tenable.ot™
Powered by Indegy

Absicherung von Gebäudemanagementsystemen

WICHTIGSTE TRENDS

- Zunehmende Verbreitung von automatisierten Kontrollsystemen zur Steuerung mechanischer Anlagen (wie etwa Elektrik, Belüftung, Beleuchtung, Strom, Brandschutz, Sicherheit)
- Entstehung von Gesetzen und Initiativen zur Förderung der Entwicklung und Einführung von GMS-Technologien
- Zunehmende Konvergenz von IT und OT und damit verbundene Akzeptanz
- Erhöhte Konnektivität von geregelten Systemen, die extern zugänglich sind

ZENTRALE HERAUSFORDERUNGEN

- Sicheres Design ist kein evolutionärer Bestandteil von GMS.
- Öffentlich verfügbare Standardprotokolle können für destruktive Steuerbefehle missbraucht werden.
- Mit GMS verwaltete Gebäude werden häufig von großen Menschenmengen und nicht überprüften Besuchern frequentiert. Dieser physische Zugang könnte für böswillige Zwecke und Manipulation missbraucht werden.
- GMS erfordern eine Vernetzung von Controllern und IO-Geräten an vielen verschiedenen Orten, sodass die Abschottung der einzelnen Systeme („Air-Gapping“) nahezu unmöglich ist.

HINTERGRUND

In Gebäuden kommt immer mehr intelligente Technik zum Einsatz. Von der Zugangskontrolle über Brandschutz, Klimatisierung, Beleuchtung und Luftfeuchtigkeitsregelung: Alles lässt sich zentral steuern und optimieren, um den Anforderungen von spezifischen Gebäuden und einzelnen Mitarbeitern bestmöglich Rechnung zu tragen. Die Systeme, die dies erst möglich machen, werden als Gebäudemanagementsysteme (GMS) bezeichnet. GMS senken die Energie- und Wartungskosten von Gebäuden. Zudem reduzieren sie den ökologischen Fußabdruck und erhöhen die Sicherheit der Gebäudenutzer und des darin befindlichen Sachvermögens. Die heute gängigen GMS haben signifikante und komplexe Veränderungen durchlaufen. Noch vor einem Jahrzehnt regelte GMS-Technik lediglich Heizung, Lüftung und Klimaanlage und vielleicht noch ein physisches Sicherheitssystem. Heute hingegen steuern GMS praktisch jeden Teilaspekt intelligenter Gebäude. Da intelligente Technologien erhebliche Effizienzsteigerungen und Kosteneinsparungen bieten, erfreuen sie sich immer größerer Akzeptanz.

Somit ist auch zu erwarten, dass Risiken in geometrischem Verhältnis zunehmen, da immer mehr Gebäude „intelligent“ werden, mehr Infrastrukturen konvergieren und das IoT sich zum De-facto-Standard von GMS entwickelt. Data Bridge Market Research zufolge belief sich der Weltmarkt für Gebäudemanagementsysteme im Jahr 2016 auf einen Gesamtwert von 54,0 Milliarden USD[1]. Während des Prognosezeitraums von 2019 bis 2026 wird er eine durchschnittliche jährliche Wachstumsrate (CAGR) von 11,0 % aufweisen. Auch wenn GMS riesige Vorteile versprechen, können sie sich im Hinblick auf optimierte Prozesse und sinkende Kosten als ebenso nachteilig erweisen, wenn Sicherheit im Rahmen von Bereitstellung und Management außer Acht gelassen wird.

[1] Data Bridge Market Research, 24. April 2019

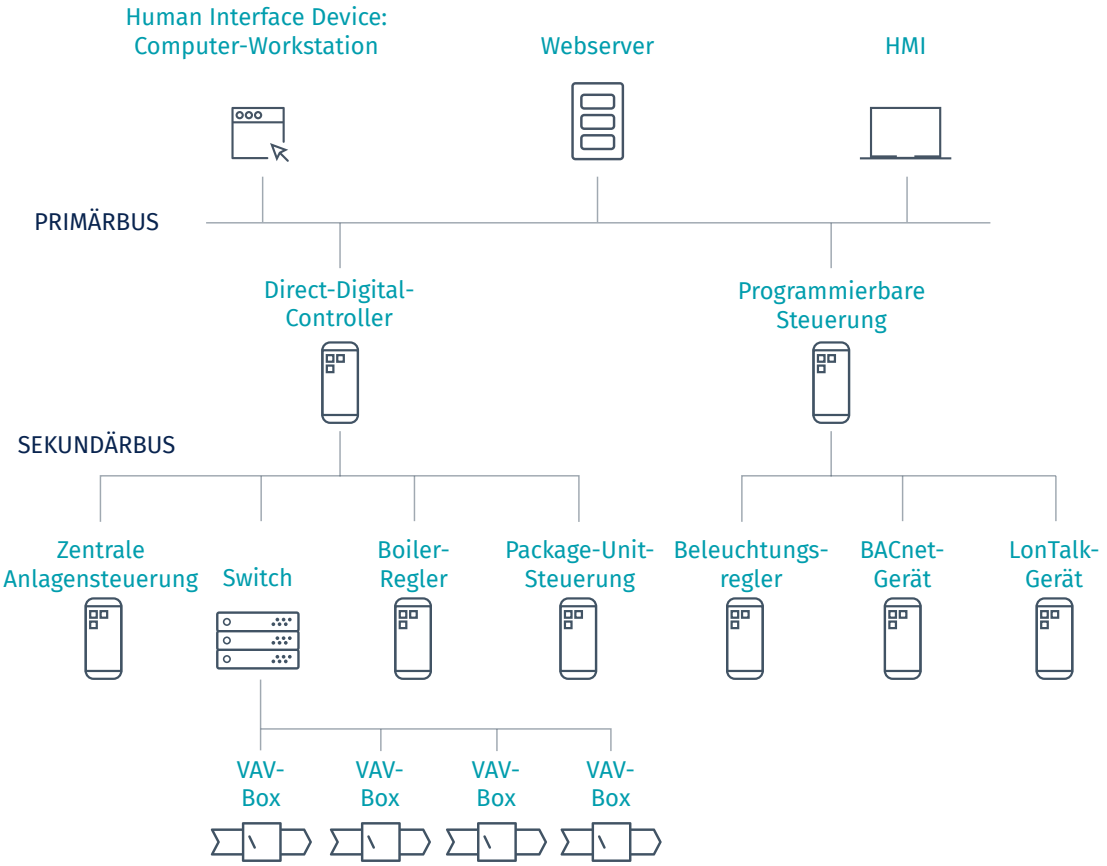
ANATOMIE EINES CYBERANGRIFFS AUF GMS

- Anfängliches physisches oder virtuelles Eindringen in das GMS-Netzwerk
- Errichtung eines Brückenkopfes in einem der Assets des Netzwerks
- Auskundschaftung zwecks Bestimmung von Zielen und anfälligen Geräten oder Systemen
- Ausbreitung auf andere Assets, um in andere Bereiche von Interesse zu gelangen
- Abschluss der „letzten Meile“ des Angriffs, in der Gebäudesysteme gestört werden

Kürzliche Ereignisse[2]

- **Dezember 2018** – Das FBI warnte, dass nicht gepatchte Geräte in GMS-Netzwerken Hackern ausgesetzt sind, die Schwachstellen in dem in GMS-Systemen gängigen FOX-Protokoll ausnutzen.
- **2014** – Ein Hacker verschaffte sich unbefugt Zugriff auf die Gebäudeleittechnik eines Fünf-Sterne-Hotels im chinesischen Shenzhen, um Raumregelungssysteme zu manipulieren und Kundendaten zu stehlen.
- **2013** – Filialen des Einzelhandelskonzerns Target wurden von Hackern angegriffen, die sich vom Parkplatz aus Zugang zum standorteigenen WLAN verschafften, das zur Kreditkartenabwicklung eingesetzt wurde. Dieser Übergriff gelang durch einen gezielten Angriff auf das HLK-System des Gebäudemanagementsystems.

STANDARDBEREITSTELLUNG VON GMS



[2] Search Security Tech Target

HÄUFIGE SCHWACHSTELLEN IN GMS

- Wie in vielen anderen Industriezweigen sind GMS-Protokolle nicht auf Sicherheit ausgelegt und lassen sich leichter ausnutzen. So weist beispielsweise das in einigen GMS angewendete FOX-Protokoll bekannte Schwachstellen auf. Eine Shodan-Abfrage identifizierte 20.000 Komponenten, die über Port 1911 direkt mit dem Internet verbunden sind.

- Da viele Systeme bereits älter sind, existiert keine geeignete Dokumentation zur Beseitigung von offenen Schwachstellen. Daher sind sie möglicherweise völlig ungepatcht, ohne dass neue Patches veröffentlicht werden. Da GMS heutzutage keine Air-Gapped-Systeme mehr sind, könnte eine besonders hohe Anfälligkeit für Angriffe vorliegen.

- Gebäude sind im Normalfall nicht nur für Mitarbeiter, sondern auch für ein breites, heterogenes Publikum zugänglich. Mangelhafte physische Sicherheitskontrollen könnten also dazu führen, dass unbefugte Personen Zugriff auf Gebäudesysteme erlangen, sobald sie sich Zutritt zum Gebäude verschafft haben.

- Durch die weitverbreitete Akzeptanz des IoT und der Konvergenz von IT und OT ist das mit Air-Gapped-Systemen verbundene Maß an Sicherheit immer weniger präsent, da alles online und vollständig zugänglich ist.

Gängige Protokolle

- DeviceNet
- BACnet
- C-Bus
- Niagra FOX
- LonWorks
- XML
- Modbus

Tenable.ot™ nutzt patentierte[3] Technologien für aktive Abfragen und ist zudem die erste Lösung mit spezifischen Active Querying-Engines für GMS. Die Technologie setzt aktive Abfragen sowohl für Standard- als auch proprietäre Protokolle ein, um eine maximale Abdeckung aller Geräte im verteilten OT-Netzwerk zu gewährleisten.

PHYSISCHER ZUGANG

Im Gegensatz zu herkömmlichen IT-Netzwerken ist in Gebäuden ein breites, heterogenes Publikum anzutreffen. Bei einigen dieser Personen handelt es sich natürlich um entsprechend befugte Mitarbeiter. Viele andere dürften hingegen Besucher am Standort sein (wie etwa Zulieferer, Kunden, Wartungspersonal usw.). Die meisten Gebäude verfügen über physische Zugangsbeschränkungen. Sind diese jedoch erst einmal überwunden, könnten eingedrungene Personen leicht zugangsbeschränkte Bereiche des Gebäudes betreten – einschließlich solcher, in denen sich GMS-Systeme befinden. Eine Sicherheitslösung für GMS muss einzelne Geräte an sämtlichen Standorten regelmäßig abfragen und feststellen, ob per physischer Verbindung zum Gerät Änderungen vorgenommen wurden. Nur so kann physischen Bedrohungen oder Bedrohungen vor Ort wirksam begegnet werden. Dabei ist es außerdem wichtig, Server, Workstations, Netzwerkgeräte, Gateways und alle anderen Geräte abzufragen, die für den regulären Netzwerkbetrieb von kritischer Bedeutung sind.

INTELLIGENTE UND SICHERE GEBÄUDE

GMS-Netzwerke haben in der Regel eine heterogene Infrastruktur. Ein Multi-Vendor-Szenario ist daher allgemein die Norm, wobei unterschiedliche Systeme zur Steuerung der einzelnen Komponenten eingesetzt werden – von den Aufzugsbänken bis zur Solaranlage auf dem Dach. Auf einem eher verteilt angelegten Campus können viele verschiedene Geräte ein oder mehrere Gebäude steuern. Eine Lösung sollte daher mehrere Erfassungsmethoden nutzen können, um eine präzise Asset-Bestandsaufnahme in Echtzeit zu gewährleisten. Auf diese Weise kann der gesamte Satz von Produkten mehrerer Anbieter abgesichert werden, aus dem sich das GMS zusammensetzt. Hinzu kommt, dass auch inaktive Geräte berücksichtigt werden müssen, die nicht regelmäßig über das Netzwerk kommunizieren. Selbst wenn Assets nicht über das Netzwerk kommunizieren, besteht die Möglichkeit, dass sie auf einen Befehl reagieren. Umfassendes Wissen, einschließlich Einblick in sämtliche Gerätetypen, Revisionsnummern, Firmware-Versionen und Backplane-Informationen, ist unerlässlich. Tenable.ot kombinierte passive Technologien mit seiner patentierten Technologie für die aktive Abfrage von Geräten, damit neben der tatsächlichen Netzwerkaktivität auch spezifische Details zu den Geräten berücksichtigt werden, die Teil des Netzwerks sind.

[3] US-Patent 10261489 – April 2019

SCHWACHSTELLEN RECHTZEITIG AUFSPÜREN

GMS-Umgebungen enthalten häufig eine Mischung aus älteren Geräten, die für die Steuerung älterer Technologien zuständig sind, wie etwa Brandbekämpfungs- und physische Sicherheitssysteme. Parallel dazu gibt es Geräte, die im Zusammenhang mit neueren Technologien eingesetzt werden, wie etwa zur Dachbegrünung und bei sich adaptiv verdunkelnden Fenstern. In einer Multi-Vendor-Umgebung mit mehreren Gerätegenerationen kann es schwer sein, den Überblick über die verschiedenen Revisionsnummern der einzelnen Gerätetypen zu behalten. Ein aktuelles Patch-Management-Programm zum Schutz vor neu entdeckten Schwachstellen ist ebenso aufwändig. Wäre diese Aufgabe manuell zu erledigen, ginge sie mit erheblichem Zeitaufwand einher und wäre zudem anfällig für menschliche Fehler.

Um angemessene Sicherheit zu gewährleisten, müssen der Zustand und sämtliche Merkmale jedes Geräts genauestens bekannt sein. Zudem muss der spezifische Zustand von Geräten genau mit der verfügbaren Wissensdatenbank zu Schwachstellen verglichen werden, um falsch-positive Ergebnisse auszuschließen. Aufgrund der sich ständig ändernden Bedrohungsbedingungen sollten diese Informationen regelmäßig aktualisiert und mit neu aufgedeckten Schwachstellen abgeglichen werden. Mit Tenable.ot können Sie detaillierte Informationen zu Geräten abrufen (z. B. Modell, Firmware, Revisionsnummer, installierte Software, Seriennummer). Das daraus resultierende Patch-Management sorgt dafür, dass alle Geräte stets auf dem neuesten Stand sind.

ZUSAMMENFASSUNG

Industrielle Cybersecurity ist unverzichtbar, um viele der Kernrisiken auszuschalten, die mit den neuen Gegebenheiten in GMS-Umgebungen einhergehen. Lückenlose Transparenz über sämtliche operativen Assets, die die unzähligen GMS-Systeme eines Gebäudes oder Campus steuern, ist für die Eindämmung dieser Risiken unerlässlich. Dazu gehören Klimatisierungssysteme, Zugangskontrollen, Brandbekämpfungs-, Beleuchtungs- und physische Sicherheitssysteme sowie Aufzüge und weitere Geräte.

Tenable.ot nutzt sowohl passive Erkennung und als auch eine patentierte Technologie für aktive Abfragen, um Bedrohungen aller Art in Ihrem Netzwerk aufzuspüren. Darüber hinaus hat Tenable einen umfassenden Richtlinienmechanismus entwickelt, mit dessen Hilfe für das Netzwerkmanagement zuständige Teams Regeln erstellen können, die sich an die Abläufe des jeweiligen Netzwerks anpassen lassen. Tenable.ot nutzt beide Arten der Datenerfassung. Zusätzlich zum Richtlinienmechanismus werden flexible Bereitstellungsoptionen eingesetzt, damit Security-Teams sicherstellen können, dass Unternehmen ein Höchstmaß an Effizienz erreichen und dabei keine inakzeptablen Risiken eingehen.

ÜBER TENABLE

Tenable®, Inc. ist das Cyber Exposure-Unternehmen. Über 30.000 Unternehmen aus aller Welt verlassen sich auf Tenable, wenn es um die Erkennung und Minimierung von Cyberrisiken geht. Als Erfinder von Nessus® hat Tenable sein Know-how im Bereich des Schwachstellen-Managements erweitert, um die weltweit erste Plattform bereitzustellen, mit der jedes digitale Asset auf jeder beliebigen Computing-Plattform erkannt und abgesichert werden kann. Zu den Kunden von Tenable zählen mehr als die Hälfte derFortune 500-Unternehmen, mehr als 30 Prozent der Global 2000 sowie große Regierungsbehörden. Erfahren Sie mehr über uns auf **de.tenable.com**.