ComConsult GmbH
Beratung + Planung + Schulung

Der Netzwerk Insider

November 2019

Systematische Weiterbildung für Netzwerk- und IT-Professionals

SD-Lösungen für Campusnetze

von Florian Hojnacki

Der Wunsch nach intelligenten Netzen wird immer größer. SDN, SDA, SD-WAN, SD Branch, Cognitive Campus, Fabric Connect, Overlays, Fabrics, VXLAN, IaaS, SPB, NFV, SDDC, SDI, SDS, NSX; vom WAN, über das RZ bis zum Campus-Bereich erreicht die Flut von Abkürzungen und Marketing-Namen ein neues Allzeithoch. Was ist die Grundidee dahinter? Software-defined Networking.

In diesem Artikel beleuchte ich die Vielzahl von Produkten und Technologien, welche den Einstieg zu intelligenten und (voll-)automatisierten Netzen darstellen. Ich hinterfrage dabei, welche

Vorteile tatsächlich kosteneffektiv erreicht werden können.

Software-defined Networking ist nichts Neues. Es ist ein weiterer Schritt in dem andauernden Wandel zu intelligenterer Informations- und Kommunikationstechnologie (IKT). Neben VLANs, die bereits seit 1998 virtuelle Netze über physische Switch-Grenzen aufspannen, ist in diesem Kontext auch die Virtualisierung zu nennen. Die Idee virtueller Maschinen (VM) wurde bereits in den 60er Jahren umgesetzt und ist heutzutage aus Rechenzentren nicht mehr wegzudenken.

weiter auf Seite 5

IoT-Sicherheit – (Un-)möglich?

von Tanja Ulmen

Das Internet of Things ist ein Netzwerk aus vielen verschiedenen "smartifizierten" Endgeräten. Fast alles kann mittlerweile miteinander vernetzt werden. Die Steckdose spricht mit der Glühbirne, der smarte Eierbehälter nutzt das Heim-WLAN, aus modernen Autos ist Sensorik nicht mehr wegzudenken, und auch die Industrie baut mehr und mehr auf smarte Systeme, um Prozesse zu automatisieren.

Doch wie sicher sind smarte Geräte? Wie sicher sind die Netzwerke, an die ein solches Gerät angeschlossen ist? Wie sicher sind diese Netzwerke, wenn sie tausende smarte Geräte miteinander verbinden?

Dieser Beitrag befasst sich mit den neuen Bedrohungsszenarien, die mit IoT entstehen, und zeigt Lösungsmöglichkeiten, mit denen ein möglichst sicheres Netzwerk mit IoT-Geräten betrieben werden kann.

weiter auf Seite 21

Geleit

Mandantenfähigkeit: Standards versus Herstellerspezifisches

auf Seite 2

Standpunkt

Von Aluhüten und Elektrolurchen

auf Seite 14

Intensiv-Seminar

Winterschule – Neueste Trends der IT-Infrastruktur

ab Seite 11

Aktuelle Kongresse

ComConsult Cloud Forum

ab Seite 15

ComConsult UC-Forum

ab Seite 26

ComConsult Netzwerk Forum

auf Seite 4

Geleit

Mandantenfähigkeit: Standards versus Herstellerspezifisches

In Providernetzen ist Mandantenfähigkeit keine neue Eigenschaft. Provider bedienen eine Vielzahl von Kunden. Diese Kunden teilen sich die Providernetze, ohne darüber miteinander kommunizieren zu können. Dasselbe physische Netz dient dabei als Basis verschiedener logischer Netze. Jedem Kunden wird sein eigenes logisches Netz zugewiesen. Die logischen (virtuellen) Netze sind voneinander getrennt.

Jedem Kunden erscheint das über die Infrastruktur des Providers gespannte Netz als ein „privates". So hat sich der Begriff Virtual Private Network (VPN) etabliert. Zum Beispiel bedeutet MPLS-VPN ein virtuelles privates Netz, das gemäß dem Verfahren Multi-Protocol Label Switching (MPLS) konfiguriert ist. MPLS basiert auf Standards der Internet Engineering Task Force (IETF). Die meisten mandantenfähigen Providernetze nutzen MPLS.

Auch in einer Reihe von Unternehmensnetzen müssen verschiedene virtuelle Netze voneinander getrennt werden. Seit Jahren ist dies zum Beispiel in Flughafennetzen der Fall. Verschiedene Flughafenbereiche, aber auch Fluglinien und Sicherheitsorganisationen, bekommen in einem Flughafennetz ihre eigenen logischen Netzbereiche, die von anderen logischen Netzbereichen im selben physischen Netz strikt getrennt sind. Diese Trennung verschiedener „Mandanten" müssen immer mehr Campusnetze von Unternehmen unterstützen. Typische Mandanten sind die Gebäudeautomatisierung und die industrielle Fertigung. Mit der zunehmenden Digitalisierung kommt es zu immer mehr intelligenten („smarten") vernetzten „Dingen". Wir sprechen vom „Internet of Things" (IoT). Dabei ist dieser Begriff irreführend. Denn diese Dinge, wie zum Beispiel ein Industrieroboter, sollen nicht an das Internet angeschlossen werden. Genauso wenig sollen alle diese Dinge über ein einziges neues „Internet" erreichbar sein. Vielmehr gibt es eine Vielzahl von in sich geschlossenen Netzen mit daran angebundenen Sensoren, Aktoren, Steuerungen, Messgeräten, Kameras usw. „Smart Everything" bedeutet nicht, dass alle mit allen kommunizieren sollen. Der Patient, der über das Krankenhausnetz Netflix-Filme konsumiert, darf nicht auf die Systeme im Operationsbereich zugreifen.

Interessen der Netzverantwortlichen und Interessen der Hersteller

Die für ein Netz Verantwortlichen sind an bestimmten Eigenschaften des Netzes stark interessiert. Neben Mandantenfähigkeit sind es zum Beispiel Sicherheit, Leistungsfähigkeit, Verfügbarkeit, Skalierbarkeit, Zukunftssicherheit, Beherrschbarkeit, Benutzerfreundlichkeit und Wirtschaftlichkeit. Die Erfahrung hat vielen Netzverantwortlichen gelehrt, dass sie sich beim Netzdesign am besten an herstellerunabhängigen Standards orientieren sollen. Wer möchte schon eine kritische Infrastruktur verantworten, deren Kosten und Zukunft von der geschäftlichen Situation und vom Gutdünken eines einzigen Herstellers abhängen?

Dass Hersteller von Netzkomponenten andere Interessen haben, ist bekannt. Jeder marktwirtschaftlich orientierte Hersteller strebt Profitmaximierung an. Dazu kommen einige Hersteller immer wieder auf die Idee, ihren eigenen Kunden den Wechsel zu einem anderen Hersteller möglichst zu erschweren. Solchen Herstellern bietet dazu jede neue Anforderung neue Chancen. Mit der Mandantenfähigkeit verhält es sich nicht anders. Herstellerunabhängige Standards werden immer für bekannte Anforderungen entwickelt, in vielen Fällen in einem langwierigen Prozess. Deshalb gibt es immer wieder neue Anforderungen, die von bestehenden herstellerunabhängigen Standards nicht oder nicht optimal erfüllt werden. Das ist die Lücke, in die Hersteller vorpreschen können, um Lösungen mit Alleinstellungsmerkmalen zu verkaufen.

Vielleicht fragen Sie sich, ob es sich beim Begriff „herstellerunabhängiger Standard" nicht um eine Tautologie handelt. In vielen technischen Gebieten, so auch bei Netzen, gibt es leider auch Standards, die sich nicht herstellerübergreifend etablieren. Beispiele sind solche Netzstandards, welche die Herstellerauswahl stark eingrenzen, in der Praxis oft auf einen einzigen Hersteller. Dieser nennt die Spezifikationen des entsprechenden Standards und weist die Einstufung der eigenen Lösung als „proprietär" von sich. Für den Kunden bleibt die Lösung herstellerspezifisch, auch wenn sie nicht proprietär im engeren Sinne ist. Denn ein Herstellerwechsel ist mit einem Lösungswechsel verbunden.

Lösungen für Mandantenfähigkeit

Seit über einem Jahrzehnt gibt es den Wettbewerb zwischen verschiedenen Lösungen für die Mandantenfähigkeit in Unternehmensnetzen. In den vergangenen zehn Jahren sahen wir so manche Lösung kommen und wieder in Vergessenheit geraten. Einige Standards beschäftigten zunächst mehrere Hersteller, um letztlich nur von wenigen oder gar einem einzigen Hersteller implementiert zu werden. Beispiele für Standards ohne breite Herstellerunterstützung sind Shortest Path Bridging (SPB) und Locator / Identifier Separation Protocol (LISP).

Wie eingangs erwähnt, sind die Providernetze den Unternehmensnetzen in Sachen Mandantenfähigkeit Jahre voraus. Provider orientieren sich stärker als andere Unternehmen an herstellerunabhängigen Standards. Viele Standards für Providernetze sind unter Mitwirkung von Providern (d.h. Netzbetreibern) entstanden. Das ist bei Unternehmensnetzen häufig anders. Netzbetrieb ist das Kerngeschäft der wenigsten Unternehmen. Deshalb leisten es sich die wenigsten Unternehmen, Mitarbeiter für die Entwicklung von Netzstandards abzustellen. Das sind nicht die besten Voraussetzungen für die Etablierung von herstellerübergreifenden Standards als Basis von unternehmensinternen Netzen. Ausnahmen wie Ethernet bestätigen die Regel.

Die Frage ist, ob man für Mandantenfähigkeit in Unternehmensnetzen andere Lösungen braucht als seit Jahren in Providernetzen erprobte und bewährte, insbesondere andere Lösungen als MPLS. Einige führende Hersteller bejahen diese

SD-Lösungen für Campusnetze

Fortsetzung von Seite 1

Florian Hojnacki ist seit 2010 bei der ComConsult GmbH als Berater tätig. Im Competence Center Netze liegt sein Fokus auf der Planung und Konzeption von LAN und WLAN-Infrastrukturen im large Enterprise Umfeld. Das erlernte Wissen seiner Masterabschlüsse aus Köln und Melbourne setzt er seit 2019 erfolgreich bei Kundenprojekten ein.

Nachdem diese VMs inzwischen oftmals auf riesigen Verbünden physischer Server betrieben und quer durchs RZ bewegt werden, liegt die Anforderung eines intelligenten Netzes zur optimalen Anbindung dieser sprunghaften Dienste nahe. Die Grundidee von SDN ist simpel:

Durch Entkopplung von Daten- und Kontrollschicht wird eine automatisierte und zentralisierte Konfiguration eines Netzes ermöglicht.

Die Verlagerung der Netzintelligenz an eine zentrale Stelle ermöglicht somit eine wesentlich effizientere Nutzung vorhandener Ressourcen. Rechenleistung wird auf optimierter Hardware zur Verfügung gestellt. Switching und Routing erfolgen auf sparsam dimensionierten Netzkomponenten, die lediglich Befehle der zentralen Instanz ausführen. Im Vergleich zur autonomen Wegfindung eine deutlich effizientere Art des Umgangs mit Ressourcen. VMs beispielsweise bieten dieselben Vorteile hinsichtlich Ressourcen-Optimierung.

Aktuelle (lokale) Netze operieren im Wesentlichen auf den Schichten 2 (Data Link Layer) und 3 (Network Layer) gemäß OSI (Open Systems Interconnection) und verfolgen das Prinzip autonomer Systeme. Einzelne Knotenpunkte treffen Entscheidungen basierend auf ihren aus Nachbarschaftsbeziehungen erhaltenen Informationen. Am Beispiel des Taxi-Verkehrs einer Großstadt lässt sich dieses Modell recht anschaulich darstellen:

Fahrgäste (Datenpakete) steigen an beliebigen Kreuzungen in die Taxen ein und wollen möglichst schnell zu ihrem Wunschziel gebracht werden. Die Taxifahrer (Router, Switches) treffen an jeder Kreuzung der Strecke basierend auf Sperrungen und Entfernungsschildern Entscheidungen, um das gewünschte Ziel bestmöglich und schnellstmöglich (best-effort) zu erreichen.

Stellen Sie sich nun vor, die Taxen wären konstant über Funk mit einem Hubschrauber verbunden, der das gesamte Verkehrsnetz überblickt. Der Pilot kennt sämtliche Sperrungen und Staus, weiß exakt über alle Taxen und deren Ziele Bescheid und koordiniert den gesamten Verkehr. Diese allwissende Instanz (zentralisierte Kontrollschicht) nimmt damit den Taxen sämtliche Überlegungen und Entscheidungen bezüglich der Wegfindung ab. Die Fahrer folgen lediglich den Anweisungen.

SDN hat viele Anwendungsbereiche

Im Prinzip gibt es drei große Netzbereiche, in denen Software-defined-Ansätze verfolgt werden können: in Rechenzentren, im Weitverkehrsnetz (WAN) und im Campus-Umfeld (LAN). Aufgrund der Komplexität von Software-defined-Lösungen erhalten diese Ansätze ihre Daseinsberechtigung hauptsächlich in besonders großen Umgebungen. Bei kleineren Netzen ist man meist mit klassischen Lösungen besser bedient. Schauen wir uns aber nun die verschiedenen Technologien genauer an, um die fließenden Grenzen dazwischen besser definieren zu können.

Neben dem hier gesetzten Fokus auf Campus-Lösungen lohnt sich ein Blick in SD-DC (Software-Defined-Data-Centre) und SD-WAN-Umsetzungen, um den Begriff „Software-defined“ weiter zu festigen.

SDDC – Software-defined Data Centre

Die Anforderungen an Rechenzentrumsnetze habe ich bereits am Beispiel der flexiblen Bereitstellung virtueller Maschinen grob dargestellt. Damit sollte nachvollziehbar sein, worin die Vorteile eines Software-defined-Ansatzes liegen. Im Folgenden gehe ich darauf etwas detaillierter ein.

Virtuelle Maschinen werden idealerweise im RZ konstant dorthin verschoben, wo die physische Hardware die notwendigen Ressourcen aktuell effizient bereitstellen kann. Aus Netzsicht ist das problematisch, weil die passenden Netzbereiche in der Lage sein müssen, diese Umzüge abzubilden. SDN hilft hierbei insofern, dass diese Flexibilität durch eine zentrale Kontrollschicht gut realisiert werden kann.

VMware bietet hier sehr gute und inzwischen weit verbreitete Lösungen an. Durch die Bereitstellung von Server- und Netz-Virtualisierung kann VMware mit wichtigen Synergien punkten.

Die Daseinsberechtigung vom SDDC liegt in der aktuell gängigen, dynamischen Bereitstellung und Verteilung virtueller Maschinen. Mit einem intelligenten und automatisierten Netz wird die Effizienz moderner Rechenzentren ohne unverhältnismäßig hohen Administrationsaufwand weiter gesteigert.

SDDCs haben also nicht nur virtualisierte Server-, Storage- und Security-Umgebungen, sondern auch ein virtualisiertes Netz. Eine (Teil-)Auslagerung in verschiedene (private & public) Clouds kann hier auch als zentraler Bestandteil gesehen werden. Eine solch flexible Infrastruktur bietet somit eine sehr effiziente Möglichkeit, Ressourcen (Software, Dienste, Infrastrukturen) bedarfsgerecht und einfach bereitzustellen.

Neben VMware bieten auch diverse andere Hersteller Lösungen (zB. Intel Omni-Path und Fujitsu Primeflex) im Bereich der RZ-Virtualisierung an. Da wir uns je-

SD-Lösungen für Campusnetze

doch auf den Campus-Bereich konzentrieren wollen, gehen wir an dieser Stelle zum zweiten großen Einsatzgebiet des Software-basierten Ansatzes über.

SD-WAN

Hier liegt der Fokus auf der Optimierung von Weitverkehrsnetzen. Der Vorteil steckt in der automatisierten Flexibilität in Bezug auf intelligentere Routingentscheidungen.

Die kontinuierlich steigenden Anforderungen an Wide Area Networks (WAN) basieren zu großen Teilen auf dem wachsenden Einsatz von Cloud-Lösungen. So steigt mit jedem Dienst, der aus dem eigenen RZ ausgelagert wird, die benötigte WAN-Kapazität. Zudem haben viele dieser Cloud-basierten Dienste auch den Bedarf nach geringer Latenz. Stichworte sind hier Software-as-a-Service (SaaS) und Infrastructure-as-a-Service (IaaS). Besonders Unternehmen mit vielen Außen- oder Zweigstellen brauchen auch ohne Cloud-Services ein effizientes, wartungsarmes Weitverkehrsnetz. Zweigstellen müssen performant und redundant angebunden sein, im Fehlerfall sollten auch alle übrigen Leitungen den Ausfall effektiv abfangen.

Worin liegen die Vorteile eines Software-basierten Ansatzes?

Hochverfügbare, leistungsfähige WAN-Anbindungen kosten Geld. Die Aufteilung des Netzverkehrs auf verschiedene WAN Strecken nach Priorität und Anwendungsanforderungen ist mit aktuellen Netztechnologien nur schwer zu realisieren, da die Routingentscheidungen meist nicht auf der Anwendung, sondern dem Zielnetz basieren.

SD-WAN bietet hier Möglichkeiten der Kostensenkung durch unabhängige, anwendungsbasierte Routingentscheidungen für verschiedene WAN-Strecken eines Unternehmens (DSL, MPLS, 3G/4G/5G, Dark Fiber, usw.). So können zum Beispiel zeitkritische Systeme über eine schnelle, aber schmalbandige Verbindung geleitet werden, wohingegen das datenintensive Zweigstellen-Backup zeitlich und automatisch über einen Breitband-DSL-Anschluss fließt.

Zu den stärksten Anbietern in diesem Bereich zählt VMware. Der Grund ist offensichtlich. Das virtualisierte RZ-Netz möchte natürlich auch aus der Cloud und aus Zweigstellen kosteneffizient und sicher erreichbar sein.

Silver Peak und Cisco sind nur zwei der vielen Anbieter, die in diesem Kontext Lösungen anbieten. Silver Peak wirbt zusätzlich zum Software-defined WAN auch noch mit einem Self-Driving WAN, das Automatisierung und Machine Learning kombiniert. Naja, die Abkürzung SD-WAN passt ja trotzdem noch!

Wie macht Google das eigentlich?

Eines der größten Firmennetze weltweit gibt es ohne Zweifel bei Google. Ca. 25% des globalen Internetverkehrs wandert täglich über Googles Leitungen. Ein Blick auf diese Infrastruktur ist durchaus lohnenswert.

“Early on, we realized that the network we needed to support our services did not exist and could not be bought.” (Amin Vahdat, Technical Lead for Networking at Google)

Diese Aussage ist am Beispiel vom Google Assistant nur allzu gut nachvollziehbar. Der Gedanke an die Anforderungen eines globalen Netzes mit Echtzeit-Sprach-Kommunikation lässt so manchen Administrator erzittern. Auf die gesprochene Frage nach den neuesten Nachrichten in jeder Sprache, jedem Akzent und in jedem Land der Welt muss der Google Assistent in Sekundenbruchteilen eine Antwort parat haben. Und wie? Die Sprachdatei wird vom Smartphone zum nächsten „Peering-Point“ von Google geleitet. Von dort sucht das Software-gesteuerte Netz den schnellsten Weg zum nächsten Speech-to-text-RZ. Sind die Daten nun in Textform vorhanden, suchen Google-Server auf der ganzen Welt nach den neuesten Nachrichten, filtern diese nach persönlichen Präferenzen, bereiten sie auf und senden sie auf das Smartphone des Nutzers. All dies in Sekunden oder Sekundenbruchteilen. Im Vergleich zu dieser Aufgabe scheint unterbrechungsfreies Telefonieren im eigenen Firmen-WAN eine Banalität. Und trotzdem ist dies in vielen Konzernen noch immer problematisch.

Kommen wir aber zurück zu unserem Taxi-Beispiel. Ein riesiger Vorteil wäre doch, wenn der Hubschrauber seine Informationen mit den Fahrern aller Taxi-Unternehmen teilen würde. Leider ist das größtenteils noch Wunschdenken. Haben Hersteller erst einen potenten Hubschrauber entwickelt, teilen sie diesen nur äußerst ungern mit der Konkurrenz.

Openflow

Ein nennenswerter Ansatz in Bezug auf herstellerunabhängige, Software-basierte Netze ist die Arbeit der Open Networking Foundation (ONF).

Google, Telekom, AT&T und viele andere namhafte Konzerne beteiligen sich seit Jahren an der Weiterentwicklung von of-

IoT-Sicherheit – (Un-)möglich?

Fortsetzung von Seite 1

Tanja Ulmen ist als Beraterin im Competence Center Smart Technologies der ComConsult GmbH tätig. Sie beschäftigt sich mit der Datenverarbeitung in smarten Systemen und im Rahmen ihrer beruflichen Tätigkeit setzt sie sich intensiv mit intelligenten Gebäuden auseinander.

Das Internet of Things

1999 wurde der Begriff Internet of Things zum ersten Mal in einer Veröffentlichung von Kevin Ashton verwendet. Mittlerweile wurde aus der Vision eine Vielzahl real existierender Netzwerke aus intelligenten Geräten, die Informationen erfassen, speichern, verarbeiten und dafür auch miteinander kommunizieren. Diese Kommunikation läuft mittlerweile völlig automatisch und ohne menschliche Interaktion.

Solche Netzwerke gibt es in sämtlichen Bereichen der Technik. Es fängt an mit dem Smart Home, wo Haushaltsgeräte, aber auch Geräte der Haustechnik sowie Unterhaltungstechnik miteinander vernetzt werden. So wird es ermöglicht, dass beim Verlassen des Hauses automatisch das Licht ausgeht, sich die Heizung herunter regelt und der Saugroboter seine Arbeit aufnimmt, ohne dass ein einziger Schalter oder Regler benutzt werden muss. Von unterwegs schaut man in den Kühlschrank, selbstverständlich über das Smartphone, dem Postboten wird aus der Ferne die Tür entriegelt und der leere Hundenapf bestellt selbstständig online Nachschub.

Bei Smart Buildings hat man diese Vernetzung in einem weitaus größeren Maßstab. Hier können neue Besucher vom smarten Teppich in ihren reservierten Meetingraum geführt werden. Die Information hat der Teppich durch Kommunikation mit dem Smartphone und dem Raumbuchungssystem. Das Raumbuchungssystem hat bereits Kaffee und Kekse bestellt und auch das Facility-Management hat Meldung vom Raum bekommen, diesen anschließend zu reinigen.

In der smarten Fabrikhalle (Industrie 4.0) geht es ebenfalls darum, Prozesse zu automatisieren und Ausfallzeiten zu minimieren. Zum Beispiel überwachen Maschinen sich selbst mit Sensorik und können so ihren eigenen Defekt vor dem Eintreten melden (Predictive Maintenance). Das reduziert Ausfälle und spart Wartungskosten.

Aus modernen Autos und Flugzeugen ist die Sensorik schon gar nicht mehr wegzudenken. Und auch über die genannten Kategorien hinaus gibt es zahlreiche Bereiche, die für das Internet of Things eine ebenso große Rolle spielen (Medizintechnik, Smart Grids, …).

Insgesamt gab es laut einer Studie von Juniper Research 2018 weltweit 22 Milliarden vernetzte Geräte [1]. Bis 2022 sollen es insgesamt rund 50 Milliarden vernetzte Geräte werden. Also eine Steigerung von mehr als 50%. Zum Vergleich: die Weltbevölkerung liegt dann ungefähr bei 7,6 Milliarden.
Das Ziel ist, möglichst alle Geräte komfortabel über eine IP-basierte Schnittstelle steuern zu können. Durch die somit mögliche Kommunikation und den Datenaustausch der Geräte lassen sich etliche Vorteile ziehen. Es werden Ausfallzeiten reduziert und Gefahrensituationen vermieden. Der Komfort steigt enorm. Energie kann gespart werden. Die so gesammelten Daten über die Nutzung der Geräte sind für manche Unternehmen von großem Wert.

Wie sicher ist das IoT?

Doch wie sicher ist das IoT eigentlich? Um das zu beantworten, richten wir den Fokus zunächst auf die einzelnen Geräte, die das IoT bilden.

Der Schwerpunkt liegt bei der Entwicklung der meisten Geräte auf einer kompakten und leichten Bauweise. So gibt es meist nur eine verhältnismäßig geringe CPU-Leistung. Auch die Speicherkapazität eines solchen Gerätes ist extrem gering. Das führt oft dazu, dass die Implementierung von Sicherheitsmechanismen auf dem jeweiligen Endgerät extrem schwierig bis unmöglich ist. Aber die Geräte fügen sich so perfekt in ihre Umgebung ein. Sensoren sind besonders klein und unauffällig, die Smart Watch bleibt klein und komfortabel am Handgelenk tragbar, und auch der Leuchtkörper hat die Maße einer klassischen Glühbirne und passt somit perfekt in vorhandene Fassungen.

Die IP-Schnittstelle ist bei den meisten Geräten eine verhältnismäßig neue Funktion und soll bei Wahrung einer kleinen, leichten Bauweise die Kommunikation mit anderen Geräten ermöglichen. Dies führt dann beispielsweise zu unverschlüsselter Kommunikation der Geräte. Laut einer Studie werden zurzeit rund 90 % des Datenverkehrs zwischen IoT-Geräten unverschlüsselt ausgetauscht. [2]

Aber nicht nur die IP-Schnittstelle an sich kann ein Problem darstellen. Neben der enorm großen Vielfalt an smarten Endgerätkategorien gibt es mindestens genauso viele Übertragungstechniken. Diese Techniken machen ein herkömmliches zu einem smarten Gerät. Hier kommen Protokolle wie WLAN, Bluetooth, BLE, ZigBee, Z-Wave, EnOcean, NFC, Lemonbeat oder 6LoWPAN ins Spiel. Jedes Protokoll hat dabei seine ganz eigenen Schwachstellen und Sicherheitslücken. Viele davon werden schnell öffentlich bekannt, doch stellt jeder Hersteller sofort einen Patch bereit? Und selbst wenn, wird dieser zeitnah installiert?

In einigen Geräten findet man nicht änderbare Standard-Passwörter, die problemlos durch Ausprobieren der gängigsten Passwörter geknackt werden können. (siehe Abbildung 1)

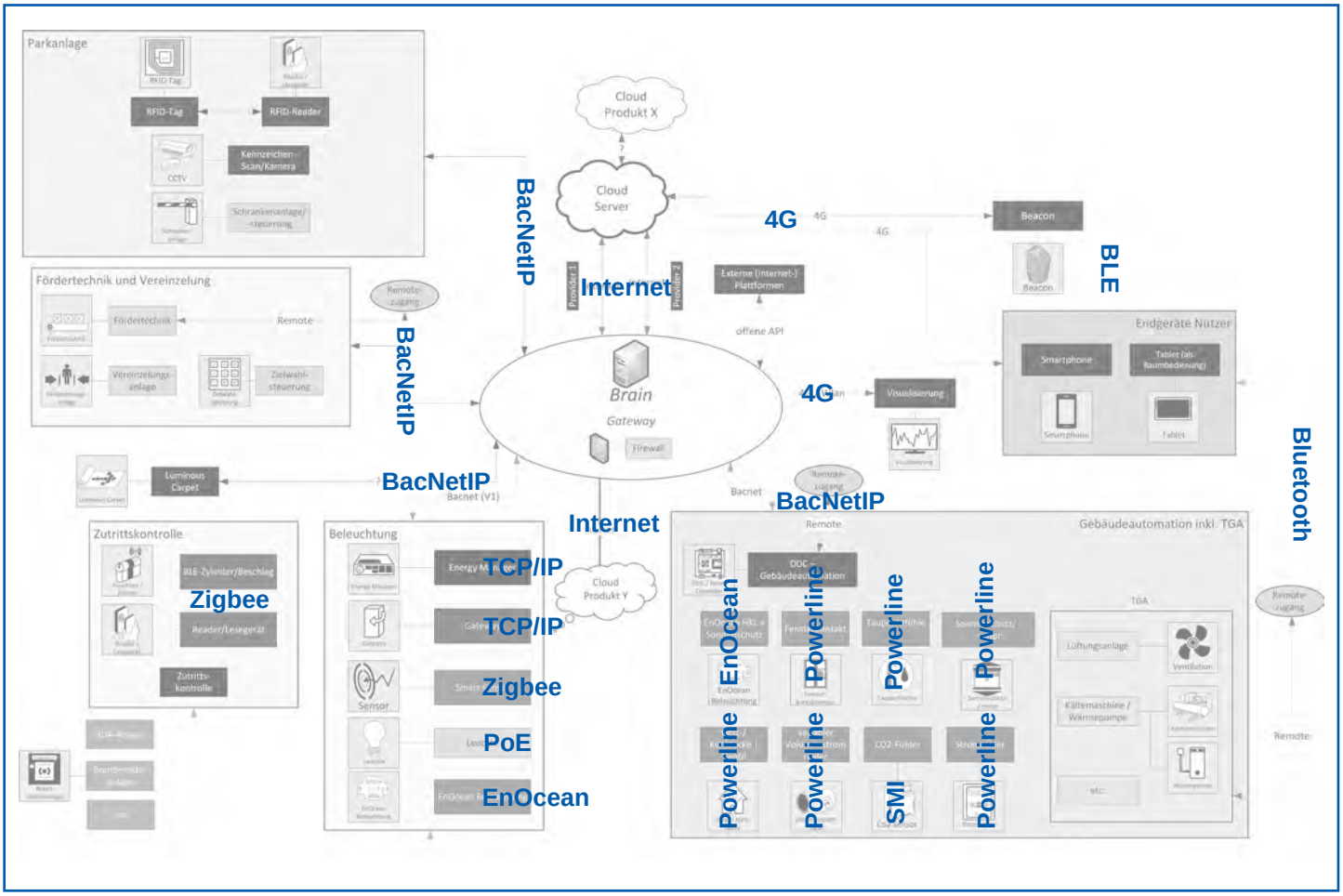

Abbildung 1: Protokolle in der Gebäudeautomation. In einigen Geräten findet man nicht änderbare Standard-Passwörter, die problemlos durch Ausprobieren der gängigsten Passwörter geknackt werden können.

Letztes Jahr wurde bekannt, dass in vielen namenhaften IP-Überwachungskameras die gleiche chinesische Hardware verbaut ist. Diese enthielt eklatante Sicherheitslücken, wie zum Beispiel nicht abgesicherte Server und die Möglichkeit, Standard-Passwörter unverändert zu lassen. So war es möglich, auf zahlreiche Überwachungsvideos zuzugreifen – weltweit. [3]

Mittlerweile gibt es ganze Suchmaschinen, die das Aufspüren solcher Geräte vereinfachen und das Testen auf Standard-Sicherheitslücken ermöglichen. So kann jeder Einsicht in diverse Geräte erhalten. Hier wurden ebenfalls Sicherheitskameras, aber auch Onboard-Überwachungssysteme von LKWs, sowie Heizungs- und Sicherheitskontrollsysteme von Banken gefunden. [4]

Ein weiterer Punkt ist, dass viele Geräte Nutzerdaten lokal speichern. Bei einer Zurücksetzung auf Werkseinstellungen sollten diese gelöscht werden, was aber nicht immer der Fall ist. Das heißt, dass sich durch das Erwerben von gebrauchten IoT-Geräten unter Umständen viel über den ursprünglichen Besitzer herausfinden lässt.

Diese genannten Schwachstellen beziehen sich hauptsächlich auf die Endgeräte. Ein weiterer wichtiger Faktor ist die App bzw. das Smartphone, mit dem viele Geräte gesteuert werden. Abgesehen von den ab und zu sehr fragwürdigen Berechtigungen, die beim Installieren der App bestätigt werden, stellt sich die Frage, ob jeder Nutzer die einzelnen Apps über Passwörter sichert. Ist Ihr Smartphone passwortgeschützt? Bei vielen ist dies nicht der Fall. Somit haben einfache Taschendiebe über das Smartphone bereits Zugriff auf sämtliche Geräte in Ihrem Haushalt.

Was kann schon passieren?

All diese Schwachstellen führen zu ganz neuen Bedrohungsszenarien, und das in allen erdenklichen Umgebungen.
Smart-Home-Geräte sind meistens in das normale Heim-WLAN integriert. Das heißt: Hat ein Angreifer Zugriff auf ein unsicheres IoT-Gerät, hat er oft auch schnell Zugriff auf das gesamte Netz. Hierfür muss nur bei Erstinstallation das WLAN-Passwort im Klartext übertragen werden oder das IoT-Gerät die WLAN-Zugangsdaten unverschlüsselt lokal speichern, was oft der Fall ist. Es reicht also lediglich ein unsicheres Gerät im Netzwerk aus.

Wenn man dies jetzt in größerem Maßstab betrachtet - beispielsweise in smarten Bürogebäuden oder Industriehallen - können die Auswirkungen schon um einiges gravierender sein. Hier können sensible Daten abgegriffen werden, sobald sich ein entsprechend unsicheres Gerät im Netzwerk befindet und das Tor zu diesem öffnet.

Unsichere smarte Geräte ermöglichen nicht nur Einlass zum restlichen Netzwerk, sondern können von Dritten gesteuert werden und Schaden verursachen. Dieser Schaden kann rein wirtschaftlich signifikant sein. Personen- oder Imageschäden sind vorstellbar.

In Finnland wurde im Jahr 2016 die Heizungsanlage von zwei Wohnblocks durch einen gezielten DDoS-Angriff auf die