



# Cyberterror in Gebäudeinfrastrukturen?

Immer öfters wird IT auch in sogenannten kritischen Infrastrukturen eingesetzt, dazu gehört auch die Gebäudeautomation. Viele Gebäudebetreiber sind sich heute der Gefahren und möglichen Schwachstellen in der IT-Gebäudeinfrastruktur nicht bewusst. Das Forum der Bauindustrie 2015 widmete sich diesem Thema.

**Text und Fotos: Werner Aebi**

Dr. Felix Gassmann, CEO Sauter Building Control Schweiz AG, Reinach, ist auch Präsident der Gruppe der Schweizerischen Gebäudetechnik-Industrie GSGI. Im Namen der Gastgeber begrüsste Felix Gassmann am 21. Mai 2015 über 80 Fachspezialisten und Geschäftsleiter der Gebäudetechnik- und Baubranche. Zum Anlass eingeladen hatten fünf namhafte Schweizer Fachverbände, welche sind: die GSGI, der Verband Schweizerischer Generalunternehmer «Entwicklung Schweiz» (ehemals VSGU), der Fachverein Gebäudetechnik und Energie FGE, die Schweizerische Vereinigung Beratender Ingenieurunternehmungen Usic und die Swiss Engineering STV. Felix Gassmann moderierte den Anlass im Renaissance Zürich Tower Hotel an diesem Donnerstag, 21. Mai 2015, zum Thema «Cyberterror – Gefahr über Gebäudeinfrastrukturen?». Zunehmend wird IT auch in den «kritischen Infrastrukturen» eingesetzt, wie zum Beispiel für Wasser- und Stromversorgungen, Finanzsysteme, Telekommunikation und Notfallsysteme, aber auch Gebäudeinfrastrukturen. Die Abhängigkeit von der IT liegt in den Industrieländern bei über 90 Prozent, deren Ausfall oder Fremdmanipulation wirkt sich jeweils fatal aus.

Um gegen die Cyberangriffe gewappnet zu sein, sind noch viele Fragen zu klären, wie zum Beispiel: Welche Motive stecken hinter den Cyberangriffen? Wie gross ist das Gefahrenpotenzial? Wie können Infrastrukturen geschützt werden? Aus welchen Praxisbeispielen können wir lernen? Zwei ausgewiesene Spezialisten stellten die richtigen Fragen und informierten über die Möglichkeiten.

### Auch im Gebäudebereich: Cyberattacken nehmen weltweit zu

Barnaby Skinner ist von Beruf Datenjournalist und Technologieredaktor bei der SonntagsZeitung und beim Tages-Anzeiger in Zürich. In seiner Tätigkeit wird der Kenner zeitgenössischer Geschichte und Technik immer wieder mit Vorfällen in der Cyberkriminalität konfrontiert. Allerdings sprechen die Betroffenen nicht gern über dieses Thema, da dies ihrem Image schaden könnte. Sicherheitsfirmen veröffentlichen jährlich mehrere Reports, worin erklärt wird, wie die Angriffe zunehmen und dass sie sich bis ins Unermessliche steigern. Doch konkrete Fälle werden aufgrund des Persönlichkeitsschutzes nicht genannt. Das ist schade, da das Bewusstsein für die Ernsthaftigkeit einer Bedrohung meist nur durch echte Beispiele geweckt würde.

Trotzdem hier ein Beispiel, das jüngst in der Presse zu lesen war: Der Gründer der US-Sicherheitsfirma One World Labs, Kris Roberts, konnte sich in das Flugmanagementsystem eines grossen Passagierflugzeugs, worin er gerade sass, einloggen. Das Vorgehen ist für einen Experten einfach: Man verbindet seinen Laptop via Ethernetkabel mit dem Entertainmentsystem des Flugzeugs und kann daraufhin das ganze Flugzeug unter Kontrolle bringen. Es scheint, dass sich da bisher niemand mit der internen Sicherheit beschäftigt hat.

Im Nachhinein hat das FBI die Sache bestritten: Es sei zu keinen Fällen gekommen. Trotzdem wurde es später publik, da Roberts selbst darüber berichtete. Dieses Beispiel bringt es auf den Punkt: Alle wissen, dass es diese Pro-


**1.** Im Namen der Gastgeber begrüsste Felix Gassmann am 21. Mai 2015 über 80 Fachspezialisten und Geschäftsleiter der Gebäudetechnik- und Baubranche.

**2.** Barnaby Skinner: «Es ist unbestritten, dass die Cyberkriminalität zunimmt.»

**3.** Steffen Wendzel: «Für IT-Systeme gibt es stapelweise Bücher zum Thema Sicherheit, für die Gebäudeautomation ist fast nichts vorhanden.»

bleme gibt, aber niemand möchte über die Details sprechen. Unbestritten ist aber, dass die Cyberkriminalität zunimmt. Beispielsweise wurden allein im letzten Jahr weltweit 432 Millionen E-Mail-Konten gehackt. Der weltweite Schaden durch Cyberangriffe ist enorm und wird mittlerweile auf 2,2 Billionen US-Dollar geschätzt. Wer sich ein Bild der globalen Cyberattacken machen möchte, dem sei die Website des amerikanischen Norse-Netzwerks empfohlen. Eigentlich ist es logisch, dass die Cyberattacken zunehmen. So hängen immer mehr Computer, aber auch Geräte am Internet, so auch Kühlschränke, Solaranlagen, Kaffeemaschine bald auch das Auto und heute viele Gebäudeinfrastrukturen. Diese Geräte und Maschinen findet die Suchmaschine des «Internet of Things» unter shodan.io. Im September 2013 starteten rund 2700 Anlagen komplett offen – das heisst ohne Schutz und frei nutzbar – im Internet zur Verfügung. Gemäss neuster Messung sind es heute etwa doppelt so viele. Zum Beispiel stand 2013 das Haupttor des Stadions St. Jakob offen benutzbar im Internet, erst auf Nachfrage der SonntagsZeitung schloss der Betreiber diese Sicherheitslücke. Zur gleichen Zeit waren auch 216 Schweizer Solaranlagen im Internet offen zugänglich, das heisst es war möglich, über den Browser auf die Steuerung zuzugreifen. Auf Anfrage hatte niemand eine Ahnung davon, dass die Anlage ungeschützt im Web stand.

Dieselben Probleme könnten auch in Zukunft in den sogenannten Smartgrids des Stromnetzes auftauchen. Das Gefährden von Anlagen, Kraftwerken, Flugzeugen, Spitälern usw. durch Nachlässigkeit könnte sich zum Supergau auswirken, dem digitalen Schutz ist deshalb höchste Priorität beizumessen.

### Kommunizierende Module brauchen Schutz

Dr. rer. nat. Steffen Wendzel, Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie, Bonn, Abteilung Cybersecurity, referierte zum Thema «Auf dem Weg zum sicheren Smart Building». Mit fortschreitender Technologie und steigenden Ansprüchen gelangen mehr Gebäudeautomationen zum Einsatz. Die Hersteller bauten häufig keine Sicherheit ein, weil niemand danach fragte – die IT-Sicherheit war in diesem Bereich auch nicht vorgegeben. Stets wurden mehr Features mit eingepackt, aber an die Sicherung der Systeme wurde nicht gedacht. Hinzu kommt, dass ein automatisches System gegebenenfalls im Einbaujahr modern und geschützt ist, dieses verbleibt dann aber über Jahre im Gebäude und wird nicht mehr aktualisiert. Auch lässt sich ein System nach einigen Jahren nicht mehr nachrüsten, weil es auch hardwaremässig veraltet ist. Fakt ist, dass heute massenweise jahrzehntealte Gebäudesysteme in Betrieb sind.

Üblicherweise erhalten IT-Systeme oder Automationen regelmässige Updates/Upgrades, das nennt man Patching. Künftig werden noch viel mehr Chips, Sensoren, Controller und Systeme im «Internet der Dinge» miteinander kommunizieren, Beispiele dafür sind wearables oder im Bereich Health Care. Ältere Menschen tragen kommunikative Systeme mit sich, solches bedeutet aber, dass gesundheitskritische Daten im Internet kursieren. Das sind Daten, die viele Leute nicht Externen preisgeben möchten. Häufig weisen die kommunikativen Systeme in ihren Internetprotokollen Informationen von mehreren 1000 Seiten auf – bei derartig grossen Datenmengen sind die Sicherheitslücken voraussehbar. Die IT-Administratoren können wohl ihre Anlagen sichern und warten, sind aber für die IT-Sicherheit von Gebäudeautomationen nicht ausgebildet. Sie benötigen also dahingehende Schulung, damit sie zum Beispiel wissen, wie man historische Sensordaten speichert. Für IT-Systeme gibt es stapelweise Bücher zum Thema Sicherheit, für den Bereich Gebäudeautomation ist darüber praktisch nichts vorhanden. Um etwas zu bewegen, müssten die Schwachstellen und die realen Attacken bekannt werden, die aber – wie schon vom Vorredner erwähnt – aus Imagegründen meistens nicht an die Öffentlichkeit kommen.

### Die Baukonjunktur und das nächste Forum

Prof. Dr. Jan-Egbert Sturm, Leiter KOF, ETH Zürich, referierte über das «konjunkturelle Umfeld der Bauindustrie». Die Situation im schweizerischen Umfeld zeigt sich etwas stabilisierend, weil die europäische Wirtschaft sich «normalisiert». Das heisst, es sind in unserer Nachbarschaft keine besonderen Auf- und Abwärtsbewegungen zu erwarten. Die treibende Kraft kommt aus den Schwellen- und Entwicklungsländern, speziell bezüglich Industrieproduktion. Zum Schluss verglich Jan-Egbert Sturm den Nutzen des Internet zwischen den Branchen in der Schweiz. Wie die Statistik zeigt, wird die Vernetzung über das Internet im Baugewerbe deutlich schwächer eingesetzt, als das in der Industrie oder im übrigen Dienstleistungsgewerbe der Fall ist. Das nächste Forum der Bauindustrie wird am Donnerstag, 19. Mai 2016, stattfinden. ■

**www.forum-bauindustrie.ch**