

Haustechnik – In Zukunft werden sich Hausbesitzer auch um das Absichern ungewohnter Einfallstore kümmern müssen, etwa im Heizungskeller oder bei der Lichtsteuerung. Denn mit der wachsenden Zahl internetfähiger Geräte im Haus wächst auch die Zahl der möglichen Angriffspunkte.

Heizkessel hinter Schloss und Riegel

Für den schlüssellosen Zutritt ins Haus gibt es vielfältige und robuste Lösungen. Codetastaturen, Badgeleser oder Fingerabdruckscanner versprechen zudem einen hoch-

MICHAEL STAUB
Journalist BR, Kriens

stehenden Einbruchschutz. Wer eine gute und angemessene Lösung für seine Bedürfnisse erwägt, sollte mit einem Spezialisten sprechen. «Zuerst muss man wissen, was man will und was einem wichtig ist», sagt Markus Fischbacher, Technischer Leiter bei der Telcom AG in Stansstad. Dies beginne beim mechanischen System. Reicht ein einfacher Elektrotüröffner für hundert Franken, oder soll es ein dreipunktverriegeltes Motorschloss für 2500 Franken sein? Auch beim Medium für die Türöffnung ist die Bandbreite gross: Vom guten alten Schlüssel bis zu Handvenenscannern ist fast alles möglich.

Nutzerverhalten einbeziehen

Den grössten Einfluss auf die effektive Sicherheit haben die Benutzer. So ist Familien von PIN-Systemen eher abzuraten. Das Abdecken der Zahleneingabe gelingt Kindern nicht immer, und rasch kennen auch die Spielplatzfreunde den Code. «Wir raten in solchen Fällen eher zu einem Fingerabdruckleser», sagt Fischbacher. Je nach Bedürfnis können die einzelnen Komponenten auch entsprechend kombiniert werden, etwa indem ein Badgeleser mit Codetastatur und Fingerprintleser ergänzt wird.

Rein elektronische Lösungen kommen für den Fachmann nicht in Frage. «Jede Türe benötigt nach wie vor einen Schliesszylinder. Falls der Strom oder die Steuerung ausfällt,



Gesprächige Kessel: Viele neue Heizanlagen besitzen heute eine Internet-Verbindung.

BILDER VISSMANN

muss immer noch ein Noteintritt möglich sein», sagt er. Die Sicherheit wird so mechanisch wie elektronisch gewährleistet.

Gesprächige Heizanlagen

Das Absichern von Aussentüren und Fenstern gehört zum Standard. In Zukunft werden Hauseigentümer beim Einbruchschutz jedoch auch an die Heizung denken müssen. Denn moderne Kessel oder Wärmepumpen hängen oft am Internet. Dadurch sind sie mit einem Garagentor vergleichbar: Sie führen nicht geradewegs in die gute Stube, ermöglichen aber den Zugang ins Innere des Gebäudes. Unzureichend abgesicherte Verbindungen erlauben im schlimmsten Fall den Einbruch in das lokale Computernetzwerk des Gebäudes. Dieses potenziel-

le Einfallstor muss deshalb sorgfältig gesichert werden.

Mit der seit 2012 erhältlichen «Vitol»-App von Viessmann können Hausbesitzer ihre Heizungsanlage auch von unterwegs bedienen. Der Hersteller legt grosses Gewicht auf die Sicherheit der Anwendung. «Unser Fernüberwachungssystem ist so konstruiert, dass nach aktuellem Stand der Technik kein Hacken möglich sein sollte», sagt Urs Schnellmann, Produkt-Marketing-Manager bei der Viessmann (Schweiz) AG. So werden unter anderem sichere SSL-Verbindungen genutzt und die Endgeräte im Netzwerk unsichtbar gemacht. Zudem überwacht man die Kommunikation zwischen Heizung und App-Server auf Auffälligkeiten. «In Zukunft werden immer mehr Haustechnikanlagen mit



Mit der «Vitol»-App von Viessmann lässt sich die Heizung via Tablet steuern.

einer integrierten LAN-Schnittstelle ausgerüstet werden», sagt Schnellmann. Dieses «Internet der Dinge» führe zu einer wachsenden Zahl von internetfähigen Heizungen, Lüftungen oder gar Kühlschränken. Diese smarten Geräte angemessen abzusichern und zu überwachen, wird darum immer wichtiger.

Vernetzte Gebäude

Während Konzepte wie das Anfang 2014 vorgestellte «Smart Home» von Samsung vor allem Haushalts- und Unterhaltungselektronik wie Staubsauger, Waschmaschine und den Fernseher vernetzen, existieren für die Kontrolle der Haustechnik schon länger etablierte Systeme. Die Beschattung, Beleuchtung und Heizung lässt sich zum Beispiel über das Bussystem

KNX regeln. Es kann über eine WLAN-Verbindung auch vom Smartphone oder Tablet aus gesteuert werden. Öffnet diese Funkverbindung potenziellen Hackern eine Tür zur Haustechnik? Und wäre ein solcher Zugang zur ganzen Gebäudeinfrastruktur nicht gefährlicher als «nur» eine Heizung mit Internetzugang? Andreas Lenz ist Automations-Sachbearbeiter bei der Elektro Burkhalter AG in Bern. Er arbeitet seit Jahren mit KNX und wiegelt ab: «Zuerst müsste der WLAN-Zugang oder die stationäre Internetverbindung ins Gebäude geknackt werden.» Selbst wenn ein Angreifer Zugriff auf das KNX-System hätte, bleibe die Frage, was ihm dies bringe. «Wer will schon Ihre Jalousien hochfahren oder das Licht ausschalten?» Selbst eine Umprogrammierung der gesamten KNX-Anlage wäre laut Lenz einfach zu beheben. «Man spielt ganz einfach die Backup-Daten ein», erklärt er.

Für das Ausspionieren eines Gebäudes oder gar die Vorbereitung eines Einbruches wäre ein KNX-Angriff laut Lenz viel zu aufwendig. Das komplexe System biete nach den bisherigen Erfahrungen eine ausreichende Sicherheit.

Handvenenleser bieten eine sichere Identifikation.

BILD FRANK TÜREN AG

