Virtuelle Angriffe auf moderne Gebäude mit handfesten Auswirkungen – und wie sich ein wirksamer Schutz umsetzen lässt

Nahezu jeder gewerblich oder industriell genutzte Neubau und viele gehobene Privathaushalte verfügen mittlerweile über intelligente Elektroinstallationen. Dabei werden Licht, Rollläden und andere elektrische Verbraucher nicht direkt von einem Schalter aus gesteuert, sondern über sog. Aktoren durch eine vernetzte Steuerung. Schalter dienen hierbei als Sensoren. In der Steuerung lässt sich jeder beliebige Sensor mit jedem Aktor verknüpfen. So kann nicht nur geänderten Gebäudenutzungen kostengünstig Rechnung getragen werden. Auch können übergeordnete Managementsysteme zentrale Steuerfunktionen übernehmen, ebenso wie von meteorologischen Sensoren gesteuerte Abhängigkeiten etc.

Im angesprochenen Segment ist dabei ein Steuerungsprotokoll vorherrschend, der sog. KNX-Standard (früher auch als Europäischer-Installations-Bus (EIB) bekannt). Das KNX-Protokoll definiert, wie bei einer Installation Sensoren und Aktoren in einem Haus miteinander verbunden werden können und wie Sensoren und Aktoren miteinander kommunizieren müssen. Um diese Kommunikation zwischen Sensoren und Aktoren zu ermöglichen, werden alle Teilnehmer mittels einer BUS-Leitung miteinander verbunden. Insbesondere zum Zweck der Visualisierung auf anderen Systemen, aber auch zur Fernsteuerung, wird der KNX-BUS fast immer mittels eines IP-Gateways mit dem Internet verbunden. Damit kann das betreffende Gebäude von jedem Internetanschluss weltweit erreicht werden.

Sicherheit bislang unberücksichtigt

Bei der Entwicklung des Standards standen die Funktionen im Vordergrund. Die einschlägige Norm, die ISO/IEC 14543-3 enthielt keinerlei nennenswerte Festlegungen zur Implementierung der IT-Sicherheitsziele, wie Vertraulichkeit und Authentizität. Und auch in der praktischen Umsetzung wurden entsprechende Aspekte nicht berücksichtigt. Zwischenzeitlich hat man im ISO-Gremium die Notwendigkeit der Anpassung des Standards unter dem Gesichtspunkt der Sicherheit zwar erkannt, doch bis zur Umsetzung als Norm wird sicher noch etwas Zeit ins Land ziehen. Jedoch: Normierte Sicherheit schützt nicht in der Praxis. Nur weil es Normen für Einbruchschutz-Produkte gibt, wird nicht weniger eingebrochen. Nur, weil Sicherheit im KNX-Standard normiert ist, wird KNX nicht automatisch sicherer: Entsprechende Festlegungen und Mechanismen müssen in der Praxis auch eingesetzt werden, und zwar wirksam.

Was kann eigentlich passieren?

Ein Angreifer hat im Regelfall zwei Möglichkeiten, vorzugehen: Entweder er greift vor Ort direkt auf den KNX-BUS zu oder er greift aus der Ferne aus an. Beides ist in der Praxis keine Schwierigkeit und vollkommen unauffällig zu bewerkstelligen. Hat ein Angreifer den Zugriff auf den BUS erlangt, kann er alles ausführen, was der Betreiber des Gebäudes auch kann: Licht ein- und ausschalten, Heizungen regeln, Rollläden rauf- und runterfahren, Fenster öffnen und schließen usw. Der Schaden durch eine immerwährend eingeschaltete Beleuchtung mag sich noch in Grenzen halten, doch bei Regen kann ein geöffnetes Dachfenster einen ganz erheblichen Wasserschaden verursachen. Durch geöffnete Fenster oder Türen können Einbruchdiebstahlschäden entstehen. Eine abgeschaltete Heizung kann einen Frostschaden hervorrufen. Abgeschaltete Lüftungseinrichtungen können zur Überhitzung der geschützten Maschinen und im schlimmsten Fall zum Ausbruch eines Brandes führen. All diese Angriffe können dazu führen, dass es zu Betriebsunterbrechungen kommen kann.

Doch damit nicht genug. Aufgrund der schwachen Sicherheitsarchitektur des KNX-BUSses besteht für einen Angreifer sogar die Möglichkeit, alle Komponenten so zu „rekonfigurieren“, dass diese unbrauchbar werden. Funktionen lassen sich dann nicht wieder herstellen, stattdessen müssen alle Komponenten ausgebaut und ins Werk zur Reparatur eingeschickt werden.

Das worst-case-Szenario wäre ein Täter, der gleichzeitig eine Vielzahl von KNX-Installationen unter seine Kontrolle gebracht hat. Durch gleichzeitiges Aus- und Einschalten aller Verbraucher aller Gebäudeinstallationen würde eine Lastspitze erzeugt, durch die das Energieversorgungsnetz einer ganzen Region in kurzer Zeit zum Zusammenbruch gebracht werden könnte.

Vorgefertigte Hard- und Software für Angriffswerkzeuge existieren bereits und sind öffentlich verfügbar. Das erhöht die Wahrscheinlichkeit eines Angriffs, zumal der Täter kein KNX-Spezialist zu sein braucht, um die Angriffswerkzeuge einzusetzen.

Schutz ist möglich

Die gute Nachricht: Vor diesen Szenarien können Sie sich und Ihre Kunden schützen. VdS hat Richtlinien erarbeitet, die beschreiben, wie eine KNX-Installation sicher aufgebaut werden kann. Dazu gehört auch die Einhaltung der zukünftig in der Norm enthaltenen Sicherheitsanforderungen, aber auch darüber hinausgehender VdS-Anforderungen.

VdS bietet die unabhängige Prüfung und Zertifizierung von KNX-Gebäudeinstallationen unter dem Gesichtspunkt der Sicherheit an. Dabei nehmen wir die Installation unter die Lupe und prüfen, ob vorhandene Sicherheitsmaßnahmen umgesetzt wurden und wirksam sind. Nur wenn alle Anforderungen erfüllt sind, vergibt VdS für die konkrete Gebäudeinstallation das begehrte VdS-Siegel.

Vertrauen durch Sicherheit – Zertifizierte Sicherheit des Gebäudeleitsystems