6/2015

HLH

Lüftung/Klima
Heizung/Sanitär
Gebäudetechnik

Organ des VDI für Technische Gebäudeausrüstung

www.hlh.de

Springer VDI Verlag

Immer im Bilde

Das Internet macht auch vor der Gebäudeautomation nicht Halt. Am weitesten fortgeschritten sind diese Bemühungen heute vielleicht bei sogenannten Smart Grids, bei denen einzelne Verbraucher in Gebäuden intelligent über externe Steuersignale des Stromnetzbetreibers zu- und abgeschaltet werden, um Verbrauchsspitzen im Stromnetz zu minimieren oder sie zu verschieben.

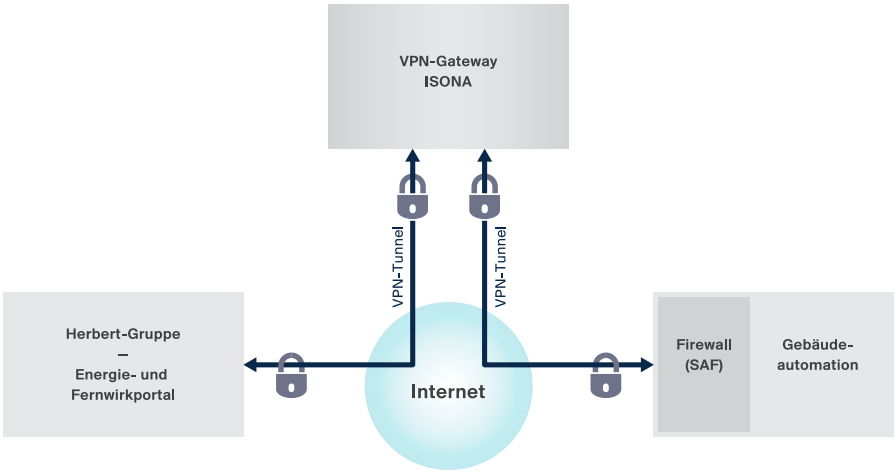


Bild 1

Die Anlagendaten werden per VPN-Verbindung übertragen. Über das Energie- und Fernwirkportal hat man damit Zugriff auf das aktuelle virtuelle Abbild der realen Daten. Diese Architektur schließt die Sicherheitsrisiken eines direkten Zugriffs auf die Anlage aus

Jede direkte Öffnung hausinterner Netzwerke und Kommunikationsinfrastrukturen, wie z. B. Bussysteme, birgt auch Gefahren, denn lokale Gebäudeautomationssysteme werden somit angreifbar und können manipuliert werden. Ursprünglich sind die in der Gebäudeautomation eingesetzten Systeme nicht für die Anbindung an das Internet oder IT-Infrastrukturen konzipiert worden, was erhebliche Sicherheitslücken bedingt. Das Thema IT-Sicherheit hat aber höchste Priorität, vor allem dort, wo es um hochverfügbare Industrieanlagen geht. Daher sind bei der Verbindung von Industrieanwendungen mit Internetdiensten Lösungen gefragt, die möglichen Cyber-Angriffen den Riegel vorschieben. Auch im privaten Bereich hört man immer mehr vom „Smart Home“, bei dem sich via Internet mit einer App Gewerke fernsteuern lassen, zum Beispiel, um die Heizung zu aktivieren, bevor man nach Hause kommt.

Ob Klimaanlagen, Kältemaschinen, Heizungen, Solarthermie oder BHKW, alle gebäudetechnischen Gewerke verfügen heute über elektronische Steuerungssysteme für Regelungsaufgaben. Sie sind über sog. Direct Digital Controls, kurz DDC, untereinander vernetzt und zu komplexen Systemen integriert. Hinzu kommen Energie- und Verbrauchszähler. Darüber hinaus gibt es in der Regel eine übergeordnete Gebäudeleittechnik. All diese Komponenten verfügen über standardisierte Schnittstellen, über die Energie- und Betriebsdaten sowie Konfigurationen ausgelesen werden können. Viele Komponenten unterstützen zudem Anlagenvisualisierungen via Webbrowser.

Ein direkter Zugriff auf solche Infrastrukturen via Internet wäre viel zu riskant. Wie sorgt man nun für die si-

Autor

Dr. Sven Herbert, Jahrgang 1973, Geschäftsführer der Unternehmensgruppe Herbert, Bensheim. www.herbert.de

Netzwerksicherheit und Automation

Herbert setzt mit seinem Energie- und Fernwirkportal auf eine Lösung der Firma ISONA aus Dienheim bei Mainz (siehe Beitrag „Immer im Bilde“). Das innovative Unternehmen realisiert anspruchsvolle Webseiten und verknüpft sie mit Kunden-Applikationen. In den Bereichen IT-Security und Webportale verfügt ISONA über jahrelange Expertise. Einen besonderen Schwerpunk bilden Lösungen zum sicheren Zugriff auf Automatisierungssysteme von Maschinen und Anlagen sowie Gebäudetechnik. In diesem Bereich gibt es zahlreiche Security-Lücken, die das „Secure Automation System“ von ISONA komfortabel umgeht. Im Folgenden ein Interview mit Inhaber und Geschäftsführer Wolfgang Heck zum Thema IT-Sicherheit von Industrieanlagen.

Industrieanlagen, aber auch Gebäudeautomationssysteme werden zunehmend mit IT-Systemen verknüpft. Dadurch werden sie prinzipiell auch vom Internet aus angreifbar. Was sind die wesentlichen Schwachstellen bei Industrieanlagen?
Viele Betreiber industrieller Anlagen, vor allem kleinere und mittlere Unternehmen, unterschätzen noch immer die Gefahren, die daraus erwachsen können, wenn Automatisierungssysteme, IT- und Internet-Technologie miteinander verknüpft werden. Viele, vor allem kleinere Anlagen lassen sich sogar direkt via Internet ansprechen, wenn man lediglich die IP-Adresse kennt und sie im Webbrowser aufruft. Hier fehlen nicht selten die elementarsten Schutzmechanismen. Die Anlagen werden damit ebenso angreifbar wie ein PC oder Webserver. Dabei ließen sich unberechtigte Zugriffe auf die Bedienoberfläche einer Steuerung schon durch relativ einfache Maßnahmen stark erschweren, wie z.B. eine spezielle Firewall oder VPN-Box für die Steuerung und eine sichere Authentifizierung.
Ein weiteres Problem sind die Steuerungen selbst, bei denen IT-Experten immer neue Schwachstellen aufdecken. Anders als beim Endanwender-PC werden solche Lücken allerdings meist nicht immer direkt geschlossen, da das Update einer Steuerung umständlicher ist als das eines PCs. Mit dem Effekt, dass die bekannten Schwachstellen für Angriffe weiter genutzt werden können. Bei unserer Lösung mit VPN-Gateway und sicherer 2-Faktoren-Authentifizierung muss man sich wegen solcher Sicherheitslücken keine Sorgen machen.
Auch problematisch ist die direkte Verknüpfung von Office- und Automatisierungsnetzen, so dass z. B. Angriffe oder Manipulationen über das Officenetz ausgeführt werden können. Wie gefährlich das werden kann, zeigt dieses Beispiel: 2014 wurde laut Bundesamt für Sicherheit in der Informationstechnik sogar ein Stahlwerk über einen solchen Weg angegriffen. Über das Büronetz verschaffte sich der Angreifer Zugriff auf das Produktionsnetz mit dem Effekt, dass der Hochofen nicht mehr geregelt heruntergefahren werden konnte und die Anlage massiv beschädigt wurde.
Wie real ist die Gefahr von Cyberangriffen auf Industrieanlagen oder Gebäudeautomationssysteme in Ihren Augen und welchen konkreten Schaden können solche Angriffe anrichten?
Die Schadensszenarien sind sehr vielfältig und reichen von Unfällen an Leib und Leben über Produktionsausfälle und Schäden an Maschinen und Anlagen bis zum Verlust von Unternehmensgeheimnissen, wie z. B. Rezepturen in Pharmabetrieben. Es kann aber auch um Datenschutz gehen. Um es konkreter zu machen: Stellen Sie sich z. B. ein großes Krankenhaus vor, bei dem es an einem kalten Wintertag unbemerkt zu einer Manipulation an der Gebäudeleittechnik kommt und die Heizungsanlage außer Betrieb gesetzt wird. Bleibt der Ausfall zu lange unbemerkt, muss das Krankenhaus möglicherweise sogar evakuiert werden, weil das Gebäude schon zu weit ausgekühlt ist, um es bei der großen Heizlast wieder schnell genug hochheizen zu können. Dieses Gedankenexperiment zeigt aber auch, wie wichtig verlässliche und sichere Alarmierungssysteme sind.

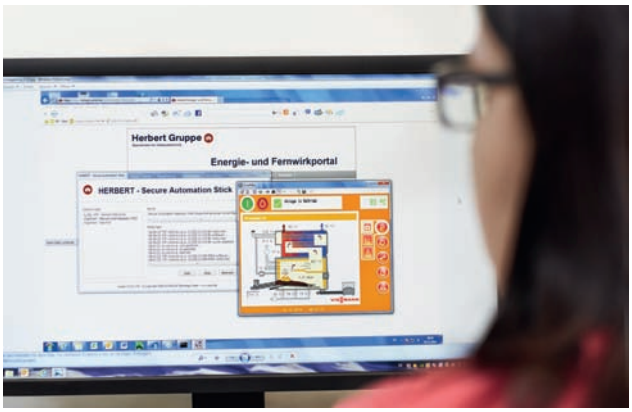

Bild: ISONA

„Sichere Automatisierung hört nicht an der Ethernet-Schnittstelle der Steuerung auf“, so Wolfgang Heck, Geschäftsführer bei der ISONA Services GmbH

Wie gehen Unternehmen mit diesen Risiken bzw. Sicherheitslücken um?
Organisatorisch liegt in vielen Unternehmen das Problem bei den unterschiedlichen Verantwortlichen für die Automatisierungssysteme und die IT. Wir haben es hier, wie bereits gesagt, aber meist mit technisch nicht so klar trennbaren Welten zu tun, weil z. B. der technische Leiter auch an seinem Office-PC direkten Zugriff auf die Gebäudeleittechnik haben möchte. Die Automatisierung hört aber nicht an der Ethernet-Schnittstelle der Steuerung auf. „Brückenschläge“ zwischen Büro-IT und Automatisierungsnetzwerk können schnell zum ernsten Problem werden, wenn nicht hinreichende Sicherheitsmaßnahmen ergriffen werden. Das Bewusstsein in Unternehmen für solche Themen wächst allerdings.
Auf der anderen Seite eröffnet die Verknüpfung mit IT und Internet natürlich zahlreiche neuartige Anwendungen, von der Fernwartung über Fehlerdiagnose via Smart Device bis hin zum standortübergreifenden Energiemanagement. Was sind aus Ihrer Sicht die wesentlichen Trends, die uns in den nächsten Jahren noch beschäftigen werden?
Wir werden in Zukunft sicher vermehrt Tablets einsetzen, um auf Industrieanlagen und Gebäudetechnik zuzugreifen, zumal jüngere Beschäftigte nachrücken, die mit diesen Technologien groß geworden sind. An guten Konzepten für einen sicheren Zugriff auch auf Industrieanlagen via Smart Devices wird daher kein Weg vorbeiführen. Zurzeit beobachten wir noch, dass viele Hersteller eigene Lösungen für den Zugriff auf ihre Steuerungen schaffen. Gerade im Umfeld der Gebäudeautomation, wo es heute schon für jedes Gewerk eine extra App gibt, wird das aber schnell unpraktikabel. Für den Anwender wäre eine Standardisierung wünschenswert, so dass auf Betriebs- und Anlagendaten sowie Anlagenvisualisierungen gewerkeübergreifend mit nur einer App zugegriffen werden kann. ISONA entwickelt hier zurzeit erste Pilotanwendungen in diese Richtung.
Von den vielfältigen neuen Möglichkeiten des sicheren Fernzugriffs werden Anlagenbetreiber und Servicepartner gleichermaßen profitieren. Das fängt beim schnelleren und kostengünstigeren Support bei Störungen oder Wartungsarbeiten an. Updates oder Änderungen in der Programmierung sind aus der Ferne möglich. Selbst im Urlaub oder bei Rufbereitschaft kann ein technischer Leiter jederzeit auf die Anlage zugreifen. Durch eine direkte und schnelle Alarmierung der zuständigen Personen bei Störungen können kostspielige Anlagen- und Produktionsausfälle vermieden werden. Eine weitere wichtige Einsatzmöglichkeit von Energie- und Fernwirkportalen sind Energiemanagementsysteme gemäß DIN EN ISO 50001. Herbert als Unternehmen, das das gesamte Leistungsspektrum der Technischen Gebäudeausrüstung abdeckt, kann mit dem Energie- und Fernwirkportal von ISONA seinen Kunden schon heute eine ganzheitliche und gewerkeübergreifende Fernwartungslösung anbieten, die nach dem heutigen Stand der Technik höchste Sicherheitsstandards erfüllt.

chere Umsetzung? Die Helmut Herbert GmbH & Co., Bensheim, nutzt ein innovatives Energie- und Fernwirkportal, das, bedingt durch seine Architektur (**Bild 1**), einen manipulationssicheren Zugriff auf Anlagendaten und Verbrauchswerte weit verteilter Anlagen via Internet erlaubt. Für das Portal setzt Herbert eine Lösung der ISONA Services GmbH aus Dienheim bei Mainz ein (siehe dazu auch das Interview mit dem Geschäftsführer zum Thema Secure Automation). Die Daten der aufgeschalteten Anlagen werden nicht direkt zugänglich gemacht, sondern über einen Server, der die reale Infrastruktur der Gebäudeautomation virtuell spiegelt. Die Webanwendung lässt sich in jedem Webbrowser aufrufen (**Bild 2**). Via Smartphone und Tablet (Apple iOS und Android) ist auch ein mobiler Zugriff auf Anlagenvisualisierungen möglich. Damit kann ein besonders schneller Anlagensupport geleistet werden, und der Betreiber hat jederzeit und von überall Zugriff auf Anlagendaten und die Anlagenvisualisierungen. Das Energie- und Fernwirkportal für die Gebäudeautomation erfüllt im Wesentlichen die Funktionen: Monitoring, Alarmierung, Protokollierung, Zählerauslesung und Energieerfassung. Darüber hinaus gestattet es einen schnellen Überblick über alle installierten Geräte und ihre Konfiguration, was im Fernsupport von unschätzbarem Wert ist.

Dank des Portals lassen sich viele Störungen in Zusammenarbeit mit einem Techniker vor Ort kostengünstig und umgehend aus der Ferne beheben und



Bilder: Helmut Herbert GmbH & Co.

Bild 2
Über das Herbert Portal kann man Anlagenvisualisierungen mit aktuellen Werten sicher aus der Ferne anzeigen, hier für eine Holzhackschnitzelheizung

Programmanpassungen (Sollwerte, Schaltzeiten etc.) vornehmen. Durch die permanente Überwachung und die Möglichkeit eines automatisierten SMS- oder E-Mail-Versands bei Störungs- oder Wartungsmeldungen wird das Risiko kostspieliger Ausfälle minimiert. Es wird direkt das zuständige Personal benachrichtigt, um bei Störungen schnell eingreifen zu können. Erleichtert wird dem Servicepersonal die Störungsbeseitigung durch den direkten Zugriff auf die im Portal abgelegten Anlagendokumente wie Schaltpläne, Regelschemata, Produktdatenblätter etc.

Die Protokolle gängiger Steuerungshersteller im Bereich Gebäudeautomation werden unterstützt. Betreiber und technischer Support haben so via Webbrowser schnell Zugriff z. B. auf Anlagenvisualisierungen, um z. B. Störungen zu analysieren. Bei nahezu allen Reglern stehen auch Daten wie Energieverbrauchswerte oder Effektivitätsgrade zur Verfügung.

Der Zugriff auf das Webportal erfolgt über eine sichere VPN-Verbindung, sodass man auch Regler-Programme direkt ändern kann. Der Betreiber hat über eine VPN-Verbindung passiven Zugriff auf Anlagenvisualisierungen und Betriebsdaten, was z. B. hilfreich sein kann, um gemeinsam Probleme an der Anlage zu finden und zu lösen.

Um auf das Webportal zuzugreifen, ist eine hochsichere Zwei-Faktor-Authentifizierung mit Passwort und einem Einmalkennwort erforderlich, das mit einem Kennwort-Generator erzeugt oder per SMS versendet wird, vergleichbar mit der SMS-TAN beim Online-Banking.

Die Erreichbarkeit der Geräte wird über ein Monitoringsystem via VPN-Verbindung dauerhaft überwacht, denn die Daten müssen im Energie- und Fernwirkportal stets verfügbar und immer aktuell sein. Kommunikationsstörungen oder Ausfälle bei der Internetverbindung werden sofort gemeldet.