KORAMIS

Whitepaper

Project Haunted House

Publisher:
Koramis GmbH
Quartier Eurobahnhof
Europaallee 5
66113 Saarbrücken

Mit freundlicher Unterstützung von:

SOPHOS
Security made simple.

Inhaltsverzeichnis

1 Einleitung

Digitalisierung, Maschine-zu-Maschine-Kommunikation - oder anders ausgedrückt, der Datenaustausch zwischen Endgeräten aller Art sowie die Automatisierung in allen Lebensbereichen wird zur Normalität. Die Welt vernetzt sich zusehends und das Internet der Dinge (IoT) gehört längst zur Lebenswirklichkeit. Dabei beschränkt sich dieses Phänomen keineswegs auf den Arbeitsplatz. Auch im häuslichen Umfeld sind internetfähige Geräte und Anwendungen – das IoT – auf dem Vormarsch. Ob sprachgesteuerte Beleuchtung, der intelligente Kühlschrank, der beispielsweise Milch nachbestellt, wenn diese zu Neige geht, die über Handyapp steuerbaren Rollläden oder die Heizung, die wir von unterwegs aus und einstellen können: Das Gerät der Zukunft ist smart und kommuniziert über das Internet mit der Außenwelt, schon heute.

Für das Jahr 2017 werden in den fünf größten Smart-Home-Märkten sowie in den meisten anderen Industrieländern steigende Umsätze erwartet. Die nachfolgende Abbildung zeigt die umsatzstärksten Märkte 2017 mit den prognostizierten Werten.

Abbildung 1.1: Umsatz mit Smart-Home-Komponenten 2017

Zu diesen Smart-Home-Geräten gesellen sich weitere vernetzte Alltagsgegenstände: Vom digitalen Videorecorder über die Kamera im Eingangsbereich bis hin zum Teddybär im Kinderzimmer. Allen ist eins gemein: Sie erleichtern den Alltag, helfen Energie zu sparen und sind, erst einmal konfiguriert, kinderleicht zu bedienen.

Aber sie sind auch, jedes für sich genommen, kleine netzfähige Computer, die auf die ein oder andere Art von außen steuerbar sind. Diese Tatsache weckt Begehrlichkeiten, macht unser Smart-Home zum potenziellen Ziel für Hacker, Cracker und Cyberkriminelle, die das Ziel verfolgen in unsere Privatsphäre einzudringen. Sei es, um persönliche Daten zu sammeln oder die kulminierte Rechenleistung unserer IoT-Geräte in einem Bot-Netz wie MIRAI zu nutzen, um mächtige Cyberattacken auszuführen.

Daher hat eine sachgerechte, den Security-Anforderungen entsprechende Installation, höchste Priorität. Denn ist die zentrale Kontrolleinheit unserer Heimautomatisierung schlecht oder unzureichend geschützt und über das Internet erreichbar, könnten Hacker dieses Einfallstor nutzen und das gemütliche Smart-Home in ein Haunted House verwandeln.

Da es bisher keine validen Daten zu dem Themenkomplex Smart-Home-Hacking gibt, bildete KORAMIS mit dem Haunted House eine Smart-Home-Infrastruktur nach und stellte diese als Honeypot ins Internet, um zu analysieren, wie Angriffe auf Smart-Home-Geräte ablaufen, welche Angriffsvektoren bevorzugt genutzt werden und wie verbreitet das dazu benötigt Wissen bereits ist.

Dadurch sollen Kenntnisse über Qualität, Quantität und Aggressivität der Angriffsanatomie gewonnen werden. Dabei wurden Komponenten und Systeme verschiedener Hersteller in der Testumgebung verwendet, um ein möglichst umfassendes Bild zu erhalten.

Ziel der Untersuchung ist das Aufzeigen und die Dokumentation möglicher Risiken und Gefahren, die durch mangelhaft oder falsch konfigurierte Smart-Home-Systeme entstehen, um ein Bewusstsein für dieses Thema zu schaffen.

Zudem soll dem interessierten Nutzer ein Überblick über einige Komponenten und Security-Ansätze an die Hand gegeben werden, die ihm helfen, die eigene Smart-Home-Umgebung sicherer zu gestalten.

2 Projekt Haunted House

Um einen Überblick über die Gefahr von Attacken und die von Hackern angewandten Methoden bei Angriffen auf Smart-Homes zu erhalten, hat SOPHOS in Kooperation mit KORAMIS eine Smart-Home-Infrastruktur nachgebildet und als Honeypot im Internet zur Verfügung gestellt: Das Projekt Haunted House.

Abbildung 2.1: Eingangsbereich des Haunted House

Bei der Konfiguration der Systeme wurden die von Herstellern empfohlenen Vorgehensweisen und Techniken beachtet, damit die Infrastruktur einem realen smarten Haus so nah wie möglich kommt.

Abbildung 2.2: Simulation einer Heizungssteuerung

Dieser realitätsnahe Systemaufbau erlaubt es von Angreifern zu lernen, indem die verschiedenen Angriffe beobachtet, aufgezeichnet und analysiert werden.

2.1 Aufbau und Layout

Zur Veranschaulichung sind die aus Nutzersicht sichtbaren Geräte auf einer 4,00m x 2,50m großen, einer Wohnung nachempfundenen, Fläche verbaut. Um die Zuordnung von Gerät und Hersteller zu erleichtern, sind die Geräte jeweils in den einzelnen Räumen gruppiert. Die Verkabelung der Infrastruktur erfolgt für den Nutzer nicht sichtbar auf der Rückseite.

Die Verbindung zum Internet und das WLAN für das Haunted House wird über eine FritzBox bereitgestellt. Die Verbindung der zentralen Steuereinheiten der verschiedenen Systeme erfolgt kabelgebunden per Ethernet über einen gemanagten Lancom Switch. Per Spiegelung wird der gesamte Datenverkehr mit dem Internet an die Analyse weitergeleitet. Neben dem WLAN betreiben einige der Geräte eigene drahtlose Verbindungen, über die sie mit ihren Aktoren und Sensoren kommunizieren.

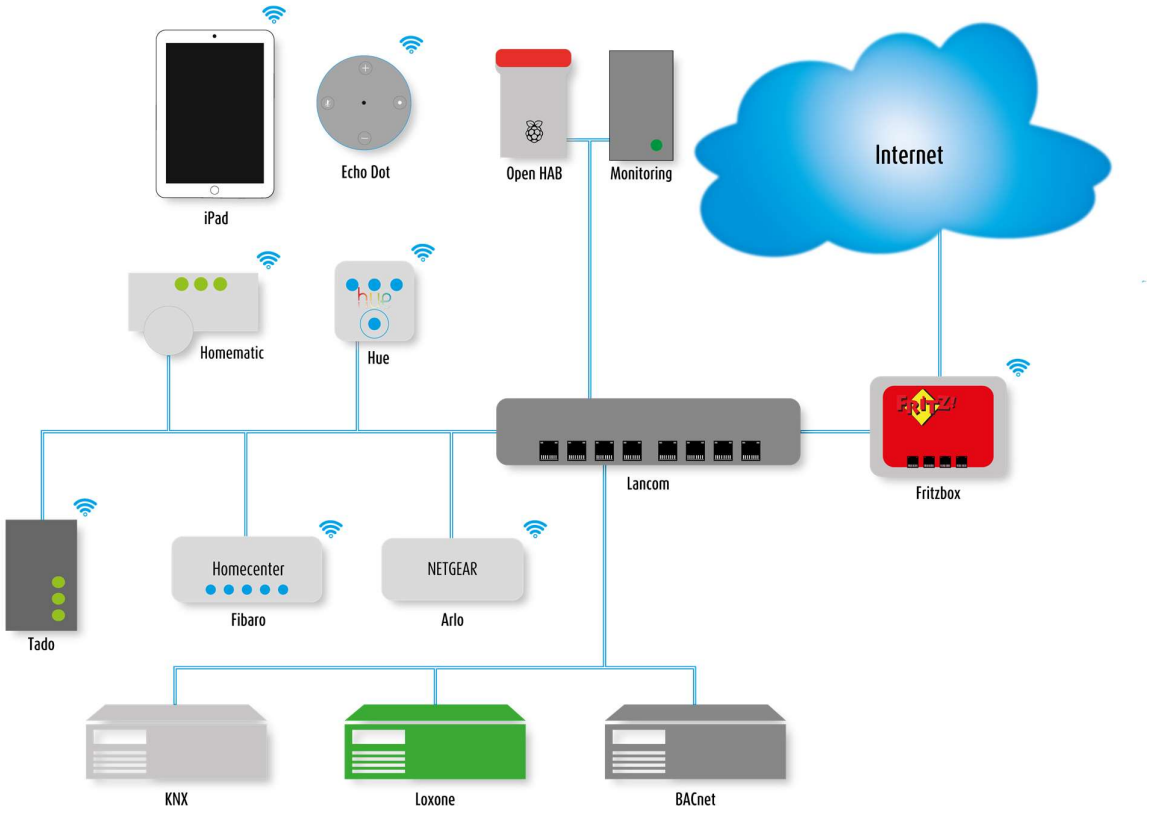


Abbildung 2.3: Layout Haunted House

2.2 Verbaute Komponenten

Bei der Komponentenauswahl wurde darauf geachtet, dass ein breites Spektrum von am Markt etablierten Herstellern und Protokollen vertreten ist. Während bei einer privaten Installation gegebenenfalls darauf geachtet wird, möglichst nur Komponenten eines Herstellers zu verwenden, wurden im Haunted House bewusst eine Vielzahl unterschiedlicher Systeme verbaut, um eine möglichst vielseitige Angriffsfläche zu bieten.

Bei der Installation der Komponenten wurde nach Herstelleranweisung vorgegangen.

KNX (Ekinex)

KNX ist ein Feldbus-System, bei dem die Gerätesteuerung und die Stromversorgung in zwei getrennten Netzen erfolgt. Die Aktoren werden über den 2-Leiter KNX-Bus mit Datenpaketen in Telegrammform gesteuert. Über einen IP-KNX-Koppler können die Datenpakete auch über Ethernet versendet werden.

BACnet (Loytec)

BACnet ist ein Feldbus-System, das Ende der 1980er Jahre als herstellerunabhängiger Standard für die Datenkommunikation in der Gebäudeautomatisierung entwickelt wurde.

HomeMatic

Die HomeMatic Zentrale CCU2 ist die zentrale Steuereinheit und das Gateway für die Aktoren und Sensoren, die über den proprietären Funkstandard BidCoS (Bidirectional Communication Standard) eingebunden sind. BidCoS wurde von eQ-3 speziell für die drahtlose Ansteuerung von Aktoren und Sensoren zur Hausautomation entwickelt und nutzt eine Frequenz von 868 MHz.

Loxone Miniserver

Der Loxone Miniserver stellt in der Grundausführung digitale und analoge Eingänge sowie analoge Ausgänge und Relais-Ausgänge bereit. Zusätzlich ist eine Ethernet- und eine KNX-Schnittstelle vorhanden. Über Erweiterungsmodule können Schnittstellen zu anderen Protokollen hinzugefügt werden.

Fibaro HCL

Das Fibaro Home Center Lite ist die zentrale Steuereinheit und das Gateway für die Aktoren und Sensoren, die über den Z-Wave Funkstandard eingebunden sind. Z-Wave wurde Anfang der 2000er Jahre als drahtloser Kommunikationsstandard entwickelt, der Frequenzen zwischen 850 und 950 MHz verwendet und eine maximale Datenrate von 100 kB/s bei einer Funkreichweite von mindestens 40 m in geschlossenen Gebäuden erreicht.

Philips HUE

Die Philips HUE Bridge ist die zentrale Steuereinheit und das Gateway für die Leuchtmittel, die über den ZigBee Light Link Funkstandard eingebunden sind. ZigBee wurde Anfang der 2000er Jahre als drahtloser Kommunikationsstandard entwickelt, der Frequenzen zwischen 2400 und 2483,5 MHz. verwendet.

tado

tado ist eine intelligente Heizungskörpersteuerung, die im Wesentlichen aus zwei Hardwarekomponenten, dem Smart-Thermostate und der tado Bridge, besteht. Diese kommunizieren per Funk auf 868 Mhz und mittels des dafür ausgelegten Protokolls „6LoWPAN“. Die Heizungssteuerung wird dabei mit einer App gesteuert und konfiguriert.

Netgear Arlo

Die Netgear Arlo ist eine kabellose Smart-Home-Sicherheitskamera, die die Aufzeichnung bei Bewegung automatisch startet. Die Kamera kommuniziert über Funk mit dem Arlo Gateway. Auf dieses kann der User mit einer App zugreifen und das aufgezeichnete Bildmaterial einsehen.

Amazon Echo Dot

Der Amazon Echo Dot ermöglicht die Steuerung kompatibler Smart-Home-Komponenten über Sprachsteuerung und Stimmerkennung. Der Echo Dot verbindet sich mit dem Alexa Voice Service von Amazon und ermöglicht dadurch sogar Einkäufe über Amazon.

Apple iPad mini

Das iPad mini ist per WLAN in das Smart-Home-Netzwerk eingebunden und dient als Anzeige- und Steuerungselement für die meisten Smart-Home-Komponenten des Haunted House.

openHab

OpenHab ist eine Softwarelösung, die Smart-Home-Geräte diverser Anbieter hersteller- und protokollneutral miteinander verbindet und eine benutzerfreundliche Visualisierung ermöglicht. Die Software kann beispielsweise auf einem Raspberry Pi installiert werden und ersetzt dann die Steuerzentralen der jeweiligen Systeme.

Abbildung 2.4: Weitere Räume des Haunted House

2.3 Analyse- und Monitoring Tools

Zur detaillierteren Analyse der Angriffe wurden zwei unabhängige Monitoring-Instanzen und mehrere Analysetools, zum Logging und Reporting aufgebaut. Die verwendeten Analysetools sind speziell auf die Anforderungen des Systems ausgelegt.
Die erste Instanz überwacht den eingehenden Traffic aus dem Internet und protokolliert mit Hilfe von Loggings und Network-Sniffern die Zugriffe aus dem Internet. Anhand aktueller Provider-Datenbanken und Geolocater können die zum Zugriff genutzten IP-Adressen Ländern und Regionen zugeordnet werden.

Die zweite Instanz ist im eigentlichen Smart-Home-Netzwerk installiert und ermöglicht durch den Einsatz eines Network-Sniffers und eines Intrusion-Detection-Systems die Vorgehensweise und Handlungen eines Angreifers detailliert nachzuvollziehen.
Zusätzlich zu den Monitoring Tools werden die System-Events der einzelnen Komponenten zur weiteren Auswertung herangezogen, was die Bewertung der Auswirkungen eines Angriffes ermöglicht.

3 Smart-Home-Geräte

3.1 Grundsätzlicher Aufbau

Der Aufbau einer Smart-Home-Infrastruktur ist in den zugrundeliegenden Systematiken bei allen Anbietern sehr ähnlich. Die Funktionsbausteine Messen, Regeln, Visualisieren und Kommunizieren sind vorhanden. Am Beispiel einer Heizungsanlage kann anschaulich dargestellt werden, wie die unterschiedlichen Funktionsbausteine zum Einsatz kommen und wie sie mit einander verknüpft sind.

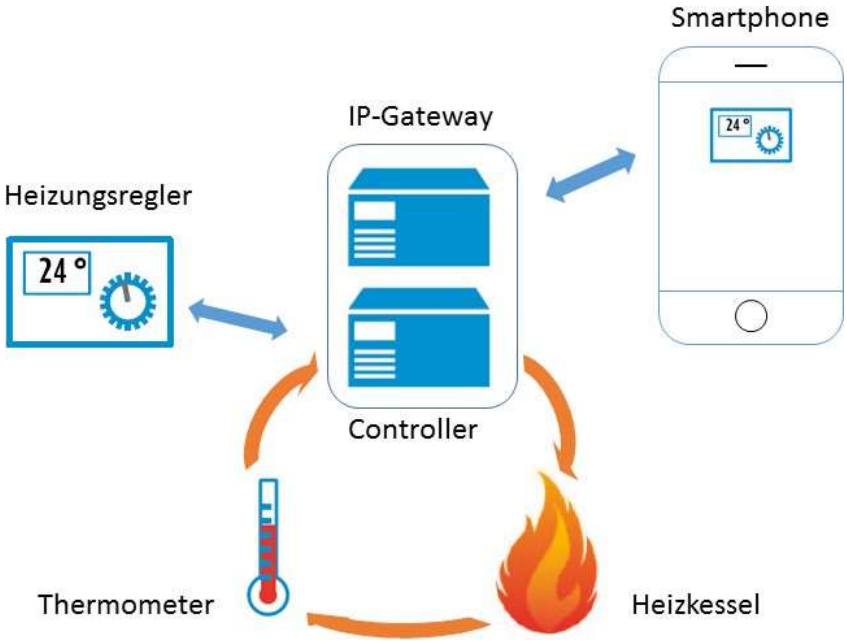


Abbildung 3.1: Schmatischer Aufbau - Heizungssteuerung und Industrial Control System

Über die Bedienelemente ’Heizungsregler’ und ’Smartphone’ erfolgen die Visualisierung und die Einstellung. Die zentrale Einheit mit ’Controller’ und ’IP-Gateway’ nimmt die Regelungen am ’Heizkessel’ vor. Das ’Thermometer’ gibt die Messwerte an die zentrale Einheit weiter. In vielen Geräten sind heute mehrere oder alle Funktionsbausteinen in einem Gehäuse untergebracht. Der Bewegungsmelder (Messen) einer Überwachungskamera aktiviert diese (Regeln) und das Bild wird per WLAN (Kommunizieren) auf ein Smartphone (Visualisieren) übertragen, dieses Gerät vereint alle vier Funktionen.

Von besonderem Interesse für diese Untersuchung sind Geräte, die über ein IP-Gateway verfügen und damit eine Verbindung zum Internet aufbauen können. Die Verbindung kann kabelgebunden oder mittels Funktechnologie erfolgen. Die Bedienung der Geräte kann klassisch per Schalter erfolgen, per Smartphone-App, im Webbrowser oder über eine Spracherkennung, wie sie z.B. Amazon Echo oder Apples Siri ermöglicht.

3.2 Smart-Home-Geräte im Internet

Um die Einordnung der Untersuchungsergebnisse in einem größeren Kontext zu ermöglichen, wurden parallel zum Betrieb des Honeypots aktive Internet-Scans durchgeführt. Dabei wurde nach Geräten gesucht, die als Gateway eine Verbindung zu Smart-Home-Installationen ermöglichen. Der Fokus der Scans lag auf den Protokollen KNX/IP, BACnet und FOX. Außerdem wurden Web-GUIs bekannter Smart-Home-Komponenten gesucht.

Smart-Home-Protokolle

In den Gateways findet die Übersetzung zwischen den verschiedenen Netzwerktypen und den jeweils verwendeten Protokollen statt und ermöglicht so die Verbindung von unterschiedlichen Systemen. Im OSI-Modell ist die Arbeit der betrachteten Gateways auf Layer 2 angesiedelt. Die regionale Verteilung der verwendeten Komponenten und der unterstützten Protokolle ist dabei sehr unterschiedlich.

Region	FOX	BACnet	KNX/IP
Deutschland	84	107	1.227
Europa	4.784	2.329	9.719
Welt	27.237	16.418	11.695

Tabelle 3.1: Verteilung der Komponenten je Protokoll und Region

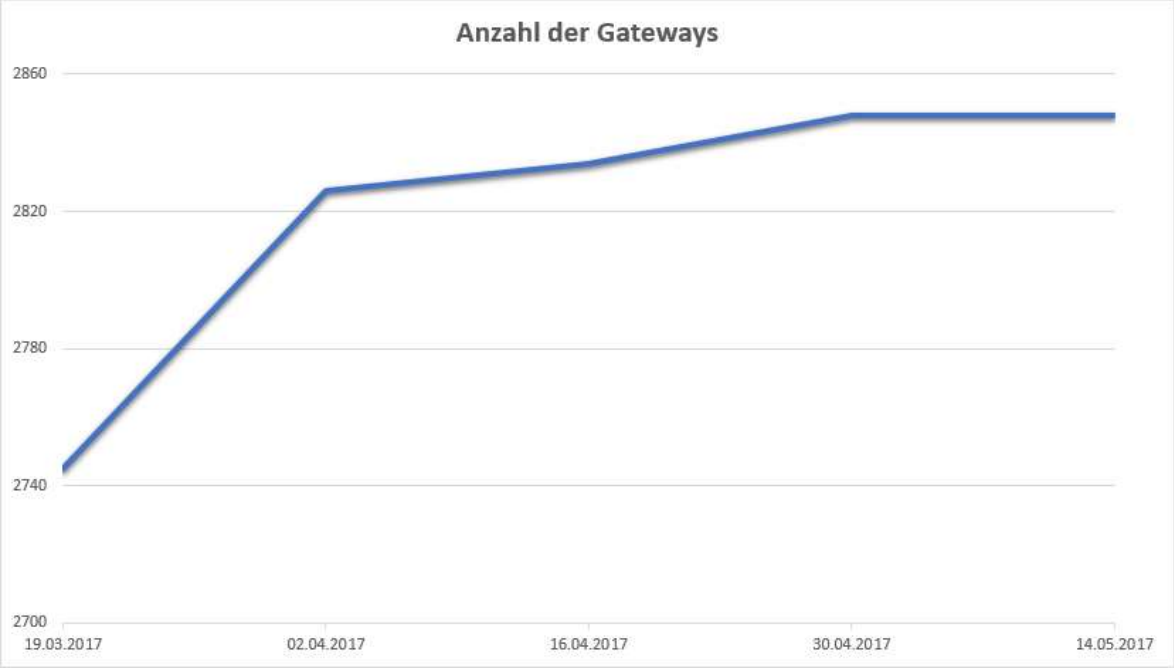
Das in Deutschland wenig verbreitete FOX-Protokoll ist dabei weltweit am häufigsten vertreten. Dahingegen wird das in Deutschland weit verbreitete KNX-Protokoll in anderen Regionen seltener eingesetzt. Aufgrund regional unterschiedlicher Anforderungen und regulatorischer Vorschriften hat sich noch kein weltweiter Standard zur Vernetzung von Smart-Home-Geräten etabliert.

Während des Untersuchungszeitraums wurde zu mehreren Zeitpunkten ein Scan durchgeführt, um die Entwicklung im zeitlichen Ablauf zu analysieren. Bei der Betrachtung aller Protokolle zusammen, lässt sich im Zeitraum vom 19.03.2017 bis zum 14.05.2017 in der Region DACH (Deutschland, Österreich, Schweiz) ein Zuwachs von 103 offenen Gateways feststellen. Dies entspricht einer Wachstumsrate von ca. 3,7% über zwei Monate gesehen.

Datum	FOX	BACnet	KNX/IP
19.03.2017	190	204	2.351
02.04.2017	190	215	2.421
16.04.2017	188	194	2.452
30.04.2017	185	195	2.468
14.05.2017	184	191	2.473

Tabelle 3.2: Anzahl der Geräte im Zeitablauf Region DACH

Für den Smart-Home-Markt wird für die nächsten fünf Jahre eine durchschnittliche Wachstumsrate von ca. 25% in der DACH-Region prognostiziert.[1] Bei einem Wachstum von 3,7% in zwei Monaten erhält man bei linearer Fortschreibung eine jährliche Wachstumsrate von 22,2%. Trotz der geringen Dauer des Beobachtungszeitraums und der Konzentration auf wenige Protokolle ist davon auszugehen, dass die gemessenen Werte die prognostizierte Marktentwicklung gut widerspiegeln und



bestätigen.

Abbildung 3.2: Anzahl der gefundenen Gateways in der Region DACH

[1] Quelle: www.statista.com

Weltweit ließ sich im gleichen Zeitraum ein Zuwachs von 1672 offenen Gateways beobachten. Dies entspricht einer Wachstumsrate von ca. 3,1% im Beobachtungszeitraum.

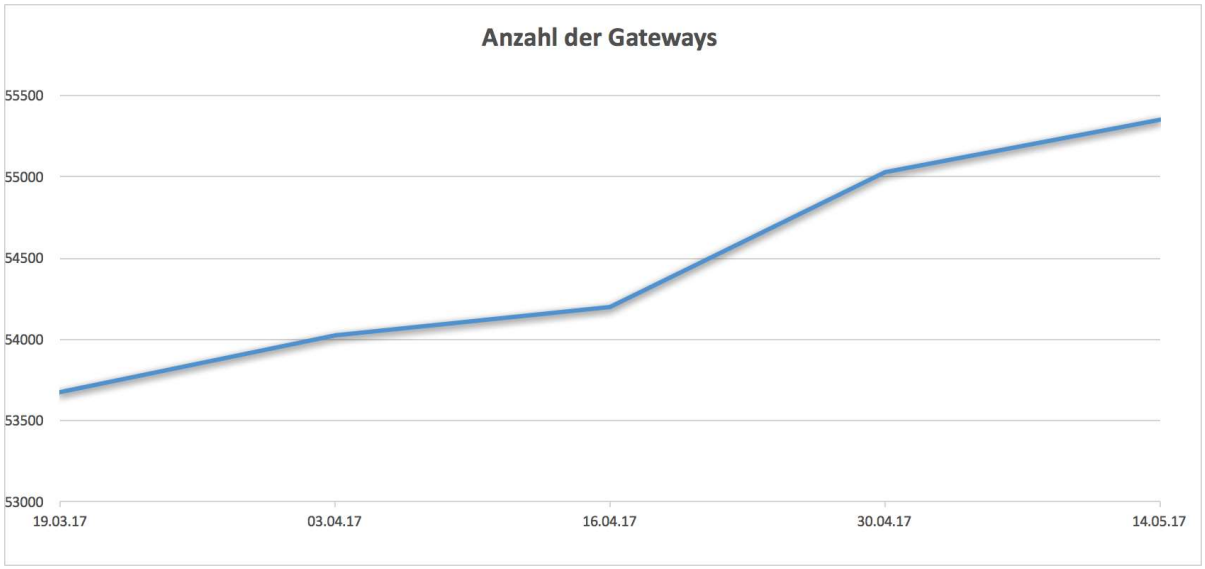


Abbildung 3.3: Anzahl der gefundenen Gateways global

Auf den nachfolgenden Karten sind erreichbare Gateways verzeichnet. Für die Bestimmung des Standortes wurden die IP-Adressen verwendet. Bei der Ermittlung von Standortinformationen über die IP-Adresse sind Ungenauigkeiten systembedingt nicht zu vermeiden. Je dichter das Netzwerk in einer Region ist, desto genauer kann der Standort über die IP-Adresse ermittelt werden. In ländlichen Regionen ist die Standortbestimmung entsprechen größeren Schwankungen unterworfen. Um regionale Unterschiede in der Verfügbarkeit offener Gateways zu visualisieren, ist die verfügbare Genauigkeit ausreichend.

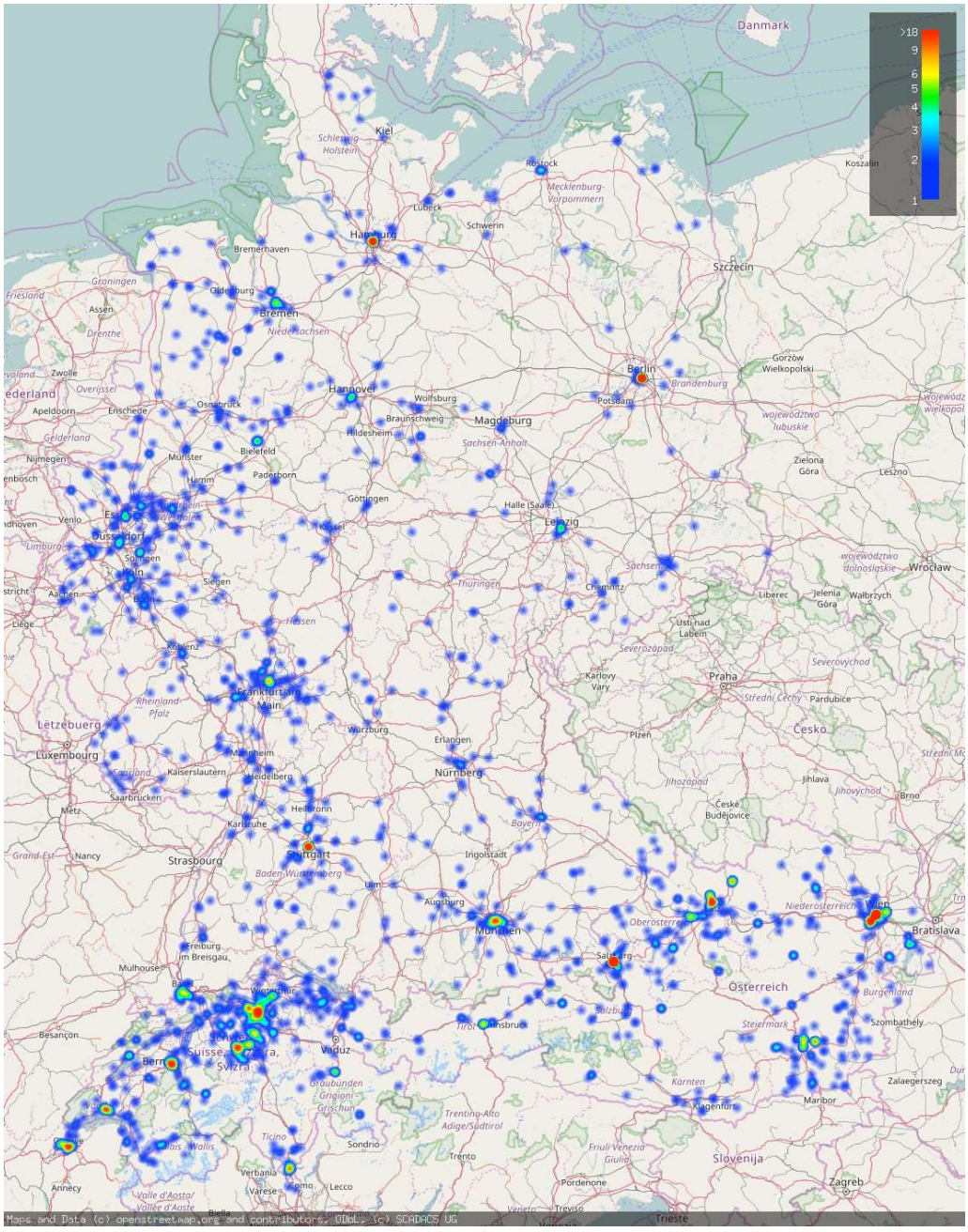


Abbildung 3.4: Gateways in DACH

Auf europäischer Ebene ist zu erkennen, dass die Konzentration der gefundenen Smart-Home-Gateways in Mitteleuropa am stärksten ist.

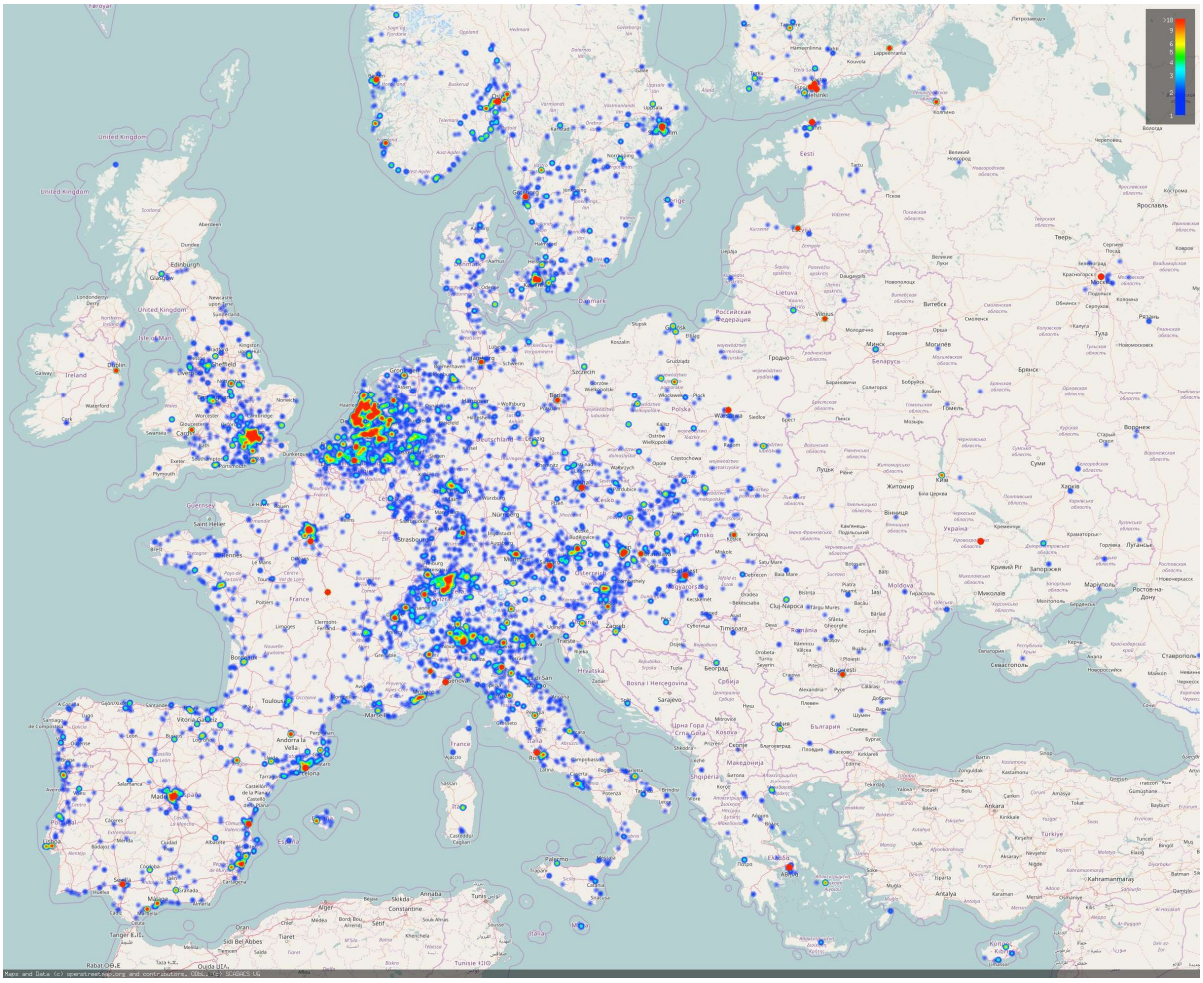


Abbildung 3.5: Gateways in Europa

Im Vergleich der Regionen ist deutlich zu erkennen, dass in Europa und den USA die meisten Gateways gefunden wurden. Zum einen sind aufgrund der Bevölkerungsdichte und Wirtschaftskraft grundsätzlich mehr Geräte installiert als beispielsweise in Afrika. Zudem werden in anderen Regionen wie beispielsweise Asien andere Protokolle und Standards verwendet, die durch die Scans nicht erfasst wurden.

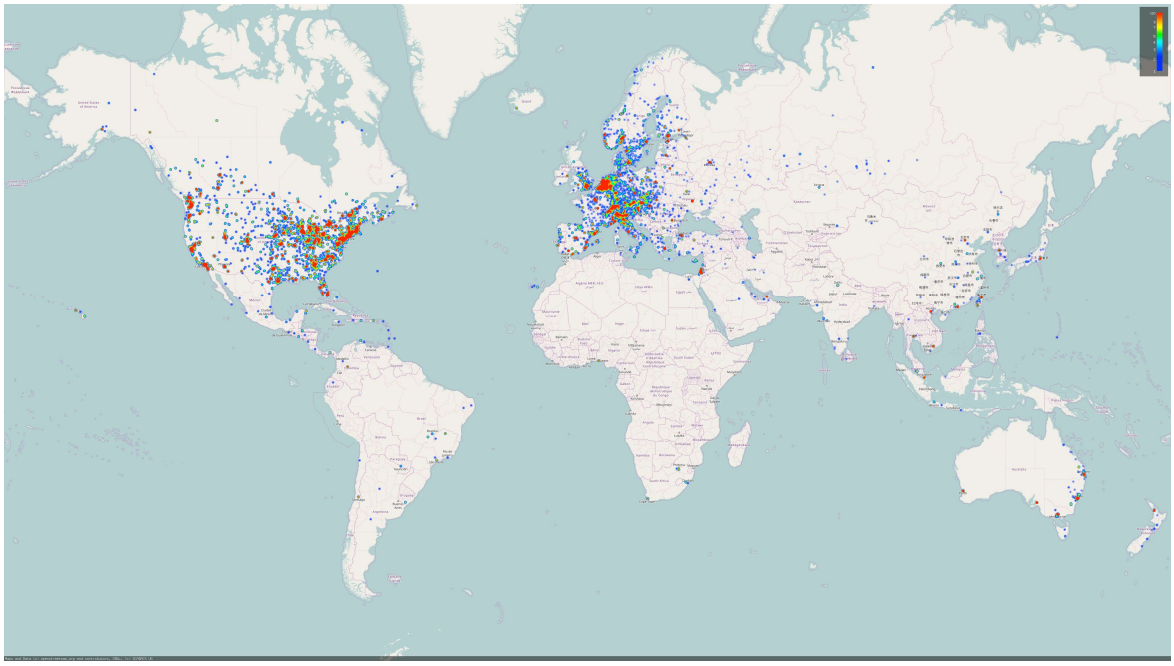


Abbildung 3.6: Gateways global

Web-GUIs von Smart-Home-Komponenten

Die Web-GUIs (engl. graphical user interface, Grafische Benutzeroberfläche) dienen als Interface für die Konfiguration und als Plattform für die Visualisierung der aktuellen Zustände des Systems. Werden die Zugangsdaten beim initialen Setup nicht geändert oder schwache Passwörter verwendet, erhalten Angreifer eine leicht auszunutzende Gelegenheit die betroffenen Systeme zu kompromittieren und private Daten auszuspähen.

Bei den Scans nach Web-GUIs sind in der DACH-Region deutlich mehr Treffer zu verzeichnen als bei der Suche nach den Komponenten von FOX, BACnet oder KNX/IP. Zum einen sind bei der Suche nach den Web-GUIs mehr Treffer zu erwarten, da eine größere Auswahl an Systemen bei der Suche berücksichtigt wird. Zum anderen werden Systeme, die direkt an den Endnutzer vertrieben werden ggf. häufiger von technisch weniger versierten Personen installiert und sind entsprechend häufiger im Internet auffindbar, ohne dass sich der Nutzer darüber im klaren ist.

Auf der nachfolgenden Karte sind erreichbare Web-GUIs verzeichnet. Für die Bestimmung der Standortes wurden die IP-Adressen verwendet. Bei der Ermittlung von Standortinformationen über die IP-Adresse sind Ungenauigkeiten systembedingt nicht zu vermeiden. Je dichter das Netzwerk in einer Region ist, desto genauer kann der Standort über die IP-Adresse ermittelt werden. In ländlichen Regionen ist die Standortbestimmung entsprechen größeren Schwankungen unterworfen.

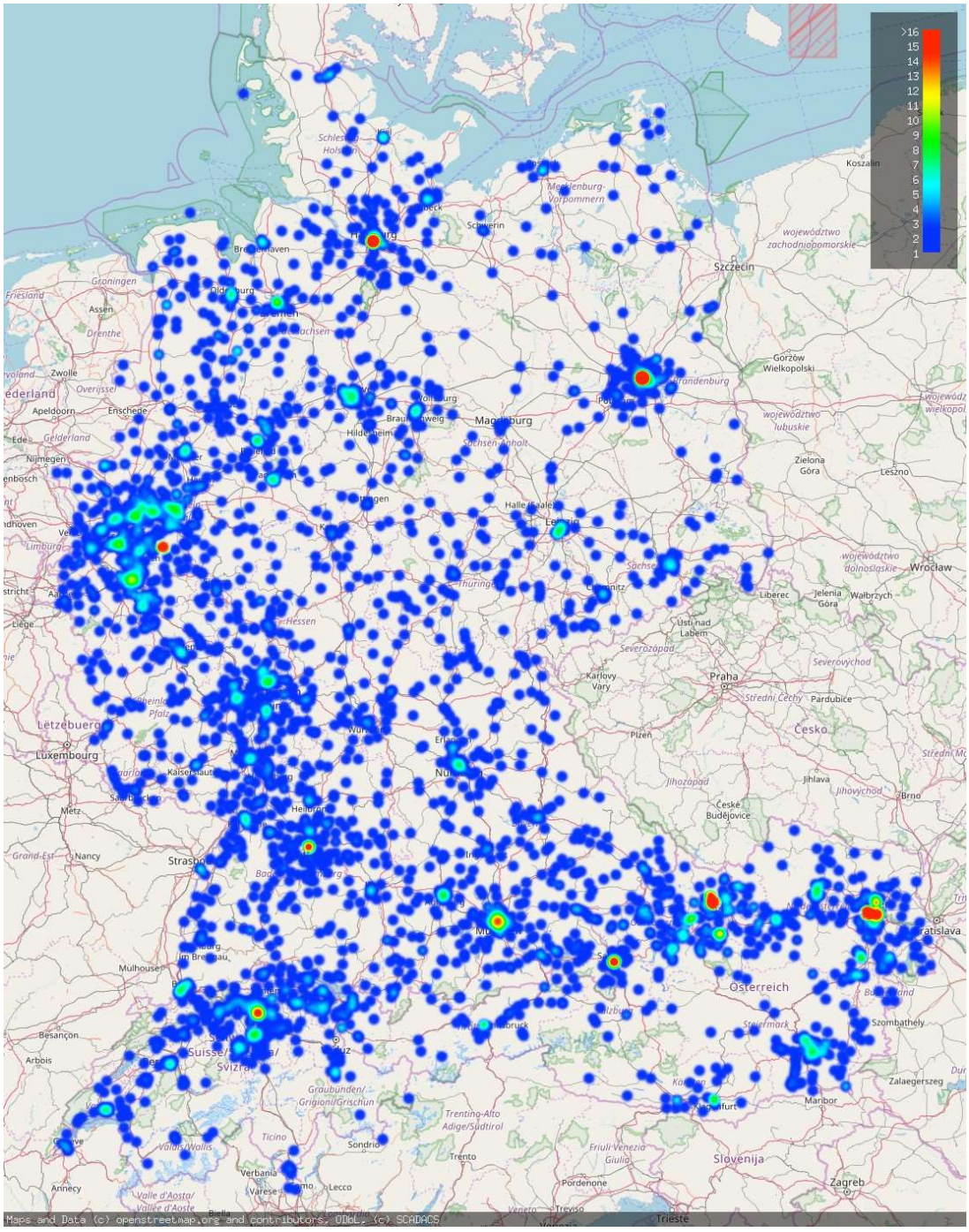


Abbildung 3.7: Offene Web-GUIs in DACH

4 Projektablauf

Nachdem der Aufbau, die Installation sowie die Konfiguration der Smart-Home-Infrastruktur beendet war, wurde eine eigene öffentliche IP-Adresse für das Haunted House konfiguriert und in der FritzBox ein Portforwarding auf die einzelnen Komponenten eingerichtet. Dieses Vorgehen entspricht dem Standard-Setup vieler Smart-Home-Besitzer und ermöglicht den direkten Zugriff auf Smart-Home-Komponenten von unterwegs.

Alle Systeme wurden nach Herstellerangaben eingerichtet. Standardpasswörter wurden zunächst für die 1. Testphase (6 Wochen) durch eigene sichere Passwörter ersetzt und alle nicht benötigte Services deaktiviert.

Während der 2. Testphase (3 Wochen) wurden die Systeme auf die Standardeinstellungen und -passwörter des Herstellers zurückgesetzt.

Um die größtmögliche Verbreitung der Infrastruktur zu erreichen, wurde ein schnelles Listing der einzelnen Komponenten bei den „Internet-of-Things“-Suchmaschine SHODAN (www.shodan.io) und Censys (www.censys.io) durchgeführt.

Über diese Suchmaschinen werden alle Komponenten des Haunted House mit ihren erreichbaren Services aufgezeigt. Dabei werden nicht nur die offenen Ports, sondern auch die Versionsnummer der entsprechenden Services angezeigt.

SHODAN

SHODAN ist eine „Internet-of-Things“-Suchmaschine, die es Nutzern ermöglicht Dienste von Geräten zu finden, die mit dem Internet verbunden sind. Dazu verbindet sich SHODAN auf verschiedenen Ports mit den Geräten und katalogisiert die Service-Banner, mit denen sich die jeweiligen Geräte ausweisen. Darüber hinaus werden Meta-Daten wie Standort, Betriebssystem und Hostname gesammelt. So entsteht ein Datenpool mit IP-Adressen und Informationen zu der Softwareversion und verfügbaren Diensten sowie den jeweils unterstützen Optionen. Dieser Datenpool kann über das Webinterface auf der Internetseite shodan.io durchsucht werden.

Die Informationen, die die Service-Banner enthalten unterscheiden sich je nach Hersteller des Gerätes und seines Einsatzzweckes.

Die Crawler, die die Daten sammeln sind rund um die Uhr im Einsatz. Um eine Verzerrung der gefundenen Geräte, beispielsweise durch das Blockieren landespezifischer IP-Adressen, zu vermeiden, betreibt SHODAN Server in acht Ländern, verteilt über den Globus. Die IP-Adressen für die Scans werden zufällig erzeugt.

Für einige Schwachstellen (z.B. Heartbleed) wird auf jedem Gerät eine automatische Prüfung durchgeführt.

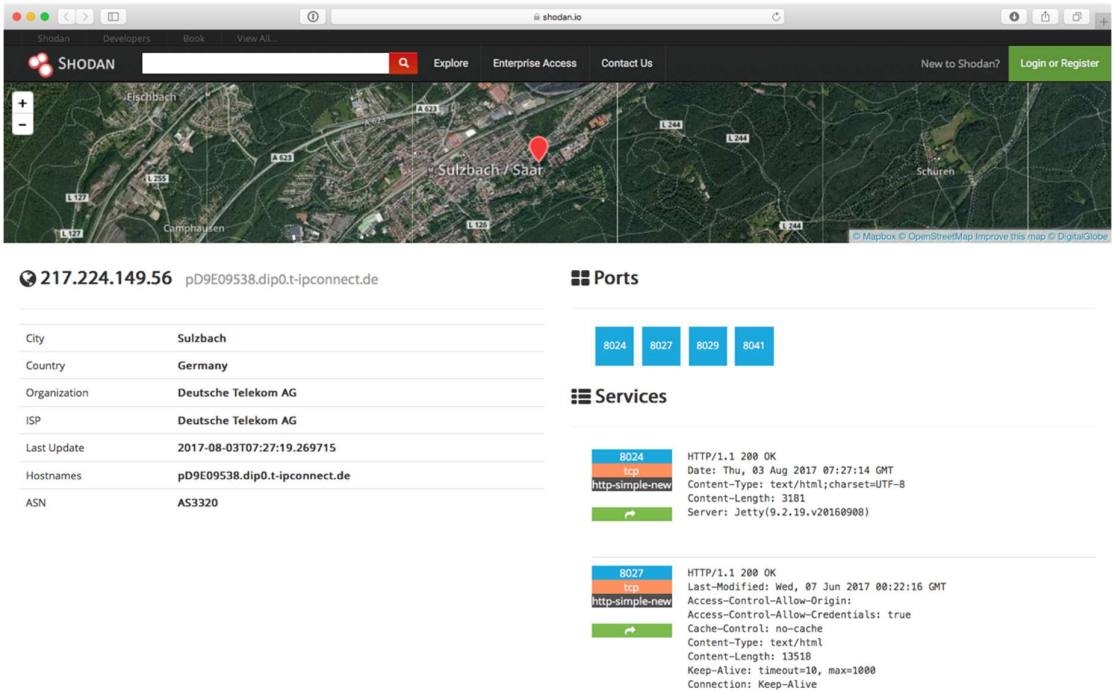


Abbildung 4.1: Einzelansicht der Haunted House Komponenten bei SHODAN

Censys

Censys nutzt die Openscource-Tools ZMap und ZGrap, um täglich einen Scan sämtlicher IPv4-Adressen durchzuführen und so Daten zu Geräten, Hosts und Diensten zu sammeln. Das ZMap-Projekt wurde 2013 an der University of Michigan ins Leben gerufen und wird mittlerweile von einer großen Community als Open-Source Projekt weitergeführt. Die Software ZMap ist so ausgelegt, dass sie innerhalb von 45 Minuten den gesamten öffentlichen IPv4-Adressbereich scannen kann. Mit entsprechend ausgestatteter Internetverbindung kann dieser Vorgang auf fünf Minuten verkürzt werden. Durch die Ergänzung ZGrap können - ähnlich wie bei SHODAN - die Service-Banner ausgelesen und gespeichert werden. Die von Censys gesammelten Daten können über ein Webinterface auf der Seite censys.io durchsucht werden.

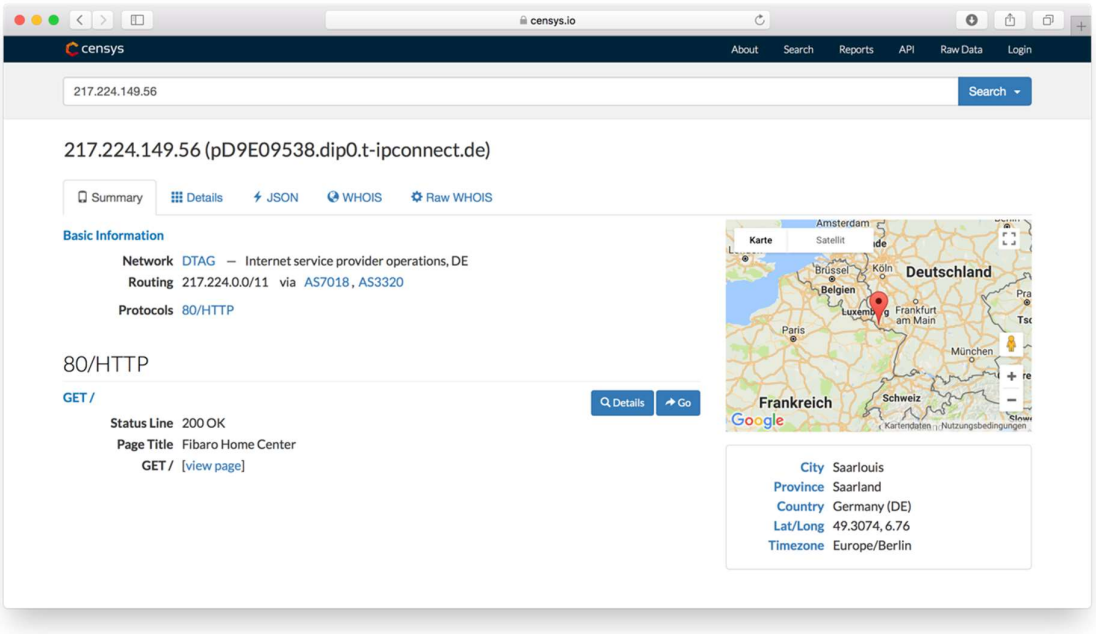


Abbildung 4.2: Einzelansicht der Haunted House Komponenten bei Censys

Während des gesamten Betriebes wurde mit Hilfe der Analysetools sowohl der Netzwerkverkehr als auch die Systemevents aufgezeichnet und archiviert.

5 Ergebnisse

Das folgende Kapitel gliedert sich in drei Abschnitte. Zunächst werden die Ergebnisse der beiden Testphasen, an denen das Haunted House mit unterschiedlicher Konfiguration mit dem Internet verbunden war, präsentiert. Anschließend folgt die Analyse der beobachteten Aktivitäten während der beiden Testphasen.

5.1 Testphase 1

In der ersten Testphase wurde die Haunted House Infrastruktur über einen Zeitraum von sechs Wochen mit eigenen, sicheren Passwörtern betrieben. Im Anschluss wurden die Zugriffe und Zugriffsversuche analysiert und bewertet.

Folgende Erkenntnisse konnten gewonnen werden:
Insgesamt wurden 70.526 Zugriffsversuche von 24.089 unterschiedlichen IP-Adressen detektiert. Das entspricht täglich ca. 1.500 Zugriffsversuchen.

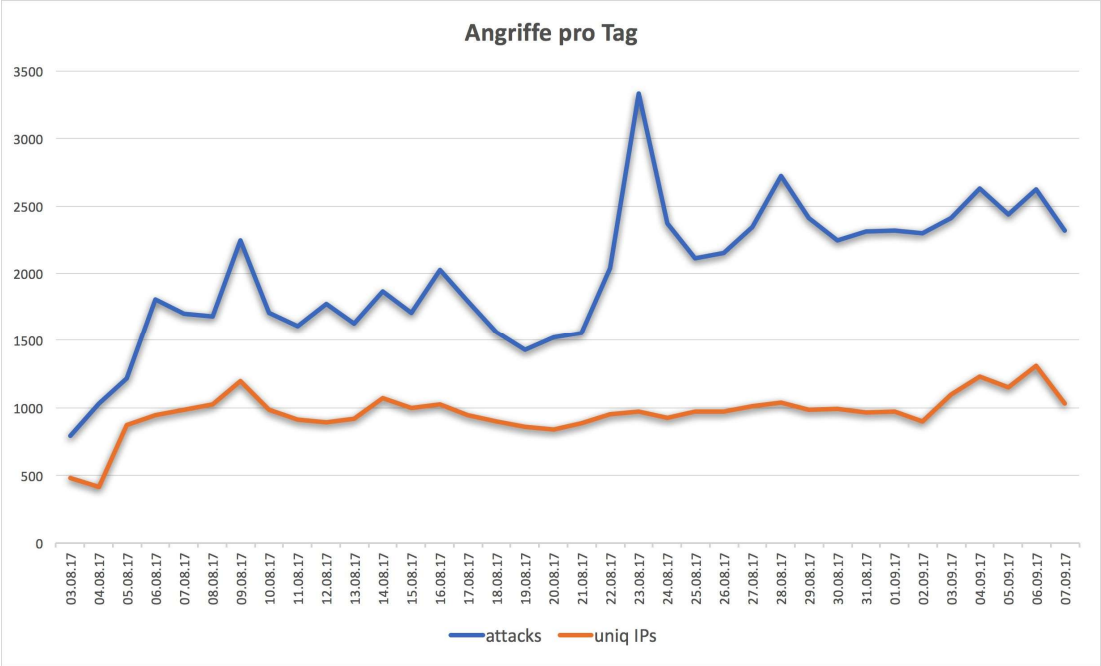


Abbildung 5.1: Zugriffsversuche pro Tag

Aus fast jedem Land der Welt wurde im Versuchszeitraum mindestens einmal versucht eine Komponente anzusprechen.

Folgende Grafik zeigt die Top 10 Länder nach Angriffsversuchen auf:

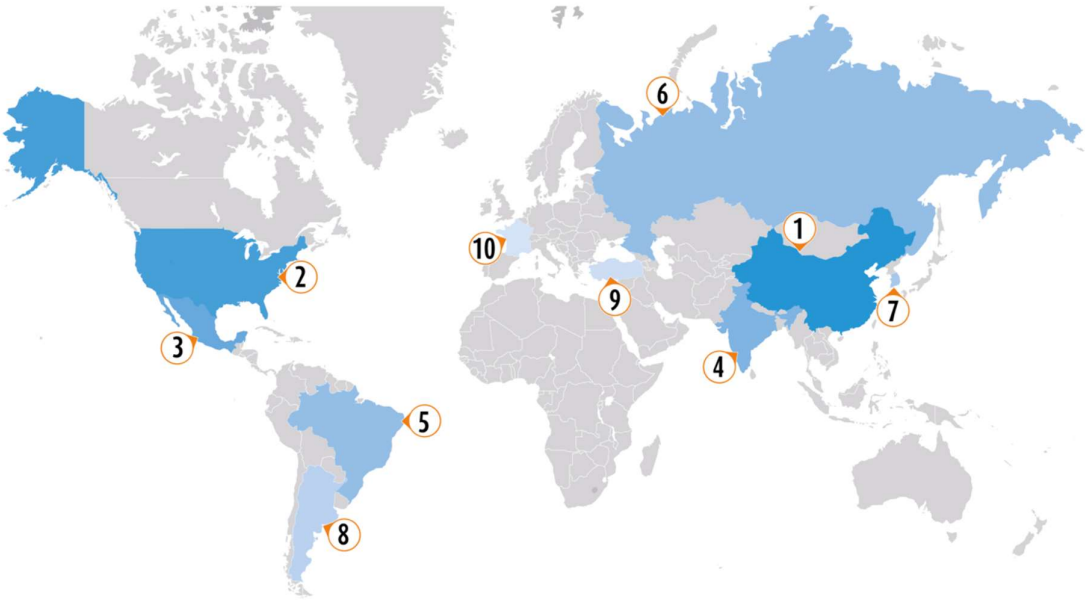


Abbildung 5.2: Weltkarte mit den Top 10 der Länder aus denen Zugriffe erfolgt sind

Die hier dargestellten Länder repräsentieren nur die letzte auflösbare IP-Adresse des Zugriffs. Der tatsächliche Standort des Zugreifenden kann gegebenenfalls davon abweichen.

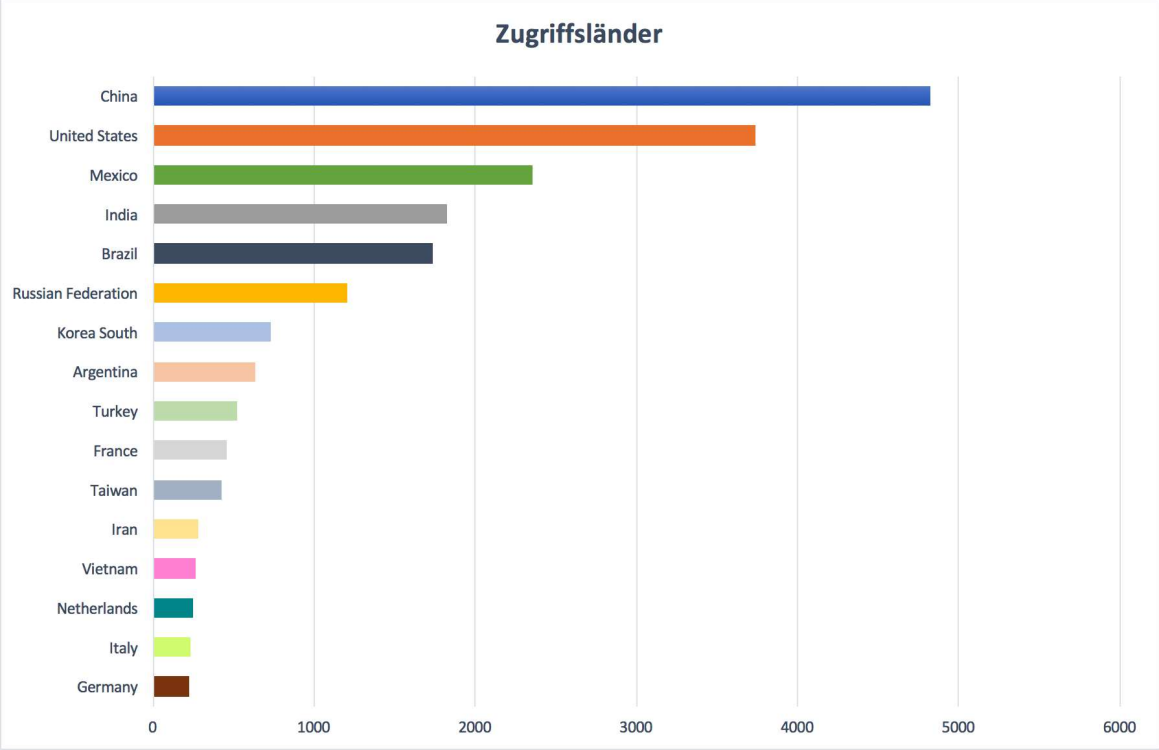


Abbildung 5.6: Länder aus denen die Zugriffe erfolgten

Die Zugriffsversuche erfolgten dabei über verschiedene Netzwerkports. Durch eine genauere Analyse der Zugriffsversuche konnte festgestellt werden, dass ein Großteil aller Zugriffe automatisiert durchgeführt wurden.

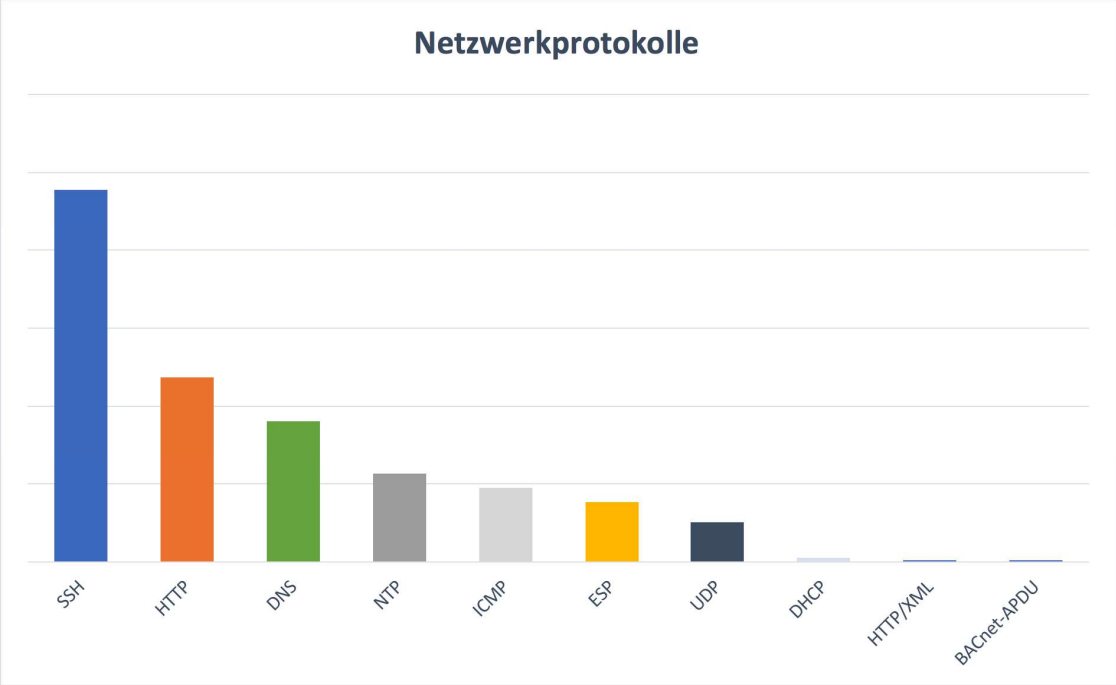


Abbildung 5.3: Top10 der angewählten Netzwerkports

Zusätzlich konnten innerhalb des Test-Zeitraums vier Login-Versuche mit Standard-Login-Credentials festgestellt werden. Jeweils zwei Login-Versuche wurden von der selben IP-Adresse aus durchgeführt.

```
Login-Attempts:

"13793","2017-08-03 13:42:47.762433","178.209.51.227","55438","217.224.149.56","8041","HTTP","432","GET /snapshot.cgi?user=admin&pwd= HTTP/1.1 "
"13796","2017-08-03 13:42:47.773798","178.209.51.227","55441","217.224.149.56","8041","HTTP","437","GET /snapshot.cgi?user=admin&pwd=admin HTTP/1.1 "

"141069","2017-08-03 23:17:04.643370","189.206.78.125","53380","217.224.149.56","8041","HTTP","113","GET /snapshot.cgi?user=admin&pwd= HTTP/1.0 "
"141086","2017-08-03 23:17:05.310134","189.206.78.125","53384","217.224.149.56","8041","HTTP","113","GET /snapshot.cgi?user=admin&pwd=admin HTTP/1.0 "
```

Abbildung 5.4: Login-Versuche mit Standard-Login-Credentials

Die Angriffsversuche blieben aufgrund der geänderten Passwörter erfolglos. Ebenso ist die geringe Anzahl der Angriffe vermutlich auf die eingerichtete Passwortbarriere zurückzuführen. So lange noch viele Smart-Home-Systeme offen und ohne Schutz online verfügbar sind, ist es für Angreifer lukrativer offene Systeme anzugreifen. Es ist aber davon auszugehen, dass die Angriffe auf passwortgeschützte Smart-Home-Geräte zunehmen werden.

5.2 Testphase 2

Während der zweiten Testphase wurde die Haunted House Infrastruktur über einen Zeitraum von drei Wochen mit den Standardeinstellungen und -passwörtern des Herstellers betrieben. Im Anschluss wurden die Zugriffe und Zugriffsversuche analysiert und bewertet.

Folgende Erkenntnisse konnten gewonnen werden:
Insgesamt wurden 81.083 Zugriffsversuche von 22.348 unterschiedlichen IP-Adressen detektiert. Das entspricht täglich ca. 3.800 Zugriffsversuchen.

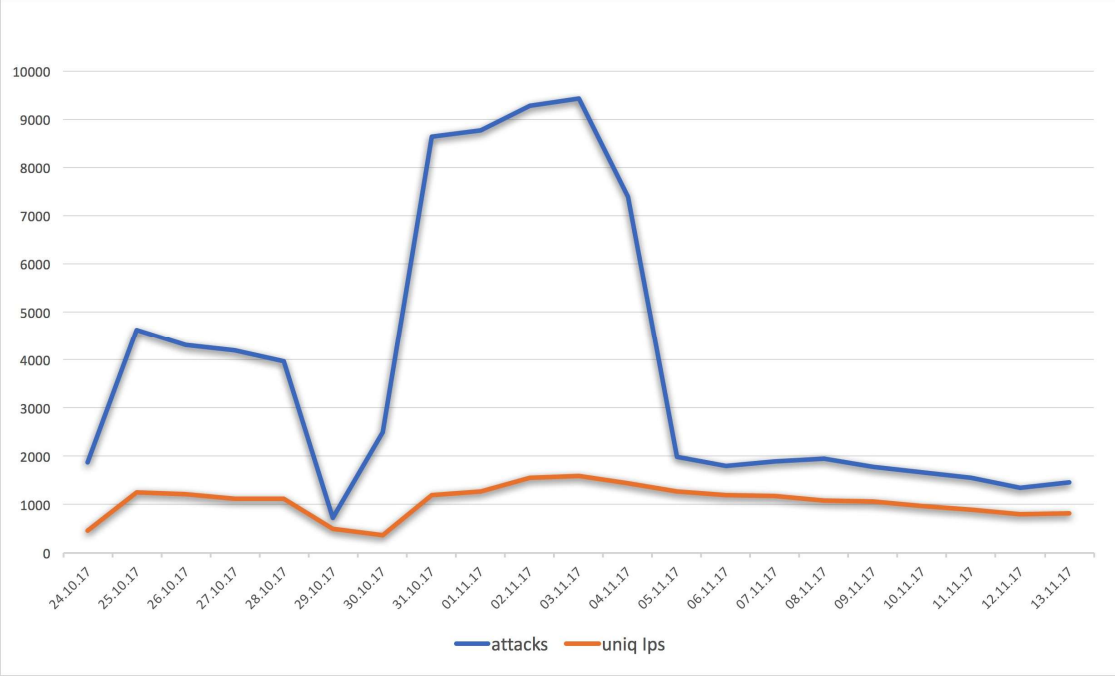


Abbildung 5.5: Zugriffsversuche pro Tag

Aus fast jedem Land der Welt wurde im Versuchszeitraum mindestens einmal versucht eine Komponente anzusprechen.

Folgende Grafik zeigt die Top 10 Länder nach Zugriffsversuchen auf:

Abbildung 5.6: Weltkarte mit den Top 10 der Länder aus denen Zugriffe erfolgt sind

Die hier dargestellten Länder repräsentieren nur die letzte auflösbare IP-Adresse des Zugriffs. Der tatsächliche Standort des Zugreifenden kann gegebenenfalls davon abweichen.

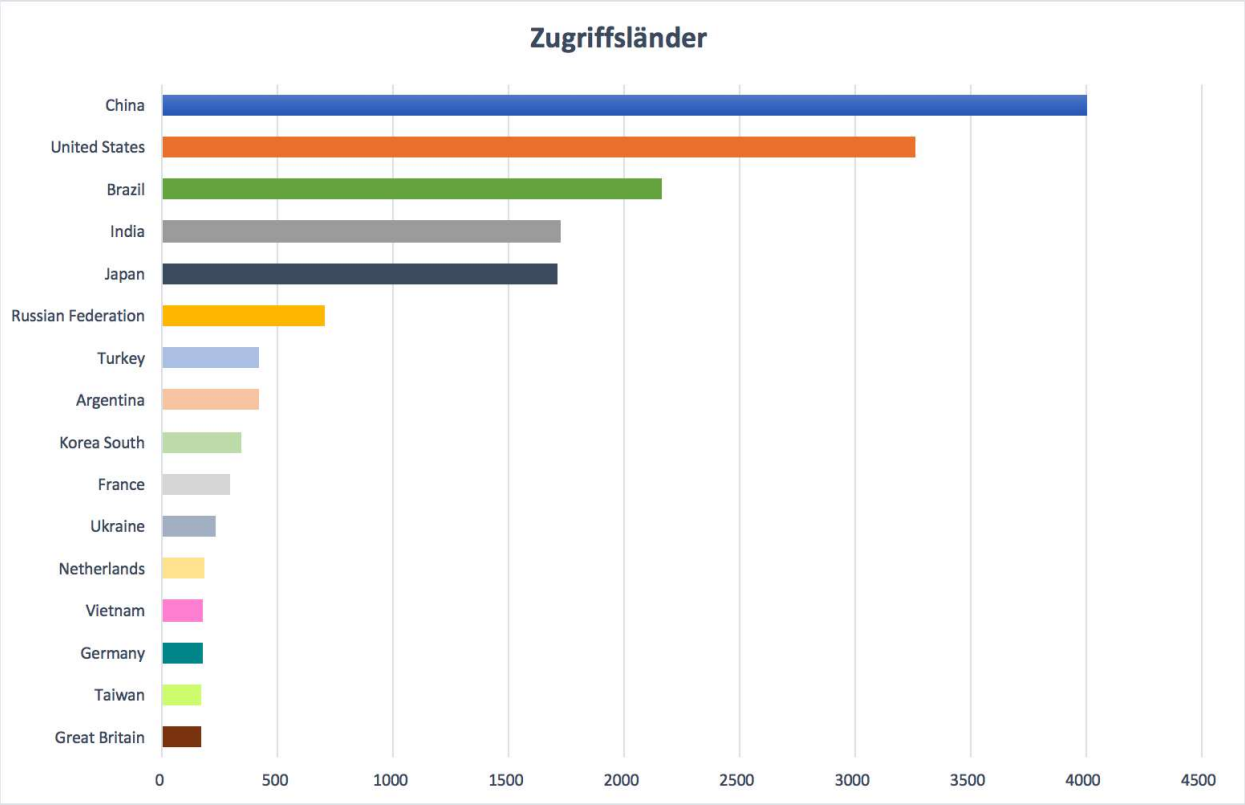


Abbildung 5.7: Länder aus denen die Zugriffe erfolgten

Im Haunted House wurden mehrere Komponenten betrieben, die alle über einen Router mit dem Internet verbunden sind. Daher konnten nicht bei allen Komponenten die Standardports weitergeleitet werden. In Folge dessen kann die Verteilung der Zugriffsversuche im Testaufbau verzerrt sein. Die Zugriffsversuche erfolgten dabei über verschiedene Netzwerkports. Durch eine genauere Analyse der Zugriffsversuche konnte festgestellt werden, dass ein Großteil aller Zugriffe automatisiert, in Form von Wörterbuchattacken, durchgeführt wurden.

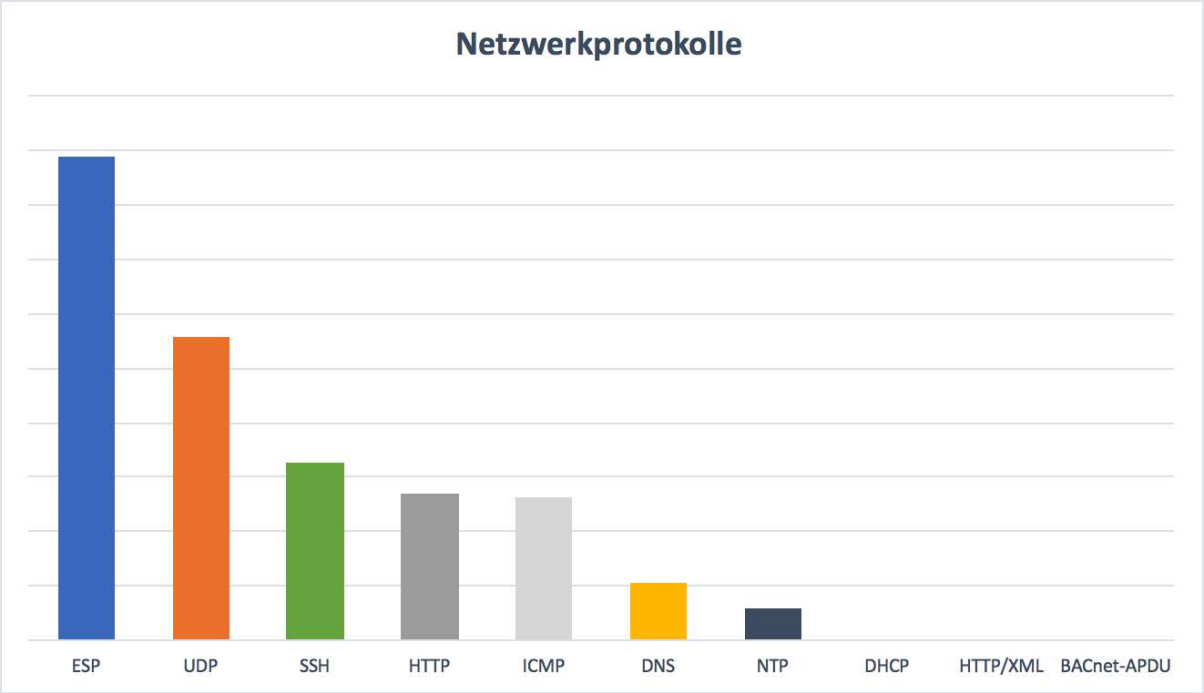
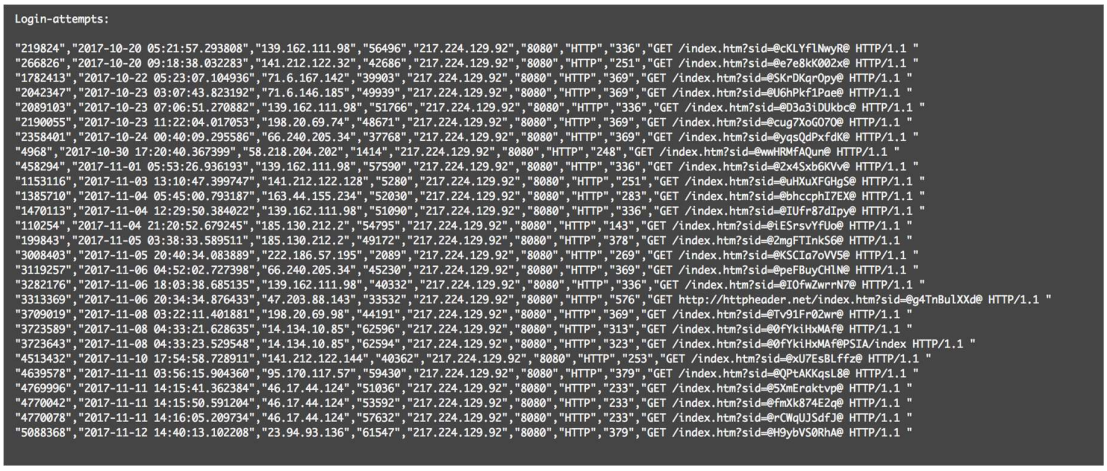


Abbildung 5.8: Top10 der angewählten Netzwerkports

Innerhalb des Test-Zeitraums konnten zusätzlich 27 Zugriffe identifiziert werden. Da die Systeme mit den Standardeinstellungen betrieben wurden, war es den Angreifern möglich, sich ohne Authentifizierung mit vollen Rechten auf der Anlage umzusehen und Veränderungen durchzuführen.



```
Login-attempts:

"219824","2017-10-20 05:21:57.293808","139.162.111.98","56496","217.224.129.92","8080","HTTP","336","GET /index.htm?sid=@cKLYflNwyR@ HTTP/1.1 "
"266826","2017-10-20 09:18:38.032283","141.212.122.32","42686","217.224.129.92","8080","HTTP","251","GET /index.htm?sid=@e7e8kK002x@ HTTP/1.1 "
"1782413","2017-10-22 05:23:07.104936","71.6.167.142","39903","217.224.129.92","8080","HTTP","369","GET /index.htm?sid=@SKrDKqrQpy@ HTTP/1.1 "
"2042347","2017-10-23 03:07:43.823192","71.6.146.185","49939","217.224.129.92","8080","HTTP","369","GET /index.htm?sid=@UGhPkf1Pae@ HTTP/1.1 "
"2089103","2017-10-23 07:06:51.270882","139.162.111.98","51766","217.224.129.92","8080","HTTP","336","GET /index.htm?sid=@D3a3iDUkbc@ HTTP/1.1 "
"2190055","2017-10-23 11:22:04.017053","198.20.69.74","48671","217.224.129.92","8080","HTTP","369","GET /index.htm?sid=@cug7XoGO7O@ HTTP/1.1 "
"2358401","2017-10-24 00:40:09.295586","66.240.205.34","37768","217.224.129.92","8080","HTTP","369","GET /index.htm?sid=@yqsQdPxfdK@ HTTP/1.1 "
"4968","2017-10-30 17:20:40.367399","58.218.204.202","1414","217.224.129.92","8080","HTTP","248","GET /index.htm?sid=@wwHRMfAQun@ HTTP/1.1 "
"458294","2017-11-01 05:53:26.936193","139.162.111.98","57590","217.224.129.92","8080","HTTP","336","GET /index.htm?sid=@2x4SxbGKVv@ HTTP/1.1 "
"1153116","2017-11-03 13:10:47.399747","141.212.122.128","5280","217.224.129.92","8080","HTTP","251","GET /index.htm?sid=@uHXuXFGHgS@ HTTP/1.1 "
"1385710","2017-11-04 05:45:00.793187","163.44.155.234","52030","217.224.129.92","8080","HTTP","283","GET /index.htm?sid=@bhccphI7EX@ HTTP/1.1 "
"1470113","2017-11-04 12:29:50.384022","139.162.111.98","51090","217.224.129.92","8080","HTTP","336","GET /index.htm?sid=@IUfr87dIpy@ HTTP/1.1 "
"110254","2017-11-04 21:20:52.679245","185.130.212.2","54795","217.224.129.92","8080","HTTP","143","GET /index.htm?sid=@iESrsvYfUo@ HTTP/1.1 "
"199843","2017-11-05 03:38:33.589511","185.130.212.2","49172","217.224.129.92","8080","HTTP","378","GET /index.htm?sid=@ZmgFTInkS6@ HTTP/1.1 "
"3008403","2017-11-05 20:40:34.083889","222.186.57.195","2089","217.224.129.92","8080","HTTP","269","GET /index.htm?sid=@KSCIa7oVV5@ HTTP/1.1 "
"3119257","2017-11-06 04:52:02.727398","66.240.205.34","45230","217.224.129.92","8080","HTTP","369","GET /index.htm?sid=@peFBuyChlN@ HTTP/1.1 "
"3282176","2017-11-06 18:03:38.685135","139.162.111.98","40332","217.224.129.92","8080","HTTP","336","GET /index.htm?sid=@IOfwZwrrN7@ HTTP/1.1 "
"3313369","2017-11-06 20:34:34.876433","47.203.88.143","33532","217.224.129.92","8080","HTTP","576","GET http://httpheader.net/index.htm?sid=@g4TnBulXXd@ HTTP/1.1 "
"3709019","2017-11-08 03:22:11.401881","198.20.69.98","44191","217.224.129.92","8080","HTTP","369","GET /index.htm?sid=@Tv91Fr02wr@ HTTP/1.1 "
"3723589","2017-11-08 04:33:21.628635","14.134.10.85","62596","217.224.129.92","8080","HTTP","313","GET /index.htm?sid=@0fYkiHxMAf@ HTTP/1.1 "
"3723643","2017-11-08 04:33:23.529548","14.134.10.85","62594","217.224.129.92","8080","HTTP","323","GET /index.htm?sid=@0fYkiHxMAf@PSIA/index HTTP/1.1 "
"4513432","2017-11-10 17:54:58.728911","141.212.122.144","40362","217.224.129.92","8080","HTTP","253","GET /index.htm?sid=@xU7EsBLffz@ HTTP/1.1 "
"4639578","2017-11-11 03:56:15.904360","95.170.117.57","59430","217.224.129.92","8080","HTTP","379","GET /index.htm?sid=@QPtAKKqsL8@ HTTP/1.1 "
"4769996","2017-11-11 14:15:41.362384","46.17.44.124","51036","217.224.129.92","8080","HTTP","233","GET /index.htm?sid=@SXmEraktvp@ HTTP/1.1 "
"4770042","2017-11-11 14:15:50.591204","46.17.44.124","53592","217.224.129.92","8080","HTTP","233","GET /index.htm?sid=@fmXk874E2q@ HTTP/1.1 "
"4770078","2017-11-11 14:16:05.209734","46.17.44.124","57632","217.224.129.92","8080","HTTP","233","GET /index.htm?sid=@rCWqUJSdfJ@ HTTP/1.1 "
"5088368","2017-11-12 14:40:13.102208","23.94.93.136","61547","217.224.129.92","8080","HTTP","379","GET /index.htm?sid=@H9ybVS0RhA@ HTTP/1.1 "
```

Abbildung 5.9: Angriffsversuch auf das Steuerungssystem

An dem System wurde von keinem der Angreifer Veränderungen durchgeführt.

Angriffsversuche auf weitere Smart-Home-Geräte konnten während dieser Testphase nicht identifiziert werden. Automatisierte Angriffsversuche konzentrieren sich momentan noch vorwiegend auf komplett ungesicherte Systeme. Die Wahrscheinlichkeit für Angriffe steigt, je länger ein System ungesichert bzw. unzureichend gesichert am Internet ist.

5.3 Analyse

Die Verteilung der Zugriffe aus den einzelnen Ländern sind in der ersten und zweiten Testphase relativ konstant geblieben. Einen deutlichen Ausreißer gibt es jedoch. In der ersten Testphase lag Mexico an Platz drei der Ursprungsländer. In der zweiten Testphase erscheint es aber nicht mehr in den Top 10. Umgekehrt liegt Japan während der ersten Testphase außerhalb der Top 10, kommt für die zweite Testphase auf Platz 5 der Länder aus denen die meisten Zugriffe erfolgten. Da es bei den übrigen Platzierungen nur geringe Verschiebungen gegeben hat, fällt dieser Wechsel besonders stark auf.

Im 2. Testlauf ist eine deutliche Spitze bei den Zugriffen in der Zeit vom 31.10. - 05.11. zu erkennen. Da einige Angreifer sich mit den Systemen verbunden haben, konnten sie nicht nur auf die Startseiten zugreifen, sondern auch die Unterseiten scannen und auf Schwachstellen untersuchen. Nachdem alle Seiten der Systeme erfasst wurden, wurde nur geprüft, ob die Seiten noch verfügbar sind. Daher fallen die Zugriffsversuche zum Ende hin wieder ab.

Entsprechend liegen die durchschnittlichen täglichen Zugriffsversuche in der zweiten Testphase mit ca. 3.800 auch deutlich über den ca. 1.500 aus der ersten Phase.

Zugriffe aus dem Darknet konnten keine identifiziert werden. Hierzu wurden die IP-Adressen der Zugriffsversuche mit veröffentlichten IP-Adressen der Exit-Nodes abgeglichen. Dies ergab keine Treffer.

Werden die Smart-Home-Systeme mit Standard-Passwörtern betrieben oder gar mit Auto-Login, ist die Wahrscheinlichkeit sehr groß, dass sich innerhalb weniger Tage erste ungebetene Gäste im System umschauen. Bei 27 Angriffen in drei Wochen während der zweiten Testphase ist das im Durchschnitt mehr als ein Angriff pro Tag.

6 Empfehlungen

Bereits kleine Maßnahmen können helfen, das Auffinden von und den unerlaubten Zugriff auf Smart-Home-Geräte über das Internet zu verhindern. Neben der grundlegenden Planung zum Layout und der Konfiguration von Smart-Home-Systemen, ist es insbesondere das Management von Nutzernamen und Passwörtern, das mit geringem Aufwand erhebliche Sicherheits-Verbesserungen ermöglicht.

Nutzernamen und Passwörter

- Alle Standardzugangsdaten bei der Inbetriebnahme ändern.
- Sichere Passwörter verwenden.
- Wiederverwenden von Passwörtern vermeiden.
- Nicht benötigte Benutzerkonten deaktivieren.
- Wenn möglich Zwei-Faktor-Authentifikation verwenden.

TIPP: Passwort-Manager verwenden, um sichere Passwörter zu erzeugen und zu verwalten.

Netzwerkplanung

- Einrichten von mehreren abgeschotteten Netzwerksegmenten. (z.B. Gast-WLAN, Home-Office-WLAN, Gebäudetechnik-WLAN)
- Einrichten einer Firewall, um Kommunikation zwischen den Netzen zu kontrollieren.
- Portforwarding deaktivieren, stattdessen VPN-Verbindungen nutzen, um eigene Fernzugriffe aus dem Internet zu ermöglichen.
- Nicht benötigte Dienste (z.B. UPnP) deaktivieren.

Außerdem bieten die OWASP TOP 10 IoT ein fundiertes Gerüst der häufigsten Schwachstellen und Fehler. Daraus abgeleitet bieten die nachfolgenden Fragen eine gute Basis für eine tiefer gehende Beschäftigung mit dem Thema.

Unsicheres Webinterface

- Verhindert das Webinterface die Nutzung von schwachen Passwörtern?
- Wird der Zugang nach wiederholter Eingabe von falschen Zugangsdaten gesperrt?
- Werden Informationen nur gesichert über HTTPS übertragen?
- Ist das Webinterface auf XSS, SQL-Injections und CSRF Schwachstellen getestet worden?

Fehlende Transportverschlüsselung

- Wie ist die Kommunikation zwischen den Geräten untereinander und zum Internet gesichert?
- Werden allgemein anerkannte Verschlüsselungsstandards genutzt und keine proprietären Lösungen verwendet?
- Ist eine Firewall-Option vorhanden?

Unzureichende Konfigurationsmöglichkeiten

- Gibt es Optionen um Anforderungen an Passwörter einzurichten?
- Welche Möglichkeiten gibt es, die Verschlüsselung zu konfigurieren?
- Werden sicherheitsrelevante Vorgänge in einem Log-File protokolliert?
- Kann eine automatische Benachrichtigung bei Sicherheitsvorfällen konfiguriert werden?

Unzureichende Authentifikation/Autorisierung

- Können starke Passwörter erzwungen werden?
- Kann Zwei-Faktor-Authentifikation verwendet werden?
- Wie ist der Passwort-Wiederherstellungsmechanismus implementiert?
- Müssen die Standardzugangsdaten (Nutzer und Passwort) während des Setup-Prozesses geändert werden?
- Kann ein Ablaufdatum für Zugangsdaten konfiguriert werden?

Unsichere Cloud Anbindung

- Verhindert das Cloudinterface die Nutzung von schwachen Passwörtern?
- Kann Zwei-Faktor-Authentifikation verwendet werden?
- Ist das Cloudinterface auf XSS, SQL-Injections und CSRF Schwachstellen getestet worden?
- Werden Informationen nur gesichert über HTTPS übertragen?
- Wird der Zugang nach wiederholter Eingabe von falschen Zugangsdaten gesperrt?
- Wie ist der Passwort-Wiederherstellungsmechanismus implementiert?

Unsicheres mobiles Interface

- Verhindert das Cloudinterface die Nutzung von schwachen Passwörtern?
- Kann Zwei-Faktor-Authentifikation verwendet werden?
- Werden Informationen nur gesichert über HTTPS übertragen?
- Wird der Zugang nach wiederholter Eingabe von falschen Zugangsdaten gesperrt?
- Wie viele persönlich Daten werden abgefragt und gesammelt?

Datenschutz

- Wie viele persönlich Daten werden abgefragt und gesammelt?
- Kann der Nutzer das Sammeln von Daten konfigurieren?
- Werden die gesammelten Daten geschützt übertragen und verschlüsselt gespeichert?
- Werden die gesammelten Daten anonymisiert gespeichert?
- Werden die gesammelten Daten an Dritte weitergegeben?

Unsichere Software/Firmware

- Können die Geräte Softwareupdates erhalten?
- Werden Softwareupdates, nachdem Schwachstellen entdeckt wurden, zeitnah durch den Hersteller bereitgestellt?
- Werden Softwareupdates verschlüsselt übertragen und signiert, um die Integrität validieren zu können?

Unsichere Schnittstellen

- Verfügt das Gerät nur über die notwendigen externen Schnittstellen und kann nicht über z.B. einen unnötigen USB-Port angesprochen werden?
- Ist das Gerät gegen Buffer Overflow, Fuzzing und Denial of Service Angriffe gesichert?
- Wurden alle Netzwerk-Ports, die nicht benötigt werden, geschlossen?
- Werden Netzwerk-Ports durch UPnP geöffnet?