Müller, Neumair, Reiser, Dreo Rodosek (Hrsg.): 9. DFN-Forum Kommunikationstechnologien,
Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2016 115

Zusammenwachsen von Gebäudeautomation und Computernetzwerken — Eine erste Sicherheitsanalyse

Thomas Mundt[1] und Peter Wickboldt[2]

Abstract: In diesem Papier schildern wir beispielhaft, welche Risiken bei der vernetzten Gebäudeautomation bestehen und wie diese Risiken beschränkt werden können. Dabei legen wir einen besonderen Fokus auf die Integration von Gebäudenetzwerken und allgemein bekannten Computernetzwerken - letztere durchaus auch in den Dimensionen des Internets. Wir betrachten dabei vor allem Büro- und Zweckbauten, in denen die Gebäudeautomation seit Jahren Standard ist, während sie unter dem Stichwort "Smart Home" gerade die Privathaushalte erobert. Klassische Verfahren zur Absicherung, wie Verschlüsselung und Authentisierung, Firewalling, Intrusion Detection / Prevention und Zonenkonzepte sind in der Gebäudeautomation weitgehend unbekannt.

Keywords: Sicherheit, Gebäudeautomation, Konvergenz der Netze.

Danksagung

Vielen Dank an Daniel Horak, Marc Stefan Martens, Claas Fastnacht, Dmitrij Nesterenko, Stephan Saß, Stefan Jastram, Dennis Retsch und Paul Töpper für die Unterstützung im Rahmen ihrer studentischer Abschlussarbeiten. Vielen Dank an Sven Thesenvitz von der Firma "Kieback & Peter - Technologie für Gebäude-Automation" für wertvolle Hinweise und Einblicke. Besonderen Dank an unsere Kollegen Hans-Walter Glock, Till Wollenberg und Andreas Dähn für die Unterstützung bei der forensischen Untersuchung des KNX-Netzwerkes.

1 Einleitung

Gebäudeautomation ist in Zweckbauten allgegenwärtig und wird von unterschiedliche Gewerken genutzt, angefangen von der Zutrittskontrolle über die Heizungs-, Klima- und Beleuchtungssteuerung bis zu Einbruchs- und Brandmeldung. Sie dient der funktionalen Betriebssicherheit, der Einsparung von Energie (z.B. Strom, Fernwärme) und andere Verbräuche (Wasser, Gas etc.), dem Umweltschutz und dem Komfort der Nutzer [As14].

Zur zentralen Steuerung und Überwachung (der Betriebsführung) werden dabei typischerweise mehrere Gebäude mit der Gebäudeleittechnik und auch untereinander vernetzt. Neben den für die Gebäudeautomation typischen Protokollen und Infrastruktur werden dabei

[1] Universität Rostock, Institut für Informatik, thomas.mundt@uni-rostock.de, Telefon +49 381 498 7505
[2] Universität Rostock, Zentrale Verwaltung - Dezernat Technik, Bau und Liegenschaften, peter.wickboldt@uni-rostock.de, Telefon +49 381 498 1397

in der Regel auch auf IP basierende Protokolle eingesetzt. Hierbei ist es natürlich sinnvoll, die ohnehin vorhandene Netzwerk-Infrastruktur gemeinsam zu nutzen. In Zukunft erwarten wir eine immer stärkere Konvergenz der Dienste aus der Gebäudeautomation hin zu IP-Netzwerken. Schon heute werden IP-Netzwerke in Bereichen eingesetzt, die noch vor kurzem eine ausschließliche Domäne von Feldbussen, seriellen Protokollen und Automationsnetzwerken waren.

Dabei wird entweder ein auf IP basierendes Protokoll zum Tunneln von Nachrichten zwischen Komponenten der Gebäudeautomation benutzt oder es wird gleich von Anfang bis Ende auf IP gesetzt. Ein Beispiel aus dem eigenen Universitätsgebäude: Das häufig auf der sogenannten Feldebene zu findende KNX-Protokoll zur Verbindung von Sensoren und Aktoren wird über Twisted-Pair Kupfer-Kabel im Gebäude übertragen, lässt sich aber auch durch IP über weite Entfernungen tunneln. Anbindungen zwischen verschiedenen Etagen und Gebäudeteilen sind so leicht zu erstellen.

In Zukunft dürfte dabei auch immer häufiger das Internet als Medium genutzt werden, insbesondere dann, wenn Aufgaben zusammengefasst werden und z.B. von externen Dienstleistern übernommen werden. Die zunehmende Vernetzung und Komplexität der Systeme zur Gebäudeautomation stellt enorme Anforderungen an die Sicherheit. Gemeint ist dabei nicht ausschließlich die funktionale Sicherheit, sondern auch der Schutz vor Missbrauch und Manipulation. Hier nimmt sogar der private ”Smart Home” Bereich eine Vorreiterrolle ein, zumindest sind private Anwender sensibilisierter und achten auf ”Versprechungen” von Sicherheit.

Die Tatsache, dass die Berichterstattung über erfolgreiche Angriffe von über das Internet ausgeführten Hacker-Angriffen auf traditionelle Computertechnik dominiert wird, sollte nicht über das gegenwärtige Gefährdungspotential in der Gebäudeautomation hinwegtäuschen. In mehreren Fallstudien haben wir Gebäudenetzwerke untersucht. Wir stellen im weiteren Verlauf die Ergebnisse vor und zeigen einige Lösungsmöglichkeiten auf.

2 Typischer Aufbau

Die Abbildung 1 zeigt den typischen Aufbau eines Gebäudeautomationssystems. Auf der untersten Ebene - Feldebene genannt - verbinden sogenannten Feldbusse die vorhandenen Sensoren und Aktoren miteinander. Sensoren können z.B. Schalter, Präsenzsensoren, Temperaturfühler, Schaltkontakte oder ähnliche Geräte sein. Als Aktoren dienen Relais (Jalousiensteuerung, Lampensteuerung etc.), Thermostate, Schlösser und viele andere mehr. Typischerweise werden hier Feldbusse (KNX [Th10], LON, ISOBUS uva.), drahtlose Übertragungsprotokolle (ZigBee, Z-Wave, EnOcean) oder vorhandene Kommunikationsdienste (WLAN, BACnet over IP, KNX over IP, HTTP usw.) eingesetzt.

Daneben werden auch einfachste, oftmals binär / seriell arbeitende, Datenverbindungen eingesetzt (EIA-485, EIA-232 usw.). Einfache Prozesse (auch Rezepte genannt), wie beispielsweise das Einschalten der Beleuchtung bei Aktivierung eines Bewegungssensors werden direkt in der Feldebene automatisiert. Komplexere Prozesse werden durch die Automatisierungsebene ausgeführt.

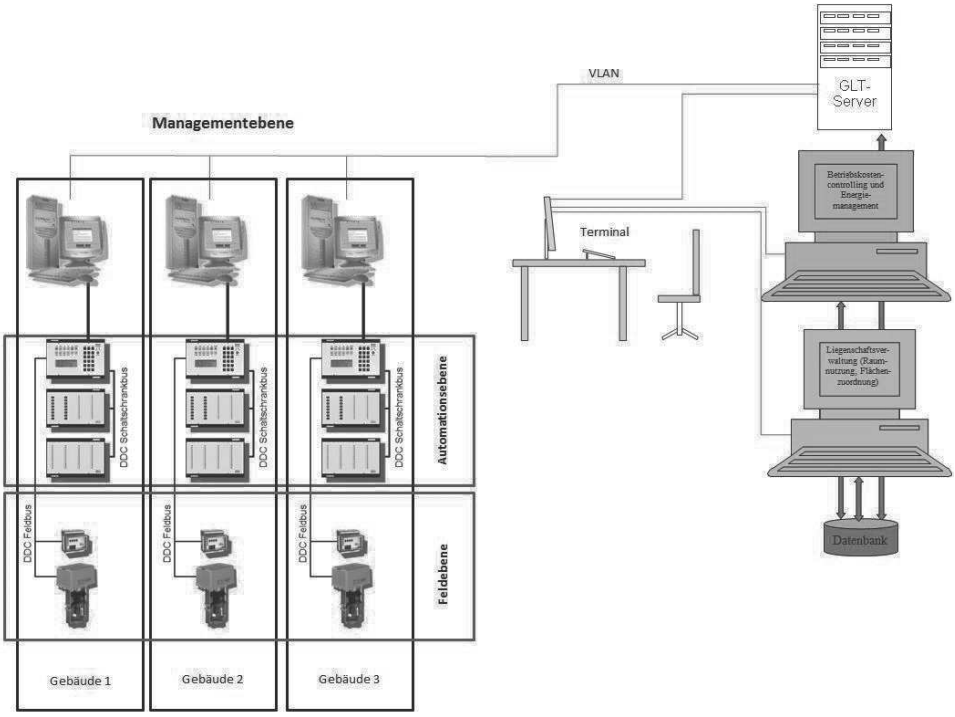

Abb. 1: Typischer Aufbau eines Systems zur Gebäudeautomation.

Auf der eben erwähnten, über der Feldebene liegenden, Automatisierungsebene steuern Controller oder Computer (Direct-Digital-Control-Gebäudeautomation, DDC-GA) die wesentlichen Prozesse im Gebäude. Sie bedienen sich dazu der Sensoren und Aktoren auf der Feldebene und sind mit der Feldebene über Gateways und höhere Protokolle (BACnet [Bu97], IP und darauf basierende Protokolle wie KNX/IP uva.) oder direkt über die zugeführten Feldbusse verbunden. Abhängig von Regelungsvorgaben und den gemessenen Sensorwerten werden Aktoren angesteuert.

Die Gebäudeleittechnik übernimmt die Aufgaben zum Bedienen und Beobachten (Überwachung), zur Messwertarchivierung, zur systemweiten Informationsweitergabe und zur Vorgabe der gewünschten Regelungsprozesse sowie deren Konfiguration.

3 Vernetzung in der Gebäudeautomation

Auf der Feldebene sind aus Kostengründen einfache Protokolle zu finden, häufig auf Twisted Pair Medien [MHH07]. In Europa sind KNX und LON [HBE11] in Zweckbauten besonders beliebt. Gelegentlich findet man auch PowerLine oder Funk als physische Medien. Vor allem im privaten Bereich oder bei der nachträglichen Aufrüstung sind letztere beliebt, da der Installationsaufwand reduziert wird.

Müssen größere Entfernungen überwunden werden, wird das Feldbus-Protokoll oftmals über ein IP-basierendes Protokoll getunnelt (KNX/IP oder LON over IP [DI14]). Bei großen Feldbussen kann das bereits in der Etagen-übergreifenden Installation sinnvoll sein. Zwischen den Geräten auf der Automatisierungsebene und der Gebäudeleittechnik werden regelmäßig IP-basierende Protokolle eingesetzt (weit verbreitet ist dabei BACnet/IP).

Die Zugangsmöglichkeiten zum Netzwerk sind unterschiedlich. Oft reicht es bei einer Zweidraht-Twisted-Pair-Leitung mit freier Topologie und unauthentisiertem und unverschlüsseltem Protokoll, ein Gerät an irgendeiner Stelle im Netzwerk auf der Feldbus-Ebene anzuschließen. Ebenso verbreitet ist der Einsatz von VPNs als Zugangsmöglichkeit auf die Gebäudeleittechnik oder zur Fernwartung der Steuerungssysteme. Über das Internet lassen sich so beispielsweise Updates einspielen oder Konfigurationen ändern. In einigen Ausnahmefällen sind Geräte direkt über offizielle IP-Adressen aus dem Internet erreichbar.

4 Gefährdungspotential

Zunächst stellt sich die Frage, welche Schäden denn überhaupt durch oder an der Gebäudeautomation entstehen können. Ohne übermäßig zu dramatisieren, sind eine ganze Reihe von Angriffen mit hohem Schadenspotential denkbar - siehe auch [PSS00]. Offensichtlich hochgefährlich sind erfolgreiche Angriffe auf Zugangskontrollsysteme sowie kostspielige Angriffe bei denen eine Zerstörung eintritt. Oftmals reicht es dem Angreifer aus, Chaos zu verursachen, ein Gebäude unnutzbar zu machen oder Aufmerksamkeit zu erregen. Unter Umständen kann dabei materieller oder gesundheitlicher Schaden entstehen. Mögliche Szenarios dazu sind:

- Mechanische Überlastung von z.B. Jalousie-Motoren oder Stellmotoren von Lüftungen durch wiederholtes, pausenloses Öffnen und Schließen.
- Elektrische Überlastung von z.B. Transformatoren durch gleichzeitiges Ein- oder Ausschalten von Verbrauchern mit induktiver Last.
- Vorzeitige Alterung von Bauteilen, z.B. Leuchtstoffröhren durch wiederholtes Zünden.
- Manipulation von Schranken oder automatischen Türen, so dass z.B. Autos beschädigt werden.
- Türen werden dauerhaft verschlossen. Mitarbeiter können sich nicht frei im Gebäude bewegen.
- Die Klimatisierung wird mit zu hoher oder zu niedriger Temperatur betrieben. Das wirkt sich auf Mitarbeiter aus, kann aber auch Auswirkungen auf installierte Technik haben. Insbesondere zu kühlenden Computertechnik reagiert sensibel auf deutlich zu hohe Temperaturen.
- Die Beleuchtung wird dauerhaft abgeschaltet oder zum Blinken gebracht. Geräte gehen kaputt oder werden unnötig verschlissen. Mitarbeiter werden am Arbeiten

gehindert. Ein Reputationsschaden kann auch auftreten, wenn mittels der Beleuchtungssteuerung von außen sichtbare Nachrichten auf der Fassade angezeigt werden.

- Die Belüftung wird so gesteuert, dass ein Unterdruck im Raum das Öffnen einer Tür verhindert oder die Tür selbständig öffnet.
- In sensiblen Bereichen (z.B. solche mit chemischen oder biologischen Apparaturen) kann eine Änderung der Belüftung / Ablüftung zur Freisetzung gefährlicher Substanzen führen.

Angriffe gegen die Vertraulichkeit der persönlichen Lebensumstände sind für die Betroffenen äußerst unangenehm. Darüber hinaus lassen sich diese Informationen ebenso als Grundlage für andere Angriffe nutzen. Beispiele sind:

- Überwachung der Anwesenheit von Mitarbeitern in einzelnen Büros.
- Überwachung des Sozialverhaltens. Wir konnten beispielsweise anhand der Daten der Anwesenheitssensoren im Gebäude aufzeigen, wie lange sich eine Person bei der Rückkehr ins Büro im Waschraum aufhielt.
- Nutzung der Gebäudesensoren, um festzustellen, ob gefahrlos in das Gebäude oder in einen bestimmten Bereich eingebrochen werden kann.

Angreifer können dabei ganz unterschiedliche Ziele und Motive haben. Denkbar sind wirtschaftliche Interessen (Störung von Konkurrenten), soziale Motive (beispielsweise Aufmerksamkeit erregen, Lehrveranstaltung oder Prüfung vermeiden) oder auch politische oder gar terroristische Motive bis zu geheimdienstlichen Aktivitäten, beispielsweise zum Zwecke der Destabilisierung.

5 Fallstudien

In mehreren Studien und mit Hilfe studentischer Arbeiten - siehe Danksagung - haben wir die Sicherheit typischer Gebäudeautomatisierungs-Systeme der Universität Rostock untersucht. Die dort verbaute Technik ist recht repräsentativ. Dabei wurde eine Methodik verwendet, die eng an die Sicherheitsanalyse von Computernetzwerken nach dem BSI-Standard 100-3 [BS05] angelegt ist.

Untersuchungsgegenstände waren dabei:

- **Sicherheit der verwendeten Protokolle**. Werden Nachrichten authentisiert und verschlüsselt? Hierbei ist wichtig, ob die Protokolle verlangen, dass Aussendungen nur von definierten Geräten erfolgen können (Authentisierung) oder ob Angreifer beliebige Nachrichten fälschen können. Für die Wahrung der Privatsphären der Nutzer des Gebäudeautomationssystems ist es wichtig, zu überprüfen, ob die Protokolle verschlüsselt oder unverschlüsselt arbeiten. Ebenso spielt es eine Rolle, ob die physikalische Schicht leicht abhörbar ist.

- **Zugriffsmöglichkeiten**. Über welche Wege kann sich ein potentieller Angreifer mit dem System zur Gebäudeautomation verbinden? Muss er vor Ort sein? Benötigt er Zugang zu bestimmten Räumen? Muss er sich physisch mit einem Medium verbinden? Welche Ausrüstung benötigt er für den Zugriff? Benötigt er Kenntnis von kryptografischen Schlüsseln?
- **Mögliche Auswirkungen eines Angriffs**. Welche Gerätschaften sind erreichbar? Welche Schadfunktionen können ausgelöst werden? Wie hoch wäre ein möglicher Schaden?
- **Organisatorische Aspekte**. Wer hat Zugang? Wie werden Zugänge verteilt und weitergegeben? Werden Zugriffe protokolliert?

Beim **ersten untersuchten Gebäude** handelte es sich um das gemeinsam vom IT- und Medienzentrum (ITMZ) und dem Institut für Informatik gemeinsam genutzte **Konrad-Zuse-Haus**. Das Gebäude wurde 2012 fertiggestellt. Auf der Feldebene kommt großflächig KNX über Zweidraht-Twisted-Pair-Kupferleitungen zum Einsatz. Daran angeschlossen sind als Sensoren alle Lichtschalter im Gebäude, sehr engmaschig ausgelegte Infrarot-Bewegungsmelder, Temperatursensoren in den klimatisierten Räumen und einige externe Sensoren für Wind, Regen usw. Als Aktoren sind Relais für Motoren der Jalousien und der innenliegenden Verdunkelungsrollos, Relais und Dimmer für die Beleuchtung und Thermostate über KNX angebunden.

Die elektronische Lautsprecheranlage, die Brandmeldeanlage, elektronische Zugangskontrolle über RFID-Karten, die Computer- und Telefonnetze sowie punktuell vorhandene Multimedia-Funktionen werden hier nicht detailliert betrachtet.

Das KNX-Netzwerk wurde bei der Installation in vier Areas unterteilt, diese wiederum in mehrere Lines. Eine Area bedient dabei eine Etage. Zwischen den Areas wurden Gateways installiert. Diese tunneln KNX-Telegramme über ein VLAN auf der ohnehin vorhandenen strukturierten Ethernet-Verkabelung.

Auf der Automatisierungsebene steuern mehrere DDC-Controller die Heizung und Klimatisierung / Lüftung im gesamten Gebäude. Die Controller sind dazu untereinander und mit dem KNX-Bus unter anderem über Ethernet und IP (VLAN) verbunden. Als Protokoll kommt unter anderem BACnet zum Einsatz. Darüber hinaus verfügen die DDCs über diverse Schnittstellen, beispielsweise HTTP. Das erwähnte VLAN ist von außen über ein VPN angebunden. Als IPv4-Adressen wird augenscheinlich ein privates Netzwerk (10.X.0.0/16) genutzt.

KNX als Protokoll kennt keinerlei Sicherheitsmaßnahmen. Alle Telegramme sind unverschlüsselt und werden nicht vom Absender authentisiert. Einen vermeintlichen, primitiven Schutz bieten lediglich der mechanische Schutz der verbauten Kabel vor Zugriff und die Unterteilung des gesamten Netzwerks in Areas. In einer Area konnten alle Nachrichten mit Quelladresse innerhalb der Area mitgelesen werden. Dazu wurde anfangs die Abdeckung eines öffentlich zugänglichen Lichtschalters entfernt und ein eigenes KNX/IP-Gateway an die vorhandene Zwei-Draht-Leitung angeschlossen. In einem zweiten Expe-

riment [MDG14] konnten die Telegramme berührungslos anhand der elektromagnetisch Abstrahlung des Twisted-Pair-Kabels aufgezeichnet werden. Die Metadaten (Zuordnung der Adressen zu Geräten und damit Standorten) konnten durch Beobachtung oder Provozieren von Aussendungen und Aufzeichnen der Telegramme gewonnen werden. Für Wartungszwecke sind zudem in allen Schaltschränken mit KNX-Bauteilen KNX/USB-Gateways eingebaut worden. Das betrifft auch Schaltschränke in nicht besonders gesicherten Räumen.

Eine Ansteuerung beliebiger Aktoren wäre durch das Aussenden von entsprechenden Telegrammen problemlos möglich gewesen. Sogar die Neukonfiguration der verbauten Lichtschalter etc. hätte von einem Angreifer vorgenommen werden können. So ließen sich zum ”Spaß” die Funktionen zweier Schalter im Gebäude vertauschen. Ebenso hätte zumindest eine Line komplett gestört werden können, durch simplen Kurzschluss oder durch Aussenden von Störimpulsen. Hätte man beispielsweise ein GSM-Modem unauffällig platziert oder eine ohnehin überall im Gebäude mögliche Verbindung zum Internet geschaffen, wäre Abhören und Aussenden eigener Steuerkommandos weltweit möglich. Gateways zu anderen Netzbereichen ermöglichen weitere Angriffe.

Noch gefährlicher sind Angreifer, die direkten, physischen Zugang, zum IP-basierten Backbone-Netz haben. Einige der angeschlossenen Geräte (Computer in der Gebäudeleittechnik, DDC-Controller, Gateways) sind mit Nutzername und Passwort vor dem direkten Zugriff geschützt, andere Geräte ließen unkontrollierten Zugriff auch auf relevante Funktionen zu. Zugang zu diesem übergreifenden Backbone-Netzwerk über ein VPN haben viele Mitarbeiter der Universitätsverwaltung, aber auch mehrere externe Vertragspartner zum Zwecke der Wartung. Eine Überwachung der Zugriffe findet nicht statt. Ob ein Hersteller von technischen Aggregaten darüber hinaus unangemeldete Zugänge über Mobilfunk eingebaut hat, konnte nicht vollständig ausgeschlossen werden. Unüblich wäre ein solches Vorgehen in der Branche nicht.

Mit Hilfe einfacher Netzwerktools (nmap, tcpdump, wireshark, nc, nrep) und einem Webbrowser mit Java konnten wir die Geräte des Backbone-Netzwerkes und deren Funktion ermitteln. Begünstigt durch teilweise vorhandene Hubs (statt Switches) und einer großen Anzahl von Broadcasts konnte die Struktur schnell erkannt werden. Ebenso konnten viele Nachrichten (Statusmeldungen, Steuerkommandos, Abfragen) im Klartext mitgelesen werden. Auf eine weitergehende forensische Untersuchung der Geräte und Netzwerke wurde mit Hinblick auf den laufenden Betrieb verzichtet. Für den Anschluss an das Netzwerk war in diesem Fall Zugang zu nichtöffentlichen Betriebsräumen notwendig.

Eine genauere Untersuchung des IP-basierten Backbone-Netzwerkes (VLAN über die universitätsweit verbreitete Infrastruktur mit inzwischen privaten Adressen), der Zugangsmöglichkeiten und der Maßnahmen zum Schutz dieses Netzwerkes (physische Zugansgbeschränkungen, Vermeidung von Konfigurationsfehlern, Regelungen zum VPN-Zugang etc.) konnte nicht erfolgen, da das ITMZ aus zeitlichen Gründen längere Zeit für eine Befragung nicht zur Verfügung stand. Das öffentlich einsehbare Sicherheitskonzept des ITMZ fokusiert auf die Sicherheit von Computern und traditionellen Computernetzwerken.

In einer **zweiten Analyse** wurden die Gebäude der Bereiche **Chemie und Biologie** untersucht. Hier wurde besonderes Augenmerk auf die Behandlung von giftigen oder gesundheitsgefährdenden Stoffen gelegt. Die Gebäude wurden um 2002 bezogen. Die Gebäudeautomatisierung betrifft im Wesentlichen die Klima- und Lüftungssteuerung. Die übrie Elektroinstallation (Licht, Verdunkelung) ist noch konventionell ausgelegt. Hervorhebenswert sind auf Grund der besonderen Brisanz der Anwendung per LON wiederum über Twisted-Pair-Kabel angebundene Abluftschränke und die Lüftungssteuerung im Laborbereich. Der physische Zugriff auf die Verkabelung ist trivial, zum einen weil die Topologie sehr flexibel ist, man sich also überall "anklemmen" kann, zum anderen, weil an den Lüftungsschränken Anschlussklemmen zu Überwachungs- und Wartungszwecken herausgeführt worden sind.

Für das verwendete LONworks-Protokoll sind zwar rudimentäre Verschlüsselungs- und Authentisierungsmöglichkeiten im Standard vorgesehen, in der Praxis werden diese aber so gut wie nie eingesetzt. Großen Schutz böten diese ohnehin nicht, da die Schlüssel nur 64bit lang sind und in jedem Gerät hinterlegt werden müssen.

Zum Anschluss der DDCs auf der Automatisierungsebene gilt das zuvor beim Konrad-Zuse-Haus gesagte. Auch hier ist das selbe VLAN als Backbone ausgelegt. Schutzmaßnahmen im Netzwerk wurden nicht gefunden, man verlässt sich auf die Abschottung des VLANs gegenüber anderen Netzbereichen. Über den selben, zuvor erwähnten, VPN-Zugang ist auch hier ein universeller Zugriff auf alle Komponenten der Gebäudeautomation möglich. Fremde Rechner können an vielen Stellen unauffällig und dauerhaft in dieses Netzwerk eingeschleust werden. Sobald sich ein Hersteller oder ein Wartungsunternehmen an einem Angriff beteiligen würde, hätte vermutlich selbst der Betreiber keine Chance, die Manipulation zu bemerken.

In einer **dritten Feldstudie** wurde die Anbindung der **Gebäudeleittechnik** betrachtet. Zwischen Leitrechner und DDCs wird überwiegend BACnet über IP eingesetzt. Der Leitstand selbst greift über das Microsoft Remote Desktop Protokoll auf den Leitrechner und auf andere Systeme der Gebäudeautomation zu. Hierbei kommt ebenfalls das schon mehrfach erwähnte VLAN zum Einsatz. Der Leitrechner befindet sich in einem gesicherten Raum. Das VLAN wird vom ITMZ bereitgestellt und lässt sich in nahezu allen Gebäuden der Universität auf freie Ports der dort verbauten Switches schalten. Dort werden dann weitere Steuerungssysteme der Gebäudeleittechnik angeschlossen. Die verwendeten IP-Adressen sind im übrigen überall an den Schaltschränken notiert und können bei der Wartung eingesehen werden. Offensichtlich wurde in den untersuchten Gebäuden der Adressbereich erst nach einiger Zeit von offiziellen IPv4-Adressen auf private Adressen umgestellt, vermutlich um ein einfaches, unbeabsichtigtes Verbinden mit dem Internet zu unterdrücken.

Der mit der Steuerung und Überwachung der Gebäudeautomation betraute Mitarbeiter muss sich individuell am Leitrechner einloggen, hat danach aber umfassende Rechte.

6 Auswertung der Feldstudien

Der "Zoo" von Protokollen, verschiedensten Anwendungen und unterschiedlicher Herstellern aus unterschiedlichen zeitlichen Abschnitten macht eine Absicherung des Systems überaus schwierig. Selbst eine Inventarisierung der verbauten Technik dürfte sich nach mehreren Umbauten und Ergänzungen als problematisch erweisen, erst Recht, wenn die Verantwortlichen wechseln und Drittfirmen ihrer Dokumentationspflicht nicht vollständig nachkommen. Die Ergebnisse der Analysen lassen sich wie folgt zusammenfassen:

- **Sicherheit der verwendeten Protokolle.** Dieser Punkt muss bei den am häufigsten auf der Feldebene eingesetzten Protokollen KNX und LON als verheerend bezeichnet werden. Einfachste Sicherheitsmaßnahmen, wie Verschlüsselung und Authentisierung, sind entweder in den entsprechenden Standards überhaupt nicht vorgesehen oder praktisch nicht von Nutzen. Ein Umstieg auf Protokolle mit besserem Schutz scheidet kurz- und mittelfristig aus, da dazu große Teil der Haustechnik ersetzt werden müssten. Das ist ohne längere Nutzungspause undurchführbar. Auch in den IP-basierten Netzwerken wird das Potential bekannter Schutzmaßnahmen nur selten genutzt. Hier sind ebenfalls ungesicherte Protokolle eher die Regel als die Ausnahme.
- **Zugriffsmöglichkeiten.** Potentiellen Angreifern gelingt es, nach Erlangung des physischen Zugangs, z.B. durch Installation eines Zwischensteckers hinter der Deckenverkleidung oder Öffnen eines Lichtschalters, beliebige Aktionen auf der Feldebene auszulösen. Durch die Strukturierung der Netzwerke und das Übergehen von Nachrichten in andere Netzbereiche wäre ein universeller Zugriff leicht zu bewerkstelligen. In IP-basierten Netzbereichen (VLAN) schützt man sich vor physischem Zugang durch Abschließen der entsprechenden Räume. Die Vielzahl der Räume an sich mit vielen Berechtigten und die Vielzahl der möglichen Netzzugänge und Möglichkeiten zur Fehlkonfiguration lassen das als gültigen Schutz fraglich erscheinen. Generell wurden einige - nicht alle - der untersuchten Zugänge auf Programme, Geräte und Gerätefunktionen mit Passwörtern gesichert. Gerade dann, wenn Zugänge auch an Fremdfirmen gegeben werden (müssen), erscheint auch das überdenkenswert.
- **Mögliche Auswirkungen eines Angriffs.** Wir schätzen das Risiko eines erfolgreichen Angriffs als sehr hoch ein. Einerseits kann der Angriff einfach durchgeführt werden, andererseits sind beträchtliche Schäden möglich. Angriffe mit dem Ziel von Chaos und Aufmerksamkeit sind in den untersuchten Gebäuden besonders leicht durchführbar. Beliebige Aktoren können auf der Feldebene angesteuert werden. Der Datenschutz muss verbessert werden. Sensordaten können zur Zeit einfach aufgezeichnet werden. Das Aufzeichnen von Protokollnachrichten im Backbone-Netz erfordern das Überwinden von Gateways oder das Vordringen in nichtöffentliche Räumen. Mit wenig Fantasie lassen sich Risiken in beträchtlicher Höhe ausmalen, die allesamt einfach und preiswert zu realisieren wären.
- **Organisatorische Aspekte.** Die Zusammenarbeit zwischen Gebäudetechnikern und Verantwortlichen für die Computernetzwerke wird zunehmend wichtiger. Sie soll-

te sich nicht auf das ”Durchschieben” von Nachrichten beschränken. Das Know How aus jahrelanger Erfahrung von Angriffen auf Computernetzwerke ist für die Gebäudeautomation ein wertvoller Wissensschatz, den es zu heben gilt. Hier gibt es Nachholbedarf. Grundsätzlich ist die lange Lebensdauer von Gebäudeautomationssystemen eine Herausforderung. Als unsicher erkannte Technologie kann nicht ohne größere Seiteneffekte problemlos ausgetauscht werden. Hinzu kommt der Wechsel von Verantwortlichkeiten während der Lebensdauer, die Vielzahl der Beteiligten (Planer, Errichter, Betreiber, Nutzer, oftmals jeweils durch Dritte vertreten), die Ergänzung und eventuell der Wechsel von Nutzungsszenarien. Nachträgliche Umbauten wurden und werden oftmals nicht dokumentiert. In vielen Fällen sind die Zuständigkeiten zwischen Gebäudeverwaltern und Netzwerktechnikern getrennt.

Fazit: Um die Sicherheit in der Gebäudeautomation ist es schlecht bestellt. Es muss offensichtlich zunächst etwas passieren, bevor geeigneten Abwehrmaßnahmen ergriffen werden. Gefordert sind hierbei zunehmend auch die Netzwerktechniker.

Literaturverzeichnis

[As14] Aschendorf, Bernd: Energiemanagement durch Gebäudeautomation: Grundlagen-Technologien-Anwendungen. Springer-Verlag, 2014.

[BS05] BSI: BSI-Standard 100-3 - Risikoanalyse auf Basis von IT-Grundschutz. Bundesanzeiger-Verlag. Bonn, 2005.

[Bu97] Bushby, Steven T: BACnet: a standard communication infrastructure for intelligent buildings. Automation in Construction, 6(5):529–540, 1997.

[DI14] DIN: , DIN EN 14908-4:2014 - Firmenneutrale Datenkommunikation für die Gebäudeautomation und Gebäudemanagement – Teil 4: Kommunikation mittels Internet Protokoll (IP) (Ursprüngliche Norm ANSI/CEA-852 – LonMark IP-852 IP-tunneling channel specification), 2014.

[HBE11] Hersent, Olivier; Boswarthick, David; Elloumi, Omar: The Internet of Things: Key Applications and Protocols. John Wiley & Sons, 2011.

[MDG14] Mundt, Thomas; Dähn, Andreas; Glock, Hans-Walter: Forensic analysis of home automation systems. In: The 14th Privacy Enhancing Technologies Symposium. Amsterdam, 2014.

[MHH07] Merz, Hermann; Hansemann, Thomas; Hübner, Christof: Gebäudeautomation: Kommunikationssysteme mit EIB/KNX, LON und BACnet. Hanser Verlag, 2007.

[PSS00] Palensky, Peter; Sauter, Thilo; Schwaiger, Christian: Security und Feldbusse - ein Widerspruch? it-Information Technology, 42(4):31–44, 2000.

[Th10] The KNX Consortium: , KNX Standard - System Specifications - Interworking, 04 2010.