Sauber recherchiert?

Ohne Recherche keine Informationen und kein Beitrag. Welches Thema wähle ich, wo finde ich etwas und vor allem – wer ist der richtige Ansprechpartner für mein Thema. Welchen Aufwand muß ich einplanen und wann ist ein Thema „tot" recherchiert? Recherchieren heißt auch, dass man gezielt nach Informationen sucht – die für den Beitrag richtig sind. Und vor allem benötigt man für einen fundiert recherchierten Beitrag zuverlässige Informationen.

Seit geraumer Zeit gibt es eine Firma, die in eigener Sache unterwegs ist und mit einem Fernsehbeitrag, der ja von starken Bildern lebt, durch die deutschsprachigen Sender „wandert" und sein Wissen über die „Sicherheit" im „SmartHome" verbreitet. Das ist an sich nicht schlimm. Leider tut das der Sache nicht gut, denn dieser Beitrag trägt nur weiter zur Verunsicherung der ohnehin schon verunsicherten Bürger bei, was das „intelligente Haus" betrifft. Das Unternehmen führt eine Kampagne für die Überprüfung von KNX Anlagen. Die in den Beispielen gezeigten Schwächen sind aber planungsverursacht. Im Wesentlichen kommt zum Ausdruck „Dein SmartHome ist nicht sicher" – das wird am Beispiel KNX anschaulich dargestellt, auf Kosten von KNX und deren Nutzern. Im Beitrag werden die Schwächen des Systems aufgegriffen. Die gibt es, man muss sich ihnen stellen und man arbeitet bereits an den Schwachstellen.

Wir finden, es ist an der Zeit, die zu befragen, die tagtäglich den Umgang mit dem „intelligenten Haus" oder dem „Smart Home" haben. Wir befragten den KNX Professionals Deutschland e.V. dazu und baten den Verband um eine Stellungnahme zu diesem Thema, die Sie auf der folgenden Seite finden.

Viel Ehre

In unser komplexer werdenden technischen Welt ist Aufmerksamkeit ein hohes Gut. Große und kleine Firmen beschäftigen viele fleißige Hände und Hirne, um ihre Interessenten Produkte und Lösungen näherzubringen. Aufmerksamkeit ist sicher, wenn David gegen Goliath antritt und wenn es dazu noch um Datensicherheit geht, ist Aufmerksamkeit so gut wie garantiert. Das ist gewiss erst einmal nicht falsch. Es ist aber irreführend, wenn die Sicherheit von Smart Home lediglich aus der Perspektive: "Was da alles passieren könnte..!" geschildert wird. Es ist gar unseriös, wenn sich an solchen Spekulationen die Presse der bewegten Bilder versucht, ohne kompetent nachzufragen.

3 Sat ist in seiner Sendung zur Smarten Welt und in der Wiederholung eines Beitrages in diese Aufmerksamkeitsfalle gegangen. Aber auch durch ständige Wiederholung werden falsche Argumente, wie: KNX ließe sich kinderleicht knacken, nicht richtiger.

Klar, wenn man grundlegende Sicherheitsaspekte (KNX gibt hier detaillierte Instruktionen) ignoriert, kann die Sicherheit eines komplexen Systems ausgehebelt werden. Aber der 3 Sat-Beitrag schenkt falscher Installation und falscher Inbetriebnahme zu viel Beachtung und schreibt das dann dem gesamten System zu. Zu viel Ehre für Pfusch!

Das ist unsauber recherchiert und einseitig dargestellt, liebe Kollegen.

"Audiatur et altera pars". Man höre auch den anderen Teil, ein Grundsatz altrömischer Rechtsprechung und sauberer journalistischer Arbeit, wurde hier dem David gegen Goliath Effekt geopfert.

Das ist nicht die gewohnte Art des Kultursenders 3 Sat. Das ist wie wenn der Geisterfahrer die hohe Anzahl der entgegenkommenden Autos beklagt. Schließlich kann es auch zu einem Sicherheitsproblem werden, wenn ein unbedarfter "Installateur" 230 V direkt an den Türgriff legt. Professionell geht sicher und anders.

Die Redaktion

Den neuen Anforderungen entsprechen

Vorstand der KNX Professionals – von links: Marco Koyne (erster stellvertretender Vorsitzende), Jochen Katzenmeier (Protokollführer), Frank Hujer (Schatzmeister), Dirk Müller (erster Vorsitzender), Dirk Beyer (zweiter stellvertretender Vorsitzender)

„Wenn ich den Schlüssel im Auto stecken lasse, muss ich mich nicht wundern, wenn das Begehrlichkeiten weckt und ungebetene Gäste die Chance nutzen", sagt einer der KNX Professionals gebetsmühlenartig seit Jahren, wenn es um das Thema Sicherheit geht – das brandaktuell ist.

Das System ist nicht schuld, lediglich diejenigen, die ihre Ausbildung als Elektriker nicht ernst nehmen. Oder die selbsternannten Fachleute, die nicht die nötige Qualifikation aufweisen und Anlagen – sozusagen – hinwurschteln.

So z. B. einen Bewegungsmelder IP 20 im Außenbereich planen, anstatt die richtige Alternative, wie den IP 65, anzubieten. Das hat nichts mit KNX zu tun, sondern mit den Grundlagen der Elektrotechnik.

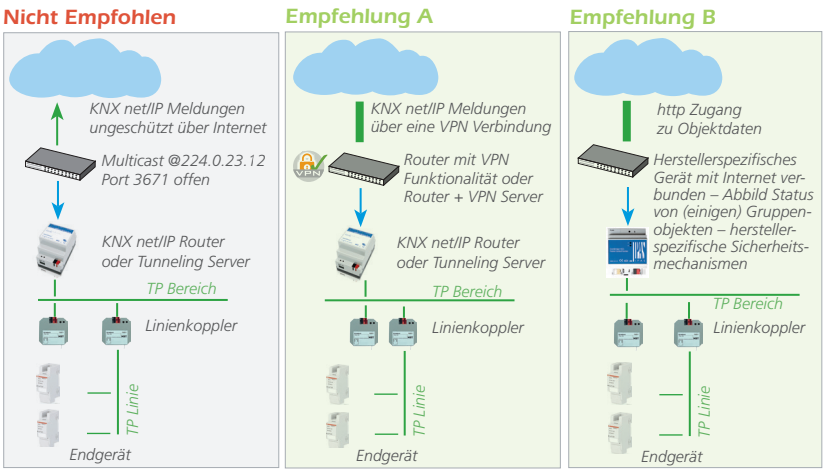
Ein sicheres System ist eine feine Sache, aber wenn beim Router die Firewall abgeschaltet wird und keine Passwörter vergeben werden, dann ist das nicht sicher. Da ist das System aber nicht schuld.

Auch kriminelle Energie, gepaart mit Fachwissen, kann Schaden anrichten. Hacker, die sich den Spaß erlauben, um in fremde Gebäude einzudringen und Schabernack treiben.

Und schlussendlich die paranoiden Vorstellungen, was das Knacken von EIB/KNX Anlagen betrifft. Eher wird der Bademantel aus dem Hotelzimmer entwendet, als dass sich jemand die Zeit nimmt, eine KNX Anlage

Zugang zu KNX Netzwerken über Internet

Kopplung KNX IP ↛ IP Netzwerk ↛ Fernzugriff



Quelle: KNX Secure Position Paper – KNX Association

auszulesen, selbige auszuwerten, um danach Unfug zu treiben. Das braucht Zeit und die wiederum hat ein Einbrecher eigentlich nicht. Es sei denn, er sitzt gemütlich im Hotel und hat nichts anders zu tun. Wie oft aber kommt das vor?

KNX wird bisher schon den Sicherheitsansprüchen gerecht, wenn Installateure der Gebäudesystemtechnik die empfohlenen Schutzmaßnahmen gegen Manipulation beachten.

Mit neuen Medien wie LAN und WLAN, mit Internetzugang, drahtlosen Bedienkonzepten und Anwendungen in sensiblen Bereichen erhöht sich das Schadensrisiko durch unerwünschte Eindringlinge. Diesen und anderen Anforderungen entsprechend, hat KNX neue Sicherheitskonzepte entwickelt: KNX Data Secure und KNX IP Secure. Beide basieren auf weltweit etablierten Sicherheitsprotokollen und können auch in die bestehenden KNX Anlagen nahtlos integriert werden.

In Bussysteme *(2 / 2016, Seite 94 und 95)* finden Sie dazu Ausführungen von der KNX Association zum Thema – KNX IP Secure und KNX Data Secure, die KNX Installationen zugriffssicher machen.

Das größte Problem besteht ja schon vor der Installation – bei der Planung aller Gewerke.

Der Beruf „Systemintegrator" hat seine Berechtigung, denn er sollte an dieser Stelle mit dazugezogen werden.

Das haben die KNX Professionals schon lange erkannt und haben 1998 den „KNX Professionals Deutschland e.V." gegründet. Inzwischen gibt es die KNX Professionals oder auch mitunter KNX Userclubs genannt, in vielen Ländern – sozusagen weltweit. Diese internationale Gemeinschaft wächst ständig und die Mitglieder treiben den Gedanken voran, die Akzeptanz für das KNX System in der Fachwelt und besonders bei den Bauherren, voranzutreiben. Sie sind tagtäglich in ihrer Arbeit damit beschäftigt zu schauen, wie es um die Sicherheit in ihren Projekten steht.

Sie wissen um die Probleme und prüfen bei den Projekten jeweils die wesentlichen Punkte ab – wie Twisted Pair Installation, KNX IP im Gebäude, Kopplung KNX IP ➞ IP Netzwerk, den Fernzugriff auf KNX IP und natürlich auch alles rund um den KNX Funk. Bei der Twisted Pair Installation z. B., ob die Busleitung innerhalb des Hauses geschützt verlegt ist, die KNX Geräte gegen eine einfache Demontage geschützt sind, die Linienbereiche durch Koppler / Router sicher getrennt sind, die Filtertabellen gesetzt und aktiviert sind und sich die Unterverteilungen in Räumen mit gesichertem Zugang befinden.

Eine Menge Informationen und Wissen, welches benötigt wird und es gibt immer wieder Neuheiten zum Thema. Deshalb trifft man sich regelmäßig zur Weiterbildung, um am Ball zu bleiben was die Funktionen und Möglichkeiten der angebotenen Produkte betrifft.

Weitere Informationen zum Thema KNX Sicherheit finden Sie auf der KNX Webseite unter Download > Marketing > Flyer (http://www.knx.org/knx-de/downloads/index.php)

- *KNX Secure Checklist*
- *KNX Secure Positionspapier*

https://KNXSecure.knx.org

Mit dem kostenlosen Webinar „KNX Security" werden Sie aktuell über die notwendigen Schutzmaßnahmen für Ihre KNX Anlage informiert.

Anmeldung unter: http://www.knx.org/knx-de/schulung/knx-eacademy/webinars/index.php