

IQ.Wissensforum am Donnerstag, 19. Oktober 2017

## Wie hackt man eine Gebäudeautomation?

Wir zeigen, wie's geht. Und wie man sich davor schützen kann.

Die Gebäudetechnik ist im Umbruch. Neue Impulse durch die Digitalisierung stellen Betreiber von Liegenschaften, Planungsingenieure und Entwickler vor neue Herausforderungen. Unser IQ.Wissensforum soll Teilnehmer in die Lage versetzen, Schwachstellen bezüglich der Gebäudesicherheit zu erkennen. Darüber hinaus werden Problemlösungen aufgezeigt.

Wir haben Experten eingeladen, die sich mit Risikobewertung und Industrie 4.0 seit Jahren auseinandersetzen und über wichtige Facetten der Digitalisierung aufklären können.

[Anmeldung](#)

### Programm

**13:00**      **Einlass**  
Kanapees und Getränke

---

**13:30**      **Dipl.-Ing. Maurice Al-Khaliedy**  
**Cyber Security Lead, CSPI Technology Solutions**

- Live-Hack an einer Steuerung der Gebäudeautomation
- Cyber-Attacken und Industrie 4.0
- Sinnvolle Vernetzung, Rückwirkungen bei Systemausfall
- Digitalisierung und BIM vs Gebäudesicherheit

Diskussionsrunde

---

**Zirka 14:30**      **Prof. Dr. Wolfgang Weck**  
**Fachhochschule Nordwestschweiz FHNW**

- BACnet/IT: Gebäudeautomation in Zeiten des Internet
- BACnet/SC: Sichere Datenkommunikation für BACnet-Geräte
- Wohin geht die Reise bei ASHRAE?

Diskussionsrunde

---

**Zirka 16:00**      **Eröffnung des Bayerischen Buffets**

**18:00**      **Ausklang**

---

Dipl.-Ing. Maurice Al-Khaliedy  
**CSPI Technology Solutions**

### Cyber-Sicherheit im Zeitalter Industrie 4.0

Cyberangriffe auf Produktionsanlagen oder im Allgemeinen auf ICS-Umgebungen (ICS = Industrial Control Systems) sind heute keine Fiktion mehr, sondern Realität. Daher ist es notwendig, dass Unternehmen mit derartigen Umgebungen ihre Haltung gegenüber Cybersicherheit ändern. Bisherige Schutzmaßnahmen setzten darauf, dass industrielle Infrastrukturen in physisch isolierten Umgebungen betrieben werden. In

Zeiten von Industrie 4.0 und der zunehmenden Digitalisierung kann diese Trennung in vielen Fällen nicht mehr gewährleistet werden oder ist bereits vollständig aufgehoben.

Eine von Kaspersky erstellte Studie bestätigt, dass weltweit 188.019 ICS-Rechner (Hosts) über das Internet erreichbar sind. Von diesen wurden ca. 14 Prozent in Deutschland identifiziert. Des Weiteren ist in den vergangenen fünf Jahren die Anzahl gefundener Schwachstellen innerhalb von ICS-Komponenten um das Zehnfache gestiegen. Bei knapp der Hälfte der Fälle handelt es sich um kritische Lücken in Benutzerschnittstellen beziehungsweise „Human Machine Interfaces (HMI)“. Man kann beobachten, dass diese Sicherheitslücken kein Phänomen einzelner Branchen sind, sondern sie ziehen sich über alle Industriezweige hinweg.

### **Live-Hack an einer Steuerung der Gebäudeautomation**

Dem Auditorium soll veranschaulicht werden, welche Herausforderungen heute im Design von Produktionsanlagen oder in der Gebäudetechnik zu bewältigen sind, um Kompromittierungen, Manipulationen oder Zerstörungen derartiger Infrastrukturen zu verhindern. **Darüber hinaus zeigen wir live**, welche möglichen Angriffsvektoren existieren, um Zugriff auf derartige Infrastrukturen zu bekommen und manipulativ auf diese einzuwirken.

Prof. Dr. Wolfgang Weck

**Fachhochschule Nordwestschweiz, Hochschule für Technik**

### **BACnet/IT:**

### **Neue Wege zu einem sicheren BACnet Data Link dank Internet-Technologie**

Datenkommunikation ist bereits seit längerem ein zentrales Element technischer Gebäudeautomation. Dafür eignen sich spezifische Feldbus-Systeme, aber auch preiswerte Standardkomponenten, wie sie die Industrie für Büro-Automation, Internet und andere Anwendungen bietet. Das heute gebräuchliche *BACnet/IP* beispielsweise beruht auf dem Einsatz solcher Komponenten auf der Hardware-Ebene, nutzt aber nicht die höheren Standard-Protokolle des Internets. Das hat zwei Nachteile: Die Datenkommunikation ist weder gegen Abhören noch gegen Manipulation gesichert und das bestehende Internet kann nicht einfach zur Integration über Gebäudegrenzen hinweg genutzt werden, um *SmartCampus*-Lösungen zu realisieren oder *CloudServices* zu nutzen.

Als Lösungsansatz für beide Nachteile zugleich wird bei ASHRAE im Projekt *BACnet/IT* an der Standardisierung eines neuen Daten-Links für *BACnet* gearbeitet, der auf *Websockets*, X.509-Zertifikaten und *TLS* beruht. Diese Standardmechanismen des Internets können leichter auch über Gebäudegrenzen genutzt werden und erlauben dank Public Key Kryptografie verschlüsselte Datenübertragung und Authentifizierung des Senders.

### **Hintergrund zum Vortrag**

Das *Institut für Mobile und Verteilte Systeme* der *Fachhochschule Nordwestschweiz* hat in den vergangenen Jahren ein von der schweizerischen *Kommission für Technologie und Innovation (KTI)* gefördertes Projekt bearbeitet, in dessen Rahmen *BACnet/IT Drafts* parallel zu den Standardisierungsarbeiten der *ASHRAE* prototypisch implementiert und untersucht wurde. Ziel von *BACnet/IT* ist Internet-Standards für *BACnet* nutzbar zu machen, die sichere Kommunikation über Leitungen ermöglicht, die auch von anderen Internet-Diensten genutzt werden (können).

Aktuell wird von *ASHRAE* der Standard für den Data Link von *BACnet/IT* als *BACnet/SC* (Secure Communication) überarbeitet.

[Zur Anmeldung](#)