Foto: www.i-magazin.com

Andreas Kaider schreibt für die Leser des i-Magazins und sorgt so für eine noch größere fachliche Vielfalt.

(Mutmaßlich) Sicheres Eigenheim

Lotte X* gruselt es bei dem Gedanken an das Erlebnis heute noch. Sie hielt sich eines schönen Tages gegen Mittag in der Küche im ersten Stock ihres Eigenheims auf, als sie das Motorgeräusch der Eingangstür im Keller bemerkte. Verunsichert ob der Tatsache, dass sie ihren Partner um diese Uhrzeit nicht zurückerwartete, ging sie der Sache auf den Grund und fand einen fremden in Zivil gekleideten Mann, der ein Paket in der Hand hielt, im Eingangsbereich vor. Nach dem ersten Schreck erfasste Lotte X den Ernst der Lage und konfrontierte den Fremden mit Fragen. Er gab sich als Botendienst aus, der nach einer Lieferadresse suchte und meinte, dass er das Haus betreten hatte, weil die Türe offenstand. Ein Blick auf die Straße und auf das Fahrzeug vor der Türe verriet Lotte X, dass es sich um keinen klassischen Paketdienst handelte – außer einem PKW mit ausländischem Kennzeichen war weit und breit kein anderes Auto zu sehen. Als der Fremde realisierte, dass sich Lotte X mit seinen Erklärungen nicht zufriedengab, verließ er mit dem Satz, er werde die Lieferadresse schon finden, fluchtartig das Haus, sprang in das Fahrzeug und brauste davon.

Bild: AdobeStock

Warum ich Ihnen dieses Szenario schildere, fragen Sie sich? Weil es sich bei dem betreffenden Einfamilienhaus um ein Smart Home mit KNX-Anlage und Gebäudevisualisierung handelte.

Was war geschehen?

Lotte X und ihr Mann hatten vor einigen Monaten von einem Kabelanbieter einen WLAN-Router installiert bekommen, an dem das Heimnetzwerk samt Visualisierung für die KNX-Steuerung angeschlossen wurde. Doch damit nicht genug: Über die Visualisierung konnte auch die Eingangstür geöffnet werden. Trotz der intensiven Warnung des Elektrikers, von einem derartigen Feature abzusehen, da die Gefahr, dass jemand die Anlage hacken könnte, groß war, zeigte sich der Kunde völlig unbesorgt – er meinte nur: „Wen interessiert schon meine Anlage?“

Mit ziemlicher Wahrscheinlichkeit hat sich der Fremde mit dem WLAN-Netzwerk des Einfamilienhauses verbunden, woraufhin er vollen Zugriff auf die Visualisierung und somit auch auf die Türsteuerung der Eingangstür hatte. Die Frage lautet allerdings: Wie kam er in das WLAN-Netzwerk trotz der Verschlüsselung? Darüber können wir nur Mutmaßungen anstellen. User neigen allerdings allzu oft dazu, Router mit voreingestellten Benutzernamen und Passwörtern zu betreiben. Ein Umstand, der es Kriminellen erleichtert, in Netzwerke und in manchen Fällen schließlich auch ins Gebäude einzudringen. Wenn man das Risiko so gering wie möglich halten möchte, ist es daher unumgänglich, ein 15-stelliges Passwort mit Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen zu erstellen und von Zeit zu Zeit zu ändern.

Das taten nun auch Lotte X und ihr Partner. Aber dabei blieb es nicht alleine – um die zweifellos begründeten Bedenken von Lotte X zu zerstreuen und ihr ein größtmögliches Maß an Sicherheit zu vermitteln, hinterlegten wir als zuständige KNX-Techniker eine Zeitsteuerung in der Visualisierung, damit die Türsteuerung (Fingerprint usw.) in der Nacht stromlos und somit funktionsunfähig ist.

Derartige Maßnahmen können allerdings nur gesetzt werden, wenn es die Gebäudeautomatisierung zulässt – bei KNX ist das ein Kinderspiel. Vorausgesetzt, der zuständige Elektrotechniker hat es drauf!

Andreas Kaider ist Systemintegrator, KNX Trainer und DALI Spezialist

**Der Name ist dem Autor bekannt.*