BACtag – Data Leakage Protection für Gebäude

Eva Maria Anhaus[1] · Steffen Wendzel[2]

[1]FernUniversität Hagen
eva.anhaus@fernuni-hagen.de

[2]Fraunhofer FKIE
steffen.wendzel@fkie.fraunhofer.de

Zusammenfassung

Netze der Gebäudeautomation sind potentiell – wie jedes andere Netzwerk – nicht vor Sicherheitsproblemen gefeit. Viele Sicherheitslücken wurden bereits geschlossen, für andere müssen erst Ansätze ausgearbeitet werden. Dieser Beitrag konzentriert sich auf Data Leakage in der Gebäudeautomation. Bisher wurde dieses Thema in der Literatur kaum aufgegriffen. Neben einer Einführung in die Problematik soll dieser Beitrag auch einen konkreten Lösungsvorschlag für den praktischen Einsatz unter Verwendung von BACnet vorstellen, welcher durch eine einfache Umsetzung und ohne kostenintensive Maßnahmen Vorkehrungen gegen Data Leakage in der Gebäudeautomation realisiert.

1 Einleitung

Der Bereich Gebäudeautomation hat in den letzten Jahren einen wahren Boom erfahren. Längst sind es nicht mehr nur die Kernbereiche Heizungs-, Lüftungs- und Klimatechnik, welche durch die Gebäudeautomation abgedeckt werden. Die Hausautomation als Teilbereich der Gebäudeautomation hat sich in den Wohnzimmern des technisch interessierten Gebäudebesitzers etabliert und ist durch einfache Konfiguration und intuitive Handhabung für jedermann zugänglich geworden. Der Sicherheitsaspekt wurde dabei allerdings eher stiefmütterlich behandelt– die Devise lautete „Funktionalität“. Was aber, wenn die Daten im Gebäudenetzwerk sensibler Natur sind und ein Abfließen derselben eine Preisgabe von personenbezogenen Informationen bedeutet? Betrachten wir als Beispiel den Bereich Ambient Assisted Living, in welchem die Gebäudeautomation der Beibehaltung der Selbständigkeit von körperlich eingeschränkten Personen dient, so ist das Risiko des Abflusses von sensiblen Daten durchaus gegeben. Sensoren, welche die Vitalparameter von kardiologisch vorbelasteten Personen an das Gebäudenetzwerk weitergeben, übermitteln unter anderem Daten, welche für die Pharmaindustrie von wirtschaftlichem Interesse sein könnten – ganz abgesehen von einer eklatanten Verletzung der Privatsphäre.

1.1 Problemstellung

Die Gebäudeautomation unterscheidet sich in einigen Aspekten von der konventionellen IT: häufig kommen Geräte zum Einsatz, welche nur über eine eingeschränkte Rechenleistung ver-

P. Schartner · K. Lemke-Rust · M. Ullmann (Hrsg.) · D•A•CH Security 2015 · syssec (2015) 417-428.

fügen, die Netzwerkverbindungen sind oftmals durch einen niedrigen Datendurchsatz gekennzeichnet. Insbesondere ist es allerdings ein weiterer Faktor, welcher den Einsatz von „konventionellen“ Sicherheitslösungen wie Firewalls in der Gebäudeautomation verhindert: die dort verwendeten Protokolle unterscheiden sich von denen der IT-Welt. Beispielhaft für die Reihe von Protokollen, welche in der Gebäudeautomation zum Einsatz kommen, soll in diesem Beitrag BACnet betrachtet werden. Die DIN EN ISO 16484-5 [DIN+12] sieht zwar Möglichkeiten zur Verschlüsselung des Netzwerkverkehrs vor, allerdings kommen diese in der Praxis bisher kaum zum Einsatz. Zum jetzigen Zeitpunkt gibt es keine ausgereifte Sicherheitslösung, welche den Datenfluss im Automationsnetzwerk kontrollieren und begrenzen kann.

1.2 Relevanz

Auch wenn der Bereich Gebäudeautomation schon seit den 1950er Jahren besteht, so geht die Einführung von Sicherheitslösungen eher schleppend vonstatten. Erst in den letzten Jahren hat sich der Fokus der Forschung in diesem Sektor vermehrt auf dieses Thema verlagert, wenn auch die Optimierung der Funktionalität nach wie vor im Vordergrund steht. Gerade für „neue“ Bereiche wie Ambient Assisted Living, welche sensible, personenbezogene Daten in das Netzwerk einbringen, erscheint die Umsetzung von Sicherheitsmaßnahmen allerdings beinahe unverzichtbar.

Die Einführung von Sicherheitsmaßnahmen in der Gebäudeautomation scheiterte oftmals an der komplexen praktischen Konfiguration oder am Kostenfaktor. Einige Ansätze, welche in den letzten Jahren vorgestellt wurden, finden in Abschnitt 2 Erwähnung.

Die in diesem Beitrag vorgestellte Lösung zeichnet sich durch eine simple Konfiguration und niedrige Investitionskosten aus.

1.3 Beitrag

In diesem Beitrag soll eine Möglichkeit erläutert werden, welche den Traffic in einem Gebäudenetzwerk im Hinblick auf sensible Daten reglementiert und es auf diese Art ermöglicht, Data Leakage in der Gebäudeautomation vorzubeugen.

1.4 Struktur

Nach einer kurzen Vorstellung von Related Work in Kapitel 2 wird in Kapitel 3 nach einer Einführung in die Thematik (3.1) ein Ansatz zur Vermeidung von Data Leakage vorgestellt (3.2), bevor in Abschnitt 3.3 auf die praktische Umsetzung eingegangen wird. Die Evaluation erfolgt in Kapitel 4, bevor in Kapitel 5 ein Fazit gezogen und ein Ausblick auf die zukünftige Entwicklung gewagt wird.

2 Related Work

Bereits in den 2000er Jahren wurde erkannt, dass die Sicherheit auch in der Gebäudeautomation nicht vernachlässigt werden darf. 2003 erschien im ASHRAE Journal ein Artikel mit dem Titel „Enemies at the Gates“ [Holm03], welcher darauf hinweist, dass die Öffnung der Protokolle in der Gebäudeautomation neue Sicherheitsrisiken in sich birgt. Im Jahr 2005 geht David G. Holmberg erneut auf dieses Thema ein und schlägt in [Holm05] konkrete Maßnahmen vor,

welche eine sichere Kommunikation im Gebäudenetzwerk ermöglichen sollen. Die von Holmberg vorgeschlagene Verschlüsselung und in [DIN+12] für BACnet definierten Verfahren konnten sich bis dato allerdings nicht in der Praxis durchsetzen.

2010 greifen auch Granzer et al. in [GrPK10] das Thema Verschlüsselung und sichere Kommunikation in der Gebäudeautomation auf, wobei das Hauptaugenmerk dieser Publikation allerdings auf potentielle Angriffe von außerhalb des Netzwerkes gerichtet ist.

Zwei Jahre später präsentieren Wendzel, Kahler und Rist in [WeKR12] ein Paper, in dem sie auf das Risiko von verdeckten Kanälen in der Gebäudeautomation hinweisen und die Einführung einer mehrstufigen Sicherheitslösung unter Einsatz des BACnet Firewall Routers (BFR) vorschlagen. Der dort vorgestellte Ansatz kann durchaus auch für Data Leakage Protection eingesetzt werden, allerdings gestaltet sich die Konfiguration, welche stark auf die physische Organisation des Netzwerkes gestützt ist, als eher umständlich.

Konkrete Maßnahmen, welche die Sicherheit innerhalb des Gebäudenetzwerkes verbessern sollen, werden von Neilson in [Neil13] zusammengefasst.

3 Contribution

Mit dem starken Wachstum des Marktsegments Gebäudeautomation hat sich die Notwendigkeit ausgereifter Sicherheitsvorkehrungen immer mehr herauskristallisiert. Selbst wenn keine spezifisch auf die Gebäudeautomation bezogenen Statistiken über Data Leakage vorliegen, so ist anzunehmen, dass auch diese von einem unerwünschten Datenabfluss nicht verschont geblieben ist und auch weiterhin davon betroffen sein wird. Das daraus resultierende Schadenspotential ist nicht zu unterschätzen.

Der vorliegende Beitrag soll ein Plus an Sicherheit in die Gebäudeautomation einbringen, indem er einem unerwünschten Datenabfluss vorbeugen soll.

3.1 Grundlagen

Damit die in diesem Paper vorgeschlagen Konzepte verständlicher werden, folgt nun in den Abschnitten 3.1.1 und 3.1.2 eine genauere Definition der Begriffe „Data Leakage“ und „BACnet“, Abschnitt 3.1.3 gibt einen Überblick über die Angriffsvektoren im Gebäudenetzwerk. Abschnitt 3.2 stellt den Ansatz zur Vermeidung von Data Leakage in der Gebäudeautomation dar, bevor in Abschnitt 3.3 auf die Vorgehensweise bei der praktischen Umsetzung der DLP-Lösung eingegangen wird.

3.1.1 Data Leakage

Um ein Verständnis für Data Leakage in der Gebäudeautomation zu ermöglichen, gilt es natürlich, den Begriff Data Leakage abzugrenzen und zu definieren. Shabtai et al. definieren in [ShER12] Data Leakage als „versehentliche oder ungewollte Verteilung privater oder sensibler Daten an einen nicht berechtigten Dritten“. Der vorliegende Beitrag schließt sich dieser Definition an. Bei einer Data-Leakage-Protection-Lösung muss es sich also um eine Lösung handeln, welche diese versehentliche oder ungewollte Verteilung von Daten eindämmen oder bestenfalls sogar gänzlich unterdrücken kann.

3.1.2 BACnet

Als einer der wichtigsten (im amerikanischen Raum der meistverbreitete) Vertreter der in der Gebäudeautomation verwendeten Protokolle soll im weiteren Verlauf des Beitrags BACnet als Referenzprotokoll verwendet werden. BACnet wird in der Norm DIN EN ISO 16484-5:2012 „Systeme der Gebäudeautomation – Teil 5: Datenkommunikationsprotokoll“ [DIN+12] spezifiziert. Im Grunde handelt es sich bei BACnet nicht um ein einziges Protokoll, sondern um einen Protokollstapel. Der Aufbau des BACnet-Protokollstapels ist aus Abbildung 1 ersichtlich. Die Kommunikation in BACnet findet nach dem Client-Server-Prinzip, wie es auch in der „konventionellen“ IT verwendet wird, statt (Request-Reply-Verhalten). Der Protokollstapel von BACnet ist in 4 Schichten organisiert, welche in den nächsten Abschnitten kurz eingeführt werden.

Die Mannigfaltigkeit von Protokollen auf Layer 1 und 2 rührt daher, dass in der Gebäudeautomation eine Vielzahl von Techniken zur Vernetzung der Geräte zum Einsatz kommt. Dies ermöglicht eine flexible Vernetzung unter Verwendung verschiedener Technologien, u.a. kabellose Verbindung (ZigBee), serielle Verbindungen (RS232) oder Ethernet (IEEE 802.3).

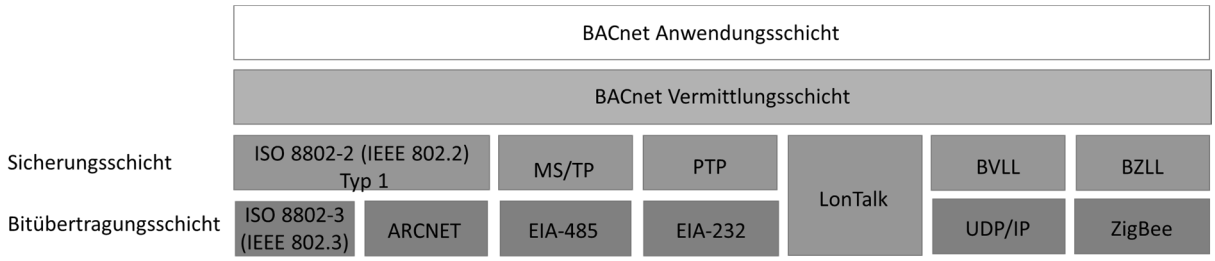

Abb. 1: BACnet Protokollstapel

Einen Sonderstatus im BACnet-Protokollstapel nimmt BACnet/IP ein. BACnet/IP wird im Anhang J der DIN EN ISO 16484-5:2012 [DIN+12] definiert. Sollen zwei Gebäudenetzwerke, welche durch ein dazwischenliegendes IT-Netzwerk getrennt sind, miteinander kommunizieren können, so bietet sich die Verwendung von BACnet/IP an. BACnet/IP kommt allerdings oftmals auch in der direkten Kommunikation zwischen Geräten, welche BACnet/IP unterstützen, zum Einsatz. IP wird in der Gebäudeautomation aus Performancegründen in Kombination mit UDP (normalerweise Port 47808) eingesetzt, da der Overhead bei der Verwendung von TCP wesentlich höher liegen würde. Im Unterschied zu konventionellen Netzwerken ist BACnet/IP nicht auf den ISO/OSI-Schichten 3 bzw. 4 angesiedelt, sondern auf Layer 1 (UDP/IP) bzw. Layer 2 (BACnet Virtual Link Layer, BVLL).

Auf Layer 3 befindet sich die BACnet Vermittlungsschicht. Diese dient dazu, die Kommunikation zwischen mehreren Automationsnetzen zu ermöglichen und ist für die Vermittlung von Paketen zwischen den Netzwerken zuständig.

Auf Layer 4 ist die BACnet Anwendungsschicht angesiedelt. Die Transport-, Sitzungs-, Darstellungs- und Anwendungsschicht werden bei BACnet zu einer einzigen Anwendungsschicht zusammengefasst. Dieser Layer übernimmt damit auch mehrere Aufgaben, welche im ISO/OSI-Referenzmodell in höheren Schichten untergebracht sind.

3.1.3 Angriffsvektoren im Gebäudenetzwerk

Wie auch „konventionelle“ IT-Netzwerke sind die Netzwerke im Bereich der Gebäudeautomation nicht vor Angriffen gefeit. Exemplarisch sollen an dieser Stelle einige Angriffsvektoren angeführt werden, welche für die Gebäudeautomation erwähnenswert erscheinen.

Denial-of-Service (DoS)-Angriffe: Bei Denial-of-Service-Angriffen versucht der Angreifer, das Netzwerk bzw. einzelne Komponenten durch eine Überflutung mit Paketen außer Betrieb zu setzen. Angriffe dieser Art sind im Gebäudenetzwerk ebenso wie in IT-Netzwerken möglich. Die Lösungsansätze für eine Vermeidung von DoS-Angriffen unterscheiden sich in der Gebäudeautomation aufgrund der reduzierten Systemressourcen und der Verwendung anderer Protokolle von der konventionellen IT. Einen Ansatz, wie dieser Thematik in der Gebäudeautomation begegnet werden kann, stellen Granzer et al. in [GrRK08] vor.

Sniffing: Das Mitlesen des Datenverkehrs wird als Sniffing bezeichnet. Werden die physischen Zugänge zum Gebäudenetzwerk nicht hinreichend abgesichert, so kann der (meist unverschlüsselte) Datenverkehr relativ einfach mit Tools wie Wireshark mitgelesen werden.

Spoofing: Spoofing (auch Maskierungsangriff genannt) ist ein Angriff, bei welchem ein Gerät vorgibt, ein anderes (bereits im Gebäudenetzwerk integriertes) zu sein. Angriffe auf Gebäudenetzwerke laufen hierbei praktisch identisch zu jenen in IT-Netzwerken ab. Gibt ein Gerät dabei vor, der Router im Gebäudenetzwerk zu sein, so ist es ein Leichtes, einen Großteil der Kommunikation abzuhören.

Angriffe von außen: Die Anbindung des Gebäudenetzwerkes an öffentliche Netzwerke (Internet) sorgt nicht nur für eine einfache Erreichbarkeit, sondern bietet auch zusätzliche Angriffsfläche für Eindringlinge. Umso wichtiger ist eine restriktive Konfiguration der Schnittstellen (Security-Gateways) zwischen dem Gebäudenetzwerk und dem öffentlichen Netzwerk, sodass diese Zugangspunkte nur einem klar definierten Benutzerkreis zur Verfügung stehen. An dieser Stelle können Sicherheitskonzepte aus der konventionellen IT genutzt werden (z.B. VPN).

Einen Überblick über mögliche Angriffsszenarien bieten Wendzel und Szlósarczyk in ihrem Beitrag zur „Hack in the Box“ Amsterdam im Mai 2014 [WeSz14].

3.2 Ansätze zur Vermeidung von Data Leakage

Zur Ausarbeitung einer Lösung, welche zur Vermeidung von Data Leakage dient, muss geklärt werden, an welchen Punkten in einem Netzwerk dieser Abfluss von Daten stattfinden kann. Shabtai et al. haben in [ShER12] dafür die Punkte „Data at Rest“, „Data in Use“ und „Data in Motion“ ausfindig gemacht. Unter „Data At Rest“ sind dabei sämtliche persistenten Daten, wie beispielsweise Datenbanken auf Managementstationen, zusammengefasst. Bei „Data in Motion“ handelt es sich um Daten, welche für die aktuellen Operationen benötigt werden (z.B. Werte, welche sich für aktuelle Berechnungen im RAM befinden). „Data in Motion“ hingegen bezeichnet jene Daten, welche sich auf den Übertragungswegen (Netzwerk) befinden, so z.B. Sensordaten, welche gerade vom Sensor an die Managementstation übertragen werden. Diese potentiellen Abfluss-Stellen sind in einem Gebäudenetzwerk genauso wie in einem IT-Netzwerk anzutreffen. Während für „Data at Rest“ und „Data in Use“ DLP-Lösungen aus der IT-Welt durchaus auch für den Einsatz in der Gebäudeautomation geeignet sind – häufig sind Managementstationen mit Standard-Betriebssystemen ausgestattet –, ist die Situation für „Data

in Motion“ eine grundlegend andere. Da in der Gebäudeautomation eigene Protokolle verwendet werden, sind es gerade die Daten auf den Übertragungswegen, für welche in einem Gebäudenetzwerk ein neuer Ansatz gesucht werden muss.

Die Norm DIN EN ISO 16484-5 [DIN+12] sieht die Möglichkeit einer verschlüsselten Kommunikation vor. In der Praxis wird diese allerdings kaum verwendet, nicht zuletzt aufgrund der Tatsache, dass die Rechnerleistung in der Gebäudeautomation oftmals begrenzt ist.

3.2.1 Tagging – BACtag

Um eine spätere Filterung von sensiblen Daten umsetzen zu können, muss die filternde Komponente die Möglichkeit haben, diese überhaupt erst identifizieren zu können. Das Konzept der Markierung von Paketen wird in der IT vielfach verwendet und als „Tagging“ bezeichnet. Das Tagging ist dabei nichts anderes als eine „Kennzeichnung“, die auf Pakete mit bestimmten Eigenschaften angewandt wird. Erst wenn PDUs, welche sensible Daten enthalten auch als solche ausgewiesen und damit erkennbar sind, kann eine Filterung durchgeführt werden.

Da potentiell sensible Daten auf der Anwendungsschicht angesiedelt sind, gilt es, diese Schicht auf die Realisierbarkeit des Taggings zu untersuchen. Die Norm DIN EN ISO 16484-5 [DIN+12] definiert auf der Anwendungsschicht acht Typen von Nachrichten („APDU Types“): BACnet-Confirmed-Request-PDU, BACnet-Unconfirmed-Request-PDU, BACnet-SimpleACK-PDU, BACnet-ComplexACK-PDU, BACnet-SegmentACK-PDU, BACnet-Error-PDU, BACnet-Reject-PDU, BACnet-Abort-PDU. Die verschiedenen Arten von Nachrichten sind zum Großteil selbsterklärend, für detaillierte Informationen wird auf Kapitel 20.1 der DIN EN ISO 16484-5 [DIN+12] verwiesen. Potentiell sensible Daten werden nur in zwei dieser acht Protokolldateneinheiten übermittelt, konkret BACnet-Confirmed-Request-PDU und BACnet-Unconfirmed-Request-PDU. Der Aufbau der PDUs dieser zwei Typen ist in Abbildung 2 bzw. Abbildung 3 dargestellt.

Wie aus den Abbildungen ersichtlich ist, bestehen BACnet APDUs aus einem festen Bestandteil, welcher die Kontrollinformationen umfasst (APCI), und einem variablen Anteil, der die Nutzinformationen erhält.

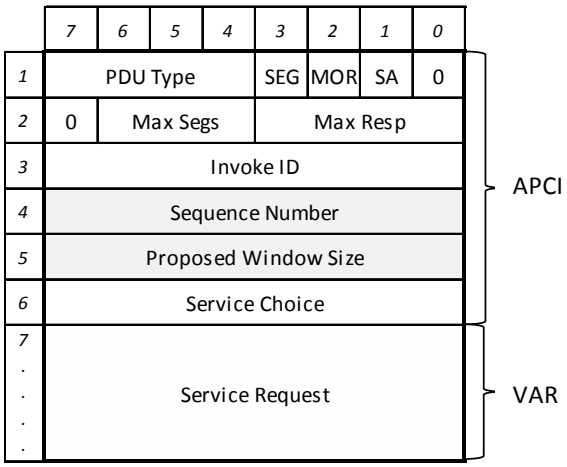

Abb. 2: BACnet-Confirmed-Request-PDU

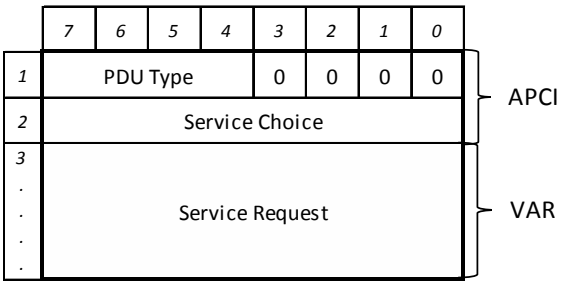

Abb. 3: BACnet-Unconfirmed-Request-PDU

Für ein Tagging von Paketen kommt nur eine Komponente in Frage, welche den beiden Arten von APDUs gemein ist. Damit beschränken sich die Möglichkeiten auf den variablen Anteil

der APDU, die Bit 7-4 des ersten Bytes („PDU Type“), Bit 0 des ersten Bytes und das Service Choice Byte.

Der variable Teil der APDU richtet sich nach der Art des verwendeten Dienstes (readProperty, writeProperty, *) und fällt je nach Dienst in seiner Zusammensetzung sehr unterschiedlich aus. Die Einbringung eines Tags in den variablen Teil würde eine komplexe Umsetzung bedeuten und wäre in der Praxis schwer handhabbar.

Der PDU Type gibt Auskunft über die Art der APDU. Zum aktuellen Stand (Dezember 2014) sind in [DIN+12] acht Arten von PDUs definiert. Sollte in einer zukünftigen Fassung ein weiterer „PDU Type“ eingeführt werden, so sind hierfür bereits 4 Bit notwendig - die zur Verfügung stehende Bitzahl wäre in der Folge erschöpft. Die „Abspaltung“ eines Bits des „PDU Type“ würde damit eine starke Einschränkung der Flexibilität für zukünftige Entwicklungen bedeuten.

Bit 0 des ersten Bytes ist laut Norm mit einer 0 belegt und für zukünftige Verwendung durch das ASHRAE (American Society of Heating, Refrigerating and Air-Conditioning Engineers) reserviert. Sollen die Vorgaben der DIN EN ISO 16484-5 [DIN+12] eingehalten werden, sollte von einer Verwendung dieses Bits abgesehen werden.

Das Service Choice Byte legt fest, welche Art von Dienst verwendet wird. Aktuell bietet BACnet 29 Dienste für Confirmed Requests („BACnetConfirmedServiceChoice“) und 9 Dienste für Unconfirmed Requests („BACnetUnconfirmedServiceChoice“), welche in Kapitel 20 der DIN EN ISO 16484-5 [DIN+12] festgelegt sind. Für die Unterscheidung von 29 Diensten sind 5 Bit notwendig. Damit könnten für ein Tagging die Bit 7-5 des Service Choice Bytes genutzt werden. Für eine simple binäre Unterscheidung „sensibel“/„nicht sensibel“ ist im Grunde allerdings die Verwendung eines einzigen Bits ausreichend. Um den größtmöglichen Spielraum für zukünftige Entwicklungen offenzuhalten, wird die Verwendung von Bit 7 des Service Choice Bytes vorgeschlagen. Im Folgenden wird Bit 7 des Service-Choice-Bytes als BACtag bezeichnet.

Doch wie kann nun der Ablauf für das Setzen des BACtag und die Filterung von Paketen vonstattengehen? Da der Einsatz der Lösung für das Verhindern von Data Leakage auch für eine bereits bestehende Infrastruktur und vorhandene Geräte möglich sein soll, ist eine Variante anzustreben, welche die Kommunikation zwischen den Geräten unberührt lässt. Würde das Setzen des BACtag an den Endgeräten erfolgen, so würde dies die Notwendigkeit einer Neudefinition der Kommunikation nach sich ziehen, da die Endgeräte mit getaggten Paketen schlicht und einfach nicht umgehen könnten. Kommt allerdings eine Technik zum Einsatz, welche die von als „sensibel“ eingestuften Geräten (z.B. Sensoren, welche Vitalparameter erfassen) stammenden Pakete unmittelbar hinter diesen markiert, so werden die Spezifikationen für die Kommunikation zwischen den Geräten eingehalten. Selbstverständlich muss das BACtag vor der Zustellung an den Empfänger wieder zurückgesetzt werden – was durch die Positionierung einer weiteren Appliance unmittelbar vor dem Zielgerät bewerkstelligt werden kann.

3.2.2 Filterung

Nachdem im vorangehenden Abschnitt erläutert wurde, wie Pakete, die sensible Daten enthalten, getaggt werden können, soll im Folgenden auf die Filterung eingegangen werden.

Das durch das BACtag angestrebte Ziel ist die anschließende Filterung von Paketen. Ist das BACtag gesetzt, so soll es einen klar definierten Weg vom Sender zum Empfänger verfolgen können. Realisiert werden kann dies durch die Einführung von „BACtag-Ports“, also Ports,

welche ausschließlich sensible Informationen an den nächsten Hop weiterleiten. Sämtliche Hops, welche die Daten durchlaufen, leiten sensible Informationen – durch das BACtag können diese identifiziert werden – auf dedizierten Ports weiter. Geräte, welche diese Pakete vermitteln, können durchaus auch anderen Traffic verarbeiten. Dieser wird jedoch getrennt vom „sensiblen“ Informationsfluss weitergeleitet. Auf diese Art können logische Teilnetze geschaffen werden, die sensiblen Daten werden folglich von den übrigen isoliert. Eine unerwünschte Verteilung von Nachrichten mittels Broadcast an das gesamte Netzwerk wird durch die Schaffung der neuen, verkleinerten Broadcast-Domäne vermieden.

Der Ablauf wird in Abbildung 4 zusammenfassend dargestellt.

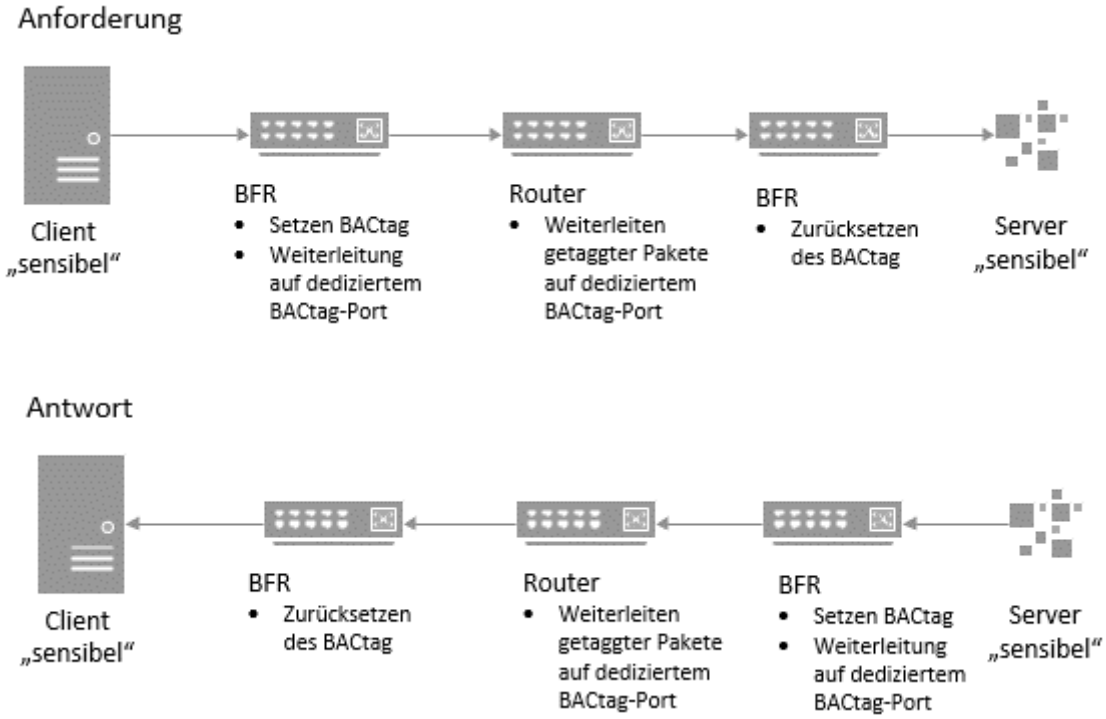

Abb. 4: Ablauf der Kommunikation bei Einsatz von BACtag und Filterung

3.3 Praktische Umsetzung

Für den BACnet-Protokollstapel wurde auf sourceforge.net unter Public Domain Lizenz eine Implementierung des so genannten „BACnet Firewall Router“ (BFR) veröffentlicht. Der Quellcode des BFR wurde in der Programmiersprache C++ von Joel J. Bender verfasst.

Neben der Implementierung des BACnet-Vermittlungsschicht-Protokolls umfasst der Code auch die Implementierung der BACnet-Anwendungsschicht, sowie jene von BACnet/IP.

Der BFR kann sowohl als BACnet Router als auch als BBMD (BACnet Broadcast Management Device, Geräte, welche für die Verteilung von Broadcast-Nachrichten unter BACnet eingesetzt werden) fungieren. Zusätzlich zu dieser „Grundfunktionalität“ bietet der BFR verschiedene Möglichkeiten der Paketfilterung an und ist in der auf Sourceforge abrufbaren Version bereits sehr weit fortgeschritten. Die Konfiguration der Filterung kann komfortabel mittels einer in XML-Notation verfassten Datei eingelesen werden, welche durch einen Parser in Parameter für den BFR umgewandelt wird. Die Filterung kann hierbei nach verschiedenen Kriterien erfolgen,

wobei auch eine Kombination mehrerer Kriterien (auch auf verschiedenen Protokollschichten) möglich ist.

Es liegt nahe, die bestehende Implementierung auch als Basis für die in diesem Papier erläuterten Konzepte des BACtag zu verwenden und um diese zu erweitern. Die Erweiterung muss dabei für die Punkte der Abschnitte 3.2.1 und 3.2.2 umgesetzt werden.

Der BFR inspiziert bei Eingang eines Paketes jene Bestandteile, welche in der in XML verfassten Konfigurationsdatei mit einem Allow bzw. Reject versehen sind. Wird eine Allow-Regel mittels *<Allow function="UNCONFIRMED" />* definiert, so kann die Inspektion der „Unconfirmed Request"-Pakete gleichzeitig dazu genutzt werden, um das in Abschnitt 3.2.1 eingeführte BACtag für sämtliche Pakete dieses Typus zu setzen. Diese Vorgehensweise ist auf alle weiteren Typen von APDUs anwendbar.

In der Praxis wird der Sourcecode der Quelldatei BFRFilter.cpp des BFR um die Codezeilen

int TagPos = (pduData[0] & 0x08) ? 5 : 3;

pduData[TagPos]=pduData[TagPos]+0x80;

der Switch-Anweisung der Filterung für „Confirmed-Requests" bzw.

pduData[1] = pduData[1] + 0x80;

für „Unconfirmed-Requests" in der Quelldatei BFRFilter.cpp ergänzt. Durch diese Erweiterung werden nun alle Pakete der Typen „Confirmed Request" und „Unconfirmed Request" gekennzeichnet. Durch das BACtag werden damit neue Arten von (sensiblen) Diensten eingeführt, welche allerdings nur auf den Übertragungswegen genutzt werden. So wird aus einem „readProperty" durch das BACtag ein „readSensitiveProperty".

Der BFR nutzt in der bestehenden Implementierung Schlüsselwörter, welche durch eine in XML verfassten Konfigurationsdatei an einen Parser übergeben und anschließend für die Filterung verwendet werden. Für die Überprüfung, ob ein Schlüsselwort als Filterkriterium zulässig ist, wird jedoch nicht die Zeichenfolge genutzt, sondern ein daraus berechneter Hashcode. Die Funktion zur Berechnung des Hashwertes kann der Quelldatei BFRFilter.cpp entnommen werden, in welcher auch das Keyword bzw. dessen daraus berechneter Hashwert erfasst ist. Beispielhaft soll in diesem Beitrag der Dienst „readSensitiveProperty" betrachtet werden. Die Berechnung des Hashwertes laut der genannten Funktion ergibt für das Schlüsselwort „READSENSITIVEPROPERTY" 0x1D32ABAE. Für die Filterung wird nun dieser Hashcode, sowie der Wert des Bytes, welches den Dienst definiert, herangezogen. Bei einem getaggten „readProperty"-Paket, welches durch das BACtag zu einem „ReadSensitiveProperty" wird, entspricht dieser Wert 140 (Binär 10001100). Der BFR kann nun durch *<Reject function="READSENSITIVEPROPERTY"/>* angewiesen werden, Pakete des Dienstes „readSensitiveProperty" zu filtern. Das eingehende Paket selbst wird daraufhin überprüft, ob das „ServiceChoice"-Byte dem im Paar (Hashcode, Wert „ServiceChoice"-Byte) (im konkreten Fall (0x1D32ABAE, 140)) definierten Wert entspricht und gegebenenfalls verworfen. Für den praktischen Einsatz sollte die Erweiterung der Schlüsselwort-Tabelle unter dem Aspekt der Usability dahingehend umgesetzt werden, dass ein einziges Keyword „SENSITIVE" eingeführt wird (Hascode 0x2A28B3C8), welchem als rechter Partner der Wert des ungetaggten „ServiceChoice"-Bit + 128 zugewiesen wird.

Wird nun auf sämtlichen Hops zwischen Sender und Empfänger nur mehr auf bestimmten Ports eine „Allow function = xxxSensitivexxx"-Regel für sensible Pakete gesetzt und für alle anderen

eine „Reject function = xxxSensitivexxx“-Regel definiert, so können sensible Daten nur mehr auf einem stark verkleinerten Teilnetz übertragen werden. Auf diese Art und Weise werden auch die möglichen Abflusspunkte von Daten stark eingeschränkt.

4 Evaluation

Wie sind die in diesem Beitrag verfolgten Ansätze zu bewerten? Grundlegend muss sicherlich erwähnt werden, dass das in 3.2.1 eingeführte BACtag nicht dazu geeignet ist, sämtliche Sicherheitsprobleme, welche es in der Gebäudeautomation noch zu lösen gilt, zu beseitigen. Wird allerdings der reine Aspekt „Data Leakage“ betrachtet, so kann durch das BACtag kombiniert mit dem Routen von Paketen über ein eigenes, als vertrauenswürdig geltendes Netzwerksegment, durchaus eine Verbesserung der bestehenden Situation, in welcher sensible Daten im gesamten Netzwerk exponiert sind, erzielt werden. Daten in Bewegung folgen auf diese Art und Weise ausschließlich klar definierten Wegen. Ein unbefugter Gewinn von sensiblen Informationen wird erschwert - allein schon aus dem Grund, dass die „Angriffsfläche“ für einen unerwünschten Datenabfluss erheblich reduziert wird und sich nur mehr auf ausgewählte Segmente beschränkt.

Oftmals scheitert die Einführung einer Sicherheitslösung an den Investitionskosten, welche mit deren Umsetzung verbunden sind. Die in diesem Beitrag aufzeigten Optionen können ohne größere Investitionen umgesetzt werden. Die Geräte auf der Feld- und Managementebene bleiben von den Anpassungen völlig unberührt, Adaptionen sind ausschließlich auf der Automationsebene angesiedelt. Trotz der begrenzten Zusatzkosten kann für ein nennenswertes Plus an Sicherheit gesorgt werden.

Die Skalierbarkeit eines bestehenden Systems erfährt durch die BACtag-Lösung keine Einbußen. Im Gegenteil: die BACtag-Lösung selbst lässt noch Spielraum zur Erweiterung. Soll zu einem späteren Zeitpunkt eine Verfeinerung von Sicherheitsstufen (vgl. hierzu auch [WeKR12]) oder die Einführung weiterer VLANs angestrebt werden, so kann dies durch eine Erweiterung des Taggings erreicht werden. Zu diesem Zweck könnte die in Abschnitt 3.2.1 vorgestellte Methode durch die Hinzunahme von Bit 6 des „ServiceChoice“-Bytes auf insgesamt 3 Abstufungen/VLANs (2^2-1) oder bei zusätzlichem Einsatz von Bit 5 auf 7 (2^3-1) Optionen ausgedehnt werden.

Ein positiver Nebeneffekt, welcher sich durch die Einführung des BACtags ergibt: versucht ein Angreifer, Pakete in das Netzwerk einzubringen, welche an als sensibel eingestufte Endpunkte gerichtet sind, so werden diese nur dann weitergeleitet, wenn sie direkt an einen BFR übergeben werden, welcher diese mit dem BACtag versieht. Das Weiterleiten nicht getaggter Pakete wird durch die in diesem Beitrag skizzierte Vorgehensweise unterbunden.

Die Markierung der Pakete könnte des Weiteren dazu genutzt werden, um Seitenkanäle in einem Gebäudenetzwerk aufzudecken: werden getaggte Pakete an Positionen im Netzwerk angetroffen, welche sie eigentlich nicht passieren sollten, so weist dies auf einen Konfigurationsfehler oder ein Sicherheitsproblem hin und bedarf einer genaueren Analyse. Sollte ein Extrusion Detection System zum Einsatz kommen, können hierbei getaggte Pakete berücksichtigt werden.

Bei allen Vorteilen, die die vorgeschlagene Vorgehensweise mit sich bringt, soll aber auch auf einen Aspekt hingewiesen werden, welcher bei der Umsetzung zu berücksichtigen ist: in verschiedenen Arbeiten (z.B. in [SWK+14]) wird die Einführung eines Traffic-Normalizers vorgeschlagen, welcher Pakete auf ihre Entsprechung mit der Norm hin überprüft. Beim Einsatz eines Normalizers muss berücksichtigt werden, dass getaggte Pakete in ihrem Aufbau zwar

nicht der aktuellen Norm DIN EN ISO 16484-5:2012 [DIN+12] entsprechen, eine Normalisierung aber ein „Untagging“ bedeuten würde, was einen Rückschritt zur bereits vorherrschenden Situation nach sich zieht.

5 Fazit und Ausblick

Auf Standard-Sicherheitsmaßnahmen darf in der Gebäudeautomation trotz der in dieser Arbeit eingeführten, zusätzlichen Mechanismen nicht verzichtet werden. So kann unter anderem eine Trennung von Implementierung des Automationsnetzwerkes und anschließender Konfiguration des BFR durch verschiedene Dienstleistungsanbieter bereits zur zusätzlichen Sicherheit beitragen. Auf diese Weise wird ein Vier-Augen-Prinzip umgesetzt, welches Fehlimplementierungen, Konfigurationsfehler, aber auch eine beabsichtigte Konfiguration, welche Daten aus dem Gebäudenetzwerk abfließen lassen würde, auf einfache Art aufdeckt.

Verschlüsselung, Traffic Normalisierung und andere Ansätze, auf welche sich die Forschung im Bereich Gebäudeautomation konzentriert, stehen nicht im Widerspruch zum Konzept des BACtags.

Letztlich muss aufgrund der Einstufung der Sensibilität der im Netzwerk übertragenen Daten entschieden werden, ob ein reines Tagging für ein ausreichendes Mehr an Sicherheit sorgen kann, ob weitere Maßnahmen ergriffen werden müssen oder ob – wie es im Falle von hochsensiblen Daten der Fall sein könnte – sogar ein isoliertes Gebäudenetzwerk für sensible Komponenten implementiert werden sollte.

Es ist davon auszugehen, dass die Gebäudeautomation, deren Wachstumspotential noch lange nicht ausgeschöpft ist, auch in den nächsten Jahren ein stark wachsender Markt bleiben wird. Damit einhergehend wird auch die Menge der zur Verfügung stehenden Daten stark anwachsen, was seinerseits wieder das Interesse von Angreifern daran verstärken kann. Insbesondere im Gesundheitswesen kann das Risiko, welches für den unbefugten Informationsgewinn eingegangen wird, schnell durch lukrative Geschäftsmöglichkeiten aufgewogen werden. Aber auch in anderen Sektoren können die abgeflossenen Informationen wirtschaftlich verwertet werden – man denke an einen Energieberater, welcher unaufgefordert Konzepte zur energetischen Optimierung vorschlägt oder eine Firma, welche „zufällig“ maßgeschneiderte Konzepte zur Einbruchsicherung anbietet. Die Notwendigkeit, dass sich die Forschung im Bereich der Gebäudeautomation laufend mit dem Thema Sicherheit beschäftigt, liegt damit auf der Hand, nicht zuletzt aufgrund der Tatsache, dass sich der ortsunabhängige Zugriff auf die Daten des Automationsnetzwerkes immer größerer Beliebtheit erfreut.

Literatur

[DIN+12] DIN EN ISO, Systeme der Gebäudeautomation (GA) - Teil 5: Datenkommunikationsprotokoll (ISO 16484-5:2012): Englische Fassung EN ISO 16484-5:2012, 2012

[Holm03] D. G. Holmberg, „Enemies At The Gates – Securing the BACnet Building“, BACnet Today | A Supplement to ASHRAE Journal, November 2003

[Holm05] D. G. Holmberg, „Secure Messaging In BACnet“, BACnet Today | A Supplement to ASHRAE Journal, November 2005

[GrRK08] W. Granzer, C. Reinisch und W. Kastner, „Denial-of-Service in Automation Systems," Proc. of 13th IEEE Conference on Emerging Technologies and Factory Automation (ETFA '08), pp. 468-471, September 2008

[WeSz14] S. Wendzel, S. Szlósarczyk, „Alice's Adventures in Smart Building Land – Novel Adventures in a Cyber Physical Environment", Hack in the Box (HITB), Amsterdam, Mai 2014

[ShER12] A. Shabtai, Y. Elovici und L. Rokach, A Survey of Data Leakage Detection and Prevention Solutions, New York Heidelberg Dordrecht London: Springer, 2012

[GrPK10] W. Granzer, F. Praus und W. Kastner, „Security in Building Automation Systems," IEEE TRANSACTIONS ON INDUSTRIAL ELECTRONICS, Vol. 57, NO 11, pp. 3622-3630, November 2010

[WeKR12] S. Wendzel, B. Kahler und T. Rist, „Covert Channels and their Prevention in Building Automation Protocols - A Prototype Exemplified Using BACnet," 2012 IEEE Conference on Green Computing and Communications, Conference on Internet of Things, and Conference on Cyber, Physical and Social Computing, pp. 731-736, 2012

[Neil13] C. Neilson, „Securing a Control Systems Network", BACnet Today and the Smart Grid | A Supplement to ASHRAE Journal, November 2013

[SWK+14] S. Szlósarczyk, S. Wendzel, J. Kaur, M. Meier und F. Schubert, „Towards Suppressing Attacks on and Improving Resilience of Building Automation Systems - an Approach Exemplified Using BACnet," GI Sicherheit, Wien 2014, pp. 407-418, 2014