IT-Sicherheit im Handwerk

Hausautomatisierung

IT-Sicherheit im Haus der Zukunft

Dozentenhandbuch

Gefördert durch:

Bundesministerium für Wirtschaft und Energie

aufgrund eines Beschlusses des Deutschen Bundestages

TASK FORCE
IT-SICHERHEIT IN DER WIRTSCHAFT
Mehrwert und Schutz für Rechner.

Das diesem Buch zugrundeliegende Verbundvorhaben "IT-Sicherheitsbotschafter im Handwerk - qualifizierte, neutrale Botschafter für IT-Sicherheit im Handwerk finden, schulen und Awarenesskonzepte erproben (ISiK)" wurde mit Mitteln des Bundesministeriums für Wirtschaft und Energie (BMWi) im Rahmen der Task Force "IT-Sicherheit in der Wirtschaft" gefördert und durch den Projektträger im Deutschen Zentrum für Luft- und Raumfahrt (PT-DLR) betreut.

Die Task Force "IT-Sicherheit in der Wirtschaft" ist eine Initiative des Bundesministeriums für Wirtschaft und Energie, die gemeinsam mit IT-Sicherheitsexperten aus Wissenschaft, Wirtschaft und Verwaltung vor allem kleine und mittelständische Unternehmen für IT-Sicherheit sensibilisieren und dabei unterstützen will, die Sicherheit der IKT-Systeme zu verbessern. Weitere Informationen zur Task Force und ihren Angeboten sind unter: *www.it-sicherheit-in-der-wirtschaft.de* abrufbar.

Herausgeber:

Institut für Technik der Betriebsführung (itb) im
Deutschen Handwerksinstitut (DHI) e.V.
Kriegsstraße 103a • 76135 Karlsruhe (Konsortialführer)

Kompetenzzentrum IT-Sicherheit
und Qualifizierte Digitale Signatur (KOMZET) der
Handwerkskammer Rheinhessen
Dagobertstraße 2 • 55116 Mainz (fachliche Leitung)

Westfälische Hochschule
Institut für Internet-Sicherheit – if(is)
Neidenburger Straße 43 • 45877 Gelsenkirchen
(Kooperationspartner)

Interessengemeinschaft des Heinz-Piest-Instituts für Handwerkstechnik (HPI) an der Leibniz-Universität Hannover
Wilhelm-Busch-Straße 18 • 30167 Hannover
(Kooperationspartner)

ISBN **978-3-944916-12-5**

Verlag: Handwerkskammer Rheinhessen
Dagobertstraße 2 • 55116 Mainz
www.hwk.de

Autorenteam

Sascha Remmers

Elektrotechnikermeister und Betriebswirt (HWK). Seit 2008 im technischen Vertrieb von Gebäudeautomationssystemen tätig. Derzeitiger Arbeitgeber: LOYTEC electronics GmbH mit Hauptsitz in Wien.

Falk Gaentzsch

Bachelor of Science und wissenschaftlicher Mitarbeiter am Institut für Internet-Sicherheit – if(is) an der Westfälischen Hochschule in Gelsenkirchen. Projektleiter für das Projekt „IT-Sicherheit im Handwerk“.

Schwerpunkte:
IT-Sicherheit & Awareness
Cloud-Computing
Virtualisierung

Prof. Norbert Pohlmann

Informatikprofessor für Verteilte Systeme und Informationssicherheit sowie geschäftsführender Direktor des Instituts für Internet-Sicherheit - if(is) an der Westfälischen Hochschule in Gelsenkirchen.

Einleitung

IT-Sicherheit ist nicht nur ein Thema für Computer, von gleicher Bedeutung ist sie für Automationsnetzwerke, wie sie heutzutage in Gebäuden eingesetzt werden.
Bei Neubauprojekten im Bereich Nichtwohngebäude (zum Beispiel Büro- und Verwaltungsgebäude) sind Gebäudeautomationssysteme derzeit kaum noch wegzudenken. Grund für den Einsatz sind zahlreiche Vorteile bei Themen wie Energieeffizienz, Gebäude- und Energiemanagement, Komfort, Nutzungsflexibilität.
Aber auch bei Wohngebäuden, beziehungsweise Privathäusern ist ein immer größer werdendes Interesse für Automationssysteme festzustellen. Einer Studie[1] zufolge wird dem Markt für sogenannte Smart-Home-Systeme ein Gesamtjahresumsatz in Deutschland von 2,4 Mrd. Dollar bis zum Jahre 2017 prognostiziert (2011 ca. 400 Mio. Dollar). Demnach sollen bis dahin bis zu 22 Prozent der deutschen Haushalte, die über Breitbandtechnik verfügen, mit einem Smart-Home-System ausgestattet sein. Der Wunsch, ihre Smartphones und Tablet-PCs mit der Haustechnik zu vernetzen, sei dabei der ausschlaggebende Motivationsfaktor für die Verbraucher. Sie wollen nicht nur in der Lage sein, Energiemanagement durchzuführen, sondern auch weitere Systeme – wie Videokameras, Bewegungsmelder und Heim-Unterhaltungssysteme- übers Internet überwachen und steuern können. (Arnold, 2012)

Wie auch immer sich Automations-, Fernüberwachungs- und andere Funktionen im „Haus der Zukunft“ noch entwickeln werden, eines steht schon heute fest:
Je komplexer die technischen Systeme werden und je weiter die digitale Vernetzung in Gebäuden voranschreitet, desto kritischer müssen die damit verbundenen Sicherheitsaspekte betrachtet werden. Wie kann ich mein intelligentes Gebäude gegen unerwünschte Zugriffe schützen? Wie kann ich verhindern, dass jemand den Datenverkehr meines Automationssystems „belauscht“, um daraus Rückschlüsse auf bestimmte Verhaltensgewohnheiten oder Anwesenheitsmuster zu ziehen, um einen Einbruch zu planen. Welche Möglichkeiten gibt es, um eine Anbindung der Haustechnik ans Internet so abzusichern, dass niemand unberechtigter Weise die Kontrolle über mein Haus übernehmen kann?

Dieses Dozentenhandbuch soll die Zusammenhänge von IT-Sicherheit und Gebäudeautomation aufzeigen und auf die Gefahren aufmerksam machen. Es werden unter anderem verschiedene Kommunikationsprotokolle für die Datenübertragung, die in der Praxis für Gebäudeautomationssysteme eingesetzt werden, erläutert und vor dem Hintergrund der IT-Sicherheit beleuchtet.

Anmerkung zu den Beispielen in diesem Handbuch

Die Betriebe, Angriffsszenarien und Schadensbeispiele in diesem Handbuch sind frei erfunden und sollen nur die möglichen Auswirkungen von Fehlern und Angriffen verdeutlichen.

[1] *Studie: Strategy Analytics Inc. - Smart Home Strategies 2012*

Seminarziele

Ziel dieses Handbuchs ist es, Ihnen den Hintergrund und die technischen Grundlagen zum Verständnis von IT-Sicherheit in der Gebäudeautomation an die Hand zu geben.

Anhand von Beispielen werden mögliche Angriffsvektoren auf Automationsnetzwerke in Gebäuden und auch Lösungsansätze und Möglichkeiten der Umsetzung präsentiert. Der Fokus wird hierbei auf den Bereich Wohngebäude/Privathäuser (sogenannte „Smart-Home-Systeme“) gelegt.

Am Ende dieses Seminars sind Sie in der Lage:

- Kommunikationsprotokolle und Technologien der Haus- und Gebäudeautomation im Kontext der IT-Sicherheit zu hinterfragen und zu bewerten
- Lösungsansätze zu vermitteln
- Betriebe zu sensibilisieren

Inhaltsverzeichnis

1. Möglichkeiten der Gebäudeautomation

Der Begriff Gebäudeautomation ist in der Norm EN ISO 16484 wie folgt definiert:

Bezeichnung der Einrichtungen, Software und Dienstleistungen für automatische Steuerung und Regelung, Überwachung und Optimierung sowie für Bedienung und Management zum energieeffizienten, wirtschaftlichen und sicheren Betrieb der Technischen Gebäudeausrüstung.
(DIN EN ISO 16484-2, 2004)
Nach dem Gebäudetyp, in dem Gebäudeautomationssysteme eingesetzt werden, lassen sich diese grundsätzlich kategorisieren in

- Systeme für Wohngebäude (Privathäuser, Mehrfamilienhäuser)
  Hierbei wird eher der Begriff „Gebäudesystemtechnik“ verwendet
- Systeme für Nichtwohngebäude (Bürogebäude, Schulen, Hotels).

Die drei wesentlichen Aufgaben der Gebäudeautomation

- Überwachung
- Steuerung
- Regelung

werden im Folgenden erläutert.

Die drei Hauptaufgaben der Gebäudeautomation sind Überwachung, Steuerung und Regelung

Überwachung

Automatisch ausgeführte Systemaktivität zur Beobachtung des Ist-Zustandes einer Einheit und Signalisierung einer definierten Abweichung vom Normalzustand als Zustandsmeldung über das Ereignis.

Beispiel:
Ein Sensor (siehe Kapitel 2.3.1) misst in einer Heizungsanlage eine Temperatur. Dieser Wert wird über das Gebäudeautomationsnetzwerk grafisch auf einem zentralen Leitrechner visualisiert. Wenn der gemessene Temperaturwert einen definierten Wert über-, beziehungsweise unterschreitet, wird dies entsprechend grafisch signalisiert und/oder eine Alarmmeldung wird ausgelöst, beziehungsweise versendet (E-Mail, SMS).

Steuerung

Vorgang, bei dem eine oder mehrere Eingangsgrößen (zum Beispiel die Stellung eines Schalters) die Ausgangsgrößen (zum Beispiel die Beleuchtung) beeinflussen.

Beispiel:
Dimmen einer Lampe durch Betätigung eines Tasters.

Regelung

System, bei dem der Ausgabewert in solcher Weise auf einen Prozess einwirkt, dass die Differenz zwischen dem gemessenen Wert und dem angestrebten Sollwert im Sinne einer Angleichung bis auf den Wert 0 vermindert wird.

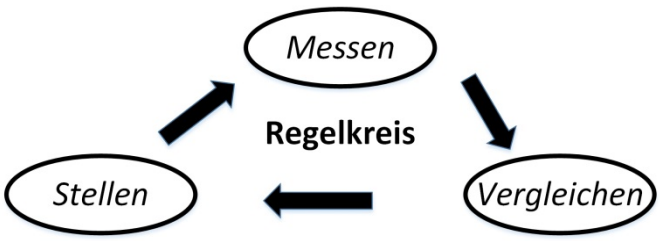


Abbildung 1: Regelkreis

Beispiel Raumtemperatur:

Über einen Sensor (siehe Kapitel 2.3.1) wird die aktuelle Raumtemperatur gemessen (Regelgröße/Istwert). Der Istwert wird als Eingangswert an eine Regelungslogik gesendet (beispielsweise über einen Bus[2]). Die Logik vergleicht den Istwert mit einem Sollwert, der entweder fest eingestellt ist oder verändert werden kann (ebenfalls über einen Bus). Aus einer etwaigen Differenz zwischen Ist- und Sollwert berechnet die Logik einen Stellwert, welcher an einen Aktor (siehe Kapitel 2.3.1) gesendet wird. Der Aktor wandelt den Stellwert in ein elektrisches Signal um (0-10V) und steuert so einen Heizungsstellantrieb an. Dies geschieht solange, bis die Differenz zwischen Ist- und Sollwert ausgeregelt (also = 0) ist.

Während Überwachung „nur" datenschutztechnisch kritisch sein kann, so kann aus Missbrauch von Steuerung und Regelung unmittelbar ein (finanzieller) Schaden folgen.

Wie viel Überwachung, Regelung oder Steuerung vorhanden ist, hängt von der Größe und vom Umfang der Automatisierung des Gebäudes ab.

Smart-Home

Speziell im Bereich Eigenheim fällt häufig das Wort Smart-Home.

Smart-Home ist ein Sammelbegriff für technische Systeme und Verfahren, die die Steigerung von Wohnqualität, Energieeffizienz und Sicherheit zum Ziel haben. Die folgenden Punkte zeigen auf, was der Begriff Smart-Home umfassen kann:

- Haustechnik (Lichtsteuerung, Alarmanlagen, Heizungs- und Jalousien-/Rollladen-Steuerungen etc.)
- Smart-Metering (Elektrische-Energiezähler, Wasserzähler, Gaszähler, Wärmezähler)
- Elektrohaushaltsgeräten (Herd, Kühlschrank, Waschmaschinen etc.)
- Multimedia-Geräten (Fernseher, Videorekorder, Tuner, zentraler Server etc.) und
- Internetanbindung

[2] *Ein Bus ist ein System zur Datenübertragung zwischen zwei oder mehr Teilnehmern.*

1.1 Vor- und Nachteile

Der Einsatz von Automationstechnik in Gebäuden kann für den Nutzer verschiedene Vorteile, aber auch einige zu berücksichtigende Nachteile bringen. Die wichtigsten Vor- und Nachteile sind im Folgenden aufgelistet.

Grundsätzlich gilt es, in der Gebäudeautomation Vorteile wie Komfort oder Energieeinsparungen gegen Nachteile wie hohe Kosten und IT-Sicherheitsrisiken abzuwägen

Beispiele für Vorteile

- Energieverbrauchsreduktion durch intelligente Regelung
- Komfortgewinn durch intelligente Steuerung: zum Beispiel kann auf einen Tastendruck eine vordefinierte Beleuchtungssituation hergestellt werden, ohne dass mehrere Lampen einzeln geschaltet oder gedimmt werden müssen; oder durch logische Verknüpfungen von Schaltzuständen können alternativ definierte Aktionen ausgelöst werden
- Schutz gegen Einbrüche durch Anwesenheitssimulation
- Sicherheit für die Bewohner durch Alarmierung beim Auftreten von kritischen Situationen
- Überwachung von einem externen Sicherheitsdienst durch automatische Alarmweiterleitung

Beispiele für Nachteile

- Höhere Anschaffungskosten im Vergleich zur normalen Gebäudeinstallation. Zum einen amortisieren sich aber die Kosten vielfach durch die Energieeinsparungen im Betrieb, zum anderen sind viele Funktionen mit klassischer Gebäudeinstallation gar nicht möglich oder viel teurer.
- Bei hoher Komplexität ist für den Betrieb der Anlagen qualifiziertes Personal notwendig.

Einige Smart-Home-Systeme haben noch keine adäquaten IT-Sicherheitsfunktionen implementiert und sind somit anfällig für Hackerangriffe (Schürmann, 2014)

1.2 Smart-Meter

Mit Smart-Meter werden intelligente Energiezähler (Strom, Wasser, Gas) bezeichnet. Dabei handelt es sich um Geräte, die die gemessenen Verbrauchswerte digitalisieren und über einen Bus versenden können. Smart-Meter können somit die Verbrauchswerte zum Versorgungsunternehmen senden, oder auch in einem Gebäudeautomationssystem integriert sein, um die Verbrauchswerte für ein Energiemanagement zu verwenden. Ein häufig verwendetes Protokoll für Smart-Meters ist M-Bus (siehe Kapitel 2.8.5).

1.3 Smart-Grid

Das sogenannte Smart-Grid gilt als wichtiger Baustein der Energiewende.
Einerseits soll es durch intelligente Vernetzung gelingen, die Einspeisung von Energie aus erneuerbaren Quellen (Windkraft, Solartechnik) zu optimieren, indem beispielsweise durch verbesserte Spannungsmessung effizienter die Auslastung von herkömmlichen Kraftwerken reguliert wird. Andererseits soll über intelligente Stromzähler der Verbrauch von Haushalten im Minutentakt gemessen und mit der aktuellen Lage der Stromversorgung abgeglichen werden.
Wenn zeitweilig viele Wind- und Solaranlagen arbeiten, sollen die Preise sinken, da das Angebot an Strom augenblicklich sehr hoch ist. Der intelligente Zähler sollen dann die Aufgabe haben, dies zu registrieren und dafür zu sorgen, dass zu diesen Zeiten im Haushalt die „Stromfresser“ wie Waschmaschine und Trockner arbeiten oder zum Beispiel auch ein Elektroauto aufladen.
Die Anschaffungskosten sind hier erst einmal hoch. Benötigt wird zunächst ein intelligenter Stromzähler und natürlich müssten auch Waschmaschine und Trockner über eine Möglichkeit verfügen, mit dem Zähler zu kommunizieren.
Aber nicht nur die Kosten erklären die Zurückhaltung der Verbraucher:
Nach einer Umfrage des Verbraucherportals Check24 und der Hochschule Weihenstephan-Triesdorf unter 8000 Stromkunden gaben 42% der Befragten an, Bedenken beim Datenschutz zu haben. (Check24, 2012)

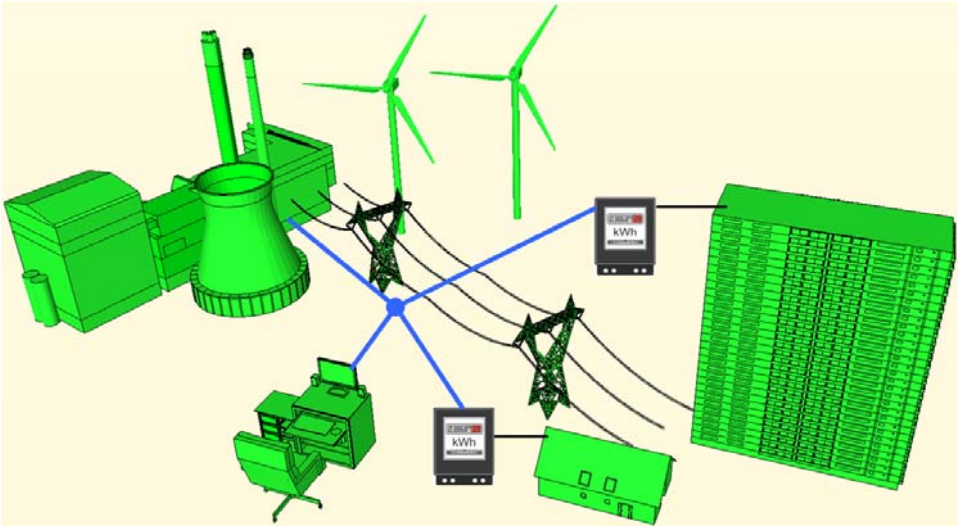


Abbildung 2: Darstellung einer Smart-Grid-Infrastruktur

2. Technische und funktionale Grundlagen

Im Folgenden werden einige der wichtigsten drahtgebundenen wie drahtlosen Technologien vorgestellt, die sich am Markt der Gebäude- und Hausautomation etabliert haben. Darüber hinaus dient dieser Abschnitt der Erklärung von grundlegenden Begriffen.

2.1 Einführung und Überblick

Wie in den vorangegangenen Kapiteln erläutert, geht es für den Nutzer eines automatisierten Gebäudes u.a. darum, dass sein Gebäude durch intelligente Steuerung und Regelung energieoptimiert betrieben wird und dass sich komfortable Steuerungsfunktionen sowohl im Gebäude als auch aus der Ferne (übers Internet) umsetzen lassen.

Technisch gesehen ist für all dies vor allem eins Grundvoraussetzung:
Verschiedene elektronische Geräte müssen untereinander Daten austauschen.

Ein Kommunikationsprotokoll ist das Regelwerk für einen Datenaustauschprozess zwischen zwei Teilnehmern.

Um das zu ermöglichen, müssen sich alle an einem Datenaustauschprozess beteiligten Kommunikationsteilnehmer (Sensoren und Aktoren [siehe Kapitel 2.3.1]) an bestimmte Regeln halten. Das Regelwerk, welches diese Kommunikationsregeln definiert, wird Kommunikationsprotokoll genannt.

Hierin ist u.a. festgelegt:

- Welche Medien für den Austausch von Daten genutzt werden können (drahtgebunden oder Funk)
- Wie eine Botschaft (Datentelegramm) beginnt und endet
- Was mit beschädigten oder falsch formatierten Botschaften getan wird
- Wie und wann eine Verbindung beendet wird

Auch die Aspekte der IT-Sicherheit sind hier festgelegt, unter anderem ob die Daten verschlüsselt übertragen werden, oder ob es Mechanismen zur Authentifizierung der Kommunikationsteilnehmer gibt.
Für Automationsnetzwerke in Gebäuden existiert eine Reihe von Kommunikationsprotokollen am Markt.

Zu den wichtigsten zählen heute u.a.

- BACnet
- KNX
- LON

als drahtgebundene und

- Z-Wave und
- ZigBee

als drahtlose Technologien.

Allen gemeinsam ist, dass es sich um standardisierte Protokolle handelt.

Für Bauherren und Nutzer hat dies u.a. den Vorteil, dass sie sich nicht von einem Hersteller abhängig machen, sondern dass am Markt eine Vielzahl von Herstellern existieren, die Produkte basierend auf diesen Standards entwickeln. Damit ist eine herstellerunabhängige Kommunikation einzelner Geräte möglich. Der Einsatz von Produkten, deren Kommunikationsprinzip auf einer standardisierten Technologie – wie die zuvor erwähnten – beruht, ist daher empfehlenswert.

2.2 Ebenen der Gebäudeautomation

Die Netzwerkstruktur eines Gebäudeautomationssystems lässt sich heutzutage in einem zweistufigen Modell darstellen.

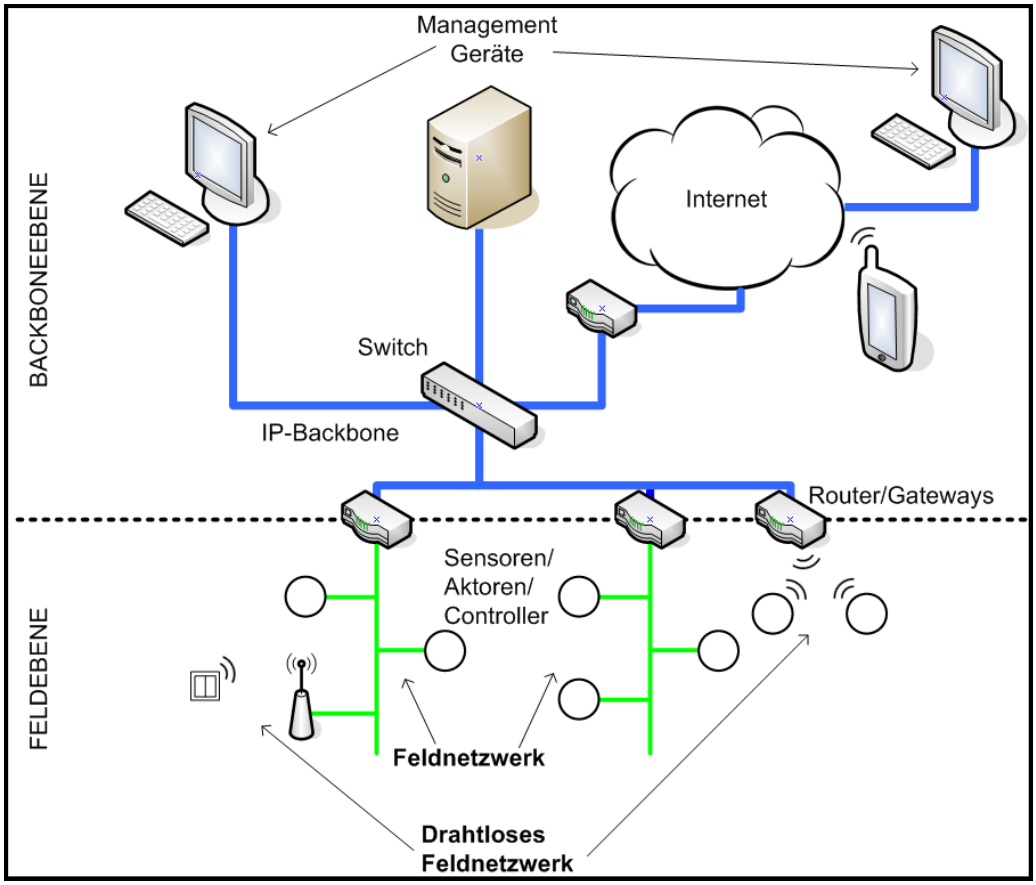


Abbildung 3: Gebäudeautomationsnetzwerk mit Feld- und Backboneebene

Feldebene

Die Feldebene beinhaltet intelligente Feldgeräte (wie Sensoren, Aktoren und Controller [siehe Kapitel 2.3.1]), durch deren kommunikatives, funktionales Interagieren üblicherweise lokale Automatisierungsaufgaben realisiert werden (eine Raumtemperaturregelung oder auch die Regelung einer Lüftungsanlage).
Für die Geräte, die hier eingesetzt werden, sind vor allem Flexibilität, Robustheit und Kosteneffizienz wichtige Kriterien. Als Übertragungsmedien für die Kommunikation der einzelnen Automationsgeräte dienen hier häufig verdrillte Zweidrahtleitungen (siehe Abbildung 4), eine vorhandene 230V-Leitung oder per Funk. Es gibt auch Feldgeräte

am Markt, die einen Netzwerkanschluss haben und somit direkt über eine Netzwerkleitung kommunizieren.

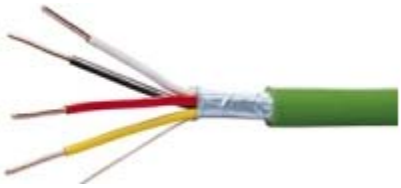


Abbildung 4: Installationsleitung J-Y(St)Y 2x2x0,8 mit verdrillten Aderpaaren, Foto: Elektro-Wandelt

Backbone Ebene

Ein Gebäudeautomationsnetzwerk lässt sich in eine Feld- und eine Backboneebene unterteilen.

Über einen sogenannten Backbone werden die einzelnen Feldnetzwerke verbunden. Daten aus dem gesamten Gebäudenetzwerk laufen hier auf, weshalb dafür hoch performante Netzwerktechnologien bevorzugt werden. In der Gebäudeautomation haben sich vor allem Internet Protocol (IP) -basierte Netzwerke etabliert. Erstens sind diese Netzwerke oft ohnehin schon im Gebäude vorhanden (Computer-Netzwerke) und zweitens wird die Errichtung und Verkabelung von IP-Netzwerken immer kostengünstiger.

2.3 Allgemeine Begriffe

Im Folgenden werden die wichtigsten Komponenten, die zu einem Gebäudeautomationsnetzwerk gehören können, vorgestellt.

2.3.1 Komponenten

Sensoren

Ein Sensor ist ein technisches Bauteil, das physikalische (Temperatur oder den Druck auf einen Schalter) oder chemische (CO_2- Gehalt der Luft) Größen misst und diese in ein elektrisches Signal umwandelt, damit der Messwert von einer übergeordneten Steuerung oder Regelung weiterverarbeitet werden kann.

Abbildung 5: Multisensor zur Messung von Licht und Präsenz, Foto: Copydon

Aktoren

Unter einem Aktor wird ein Ausgabegerät mit Bus- oder Netzwerk-Kommunikation verstanden, welches beispielsweise zur Ansteuerung einer Last, eines Schalt- oder Stellgerätes dient. Das Ein- und Ausschalten einer Lampe kann über einen sogenannten Schaltaktor realisiert werden, der ein oder mehrere Relais[3] enthält, über die die Lampe geschaltet wird.

Controller

Ein Bauteil, welches in der Lage ist, einfache oder komplexe logische Operationen durchzuführen. Ein Controller kann auch gleichzeitig Sensor- und/oder Aktorfunktionen vereinen.

Managementgeräte

Managementgeräte können verschiedene Aufgaben übernehmen, wie

- Konfigurationsaufgaben (das Setzen von initialen Parametern, Hochladen von Benutzerapplikationen auf die Geräte der Feldebene)
- Wartungsaufgaben (Alarmwerte melden, Sollwerte verstellen)
- Visualisierungsaufgaben (grafische Darstellung von technischen Anlagen)

Ein Gebäudeautomationsnetzwerk besteht aus vielen verschiedenen Komponenten. Die wichtigsten sind Sensoren, Aktoren, Controller, Managementgeräte, Router, Gateways und Switches.

Router/Gateways

Geräte, die für die Verbindung ein oder mehrere verschiedener Netzwerke (Zweidrahtnetzwerk und IP-Netzwerk), beziehungsweise für die Übersetzung von Datentelegrammen aus unterschiedlichen Protokollen (zum Beispiel LON nach BACnet [siehe Kapitel 2.5]) verwendet werden.

Switch

Ein Switch ist ein Kopplungselement, welches mehrere IP-Netzwerksegmente miteinander verbindet.

Abbildung 6: 8-Port Ethernet-Switch, Foto: Netgear

[3] *Durch elektrischen Strom betriebener, meist elektromagnetischer Schalter*

2.4 Funktionale Anforderungen der IT-Sicherheit

Um in einem digitalen Kommunikationssystem den Datenaustausch zwischen den einzelnen Teilnehmern abzusichern, lassen sich allgemein folgende funktionale Anforderungen (Kastner, 2011) definieren:

Die drei wesentlichen Funktionen der IT-Sicherheit sind Authentifizierung, Autorisierung und Übertragung über einen sicheren Kanal

1. **Authentifizierung**
   Um in der Lage zu sein, eine sichere Kommunikation innerhalb einer Kommunikationsbeziehung zu garantieren, müssen die beteiligten Kommunikationspartner zunächst ihre Identität nachweisen.
   Anders ausgedrückt: Sie müssen sich gegenseitig authentifizieren.
   Bei der Authentifizierungsmethode geht es darum zu vermeiden, dass sich ein böswilliger Kommunikationspartner als eine vertrauens-würdiger ausgibt.
   Während in den meisten Fällen beide Kommunikationspartner (Sender und Empfänger) sich authentifizieren müssen (beidseitige Authentifizierung), gibt es auch Anwendungsfälle, in denen es ausreicht, dass sich nur einer der Teilnehmer authentifiziert (einseitige Authentifizierung).
   Ein Anwendungsbeispiel für eine einseitige Authentifizierung ist ein Sensor, der periodisch nicht vertrauliche Sensorwerte sendet. Hierbei würde eine Identifizierung des Senders ausreichen.

2. **Autorisierung**
   Nachdem sich die Teilnehmer für die sichere Kommunikation authentifiziert haben, muss sichergestellt werden, dass die Kommunikationspartner die notwendigen Rechte besitzen, an der Kommunikation teilzunehmen. Falls nicht, wird die Kommunikation verwehrt. Der Autorisierungsprozess kann auch als Berechtigungskontrolle bezeichnet werden.

3. **Sicherer Kommunikationskanal**
   Nachdem sich die Teilnehmer authentifiziert haben und alle Kommunikationspartner die erforderlichen Rechte besitzen, müssen die auszutauschenden Daten durch eine sichere Methode geschützt werden. Zu diesem Zweck wird ein sogenannter sicherer Kanal eingerichtet. Ein sicherer Kanal verwendet nicht-kryptografische (physikalische oder organisatorische Maßnahmen) und/oder kryptografische (Verschlüsselungs-) Techniken, um die Datenübertragung gegen ungewollte Angriffe zu schützen.
   In Abhängigkeit der Anforderungen und der Möglichkeiten der an der Kommunikation beteiligten Geräte, kann ein sicherer Kanal folgende Sicherheitsfunktionen implementieren:
   - **Datenintegrität:**
     Stellt sicher, dass die Daten während der Übertragung nicht unautorisiert manipuliert wurden.
   - **Datenursprung:**
     Die Authentifizierung des Datenursprungs ist eine stärkere Form der Datenintegrität. Zusätzlich zum Schutz der Daten gegen Manipulation während der Übertragung kann ein Empfänger hierbei die Herkunft der Daten nachprüfen, zum Beispiel die Datenquelle.

- **Datenaktualität:**
  Garantiert, dass übertragene Daten aktuell sind und dass es sich nicht um das wiederholte Senden von vorher abgefangenen Daten eines Angreifers handelt.
- **Datenvertraulichkeit:**
  Die Enthüllung von vertraulichen Informationen muss verhindert werden. In einem Gebäudeautomationssystem kann dies ein Raumtemperaturwert sein, der –wenn zum Beispiel längere Zeit auf einem niedrigen Niveau- einem Angreifer ein Hinweis sein kann, dass sich die Bewohner im Urlaub befinden.
- **Datenverfügbarkeit:**
  Stellt sicher, dass autorisierte Kommunikationsteilnehmer Zugriff auf Daten haben und dass der Zugriff nicht von einem Angreifer unterbunden wird.

2.5 Anwendbarkeit auf die Gebäudeautomation

Im Zusammenhang mit der aktuellen Anwendbarkeit vorstehend beschriebener Sicherheitsfunktionen aus der Informationstechnik auf Heim- und Gebäudeautomationsnetzwerke muss eine differenzierte Betrachtung vorgenommen werden.

Im Folgenden sind einige branchenspezifische Herausforderungen beschrieben, die sich bei der Implementierung oben beschriebener Sicherheitsfunktionen ergeben können:

1. **Geräteressourcen**
   Die meisten am Markt erhältlichen Komponenten vor allem für die Feldebene [siehe Kap. 2.2] müssen den Anforderungen kosten- und energieeffizienter Lösungen gerecht werden. Deshalb handelt es sich dabei in der Regel um eingebettete Geräte mit niedrigem Energieverbrauch und dementsprechend auch begrenzten Systemressourcen (wie Speicher und Prozessorleistung). IT-Sicherheitsfunktionen haben jedoch mitunter einen hohen Bedarf an solchen Systemressourcen (vor allem komplexe Verschlüsselungs-algorithmen). Daher gilt es vor diesem Hintergrund, eine Balance zwischen dem notwendigen Level an Sicherheit und verfügbaren Ressourcen zu finden.

2. **Skalierbarkeit**
   Mit Skalierbarkeit ist allgemein die Fähigkeit zur Vergrößerung und Verkleinerung von Objekten gemeint. Für Haus- und Gebäudeautomationssysteme ist dieser Faktor in Bezug auf die integrierten Sicherheitsmechanismen wichtig, da die Anzahl der Kommunikationsteilnehmer zwischen einigen wenigen bis sehr viele (>1000) variieren kann.

Sicherheitsfunktionen, die aus IT-Netzwerken bekannt sind, lassen sich aus verschiedenen Gründen nur bedingt auf Netzwerke der Gebäudeautomation anwenden.

3. Nicht-IP-basierte Feld-Netzwerke

IT-Sicherheitsmechanismen sind auf die jeweils vorherrschende Netzwerktechnologie ausgerichtet. In der Heim- und Gebäudeautomation findet im Gegensatz zu IT-Systemen der Einsatz von IP-basierten Netzwerken eher auf Backbone Ebene [siehe Kap.2.2] statt. In der Feldebene [siehe Kap.2.2] existieren zwar einige Geräte, die eine direkte Schnittstelle zu IP-Netzwerken bieten; der Einsatz dieser Geräte ist jedoch aus Kostengründen noch nicht so weit verbreitet wie der von Geräten ohne direkte IP-Schnittstelle.

4. Quality of Service- (QoS-) Parameter

Hiermit sind allgemein die Anforderungen an die Qualität des Kommunikationsdienstes gemeint. In der IT-Welt existieren in der Regel Anforderungen wie das Transferieren von großen Datenmengen (im Bereich von Mega- oder Gigabytes), wobei Parameter wie Zuverlässigkeit und Reihenfolge der Datentelegramme sowie Echtzeitanforderungen[4] häufig eine eher untergeordnete Rolle spielen. Dies kann in Haus- und Gebäudeautomationssysteme genau umgekehrt sein.

2.6 Kommunikationsprotokolle

In der Heim- und Gebäudeautomation existiert eine ganze Reihe von Kommunikationstechnologien parallel auf dem Markt.

Als bedeutendste offene Kommunikationsstandards, mit denen sich Ebenen übergreifende „All-in-one“-Lösungen realisieren lassen, sollen hier KNX, BACnet, LON ZigBee und Z-Wave vorgestellt und im Zusammenhang mit den jeweils implementierten IT-sicherheitsrelevanten Funktionen betrachtet werden.
Weiterhin werden einige Subbustechnologien vorgestellt, die jeweils für bestimmte Domänen, Gewerke innerhalb der Gebäudetechnik, entwickelt wurden; DALI für die Kommunikation in Beleuchtungssystemen, SMI für Jalousien, M-Bus für Energiezähler oder Enocean als Funkstandard für die drahtlose Integration von Sensoren.
Da IT-Netzwerke zunehmend an Bedeutung in der Hausautomatisierung gewinnen, wird mit der Erläuterung einiger IT-spezifischer Begriffe begonnen.

Ausführliche Informationen rund um IT-Netzwerke sind im Handbuch Netzwerksicherheit oder entsprechender Fachliteratur zu finden.

ISO/OSI-Schichtenmodell

Das als OSI-Referenzmodell bekannte System gliedert die Kommunikation von Netzen in sieben Schichten. Auf jeder Schicht werden durch Protokolle bestimmte Aufgaben ausgeführt. Dies ermöglicht eine modulare Entwicklung von Systemen, weil Schnittstellen zu den anderen Ebenen genutzt werden können.

[4] *Echtzeitsysteme müssen in der Lage sein, einen bestimmten Wert oder ein Berechnungsergebnis innerhalb eines festgelegten Zeitintervalls zu liefern*

Abbildung 7: ISO/OSI 7 Schichten Kommunikationsmodell

Ethernet

Als Ethernet wird die nach IEEE[5] 802.3 genormte Technologie bezeichnet, welche für kabelgebundene Netzwerke die Verwendung von Software in Form von Protokollen und Hardware spezifiziert. Ethernet ist ein Protokoll der ISO-OSI-Schicht zwei. Wichtige Fakten zu Ethernet sind unter anderem:

- Maximale Kabellänge: 100m (Kupfer) bei fest verlegten Leitungen. Abgezogen werden jedoch noch Übergänge wie Stecker und Kabel für Steckverbindungen. Mit Lichtwellenleitern (LWL)[6] können weitere Strecken als mit Kupfer überbrückt werden und diese Kabel sind störungsunempfindlicher.

[5] *IEEE steht für Institute of Electrical and Electronics Engineers und ist ein Berufsverband von Ingenieuren aus den Bereichen Elektrotechnik und Informationstechnik.*
[6] *Lichtwellenleiter werden auch als Glasfaser bezeichnet*

- Die Datenstruktur, welche über Ethernet verschickt wird, nennt sich „Frame“. Ein Frame gliedert sich in unterschiedliche Felder, welche alle nötigen Informationen enthalten, um die Daten zu verarbeiten.
- Die Adressierung in Ethernet sind MAC-Adressen. MAC-Adressen werden bei der Herstellung eines Gerätes vergeben und haben einen Adressbereich von 6 Bytes. Eine MAC-Adresse wird klassischer Weise durch mit Doppelpunkten getrennten hexadezimalen Werten dargestellt: 11:22:33:AA:BB:CC. Auch wenn MAC-Adressen theoretisch pro Gerät fest vergeben sind, lassen sie sich kopieren beziehungsweise fälschen. Dies wird „MAC-Spoofing“ genannt.
- Die maximale Übertragungsrate beträgt aktuell 10 Gbit/s.

Abbildung 8 zeigt ein CAT-7-Kabel[7] aus Kupfer. Die einzelnen Adern sind paarweise miteinander verdrillt (englisch „twisted pair“) und abgeschirmt, um die Störungswirkung untereinander zu verringern.

Abbildung 8: CAT-7-Kabel, Foto: Weumas.de

Abbildung 9 zeigt vereinfacht, wie Multimode und Monomode Glasfaser funktionieren. Bei Multimode werden mehrere Lichtwellen über dasselbe Kabel gesendet. Bei Monomode wird eine einzige Lichtwelle verwendet.

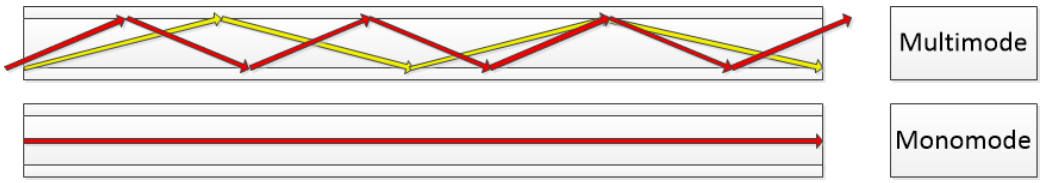


Abbildung 9: Multimode und Monomode Glasfaser

Die Tabelle 1 zeigt vier Ethernet-Standards mit deren maximaler Übertragungsgeschwindigkeit und welche Kabel mit welcher maximalen Länge verwendet werden können.

[7] *Die Kategorie (CAT) eines Kabels beschreibt dessen Leistungsvermögen in Bezug auf maximale Übertragungsfrequenz. Höhere Kategorien decken automatisch die darunterliegenden ab.*

Standard	Geschwindigkeit	Kabelart und Länge
100BASE-TX	100Mbit/s	Kupfer: CAT-5;CAT-7; 100m
1000BASE-X	1Gbit/s	Kupfer: CAT-5;CAT-7; 100m
10GBASE-LRM	10Gbit/s	Glasfaser: Multimode; 220m
10GBASE-ER	10Gbit/s	Glasfaser: Singlemode: 40km

Tabelle 1: Ethernet-Standards in Zahlen

Für weitere Informationen bezüglich Ethernet, nutzen Sie das Kapitel aus dem Handbuch Netzwerksicherheit oder entsprechende Fachliteratur.

TCP/IP

Das Internet-Protokoll oder kurz IP ist der Standard für aktuelle paketvermittlungsorientierte Netzwerke und wurde in der RFC[8] 791 (IPv4) beziehungsweise RFC 2460 (IPv6) definiert und ist ein Protokoll der OSI-Schicht drei. Es wird paketvermittlungsorientiert genannt, weil die Datenstruktur des Internet-Protokolls sogenannte Pakete (IP-Pakete) sind. Hierbei wird ähnlich eines Paketversandes jedes Paket auf dem besten und schnellsten Weg an seinen Empfänger zugestellt.
Die wichtigsten Fakten zu IP:

- Es gibt aktuell zwei Versionen von IP, welche verwendet werden: IPv4 und IPv6. Diese unterscheiden sich im Wesentlichen durch die Größe des Adressbereichs.
- IPv4 Adressen sind 32 Bit lang und ermöglichen somit die Adressierung von 2^{32} (~ 4 Mrd.) Empfängern. IPv4-Adressen werden für gewöhnlich im Dezimalsystem und durch Punkte getrennt angegeben: 123.123.123.123.
- IPv6 Adressen sind 128 Bit lang und ermöglichen damit die Adressierung von 2^{128} (~ $3{,}4 * 10^{38}$) Empfängern. IPv6-Adressen werden durch hexadezimale Zahlen angegeben und werden durch Doppelpunkte getrennt:
  2013:0724:1414:45AF:84FF:2FAAD:23FE:1BBC
- Subnetzmasken: Bei IPv4 können über sogenannte Subnetzmasken, bei IPv6 Präfixlängen genannt, IP-Netze segmentiert werden beziehungsweise in Netz- und Hostadresse geteilt werden. Hierbei werden aufeinanderfolgende Bereiche eines IP-Adressbereichs an Grenzen getrennt, welche durch die Subnetzmaske vorgegeben werden. Angegeben werden Subnetzmasken meist durch einen Backslash „/“ und einer Dezimalzahl, welche die 1-Bits der Subnetzmaske darstellen, welche an die IP-Adresse angehängt wird. Beispielsweise gibt die Darstellung 192.168.100.50/25 an, dass die ersten 25 Bits der IP-Adresse zur Netzadresse gehören und die verbleibenden sieben Bits zur Adressierung der Hosts verwendet werden. Mit Hilfe von Subnetzmasken können einzelne Abteilungen eines Unternehmens getrennt werden.

IPv4 Adressen haben 32 Bit (~4 Mrd.) und IPv6 128 Bit (~3,4 * 10 [38]).

Für weitere Informationen zu diesem Thema nutzen Sie bitte das Handbuch Netzwerksicherheit oder entsprechende Fachliteratur

[8] *RFC steht für Request For Comments und bildet sowohl die Diskussionsgrundlage für einen Standard, als auch nach Abschluss der Diskussion den Standard selbst.*

UPnP

UPnP steht für Universal Plug and Play und ist ein Begriff aus der Netzwerktechnik. Zu Deutsch bedeutet es sinngemäß, dass Geräte unmittelbar nach korrekter Verkabelung (Plug) einsatzbereit (Play) sind, ohne dass weitere Konfigurationen vorgenommen werden müssen.
UPnP sollte nur auf Netzwerkschnittstellen für das lokale Netzwerk freigeschaltet und aus dem Internet nicht erreichbar sein. Im Januar 2013 verkündete die Sicherheitsfirma Rapid7 aus Boston, dass sie in einem 6-monatigen Projekt nach UPnP-Geräten im Internet gesucht habe.[2] Dabei fanden sie 6900 Produkte von 1500 Herstellern unter 81 Millionen IP-Adressen, die auf UPnP-Anfragen aus dem Internet antworteten. 80% der Geräte sind Heim-Router für den Internetzugang, andere Geräte sind Drucker, Webcams und Überwachungskameras. Mit Hilfe des UPnP-Protokolls kann auf diese Geräte zugegriffen werden, beziehungsweise sie können sogar manipuliert werden.
(https://de.wikipedia.org/wiki/Universal_Plug_and_Play#Verwundbarkeiten.2C_die_2013_entdeckt_wurden, 2014)

2.7 Kabelgebundene Technologien

Die drei wichtigsten Protokollstandards in der Gebäudeautomation, die für kabelgebundene Netzwerke eingesetzt werden, sind KNX, LON und BACnet. Diese werden im Folgenden näher vorgestellt.

2.7.1 KNX

KNX ist ein Kommunikationsprotokoll, welches unter dem Titel „Home Electronic Systems“ international standardisiert ist (ISO/IEC 14543) und sowohl im Bereich der Heimautomation als auch im Bereich der kommerziellen Gebäudeautomation Anwendung findet. Für die Heimautomation ist KNX einer der bedeutendsten Standards, u.a. deshalb, weil diese Technologie vielfach schon während der Ausbildung im Elektrohandwerk gelehrt wird und somit das Marktangebot für die Installation und Inbetriebnahme von KNX-Systemen sehr groß ist.

Bei KNX können sogenannte Kommunikationsobjekte über Gruppenadressen miteinander kommunizieren

In einem KNX-Netzwerk werden Sensoren und Aktoren als eine Menge von Kommunikationsobjekten abgebildet. Ein Kommunikationsobjekt repräsentiert einen typisierten Wert, wie etwa eine Temperatur, einen Schalterzustand oder eine Stellgröße. Die Kommunikationsobjekte kommunizieren über Gruppenadressen (Abbildung 10). Sensoren senden eine Nachricht mit dem aktuellen Wert an alle Aktoren, die prüfen, ob ein eigenes Kommunikationsobjekt mit der Gruppenadresse verknüpft ist. Stimmt sie mit einem oder mehreren Objekten einer Gruppe überein, werden diese Objekte gesteuert.
Um Geräte verschiedener Hersteller interoperabel zu halten, verwenden Kommunikationsobjekte den Gleichen Satz standardisierter Datenpunkttypen (DPTs).

KNX-Geräte gibt es auf der Basis verschiedener Übertragungsmedien:

- Übertragung über verdrillte Zweidrahtleitung (KNX Twisted Pair = KNX TP)
- Übertragung über das vorhandene 230V Netz (KNX Power Line = KNX PL)
- Übertragung über Funk (KNX Radio Frequency = KNX RF)
- Übertragung über Ethernet (KNX IP)

Die Netzwerkintegration im KNX-System erfolgt über ein herstellerunabhängiges, datenbankbasiertes Installations-Tool (ETS - Engineering Tool Software).
Abbildung 10 zeigt eine Beispielinstallation eines KNX-Netzwerkes mit Internetanbindung.

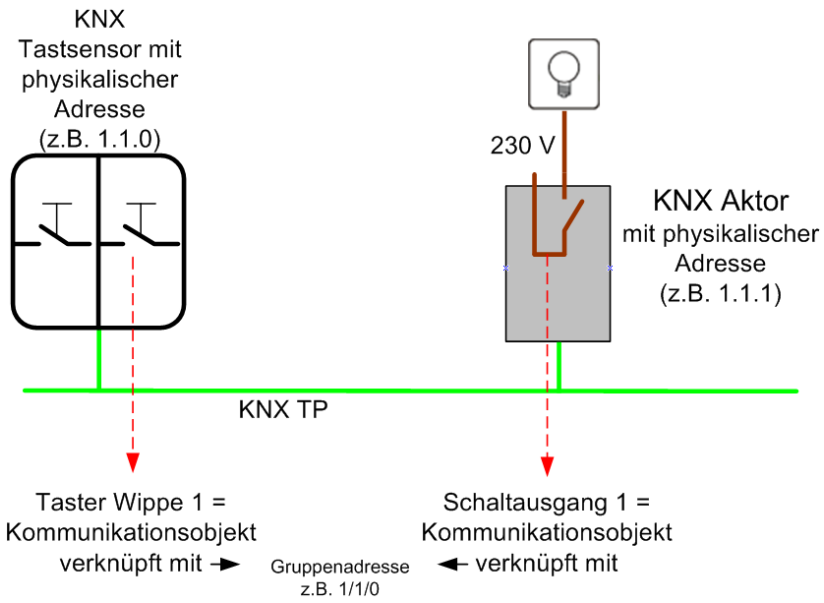


Abbildung 10: Kommunikation innerhalb eines KNX-Netzwerkes

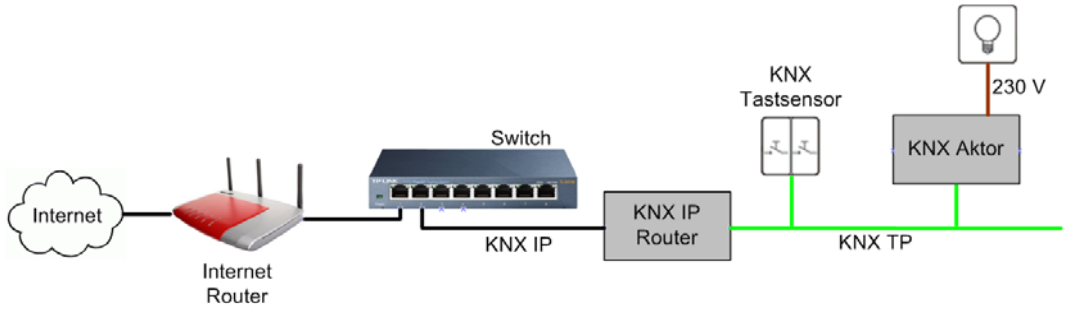


Abbildung 11: Beispielinstallation eines KNX-Netzwerkes mit Internetanbindung

KNX und IT-Sicherheit

Der KNX-Standard spezifiziert lediglich ein Schema für einen Basis-Zugriffschutz, der auf Klartext-Passwörtern basiert. Es können bis zu 255 verschiedene Zugriffsebenen definiert werden, denen jeweils unterschiedliche Privilegien zugeordnet werden können. Zugriffsebene 0 hat die höchsten Privilegien und Ebene 255 die niedrigsten. Für jede Ebene kann ein 4 Byte langes Passwort spezifiziert werden. Dieses Schema ist jedoch nur verfügbar für den Konfigurations- beziehungsweise Inbetriebnahmeprozess. Der Datenverkehr während des laufenden Systembetriebes ist ungeschützt.

Von den in Kapitel 2.4 beschriebenen IT-Sicherheitsfunktionen kann damit im KNX-Standard nur eine unsichere Implementierung der Funktion „Autorisierung“ festgestellt werden.

2.7.2 LON

LON steht für „Local operating network“ und wurde von der US-amerikanischen Firma Echelon Corporation um das Jahr 1990 entwickelt. Seit Dezember 2008 ist diese Technologie von der IEC und der ISO als internationale Norm anerkannt und in der Normenreihe 14908-x dokumentiert. Die „Sprache“ von LON heißt LONTalk-Protokoll.

Bei LON kommunizieren Netzwerkvariablen, die in Funktionsblöcken organisiert sind, über sogenannte Bindings miteinander

Verschiedenen Aufgaben im Automationsnetzwerk sind in sogenannten Funktionsblöcken (englisch: functional profiles; oft auch einfach „Objekte“ genannt) enthalten, von denen jeder Netzwerkteilnehmer (auch „Knoten“ genannt) mehrere enthalten kann.
Diese Funktionsblöcke beinhalten sogenannte Netzwerkvariablen (kurz: NV) für die Kommunikation mit anderen Funktionsblöcken (auf demselben Gerät oder auf anderen Geräten) und sogenannte Konfigurationsparameter (kurz: CP’s für englisch: Configuration Properties), mit denen das Verhalten der Funktionsobjekte verändert/parametriert[9] werden kann.
Für die softwaretechnische Verwaltung und die Inbetriebnahme des LON-Netzwerkes hat sich LonWorks Network Services (LNS) durchgesetzt, eine Client/Server-Architektur mit integrierter Datenbank. Es gibt mehrere Hersteller, die Netzwerkmanagementtools für die Inbetriebnahme von LON-Netzwerken anbieten, die jeweils auf LNS basieren.

LON-Geräte gibt es auf der Basis verschiedener Übertragungsmedien, zum Beispiel:

- Übertragung über verdrillte Zweidrahtleitung (LON FT-10)
- Übertragung über das vorhandene 230V Netz (LON-PLT)
- Übertragung über Ethernet (LON IP)

Um Daten auszutauschen, werden Ausgangsnetzwerkvariablen von Funktionsblöcken und Eingangsnetzwerkvariablen von anderen Funktionsblöcken miteinander verknüpft. Dies wird als „Binding“ bezeichnet. Netzwerkvariablen müssen hierbei vom gleichen Typ sein.

[9] *Parameter sind veränderliche Werte, die einem Programm oder Programmteil zur Berechnung/Abarbeitung seiner Aufgabe übergeben werden müssen.*

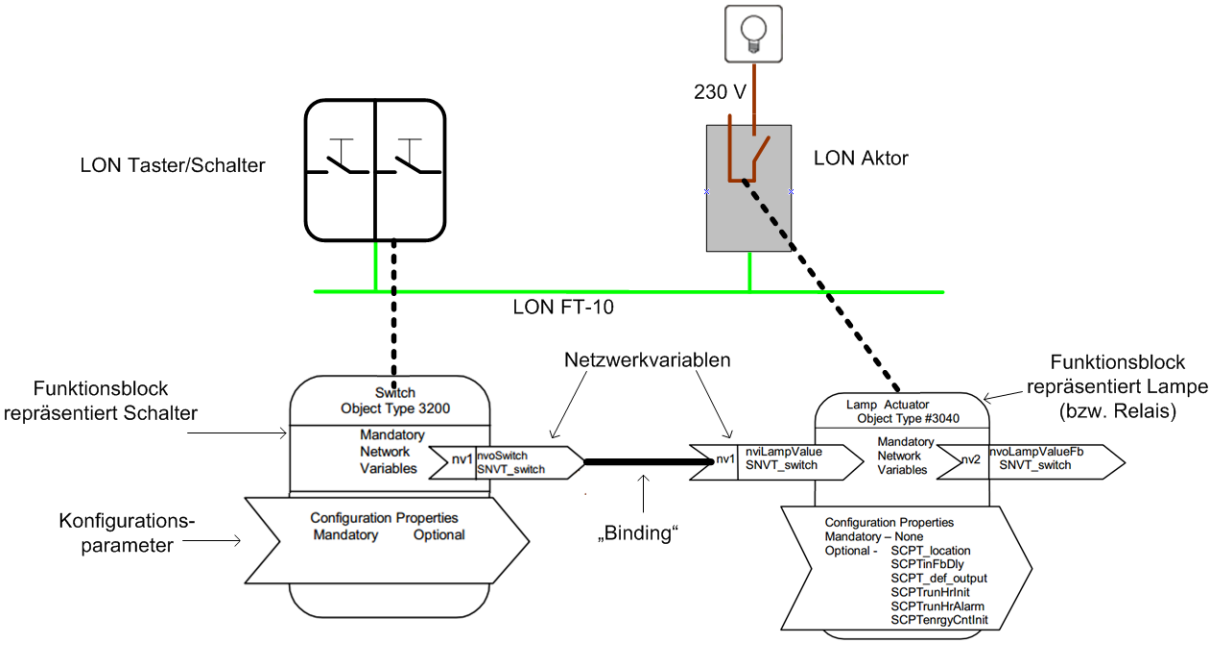


Abbildung 12: Kommunikation zwischen zwei LON-Knoten

LON und IT-Sicherheit

Das LonTalk Protokoll liefert einen Dienst zur Erhöhung der Datensicherheit. Damit kann in einem großen Netzwerk, mit Zugriff vieler verschiedener Systeme (Gewerke), ein Eintrag in der Konfigurationstabelle jeder NV einen Absender eines Telegramms als berechtigt oder nichtberechtigt ausweisen. Während der Netzwerkinstallation können zu diesem Zweck 48-bit-Schlüsselwörter an die Knoten vergeben werden. Wird ein Telegramm mit gesetztem Authentication Bit empfangen, wird das Authentifizierungsverfahren aktiviert.

Dazu erstellt der Empfänger eine mittels Zufallsgenerator erzeugte 64-bit-Zahl und sendet diese Nachricht an den ursprünglichen Sender. Dieser transformiert die Zufallszahl und die eigentliche Nachricht mit seinem 48-bit-Schlüsselwort und sendet das Replay zurück. Der Knoten transformiert ebenfalls die Nachricht mit dem 48 Bit Schlüssel. Stimmen die Werte nun überein, kann Knoten 2 den anderen Knoten als berechtigt ausweisen und das Telegramm annehmen. Die Sicherheit des System beruht daher nur auf dem sicheren Erstellen eines Zufallswertes und auf dem 48 Bit Schlüssel, den beide Netzwerkteilnehmer kennen müssen.

Weiterhin spezifiziert LonTalk für die Übertragung über IP eigene Sicherheitsmechanismen, die auf MD5 basieren. MD5 ist ein Algorithmus, der schon seit Längerem nicht mehr als sicher gilt.

Bei LON kann lediglich eine unsichere Implementierung der beiden IT-Sicherheitsfunktionen „Datenintegrität“ und „Datenaktualität“ (siehe Kapitel 2.4) festgestellt werden. Das zum Berechtigungsnachweis verwendete 48-bit Schlüsselwort ist zu kurz um unter anderem Brute-Force-Angriffen (siehe Kapitel 5.2.5) standzuhalten.

2.7.3 BACnet

BACnet (Building Automation and Control networks) ist ein standardisiertes Kommunikationsprotokoll für die Gebäudeautomation (ISO 16484: Building automation and control systems - Part 5: Data communication protocol).
BACnet wurde unter der Federführung der American Society of Heating, Refrigerating and Air-Conditioning Engineers (ASHRAE) Ende der 80er Jahre entwickelt.

BACnet Geräte gibt es auf der Basis verschiedener Übertragungsmedien.
Zu den bekanntesten und wohl am häufigsten angewendeten zählen:

- Übertragung über verdrillte Zweidrahtleitung (BACnet MS/TP)
- Übertragung über Ethernet (BACnet/IP)

Bei BACnet können die einzelnen Teilnehmer verschiedene Werte über sogenannte Server-Objekte zur Verfügung stellen. Andere Geräte können dann über unterschiedliche Dienste auf diese Werte zugreifen

Die Kommunikation im Netzwerk erfolgt über BACnet-Objekte, die als Server-Objekte von einem BACnet-Teilnehmer netzwerkweit zur Verfügung gestellt werden. Diese Server-Objekte besitzen bestimmte Eigenschaften (sogenannte Properties), die von anderen BACnet Geräten über definierte Dienste beschrieben und/oder gelesen werden können.
Ein Beispiel wäre ein BACnet-Gerät, welches einen Digitaleingang hat, an dem ein Taster angeschlossen ist. Der Digitaleingang würde im BACnet-Netzwerk vom Gerät als „Binary-Input“-Objekt dargestellt. Der aktuelle Wert des Objektes (also „An“ oder „Aus“, beziehungsweise 1 oder 0 = „Taster gedrückt“ oder „Taster nicht gedrückt“) würde über die Object-Property „Present Value“ repräsentiert.[10]

BACnet und IT-Sicherheit

Der BACnet-Standard wird ständig weiterentwickelt. Erweiterungen zum jeweils aktuellen Standard werden in sogenannten BACnet-Addenda zusammengefasst. Hier ist besonders das Addendum 2008-g interessant, welches ein umfangreiches Sicherheitskonzept vorsieht. Es wird in Kapitel 6 noch einmal aufgegriffen und detailliert beschrieben.

2.8 Funkbasierte Vernetzung

Die Datenübertagung per Funk ist vor allem überall dort interessant, wo die Verlegung von Leitungen aus wirtschaftlichen oder installationstechnischen Gründen nicht in Frage kommt (zum Beispiel für das Nachrüsten eines Automationssystems in Bestandsgebäuden). Das Thema IT-Sicherheit spielt hier sogar eine noch größere Rolle, da für einen Angreifer keine Notwendigkeit für einen physikalischen Netzwerkzugriff besteht. Denn die Daten werden in einem großen Radius um die Übertragungsstation versendet und können somit von außerhalb des Gebäudes abgegriffen oder manipuliert werden.

[10] *http://de.wikipedia.org/wiki/BACnet*

2.8.1 ZigBee

ZigBee ist eine Funknetztechnik, die auf den von IEEE 802.15.4 spezifizierten Schichten für die Funkübertragung aufsetzt. ZigBee wurde für die Industrie, für Smart Homes und die Gebäudesteuerung konzipiert. Der Standard ist eine Entwicklung der ZigBee-Allianz, die Ende 2002 gegründet wurde.

ZigBee unterscheidet drei Gerätetypen. Einfache Geräte wie zum Beispiel Lichttaster unterstützen nur einen Teil des ZigBee-Protokolls. Sie melden sich an einem ZigBee-Router an und bilden so mit ihm ein Netzwerk in Stern-Topologie. Sogenannte Full Function Devices können auch als ZigBee-Router agieren, melden sich an einem anderen existierenden Router an und bilden so ein Netzwerk in Baum-Topologie. Dadurch entsteht ein vermaschtes Netzwerk (siehe Abbildung 13). Der große Vorteil: Fällt ein Router aus, können die Daten über einen anderen weitergeleitet werden.

Jedes ZigBee-Netzwerk benötigt einen Koordinator. Er verwaltet und steuert das Netzwerk. Fällt der Koordinator aus, ist das gesamte Netzwerk blockiert. Hier liegt eine Schwachstelle des Systems. Allerdings können Router so konfiguriert werden, dass sie im Fehlerfall die Aufgabe des Koordinators übernehmen.

ZigBee und IT-Sicherheit

ZigBee bietet Sicherheitsmechanismen für die Kategorien: Authentifizierung, Datenursprung, Datenaktualität und Datenvertraulichkeit (Siehe Kapitel 2.4). Darüber hinaus gibt es Dienste für die Verwaltung und Verteilung von gemeinsamen Geheimschlüsseln (shared secret keys). Hierbei werden drei Schlüsseltypen (keys) unterschieden:
Link Keys, Network Keys und Master Keys.
Die Schlüssel können entweder vorinstalliert sein, oder sie können während der Systemlaufzeit von einem sogenannten Trust Center Applikation (Vertrauenscenter) abgerufen werden. Ein solches Trust Center kann durch den ZigBee-Koordinator oder durch eine andere Komponente realisiert werden.
In ZigBee-Netzen ist der Master Key ein vorinstallierter Schlüssel, der sich in jedem ZigBee-Knoten befindet. Er sorgt dafür, dass der Austausch der Link-Keys zwischen den Knoten vertraulich erfolgt. Der Link Key ist ein unverwechselbarer Schlüssel zwischen zwei kommunizierenden Knoten, der im AES-Verfahren[11] mit einer Schlüssellänge von 128 Bit erstellt wird. Der Link Key wird von der Anwendungsschicht verwaltet und entschlüsselt den Informationsfluss zwischen zwei Geräten. Dieser Schlüssel wird in der Praxis allerdings nicht benutzt. Der dritte Schlüssel ist der Network Key. Es ist ein im Trustcenter nach dem AES-Verfahren erzeugter 128-Bit-Schlüssel, den sich die ZigBee-Endgeräte teilen. Jedes Endgerät, das an das ZigBee-Netz angeschlossen wird, benötigt den Network Key. Der Schlüsselaustausch zwischen den Knoten erfolgt mit dem Symmetric-Key Key Establishment Protocol (SKKE).
(http://www.itwissen.info/definition/lexikon/ZigBee-Sicherheit-ZigBee-security.html, 2014)

[11] *Advanced Encryption Standard (AES) ist eine Blockchiffre zum Symmetrischen verschlüsseln von Daten.*

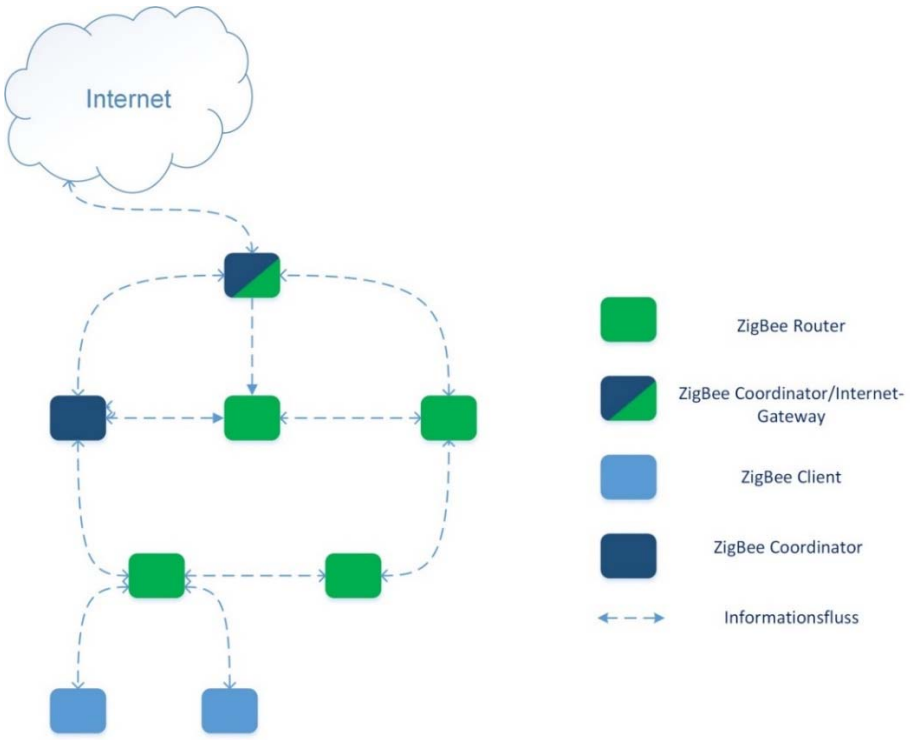


Abbildung 13: ZigBee Topologie

2.8.2 Z-Wave

Z-Wave ist ein drahtloser Kommunikationsstandard, der von der dänischen Firma Zensys und der Z-Wave Alliance speziell für die Heimautomatisierung entwickelt wurde.
Alle Komponenten werden zu einem sogenannten Mesh-Network zusammengefasst. Mesh drückt hierbei aus, dass jede Komponente mit denen in einer Reichweite von ca. 30m befindlichen Komponenten direkt kommuniziert. Jedes Gerät kann hier auch als Verstärker für andere Geräte dienen. Wenn also ein Gerät mit einem anderen kommunizieren will, welches mehr als 30m entfernt ist, kann ein dazwischen-liegendes Gerät als Vermittler dienen. Mit entsprechend vielen Komponenten lassen sich mit diesem System große Distanzen überwinden, da ein Z-Wave Netzwerk aus bis zu 232 Geräten bestehen kann.

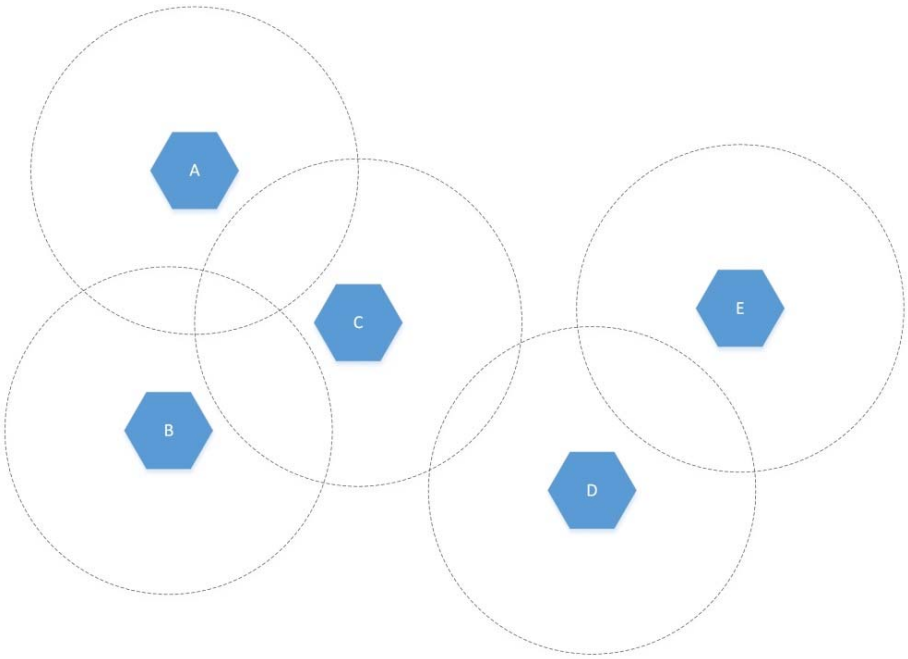


Abbildung 14: Z-Wave Funknetzwerk

Die Abbildung zeigt fünf Teilnehmer (A - E). Die gestrichelte Umrandung steht für die Reichweite. Hierbei bedeutet eine Überschneidung die Möglichkeit zur direkten Kommunikation. Teilnehmer A und E können in diesem Beispiel über die Teilnehmer C und D Informationen miteinander austauschen.

Z-Wave und IT-Sicherheit

Z-Wave bietet IT-Sicherheitsfunktionen für die Bereiche Datenintegrität, Datenaktualität, Authentifizierung und Verschlüsselung.
Hierbei wird die Datenintegrität und Authentifizierung durch einen 128 bit Message Authentification Code (MAC, siehe auch Kapitel 2.9.4) realisiert. Zum Sicherstellen der Datenaktualität wird ein 64 bit langer, einmaliger Code (sogenannter Nonce) ausgetauscht, mit dem die Daten vom Sender transformiert werden. Der auf diese Weise erzeugte sogenannte Hashcode wird dann zum Empfänger gesendet, welcher den Code zurücktransformiert. So kann ein Replay-Angriff (siehe Kapitel 5.1) verhindert werden.
Für die Verschlüsselung der Daten kommt bei Z-Wave das als sicher geltende AES-Verfahren[12] mit einer Schlüssellänge von 128 bit zum Einsatz.

Im Jahre 2013 präsentierten die beiden IT-Sicherheitsforscher Behrang Fouladi and Sahand Ghanoun eine Sicherheitsuntersuchung zum Z-Wave-Protokoll.
Dabei gelang es dem Team ohne vorherige genaue Kenntnis des Protokollstandards, die Kontrolle über ein Türschloss, das über Z-Wave kommunizierte, zu erlangen. Damit waren sie in der Lage, die Haustür zu öffnen. Fouladi und Ghanoun hatten es geschafft, mit einem selbstgebauten Netzwerkcontroller eine Schwäche bei der Implementierung des Schlüsselaustauschverfahrens auszunutzen und sich mit dem Türschloss zu verbinden.

[12] *AES – Advanced Encryption Standard. Symmetrischer Algorithmus zur Verschlüsselung von Daten.*

Der Hersteller hatte nach Kenntnisnahme der Sicherheitslücke angekündigt, diese umgehend zu beheben. Allerdings konnte nicht eindeutig geklärt werden, ob die fehlerhafte Implementierung vom Hersteller selbst herbeigeführt wurde, oder ob dieser sich nur eines Codefragmentes bedient hat, welches von der Z-Wave Alliance in einem Software Development Kit (SDK) den Herstellern zur Verfügung gestellt wird.
Falls es so wäre, könnten mit hoher Wahrscheinlichkeit auch Produkte anderer Hersteller von dem Sicherheitsproblem betroffen sein. (Fouladi, 2013) (Ray, 2013)

Das Beispiel zeigt zwei Dinge:
Erstens, dass auch der stärkste Verschlüsselungsalgorithmus nur bedingt Sicherheit bringt, wenn die Implementierung fehlerhaft ist.
Zweitens, dass das Prinzip „Security by Obscurity“[13], auf dem immer noch viele Heim- und Gebäudeautomationssysteme beruhen, sich nicht aufrechterhalten lässt.

2.8.3 WLAN

So wie Ethernet eine Spezifikation für kabelgebundene Netzwerke ist, so ist die als „WLAN“ bekannt gewordene Technik die Spezifikation für kabellose Kommunikation nach IEEE 802.11.
Die wichtigsten Fakten zu WLAN:

Wireless LAN (WLAN) ist die Spezifikation für kabellose Kommunikation nach IEEE 802.11. Neuste WLAN-Standards erreichen praktisch eine Übertragungsrate von 100-200 Mbit/s.

- Maximale Reichweite: Hardware- und umweltabhängig zwischen 30 und 100m, bei Richtantennten bis zu mehreren Kilometern.
- Maximale Übertragungsrate: Der am meisten verbreitete Standard (802.11n) bietet theoretisch bis zu 600 Mbit/s. Realistisch sind 100-200 Mbit/s bei gängigen W-LAN Routern.

W-LAN und IT-Sicherheit

WLAN-Verbindungen können auf dem Übertragungsweg verschlüsselt werden. Die aktuellste und damit empfehlenswerteste Verschlüsselung in Heimnetzwerken ist WPA2. Weiterhin ist die Wahl eines sicheren Passwortes (siehe auch Kapitel 6.2.7) ein absolut notwendiger Faktor für die Sicherheit.

2.8.4 Bluetooth

Bluetooth ist ein in den 1990er Jahren entwickelter Industriestandard für die Datenübertragung zwischen Geräten auf kurzer Distanz über Funktechnik.
Bluetooth-Netze werden Piconetze genannt. Sie können 255 Geräte umfassen, von denen nur maximal acht gleichzeitig aktiv sein können. Mehrere Piconetze können bei gleichzeitigen Verbindungen in zwei Netzen in einem sogenannten Scatternetz zusammengeschlossen werden.
Voraussetzung für Bluetooth Verbindungen ist ein sogenanntes Handshaking, bei dem frei wählbare PINs benutzt werden.

[13] *Sicherheit durch Verschleierung – Ein Prinzip, bei dem davon ausgegangen wird, dass ein Angreifer über das vorliegende System nicht genug Kenntnisse für einen effektiven Angriff besitzt.*

Für die Verbindungstechnik existieren 3 verschiedene Sicherheitsstufen.

- Stufe 1 = keine Sicherheit
- Stufe 2 = erhöhte Sicherheit mit Authentifizierung/Autorisierung
- Stufe 3 = Höchste Sicherheit mit optionaler Verschlüsselung

Bluetooth und IT-Sicherheit

Um Bluetooth-Verbindungen abhörsicher zu betreiben und diese gegen unbefugtes Eindringen zu schützen, müssen diese mit mehrstufiger dynamischer Schlüsselvergabe betrieben werden.
(http://de.wikipedia.org/wiki/Bluetooth#Aktueller_Standard:_Bluetooth_4.0, 2010)

Sicherheitsrisiken liegen unter anderem in der Wahl der PIN (mindestens 8-stellig!), in einer fehlerhaften Implementierung in den Endgeräten (Smartphones) oder bei werkseitig eingestellten PINs, die nicht verändert werden können („0000“ bei Headsets).
(http://blog.botfrei.de/2012/05/bluetooth-ein-sicherer-standard/, 2012)

2.9 Subbusse

Inzwischen hat die Ansteuerung über Datentelegramme auch bei elektrischen Endverbrauchern Einzug erhalten. So können beispielsweise Vorschaltgeräte von Leuchten nicht mehr nur über eine Spannungsmodulierung zwischen 1 - 10V oder Rollladenmotoren über zwei Relais (AUF/AB) angesteuert werden, sondern mittlerweile auch kommunikativ über Datentelegramme.
Dazu werden die jeweiligen Geräte (Motoren, elektronische Vorschaltgeräte) mit einer entsprechenden Schnittstelle ausgestattet. Daraus ergeben sich zwar z.T. höhere Anschaffungskosten, jedoch gibt es bei der Installation Vorteile durch die Möglichkeit der Busverkabelung. Auch funktional bieten die „intelligenten“ Verbraucher einige interessante Optionen, wie beispielsweise eine Rückmeldung, wenn ein Problem am Verbraucher vorliegt (defektes Leuchtmittel).
Diese Protokolle sind in der Regel für bestimmte abgegrenzte Anwendungsbereiche konzipiert (Jalousie/Rollladen, Beleuchtung, Sensoren, Energiezählen) und werden normalerweise über Gateways in ein übergeordnetes Automationssystem integriert, welches zum Beispiel auf KNX, BACnet oder LON basiert. Deshalb werden sie auch als sogenannte Subbusse bezeichnet.

Subbusse sind Kommunikationstechnologien, welche nur für einen speziellen Teilbereich in einem Automationsnetzwerk konzipiert sind (zum Beispiel Beleuchtung oder Rollladen/Jalsouien). Sie werden in der Regel durch Gateways in eine übergeordnete Automation integriert

2.9.1 DALI

Der DALI[14] Standard hat sich schon seit einigen Jahren vor allem im Zweckbau (Büro und Verwaltungsgebäude) als Standardlösung für dimmbare Beleuchtung etabliert. Für Vorschaltgeräte ist DALI in der IEC 60929 normiert.
Wie bereits einleitend beschrieben kommen in der Praxis oft Gateways zum Einsatz, die die einzelnen Teilnehmer am DALI-Bus (vor allem elektronische Vorschaltgeräte

[14] *DALI – Digital Addressable Lighting Interface (DALI) ist in der Gebäudeautomatisierung ein Protokoll zur Steuerung von lichttechnischen Betriebsgeräten.*

von Leuchten, aber mittlerweile auch Sensoren) mit einem übergeordneten Automationssystem verbinden.
Ein solches Gateway kann ein oder mehrere DALI-Kanäle bereitstellen. An einem DALI-Kanal können in der Regel maximal 64 Teilnehmer verbunden sein. Die Kommunikation zwischen Gateway und Teilnehmern erfolgt mit einer Übertragungsrate von 1200 bit/s bei einer maximalen Distanz von 300 m zwischen zwei Geräten. DALI bietet keine der in Kapitel 2.4 beschriebenen IT-Sicherheitsfunktionen.

2.9.2 SMI

SMI ist die Abkürzung für Standard Motor Interface. Es handelt sich um eine Schnittstelle für die Steuerung elektrischer Antriebe. Anwendung findet der Standard bei Rollladen- und für Sonnenschutzanlagen.
Wie bei DALI werden in der Praxis häufig Gateways eingesetzt, mit dem die SMI-Motoren in ein übergeordnetes Automationssystem integriert werden können (KNX oder LON [siehe Kapitel 2.7]).
Die Datenübertragungsrate bei SMI liegt bei 2400 bit/s und es können maximal 16 Antriebe an einem SMI Kanal betrieben werden.
SMI bietet keine der in Kapitel 2.4 beschriebenen IT-Sicherheitsfunktionen.

2.9.3 M-Bus

M-Bus steht für Meter-Bus. Es handelt sich um ein in EN 13757 standardisiertes Protokoll für die Energiedatenerfassung.
Anwendungsbereiche sind Wärme-, Wasser-, Strom- und Gaszähler.
Es wird zwischen einer drahtgebundenen Variante mit einer Übertragungsgeschwindigkeit von 300 bis 9600 bit/s und einer drahtlosen Variante (Wireless M-Bus) unterschieden.
IT-Sicherheitsfunktionen werden nur von der drahtlosen Variante unterstützt, und zwar eine mit dem als sicher geltenden AES-128-Verfahren verschlüsselten Übertragung der Daten. (Hariharasudhan, 2014)

2.9.4 EnOcean

Hierbei handelt es sich um eine Funktechnologie für Sensorsysteme, die von der Firma EnOcean GmbH entwickelt wurde. Ein zentrales Merkmal ist das sogenannte Energy Harvesting. Hierbei werden physikalische Effekte genutzt um Energie bereitzustellen. Durch eine effiziente Datenübertragung genügt eine geringe Energiemenge für die Kommunikation zwischen Sensor und Aktor.
Die bis Mitte 2012 erhältlichen Produkte mit Enocean Technologie bieten keinen hinreichenden Schutz gegen Angreifer.
Mit der 2012 erschienenen Dolphin-Technologie wurde auch die IT-Sicherheit für Enocean Geräte erhöht. So soll unter anderem die Datenaktualität sichergestellt werden, indem jeder Sender und Aktor einen Zähler für ein- und ausgehende Datentelegramme führt. Damit können sogenannte Replay-Angriffe (siehe auch Kapitel 5.1) verhindert werden. Außerdem kann für jedes Datentelegramm ein 32-bit Authentifizierungscode (sogenannter MAC = Message Authentification Code) berechnet werden, durch den das Telegramm validiert werden kann, um so die Authentizität des Senders sicherzustellen.

Für die Verschlüsselung der Daten kann der als sicher geltende AES-Algorithmus mit einem 128-Bit-Schlüssel verwendet werden.
(Ohland, 2012)

2.9.5 Weitere Protokolle

Beispiele für weitere Protokolle für die Heimautomatisierung, die proprietär, beziehungsweise auf dem Weg zur Standardisierung sind, sind Digitalstrom, LCN und HomeMatic. (http://de.wikipedia.org/wiki/Smart_Home, 2013)

2.10 Zusammenfassung

Ein Gebäudeautomationsnetzwerk lässt sich grundsätzlich in einem zweistufigen Modell in eine Backbone-Ebene und eine Feldebene einteilen.
Innerhalb dieser Ebenen tauschen eine Reihe von Geräten verschiedene Daten untereinander aus, wobei die einzelnen Geräte jeweils unterschiedliche Aufgaben innerhalb des Netzwerkes übernehmen.
Das Regelwerk, welches diesem Datenaustausch zu Grunde liegt, wird als Kommunikationsprotokoll bezeichnet. Hiervon existieren einige Protokollstandards parallel am Markt. Auch innerhalb eines Netzwerkes können unterschiedliche Protokolle zum Einsatz kommen. Gängige Übertragungsmedien sind grundsätzlich verdrillte Zweidrahtleitungen, Funk, ein vorhandenes 230V-Stromnetz oder Ethernet.
Verschiedene in der Informationstechnik etablierte Sicherheitsfunktionen sind aus historisch zweckgebundenen und wirtschaftlichen Gründen vor allem in der Feldebene in der Regel nur teilweise, beziehungsweise rudimentär implementiert.

Notizen

3. Software in der Gebäudeautomation

3.1 BMS – Building Management System

Mit einem Building Management System ist ein rechnergestütztes Softwaresystem gemeint, über das die verschiedene Systeme der Haustechnik u.a. verwaltet, bedient, grafisch visualisiert und gewartet werden können.
Im Zusammenhang mit Gebäudeautomationssytemen werden entsprechende Lösungen auch oft als GLT (Gebäudeleittechnik) bezeichnet.
Eine Anwendung aus der Praxis wäre die Visualisierung einer Lüftungsanlage auf einem zentralen Rechner, welche durch verschiedene Sensoren, Aktoren und Controller geregelt und gesteuert wird.
Das BMS kommuniziert mit den beteiligten Automationskomponenten (in der Regel direkt oder über Gateways [siehe Kapitel 2.3.1]) und stellt die einzelnen Informationen in einer Grafik mit dynamischen Elementen dar. So hat man beispielsweise in einem zentralen Gebäudemangagement (Facility Management) die Anlage jederzeit im Blick und ist über aktuelle Werte und Funktionen informiert. Hier können auch dynamische Warneinblendungen und -meldungen erfolgen, zum Beispiel wenn eine bestimmte Temperatur überschritten wird oder wenn ein Filter verstopft ist. Ebenso können häufig Zeitschaltprogramme von hier aus konfiguriert werden. Es können auch Energiemanagementfunktionen (automatischer, zyklischer Versand von Energieverbrauchswerten per E-Mail) integriert sein.

Ein Building Management System ist eine Software, mit der verschiedene Funktionen wie Visualisierung und Bedienung, Wartung und Energiemanagement realisiert werden

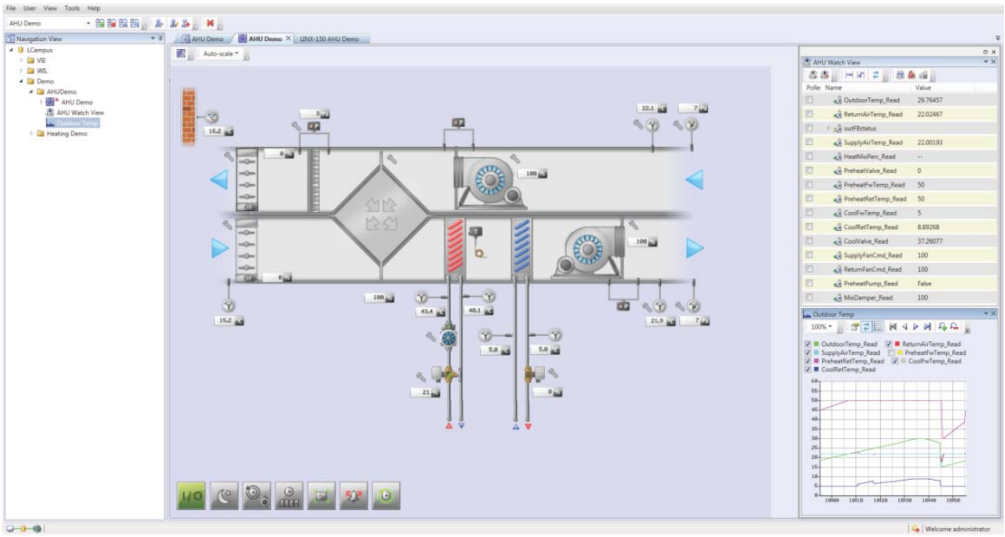


Abbildung 16: Beispiel für ein BMS mit Visualisierung einer Lüftungsanlage

3.1.1 OPC

Bei OPC[15] handelt es sich um eine standardisierte Software-Schnittstelle, die den Datenaustausch zwischen Anwendungen unterschiedlichster Hersteller in der Automatisierungstechnik ermöglichen soll.
Zuständig für die Pflege und Weiterentwicklung ist die OPC Foundation, der mittlerweile mehr als 450 Unternehmen angehören.
Der OPC-Standard besteht aus einer Reihe von unterschiedlichen Spezifikationen. Während ältere Spezifikationen ausschließlich für Windows-basierte Systeme entwickelt wurden, handelt es sich bei der neuesten Spezifikation (OPC UA) um eine plattformunabhängige Architektur.
(https://opcfoundation.org/about/what-is-opc/, 2014)
In der Haus- und Gebäudeautomation wird OPC vielfach in den Bereichen BMS (siehe oben) und Visualisierung eingesetzt.

Die aktuellste Version, die OPC-UA Spezifikation, definiert einige umfangreiche Sicherheitsfunktionen. So können für die Kommunikation als sicher geltende Verschlüsselungstechniken wie das AES-128-Verfahren verwendet werden, um Datenvertraulichkeit, -aktualität und -ursprungsauthentizität sicher zu stellen. Teilnehmerauthentifizierung wird mit Hilfe von Zertifikaten[16] realisiert.

Notizen

[15] *OLE for Process Control (OPC) war der ursprüngliche Name für standardisierte Software-Schnittstellen, die den Datenaustausch zwischen Anwendungen unterschiedlichster Hersteller in der Automatisierungstechnik.*
[16] *Ein Zertifikat ist ein digitaler Datensatz, der bestimmte Eigenschaften von Kommunikationsteilnehmern bestätigt und dessen Authentizität und Integrität durch Verschlüsselungsverfahren sicherstellt*

4. Modellhaus

In diesem Kapitel soll ein fiktives aber praxisnahes Anwendungsbeispiel (Einfamilienhaus) mit verschiedenen funktionalen Anforderungen an das Hausautomationssystem seitens des Bauherren zur Veranschaulichung vorgestellt werden.

Funktionale Anforderungen

Der Bauherr erwartet u.a. folgende Funktionen von seinem „Smart Home“:

- *Automatische Lichtfunktionen*
  Die Beleuchtung soll in den Räumen automatisch ausgeschaltet werden, wenn jemand den Raum verlässt. Damit soll unnötiger Energieverschwendung vorgebeugt werden, falls jemand das Licht beim Verlassen des Raumes nicht ausschaltet. Zusätzlich dazu soll in den Fluren das Licht beim Betreten des Raumes auch automatisch eingeschaltet werden, und zwar nur dann, wenn die Tageslichtversorgung im Raum einen bestimmten Wert unterschreitet.

- *Zentralfunktionen*
  Rollladen sollen über einen Zentralbefehl abends gemeinsam ab- und morgens gemeinsam aufgefahren werden können.
  Beim Verlassen des Hauses sollen über einen Zentralbefehl alle Räume auf einen definierten Raumtemperatursollwert regeln, der entsprechend niedriger ist als der Sollwert bei Anwesenheit; dadurch soll unnötiger Verschwendung von Heizenergie bei Abwesenheit vorgebeugt werden.

- *Anwesenheitssimulation*
  Beim Verlassen des Hauses für einen längeren Zeitraum soll das Automationssystem dafür sorgen, dass während des Tages bestimmte Verbraucher (Lichter und Rollladen) temporär ein und ausgeschaltet, beziehungsweise auf- und abgefahren werden. So soll ein potentieller Einbrecher, der versucht, durch Beobachtung des Hauses herauszufinden, ob jemand an- oder abwesend ist, den Eindruck gewinnen, dass der Besitzer zu Hause ist.

- *Smartphonebedienung*
  Zusätzlich zu lokalen Raumbediengeräten sollen alle Raumfunktionen für Beleuchtung, Rollladen und Raumtemperatur auch über das Smartphone, beziehungsweise über einen Tablet-PC steuerbar sein. Außerdem soll die Schließanlage der Haustür sowie die Steuerung des Garagentors ins Automationssystem integriert werden, so dass diese ebenfalls per Smartphone geöffnet werden können.

- *Fernzugriff*
  Der Bauherr möchte die Möglichkeit haben, mit dem Smartphone über das Internet einige Steuerfunktionen zu realisieren. So möchte er in der Lage sein, den Temperatursollwert in den einzelnen Räumen auf einen Komfortwert (zum Beispiel 22°C) einzustellen, während er auf dem Heimweg ist. So soll gewährleistet sein, dass die Räume bereits auf einen angenehmen Wert vortemperiert sind, wenn der Bauherr zu Hause ankommt.
  Zusätzlich dazu sollen bestimmte Meldungen auf sein Smartphone geschickt werden, wenn die Alarmanlage ausgelöst hat oder wenn ein Rauchmelder angeschlagen hat.

Notizen

5. Risiken und Bedrohungen

Auf Grundlage des im vorstehenden Kapitel beschriebenen Modellhauses sollen in diesem Abschnitt mögliche Risiken und Bedrohungen dargestellt werden, wenn ein Angreifer es schafft, sich in das Automationsnetzwerk einzuklinken. (Granzer, 2010)

5.1 Angriffsszenarien

Aus der Informationstechnologie sind einige Attacken bekannt, die von Angreifern durchgeführt werden, wenn es gelingt, sich Zugang zu einem Kommunikationsnetzwerk zu verschaffen.
Bezogen auf Heim- und Gebäudeautomationssysteme lassen sich diese übertragen und prinzipiell in zwei Kategorien einteilen:
Netzwerkangriffe und Geräteangriffe.
Aus den verschiedenen Angriffsmöglichkeiten lassen sich entsprechende Risiken ableiten, vor denen auch z.T. der Bauherr aus dem Modellhausbeispiel gewarnt sein sollte. Die folgende Abbildung zeigt eine Übersicht über mögliche Angriffsszenarien.

Ein Angreifer hat grundsätzlich die Möglichkeit, das Netzwerk oder die im Netzwerk vorhandenen Geräte zu attackieren

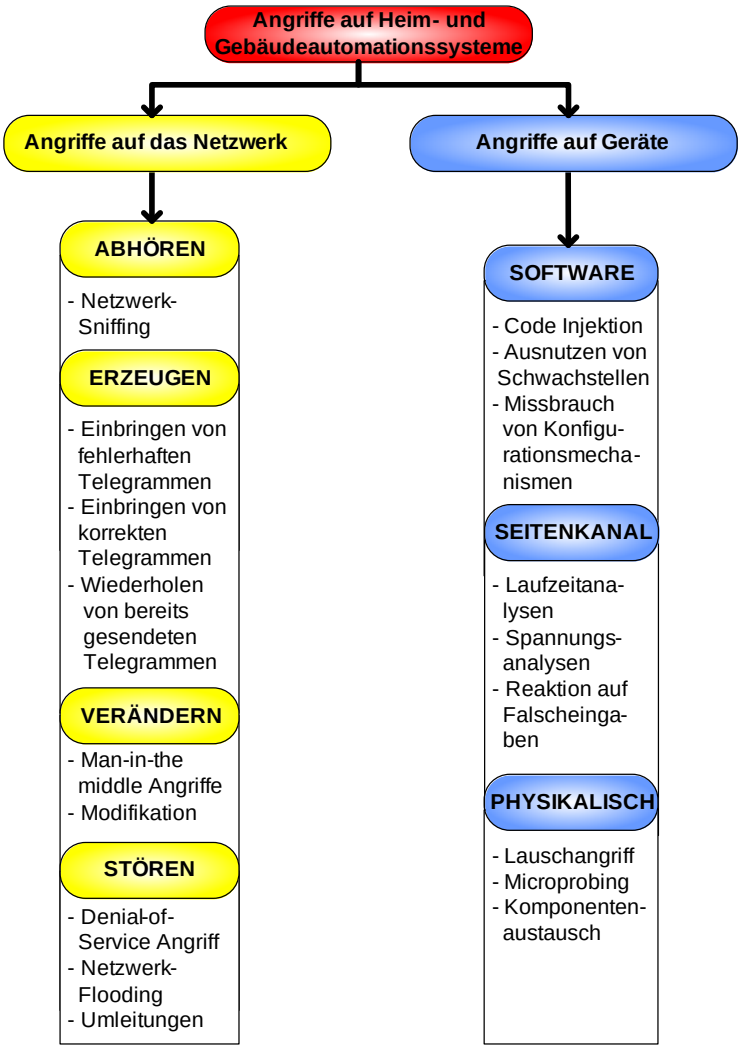


Abbildung 17: Angriffe auf Heim und Gebäudeautomationssysteme

Ein Angreifer hat folgende Möglichkeiten, sich Zugang zum Netzwerk zu verschaffen:

- **Medienzugriff**: Der Angreifer verschafft sich physikalischen Zugang über das Netzwerkübertragungsmedium. Hier können der Einsatz von Funkübertragung oder Übertragung über das 230V-Netz (Außensteckdosen) dem Angreifer in die Karten spielen, wenn diese nicht adäquat verschlüsselt sind.
- **Gerätezugriff**: Der Angreifer nutzt die Netzwerkschnittstelle eines vorhandenen Gerätes (zum Beispiel ein kompromittierter Sensor, Aktor oder Controller oder ein Gateway)

Mit der erfolgreichen Umsetzung einer der beiden o.g. Möglichkeiten ergeben sich für den Angreifer folgende Möglichkeiten, sein „Unwesen“ zu treiben:

Abhören des Datenverkehrs

Einem unerwünschten Abhören des Datenverkehrs kann durch Verschlüsselung der Daten vorgebeugt werden

Der Angreifer liest durch unautorisierten Zugriff auf das Netzwerk den Datenverkehr mit und versucht die so gewonnenen Informationen für seine Zwecke zu gebrauchen (Netzwerk-Sniffing[17]).
In unserem Modellhaus aus Kapitel 4 möchte der Bauherr u.a. eine präsenzabhängige Steuerung der Beleuchtung und eine Umschaltung aller Raumtemperatursollwerte auf einen niedrigen Wert bei Abwesenheit, um Energie zu sparen.
Ein Angreifer, dem es gelingt, den Datenverkehr innerhalb des Automationssystems abzuhören, könnte aus einem dauerhaften Fehlen einer Meldung der Präsenzmelder und einem niedrigen Raumtemperatursollwert über einen längeren Zeitraum schlussfolgern, dass sich niemand im Haus befindet.

Technisch gesehen kann dem sogenannten Netzwerk-Sniffing durch eine Verschlüsselung des Datenverkehrs [siehe Kapitel 2.4] vorgebeugt werden. Der Angreifer hat dann bei einem gut implementierten Verschlüsselungs-verfahren in der Regel keine Möglichkeit, die Daten zu entschlüsseln.
Viele Automationsgeräte, die in der Haus- und Gebäudeautomation eingesetzt werden, unterstützen jedoch aus den in Kapitel 2.5 beschriebenen Gründen keine Verschlüsselungstechniken. Hier besteht auf Seite der Hersteller erheblicher Nachholbedarf, der kurz- bis mittelfristig erfüllt werden müsste.
Für den Bauherren wäre es deshalb in diesem Fall ratsam, in die Funktion Anwesenheitssimulation [siehe Kapitel 4] auch die Präsenzmeldungen und die Raumtemperatursollwerte zu integrieren.

[17] *von engl. sniff für schnüffeln. Überprüfung des Datenverkehrs eines Netzwerkes auf Anfälligkeiten mit Hilfe einer speziellen Software („Sniffer“ genannt)*

Erzeugen von Telegrammen

Der Angreifer ist in der Lage, durch unautorisierten Zugriff auf das Netzwerk eigene Telegramme zu erzeugen (Code-Injection) oder abgefangen Telegramme einfach zu einem bestimmten Zeitpunkt zu wiederholen (sogenannte Replay-Attacken).
Für unser Modellhaus bedeutet dies, dass ein Angreifer mit unberechtigtem Zugriff auf das Netzwerk zum Beispiel das Telegramm, welches beim Öffnen der Tür oder der Garage über das Smartphone gesendet wird, abfängt. Zu einem Zeitpunkt, an dem das Haus verlassen ist, wiederholt er das abgefangene Telegramm und löst so die Öffnungsfunktion aus.
Authentifizierung, Autorisierung sowie Funktionen wie Datenintegrität, Datenursprung und Datenaktualität [siehe Kapitel 2.4] sind Sicherheitsmechanismen, die solchen Attacken vorbeugen können.

Zum Schutz vor Replay-Attacken können Authentifizierungs- und Autorisierungsfunktionen sowie Sicherstellung der Datenintegrität, des Datenursprungs und der Datenaktualität dienen.

Verändern von Telegrammen

Bei sogenannten Man-in-the-middle Attacken steht der Angreifer entweder physikalisch oder logisch zwischen den beiden Kommunikationspartnern. Er hat dabei vollständige Kontrolle über den Datenverkehr zwischen zwei oder mehreren Netzwerkteilnehmern und kann die Informationen nach Belieben einsehen und sogar manipulieren.
Wirksame Methoden gegen solche Angriffe sind Verschlüsselung der Daten, sowie die Sicherstellung der Datenintegrität durch einen Identifikationsstempel, den sogenannten Message Authentification Code, den jede gesendete Nachricht enthält und der mit Hilfe eines vorher zwischen Netz und Nutzer ausgehandelten Codes erzeugt wird.

Stören des Datenverkehrs

Bei sogenannten Denial of Service Angriffen (zu Deutsch: Dienstverweigerung) geht es darum, dass ein Angreifer bestimmte Netzwerkteilnehmer derart mit Telegrammen „bombardiert“, dass die eigentlich gewollte Funktionsweise verhindert wird. Das System kann so möglicherweise lahmgelegt werden.

5.1.1 Angriffe auf Geräte

In dieser Kategorie geht es darum, dass ein Angreifer ein Gerät aus dem Netzwerk angreift, um Zugang zu Gebäudesteuerung zu erlangen.

Softwareattacken

Der Angreifer kann Schwachstellen in der Softwareimplementierung des Gerätes ausnutzen. Um sich Zugang zur Gerätesoftware zu verschaffen, kann der Angreifer grundsätzlich das Netzwerk nutzen (einen schlecht gesicherten Konfigurationszugang), in dem sich eine Steuerungsanlage befindet oder er kann eine Schnittstelle direkt am Gerät (USB-Port) verwenden.

Ein Angreifer hat verschiedene Möglichkeiten für Attacken auf Geräte innerhalb eines Gebäudeautomationsnetzwerkes

Seitenkanalattacken (Side channel attacks)

Hier versucht der Angreifer an Informationen zu gelangen, indem er externe Parameter misst und für seine Zwecke zu interpretieren versucht, während das Gerät bestimmten Rechenoperationen ausführt (Zeitparameter, elektrische Leistungsaufnahme des Prozessors).
Hier gibt es einige Gegenmaßnahmen, die geräteintern ergriffen werden können zum Beispiel Glättung der Laufzeit durch konstante Codeausführung oder physikalische Abschirmung gegen elektromagnetische Abstrahlungen.

Physikalische Attacken

Der Angreifer kann sich Zugang zum Gerät durch den Austausch von Hardware-Komponenten verschaffen. Hier gilt besondere Vorsicht bei der Verwendung von Werbegeschenken, sogenannten Give-Aways (ROM-Chips, USB-Sticks, Maus): Diese können manipuliert sein, beispielsweise eine Maus, die im anschließenden Einsatz den heimischen PC mit Malware (Spähsoftware o.ä.) infiziert. Es gilt immer die Quelle von Hardware im Vorhinein als vertrauenswürdig einzustufen, durch den Erwerb von autorisierten Händlern, beziehungsweise ordnungsgemäß versiegelte Ware.

5.2 Sonstige Risiken

Neben den unter 5.1 genannten Risiken existieren weitere, die in den folgenden Abschnitten beschrieben werden.

5.2.1 Veraltete Hard- und Software

Heim- oder Gebäudeautomationslösungen sind üblicherweise Systeme, die über lange Zeit in einem Gebäude ihre „Arbeit verrichten“. Wenn sich der Hauseigentümer auf Grundlage seiner individuellen Sicherheitsansprüche für ein System entschieden hat, sollte er auch darüber nachdenken, dass sich gerade im Bereich der IT-Sicherheit schnell neue Bedrohungen auftun können. Sicherheitsfunktionen können morgen schon als unsicher gelten, obgleich sie gestern noch als sicher galten.
Bei aller Sorgfalt der Hersteller kann es passieren, dass Sicherheitslücken entdeckt werden oder es können implementierte Verschlüsselungstechniken über die Jahre als unsicher deklariert werden.
Daher ist es empfehlenswert, sich regelmäßig vom Hersteller über neue Hard- und Software (vor allem Sicherheitsupdates) informieren zu lassen, diese auf Relevanz für das eigene System zu prüfen und ggf. das System entsprechend zu aktualisieren. Die Bereitstellung von regelmäßigen Sicherheitsupdates sollte ein Kriterium bei der Systemauswahl sein.

5.2.2 Übertragungsmedium

Wie bereits im vorherigen Kapitel angedeutet, ist die Auswahl des Übertragungsmediums innerhalb des Automationssystems nicht unerheblich im Hinblick auf das Gefahrenpotential durch Angreifer. In der Branche werden kabelgebundene Systeme sowie funkbasierte Systeme angeboten. Vor allem bei Funksystemen müssen sich Nutzer

sich der Gefahr bewusst sein, dass die Reichweite solcher Systeme es einem Angreifer prinzipiell erleichtern kann, sich unerlaubten Zugriff zu verschaffen. Ebenso besteht bei Systemen, die über das vorhandene 230V Stromnetz kommunizieren (Power Line) ein Risiko, da häufig Außeninstallationen vorhanden sind (Steckdosen im Garten, Gartenhaus, Außenbeleuchtung). Um die Sicherheit solcher Systeme zu gewährleisten, sollte man sich genau über die möglichen Sicherheitsfunktionen informieren. Außerdem muss gegebenenfalls darauf geachtet werden, dass diese richtig konfiguriert werden.

5.2.3 Wardriving

Beim Wardriving werden gezielt Wohnsiedlungen abgefahren und auf Funknetzwerke (im allgemeinen WLANs) hin untersucht. Je mehr Verbreitung funkbasierte Systeme in der Hausautomatisierung erfahren, desto interessanter könnten diese hinsichtlich Wardriving werden.

5.2.4 Fernwartung

Fernwartung stellt eine kostengünstige Möglichkeit dar, dass Installateure dem Kunden bei Problemen helfen. Ohne Anfahrt und die damit verbundenen Kosten kann der Installateur unmittelbar auf das System zugreifen und Fehler diagnostizieren oder auf die Konfiguration Einfluss nehmen. Fernwartungszugänge bieten jedoch auch Angreifern ein Einfallstor und sollten nach den aktuellen Anforderungen der IT-Sicherheit eingerichtet sein, um diese vor Missbrauch zu schützen [siehe auch
Kapitel 6].

5.2.5 Brute-Force-Attacken

Bei der sogenannten Brute-Force-Attacke (zu Deutsch: „rohe Gewalt“) versucht der Angreifer, ein Passwort zu knacken, indem eine Software einfach in schneller Abfolge verschiedene Zeichenkombinationen ausprobiert.
Einige Geräte aus dem Bereich der Heim- und Gebäudeautomation sind heutzutage mit einem sogenannten Webinterface ausgestattet. Hierbei handelt es sich im Allgemeinen um eine grafische Oberfläche, die eine Übersicht über diverse geräteinterne Informationen zeigt und über die auch Gerätekonfigurationsparameter verändert werden können. Diese Oberfläche wir meistens über einen im Gerät integrierten Webserver bereitgestellt und kann somit einfach über einen Internet Browser aufgerufen werden, indem die IP-Adresse des entsprechenden Gerätes in die Adresszeile des Browsers eingegeben wird, wenn man sich mit seinem PC (oder Smartphone/Tablet) im gleichen Netzwerk befindet. Auch der Zugang über das Internet kann realisiert werden, wenn das Netzwerk entsprechend konfiguriert ist.
Für beide Fälle sollte sichergestellt sein, dass bestimmte Sicherheitsfunktionen implementiert sind. Das Mindeste ist hier ein passwortgeschützter Zugang.
Aber auch wenn ein Passwortzugang existiert, gibt es weitere Sicherheitsfunktionen, wie einer Brute-Force-Attacke vorgebeugt werden kann.
Seitens des Herstellers könnten Abwehrmechanismen wie das Verlängern des Zeitraums zwischen zwei Login-Versuchen (nach der falschen Eingabe eines Passworts) implementiert sein. Mit jeder falschen Eingabe verlängert sich dieser Zeitraum. So

kann der Brute-Force-Rechner, der eigentlich in der Lage wäre, sehr viele Berechnungen pro Sekunde durchzuführen, ausgebremst werden.
Für den wirksamsten Schutz gegen solche Angriffe kann jedoch der Nutzer selbst sorgen; nämlich bei der Wahl des Passwortes und durch die Nutzung einer HTTPS-verschlüsselten Verbindung. Was hierbei zu beachten ist, wird in Kapitel 6.2.7 beschrieben.

5.2.6 Shodan

Als „erschreckendste Suchmaschine des Internets“ wurde jüngst das Projekt Shodan bezeichnet.

Bei Shodan[18] handelt es sich um eine Suchmaschine, die im Gegensatz zu Google und anderen bekannten Suchmaschinen sich nicht nur für Medien wie Texte und Bilder interessiert, sondern darüber hinaus mit dem Internet verbundene Geräte und Dienste findet; besonders diese, die häufig nicht passwortgeschützt sind.
Ampelanlagen und Sicherheitskameras sowie Kontrollsysteme für einen Wasserpark, eine Tankstelle, den Weinschrank eines Hotels und eines Krematoriums sind nur einige Systeme und Geräte, die von Shodan gefunden werden.
(t3n, 2014)

Je größer die Verbreitung von mit dem Internet verbundener Heim- und Gebäudeautomationssysteme voranschreitet, desto größer wird auch die Notwendigkeit, für die Absicherung seiner Anlagen zu sorgen.
Den bereits im vorherigen Abschnitt beschriebenen Gefahren beim unautorisierten Zugriff auf ein Webinterface eines Gerätes kann mit entsprechend gut gewählten Passwörtern [sieh Kapitel 6.2.7] sowie Implementierungen von aktuellen Sicherheitsfunktionen im Gerät entgegengewirkt werden.

[18] *http://en.wikipedia.org/wiki/Shodan_(website)*

5.3 Zusammenfassung

Aus der IT-Welt sind Sicherheitsbedrohungen und -risiken bekannt, die sich auch auf Heim- und Gebäudeautomationssysteme übertragen lassen. Ein Angreifer, der sich unerlaubt Zugriff auf das Netzwerk verschaffen will, hat dabei grundsätzlich die Möglichkeit, das Netzwerk oder die Geräte innerhalb des Netzwerkes zu attackieren und entsprechende Schwachstellen auszunutzen.

Notizen

6. Basisschutz

In diesem Abschnitt werden Möglichkeiten vorgestellt, um eine grundlegende Sicherheit eines Heim- oder Gebäudeautomationssystems herbeizuführen.

6.1 Standards nutzen

Bei der Vielzahl der am Markt existierenden Technologien sollte sich der Nutzer stets informieren, ob das präferierte oder angebotene System auf einer standardisierten Technologie beruht oder ob es sich um ein proprietäres System handelt. Bei proprietären Systemen sollte man sich darüber im Klaren sein, dass das Produkt-angebot am Markt begrenzt ist. Häufig gibt es nur einen Hersteller und auch die zu Grunde liegende Technologie besteht gegebenenfalls nur solange und wird weiterentwickelt, wie der Hersteller, der sie entwickelt hat, existiert.
Offene Standards hingegen sind häufig Grundlage für eine Vielzahl von Herstellern, die diese für Ihre Produkt- und Systemlösungen verwenden und auch eine herstellerunabhängige Kommunikation ist in der Regel problemlos möglich. Ein weiterer Vorteil standardisierter Technologien sind Gremien, die sich nachhaltig um die Weiterentwicklung und Verbesserung der Standards (auch in puncto IT-Sicherheit) kümmern. Ein Beispiel hierfür ist die BACnet-Spezifikation, die mit dem Addendum 2008-g (siehe Kapitel 6.1.2) diverse IT-Sicherheitsfunktionen für den Standard festgelegt haben.

6.1.1 KNX

Für KNX existieren Sicherheitserweiterungen, die die mangelhaften Sicherheitsimplementierungen des Standards kompensieren sollen

Wie in den vorangegangenen Kapiteln dargestellt, bringt der KNX-Standard von Haus aus keine überzeugenden und zuverlässigen IT-Sicherheitsfunktionen mit, was auch an der begrenzten Ressourcenverfügbarkeit der an einer Kommunikation beteiligten Geräte liegt.

Für KNX gibt es jedoch einige Ansätze, die ein KNX-Netzwerk (oder Teile eines KNX-Netzwerkes) sicherer machen sollen:

KNX-Guard

Hierbei handelt es sich um ein Gerät, welches bei einer bestehenden Installation den Gerätezugriff über sogenannte physikalische Telegramme verhindert. Also solche, wie sie während der Inbetriebnahme bei einer Punkt-zu-Punkt Verbindung zwischen der ETS-Software [siehe Kapitel 2.7.1] und dem zu parametrierenden Gerät verwendet werden. Dadurch soll verhindert werden, dass die KNX-Geräte unerlaubt manipuliert werden. Zusätzlich können Alarmfunktionen genutzt werden, wenn das Gerät einen unerlaubten Zugriff abwehrt.
Um eine zuverlässige Absicherung zu erzielen, sollte ein Gerät in jedem Netzwerksegment (Linie) installiert sein.

Nach Sicherheitsstufen werden folgende drei Typen unterschieden:

KNXGuard "Höchste Sicherheit"

Schreib- und Lesezugriffe auf physikalischer Telegrammebene sind nur möglich, wenn der KNXGuard aus der EIB/KNX-Installation entfernt wird.

KNXGuard "Hohe Sicherheit"

Geräteüberwachung (Lesezugriff) ist auf physikalischer Telegrammebene weiterhin möglich. Schreibzugriffe werden geblockt und sind erst bei Entfernen des KNXGuard aus der EIB/KNX Installation möglich.

KNXGuard "Benutzerdefinierte Sicherheit"

Dieser Typ wird über den Bus mittels des EIBDoktors parametriert/aktiviert/deaktiviert. Hierzu wird über die KNX-Broadcastadresse 15/7/255 mit RSA-Verschlüsselung kommuniziert. Aufgezeichnete Telegramme können aufgrund des (verschlüsselten) Zeitstempels nicht erneut eingespielt werden, wodurch ein Replay-Angriff (siehe Kapitel 5) verhindert wird. Zusätzlich wird der Zugriff über die Verifizierung der Seriennummer und die Eingabe einer PIN gesichert.
(b+b Automations- und Steuerungstechnik GmbH, 2014)

EIBsec

EIBsec ist eine Sicherheitserweiterung und eine Weiterentwicklung des Secure EIB Ansatzes, der aus einer Doktorarbeit an der TU München resultiert.

Hierbei werden die Daten mittels AES [siehe Kapitel 6.2.5] verschlüsselt, wobei die Adressierung unverändert bleibt um die Kompatibilität zum „alten“ KNX zu gewährleisten. Hinzu kommt eine 32 Bit Cylcic-Redundancy-Check (CRC) Checksumme, die gegen unautorisierte Modifikationen schützt. Ein 128 Bit Counter soll gegen Replay-Angriffe [siehe Kapitel 5.1] helfen. Somit wird hier der KNX-Standard um die Sicherheitsfunktionen Datenursprunsauthentifizierung, Datenvertraulichkeit, Datenintegrität und Datenaktualität (siehe Kapitel 2.4) erweitert.
Je nachdem in welchem Netzwerksegment eines hierarchisch aufgebauten EIB-/KNX-Netzwerkes eine sichere Kommunikation notwendig ist, kann ein sogenanntes Advanced Coupler Unit (ACU) Modul mit EIBsec Funktion verwendet werden.

6.1.2 BACnet Addenda

Der BACnet Standard, der bereits in Abschnitt 2.7.3 beschrieben wurde, wurde und wird unter der Obhut der American Society of Heating, Refrigerating and Air-Conditioning Engineers, Inc. (kurz: ASHRAE) entwickelt, beziehungsweise weiterentwickelt. In regelmäßigen Zusammenkünften werden für den Standard sogenannte Addenda (Ergänzungen) festgelegt. Aus Sicht der IT-Sicherheit besonders interessant ist das Addendum 2008-g, welches im Folgenden erläutert werden soll.

BACnet Addendum 2008-g

Hierbei handelt es sich um eine Ergänzung des Standards, um die Ziele der BACnet Netzwerk-Sicherheitsarchitektur zu erreichen. Diese sind:

- Geräte- und Benutzerauthentifizierung sowie
- Auslenden von Daten (Verschlüsselung)

Die BACnet-Sicherheit soll ermöglichen:

- Anwendung auf alle BACnet-Medientypen (BACnet/IP, MS/TP etc.)
- Anwendung für alle Arten der BACnet-Geräte (Geräte, Router, BBMDs)
- Anwendung auf alle Nachrichtentypen (Broadcast, Unicast, bestätigt und unbestätigt)
- Anwendung auf alle Nachrichten-Schichten
- Einfügen von nicht sicherheitsfähigen Geräten, wenn physikalisch sicher, hinter einem sicheren Proxy-Firewall-Router
- Einfügen sicherer Geräte in nicht sicherheitsfähige Netzwerke

BACnet Addendum 2008-g spezifiziert das IT-Sicherheitskonzept des Standards

Das Sicherheitsmodell von BACnet verwendet als „shared secret“ (deutsch: gemeinsames Geheimnis) bezeichnete Schlüsselpaare. Ein Schlüssel des Paares ist immer der Signaturschlüssel und der andere ist der „Verschlüsselungsschlüssel“.
Es gibt sechs Arten von Schlüsselpaaren:
General-Netzwerkzugriffsschlüssel, Benutzerauthentifizierungsschlüssel, anwendungsspezifische Schlüssel, Installationsschlüssel, Verteilungs- und Device-Master-Schlüssel.
(Kranz, 2013)

Das Addendum definiert die IT-Sicherheitsfunktionen Authentifizierung, Datenvertraulichkeit, Datenintegrität und Datenaktualität (siehe Kapitel 2.4) für den BACnet-Standard. Die Funktion Datenaktualität kann nur umgesetzt werden, wenn den an einer Kommunikation beteiligten Geräten jeweils eine (möglichst) synchronisierte Uhrzeit zur Verfügung steht, da der Mechanismus mit einem Zeitstempel arbeitet. Zur Authentifizierung des Datenursprungs muss der verwendete Schlüssel auf zwei Geräte limitiert sein. Bei Verwendung eines Schlüssels, der an mehrere Geräte verteilt wurde (zum Beispiel General-Netzwerkzugriffsschlüssel oder anwendungsspezifische Schlüssel) kann die Identität des Senders nicht sicher festgestellt werden.

6.1.3 Firmware-Updates

Firmware (engl. firm ‚fest‘) bezeichnet Software, die in elektronische Geräte eingebettet ist. Es handelt sich dabei im Prinzip um die Betriebssoftware eines Gerätes, die zumeist in einem Flash-Speicher, einem EPROM, EEPROM oder ROM gespeichert und in der Regel nur durch den Hersteller änderbar ist.

Hersteller von Heim- und Gebäudeautomationskomponenten stellen normalerweise in regelmäßigen Abständen Firmware-Updates für Ihre Geräte zur Verfügung. Dies kann der Fall sein, wenn neue Funktionalitäten vom Gerät unterstützt werden aber auch wenn Sicherheitslücken erkannt und geschlossen werden. Meist informiert der Hersteller beispielsweise über Newsletter automatisch über Firmware-Updates. Es emp-

fiehlt sich, neue Firmware-Updates auf Relevanz für das eigene System zu prüfen und dieses gegebenenfalls zu aktualisieren.

Tipp:

Neben Preis und Funktionalität der Geräte sollte bei der Entscheidungsfindung auch berücksichtigt werden, was der Hersteller in puncto Wartungsmanagement und Bereitstellung wichtiger Sicherheitsupdates anbietet.

6.1.4 Sicherer Zugriff über Apps

Das Smartphone ist heute weit verbreitet und damit auch die Apps, welche das Gerät personalisierbar machen. Auch im Bereich Heim- und Gebäudeautomation besteht der Anspruch zunehmend darin, mit dem Gebäude über das Smartphone kommunizieren zu können. Anwendungen können u.a. im Bereich Raumbedienung (Beleuchtung schalten, Rollladen fahren) oder verschiedenen Meldungen (Alarmanlage, Rauchmelder o.ä.) liegen. Die Kommunikation kann dabei über das lokale (Heim-Netzwerk oder über das Internet erfolgen.

Sicherheit der Applikation

Die Sicherheit der Applikation kann nur durch den Entwickler sichergestellt werden. Für den Benutzer sollte hier gelten, dass regelmäßig Updates gemacht werden. Die Kommunikation sollte verschlüsselt erfolgen. Der Zugriff über Apps sollte eine Passworteingabe voraussetzen, sonst kann bei Verlust des Handys jeder sofort auf das Automationssystem zugreifen.

Datenschutz bei Handyapplikationen

Wie bei allen Handy-Apps gilt auch im Bereich der Heimautomation zu prüfen, welche Rechte die App genau einfordert und auf welche Daten zugegriffen werden kann.

6.2 Fernzugriff und Netzwerksicherheit

Einer der Hauptmotivationsgründe für Bauherren, sich für die Investition in ein Heimautomationssystem zu entscheiden, liegt in der Möglichkeit des Fernzugriffs. Dafür notwendig ist in der Regel die Anbindung des Systems an das Internet. Spätestens an dieser Stelle kommen einige Geräte und Komponenten aus der IT-Welt ins Spiel (Internetrouter) und dementsprechend kommt es zu einer funktionalen Verschmelzung diverser Sicherheitsaspekte.

6.2.1 VPN

VPN – Virtual Private Network

Ein Gateway ist ein Protokollumsetzer zwischen unterschiedlichen Netzwerkprotokollen, der es ermöglicht, dass Daten zum Beispiel aus dem Internet in ein lokales Netz gelangen und umgekehrt. Gateways arbeiten auf den Schichten 4 bis 7 des ISO/OSI-Modells.

Ein virtuelles privates Netzwerk, kurz VPN, ist ein Netzwerk, welches in einem anderen Netzwerk gekapselt arbeitet. Als Vergleich kann ein Kabelkanal dienen, in welchen unterschiedliche Kabel eingezogen sind (siehe Abbildung 16). Der Kabelkanal ist das Trägernetz und die Kabel bilden die abgekapselten Tunnel. Heutzutage ist das Internet mit seiner weiten Verbreitung und guten Zugänglichkeit in der Regel das Basisnetzwerk in welchem gekapselt wird.
Um über das Internet ein eigenes privates Netzwerk aufzubauen, werden Gateways genutzt, wie sie auch in den heimischen Internetrouter (zum Beispiel Fritzbox) integriert sein können. Diese stellen die Verbindungspunkte zu einem Teil des privaten Netzwerks dar. Die Verwendung von Gateways bietet den Vorteil, dass sowohl andere Gateways mit dahinter geschaltetem Netzwerk, als auch Clients sich direkt mit diesen verbinden können. Die Verbindung der unterschiedlichen Punkte eines virtuellen Netzwerks wird als Tunnel bezeichnet. Dies ist darin begründet, dass alle Daten an den jeweiligen Punkten durch die Verwendung eines VPN-Protokolls ein- und wieder ausgepackt werden. Das Netzwerk wird durch eine Verschlüsselung des Tunnels privat – von außen kann der Inhalt der getunnelten Kommunikation zwar mitgelesen aber durch die starke Kryptografie nicht entschlüsselt werden. In Abbildung 18 wird exemplarisch gezeigt, wie durch die Verwendung von Gateways ein virtuelles Netz erzeugt wird.

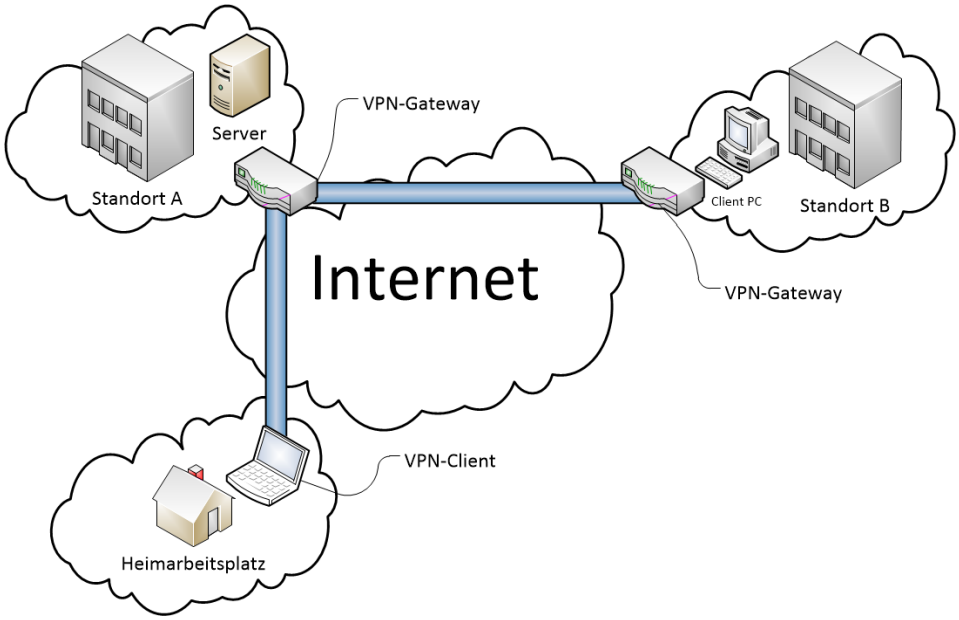


Abbildung 18: Ein VPN mit Gateways und Client

Die Abbildung 18 zeigt schematisch, dass am Standort A ein Server in einem Netzwerk vorhanden ist. Dieser soll für die Arbeitsplätze am Standort B und den Heimarbeiter zu erreichen sein. Hierzu wird ein VPN-Gateway genutzt. Da mehrere Arbeitsplätze am Standort B den Zugriff benötigen, bietet es sich an, die Verbindung von einem zentralen Punkt aus zu regeln. Aus diesem Grund wurde hier ein weiteres VPN-Gateway eingerichtet. Für alle Netzteilnehmer am Standort B ist der Server an Standort A nun so zu erreichen, als ob der Server lokal angebunden wäre. Für den

einzelnen Mitarbeiter zu Hause wird ein VPN-Client verwendet, welcher sich mit dem Gateway verbindet und damit am privaten Netzwerk teilnimmt.
Der Einsatz von VPNs bietet unter anderem folgende Vorteile:

- (VPN)-Gateways sind unabhängig von den Arbeitsplätzen und deren Betriebssystemen (Windows, Linux, Apple).
- Gateways bieten Sicherheit in der Kommunikation zwischen Geräten, welche normalerweise keine Sicherheit implementieren.
- In heterogenen Systemen (andere Hardware, Software und so weiter) kann dasselbe Gateway verwendet werden.
- Gateways sind als zentraler Punkt leichter „sicher“ zu realisieren
- Die Sicherheit ist nicht abhängig von anderen Systemkomponenten oder Anwendungen.
- Mit einem VPN-Client können Personen authentifiziert werden.

Für VPNs haben sich zwei Technologien durchgesetzt: IPSec und SSL-VPN.

IPSec – Internet Protocol Security

IPSec ist ein Sicherheitsstandard und eine Erweiterung des IP-Protokolls, das speziell für VPN entwickelt wurde.

IPSec ist ein weiterer Sicherheitsstandard und beruht auf einer ganzen Liste von RFCs. Er wurde von der Internet Engineering Task Force (IETF) entwickelt und ist eine gemeinsame Erweiterung des Internet-Protokolls (IP) um Verschlüsselungs- und Authentisierungsmechanismen für Sicherheitsprodukte verschiedener Hersteller. Als Erweiterung des IP-Protokolls bietet IPSec folgende Sicherheitsfunktionen:

- Schutz der Pakete gegen Manipulation.
- Verschlüsselung der Pakete.
- Schutz vor Wiedereinspielung der Pakete. Dies verhindert zum Beispiel, dass aufgezeichnete Befehle ein weiteres Mal von anderen gesendet werden können.
- Schutz vor Verkehrsflussanalyse. Dies verhindert, dass durch Beobachtung des Verkehrs Rückschlüsse auf die Teilnehmer gemacht werden können.
- Authentisierung der Kommunikationspartner (Gateways oder Nutzer).

Diese Funktionen bilden die vollständige Umsetzung aller Anforderungen für VPNs.

SSL-VPN

SSL-VPN nutzt das TLS-Protokoll zur Herstellung einer verschlüsselten Verbindung.
Eine bekannte Implementierung ist die Open-Source Lösung OpenVPN.

Die als SSL[19]-VPN bekannt gewordene Technologie nutzt TLS, Transport Layer Security Protocol, zur Herstellung einer sicheren, verschlüsselten Verbindung.
Die bekannteste und am weitesten verbreitete Implementierung von SSL-VPN ist OpenVPN[20]. Diese zeichnet sich besonders durch ihre einfache Konfigurierung aus und wird von vielen Betrieben schon lange erfolgreich eingesetzt. OpenVPN wird als

[19] *SSL steht für Secure Socket Layer*
[20] *www.openvpn.de*

Open-Source Software gepflegt und ist somit kostenfrei einsetzbar. Die Verschlüsselung und Authentifizierung wird bei SSL-VPN über das TLS-Protokoll hergestellt.

Wenn Sie VPNs nutzen möchten empfiehlt sich die Verwendung von OpenVPN

6.2.2 WLAN-Sicherheit

WLAN Router sind heute für die Anbindung des Heimnetzwerkes an das Internet zum Standard geworden. Grundsätzlich handelt es sich dabei um ein Gerät, welches verschiedene Teilnehmer (PCs, Smartphones, Tablets, Drucker) mit entsprechender Schnittstelle drahtlos zu einem Netzwerk verbindet und gleichzeitig diesen Teilnehmern als Internetgateway dient.
Im Smart Home kann die reine Funktion der drahtlosen Vernetzung dazu genutzt werden, um über das Smartphone innerhalb des Heimnetzwerkes bestimmte Bedienfunktionen im Haus zu realisieren (Licht schalten, Rollladen fahren).
Der wichtigste Aspekt bei der Nutzung von WLAN ist die Verschlüsselung der Daten. Denn über das WLAN übertragene, unverschlüsselte Daten können von jedem, der sich in Reichweite befindet, ohne große technische Kenntnisse abgefangen werden.
Von den drei existierenden Verschlüsselungsmethoden WEP (Wired Equivalent Privacy), WPA (Wi-Fi Protected Access) und WPA2 sollte in jedem Fall letztere (WPA2) die erste Wahl sein. WEP kann innerhalb von 2 Minuten mit einfachsten Mitteln geknackt werden, WPA ist zwar noch nutzbar, aber nicht mehr zukunftsorientiert. Auch eine WPA2 Verschlüsselung ist nur mit einem ausreichend langen und kryptischen Passwort wirklich sicher, um sich gegen Angriffe wie Wardriving [siehe Kapitel 5.2.3] zu schützen. (Pohlmann/Linnemann, 2010)

Für WLAN Netzwerke ist dringend eine WPA2-Verschlüsselung zu empfehlen

6.2.3 Firewall-Konzepte

Firewalls bilden praktisch die erste Verteidigungslinie gegen Angriffe von außerhalb. Sie sind in jedem Fall so zu konfigurieren, dass sie nur die unbedingt erforderlichen Verbindungen zulassen. Firewalls werden in vier Kategorien eingeteilt:

- Paketfilter
- Stateful Packet Inspection (SPI, im deutschen „Zustandsorientierte Paketüberprüfung“)
- Application Gateway
- Adaptive Proxy

Ein Firewall-System wird wie ein Pförtner zwischen das zu schützende und das unsichere Netz geschaltet, sodass der Datenverkehr zwischen den Netzen nur über das Firewall-System möglich ist.

Um die Funktionsweisen der verschiedenen Firewall-Systeme zu erläutern wird hier die Analogie zu einem Pförtner, welcher ankommende Lieferanten kontrolliert, hergestellt (Pohlmann, 2003).
„Paket Filter-Pförtner“ schauen auf das Logo des ankommenden LKW und lassen diesen passieren, wenn ihnen dieses bekannt ist.
„Stateful Paket Inspection-Pförtner“ schauen nicht nur nach dem LKW, sondern kontrollieren auch den Lieferschein und begutachten das Paket von außen. Ist alles ok, lassen sie den LKW mit dem Paket passieren.

Der „Application-Gateway-Pförtner" schaut nicht nur die Adressen der eingehenden Lieferungen an, er öffnet auch jedes Paket, prüft den kompletten Inhalt und checkt die Arbeitspapiere des Absenders nach einer klar festgelegten Reihe von Beurteilungskriterien. Nach der erfolgten detaillierten Sicherheitsüberprüfung unterzeichnet der Pförtner den Lieferschein und schickt den LKW wieder auf seinen Weg. Anschließend bestellt er einen vertrauenswürdigen Fahrer der eigenen Firma, der nun die Pakete zum eigentlichen Empfänger bringt. Die Sicherheitskontrolle ist an dieser Stelle wesentlich zuverlässiger und der Fahrer der Fremdfirma erhält keinen weiteren Einblick in das Firmengelände. Die Überprüfungen nehmen zwar mehr Zeit in Anspruch, dafür können jedoch auch mehr sicherheitsgefährdende Aktivitäten ausgeschlossen werden.

Die vier Firewall-Systeme sind: Paket Filter, Stateful Paket Inspection, Application-Gateway und Adaptive Proxy.

Der „Adaptive Proxy Pförtner" arbeitet in der ersten Phase (Verbindungsaufbauphase) wie der Application Proxy: Er schaut sich nicht nur die Adresse der eingehenden Pakete an, er öffnet auch das Paket und überprüft den gesamten Inhalt. Wenn der Adaptive Proxy den Lieferanten seit langem kennt, dann sendet er den LKW des Lieferanten durch das Tor, damit dieser die Lieferung direkt zustellt. Kennt er den Lieferanten jedoch nicht, dann verabschiedet er den LKW-Fahrer nach Ausladung der Lieferung und bestellt den firmeneigenen Fahrer, der im eigenen LKW das Paket zum Empfänger bringt.

Je nach Umfang des Heim- oder Gebäudeautomationsnetzes sollte eine entsprechende Firewall eingesetzt werden. Weitergehende Informationen, welche Anforderungen eine Firewall erfüllen sollte, sind vom BSI erhältlich.[21]

6.2.4 Security-Gateways

Ein Sicherheitsgateway ist der vom Bundesamt für Sicherheit in der Informationstechnik (BSI) in den IT-Grundschutz-Katalogen gekürter Name, der alle IT-Systeme umfasst, welche für IT-Sicherheit in einer Organisation Sorge tragen.

Dazu gehören eine oder mehrere topologisch sinnvoll eingesetzte Firewalls, der Betrieb von Screened Subnets (Demilitarized Zones) und deren schützenswerten Serversystemen mit diversen Diensten, Proxyserver zur inhaltlichen Kontrolle des Datenflusses zwischen dem Internet und dem LAN, sowie die aktiven Netzwerkkomponenten wie Router und Switches, welche die IT-Systeme im Sicherheitsgateway miteinander via Ethernet verbinden.
(http://de.wikipedia.org/wiki/Sicherheitsgateway, 2014)

6.2.5 Verschlüsselte Kommunikation

Ziel der Verschlüsselung ist es, Daten in einer solchen Weise einer mathematischen Transformation zu unterwerfen, dass es einem Angreifer nicht möglich ist, die Originaldaten aus den transformierten Daten zu rekonstruieren.

[21] *https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/baust/b03/b03301.html*

Damit die verschlüsselten Daten für ihren legalen Benutzer noch verwendbar bleiben, muss es diesem jedoch möglich sein, durch Anwendungen einer inversen Transformation aus ihnen wieder die Originaldaten zu regenerieren.
Die Originaldaten werden mit „Klartext“ (clear text, plain text, message) bezeichnet. Die transformierten Daten werden „Schlüsseltext“ (Chiffretext, Chiffrat, Kryptogramm, cipher text) genannt. Die Tranformation selbst wird als „Verschlüsselung“, ihre Inverse als „Entschlüsselung“ bezeichnet.

Als Verschlüsselungsverfahren sollen hier das symmetrische und das asymmetrische Verfahren kurz beschrieben werden.

Symmetrisches Verschlüsselungsverfahren

Beim symmetrischen Verschlüsselungsverfahren wird für die Ver- und Entschlüsselung der Daten derselbe Schlüssel verwendet

Beim symmetrischen Verfahren wird für die Ver- und Entschlüsselung der Daten der gleiche Schlüssel verwendet. Es wird auch als Private-Key-Verfahren bezeichnet. Ein bekanntes symmetrisches Verschlüsselungsverfahren ist der AES-Algorithmus (Advanced Encryption Standard). Als Schlüssellänge sollte mindestens 128 Bit verwendet werden (BSI, 2014).

Vorteil der symmetrischen Verschlüsselung ist, dass dieses Verfahren sehr schnell ist. Nachteil ist, dass der Schlüssel zum Entschlüsseln der Daten von einem Kommunikationspartner zum anderen übertragen werden muss. Dazu ist eine sichere Methode zur Schlüsselverwaltung notwendig, damit der Schlüssel nicht in falsche Hände gerät.

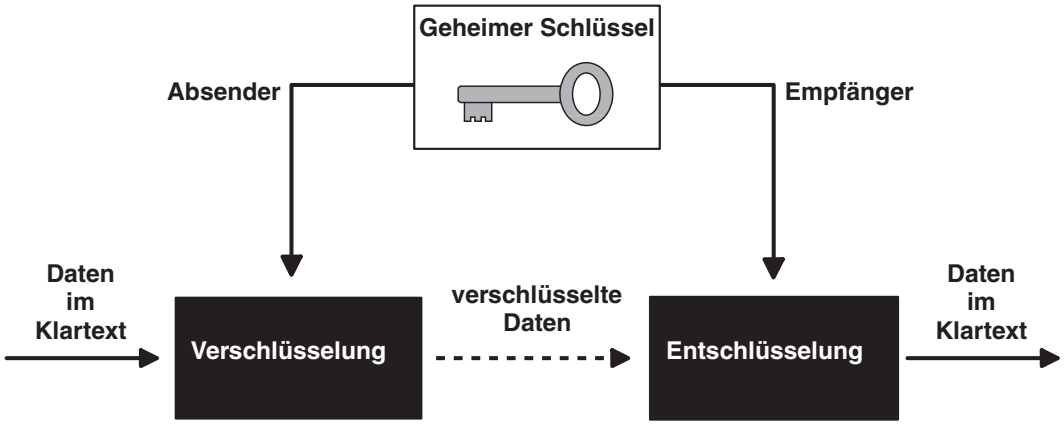


Abbildung 19: Symmetrische Verschlüsselung/ Private Key-Verfahren

Asymmetrisches Verschlüsselungsverfahren

Beim asymmetrischen Verschlüsselungsverfahren wird für die Verschlüsselung ein anderer Schlüssel verwendet als für die Entschlüsselung der Daten

Um die Schlüsselverteilung, das klassische Problem der Kryptographie, zu vereinfachen, wurden Verfahren entwickelt, die mit so genannten „öffentlichen Schlüsseln“ (public keys) arbeiten. Ein Public-Key-Verfahren oder asymmetrisches Verfahren arbeitet mit zwei verschiedenen Teilschlüsseln. Wird eine Verschlüsselung mit einem der beiden Teilschlüssel durchgeführt, kann nur mit dem entsprechenden passenden Teilschlüssel die korrekte Entschlüsselung erfolgen. Aus der Kenntnis des einen Teilschlüssels kann der andere nicht berechnet werden. Aus diesem Grund kann ein Teilschlüssel ohne Bedenken veröffentlicht werden. Dieser heißt „öffentlicher Schlüssel“. Der andere Schlüssel muss geheim gehalten werden und heißt dementsprechend „geheimer Schlüssel“.

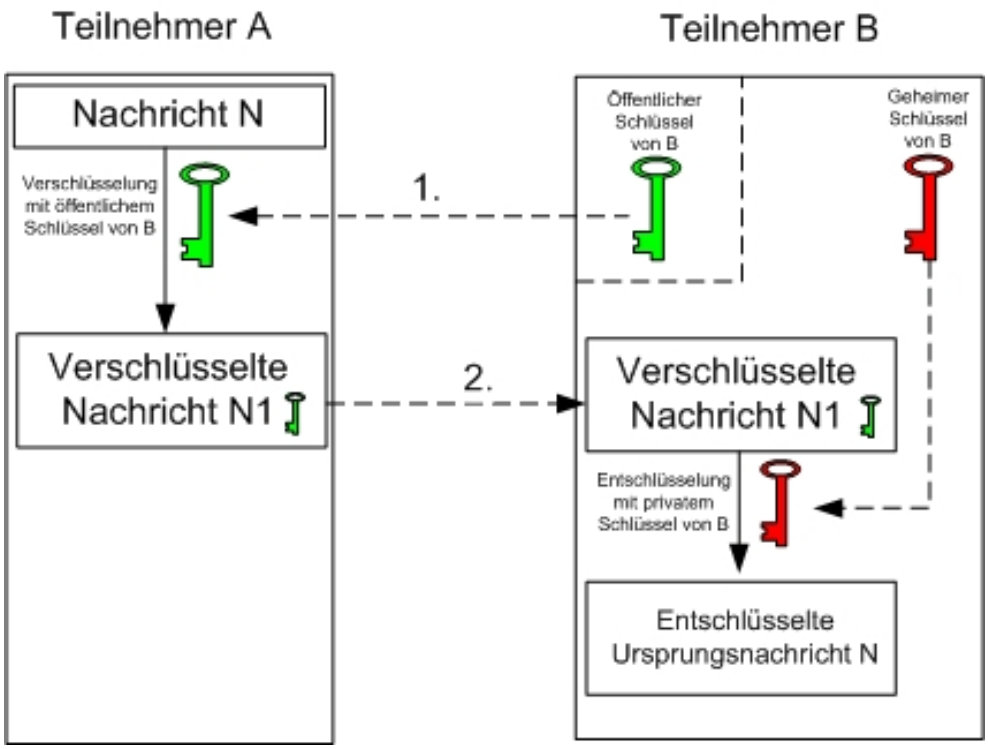


Abbildung 20: Asymmetrische Verschlüsselung/ Public Key-Verfahren

Praktische Anwendungen:

- Gesicherter Schlüsselaustausch von geheimen Schlüsseln
- Elektronische Signaturen
- Authentifizierung

Asymmetrische Verschlüsselung nutzen Sie jeden Tag, ob Sie nun auf Ihr Onlinebanking-Konto zugreifen oder wenn Sie über Ihren Browser auf einen Webmail-Account zugreifen. Dabei wird die Verbindung mittels HTTPS also mit einer SSL/TLS geschützten Verbindung gegen unbekannte Dritte abgesichert. Um eine solche Verbindung aufbauen zu können sind so genannte Stammzertifikate in jedem aktuellen Browser eingebunden. Über diese Zertifikate ist es möglich die Vertrauenswürdigkeit der Verbindung zu überprüfen. Dies erleichtert einem Nutzer zu erkennen ob der Kommunikationspartner wirklich derjenige ist, für den er sich ausgibt. Server ohne geprüfte Zertifikate werden deutlich Gekennzeichnet und ein Nutzer wird direkt vor einer Verbindung gewarnt.
Ein weiteres Beispiel ist die Verschlüsselung von Emails mittels PGP[22] oder S/Mime[23], dabei kommt ebenso eine asynchrone Verschlüsselung zum Einsatz, bei der sich die Kommunikationspartner gegenseitig Authentifizieren können. Bei S/Mime wird dies durch eine Zertifizierungsstelle übernommen. Ein Beispiel für eine solche Zertifizie-

[22] *http://de.wikipedia.org/wiki/Pretty_Good_Privacy E-Mail-Verschlüsselung mittels PGP*
[23] *http://de.wikipedia.org/wiki/S/MIME Standard für verschlüsselte E-Mail-Kommunikation mittels MIME*

rungsstelle ist D-TRUST[24] der deutschen Bundesdruckerei. PGP hingegen verlangt ein aktives und gegenseitiges Prüfen der Kommunikationspartner.

6.2.6 Subnetze

Das Bilden von Subnetzen, sogenanntes Subnetting, ermöglicht durch Konfiguration auf den Schnittstellen der Geräte, dass diese miteinander kommunizieren können oder nicht.
Dabei handelt es sich um eine von allen Netzwerkgeräten unterstützte Technologie, welche die Unterteilung von IP-Netzwerken vornimmt. Hierzu wird zu jeder IP-Adresse eine zusätzliche Nummer, die Subnetzmaske vergeben. Eine IP-Adresse unterteilt sich dann in einen Netzwerk(adress)teil und einen Host(adress)teil. Die genaue Aufteilung zwischen Netzwerkteil und Hostteil wird durch die Subnetzmaske bestimmt. Rechner befinden sich im selben Netz und können miteinander kommunizieren, wenn der Netzwerkteil ihrer Adresse gleich ist. Der Hostteil wird für jedes teilnehmende Gerät unterschiedlich vergeben. Für die Kommunikation zwischen den Netzen wird ein Router benötigt.
Die Konfiguration ist aufwendig, benötigt aber keine spezielle oder weitere Hardware. Aus diesem Grund ist es eine kostengünstige Möglichkeit der Netzseparierung.
Subnetting stellt aber keinen umfassenden Schutz her, da es durch gezielte Angriffe umgangen werden kann. Zudem besteht das Problem, dass der Empfang von Paketen nicht verhindert wird, sondern nur eine eventuelle Antwort.

6.2.7 Wahl sicherer Passwörter

Eine wichtige Rolle im Bereich passwortgeschützter Zugriffe spielt die Auswahl sicherer Passwörter.
Ein Angreifer, der versucht ein Passwort zu knacken, wird sich zum Beispiel der in Kapitel 5 beschriebenen Brute-Force-Methode bedienen. Dabei werden mit einem Programm einfach alle möglichen Zeichenkombinationen hintereinander ausprobiert, bis das richtige Passwort gefunden ist.

Bei passwortgeschützten Zugängen ist die Wahl eines sicheren Passworts von immenser Bedeutung für den Schutz gegen Hacker-Angriffe

Beim Erstellen eines Passworts stehen Ihnen in der Regel folgende Zeichen zur Verfügung:

- Zahlen (10 verschiedene: 0-9)
- Buchstaben (52 verschiedene: A-Z und a-z)
- Sonderzeichen (32 verschiedene).

Folgende Tabelle soll den Zusammenhang zwischen Länge und verwendeter Zeichen für die Sicherheit eines Passworts verdeutlichen. Dabei wird davon ausgegangen, dass der Angriff mit einem Rechner durchgeführt wird, der mit der Generierung von bis zu 2 Milliarden Schlüsseln pro Sekunde rechnet.

[24] *https://www.bundesdruckerei.de/de/176-d-trust-softtoken-class-ii D-TRUST Softtoken Class II*

Passwort besteht aus	Mögliche Kombinationen	Benötigte Zeit zum Entschlüsseln
5 Zeichen (3 Kleinbuchstaben, 2 Zahlen)	36^5= 60.466.176	60.466.176 / 2.000.000.000 = **0,03 Sekunden**
7 Zeichen (1 Großbuchstabe, 6 Kleinbuchstaben)	52^7= 1.028.071.702.528	1.028.071.702.528 / 2.000.000.000 = 514 Sekunden = **ca. 9 Minuten**
8 Zeichen (4 Kleinbuchstaben, 2 Sonderzeichen, 2 Zahlen)	68^8= 457.163.239.653.376	457.163.239.653.376 / 2.000.000.000 = 228.581 Sekunden = **ca. 2,6 Tage**
9 Zeichen (2 Großbuchsta-ben, 3 Kleinbuchstaben, 2 Zahlen, 2 Sonderzeichen)	94^9= 572.994.802.228.616.704	572.994.802.228.616.704 / 2.000.000.000 = 286.497.401 Sekunden = **ca. 9,1 Jahre**
12 Zeichen (3 Großbuchsta-ben, 4 Kleinbuchstaben, 3 Sonderzeichen, 2 Zahlen)	94^{12}= 475.920.314.814.253.376.475.136	475.920.314.814.253.376.475.136 / 2.000.000.000 = 237.960.157.407.127 Sekunden = **ca. 7,5 Millionen Jahre**

Quelle: (http://www.password-depot.de/know-how/brute_force_angriffe.htm, 2014)

Deutlich wird hier, wie wichtig die Wahl eines möglichst komplexen Passwortes ist. Zu beachten ist auch die rasante Entwicklung der Rechenleistung in der Computertechnik, womit sich die hier beispielhaft aufgeführten Zeiten zwangsläufig immer weiter verringern.
Passwortspeicherprogramme helfen bei der sicheren Ablage und Verwendung von starken Passwörtern für verschiedene Anwendungsbereiche. Schließlich sollte für jede Anwendung ein eigenes sicheres Passwort gewählt werden. Dies bedeutet zwar zunächst einen Mehraufwand – dennoch gilt es immer, einen deutlichen Sicherheitsgewinn gegenüber der Reduzierung der eigenen Bequemlichkeit abzuwägen. Ein Beispiel für ein Open-Source Passwortverwaltungsprogramm ist KeePass.

6.2.8 Zusammenfassung

Trotzdem Standards wie KNX oder BACnet ursprünglich keine oder wenige Sicherheitsfunktionen beinhalteten, gibt es einige Ansätze zur Verbesserung der IT-Sicherheit. Systeme, in denen diese Funktionen umgesetzt sind, sind jedoch noch wenig bis gar nicht vorhanden. Dies dürfte wohl auch nicht zuletzt auf mangelnde Sensibilität der Marktteilnehmer zurückzuführen sein.
Gerade wenn es um den Bereich Internetanbindung des Heim- oder Gebäudeautomationssystems geht, sollten unbedingt die in der Informationstechnik etablierten Sicherheitsfunktionen wie VPN, Firewall und die Auswahl von sicheren Passwörtern genutzt werden. Anwender sollten sich aktiv mit dem Thema IT-Sicherheit auseinandersetzen. IT-Verantwortliche in Betrieben sollten ihre Mitarbeiter für die Thematik der IT-Sicherheit auch im Hinblick auf Geräte- und Herstellerwahl sensibilisieren.

Notizen

7. Praxistipps

Im Folgenden, werden einige Praxistipps vermittelt.

7.1 Netzwerkkomponenten

Die wichtigste Netzwerkkomponente für die vielfach geforderte Funktionalität des Zugriffs auf das Automationsnetzwerkes über das Internet ist der entsprechende Router, der für die Internetanbindung des hauseigenen Netzwerkes zuständig ist.
Aus diesem Grund ist ein Router immer besonders sicher zu konfigurieren. Hierzu gehört die Abschaltung aller nicht benötigten Funktionen, die Verwendung sicherer Passwörter und ein gewissenhaftes Update-Management für die Router-Firmware.

Weitere Hinweise zur Konfiguration Ihres Routers im Handbuch „WLAN-Sicherheit“.
Das folgende Anwendungsbeispiel nennt exemplarisch die Einrichtung von VPN mittels eines Routers, in diesem Fall einer Fritzbox des Herstellers AVM.

Je nach Hersteller wird es kleine Unterschiede geben, aber die Grundfunktionen sind häufig dieselben. Es empfiehlt sich, vor der Entscheidung für ein Produkt die Leistungen und Sicherheitsfunktionen zu vergleichen und aktuelle Testberichte zu Rate zu ziehen.

7.2 Anwendungsbeispiel: VPN mit der Fritzbox

Wie in Abschnitt 6.2.1 beschrieben, ist die Einrichtung eines Virtual Private Networks (VPN) die empfehlenswerte Wahl bei der Übertragung von Daten zwischen zwei räumlich getrennten Netzwerken über das Internet.
Für eine Steuerung des Hauses per Smartphone über das Internet, wie es unser Bauherr aus dem Modellhaus in Kapitel 4 wünscht, bietet es sich daher an, zwischen dem Smartphone und dem hauseigenen Internetrouter eine VPN-Verbindung zu nutzen.
Einer der weit verbreitetsten Internetrouter in deutschen Haushalten ist die Fritzbox von der Firma AVM[25], deshalb sollen im Folgenden beispielhaft die wichtigsten Schritte beim Einrichten einer VPN Verbindung zwischen der Fritzbox und einem Smartphone beschrieben werden.

Notwendige Informationen

- **IPSec-ID des VPN-Benutzers**:
  Ein beliebiger Name, der keine Sonderzeichen enthalten sollte
- **Dynamic DNS-Domainname der FRITZ!Box**:
  Dynamic DNS ist ein Internetdienst, der es ermöglicht, dass die FRITZ!Box immer unter einem feststehenden Namen aus dem Internet erreichbar ist, obwohl sich die öffentliche IP-Adresse der FRITZ!Box ändert.
  Um diesen Dienst nutzen zu können, müssen Sie sich bei einem Dynamic DNS-Anbieter registrieren. Dabei vereinbaren Sie den feststehenden Namen

[25] *AVM Computersysteme Vertriebs GmbH, Berlin*

(Domainname), unter dem Ihre FRITZ!Box aus dem Internet erreichbar sein soll. Sie legen außerdem einen Benutzernamen und ein Kennwort fest.
[Quelle: http://service.avm.de/help/de/FRITZ-Box-7312/012/hilfe_dyndns]

- **IP-Netzwerk der FRITZ!Box**:
  Hiermit ist die Adresse der Fritzbox im Heimnetzwerk gemeint, zum Beispiel 192.168.10.0 (Subnetzmaske: 24 - 255.255.255.0)
- **IP-Adresse des VPN-Benutzers im FRITZ!Box-Heimnetz**:
  zum Beispiel 192.168.10.201
- **geheimes Kennwort** (siehe auch Kapitel 6.2.7)

[Quelle: http://avm.de/service/vpn/uebersicht/]

Programm "FRITZ!Box-Fernzugang einrichten"

Für die Konfiguration ist das Programm "FRITZ!Box-Fernzugang einrichten" zu verwenden. Dieses kann im Internet heruntergeladen werden. Ergebnis der Konfiguration über diese Programm ist die Erstellung zweier Dateien: "fritzbox_[...].cfg" und "iphone_[...].txt"

VPN-Einstellungen in FRITZ!Box importieren

In der Benutzeroberfläche der Fritzbox gilt es nun, die vorher erzeugte Datei "fritzbox_[...].cfg" zu importieren.

VPN-Einstellungen im Smartphone

Im Smartphone müssen nun die entsprechenden Informationen aus der vorher erzeugten Textdatei bei der Konfiguration eines neuen VPN-Netzwerkes (unter „Erweiterte Einstellungen“ > „VPN“) eingetragen werden
Eine detaillierte Vorgehensweise, die zum eigenen Smartphone-Betriebssystem passt, ist unter http://avm.de/service/vpn/uebersicht/ zu finden.

7.3 Clientsicherheit

Zur Interaktion mit der Gebäudeautomation können Desktop- und mobile Endgeräte, sogenannte Clients, dienen. Ein einziger unzureichend abgesicherter Client stellt ein Einfallstor für ein sicheres System dar. Beispielsweise kann dies durch eine Schadsoftware geschehen, die Tastatureingaben mitliest und protokolliert. Da über die Tastatur auch Passwörter eingegeben werden, sind diese unmittelbar gefährdet. Daher sollen im Folgenden einige Maßnahmen aufgelistet werden, mit denen ein grundlegendes Maß an Sicherheit gewährleistet werden kann.

Desktop-Clients

- Virenscanner installieren und aktuell halten
- Firewall, die den Zugriff auf Programmebene einschränkt
- Regelmäßige Updates des Betriebssystems

Mobile-Clients

- Aktuelle Software
- Zugriffsschutz mit starkem Passwort
- Verschlüsselung des Gerätes, sofern möglich
- Apps nur mit Bedacht installieren. Geforderte Rechte jeder App prüfen und kritisch hinterfragen
- Geräte nicht aus der Hand geben und bei Verlust sofort sperren lassen

7.4 Tipps für die Installation

Im Folgenden werden einige Möglichkeiten der Absicherung von Heim- und Gebäudeautomationssystemen beschrieben, die sich auf den Bereich Installation beziehen.

7.4.1 Zugänglichkeit von Bus und Geräten

Viele Kommunikationsprotokolle für die Heim-und Gebäudeautomation bieten von Haus aus aktuell bestenfalls rudimentär implementierte Sicherheitsfunktionen. Es empfiehlt es sich deshalb generell, die Zugänglichkeit zum Netzwerk für potenzielle Angreifer bestmöglich abzusichern. Geräte mit Busanschluss können deshalb schon installationstechnisch gegen unbefugten Zugriff gesichert werden, beispielsweise durch abschließbare Installationsverteiler.

Einfache Zugänglichkeit von Geräten mit Busanschluss und Businstallationen im Außenbereich können einem Angreifer in die Karten spielen

Ein weiterer kritischer Punkt kann die Installation des Buskabels im Außenbereich sein. Oftmals sollen bestimmte Wetterdaten erfasst werden, wie Außenhelligkeit, Windgeschwindigkeit oder Außentemperatur. Dazu müssen Sensoren installiert werden, die technisch in der Lage sind, die jeweiligen Messdaten in ein entsprechendes Telegramm umzuwandeln, welches das jeweilige Automationssystem verarbeiten kann (zum Beispiel in ein KNX-Telegramm). Hier gibt es Sensoren, die diese Umwandlung direkt vornehmen. Der Nachteil ist, dass dazu die Busleitung nach draußen geführt werden muss, welche dann direkt an den Sensor angeschlossen wird. Ein Angreifer hätte hier leichtes Spiel; wenn er das Gerät abmontiert, hat er direkten Zugriff auf den Bus, ohne ins Haus zu müssen.
Die sicherere Wahl wäre hier ein Sensor, der die Messwerte nicht direkt als Telegramm zur Verfügung stellt, sondern als elektrisches Signal, welches dann erst von einem Sensormodul (im Haus) in ein Telegramm umgewandelt wird.

Beispiel:
Die Außentemperatur wird von einem Sensor gemessen und als elektrische Spannung zwischen 0 und 10V zur Verfügung gestellt. Dazu stellt der Sensor einen Ausgang bereit, der entsprechend der gemessenen Temperatur einen Spannungswert wie in der folgenden Grafik dargestellt liefert.

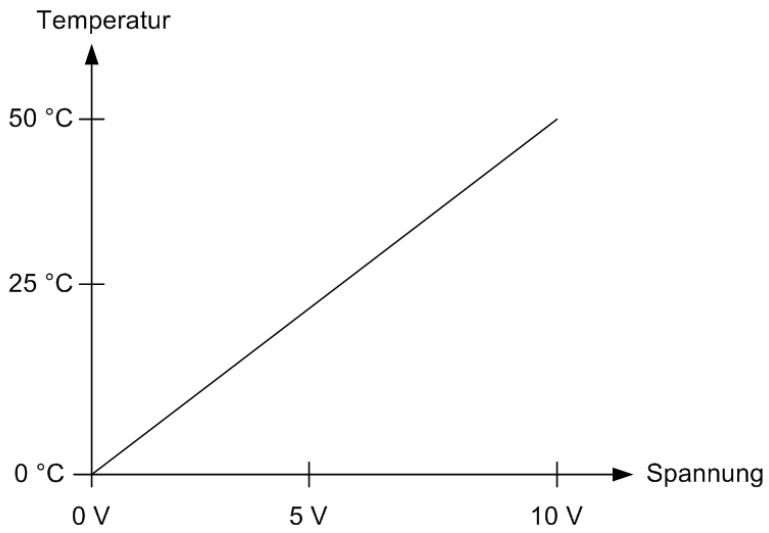


Abbildung 21: Temperatur-Spannungsverhältnis

Die Spannung, die der Sensor ausgibt, kann dann über eine Leitung auf einen Bus-Gerät angeschlossen werden, welches über einen entsprechenden (0-10V-) Eingang verfügt und in einem Unterverteiler installiert ist. Die Umwandlung des Signals in ein Datentelegramm findet dann erst im Haus über das Gerät im Verteiler statt und es muss kein Buskabel nach draußen geführt werden.

7.4.2 Überwachung der Buskomponenten

Für Installationen in besonders kritischen Bereichen empfiehlt sich die Verwendung eines Abziehschutzes für frei zugängliche Busteilnehmer und die Nutzung von Alarmüberwachungs-funktionen

In manchen Fällen lässt sich die Installation von Buskomponenten in kritischen Bereichen (oft aus Kostengründen) nicht vermeiden.
Zwar ist es nicht unbedingt wahrscheinlich, dass jemand in den eigenen vier Wänden unbemerkt einen Schalter aus der Wand ausbaut, um sich dort mit seinem Laptop anzuschließen und irgendwelchen „Unfug“ zu treiben. Jedoch bei anderen Gebäudearten, wie Mehrfamilienhäusern mit busfähigen Schaltern in Treppenhäusern, stellt sich die Situation schon anders dar. Noch kritischer ist die Betrachtung bei der Installation von Buskomponenten in Hotelzimmern: Hier hätte ein Gast mit entsprechend bösartigen Absichten bei einer unzureichend gesicherten Anlage ausreichend Zeit, Komponenten wie Schalter auszubauen und sich in aller Ruhe „auszutoben“. Noch das „Bitte nicht stören“-Schild von außen an die Tür – und los geht’s!
Für solche Fälle empfehlen sich weitere Sicherheitsmaßnahmen. Einige Hersteller bieten neben einem mechanischen Abziehschutz auch eine Überwachungsfunktion für Busteilnehmer an. Diese können zyklisch auf Verfügbarkeit überprüft und es können Alarmmeldungen generiert werden, wenn zum Beispiel jemand ein Schalteroberteil demontiert.

7.5 Praxistipps: Zusammenfassung

Für die Anbindung des Automationsnetzwerkes an das Internet ist die Einrichtung einer VPN-Verbindung mit dem hauseigenen Internetrouter empfehlenswert.
Die Endgeräte, die dann für die Fernsteuerung des Hauses genutzt werden (Smartphones, Tablets) sollen ausreichend vor Schadsoftware und mit starken Passwörtern geschützt werden.
Weiterhin können Maßnahmen ergriffen werden, um es einem potenziellen Angreifer nicht unnötig leicht zu machen (Vermeidung von Busleitungen im Außenbereich und Absicherung einzelner Geräte gegen unerlaubte Demontage).

Notizen

8. Checkliste

IT-Sicherheit im Handwerk

Checkliste IT-Sicherheit

Gefördert durch:

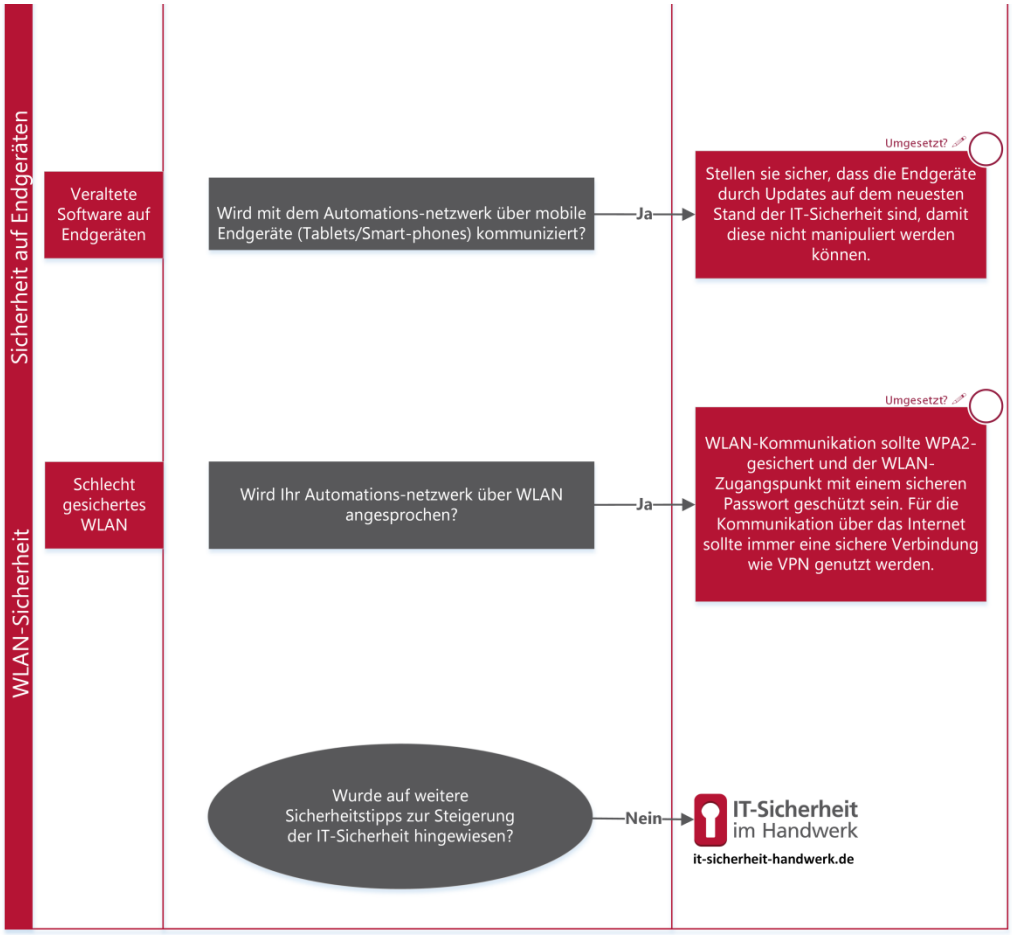
Bundesministerium für Wirtschaft und Energie

aufgrund eines Beschlusses des Deutschen Bundestages

TASK FORCE IT-SICHERHEIT IN DER WIRTSCHAFT
Mehrwert und Schutz für Rechner.

IT-Sicherheit im Haus der Zukunft

	Gefahr/ Risiko	Erhebung des Ist-Zustands		Maßnahme
Updatemechanismen	Fehlende Updates	Bietet der Hersteller der Geräte regelmäßige Sicherheitsupdates an?	Nein	Umgesetzt? Erkundigen Sie sich nach Alternativen von Herstellern, die durch regelmäßige Updates dem Nutzer die Möglichkeit geben, sein System auf dem neuesten Sicherheits-stand zu halten.
Installationshinweise	Fehlende Zugriffs-beschränkung	Sind Geräte mit direktem Busanschluss nur für befugte Personen zugänglich?	Nein	Umgesetzt? Nutzen Sie mechanische und kommunikative Vorkehrungen (wie abschließbarer Installationsverteiler oder Demontage-schutz von Bediengeräten)
		Müssen Geräte im Außenbereich installiert werden?	Ja	Umgesetzt? Verwenden Sie keine Geräte mit direktem Busanschluss, sondern greifen Sie möglichst auf konventionelle Geräte zurück, die erst über im Gebäude installierte Busgeräte auf das Automationssystem aufgeschaltet werden.
Vertraulichkeit	Unbemerkter Zugriff durch Dritte	Gibt es Geräte, die mit dem Internet verbunden sind?	Ja	Umgesetzt? Prüfen Sie, ob eine Verbindung zum Internet zwingend erforderlich ist. Sofern Geräte mit dem Internet verbunden sind, sollte dies nur über eine gesicherte Verbindung wie beispielsweise VPN möglich sein.
	Fehlende Übertragungs-verschlüssel-ung	Gibt es Geräte mit integriertem Webserver?	Ja	Umgesetzt? Stellen Sie sicher, dass die Verbindung zum Webserver nur über ein sicheres Passwort möglich ist. Außerdem sollte eine abgesicherte Kommunikation über HTTPS möglich sein.



TASK FORCE
IT-SICHERHEIT IN DER WIRTSCHAFT
Mehrwert und Schutz für Rechner.

Task Force „IT-Sicherheit in der Wirtschaft“
Die Task-Force „IT-Sicherheit in der Wirtschaft“ ist eine Initiative des Bundesministeriums für Wirtschaft und Energie, die gemeinsam mit IT-Sicherheitsexperten aus Wissenschaft, Wirtschaft und Verwaltung vor allem kleine und mittelständische Unternehmen für IT-Sicherheit sensibilisieren und dabei unterstützen will, die Sicherheit der IKT-Systeme zu verbessern. Weitere Informationen zur Task-Force und ihren Angeboten sind unter:

www.it-sicherheit-in-der-wirtschaft.de abrufbar

www.it-sicherheit-handwerk.de

itb- Institut für Technik der Betriebsführung im Deutschen Handwerksinstitut e.V.

Heinz-Piest-Institut für Handwerkstechnik an der Leibniz Universität Hannover

Handwerkskammer Rheinhessen, Kompetenzzentrum für IT-Sicherheit und qualifizierte digitale Signatur

if(is) - Institut für Internet-Sicherheit der Westfälischen Hochschule

9. Stichwortverzeichnis

K

L

M

N

O

P

R

S

T

U

V

W

Z

10. Abbildungsverzeichnis

11. Literaturverzeichnis/Weblinks

Arnold, H. (2012). *http://www.energie-und-technik.de/automatisierung/news/article/90516/*.

b+b Automations- und Steuerungstechnik GmbH. (2014). *http://www.bb-steuerungstechnik.de/cms/de/produkte/gebaeudeautomation/eibknx-betriebssicherheit/eibknx-betriebssicherheit/knxguard-der-sicherheitsbaustein.html.*

BSI. (2014). *https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102_pdf.pdf?__blob=publicationFile*.

Check24. (2012). *http://www.check24.de/studien/smart-meter-umfrage-interesse-zahlungsbereitschaft-180612-10161/*.

DIN EN ISO 16484-2. (2004).

Fouladi, G. (2013). *https://code.google.com/p/z-force/*.

Granzer, W. (2010). *http://www.auto.tuwien.ac.at/~wgranzer/dissertation_wolfgang_granzer_final_signed.pdf.*

Hariharasudhan, C. S. (2014). *http://www.all-electronics.de/texte/anzeigen/53237/Der-Wireless-M-Bus-im-Smart-Grid*.

http://blog.botfrei.de/2012/05/bluetooth-ein-sicherer-standard/. (2012).

http://de.wikipedia.org/wiki/Bluetooth#Aktueller_Standard:_Bluetooth_4.0. (2010).

http://de.wikipedia.org/wiki/Sicherheitsgateway. (2014).

http://de.wikipedia.org/wiki/Smart_Home. (2013).

http://www.itwissen.info/definition/lexikon/ZigBee-Sicherheit-ZigBee-security.html. (2014).

http://www.password-depot.de/know-how/brute_force_angriffe.htm. (2014).

https://de.wikipedia.org/wiki/Universal_Plug_and_Play#Verwundbarkeiten.2C_die_2013_entdeckt_wurden. (2014).

https://opcfoundation.org/about/what-is-opc/. (2014).

Kastner, W. G. (2011). Security Analysis of Open Building Automation Systems.

Kranz, H. R. (2013). *BACnet Gebäudeautomation 1.12.* cci Buch.

Ohland. (2012). *http://www.connected-home.de/kaufberatung/geheimfunker-1479624.html*.

Pohlmann. (2003). *Firewall-Systeme.*

Pohlmann/Linnemann. (2010). *Sicher im Internet.*

Ray, B. (2013). *http://www.theregister.co.uk/2013/08/13/wave_goodbye_to_security_with_zwave/*.

Schürmann. (2014). *www.enbausa.de/lueftung-klima/aktuelles/artikel/it-sicherheit-im-smart-home-ist-oft-unzureichend-3978.html*.

t3n. (2014). *http://t3n.de/news/shodan-erschreckendste-455939/.*

9 783944 916125