Zero Trust bringt Sicherheit an jeder einzelnen Schnittstelle

Wie ein konsequentes Security-Konzept industrielle Netze vor Angriffen auf IIoT- und OT-Geräte schützt.

Autor:
Stefan Schachinger
Product Manager Network Security
Barracuda Networks
www.barracuda.com

Im letzten Jahr hatten weltweit 90 Prozent der Unternehmen einen Sicherheitsvorfall (Barracuda Marktreport The State of Industrial Security in 2022). Mit der fortschreitenden technologischen Entwicklung nimmt die Zahl der IIoT-Geräte, die mit dem internen Netzwerk oder direkt mit dem Internet verbunden sind, zu. Dadurch wächst die Angriffsfläche für Ransomware-Attacken mit oft verheerenden Folgen. In einer Welt, in der ein einziger Angriff den Geschäftsbetrieb lähmen oder sogar vollständig unterbrechen kann, müssen Unternehmen der IIoT- und OT-Sicherheit Priorität einräumen, um ihre Anlagen wirkungsvoll zu schützen. Das geht, wenn Zero Trust als Sicherheitskonzept in allen Schnittstellen des Unternehmens implementiert wird.

Bis vor wenigen Jahren ist man mit dem Grundsatz des „Trusted Network" innerhalb des Unternehmens noch ordentlich zurechtgekommen: Herkömmliche Firewalls schützten das Firmennetz nach außen, intern wurde meist „vertrauensvoll" geschaltet und gewaltet, ohne dass es dort noch weitere besonders ausgeklügelte Schutz- und Kontrollfunktionen gegeben hätte. Mit der Digitalisierung und Vernetzung von Prozessen, Anlagen und Maschinen hat in der Industrie jedoch ein Paradigmenwechsel stattgefunden, der ein grundlegend anders Sicherheitskonzept erfordert: Intelligente Systeme verbinden heutzutage alle Komponenten einer Produktionskette miteinander und reagieren auf Produktanforderungen, was wiederum die Optimierung von Lieferketten und Produktionsnetzen in Echtzeit ermöglicht. Die zunehmende Konnektivität von Steuerungssystemen, Sensoren, Maschinen und mehr hat dazu geführt, dass ehemals isolierte Systeme den Gefahren des Internets ausgesetzt sind.

„Unsichere Geräte"

Geräte, die früher als „konstruktionsbedingt sicher" galten oder einfach nicht „wert" waren, gehackt zu werden, sind damit für Angreifer sehr viel attraktiver geworden. Damit haben die Unternehmen ein Problem, denn der Austausch solcher Geräte durch neuere und sicherere Modelle ist für sie meist keine realistische Option, oft ganz einfach deshalb, weil viel zu viele davon im Einsatz sind. Auch eine Aktualisierung der Gerätefirmware ist selten möglich. Deshalb planen die meisten Organisationen inzwischen IIoT/OT-Sicherheitsprojekte - oder setzen sie bereits um, wobei Großunternehmen gegenüber kleineren Unternehmen die Nase vorn haben. Die größten Probleme treten für größere und kleinere Firmen gleichermaßen bei Fragen rund um Konnektivität und Skalierbarkeit auf.

Zero Trust

gilt inzwischen als einer der wichtigsten Sicherheitsbegriffe der Gegenwart. Dabei geht es um die Daten und um die Implementierung von Sicherheitskontrollen, die diese schützen. Anstelle von bedingungslosem Vertrauen und uneingeschränkten Zugriffen – also der gelebten Realität in vielen Unternehmen – sollen Benutzer und Geräte kontinuierlich überprüft und deren

Aktivitäten im Netzwerk auf das Nötige reduziert werden. Cyberattacken wie Colonial Pipeline und JBS haben gezeigt, wie schädlich Angriffe auf die operative Technologie der Unternehmensinfrastruktur sein können. Attacken auf OT-Netzwerke schaden nicht nur dem Ruf und den Finanzen, sie können auch reale physische Schäden an Maschinen verursachen - mit spürbaren und unter Umständen gefährlichen Auswirkungen.

Schutz der Infrastruktur durch Mikrosegmentierung

Das Konzept Zero Trust kann hier mit einer Reihe von Maßnahmen Abhilfe schaffen. Der erste Schritt in industriellen Netzwerken ist die Adressierung der schwerwiegendsten Schwachstellen. Die Ergebnisse der genannten Studie zeigen deutlich, dass fehlende Segmentierung und unsichere Fernwartungszugänge zu den größten Problemfeldern gehören. Zero Trust bedeutet auch, dass eine Segmentierung von Funktionen in getrennte Zonen wie beispielsweise die Trennung zwischen dem Manufacturing Execution System (MES), der Mensch-Maschine-Schnittstelle (HMI) und der speicherprogrammierbaren Steuerung (SPS) dabei hilft, den Netzwerkverkehr zwischen den Zonen auf ein Minimum zu beschränken und bösartige Aktivitäten zu verhindern. Im Katastrophenfall lassen sich dadurch Bedrohungen leichter erkennen, eindämmen und bekämpfen.

Mikrosegmentierung ist die beste Methode, um die Auswirkungen eines Vorfalls abzuschwächen. Die Isolierung potenziell gefährdeter Netzwerkgeräte und die Beschränkung des legitimen Netzwerkverkehrs sind unerlässlich, um die interne Ausbreitung zu verhindern, wenn ein Angriff die Infrastruktur trifft. Dies beinhaltet die Implementierung einer Segmentierung zwischen IT und OT und die Einführung einer zusätzlichen Segmentierung (Mikrosegmentierung) im OT-Netz, die den bestmöglichen Schutz bietet, indem sie jedes einzelne Gerät oder kleine Gruppen von Geräten isoliert.

Angreifer ausbremsen und Fernzugriffe absichern

Das Aufteilen des Netzwerks in kleinere Abschnitte hat eine Reihe von Vorteilen, davon zwei besonders wichtige: Cyberkriminelle, die sich Zugang zu einem Bereich in einem segmentierten Netzwerk verschaffen, haben es so wesentlich schwerer, in das restliche Netzwerk einzudringen. Zudem es ist einfacher, sie aufzuspüren und in ihrem Tun zu stoppen beziehungsweise den Schaden zu begrenzen. Damit sparen die Unternehmen bei der Beseitigung der Folgen solcher Schäden viel Zeit und Geld. Als angenehmer Nebeneffekt wird zudem die allgemeine Datensicherheit erhöht, da die Trennung zwischen den Zonen das Risiko von Datendiebstahl oder -zerstörung verringert. Denn Cyberkriminelle haben nur in Hollywood-Firmen den sportlichen Ehrgeiz, möglichst trickreich die kompliziertesten Absicherungen zu umgehen. Im echten Leben nehmen sie den Weg des geringsten Widerstands, auch bei gezielten Angriffen.

Sicherer, temporärer VPN-Zugang

Der Fernzugriff bleibt nach der Pandemie ebenfalls ein wichtiges Thema, da viele Unternehmen immer noch aus dem Homeoffice beziehungsweise remote arbeiten oder externe Servicepartner und Maschinenhersteller für die Fernwartung und Fehlerbehebung einbinden lassen. Speziell in OT-Umgebungen ist eben diese Funktionalität allerdings der größte Bedrohungsvektor. Mit Firewall-Lösungen der neuesten Generation können Benutzer bei Bedarf problemlos einen sicheren, temporären VPN-Zugang zu verschiedenen Teilen des Netzwerks gewähren. Um die potenzielle Angriffsoberfläche so weit wie möglich zu reduzieren, können Zero-Trust-Network-Access-Lösungen einen bedingten Zugang nur zu bestimmten Anwendungen ermöglichen.

Benutzerfreundlichkeit

Ein weiterer entscheidender Faktor für den wirksamen Schutz ist neben der Technologie die Benutzerfreundlichkeit: Ein zuverlässiges Access-Sicherheitssystem muss auf allen Ebenen von allen Beteiligten ohne großen Aufwand gelebt werden können. Hilfreich ist dabei eine nachvollziehbare Zugriffskontrolle für sämtliche Anwender und Geräte – egal ob hybrid oder extern, ob firmeneigene Geräte oder jene von Mitarbeitern und Auftraggebern: Wer macht wo wie was wann und warum? Ein rollenbasierter Zugriff auf alle Applikationen und Daten im Unternehmen reduziert außerdem die Risiken, die mit Zugriffen durch Dritte auf das Unternehmen verbunden sind, und ermöglicht Transparenz bei allen Aktivitäten. Damit lassen sich der SOC-2-Standard und andere Compliance-Anforderungen ohne Mehraufwand einhalten. Dass sich damit außerdem noch Phishing-Angriffe und andere Bedrohungen auch von Mobilgeräten und Smartphones ohne die Installation zusätzlicher Software abwehren lassen, ist ein zusätzliches stichhaltiges Argument, das bei einem überzeugenden Zero-Trust-Konzept ebenfalls von Bedeutung ist.

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. ◄