Herausforderung 6:
Schutz für die „Smart Factory“

Die Fertigungsindustrie ist ganz klar ein Ziel für Cyberkriminalität. Bereits die Hälfte der Unternehmen dieser Branche waren schon mit einem Cyberangriff konfrontiert und 24% der Unternehmen geben an, finanzielle oder andere geschäftliche Verluste durch einen solchen Angriff erlitten zu haben[5]. Ein Sicherheitsbruch kann zum Verlust oder Diebstahl sensibler Daten, zu einer Unterbrechung des Zugriffs auf Systeme und betriebliche Technologien oder zu Industriespionage führen.

Die wachsende Anzahl der vernetzten „Dinge“ macht die Cybersicherheit zu einer geschäftlichen Notwendigkeit. 59% der Fertigungsunternehmen berichten, dass sie bereits von einem Kunden dazu aufgefordert wurden, die Zuverlässigkeit ihrer Cybersecurity-Prozesse unter Beweis zu stellen, und 58% der Unternehmen haben dies von einem Partner aus ihrer Lieferkette verlangt[6].

Die „Smart Factory“ ist ereignisorientiert, wird kontinuierlich von Sensoren überwacht und passt sich immer wieder neu an, lernt ständig dazu und erlaubt es Systemen, autonom zu agieren. Fertigungsunternehmen, die das gesamte Potenzial erweiterter Analytik, kollaborativer Plattformen und IIoT-Technologien nutzen möchten, sollten deshalb unbedingt die Sicherheit und die Risiken der Infrastruktur, die diese Art der Innovation unterstützt, berücksichtigen.

[5,6] EEF Cyber Report 2018

Die Lösung:
Ein mehrstufiges Cybersecurity-Konzept auf AI-Basis

Die Cybersicherheit ist ein wichtiger und absolut entscheidender Aspekt, denn ohne ein funktionierendes Sicherheitskonzept ist Ihr Unternehmen und dessen Handlungsfähigkeit gefährdet. Ein mehrstufiges Sicherheitskonzept, das die Angreifbarkeit der Plattformen reduziert, Daten schützt und intelligente Sicherheit für Geräte und Netzwerk bereitstellt, ist erforderlich.

Die Transformation der Sicherheitsstrategie ermöglicht es Ihrem IT-Sicherheitsteam, von einer defensiven zu einer proaktiven Haltung zu gelangen. Die IT-Sicherheit sollte nicht aus einem Konglomerat isolierter Aktivitäten bestehen, sondern einen Mechanismus mit vielen beweglichen Teilen darstellen, der die Echtzeit-Bedrohungserkennung umfasst, den geschäftlichen Kontext einbezieht und der so gemanagt wird, dass Ihre wertvollen Ressourcen, Daten und geistiges Eigentum sicher sind und bleiben, ohne die Innovation zu hemmen.

Dieser Ansatz beruht auf drei Säulen:

Kunden verlagern die Verantwortung für den Datenschutz immer mehr auf ihre Lieferanten

1. Kontinuierliches Risikomanagement

Kunden verlagern die Verantwortung für den Datenschutz immer stärker auf ihre Lieferanten. Um diesen Anforderungen gerecht zu werden, ist die Vereinheitlichung Ihrer Sicherheits-und Risikomanagementstrategie erforderlich. Durch die Etablierung einer kontextbasierten Transparenz kann Ihr Security-Team die Wahrscheinlichkeit und die möglichen Auswirkungen eines Ereignisses einschätzen bzw. definieren und den besten Ansatz für den Umgang mit Risiken (Vermeidung, Übertragung, Akzeptanz oder Abmilderung) festlegen. Zudem kann so die Art der einzusetzenden Sicherheitskontrollen zum Verhindern, Abschrecken, Erkennen oder Korrigieren von Angriffen bestimmt werden.

Die innovative Nutzung von Daten revolutioniert die Fertigungsindustrie

2. Sichere Infrastrukturen

Die innovative Nutzung von Daten revolutioniert die Fertigungsindustrie. Aber um tatsächlich von den neuen Möglichkeiten zu profitieren, muss ein freier Datenfluss über Mitarbeiter, Unternehmen, Ökosysteme und sogar Ökonomien hinweg möglich sein. Doch die Informationsflut hat, gemeinsam mit den vielfältigeren Benutzerpräferenzen, vernetzten Geräten und dem Management virtueller und hybrider Cloud-Umgebungen, eine ganze neue Komplexität mit sich gebracht.

Eine sichere, moderne Infrastruktur sollte daher Daten über Geräte, Identitäten, Endpunkte und Speicher hinweg in virtuellen oder hybriden Umgebungen wirksam schützen.

Kein Unternehmen ist eine uneinnehmbare Festung

3. Erweiterter Sicherheitsbetrieb

Kein Unternehmen ist eine uneinnehmbare Festung. Cyberkriminelle verfügen über umfangreichere Ressourcen und ausgefeiltere Tools als je zuvor. Ein motivierter Hacker wird also wahrscheinlich irgendwann einen Weg in die Systeme finden. Um das Risiko zu minimieren, sollte die IT-Sicherheit in Richtung einer automatischen Reaktion auf Angriffe weiterentwickelt werden. So erfolgt eine schnellere Reaktion auf ein Eindringen oder Angriffe und die Auswirkungen können begrenzt werden. Dabei gehört besonders die Absicherung der Außengrenzen zu den Top-Prioritäten des CIO und des CISO.

Kundendaten schützen – durch Analytik

Wie können Kundeninformationen und Transaktionsdaten für die Generierung von Mehrwerten genutzt und gleichzeitig wirksam geschützt werden? Mastercard, ein weltweit führender Dienstleister im Zahlungsverkehr, wollte die prognostische Analytik nutzen, um mehr über das Kaufverhalten und entsprechende Verhaltensmuster der Kunden zu erfahren und daraus wertvolle Erkenntnisse zu gewinnen. Zu diesem Zweck war eine Analyseumgebung für die Daten aus 2,2 Milliarden Kredit- und anderen Zahlungskarten sowie aus bis zu 160 Millionen Transaktionen pro Stunde erforderlich – ebenso wie ein maximaler Schutz für alle diese sensiblen finanz- und personenbezogenen Daten.

Mastercard hat gemeinsam mit Unternehmen der Dell Technologies-Gruppe an der Erstellung einer sicheren Lösung für die gewünschte Datenanalytik gearbeitet. Die Lösung hat die Sicherheit und den Schutz gegen Betrug durch die Analyse von Verhaltensmustern beim Kauf sowie der Affinitäten und Kaufrhythmen mithilfe des Maschinellen Lernens ermöglicht. Außerdem kann das Unternehmen nun aus den anonymisierten Daten über den “Share of Wallet” im Wettbewerbsvergleich, den durchschnittlichen Umsatz sowie die Kaufhäufigkeit echten geschäftlichen Nutzen generieren. So kann man bei Mastercard jetzt Marketingchancen erkennen und nutzen, den Return-on-Investment bemessen und gleichzeitig sensible Daten umfassend schützen.

mastercard

Quelle: Dell EMC Customer Stories

Die Quantifizierung der betrieblichen und kaufmännischen Auswirkungen von Sicherheitsbrüchen kann Sie bei der Entwicklung von Risikovermeidungsstrategien unterstützen, die dabei helfen können, Angriffe zu vermeiden und angemessen sowie schnell auf dennoch erfolgte Angriffe zu reagieren.

Quelle: Dell Technologies