Bild: Achtwerk GmbH & Co KG

Security-Leitwarte

Ransomware- oder andere Cyberattacken

MES benötigt Cybersicherheit

Am Freitagmittag, dem 7. Dezember 2018 berichtet Spiegel Online, dass KraussMaffei von einem schweren Cyberangriff durch eine Ransomware getroffen wurde. Welcher Produktionsverantwortliche denkt sich da nicht: 'Kann uns das auch passieren?' Mit dem passenden Mix verschiedener Maßnahmen können Werksleiter das Risiko wenigstens deutlich reduzieren.

Zwar gibt es eine ganze Reihe von Gründen, warum diese Angriffe so oft erfolgreich sind, etwa die zahlreichen Sicherheitslücken in gänger Software. Vor allem aber fehlt in Fertigungsunternehmen oft eine aktuelle Beurteilung eines solchen Risikos. Um einer solche Bewertung zu erhalten, lässt sich über ein kontinuierliches Cyber-Risikomanagement zunächst die Bedrohungslage untersuchen. Dabei gelten zwei Grundsätze:

- Das Risiko, das Cyberangriffe die Produktion stören, erhöht sich täglich.
- Das Risiko, betroffen zu sein und die Auswirkungen werden fast immer erheblich unterschätzt.

Gerne argumentieren Betreiber, das eigene Unternehmen sei zu unbedeutend, um in den Fokus von Hackern zu geraten. Angegriffen werden diese Unternehmen dennoch. Da gibt es einmal die 'einfachen Ziele': Hierzu zählt, ob die Schutzeinrichtung einer Unternehmens-IT einem ersten Angriff standhalten kann. Für Kriminelle, 'Hacktivists' und 'Script Kiddies' sind einfache Ziele lukrativer, da diese Angreifer in der Regel weniger Aufwand für eine Attacke betreiben. Für Staaten und Wettbewerber sind diese Ziele als Beifang durchaus interessant. Häufiger agieren diese Sorte Angreifer allerdings zielgerichteter und dann sehr intensiv an einem Cyber-Angriff. Als 'kollaterale Ziele' landen häufig solche Unternehmen im Netz von Cyber-Angreifern, wenn

sie mit Geschäftspartnern in Staaten oder Branchen arbeiten, die häufig attackiert werden. Typische Gefahren gehen also von Kriminellen, Hacktivists und Script Kiddies, Staaten und Wettbewerbern aus. Allen gemeinsam ist, dass sie Zeit haben, sich vorzubereiten, Informationen zu sammeln, die passenden Werkzeuge zu finden. Dabei dürfte den wenigsten Angreifern der unmittelbare Schaden bewusst sein, den sie anrichten. Sie probieren zunächst nur aus und erkennen erst später, welches Potenzial der Angriff entfaltete.

Was bedeutet das für die MES-Ebene?

Wenn ein Cyberangriff auf die Werksebene durchschlägt, hat das drastische Folgen. Das MES ist für die Betriebsführung das Rückgrat, wie folgende Szenarien illustrieren: Die Aufträge werden entgegengenommen und geplant. Das notwendige Material, die Maschinen- und Personalverfügbarkeit geprüft und in die Arbeitsaufträge eingetragen. Es gilt die Lieferzeit einzuhalten. Und dann eine Störung. Ist die Maschine kaputt oder nur der Datenfluss unterbrochen? Das Steuersystem ist nicht erreichbar, die Arbeitsaufträge laufen – Fehlermeldung! Auswahl der nächsten verfügbaren Maschine? Auch nicht erreichbar. Bei einem Cyberangriff werden fast immer die gleichen Komponenten gestört. Ein zweiter Angriffsvektor betrifft die Erfassung der Kennzahlen. Die Rückmeldungen zu den Maschinendaten scheinen alle in Ordnung – wirklich? Kaum eine Kommunikation in der Produktionsanlage ist etwa durch Authentifizierung oder Verschlüsselung abgesichert. Es ist ein vergleichsweise einfaches Unterfangen, die Daten dieser Kommunikationen zu manipulieren. Erst im letzten Qualitätscheck der Betriebsdatenerfassung wird festgestellt, dass das Produkt nicht den notwendigen Maßstäben entspricht. Generell gibt es hohe Risiken in Bezug auf Qualität und bei zeitkritischen Produktionen. Wie lange darf ihre Produktion ausfallen? Wie schnell können Störungen und Manipulationen beseitigt werden? Für Unternehmen lohnte sich, folgenden Vorfall einmal durchzuspielen: Ein System, etwa die Datenerfassung oder eine Steuerung, wird verschlüsselt. Wie schnell sind die notwendigen Personen vor Ort? Ist der Systemintegrator erreichbar? Welchen Stand hat das Backup? Sind die letzten Änderungen der Steuerung zur Qualitätsverbesserung gespeichert?

Die rechtlichen Anforderungen werden verschärft

Der Gesetzgeber hat mit dem IT-Sicherheitsgesetz (ITSiG) bereits 2015 den rechtlichen Rahmen zur Erhöhung der IT-Sicherheit für die unterschiedlichen Branchen vorgegeben. Wie das Magazin WirtschaftsWoche berichtete, plant das Bundesinnenministerium im Rahmen des sogenannten IT-Sicherheitsgesetzes 2.0 die Meldepflicht von Unternehmen bei Angriffen auf ihre IT-Infrastruktur Ende 2019 zu verschärfen. Beispielsweise soll die Meldepflicht für erhebliche IT-Sicherheitsvorfälle auf weitere Unternehmen übertragen werden, bis in den Mittelstand hinein. Diese Pflicht gilt bislang nur für Betreiber kritischer Infrastrukturen. Das bedeutet, dass sich nahezu jeder Produktionsbetrieb um seine IT-Sicherheit zu kümmern hat. Annahmen wie: 'uns betrifft das nicht' oder 'wir sind nicht im Internet, wir haben eine Insellösung' dürften dann nicht mehr reichen. Zumal schon eine Fernwartung oder ein Zugriff über den kompromittierten Laptop eines Dienstleisters reicht, um einen Hackerangriff einzuleiten.

Grundlagen für eine abgesicherte Produktions-IT

Ein effektives Security-Managementsystem für die Werks-IT basiert auf den drei Säulen:

- Organisatorische Maßnahmen
- Technische Maßnahmen
- Personelle Maßnahmen

Damit scheint die Umsetzung des Sicherheitsstandards auf den ersten Blick jedoch etwas problematisch, da häufig die Budgets sowie die Fachkräfte fehlen, um ein durchgängiges Sicherheitsniveau und den im ITSiG geforderten Stand der Technik umzusetzen. Ein Lösungsweg könnte sein, bei den methodischen Vorgaben am bereits vorhandenem Asset- und Risikomanagement in der Produktweiterentwicklung anzuknüpfen. Mit einfach bedienbaren Werkzeugen sollen die grundlegend notwendigen Maßnahmen geplant, die Umsetzung unterstützt und dokumentiert werden. Ein großes Problem bei der Implementierung von Sicherheitslösungen für vernetzte Automatisierungen ist der Einfluss, den diese auf die Verfügbarkeit haben können. Standard-

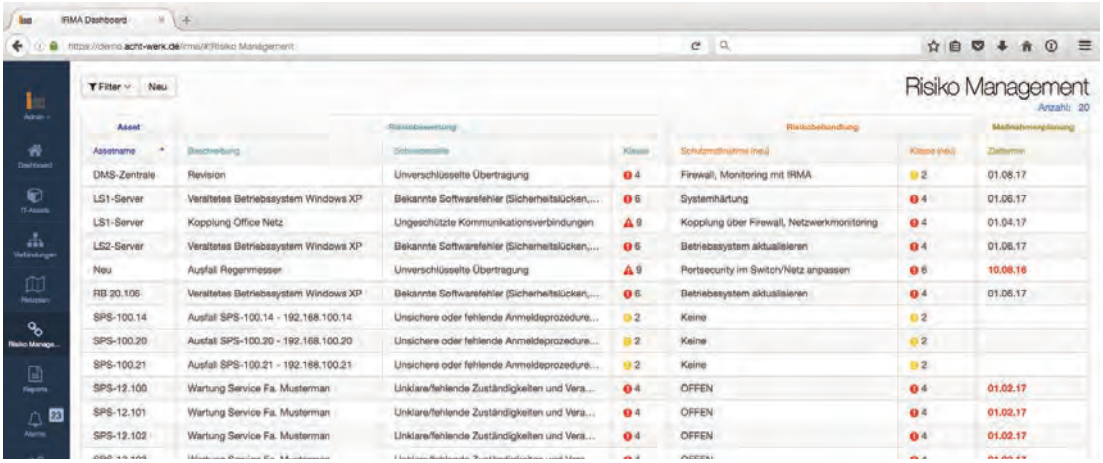

Bild: Videc Data Engineering GmbH

Technische Lösungen lassen sich passiv an die Automatisierung anschließen, um ein Risikomanagement für die Datenzugriffe auf Werksebene einzurichten.

IT-Security-Tools haben das Potenzial, die Leistung zu beeinträchtigen, Latenzzeiten oder sogar Abstürze zu verursachen. Profinet, Modbus TCP, Ethercat und Co. sind spezielle Protokolle auf Basis der heute weitgehend genutzten Standardtechnologie des Industrial Ethernet für die Anforderungen der zeitkritischen Datenkommunikation in Produktionsanlagen. Jede zusätzliche Aktivität im Produktionsnetz kann diese Kommunikation stören oder in Systemen Fehlfunktionen bis hin zum Ausfall der gesamten Produktionsanlage herbeiführen. Daher ist das passive Scannen und Überwachen des Produktionsnetzes vorteilhaft. So wird die Automatisierungsebene mit ihren nicht-patchbaren Altsystemen nicht durch aktive Abfragen beeinträchtigt.

Bedienen ohne Spezialwissen erforderlich

Des Weiteren sollte die Bedienung auch für Anwender ohne Vorkenntnisse möglich sein und sich in die Betriebsprozesse, etwa im MES und Alarmmanagement, integrieren. Um die entsprechenden IT-Sicherheitsmaßnahmen in einem überschaubarem Zeitrahmen projektieren zu können, bietet der Markt mittlerweile Lösungen, die sich ohne Vorab-Analysen und komplizierte Konzepte in den Betrieb integrieren lassen. Diese Systeme werden passiv an die Automatisierung angeschlossen, bevor sie die IT-Infrastruktur eigenständig identifizieren, überwachen und deren Status beurteilen. Auf Basis dieser Daten lässt sich die Risikoanalyse starten, ohne die verhandene Systemwelt vorher manuell dokumentieren zu müssen. Später lassen sich die Systeme auf Werks-Ebene kontinuierlich überwachen, die Zugriffe analysieren und eine Alarmierung aufsetzen. Selbstverständlich müssen System wie diese durch eine Reihe von weitren Maßnahmen ergänzt werden, um das IT-Sicherheitsniveau auf ein zufriedenstellendes Maß zu heben. Aber ein Echtzeitmonitoring der vernetzten Automatisierung und des Datenaustausches in der Produktion ist ein sehr gutes technisches Fundament, um weitere Prozesse rund um die IT-Sicherheit im Werk daran anzuknüpfen. ■

www.videc.de

Autoren

Achim Mehrmann ist Key Account Manager bei Videc Data Engineering GmbH.
Jens Bußjäger ist Geschäftsführer bei Achtwerk GmbH & Co KG.