Sicherheit!

www.LCN.eu

Ihr Smart Home ist bei LCN in besten Händen!

Wir leben in bewegten Zeiten. Das gilt auch für die Haustechnik:

Es gibt immer häufiger Berichte über Angriffe auf Systeme der Gebäudeleittechnik / Smart Home. Ein bedeutendes europäisches System kann sogar bis zum Totalausfall gehackt werden. Ist das bei LCN auch möglich?

Nein!

Sicherheit!

Die technischen Hintergründe:

Tatsächlich ist die Gefahr abhängig vom Medium, über das die Steuerbaugruppen kommunizieren:

Funk-Systeme

Besonders leicht lassen sich natürlich Funksysteme angreifen: Die Funkfrequenzen sind bekannt und einschlägige Sender-/Empfänger sind handelsüblich. Deshalb sind sehr viele Systeme verschlüsselt. Falls der Hersteller einen guten Algorithmus verwendet, wird der Zugriff von Außen weitgehend verhindert. Natürlich sollte der Installateur vertrauenswürdig sein; denn er kennt die Passwörter …

Aber Vorsicht bei Alarmanlagen: Manche Hersteller bieten Funk-Alarmanlagen als „sicher“ an, da sie ja verschlüsselt seien. Das ist Unfug: Mit einem Jammer (Störsender) kann ein potenzieller Einbrecher den Empfänger mit einem Störsignal ganz einfach zustopfen. Dann kann die Zentrale kein Sensorsignal mehr empfangen. Die Zentrale kann gegebenenfalls noch eine Warnung ausgeben, eine Funktion hat sie aber nicht mehr.

Drahtgebundene Systeme

Drahtgebundene Systeme sind naturgemäß schwerer anzugreifen: Der Angreifer braucht einen direkten Zugang zum Kabel. Wenn das Kabel nicht gerade im Außenbereich verlegt ist, ist ein handfester Einbruch ins Gebäude nötig, um an das Buskabel zu gelangen. In diesem Fall dürfte der Angriff auf den Bus wohl das geringere Problem sein.

Es sind aber Szenarien denkbar, in denen ein Angreifer leichter an das Kabel kommt, z.B. im Hotel. Dann wird es für die vielen Systeme gefährlich, die die Nachinstallation von Software auf den Modulen vorsehen, z.B. KNX. Der Angreifer könnte ganz einfach Schadcodes in Baugruppen herunterladen und über diesen Code die Kontrolle übernehmen – so wie bei einem Virus auf einem PC. Das wäre der Horror für den Betreiber des Gebäudes.

Es geht auch einfacher: Der Angreifer könnte zum Beispiel wichtige Funktionen, wie die Zugangskontrolle umparametrieren und sich so Zugang an beliebigen Stellen des Gebäudes verschaffen.

Nicht bei LCN:

Der Software Code ist fest im Modul gespeichert, er kann nicht (wie bei fast allen anderen Systemen) verändert werden. Ein Nachladen von schadhafter Software ist physikalisch unmöglich. Nur der Hersteller kann mit einem speziellen Adapter direkt am Modul Software installieren.
Zusätzlich hat LCN eine sehr wirksame zweite Sicherheitsebene:

Ein Passwortsystem auf Modulebene: Wenn ein Passwort vergeben ist, kann die Parametrierung weder gelesen noch verändert werden. Die Passwörter sind sehr sicher – ein Ausspähen ist praktisch unmöglich. Speziell für die Zugangskontrolle verfügt LCN auf Busebene über weitere Sicherheitsfunktionen: So kann ein Modul für einen Türöffner im Empfang von Kommandos so begrenzt werden, dass es Befehle nur von wenigen, vorher definierten Modulen annimmt – alle anderen Module werden ignoriert. Das geht so weit, dass man es nur auf sich selbst hören lassen kann – dann ist es „ganz dicht.“ Wenn man diese Funktion dann noch mit Tasten- oder Ausgangssperren verfeinert, haben Angreifer selbst dann keine Chance, wenn sie – wie auch immer – an die Datenader gekommen sind.

Fazit

LCN ist super sicher: ein Angriff ist praktisch unmöglich:

- **Kabelgebunden**
  Störsender haben keine Chance!
- **Auf Wunsch ohne Cloud**
  Ihre Daten bleiben in Ihrem Haus!
- **Software nicht veränderbar**
  Es ist unmöglich, Viren einzuschleppen!
- **Mehrstufiges Passwortsystem**
  Auch im täglichen Betrieb super sicher!

Rufen Sie an!
05066 99 88 55
Unsere Experten sind für Sie da!

ISSENDORFF KG **Perfektion.**
Magdeburger Str. 3 30880 Laatzen T.: 05066 998-0