten sollte man also loslegen?

Auch wenn es in Thrillern häufig anders dargestellt wird: Hacker verbringen im Schnitt rund 20 Tage damit, das Zielsystem zu verstehen, auszuspionieren und nach interessanten Inhalten zu durchstöbern, bevor sie zuschlagen, Festplatten verschlüsseln und Lösegeld fordern.Wenn wir also einen unerwünschten Eindringling sofort als solchen erkennen, haben wir noch einige Zeit, um in Ruhe zu überlegen, wie wir ihm das Handwerk legen. Dabei funktionieren Hacker wie Einbrecher: Werden sie ertappt, suchen sie das Weite. Wenn sie clever sind, verwischen sie ihre Spuren so gut wie möglich, um vielleicht irgendwann einen zweiten Versuch zu starten.

Auch für Netzwerke gibt es Einbruch-Meldeanlagen – im Englischen heißen sie Intrusion-Detection-Systems (IDS). Die Kernaufgabe eines IDS ist es, den gesamten Netzwerkverkehr mitzuhören und sofort Alarm zu schlagen, wenn sich ungewöhnliche Dinge tun.

Wie erkennt ein IDS, ob ein neuer Teilnehmer dazu kommt oder ob sich etablierte Teilnehmer über Kanäle austauschen, über die sie noch nie kommuniziert haben?

Im Prinzip wird jeder Kommunikationsvorgang gegen eine Liste erlaubter Zustände geprüft – eine sogenannte Positivliste, auch Allow- oder White-List genannt. Findet ein Vorgang statt, der nicht in der Liste aufgeführt ist, egal ob es sich um einen neuen Teilnehmer, einen unüblichen Gesprächskanal oder eine nicht übliche Kommunikation zweiter Netzwerkpartner handelt, schlägt das IDS Alarm. Ein Mensch schaut sich dann die Meldung genauer an und gibt dem System auch eine entsprechende Rückmeldung, damit es lernen und seine Regel selbst optimieren kann.

»Lernen« und »Selbst-optimieren« klingt nach KI, oder?

Richtig. Unser IDS »alphaWatch« setzt KI-Algorithmen ein, damit Kunden nicht Wochen damit verbringen müssen, diese Positivliste zu erstellen. Das kann das System selbst übernehmen und ist dabei erstaunlich schnell. Je nach Anlagengröße dauert es wenige Stunden bis wenige Tage. Danach lernt ein intelligentes IDS wie »alphaWatch« mittels Beobachtung permanent weiter dazu. Wichtig ist, dass es sofort Alarm schlägt, wenn es unbefugte Verbindungen oder einen unbekannten zusätzlichen Kommunikationsteilnehmer erkennt. Um sich dem Zielsystem anpassen zu können, ist ein gutes IDS flexibel skalierbar.

Bei alphaWatch ist ein automatisiertes Sperren bei unzulässigen Datenflüssen grundsätzlich möglich. Es ist aber meist nicht sinnvoll. Denn wenn ein Hacker gerade die Sicherheitsmechanismen umgangen und begonnen hat, sich umzuschauen, kann man die Zeit dazu nutzen, um herauszufinden, wo der unerwünschte Eindringling herkommt und über welche Hintertürchen und undichte Stellen er eingesickert ist.

Gibt es aus Ihrer Sicht ein unterschiedliches Vorgehen bei IT- und OT-Systemen?

Nicht grundsätzlich. Die Endziele sind die gleichen. Aber man muss sich darüber im Klaren sein, dass diese Welten häufig sehr unterschiedlich sind. Im OT-Bereich ordnet sich alles der Verfügbarkeit unter – die Produktion muss laufen. Zudem habe ich es häufig mit sehr heterogenen Kommunikationsteilnehmern zu tun, etwa mit allen möglichen Betriebssystemen, auch solchen, für die es schon lange keine Sicherheits-Updates mehr gibt. Das IDS muss also in der Lage sein, sich jedem Teilnehmer anzupassen. Daher gibt es in diesem Bereich auch keine Einheitslösung, die sofort für alle passt.Wenn jemand ein OT-System angreift, dann muss ich davon ausgehen, dass ich einen Profi vor mir habe, der in der Lage ist, herkömmliche Sicherheitsmaßnahmen zu umgehen. Genau aus diesem Grund ist es eminent wichtig, den Eindringling sofort zu erkennen, weit bevor andere Systeme überhaupt in der Lage sind, die Signaturen spezifischer Schadsoftware zu detektieren.

Heißt das im Umkehrschluss: Wenn ich ein IDS im IT-Bereich installiere, ist der OT-Bereich automatisch mit abgedeckt?
Eben nicht. Gegenüber der idealen Welt der IT gibt es in der OT diese Einschränkungen, gegen die ich erst einmal machtlos bin. Alte Betriebssysteme etwa – oder Beschränkungen durch vertragliche Vereinbarungen zu bestimmten Service-Levels, etwa weil ein Maschinenhersteller ein bestimmtes Update eines Betriebssystems nicht freigibt, weil die Kompatibilität mit den Maschinen im Feld nicht gewährleistet ist.

Eher ist es so, dass umgekehrt ein Schuh draus wird: Häufig richtet sich ein Angriff zunächst gegen das IT-System und erreicht nur OT-Systeme, die nicht sauber abgekoppelt sind. Ist der Angriff aber auch nur teilweise erfolgreich, trägt das OT-System die Hauptlast, weil es in diesem heterogenen Umfeld ungleich schwieriger zu reparieren ist und im Extremfall jede einzelne Maschine nach unterschiedlichen Vorgehensweisen gereinigt und wieder hochgefahren werden muss.

Wie würden Sie die Vorteile eines IDS gegenüber klassischen IT-Sicherheitstools zusammenfassen?
Ein gutes IDS erkennt Anomalien auf Anhieb und schlägt sofort Alarm, und zwar lange bevor eingeschleuste Schadsoftware überhaupt erkannt werden kann. Damit verschafft das IDS dem Kunden zwei Dinge: die Sicherheit, immer zu wissen, dass niemand im digitalen Raum ist, der da nicht hingehört – und die Zeit, den Ursachen einer erkannten Anomalie auf den Grund zu gehen.

Die Fragen stellte Andreas Knoll.