Compliance und Risk Management
Das Ökosystem des Gesundheitswesens besteht aus einer Vielzahl von Partnern und Anbietern innerhalb der Wertschöpfungskette. In dieser vernetzten – aber ungleichen – Struktur muss jeder Beteiligte individuell für Cybersecurity sorgen.

Unternehmen müssen effektive Partner-Risikomanagement-Programme entwickeln und implementieren, um Daten zu sichern und vor Cyberangriffen zu schützen. Dies kann durch eine Bewertung der Sicherheitslage von Partnern erreicht werden, gefolgt von einer risikobasierten Partnersegmentierung sowie der Definition an „Zero-Trust"-Prinzipien in Sachen Konnektivität und Zugriffsmanagement für Partner.

Managed Detection und Response
Die Cyber-Bedrohungslandschaft entwickelt sich stetig weiter. Dies führt dazu, dass fast jeden zweiten Tag neue Bedrohungen auftauchen. Daher ist ein gut definiertes Playbook für die schnelle Erkennung von Bedrohungen und Sicherheitsverletzungen und die Reaktion darauf entscheidend.

Organisationen des Gesundheitswesens müssen KI-Systeme mit Machine Learning und Verhaltensanalysen einsetzen, um Anomalien und Bedrohungen proaktiv zu erkennen und schnelle Sandboxing- und Wiederherstellungsprozesse zu entwickeln. Nur dann können sie sich „cyber-resilient" (widerstandsfähig) aufstellen und schützen.

Vishal Salvi

Cyber-Risiko Lieferkette: Warum die Cybersecurity Ihrer Partner auch Ihre Angelegenheit ist

Die Zahl der Cyberangriffe auf Industrieanlagen aller Größenordnungen nimmt seit Jahren deutlich zu. Dabei erstreckt sich das Risiko über die gesamte Lieferkette. Eine Studie mit 150 Cybersecurity- und IT-Fachleuten in mittelständischen und großen Unternehmen der Fertigungsindustrie hat unlängst gezeigt, dass jede zweite OT-Infrastruktur für Cyberangriffe anfällig ist. 53 Prozent der Befragten gaben zudem an, dass ihr Unternehmen in den letzten 12 bis 24 Monaten bereits von einem Cyberangriff oder einem anderen Sicherheitsvorfall betroffen war, der auch die OT-Netzwerke beeinträchtigte.

Moderne Lieferketten sind längst komplizierte, miteinander verflochtene Partnernetzwerke. Und wenn ein Partner kompromittiert wird, hat dies Auswirkungen auf alle Partner in der Lieferkette. Die Auswirkungen eines Angriffs auf einen First-Tier-Lieferanten können dabei genauso verheerend sein, wie ein Angriff auf die eigenen Systeme: Ganze Produktionslinien können ausfallen, was erhebliche Kosten verursacht, sich negativ auf den Umsatz auswirkt und den Ruf des Unternehmens schädigt.

Seit Jahren nutzen Angreifer Schwachstellen in der Lieferkette als Sprungbrett, um andere Unternehmen zu infiltrieren. Vielleicht erinnert sich so mancher noch an den Datenvorfall beim US-amerikanischen Handelsunternehmen Target vor knapp zehn Jahren. Hier haben Angreifer gestohlene Zugangsdaten eines Klimaanlagen-Herstellers genutzt, um auf das Netzwerk von Target zuzugreifen und sich lateral zu bewegen. Das Ergebnis: Millionen gestohlener Kundendaten, inklusive Zahlungsinformationen. Ein paar Jahre später sahen wir mit der Ransomware NotPetya einen weiteren hochkarätigen Angriff auf die Lieferkette, der zunächst Software einer ukrainischen Buchhaltungsfirma infizierte. Im weiteren Verlauf wurden multinationale Unternehmen getroffen und es entstand ein geschätzter Gesamtschaden von 10 Milliarden US-Dollar. Und erst kürzlich ermöglichte die Kompromittierung der SolarWinds Orion-Software und die SUNBURST-Backdoor Angreifern den Zugang zu zahlreichen Unternehmen und Behörden auf der ganzen Welt. Das Ausmaß und die Auswirkungen dieses Angriffs sind derzeit noch nicht abzusehen.

Yaniv Vardi, CEO, Claroty

Maßnahmen der Industrie
Cybersicherheit in der Lieferkette wird mittlerweile als bedeutendes Thema von Führungskräften und Sicherheitsverantwortlichen in (nahezu) allen Branchen wahrgenommen. Entsprechend ergreifen Behörden, Branchenverbände und Regulierungsbehörden Maßnahmen, um das Risiko zu minimieren. Als ein Impfstoff für COVID-19 in greifbare Nähe rückte, gab IBM eine Warnung vor unbekannten Bedrohungsakteuren heraus, die auf die Lieferkette für den Impfstoff COVID-19 zielen. Die Security-Experten wiesen dabei besonders auf die gestiegenen Fähigkeiten von Angreifern sowie die Dringlichkeit und Schwere des Lieferketten-Risikos hin und mahnten, die Gefährdung von OT-Umgebungen zu reduzieren. Ab Juli 2024 werden neue Cybersecurity-Vorschriften für die Automobilindustrie für alle in der Europäischen Union produzierten Neufahrzeuge verpflichtend sein. Entsprechend sind derzeit neue Cybersicherheitsstandards zur Etablierung von „Cybersecurity by Design" über den gesamten Lebenszyklus eines Fahrzeugs in der Entwicklung.

Was Sicherheitsverantwortliche tun können
Cyber-Risiken in der Lieferkette sind kompliziert und erstrecken sich über den gesamten Lebenszyklus eines Produkts – von der Entwicklung über die Herstellung, den Vertrieb und die Lagerung bis hin zur Wartung. Je umfangreicher und komplexer der Lebenszyklus ist, desto mehr Angriffsmöglichkeiten und Chancen, ein schwaches Glied in der Kette zu finden und auszunutzen, gibt es. Und da Lieferketten oft global sind und mehrere Ebenen von Lieferanten umfassen, liegt

die Verantwortung für die Sicherheit nicht bei einem einzelnen Unternehmen. Jeder Partner muss hier involviert sein, wodurch die Reduzierung von Cyber-Risiken in der Lieferkette eine besondere Herausforderung darstellt. Deshalb dürfen Führungskräfte bei der Erstellung von Business-Continuity-Plänen nicht nur ihr eigenes Unternehmen im Auge behalten. Sie müssen auch die Sicherheitsmaßnahmen ihrer unmittelbaren Zulieferer im Blick haben und einbeziehen, wie diese ihrerseits das Risiko mit ihrem erweiterten Netzwerk von Zulieferern verwalten und mindern. Diese fünf Schritte können dabei helfen:

Kommunikation und Bewertung: Das Management dieses kritischen Risikos beginnt mit der Festlegung der internen Verantwortung für das Procurement und die Überprüfung der Prozesssicherheit eines Partners. Hierbei müssen sowohl die Rechtsabteilungen als auch Technologie- und Fachabteilungsleiter in allen Geschäftsbereichen einbezogen werden. Führungskräfte benötigen verlässliche Bedrohungsdaten hinsichtlich der Angriffe auf die Lieferkette, um fundierte Entscheidungen über die Risiken für das Unternehmen zu treffen. Beschaffung und Datensicherheit müssen deutlich und effektiv an Partner und Stakeholder kommuniziert werden.

Detaillierte operative Transparenz: Dedizierte industrielle Cybersicherheitslösungen sind in der Lage, OT-spezifische Herausforderungen, wie den Mangel an standardisierter Technologie, die Verwendung proprietärer Protokolle und eine geringe Toleranz gegenüber Unterbrechungen kritischer Prozesse, zu adressieren. Eine Plattform, die kontinuierlich Bedrohungen im gesamten OT-Netzwerk überwacht und erkennt, sich mit dem bestehenden Sicherheitsnetzwerk Ihres Unternehmens verbindet und auch eine Verbindung zu allen Zugangspunkten mit Ihren Partnern in der Lieferkette herstellt, erweitert diese Transparenz auf alle relevanten Partner.

Konsistente Cybersicherheitsstandards: Halten Sie sich über neue Vorschriften (etwa das geplante IT-Sicherheitsgesetz 2.0) und Standards sowie neue Warnmeldungen auf dem Laufenden. Folgen Sie branchenspezifischen Empfehlungen und setzen Sie diese zügig um.

Steigende Awareness: Angesichts der kritischen Bedrohungslage hat sich das Bewusstsein vieler Führungskräfte und Vorstandsmitglieder für die Notwendigkeit von effektiver industrieller Cybersicherheit entwickelt, um so Produktivität, Verfügbarkeit, Zuverlässigkeit und Safety zu gewährleisten. Als Sicherheitsverantwortlicher sollten Sie den Moment nutzen, um funktions- und abteilungsübergreifende Unterstützung aktueller und zukünftiger industrieller Cybersicherheitsinitiativen zu erhalten.

Kollaborativer Ansatz: Ihre Lieferkette ist ein integraler Bestandteil des Ökosystems Ihres Unternehmens. Deshalb muss sie auch in Ihr Sicherheitsökosystem integriert werden und genauso effektiv geschützt werden, wie ihre „internen" Systeme. Cloud-basierte Lösungen vereinfachen die sichere Konnektivität mit wichtigen Partnern in der Lieferkette. Außerdem können sie die Sicherheit verbessern, einfacher aktualisiert und neue Funktionen schneller hinzugefügt werden. In manchen Branchen ist eine Cloud-Transformation aufgrund gesetzlicher Vorgaben noch nicht umsetzbar. Dennoch ist es auch hier möglich, Benchmarks festzulegen sowie Berichte und Erkenntnisse über Schwachstellen und die jeweiligen OT-Netzwerk-Sicherheitslevel mit den Partnern in der Lieferkette auszutauschen.

Wir sehen, dass die Cybersicherheit der gesamten Lieferkette eine gemeinschaftliche und durchaus herausfordernde Aufgabe ist, die nur durch Zusammenarbeit bewältigt werden kann. Glücklicherweise gibt es Maßnahmen, die jedes einzelne Unternehmen ergreifen kann, um das Risiko zu reduzieren. Es ist höchste Zeit, dies jetzt schnell anzugehen.

Yaniv Vardi