

IT-Sicherheit in der Gebäudeautomation

Gebäudeautomation – ein Angriffsziel für Hacker?

Vom harmlosen Schabernack über handfeste Erpressung bis zur digitalen Kriegsführung: Die Motive für Hacker sind ebenso vielfältig wie ihre Angriffsvektoren. Sogar Steuer- und Regeltechnik für Gebäude kann ins Visier von Cyber-Attacken geraten. Hier heißt es Vorsorge treffen.



Quelle: Johnson Controls

Metasys-Benutzeroberfläche: Realistische grafische Darstellungen ermöglichen einen schnellen und umfassenden Überblick über den Systemstatus und die installierten Komponenten.



Quelle: Johnson Controls

Metasys CGM09090: Der universelle Application Controller bietet hohen Installations- und Betriebskomfort bei maximaler Manipulationssicherheit.

„Ich will einen Keks!“ Schon 1969 sahen sich Nutzer von Mini-Computern mit Erpressungen konfrontiert. Ein erster Vorgänger heutiger Malware forderte die Eingabe der Wörter „cookie“ oder „oreo“, bevor er das Betriebssystem wieder freigab (Quelle: Wikipedia).

Moderne Erpressungs-Software wie Wannacry gibt sich allerdings nicht mit digitalen Süßwaren zufrieden. Sie verschlüsselt Daten auf dem befallenen Rechner und gibt diese erst nach Zahlung eines Lösegeldes wieder frei. Der dabei entstehende Schaden in einem Unternehmen ist mit durchschnittlich 40.500 € bei weitem höher als das durchschnittlich geforderte Lösegeld – etwa 3.700 € pro Angriff (Quelle: Dato, Kroker's LookIT).

Sogar politische Ziele werden mittlerweile mit Cyber-Attacken verfolgt: Im März 2017 forderte erstmals RanRan, eine Ransomware-Variante im Nahen Osten, anstelle von Geld die Erstellung einer Website gegen einen politischen Führer (Quelle: Security Insider). Noch alarmierender: Nach Angaben des Bundesamts für Sicherheit in der Informationstechnik (BSI) gingen in der zweiten Hälfte des vergangenen Jahres 157 Meldungen über IT-Sicherheitsvorfälle ein, die kritische Infrastrukturen betreffen (Quelle: Heise Online). 19 potenzielle Cyber-Angriffe zielten allein auf das deutsche Stromnetz (Quelle: FAZ). Der nordrhein-westfälische

Verfassungsschutz warnt zudem vor einer „neuen Qualität“: „Früher handelte es sich bei den Hacker-Attacken auf die kritische Infrastruktur vor allem um Spionageangriffe. Nun gibt es immer häufiger Sabotageangriffe“ (Quelle: FAZ).

Ganz gleich, ob nun geldgierige Kriminelle die Urheber eines Hacks sind oder ausländische Geheimdienste: Die Angreifer suchen sich immer die schwächste Stelle im Sicherheitsnetz des Opfers – und das kann auch die Gebäudeautomation sein.

Eine Virusinfektion in der Heizung?

Diese Idee scheint vielen nach wie vor ziemlich abwegig – sie ist es aber keineswegs. Bereits 2010 zeigte sich bei einer gezielten Sabotageaktion gegen das iranische Atomprogramm (Quelle: Wikipedia: Iranisches Atomprogramm), dass Steuer- und Regeltechnik durchaus anfällig für Malware sein kann.

Branchenspezifische, standardisierte Kleinstcomputer haben die früher üblichen proprietären Komponenten in der Gebäudeautomation längst verdrängt. Vernetzt über ebenfalls standardisierte Protokolle und Schnittstellen, beispielsweise BACnet, ModBus, LON oder KNX, bewältigen sie heute viele Mess-, Steuer- und Regelaufgaben. Die hohen Anforderungen an Betriebseffizienz und Verfügbarkeit haben dazu geführt, dass diese Systeme fernwartungsfähig sein müssen – und dazu braucht es Schnittstellen nach außen. Die Kommunikation läuft dann häufig über Protokolle, die auf Standard-Betriebssystemen basieren. Fortschrittlichere Systeme bieten geschlossene Datentunnel über VPN (Virtual Private Network).

Aufbau und Spezifikationen der eingesetzten Hard- und Software sind also auch für Hacker zugänglich, die aufgrund der rasanten



Der Autor

Dipl.-Ing. (FH) Karl Heinz Belser, Johnson Controls Systems & Service GmbH, Niederlassung Stuttgart

Innovation in der IT immer leistungsfähigere System für ihre Aktionen zur Verfügung haben. Je schneller das Angreifersystem – und je einfacher und kürzer das Passwort – desto wahrscheinlicher ist es, dass der Code allein durch das automatisierte Durchprobieren wahlloser Zeichenfolgen gefunden wird. Man spricht dann auch von einer Brute-Force-Attacke (siehe auch: Security Insider).

Den kurzen Innovationszyklen der Schattenbranche stehen vergleichsweise sehr lange Nutzungszeiträume der technischen Anlagen in den Gebäuden und der zugeordneten Gebäudeautomation gegenüber: Rechner und Software sind nicht selten zehn Jahre alt und älter, und die Komponenten der Automations- oder Feldebene haben oft mehr als 20 Betriebsjahre auf dem Buckel. Gerade gegen Ende der Nutzungsdauer steigen also die Sicherheitsdefizite des Zielsystems, bezogen auf den Angreifer.

Wo modernste Hacker-Technik auf Uralt-Systeme trifft, steigen also die Erfolgschancen für Eindringlinge. Und wer die Gebäudeautomation kontrolliert, kann auch die darunter liegenden Ebenen schnell außer Gefecht setzen. Rechenzentren funktionieren nun mal nicht ohne Kühlung – und Stromnetze nicht ohne Rechenzentren. Dies nur als kleines Beispiel für eine Kaskadierung von Bedrohungsszenarien. Auch hier gilt: kleine Ursache, große Wirkung.

Dynamische Sicherheitskonzepte mit Updates

Die gute Nachricht: Standardisierte Hard- und Software und vernetzte Systeme haben auch ihre Vorteile. Aufgrund sicherheitsrelevanter Ereignisse und neuer Bedrohungen werden von den Technologiegebern Patches bereitgestellt, die dann für eine Vielzahl ähnlicher Systeme einsetzbar sind. Je mehr sich die Gebäudeautomation der übrigen IT annähert, desto besser greifen hier wie dort bewährte Sicherheitsstrategien, die in gängigen Büronetzwerken längst Standard sind. An die Stelle eines einmal installierten, statischen Systems tritt eine permanent aktualisierte Umgebung, die über Updates dynamisch mit den Möglichkeiten potenzieller Angreifer Schritt hält.

Für die Kommunikation gibt es ebenfalls etablierte Schutzmaßnahmen gegen Hacker und Cracker. Sobald der Datenverkehr über das eigene Netzwerk hinausgeht oder eine Internet-Schnittstelle vorhanden ist, muss, auch in der Gebäudeautomation das verschlüsselte HTTPS-Protokoll eingesetzt werden. So wird verhindert, dass an der Datenübertragung beteiligte Netzwerkkomponenten wie Switches, Router oder Kommunikations-Server Anmeldeinformationen oder Passwörter einfach mitlesen oder manipulieren.

Genau wie im Büronetzwerk gilt bei der Gebäudeautomation: Benutzer- und Zugangsberechtigungen müssen individuell und nach einer festgelegten Hierarchie angelegt sein. „1234“ ist kein sicheres Passwort, das gilt natürlich genauso beim Zugriff auf die Heizungs- und Klimatechnik. Passwörter müssen eine gewisse Länge haben und aus Buchstaben, Zahlen und Sonderzeichen bestehen, sonst kann sie ein potenzieller Angreifer allein mit Durchprobieren in Sekunden knacken. Auch müssen Passwörter in regelmäßigen Zeitabständen diszipliniert geändert werden.

Cybersecurity auch in der Gebäudeautomation

Dass die Gebäudeautomation bei mangelnder Absicherung zum Einfallstor für digitale Angriffe werden kann, hat man bei Johnson Controls schon frühzeitig erkannt. Das Gebäudeautomationsystem Metasys z. B. wird mit jeder neuen Softwareversion in puncto Sicherheit konsequent weiterentwickelt. Nach dem Motto: lieber eine Sicherheitsebene zu viel als eine zu wenig,

ist verschlüsselte HTTPS-Kommunikation im Gebäudenetzwerk selbstverständlich. Die Kopplung und Benutzervalidierung erfolgen durch RADIUS-Server-Authentifizierung (Remote Authentication Dial-In User Service). Dabei bleiben die Benutzerdaten unsichtbar. Das System protokolliert alle wichtigen Ereignisse und Meldungen der einzelnen Automationsstationen. Daraus lassen sich Reports ableiten, mit denen der Administrator Sicherheitslücken aufspüren und schließen kann. Hierzu zählen nicht benötigte Ports oder inaktive und nicht mehr verwendete Benutzerkonten.

Kontinuierlicher Service härtet das System

Die Technik der Gebäudeautomation muss heute viel flexibler angelegt sein als noch vor zehn oder zwanzig Jahren. Ein umfassender und kontinuierlicher Service ist daher zum entscheidenden Sicherheitsfaktor geworden. Am Anfang steht bei Johnson Controls stets eine konsequente Analyse der internen und externen Bedrohungssituation. Gemeinsam mit dem Kunden wird dann ein individuelles und sicheres technisches Konzept erarbeitet, das wir schließlich umsetzen und kontinuierlich auf dem neuesten Stand halten. Damit bleibt man gegen Bedrohungen geschützt, die bei der Implementierung der Anlage noch gar nicht absehbar waren.

Es lohnt sich also, bei einem Gebäudeautomationssystem wie Metasys immer die jeweils aktuelle Software-Version einzusetzen. Das gilt genauso für die Betriebssysteme, die auf den übergeordneten Rechnern laufen: Auch hier sollten Sicherheits-Patches stets eingespielt werden. Natürlich funktioniert das nicht bei Versionen, die vom Hersteller nicht mehr gepflegt werden, z. B. bei Windows XP oder Windows Server 2003. Diese veralteten Betriebssysteme stellen immer eine Sicherheitslücke dar – im Büro wie in der Gebäudetechnik. Leider sind noch viele dieser Altsysteme im Einsatz, weil diese bei der Planung von Ersatzinvestitionen häufig übersehen werden. Sie laufen ja noch.

Selbst eine erfolgreiche Cyber-Attacke verliert ihre Schrecken, wenn das System aus einem aktuellen Backup schnell wieder neu aufgesetzt werden kann. Daher ist eine konsequente und vollständige Datensicherung auch in der Gebäudeautomation unabdingbar.

Hand in Hand mit der kontinuierlichen Härtung und Absicherung von Hard- und Software sollte die Schulung und Weiterbildung des Bedienpersonals gehen. Hier gilt es, neben reinen Handlungsempfehlungen vor allem die Achtsamkeit in puncto Computersicherheit zu schärfen. Hierzu zählt auch die Sensibilisierung, um z. B. Phishing-E-Mails zuverlässig zu erkennen. Nicht vernachlässigen sollte man zudem Sicherheitsgewerke wie Videosysteme und Zutrittskontrolle, die heute mit der Gebäudeautomation immer mehr zu einem funktionalen Gesamtsystem verschmelzen – und Kriminelle und Spione physikalisch außen vor halten.

Ist die Gebäudeautomation also ein potenzielles Angriffsziel für Hacker? In jedem Fall. Vernetzung und Standardisierung haben Erpressern und Geheimdiensten neue Angriffsvektoren beschert, die sie nutzen werden. Werden die Angreifer erfolgreich sein? Nur in sehr begrenztem Umfang. Und nur dann, wenn wir längst bekannte und fundamentale Sicherheitsgrundsätze außer Acht lassen. Zum Glück hat im Bereich der Gebäudeautomation schon länger ein Umdenken eingesetzt: Bewährte Security-Strategien der IT kommen auch bei vernetzten Heizungs- und Lüftungssteuerungen zum Einsatz. Die richtige Technik gibt es also. Wir müssen sie nur einsetzen.