DCSO

THREAT DETECTION & HUNTING

Cyber-Sicherheit im Maschinenbau
2025 und darüber hinaus

Cyber-Sicherheit im Maschinenbau
2025 und darüber hinaus

Als umsatzstarke Branche und Treiber der deutschen Wirtschaft, steht der Maschinenbau naturgemäß im Fokus von Angreifern. Neben vielen ungenannten Fällen traf es in den letzten Jahren den Fahrzeugzulieferer Fritzmeier Group[1], den Pumpen- und Armaturenhersteller KSB[2] und den Hersteller von Sicherheitseinrichtungen Schmersal[3]. Auch thyssenkrupp berichtet regelmäßig von versuchten Angriffen auf die eigene Infrastruktur[4].

Das Bewusstsein für die eigene Verletzlichkeit gibt es in diesem traditionell technikaffinen Segment schon lange[5]. Maschinenbauunternehmen in Deutschland gehören deshalb auch zu den “Early Adoptern” von Cyber-Sicherheit. Dabei kommen diesen Betrieben im Vergleich zu anderen Branchen einige Faktoren zugute: Überdurchschnittliche Löhne, ein hoher Grad an Digitalisierung und die räumliche Konzentration der Standorte, bedingt durch integrierte Produktionsanlagen. Eigentlich könnten Maschinenbauer Musterschüler erfolgreicher Cyber-Sicherheit sein. Dennoch werden auch gut ausgestatte Unternehmen wie Schmersal Opfer von Cyberangriffen. Woran liegt das?

Nach allem, was über den Fall Schmersal bekannt ist, wurde die IT der Firma mit spezifisch angepasster Schadsoftware infiziert, welche durch die Endpoint-Security Lösung nicht erkannt wurde. Ein größerer Schaden wurde nur durch eine schnelle, manuelle Trennung vom Internet verhindert.

Dieses Beispiel zeigt, dass sich Unternehmen für die Cyber-Abwehr nicht nur auf Technologie verlassen können. Ebenso braucht es ausgebildetes Personal, welches die vorhandenen Tools zu nutzen weiß, und die organisatorische Vorbereitung, um schnell weitreichende Entscheidungen treffen zu können. In diesem Zusammenspiel liegt die große Herausforderung der IT-Sicherheit. Ingenieursleistungen allein schützen Unternehmen nicht umfassend.

Quellen

[1] https://www.cio.de/a/hacker-legen-deutschen-fahrzeugzulieferer-lahm,3674393

[2] https://www.chemietechnik.de/markt/cyberangriff-pumpenhersteller-ksb-musste-produktion-einstellen-443.html

[3] https://www.wuppertaler-rundschau.de/lokales/cyberangriff-wuppertaler-firmaschmersal-reagierte-in-sieben-minuten_aid-54047931

[4] https://www.spiegel.de/netzwelt/web/thyssenkrupp-hacker-verueben-angriff-auf-werkstoffsparte-a-42b0d13e-c2f7-450d-8f50-558412aa981b

[5] https://link.springer.com/chapter/10.1007/978-3-322-86213-6_2

Typische
Stolpersteine

Die praktische Umsetzung von IT-Sicherheit ist auch in fortschrittsorientierten Unternehmen wie dem Maschinenbausektor kein Selbstläufer. Als Managed Security Services Provider (MSSP) hat die DCSO dabei über die Jahre wiederkehrende Muster identifiziert, an denen der Transfer von Theorie in die Praxis krankt.

Getrennte Verantwortung
Budgets für Produkte und Personal

In vielen Unternehmen liegt die Verantwortung für Cyber-Security Produkte traditionell in der IT-Betriebsorganisation. Diese kauft mit eigenen Budgets Produkte ein, die ihren Anforderungen entsprechen. Oft bauen Unternehmen dazu parallele Strukturen für die Arbeit mit diesen Produkten auf – sei es als eigenes SOC oder durch einen Dienstleister. In der Praxis mangelt es dann an Kommunikation zwischen dem IT- und dem Sicherheitsbetrieb. Verantwortlichkeiten sind nicht klar abgesprochen. Außerdem legen IT-Betriebsteams andere Kriterien an die Auswahl von Produkten an, als es ein security-fokussiertes Team tun würde.

Endpoint Security
als Silver Bullet

In der Security-Industrie hat sich die Meinung durchgesetzt, dass einzelne Produkte immer in ein Gesamtkonzept eingebettet werden müssen. Häufig versuchen Unternehmen dennoch, IT-Sicherheit nur auf dem Endpoint zu konzentrieren. Am Fall Schmersal ist sichtbar, dass diese Strategie nicht erfolgsversprechend ist. Das gilt ganz besonders für Maschinenbaufirmen, die bedingt durch Produktionsanlagen eine große Spannbreite an Hardware- und Softwaresystemen betreiben. Endpoint Security Produkte ersetzen auch keine IT-Hygiene und regelmäßige Patches. Sie ist ein wichtiger Baustein, muss aber durch andere technische Maßnahmen ergänzt werden.

Fehlende Handlungsfähigkeit
im Krisenfall

Im seltenen Fall eines erfolgreichen Angriffs kommt es auf Minuten an. Eine schnelle Isolation von Endgeräten und Nutzern kann oft größeren Schaden verhindern oder zumindest das Fortschreiten des Angriffs verzögern. Laterale Bewegung im Netz ist auch für den Angreifer Handarbeit – Verteidigern bleibt also ein Fenster um die Bedrohung einzudämmen. In der Praxis scheitert diese Eindämmung aber häufig an einem fehlenden 24/7 Monitoring der Alarmsysteme. Ebenso fehlen Freigaben, welche Einschränkungen des Unternehmensbetriebs im Notfall hinnehmbar sind.

Produkte, Prozesse und Personal gemeinsam denken

Als Managed Security Services Provider (MSSP) unterstützt die DCSO Unternehmen bei der Realisierung einer integrierten Sicherheitsarchitektur. Für viele Betriebe übernimmt die DCSO 24/7 die Bewertung von Vorfällen. Einige Maßnahmen steigern dabei die Leistungsfähigkeit der Verteidigung nachhaltig.

Ausführenden Teams Verantwortung übertragen

Anstatt Budgets von oben zwischen dem Einkauf von Lösungen und Personalressourcen aufzuteilen, sollten diese Entscheidungen möglichst in den ausführenden Teams getroffen werden. Erfahrungsgemäß können die handelnden Personen besser einschätzen, ob es eher den Bedarf nach weiteren Produkten oder für eine personelle Verstärkung des Teams gibt. In die Auswahl von konkreten Anbietern sollten die betreuenden Teams ebenfalls frühzeitig eingebunden werden. Möglicherweise entscheiden sich Teams auch, bestimmte Aufgaben durch Dienstleister wie die DCSO erbringen zu lassen, um die eigenen Ressourcen sinnvoller einzusetzen.

Swiss-Cheese-Model für Sicherheitsprodukte verfolgen

Anstatt sich auf einzelne Kontrollpunkte zu konzentrieren, sollte eine solide Abwehr aus mehreren, gestaffelten Systemen bestehen. Neben Endpoint Security empfiehlt die DCSO für Maschinenbauunternehmen eine Überwachung ihres IT- und OT-Netzwerkes und der wichtigsten Logs aus diesen Infrastrukturen. Weniger bekannt, aber ebenfalls sinnvoll, ist die aktive Suche nach kompromittierten Identitäten und die Anbindung der integrierten Sicherheitsfunktionen von AWS, Microsoft und Google.

Handlungssicherheit schaffen

Für Notfälle muss klar sein, welche Systeme und Nutzer:innen abgeschaltet / isoliert werden können. Diese Daten müssen kontinuierlich aktuell bleiben, daher bietet sich eine Umsetzung über Tags im Asset und Identity Management an. Diese können dann via API an die zentralen Reaktionssysteme angebunden werden, und stehen dem Security Operations Center oder einem Dienstleister nahtlos zur Verfügung. Ebenso empfiehlt es sich, für größere Schadensfälle die Bereithaltung eines 24/7 Incident Response Service zu vereinbaren.

Interne und externe Leistungen
kombinieren

Nicht alle Aufgaben von der Auswahl von Produkten, Qualifikation von Mitarbeiter:innen und 24/7 Überwachung der Infrastruktur müssen intern erbracht werden. Qualifizierte Beratungsunternehmen und MSSPs wie die DCSO unterstützen dabei, die eigenen Ressourcen effizient zu nutzen. Das Portfolio reicht dabei von der Tool- und Prozessberatung über aktuelle Indikatoren, bis hin zur aktiven Überwachung und Reaktion. Sprechen Sie uns gerne an, oder informieren Sie sich über die Dienstleistungen der DCSO unter: www.dcso.de

Über die DCSO
Deutsche Cyber-Sicherheitsorganisation GmbH

Die DCSO Deutsche Cyber-Sicherheitsorganisation GmbH (DCSO) entwickelt moderne Cybersicherheits-Dienstleistungen für die deutsche Wirtschaft und bietet ihren Kunden darüber hinaus einen geschützten und herstellerneutralen Raum zum Austausch und der Zusammenarbeit in allen Fragen der Cybersicherheit.

Unter dem Dach der DCSO tauschen sich Unternehmen nicht nur untereinander, sondern auch mit Behörden und Forschungsinstituten über Cybersicherheitsgefahren aus. Die gewonnenen Erkenntnisse fließen in effektive Strategien und Lösungen für Prävention, Reaktion sowie Abwehr und sorgen so für mehr Sicherheit für Unternehmen, Wirtschaft und Gesellschaft.

Aus diesen Synergieeffekten der DCSO-Gemeinschaft und der eigenen Expertise entwickelt das Berliner Unternehmen moderne Managed Security Services in den Bereichen Bedrohungsidentifikation (Threat Intelligence), Monitoring und Detektion (Threat Detection & Hunting) sowie Hilfe zur Vorfallsbehandlung (Incident Response).

Daneben unterstützt die DCSO Firmen mit Beratungsleistungen bei der Bewertung geeigneter Sicherheitstechnologien, der eigenen Cybersicherheit und der von Dienstleistern sowie beim Aufbau resilienter Business- und Informationssicherheitsprozesse.

Mit dem Ziel der Bedrohungen durch global organisierte Cyberkriminalität und staatlich gelenkte Wirtschaftsspionage entgegenzuwirken, wurde die DCSO 2015 von Allianz SE, BASF SE, Bayer AG und Volkswagen AG für die deutsche Wirtschaft gegründet.

DCSO Deutsche Cyber-Sicherheitsorganisation GmbH
EUREF-Campus 22
10829 Berlin, Germany

+49 30 - 72 62 19 - 0

www.dcso.de