Quelle: TXOne Networks

Gebäudeautomationssysteme vor Cyberangriffen schützen

Vier Maßnahmen gegen das Hacken smarter Gebäude

Von Rechenzentren und Krankenhäusern bis hin zu Hotels, Bürogebäuden und Wohnhäusern – eine Gebäudeautomation kann die Energieeffizienz, die Sicherheit und den Komfort öffentlicher und privater Immobilien verbessern. Deren Nutzer erwarten stets eine gute Luftqualität, angenehme Temperaturen, angemessene Beleuchtung und die nötige Sicherheit. Moderne Gebäudeautomationssysteme können diese Erwartungen erfüllen. Da diese Systeme jedoch mit dem Internet sowie untereinander in Netzwerken verbunden sind, sind sie besonders anfällig für Cyberangriffe.

Wie man Gebäudeautomationssysteme (englisch: Building Automation Systems, kurz: BAS) vor Cybercrime schützen kann, hat der Operational-Technology-Cybersicherheitsspezialist TXOne Networks in einem Whitepaper (siehe **Kasten**) zusammengefasst. Das Unternehmen mit Hauptsitz in Taiwan hat vier Eckpfeiler für die Absicherung von Gebäudeautomationssystemen identifiziert – basierend auf seinem eigenen Ansatz »OT-Zerotrust« und getreu seinem Motto: »never trust, always verify« (vertraue niemals, überprüfe immer).

Gefahren bei der Gebäudeautomation

BAS-Angriffe ähneln den Angriffen auf industrielle Kontrollsysteme (ICS), aber es gibt einige wichtige Unterschiede. Wie ICS-Lösungen sind auch Gebäudeautomationssysteme anfällig für die Einbringung von Schadsoftware und die Beschädigung von Speichern, wenn ihr Code nicht ausreichend gesichert ist.

Clevere Angreifer können etwa aus einem Raspberry-Pi-Computer einen Temperatursensor basteln und mit Schadsoftware versehen zum Einsatz bringen oder einen ungesicherten UDP-Port auf einem Gerät finden, das noch das Standardpasswort verwendet. Die meisten Angriffe auf ICS-Systeme beginnen damit, dass ein Mitarbeiter selber die Cyberbedrohung an den Arbeitsplatz einschleppt oder die IT-seitigen Abwehrmaßnahmen versagen.

Angreifer können theoretisch sogar in das BAS-Netzwerk eindringen ohne Phishing-E-Mails verfassen zu müssen, da die Suche in IoT-Suchmaschinen wie »Shodan« oder »Censys« Hunderttausende von IoT-Geräten mit bekannten Schwachstellen offenbart. Ein raffinierter Hacker könnte auf Basis der Suchergebnisse ein Skript schreiben und die Such-

resultate so dafür verwenden, Malware auf jedes einzelne Gerät auf der Liste zu laden.

Ein weiterer Unterschied zu ICS-Lösungen besteht darin, dass die physischen Prozesse zur Wartung eines Gebäudes weit weniger kompliziert sind als die zur Kontrolle industrieller Produktionsanlagen. Denn um die Industrieproduktion nachhaltig zu stören, muss Malware sowohl die Sicherheitsmaßnahmen als auch die Zeitabläufe und die jeweilige IT-Umgebung berücksichtigen, welche in der Regel reglementierter und besser geschützt sind als bei einem BAS.

Vier Hauptbestandteile zur Absicherung von Gebäudeautomationssystemen

Die Hauptaufgabe von Gebäudeautomationssystemen besteht darin, ein angenehmes Wohn- und Arbeitsklima zu schaffen. Ohne Sicherheitskontrollen könnte ein Hacker jedoch das Wohnhaus, Hotel, Krankenhaus, Rechenzentrum, die Sportarena oder sogar die dort verwendeten cloudbasierten Systeme angreifen und schädigen. Der »OTZerotrust«-Ansatz von TXOne Networks beruht auf vier Eckpfeilern für die Cybersicherheit von Gebäudeautomationssystemen: prüfen, sperren, segmentieren und stärken.

1. Prüfen

Jedes digitale Gerät, das Teil des Gebäudeautomationssystems ist, sollte eine Prüfung durchlaufen. Die häufigste Art und Weise, wie Malware in das BAS eines Unternehmens gelangt, ist, dass vertrauenswürdige Personen sie entweder absichtlich oder versehentlich einschleppen. Unternehmen benötigen außerdem einen Prozess zur Identifizierung und Bearbeitung von Sicherheitsrisiken für alle extern erworbenen Komponenten. Dies kann mithilfe automatisierter Tools zur Überwachung und Verfolgung von Schwachstellen geschehen. Mit einem mobilen Sicherheitsscanner kann ein Unternehmen beispielsweise Malware aufspüren und außer Gefecht setzen, bevor das infizierte Endgerät im BAS in Betrieb genommen wird.

2. Sperren

Sperrlisten helfen dabei, die Verwendung bestimmter Endgeräte und den Netzwerkverkehr zu reglementieren und damit die Sicherheit zu verbessern. Diese Listen passen sich den aktuellen Gegebenheiten bzw. der Bedrohungslage an und bewerten die Vertrauenswürdigkeit von Endgeräten und Netzwerkverbindungen in jeder Situation. Dabei kann es sich um eine einfache Trust-List handeln, wie sie von fest installierten Endgeräten verwendet wird, oder um eine sogenannte Trust-Library mit gängigen OT-(Operational Technology)-, BAS- oder ICS-Anwendungen und Zertifikaten.

Noch besser funktioniert die Abschirmung bedrohter BAS-Lösungen mithilfe einer weiteren Schutzebene in Form von Funktionen maschinellen Lernens, die verdächtige Cyberaktivitäten erkennen können, ohne dass die unkritischen Prozesse der Trust-List unterbrochen werden müssen. Auf der Netzwerkebene können so Steuerbefehle und andere Nachrichten mittels Sicherheitszonen auf einer »Need-to-know«-Basis weitergeleitet werden – jegliche andere Kommunikation wird blockiert.

Um bestimmte Steuerbefehle zu blockieren, ist eine OT-native Anwendung erforderlich, die BAS-Protokolle wie Bacnet versteht, und Hacker daran hindert, schädliche Befehle zu senden – und zwar sowohl durch die strikte Einschränkung von Privilegien als auch durch die Festlegung, dass verdächtige oder ungewöhnliche Steuerbefehle standardmäßig blockiert werden.

Dieser Ansatz funktioniert am besten im Rahmen einer Netzwerksegmentierung, bei der diese Privilegien so definiert werden können, dass sie den speziellen Anforderungen der einzelnen BAS gerecht werden. Für die Absicherung von BAS-Lösungen ist es von entscheidender Bedeutung, dass die spezifischen Anforderungen jedes einzelnen Endpunkts berücksichtigt werden, d. h. sowohl die Bedürfnisse von Bestandssystemen für Routineaufgaben als auch von modernen Assets (Geräten), die eine Vielzahl verschiedener Aufgaben ausführen.

3. Segmentieren

Wenn das Netzwerk in einzelne Zonen aufgeteilt ist, vereinfacht das die Verteidigung gegen Cyberangriffe. Zur weiteren Verbesserung der Netzwerksegmentierung und zur Sicherstellung eines umfassenden Schutzes ist es jedoch ratsam, das Konzept der »Zonen« und »Conduits« zu übernehmen, wie es in der Norm IEC 62443 zur IT-Sicherheit industrieller Kommunikationsnetze beschrieben ist. Eine »Sicherheitszone« umfasst dabei eine Gruppe von physischen oder logischen Assets mit gemeinsamen IT-Sicherheitsanforderungen und definierten Grenzen.

Die digitalen Verbindungen zwischen diesen Zonen, die sogenannten »Conduits«, eine Art Brücken, sollten mit Sicherheitsmaßnahmen ausgestattet sein, um den Zugang zu kontrollieren, Denial-of-Service-Angriffe zu verhindern, anfällige Systeme im Netzwerk abzuschirmen sowie die Integrität und Vertraulichkeit der Kommunikation zu wahren. OT-native Protokollrichtlinien helfen dabei, zugelassene IT-Befehle festzulegen, und IP-basierte Richtlinien können bestimmen, welche Assets miteinander kommunizieren dürfen.

Die grundlegenden Werkzeuge der Netzwerksegmentierung sind das OT-»Intrusion Prevention System« (IPS) und die OT-Firewall-Anwendungen. Ein OT-IPS der nächsten Generation kann kritische BAS in Mikrosegmente oder Gruppen von Assets unterteilen, die einen 1-zu-1-Schutz erfordern. Firewalls der nächsten Generation schaffen eine transparente Segmentierung und verwenden eine breitere Definition von Netzwerksicherheitsrichtlinien.

Anwenderfreundliche »OT-native« IPS und Firewalls können transparent und ohne Änderungen an der bestehenden BAS-Architektur eingesetzt werden. Vertrauenslisten können sowohl auf der Netzwerk- als auch auf der Protokollebene festgelegt werden. Die Netzwerksegmentierung hilft dabei, anfällige IT-Assets in einer sicheren Zone zu isolieren, die leichter von Zero-Day-Angriffen und an-

deren gefährlichen Cyberbedrohungen freigehalten werden kann.

In manchen Fällen spielen Assets eine so wichtige Rolle im Systemaufbau, dass sie niemals vom Netz genommen werden können. Die Netzwerksegmentierung mit »OTZerotrust«-basierten Richtlinien verhindert, dass Angreifer sich innerhalb eines Netzwerks bewegen können, um diese hochgefährdeten Assets zu erreichen.

4. Stärken

Die Stärkung der Cybersicherheit hängt von vielen Faktoren ab: Ist ein Sicherheits-Patch verfügbar und kompatibel? Erlaubt die OT-Umgebung, dass das Asset gepatcht werden kann?

Der Status des Assets und der Patch-Status sind konstante Faktoren im Wartungsprozess. Mit virtuellen Patches werden Assets geschützt, ohne dass Änderungen an ihren Konfigurationen vorgenommen werden müssen – und das unabhängig davon, ob der Hersteller ein Sicherheits-Update veröffentlicht hat. IT-Techniker verwenden virtuelle Patches, um Risiken zu verringern, bis der richtige Zeitpunkt für ein Update und einen vom Hersteller bereitgestellten Patch gekommen ist.

Die OT-nativen IPS und Firewalls, die diese Art der Asset-zentrierten Cyberabwehr ermöglichen, verfügen über standardisierte Regelsätze, die speziell für die Abwehr von Cyberangriffen entwickelt wurden, ohne dass die Endgeräte unbedingt ein Update durchführen müssen. So fallen Systemneustarts und Produktionsausfallzeiten weg.

Empfehlungen zur Absicherung der Gebäudeautomation in drei Schritten

Durch die Absicherung von Gebäudeautomationssystemen mit dem »OTZerotrust«-Ansatz werden Gebäude komfortabler, energieeffizienter und sicherer. Der erste Schritt ist eine sichere Lieferkette: Unternehmen sollten von ihren Partnern in der gesamten Lieferkette die Einhaltung eines angemessenen Sicherheitsniveaus verlangen. Sie sollten ihre IT-Sicherheitsanforderungen in ihre Geschäftsbedingungen integrieren und IT-Anbieter auf potenzielle Schutzlücken prüfen.

Außerdem benötigen sie ein Verfahren zur Ermittlung und Verwaltung von Sicherheitsrisiken für alle extern erworbenen Komponenten. Dies kann mithilfe automatisierter IT-Tools zur Überwachung und Verfolgung von Bedrohungen und Schwachstellen geschehen.

Wie Angriffe auf Smart Buildings abgewehrt werden können

Das 18 Seiten umfassende Whitepaper »Hacking Smart Buildings« kann in englischer Sprache auf der Homepage von TXOne Networks als kostenloses PDF heruntergeladen werden. Es ist unter folgendem Link zu finden: https://www.txone.com/white-papers/hacking-smart-buildings-iot-attack-surfaces-and-defenses/.

In einem zweiten Schritt sollte eine »OTZerotrust«-Architektur zum Einsatz kommen. In Zukunft werden immer mehr Internet-of-Things-Geräte in intelligenten Gebäuden verwendet. Unternehmen können sich in Bezug auf deren IT-Sicherheit an den vier genannten Eckpfeilern orientieren: prüfen, sperren, segmentieren und stärken. »OTZerotrust« spielt dabei die Rolle des »Cybersicherheits-Ghostbusters« für Gebäudeautomationssysteme. Dies erspart Gebäudetechnikern eine Menge Entwicklungszeit und das Aneignen teuren sicherheitstechnischen Fachwissens.

Der dritte Schritt betrifft den lebenslangen Schutz von Operational-Technology-Endpunkten. OT-Endpunkte in intelligenten Gebäuden müssen über 20 Jahre lang genutzt werden, sodass für das Cybersicherheitsteam die Verwaltung älterer Endpunkte und Systeme zur neuen Norm wird. Wenn kein langfristiger Cyberschutz der Assets geplant ist, werden ernsthafte Sicherheitsprobleme entstehen. Zur Unterstützung des lebenslangen Schutzes von Endpunkten ist ein ressourcenzentrierter Ansatz erforderlich, der die Endpunktanwendungen schützt, legitime Prozesse überwacht und schädliche Programme daran hindert, Amok zu laufen.

FÜR SCHNELLLESER

Die meisten Cyberangriffe werden durch Mitarbeiter oder versagende IT-seitige Abwehrmaßnahmen verursacht

Die vier Eckpfeiler für die Cybersicherheit von Gebäudeautomationssystemen sind: prüfen, sperren, segmentieren und stärken

OT-Endpunkte in intelligenten Gebäuden benötigen einen lebenslangen Schutz

Autor:
Dmitri Belotchkine, Technical Director Europe bei TXOne Networks, Taipeh, Taiwan