1.1.1 KNX SECURE

KNX/EIB ist in den letzten Jahren aufgrund der eklatanten Sicherheitsproblematik ins Gerede gekommen. Es war lange Zeit jedem bekannt, daß man den KNX/EIB direkt am Draht manipulieren kann. Daß dies tatsächlich in der Öffentlichkeit und mit Schaden geschehen würde, hat jedoch niemand geahnt und erwartet. Unter der folgenden WEB-Seite ist zu lesen:

https://www.golem.de/news/security-smarthomes-offen-wie-scheunentore-1412-111173-6.html

„

KNX oder die Unsicherheit geschlossener Systeme

Das Protokoll KNX und dessen Vorgänger EIB werden seit den frühen 90er Jahren meist in der Gebäudeautomatisierung eingesetzt. Es handelt sich aber nicht um ein drahtloses Übertragungsprotokoll, sondern es dient zur Kommunikation zwischen verkabelten Endgeräten, Switches und Kontrollstationen. In den Spezifikationen heißt es wortwörtlich, dass *"Sicherheit in KNX-Netzwerken eine geringere Rolle spielt, da ein Angreifer einen direkten physischen Zugang zu dem Netzwerk erlangen muss."*

Das noch weit verbreitete "klassische" KNX wurde lediglich durch ein 4 Byte langes Passwort abgesichert, das im Klartext über das Netzwerk versendet wurde. Außerdem sei das Netzwerk deshalb sicher, weil Angreifer "Analysewerkzeuge und Expertenwissen benötigen", um den Netzwerkverkehr zu entziffern. KNX legt seine Spezifikationen nicht offen, sie müssen bei dem Konsortium beantragt werden. Es handelt sich also gewissermaßen um ein geschlossenes System.

KNX zerlegt

Welche Schwachstellen das klassische KNX hat, erklärte der IT-Sicherheitsexperte Aljosha Judmayer auf den Bsides im November 2014 in Wien. Da ist zum einen eine USB-Schnittstelle am Bus, der die einzelnen Sensoren und Geräte miteinander verbindet. Über diesen lässt sich Datenverkehr zwischen den Geräten nicht nur aufzeichnen, sondern auch manipulieren. Dafür gibt es bereits entsprechende Expertenwerkzeuge, etwa Eibd. Judmayer gelang es, sich zu fast allen Schnittstellen des komplexen Systems Zugang zu verschaffen. Schlimmer noch, das offizielle Konfigurationswerkzeug enthielt einen Pufferüberlauffehler.

Allerdings kamen die KNX-Experten wohl zu der Einsicht, dass solche Maßnahmen in der Zukunft nicht unbedingt für erhöhte Sicherheit sorgen werden, und implementierten ein verschlüsseltes IP-Protokoll. Es handelt sich allerdings bislang um einen internen Entwurf, der noch nicht umgesetzt wurde.

Die nächste Version des KNX-Protokolls namens KNXnet/IP Secure mit EIBsec sei aber ebenfalls mangelhaft umgesetzt worden, sagte Judmayer. Denn die offene USB-Schnittstelle am Geräte-Bus ist immer noch vorhanden. Darüber lässt sich weiterhin der Datenverkehr abgreifen. Zwischen den einzelnen Gerätebussen und dem KNX-Backbone, das künftig die verschlüsselte Version des KNX-Protokolls verwendet, befinden sich sogenannte Interconnection Devices. Diese Hardware muss aber physisch ausgetauscht werden, damit auch die Geräte-Busse von der Verschlüsselung profitieren, in einem mehrstöckigen Hochhaus möglicherweise ein kostspieliges Unterfangen. Ohne eine solche Aktualisierung ist auch das neue Protokoll unsicher, dem ohnehin noch weitere entscheidende Sicherheitsfunktionen fehlen, etwa eine ausreichende Verifizierung.

Kostspielige Aktualisierungen

Dass nicht einmal ein direkter Zugriff über die USB-Schnittstelle am KNX-Bus benötigt wird, zeigte der Hacker Jesus Molina, der sich in einem Hotel über eine falsch konfigurierte WLAN-Schnittstelle Zugriff auf dessen KNX-Netzwerk verschafft hat.

Das Beispiel KNX zeigt, wie noch nicht erkannte Probleme bei der Heimautomatisierung in Zukunft noch größere Schwierigkeiten verursachen können, darunter kostspielige Aktualisierungen. Außerdem zeigt KNX deutlich auf, dass auch geschlossene Systeme anfällig für Angriffe sein können, denn

Molina holte sich die benötigten Informationen kurzerhand aus dem Internet.

„
Zusätzlich kann man in der Zeit lesen:

„
Die Zeit

Black Hat:Das gehackte Luxushotel
Ein Hacker hat auf der Black Hat demonstriert, wie er alle vernetzten Geräte in einem Hotel unter Kontrolle brachte. Ein Beispiel für die Mängel im "Internet der Dinge".
Von Patrick Beuth, Las Vegas

Jesus Molina sitzt in einem Hotelzimmer an seinem Laptop und gibt ein Kommando ein. Durch das Fenster hinter ihm ist zu sehen, wie in einem anderen Zimmer das Licht angeht. Molina gibt noch ein Kommando ein und das Licht erlischt. Als der Spanier bemerkt, was seine Aktionen bewirken, reißt er jubelnd und feixend die Arme hoch. Er hat gerade erfolgreich ein Hotel gehackt.

Die Szene ist schon ein paar Monate alt, Molina zeigt sie am Mittwochabend auf der Black-Hat-Konferenz in einem Video, das er selbst aufgenommen hat. Sein Vortrag gehört zu den unterhaltsameren in Las Vegas, aber Molina hat eine ernst gemeinte Botschaft.

Zunächst jedoch erzählt er die Geschichte vom gehackten Hotel. Es handelt sich um das St. Regis in Shenzen, China, ein Fünf-Sterne-Hochhaus der Starwood-Kette. In fast jedem Zimmer dort liegt ein iPad, mit dem Gäste die Vorhänge, die Klimaanlage, den Fernseher und einige andere Dinge steuern können.

Als der Sicherheitsberater Molina dort im vergangenen Jahr übernachtete, fragte er sich sofort, ob er die Zimmertechnik nicht auch mit seinem Laptop steuern könnte. Wie sich herausstellte, war das nicht schwer. Das iPad in seinem Zimmer war mit dem Gäste-WLAN vernetzt, er konnte die Verbindung problemlos analysieren. Während dieses ersten Aufenthalts tat er aber nichts weiter als den Netzwerkverkehr aufzuzeichnen.

Erst als er zum zweiten Mal in dem Hotel übernachtete, sah er sich die Daten genauer an. Er bemerkte, dass das iPad und die vernetzten Dinge über einen uralten Standard namens KNX kommunizierten. KNX wurde in den neunziger Jahren für die Gebäudeautomation, also für die Steuerung von Gebäudesystemen, entwickelt. Der Standard beinhaltete zumindest bis zum Jahr 2013 keinerlei Sicherheitsvorkehrungen, schon gar nicht für WLAN-Verbindungen, für die es nicht gedacht ist.

So war es für Molina kein Problem, im Netzwerk jene Kommandos zu identifizieren, mit denen Vorhänge oder Fernseher oder Lampen in seinem Zimmer gesteuert wurden. Er fand heraus, dass jeder vernetzte Gegenstand eine Nummer zugewiesen bekam, die aus drei Teilen bestand. 2/2/3 zum Beispiel konnte der Fernseher sein, 2/2/4 eine Lampe. Und weil das iPad sich gegenüber Fernsehern und Lampen nicht authentifizieren musste, konnte Molina diese Geräte-Adressen auch mit seinen Laptop ansteuern.

Auch die Steuerung aus der Ferne wäre möglich
Molina wurde noch ein wenig neugieriger. Drei Mal verlangte er ein neues Zimmer, jedes Mal mit der Begründung, das bisherige gefalle ihm nicht. In jedem Zimmer untersuchte er das Netzwerk und die Adressen der vernetzten Geräte – und fand ein Muster. 2/2/3 war der Fernseher im ersten Zimmer, 2/4/3 der im zweiten Zimmer und so weiter. Innerhalb weniger Stunden schrieb er ein Programm, mit dem er jedes Gerät in jedem Zimmer ansteuern konnte, wenn auch nicht gleichzeitig. Das wäre möglich gewesen, aber Molina hatte ein wenig Angst, dass die Chinesen ihm seinen Hack übel nehmen und ihn verhaften lassen würden. Selbst eine Fernsteuerung der iPads wäre machbar

gewesen, sagt er, dann hätte er die Geräte bedienen können, ohne selbst im Hotel sein zu müssen.

Molina gab sich mit seinem simplen Programm zufrieden. Dass es funktionierte, merkte er in der Szene, die er auf Video festgehalten hat und die beim Publikum in Las Vegas für großes Gelächter sorgte.
Als er zum vierten Mal nach einem anderen Zimmer fragte und sogar eine Suite bekam – das schönste Zimmer, in dem er jemals war, wie er sagt – endete sein Experiment. Die Suite hatte nämlich kein iPad. Der Spanier wollte sich aber nicht noch einmal beschweren, es wäre einfach unglaubwürdig gewesen.

Er habe das Hotel über die Schwachstelle informiert, sagt er, und das Unternehmen habe sehr gut reagiert. Molina hält es aber für wahrscheinlich, dass andere Hotels auf eine ähnliche Technik setzen und ebenso anfällig für solche vergleichsweise einfachen Attacken sind. Die Hilton-Kette etwa baut sogar ihre Türschlösser so um, dass Gäste sie mit ihrem Smartphone öffnen können. Ob die Technik sicher ist, wird sich vielleicht auf der nächsten oder übernächsten Black Hat zeigen.

Molina warnt vor einem solchen sogenannten Internet der Dinge, in dem Sicherheit nur eine nachgeordnete Rolle spielt. Das Problem seien nicht Witzbolde wie er, die in den Zimmern von anderen das Licht ein- und ausschalten. Das Problem sei eher eine Regierung, die sich entscheidet, alle Fernseher an einem Ort aus der Ferne zu steuern, damit jeder Mensch die Ansprache des Präsidenten sieht. Es ist ein dystopischer Gedanke, der an Orwells 1984 erinnert und vielleicht nicht die realistischste aller Visionen zum Internet der Dinge, in dem alles mit allem vernetzt ist.

Schwachstellen in jedem vernetzten Gerät
Aber Molinas amüsanter Hotel-Hack ist ein Beispiel für die Schwachpunkte solcher Systeme. In Las Vegas geht es in mehreren Vorträgen um dieses Problem, sowohl auf der Black Hat wie auch der anschließenden DEF CON. Der Sicherheitsforscher Logan Lamb wollte zum Beispiel erklären, wie er eine Alarmanlage austrickste, weil sie auf einem uralten Kommunikationsprotokoll basierte, in dem nichts verschlüsselt oder authentifiziert wird. Der Vortrag wurde allerdings kurzfristig abgesagt – warum, ist unklar.

Dafür wollen vier Sicherheitsforscher am Samstag auf der DEF CON in nur 45 Minuten zeigen, wie sie 20 verschiedene Haushaltsgeräte gehackt haben, vom Baby-Monitor bis zu ganzen Gebäudesystemen.

Es ist zwar keine wirkliche Neuigkeit mehr, dass es im Internet der Dinge vor Sicherheitslücken wimmelt. Zuletzt hat das Unternehmen HP eine Studie veröffentlicht, nach der sich im Schnitt 25 Schwachstellen in jedem vernetzten Haushaltsgerät befinden. Der vernetzte Haushalt ist dennoch seit Jahren eine Vision der Industrie. Dass aus der Vision nicht längst Wirklichkeit geworden ist, hat mehrere Gründe.

Zum einen dürften viele Menschen ganz einfach nicht an einem vernetzten Haus interessiert sein, weil sie sich keine großen Vorteile davon versprechen. Zum anderen sorgen Aktionen wie die von Molina und den anderen Hackern dafür, dass die Menschen dem ganzen Konzept – zurecht – misstrauen. Es wird wohl noch einige gehackte Hotels und Alarmanlagen brauchen, bis die Hersteller und diejenigen, die solche Technik letztlich implementieren, das verstanden haben. „

Desweiteren wurde in 3sat ein Film über die Unsicherheit des KNX/EIB präsentiert:

„Wissen
Smart Living: Wie clever ist die Zukunft?
Wir leben in einer smarten Welt. Intelligente Geräte sollen uns im Alltag aktiv unterstützen: zu Hause, im Auto, am Flughafen. Schleichend übernehmen Geräte das Regiment. Ist das wirklich schlau?

DATUM: 29.04.2016

https://www.3sat.de/wissen/wissenschaftsdoku/smart-living-100.html „

Auch HomeMatic und ZigBee sind unsicher, die Nutzung der 868 MHz-Basisfrequenz ist unsicher weil aufgrund der 1%-Regel Telegramme gar nicht ankommen.

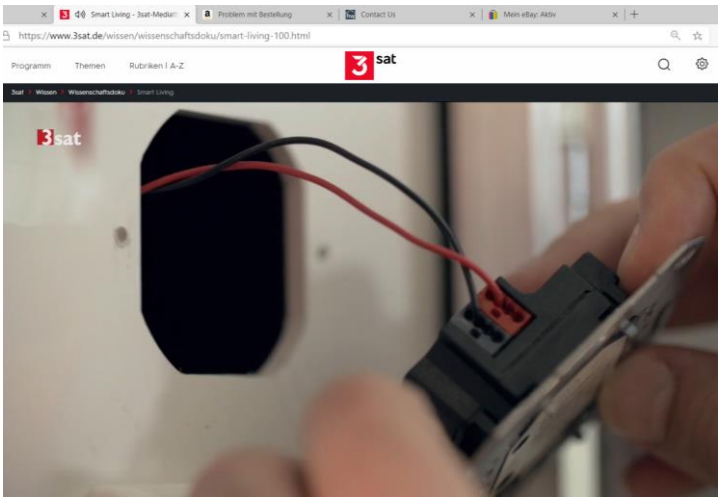

Abb. **Fehler! Kein Text mit angegebener Formatvorlage im Dokument.**.1 2 simple Drähte an jedem Gerät und man ist Herr des KNX [3sat-Video]

An den 2 Drähten wird eine Schnittstelle angeschlossen und schon kann man den Bus, wie auch das Ethernet im Haus einsehen. Ohne Verschlüsselung ist dies grob fahrlässig.

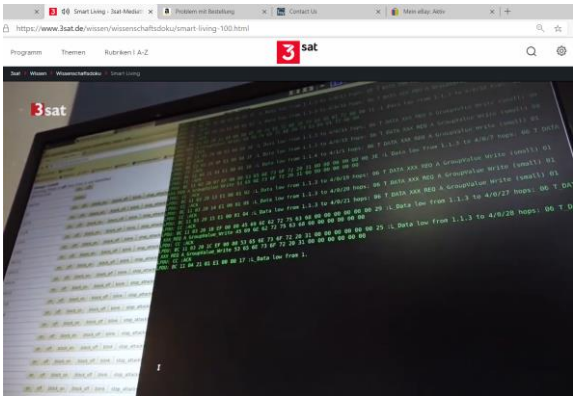

Abb. **Fehler! Kein Text mit angegebener Formatvorlage im Dokument.**.2 Protokollierung des Internet-Datenverkehrs [3sat-Video]

Ist man dann durch die Sicherheitslücken des KNX in das Haus eingedrungen und hat die Wohnung leer geräumt, hilft auch eine Versicherung nicht mehr.

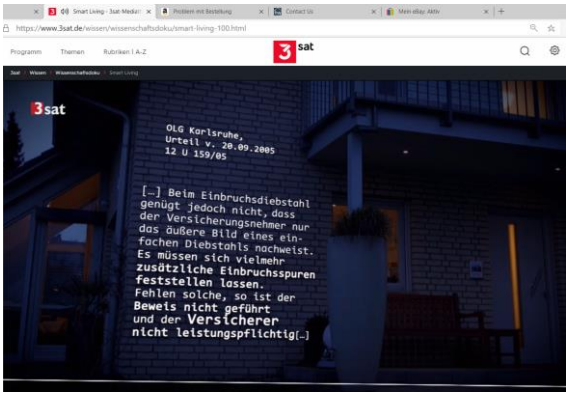

Abb. **Fehler! Kein Text mit angegebener Formatvorlage im Dokument.**.3 Gerichtsurteil zum Wohnungseinbruch [3sat-Video]

Das Unternehmen Lingg&Janke hat sich dieser Problematik gestellt und KNX secure auf den Markt gebracht. Die Telegramme des KNX kann man auf dem Bus zwar nach wie vor sehen, ohne Schlüssel, den nur der Hausherr hat, können jedoch keine Übersteuerungen des Systems erfolgen.

Abb. **Fehler! Kein Text mit angegebener Formatvorlage im Dokument.**.4 KNX secure

Der eindeutige Schlüssel wird einmalig bei der Parametrierung angewendet.

Abb. **Fehler! Kein Text mit angegebener Formatvorlage im Dokument.**.5 Der noch uncodierte Schlüssel befindet sich auf jedem Gerät im Haus

Bedauerlicherweise hat die Corona-Pandemie die Markteinführung behindert.

Dieser Hersteller hat zudem alles Notwendige zur Verfügung, um aus dem KNX/EIB in der Version 1.0 die Verion 2.0 zu machen. Im Gespräch mit Peter Janke, einem Geschäftsführer der Firma Lingg&Janke aus Radolfzell stellte sich heraus, daß KNX secure fertiggestellt wäre, ja es wurde sogar vollständig vorgeführt, aber die Zertifizierung über die Konnex in Brüssel ginge nur schleppend voran, ein anderer etwas größerer Player in der KNX-Allianz, die Firma Jung, hätte bereits eine marktfähige Lösung angekündigt, aber nicht präsentabel. Man war sich einig, daß KNX secure eine wesentliche Versionsänderung für den KNX/EIB wäre, die auch andere negative Merkmale des KNX/EIB

verbessern könnte. Hierzu zählen die viel zu geringe Funktionsanzahlmenge (Gruppenadressen), die leicht durch 2 Bits auf mehr als 100.000 Funktionen gesteigert werden könnte, die Protokollgröße, die leicht durch Einschränkung reduziert werden könnte, um die gesamte Performance zu steigern, sowie die Geschwindigkeit auf dem Bus selbst, die beim Vergleichssystem LON bei bis zu 38.400 Baud sein kann, immerhin das Vierfache der aktuellen Baudrate des KNX/EIB von 9.600 Baud. Letztendlich könnte auch die Inbetriebnahme der KNX/EIB-Geräte optimiert werden (Knöpfchen drücken), in dem QR-Codes mit dem Handy gescannt werden könnten. Diese Verbesserungsvorschläge wurden den Verantwortlichen der Konnex in Brüssel, Herrn Lux und Herrn Demarest, per Brief vorgeschlagen, eine Stellungnahme blieb jedoch aus.