Foto: Michael Traitov - stock.adobe.com

Im Kontext der Industrie 4.0 muss Cybersecurity im Business-Umfeld neu gedacht werden – auch mit KI und Machine Learning.

Cybersecurity mit KI und Machine Learning stärken

Wie IT-Sicherheit im Umfeld kritischer Unternehmensstrukturen mit dem Einsatz neuer Technologien neu gedacht werden kann.

NICO WERNER, HEAD OF CYBERSECURITY BEI DER TELENT GMBH

Im Kontext der Industrie 4.0 muss Cybersecurity im Business-Umfeld neu gedacht werden – auch mit KI und Machine Learning. Die vernetzte Industrie bietet Cyberkriminellen neue Angriffsflächen, denn in den zunehmend digitalisierten Produktionsprozessen müssen vernetzte Systeme miteinander sprechen. Genau darin liegt das Problem: Je mehr IT und OT zusammenwachsen, desto mehr Schlupflöcher entstehen, durch die schädliche Daten in Unternehmen eindringen oder Informationen unerwünscht nach außen abfließen. Um die Sicherheit zu erhöhen, braucht es eine ganzheitliche Strategie, die dem Mantra folgt: Vertraue niemanden!

In einer idealen Welt sind die Informationstechnologie (IT) und die Operational Technology (OT) physisch streng voneinander getrennt. Doch in der Realität ist die Welt eben nicht ideal. Es findet sich nahezu immer eine Schnittstelle zwischen dem in

Büros und Rechenzentren verwendeten Unternehmens LAN und den Prozessnetzwerken der Betriebe – auch wenn sich Unternehmen dessen nicht bewusst sind. Solange Produktionsumgebungen in sich geschlossen und nicht ans Internet angebunden waren, konnten Hacker sie schwerlich knacken. Doch das ändert sich, je smarter die Fabriken werden, beispielsweise damit Hersteller oder externe Dienstleister einen Fernzugriff für die Wartung erhalten. Auch durch die Vernetzung spielt es plötzlich eine Rolle, dass viele industrielle Leit- und Steuerungssysteme veraltet sind und seit Längerem keine Sicherheits-Updates mehr erhalten haben. Denn: Cyberkriminelle haben damit leichtes Spiel.

IT wird zum Einfallstor für Hacker in die OT

Die digitale Transformation verknüpft alles mit jedem und wird in wenigen Jahren IT- und OT-Netze komplett miteinander verweben. In dieser durchlässigen Welt des Industriellen Internet of Things (IIoT) nutzen Cyberkriminelle die IT als Einfallstor, um in die OT einzudringen. Im Vergleich zur klassischen Unternehmens-IT können Sicherheitsvorfälle bei industriellen Systemen zu wesentlich größeren Schäden führen – etwa, wenn eine Fertigungslinie stillsteht, eine fehlgesteuerte Anlage Menschen verletzt oder durch den Angriff auf eine Kritische Infrastruktur ein Stromnetz offline geht. Jede erfolgreiche Industrie-4.0-Strategie muss deswegen Cybersecurity hohe Priorität einräumen und Sicherheit ganzheitlich denken im Dreiklang von Technologie, Prozess und Mensch. Statische Sicherheit nach dem bisherigen Prinzip „Security as a Function“, das alleine auf der technischen Ebene ansetzt, reicht bei weitem nicht mehr aus.

Neben immer ausgefeilteren Cyberattacken durch professionelle Hacker gibt es auch die wachsende Bedrohung durch Innentäter. Konkrete Zahlen gibt es nicht, aber die Art der Angriffe lässt Rückschlüsse auf Insiderwissen zu, etwa bei Denial-of-Service-Attacken auf nur intern bekannte IP-Adressen. Diese Entwicklung ist nur ein Grund, die Sicherheitsstruktur gemäß „Zero Trust“ umzubauen. Das Konzept ist ein Paradigmenwechsel, denn es macht keinen Unterschied zwischen Nutzern, Geräten oder Diensten innerhalb und außerhalb des eigenen Netzwerks. Es vertraut prinzipiell keinem, prüft den kompletten Datenverkehr und alle Beteiligten müssen sich authentifizieren.

IT-Sicherheitsgesetz 2.0 stellt neue Anforderungen

Angesichts der steigenden Zahl an Cyberattacken stellt sich mittlerweile nicht mehr die Frage „ob“ ein Unternehmen angegriffen wird, sondern „wann“. Ohne Vorkehrungen bleiben Kriminelle in Netzwerken oft zu lange unbemerkt. Das neue IT-Sicherheitsgesetz 2.0 legt deswegen den Schwerpunkt auf die Angriffserkennung und erhöht die Kompetenzen des Bundesamtes für Sicherheit in der Informationstechnik (BSI), damit es Sicherheitslücken detektieren und Cyberangriffe abwehren kann. Betreiber von Kritischen Infrastrukturen (Kritis) müssen in der Lage sein, einen Angriff mit geeigneten Technologien zu erkennen. Dafür brauchen sie ein Monitoringsystem, wie SIEM (Security Information und Event Management), das mithilfe Künstlicher Intelligenz potenzielle Bedrohungen identifiziert, um schnell reagieren zu können. OT-Systeme sind allerdings noch nicht auf aktive Monitoring-Tools ausgelegt und fahren sich herunter, wenn die Anwendung zu scharf eingestellt ist. Im Sinne der Sicherheit lassen sich die Mauern zwar unendlich hoch ziehen, doch wenn Mensch und Maschine dann nicht mehr arbeiten können, ist auch nichts gewonnen. Ein ganzheitliches Sicherheitssystem hält deswegen die Waage zwischen Security und Usability.

Auf „Security by Design“ setzen

Um das Thema Sicherheit effektiv umzusetzen, fehlen Unternehmen oft die personellen Kapazitäten oder das qualitative Know-how. Schließen lässt sich diese Lücke durch die Automation der Sicherheit. Dabei verändert sich der Blickwinkel: weg von „Security by Function“ hin zum ganzheitlichen „Security by Design“. Dieses Prinzip integriert Sicherheit zusätzlich in schriftlich definierten Prozessen, zum Beispiel zur Risikoanalyse oder Qualitätssicherung, und bildet Rollen, Verantwortlichkeiten und Tätigkeiten innerhalb der Organisation sowie die benötigten Technologien ab. Das setzt von Anfang an ein durchdachtes Sicherheitskonzept voraus, das ausgehend von der Aufgabe der Technik unter anderem die Voraussetzungen für die prozesskonforme Anwendung durch die Nutzer analysiert. Zero Trust drückt sich an dieser Stelle darin aus, dass beispielsweise von Herstellern implementierte Standardprotokolle abgeschaltet werden, wenn sie für die eigentliche Aufgabenerfüllung nicht notwendig sind.

Nicht jede Gefahr ist offensichtlich. Um Cyberkriminellen den Weg ins Unternehmen zu versperren, ist es wichtig, sich möglicher Hacking-Tools bewusst zu sein. So harmlose Gegenstände, wie die auf Messen in großer Zahl als Giveaways verschenkten USB-Sticks oder von Kunden mitgebrachte externen Festplatten, können Viren oder Schadsoftware auf das Netzwerk übertragen. Zero Trust kann auch in diesem Fall gravierende Schäden oder Datenverluste verhindern, indem grundsätzlich jeder mobile Datenträger eine Datenschleuse, wie Index, durchlaufen muss. Erst wenn der Unternehmensrechner einen erfolgreichen Scan erkennt, erlaubt er den gefahrlosen Anschluss.

Jede Cybersecurity-Strategie ist nur so gut, wie ihr schwächstes Glied. Im ganzheitlichen Dreiklang sind das nicht die Technologien und Prozesse, sondern der Mensch. Cyberkriminelle machen sich das zunutze. Sie erzeugen Stresssituationen geschickt über Gefühle, wie Empathie oder Angst, um leichter an Informationen zu gelangen. Regelmäßige Awareness-Trainings könnten die Aufmerksamkeit gegenüber dieser Gefahr hochhalten, allerdings vernachlässigen viele Unternehmen es sträflich, ihre Mitarbeiter entsprechend zu schulen. Die Führungsebene ist hier in der Verantwortung: Cybersecurity ist Chefsache! Und je durchlässiger die Trennlinie zwischen IT und OT in der Industrie 4.0 wird, desto wichtiger wird ein zeitgemäßer Schutz gegen Cyberkriminalität gemäß dem Motto: Zero Trust! ■

telent GmbH:
www.telent.de