ANGRIFF AUF DIE VERNETZTEN MASCHINEN

Erfolgreiche Attacken auf Produktionsebene und IIoT-Geräte können große Schäden verursachen und möglicherweise zum finanziellen Desaster für eine Firma werden. Predictive Maintenance wird in diesem Zusammenhang immer wichtiger für Unternehmen.

Autor: Robert Blank **Redaktion: Diana Künstler**

➤ Wie teuer ein Angriff auf die IT-Infrastruktur eines Unternehmens werden kann, geht aus einer Studie von IBM Security und des Ponemon Instituts über die Kosten eines Datenlecks hervor. Im Jahr 2018 kostete demnach ein solches Leck das betroffene Unternehmen 3,86 Millionen Dollar. Unter die Kosten fallen Faktoren wie forensische Untersuchungen, Gegenmaßnahmen, Benachrichtigungen der Aktionäre und damit fallende Börsenkurse. Außerdem gehören rechtliche und regulatorische Auflagen dazu sowie die Kosten für Betriebsausfälle und – besonders schwerwiegend – die sinkende Reputation, die zum Verlust von Aufträgen führen kann.

Datenlecks sind aber nicht das einzige Angriffsziel krimineller Hacker. Da im Zuge der Digitalen Transformation mehr Unternehmen ihre Produktionsinseln ebenfalls digitalisieren, das heißt an das öffentliche Internet anschließen, wird aus der Maschine von gestern das IoT-Gerät von heute. Das führt aber auch dazu, dass Geräte, die mit völlig veralteter Software auf ihren Kontrolleinheiten oder mangelhaften IT-Sicherheitsprogrammen ausgestattet sind, plötzlich nicht nur über das abgeschottete Firmennetzwerk miteinander verbunden werden, sondern über den Unternehmensperimeter hinaus.

Wenn 50 Millionen Datensätze betroffen sind, also eine Mega-Datenpanne vorliegt, betragen die geschätzen Kosten rund 350 Millonen Dollar.*

Maschinen von gestern sind die IoT-Geräte von heute

So ergeben sich neue Einfallstore und bislang ungeahnte Angriffsvektoren für Cyberkriminelle, weil das SCADA-Protokoll (Supervisory Control and Data Acquisition) der Maschinen nie darauf ausgelegt wurde, mit dem öffentlichen Internet verbunden zu werden. Will ein Krimineller also einem Unternehmen schaden, so muss er nicht unbedingt die Büronetzwerke im Blick haben, Daten verschlüsseln wollen oder Rechnungen fälschen. Geht es dem Angreifer nur darum, Schaden anzurichten, kann er sich darauf konzentrieren, die Produktionsanlagen lahmzulegen. Nicht mehr durch ein tatsächliches, feindliches Eindringen in Fertigungshallen wie früher, sondern von zuhause mithilfe seines Computers, einer Schadsoftware und unter Ausnutzung der Tatsache, dass Maschinen mit dem öffentlichen Internet verbunden sind, deren Sicherheit dafür nicht ausreicht. Das Ausmaß eines Angriffes auf die IoT-Geräte eines Unternehmens kann in einem ungeahnten Schaden resultieren. Es kann nicht einfach ein Back-up aufgespielt werden, wie bei einem Angriff durch Ransomware – falls die IT-Sicherheit darauf vorbereitet ist. Stattdessen fallen Maschinen aus, stehen Fließbänder still und werden womöglich sogar Arbeiter durch verrücktspielende Geräte verletzt, weil diese nicht einmal mehr auf die Notabschaltung reagieren. Die Produktion eines Unternehmens würde empfindlich gestört oder kommt sogar zum Erliegen. Das ist für große Konzerne schon ein schwerer Schlag, aber für mittlere und kleine Firmen kann eine Woche Stillstand das Aus bedeuten. Finanziell kann ein solcher Angriff deshalb zur Katastrophe führen, weil die Schadprogramme gesucht und eliminiert, die Maschinen repariert werden müssen und Aufträge liegenbleiben oder zurückgezogen werden. Der Schaden kann sogar noch größer werden, falls ein Angriff nicht nur geschieht, sondern vom Unternehmen geheim gehalten wird und dann doch an die Öffentlichkeit gelangt. Das Vertrauen der Kunden ist zerrüttet, Investoren springen ab: Nach kurzer Zeit kann ein mittleres oder kleines Unternehmen finanziell am Ende sein.

Die überwiegende Mehrheit dieser Datenpannen (10 von 11) beruhen auf böswilligen und kriminellen Angriffen – im Gegensatz zu technischen Störungen oder menschlichem Versagen.*

Bekannte Schwachstellen rechtzeitig suchen und finden

Die Bedrohung der IoT-Geräte und Produktionseinheiten aber ist keine neue Erkenntnis und ihre Schwachstellen sind kein Geheimnis. Auch die unzureichende Absicherung wird immer wieder angemahnt. Dennoch ergab eine weitere Studie des Ponemon Instituts im Jahr

.018, dass beinahe 60 Prozent der Gefährdungen für Firmen auf bestehende und bekannte Schwachstellen zurückzuführen sind. IT-Sicherheitsabteilungen müssen also künftig von der Unternehmensführung ernster genommen werden und dürfen gleichzeitig nicht aufhören, beständig nach Schwachstellen zu suchen, um sie zu schließen, bevor ein Internetverbrecher sie ausnutzen könnte. Weil aber die Menge an möglichen Schwachstellen, Angriffsmöglichkeiten und Meldungen über angeblich gefundene Bedrohungen durch Schwachstellen-Scanner zunehmend unübersichtlicher wird, darf im Zuge des digitalen Wandels die Automatisierung nicht zu kurz kommen. Sie kann Administratoren dabei helfen, Fehlalarme schneller auszusortieren, Zugriffe zu verwalten und gefundene Bedrohungen nach ihrer tatsächlichen Gefahr einzustufen. So haben die Fachkräfte im Unternehmen mehr Zeit für die Aufgaben übrig, die tatsächlich das manuelle Eingreifen erfordern.

Zunehmend wichtiger wird auch das Thema Predictive Maintenance, also vorausschauende Wartung. Lösungen dieser Kategorie zeigen den Verantwortlichen einer Firma rechtzeitig an, wann die Maschinen eine Wartung benötigen, um überraschende Ausfälle der Produktion zu reduzieren – was sonst sehr teuer werden würde. Das bedeutet aber, dass immer mehr Maschinen mit Sensoren ausgestattet werden, die mehr und mehr Daten sammeln. Diese Daten aber müssen auf den Server und an die richtigen Standorte geschickt werden, sie dürfen also nicht durch Firewalls aufgehalten werden. Das gilt auch für die Anwendungen, die auf diese Daten zugreifen. Befinden sich die Sensoren und Server im gleichen Netzwerk, gibt es keine Hindernisse, das wäre die althergebrachte Situation. Mit der Öffnung der Produktionsumgebungen aber für das Internet und der Vernetzung von verschiedenen Fabriken, gehen die Daten an ein außenstehendes Netzwerk. Dort aber kann eine Firewall zum ungewollten Hindernis werden.

Im Schnitt verursacht eine Datenpanne mit einer Million betroffenen Datensätzen beinahe 40 Millionen US-Dollar an Kosten.*

Durchschnittlich brauchen deutsche Unternehmen 138 Tage, um eine Datenpanne zu identifizieren und 41 Tage, um sie einzudämmen.*

Dies manuell zu regeln, ist eine schier unmögliche Aufgabe und würde den Prozess stark verlangsamen sowie die Kosten in die Höhe treiben. Das aber würde die Idee hinter der Predictive Maintenance, Wartungskosten zu verringern und Ausfälle zu reduzieren, um produktiver und wirtschaftlicher sein zu können, ad absurdum führen. Eine automatisierte Sicherheitslösung dagegen, die sich im Rahmen von Richtlinien um den Zugriff kümmert, liefert die nötige Geschwindigkeit und Genauigkeit, um einen zuverlässigen Datenfluss zu gewährleisten. Das Ausmaß der vorausschauenden Wartung auf die Geschäftszahlen belegt eine Studie der Unternehmensberatung Roland Berger aus dem Jahr 2017. Die Kosten werden demnach weltweit bis ins Jahr 2022 auf 6,3 Milliarden Dollar steigen, im Vergleich zu 1,5 Milliarden Dollar im Jahr 2016. Das sind lediglich die erwarteten Prognosen, die kühneren gehen von noch höheren Kosten für eine funktionierende vorausschauende Wartung aus.

Automatisierung von Routineaufgaben entlastet die IT-Sicherheit

Mit Blick auf die hohen Unterhaltskosten für die IT-Architektur an sich kann es nur im Interesse der Unternehmen liegen, ihre Produktionsabteilungen gegen Angriffe aus dem Internet bestmöglich zu schützen. Andernfalls drohen teure Schäden und das finanzielle Desaster. Es gilt also, neben der naheliegenden Büro-IT auch die zunehmend vernetzten Maschinen in die Planung der modernen IT-Sicherheit einzubeziehen. Dabei kann die Automatisierung bestimmter Routine-Aufgaben die IT-Sicherheitsleute entlasten, das Budget senken und dabei helfen, schneller auf tatsächliche Angriffe zu reagieren.

Die Zahlen von Roland Berger verdeutlichen zudem, wie wichtig es mittlerweile geworden ist, die IT-Architektur eines Unternehmens strategisch zu planen und die IT-Sicherheit ernst zu nehmen. Nur wenn beide gut aufeinander abgestimmt sind, kann ein Unternehmen von der Digitalisierung in vollem Umfang profitieren und sich dabei sicher fühlen. So wird die IT-Sicherheit vom lästigen Hindernis zum Wegbereiter hin zu den Vorteilen einer automatisierten und digitalisierten Unternehmensstruktur.

Robert Blank, Regional Sales Manager DACH bei Algosec

Die durchschnittlichen Kosten einer Datenpanne betragen in Deutschland 3,88 Millionen Euro.*

DATENLECKS SIND NICHT DAS EINZIGE ANGRIFFSZIEL KRIMINELLER HACKER. DA IM ZUGE DER DIGITALEN TRANSFORMATION MEHR UNTERNEHMEN IHRE PRODUKTIONSINSELN EBENFALLS AN DAS ÖFFENTLICHE INTERNET ANSCHLIESSEN, WIRD AUS DER MASCHINE VON GESTERN DAS IOT-GERÄT VON HEUTE.

*„2018 Cost of a Data Breach Study", Ponemon Institute /IBM Security