Geschützte IT-Security – ungenügende OT-Security

IT und OT zuverlässig und sicher verbinden

IT-Sicherheit ist schon lange kein Thema mehr, dass man mittelständischen Unternehmen erst von der Grundlinie aus vermitteln muss. KMUs haben in den letzten Jahren gelernt, dass Abläufe im Unternehmen eine durchdachte Security-Strategie benötigen. Dieser IT-Security-Bereich deckt die internen geschäftlichen Abläufe ab, schützt die Kommunikation mit Kunden bei E-Mail und Webverkehr und sichert grundsätzlich die Daten in Form von Archivierung, Backup oder Verschlüsselung. Mitunter haben Umfragen festgestellt, dass Mittelständler im IT-Security-Bereich bis zu 50 verschiedene Security-Tools einsetzen, um aller IT-Gefahren Herr zu werden.

Ein Teil der Wahrheit

In soliden und teils traditionsreichen Unternehmen wurde neben der Verwaltung und Geschäftsführung auch die Produktion immer weiter aus- und umgebaut. Manchmal wurden aus vielen kleinen Produktionsinseln ganze Fertigungsstraßen, die durch eine Reihe Logistik und digitaler Abläufe miteinander verzahnt sind. Genau an diesem Wachstumspunkten wird allzu oft nicht an die zunehmenden Gefahren durch Cyberangriffe gedacht und schlichtweg keine Gefahrenabwehr konzipiert. Denn viele Unternehmer sind oft der Auffassung, dass die vorhandene Informations-Technologie (IT)-Sicherheit auch die wichtige Produktion mit abdeckt. Aber das ist nur ein Teil der Wahrheit, denn Produktionsmaschinen und Arbeitsnetzwerke benötigen Operative-Technologie (OT)-Sicherheit. Denn klassische IT-Security-Lösungen sind anders konzipiert als eine OT-Security.

Produzierende Geräte schützen

Ein Netzwerk mit OT-Sicherheit schützt alle darin arbeitenden Geräte und Maschinen, auch wenn diese mit den exotischsten Betriebs- oder Steuerungssystemen arbeiten. Denn es ist meist schlicht technisch nicht möglich, eine Schutz-Software oder einen Agenten auf die Maschine zu bringen. Aber ist eine Maschine (IIoT) durch ein Interface in der Lage „IP“ (Internet Protokoll) zu sprechen, kann sie in ein Netzwerk integriert werden. Sobald sich ein produzierendes Gerät innerhalb eines Netzwerks befindet, ist es damit auch theoretisch angreifbar. Spezialisten nennen diese Maschinen „Industrial Internet oft Things“, kurz „IIoT“. Angreifer nutzen dann zum Beispiel einen speziellen Code, den nur die Maschine versteht, senden ihn durch das Netzwerk und verursachen damit Schaden oder starten eine Erpressung des Unternehmens. Aber auch nicht besonders geschützte Hilfs-PCs sind ebenfalls oft ein Ziel. Ein populärer Fall zeigt den Zusammenhang von falsch gedachter IT-Sicherheit in OT-Bereichen.

Ransomware-Angriff auf Colonial Pipeline - KRITIS

Kritisch wurde es bei der Attacke auf den amerikanischen Kraftstoffversorger und Pipeline-Betreiber Colonial Pipeline. Am 7. Mai 2021 um 5 Uhr morgens erschien bei einem Mitarbeiter in einem Kontrollraum für die Pipeline an einem Steuerungs-PC am Bildschirm anstatt der gewohnten Überwachungswerte eine klassische Lösegeldforderung von Cyberkriminellen. Den Angreifern war es gelungen die Überwachungsebene für die Pipeline zu infiltrieren und dort eine Ransomware zu platzieren. Auf Anweisung des Betriebsleiters schalteten die Mitarbeiter die Pipeline ab. Damit war die Hauptquelle von Benzin, Diesel und Heizöl für die Ostküste der USA gekappt. Ein KRITIS-Versorger war lahmgelegt. Als dann nach kurzer Zeit der Angriff und die Abschaltung an die Öffentlichkeit durchsickerte, begann die Bevölkerung mit Hamsterkäufen an den Tankstellen. Diese waren nach wenigen Tagen ausverkauft und mussten zum Teil schließen. Erst am 12. Mai 2021 wurde die Pipeline wieder eingeschaltet, nachdem an die Angreifergruppe Darkside zuvor 4,4 Millionen Dollar gezahlt wurden. Die amerikanische Regierung stufte diesen Angriff auf einen KRITIS-Betreiber als terroristischen Akt ein und verfolgte die Angreifer.

Autor:
Stefan Schachinger,
PM Network Security - IoT/OT/ICS
Barracuda Networks
www.barracuda.com

Digitales Schreckenskabinett

Die frei zugängliche Webseite des MITRE ATT&CK-Framework ist eine Art Wikipedia zu allen Angriffsarten, den verwendeten Werkzeugen, den Angriffsgruppen und vieles mehr. Das digitale Schreckenskabinett führt sogar eine Liste aller APT-Gruppen (Advanced Persistent Threat), bei der einige Gruppen schon keine Namen mehr haben, sondern Nummern. Diese gehen bereits bis 41.

Was machen Cybergangster mit dem Lösegeld?

Es ist bei vielen Unternehmen die zentrale Frage eines Worst-Case-Szenarios einer Ransomware-Attacke mit verschlüsselten PCs: „Sollen wir das Lösegeld zahlen oder nicht?“. Eine Frage, die jeder für sich beantworten muss und selbst Spezialisten nur uneinig beantworten. Geht es bei einem Betrieb um die nackte Existenz, wird jeder sofort einer Zahlung zustimmen. Aber Unternehmen müssen sich darüber klar sein, dass jeder gezahlte Euro einen weiteren Angriff finanzieren kann. Lösegeld zahlen oder nicht zahlen? Die politisch korrekte Antwort lautet: nicht bezahlen. Weil das die eigene Attraktivität als zukünftiges nochmaliges Ziel reduziert. In der Praxis liegt der Fall natürlich anders. Wenn wesentliche Daten nicht mehr zugänglich beziehungsweise mit vernünftigem Aufwand wiederherstellbar sind, dann bleiben einem Unternehmen nicht mehr viele Optionen. Das ist somit weniger eine moralische als eine kaufmännische Entscheidung. Die Zahlung entbindet natürlich nicht von der Notwendigkeit einer forensischen Aufarbeitung und Aufräumaktion im Nachgang zusätzlich zu neu zu tätigen Schutzmaßnahmen, die gegen Wiederholung absichern. Umso mehr ist es angeraten, in Prävention zu investieren, solange man noch kann.

OT-Security erfordert unternehmerisches Umdenken

Automatisierung und Digitalisierung betrieblicher Abläufe bringen mittelständischen Unternehmen viele Vorteile, wie etwa bei der Produktionsflexibilität oder bei der Preisgestaltung für den Markt. Umso erfolgreicher ein Betrieb am Markt agiert, umso mehr kann er in den Fokus von Angreifern als lohnenswertes Ziel rücken. Schließlich kann ein Unternehmen mit einem guten wirtschaftlichem Flow keine Unterbrechungen des Service oder der Produktion gebrauchen.

Daher müssen produzierende KMUs in puncto OT-Security umdenken und ihre Lage prüfen. Wie gefährdet ist der aktuelle Produktionsstandort? Sind die Netzwerke getrennt, verknüpft und von außen erreichbar? Gibt es überhaupt eine passable OT-Security und wann wurde diese zuletzt überprüft? Viele dieser Fragen können Unternehmen gar nicht selbst beantworten, sondern brauchen dazu externe Beratung bis hin zum Testangriff und einer Auswertung der Verwundbarkeit.

Wie sollten Unternehmen am besten vorgehen?

Unternehmen sollten heute am besten bereits bei der Planung eines Neu- oder Umbaus eines Betriebs ihre OT-Sicherheitsstrukturen überdenken und prüfen. Am Beispiel der Planung und Umsetzung des Schutzes eines Offshore-Windparks etwa lässt sich das verdeutlichen. Jedes Gerät im Netzwerk, ob klein oder groß wie ein ganzes Windrad, wird als IoT-Gerät (Internet of Things) gesehen und innerhalb des Netzwerks geschützt. Jegliche Kommunikation im Netzwerk wird überwacht, Zugriffe nach Rechten bewertet oder Anomalien analysiert. Bei Bedarf lassen sich Teile des Netzwerks isolieren oder Zugriffe sofort sperren. Moderne produzierende Technologien sollten daher immer mit modernen OT-Schutz-Technologien zusammenarbeiten.

Zertifizierte OT-Sicherheit gegenüber Partnern und Kunden

Im Zusammenhang mit OT-Schutz von Produktionsbetrieben wird auch gerne von der Smart Factory oder Industrie 4.0 gesprochen. Diese Begrifflichkeiten haben natürlich alle eine Schnittmenge, die es für Unternehmen zu verstehen und einzuordnen gilt. Gerade bei Smart Factory wird oft nur die digitale Produktionsumgebung gesehen, die sich selbst organisiert, sowie die Fertigungsanlagen und die Logistiksysteme. Allerdings lässt sich auch eine ganze Umgebung einer Smart Factory einer Risikoanalyse in Bezug zur Informationssicherheit gemäß IEC 62443 prüfen. Zertifizierer, wie etwa VDE, bieten an die im Industriebereich bei Büro-IT und Operations-OT die Schnittstellen zwischen Maschinen, den Management- und Bürosystemen sowie zum Internet zu prüfen. „Dabei spielt es keine Rolle, ob das Netzwerk nur innerhalb einer Fabrik betrieben wird, oder ob externe Kommunikationspartner, wie beispielsweise Zweigstellen, über das Internet mit diesem Netzwerk verbunden sind“, sagt Christian Groß, Vorstandsmitglied VDE Rhein-Main. Nach erfolgreicher Prüfung erhalte der Netzwerkbetreiber das VDE Zertifikat für Informationssicherheit.

Wer schreibt

Barracuda ist bestrebt, die Welt zu einem sichereren Ort zu machen und überzeugt davon, dass jedes Unternehmen Zugang zu Cloud-fähigen, unternehmensweiten Sicherheitslösungen haben sollte, die einfach zu erwerben, zu implementieren und zu nutzen sind. Barracuda schützt E-Mails, Netzwerke, Daten und Anwendungen mit innovativen Lösungen, die im Zuge der Customer Journey wachsen und sich anpassen. ◄