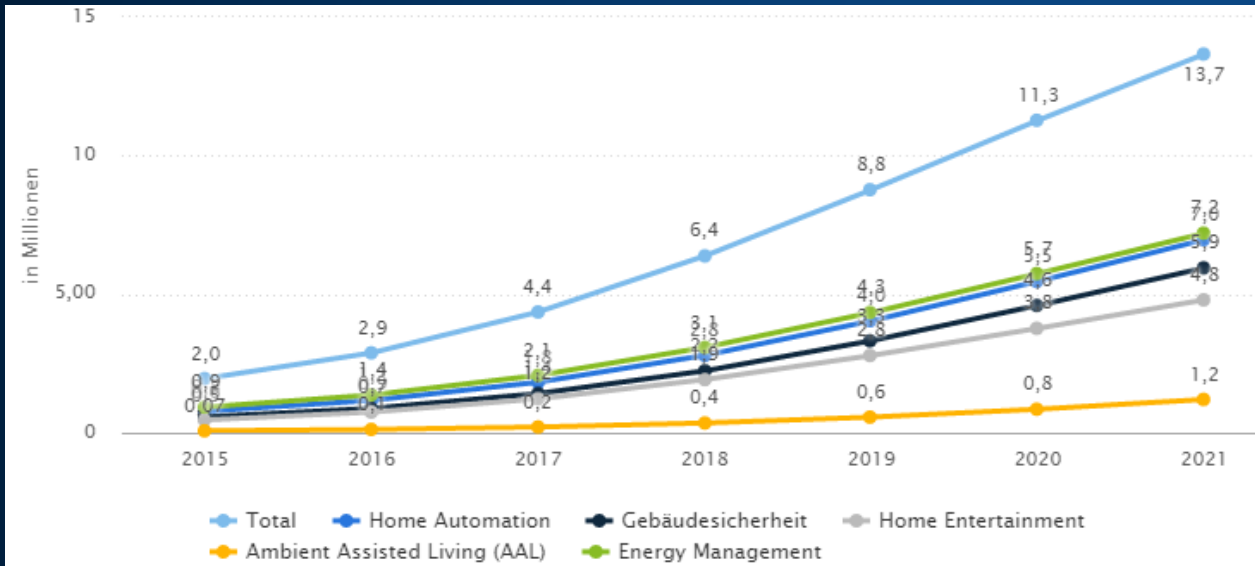




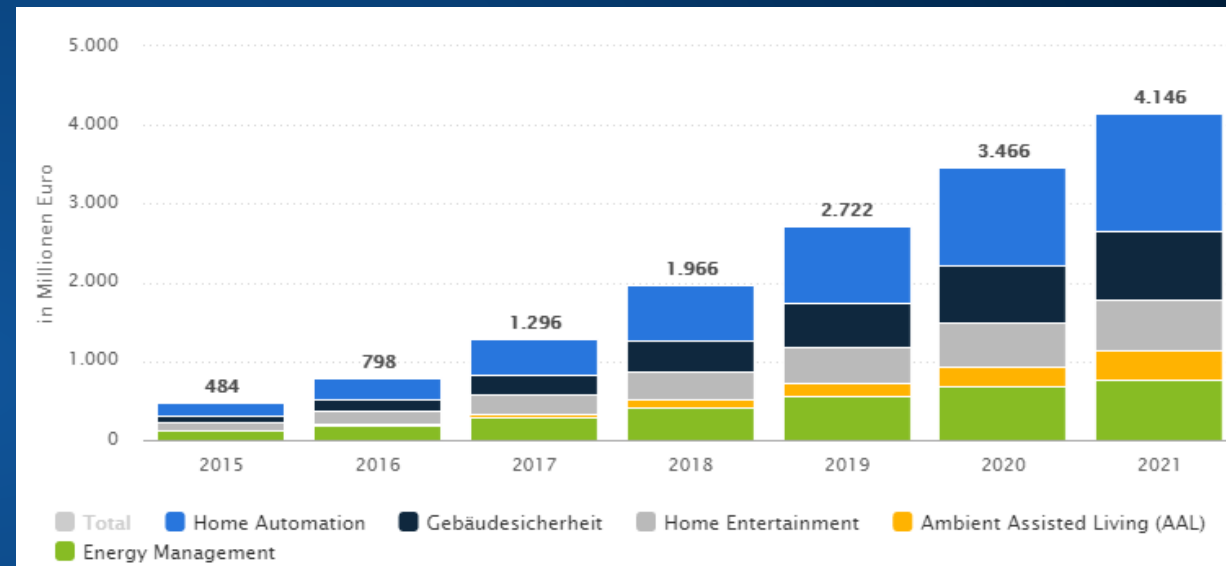
# IT-Sicherheit im Privathaushalt

SOPHOS

# Der Wohntrend Nummer Eins: SmartHome



Die Anzahl der Haushalte mit Smart Homes wird 2021 laut Prognose 13,7 Mio. betragen.



Der Umsatz im Smart Home Markt wird für 2021 auf etwa 1,3 Mrd. € geschätzt.

Quelle: Statista

# Sicherheit im SmartHome?

SOPHOS

# Warum sind IoT-Geräte oft unsicher?

- Viele IoT-Geräte bekommen selten oder nie Sicherheitsupdates
- Einfache Bedienung
- Auslieferung mit Standardpasswörtern
- Kurze Produktlebenszyklen
- Sicherheit ist oft nachträglich hinzugefügt
- Sicherheit ist oft ein Nebenprodukt
  - Keine oder Standardpasswörter
  - Portweiterleitung
  - UPNP aktiv

**WPA2: Forscher entdecken Schwachstelle in WLAN-Verschlüsselung**

16.10.2017 11:02 Uhr - Dennis Schirmmacher vorlesen



Sicherheitsforscher haben offenbar kritische Lücken im Sicherheitsstandard WPA2 entdeckt. Sie geben an, dass sich so Verbindungen belauschen lassen.

Mehrere Sicherheitslücken bedrohen den Sicherheitsstandard WPA2, der WLAN-Verbindungen absichert und Lauscher aussperrt. Mittels der KRACK getauften Attacke sollen Angreifer WPA2 aufbrechen, belauschen und manipulieren können, warnen diverse Sicherheitsforscher. Das geht aus [verschiedenen Medienberichten](#) hervor.

Bluetooth-Pairing-Codes



# Beispiel: Shodan

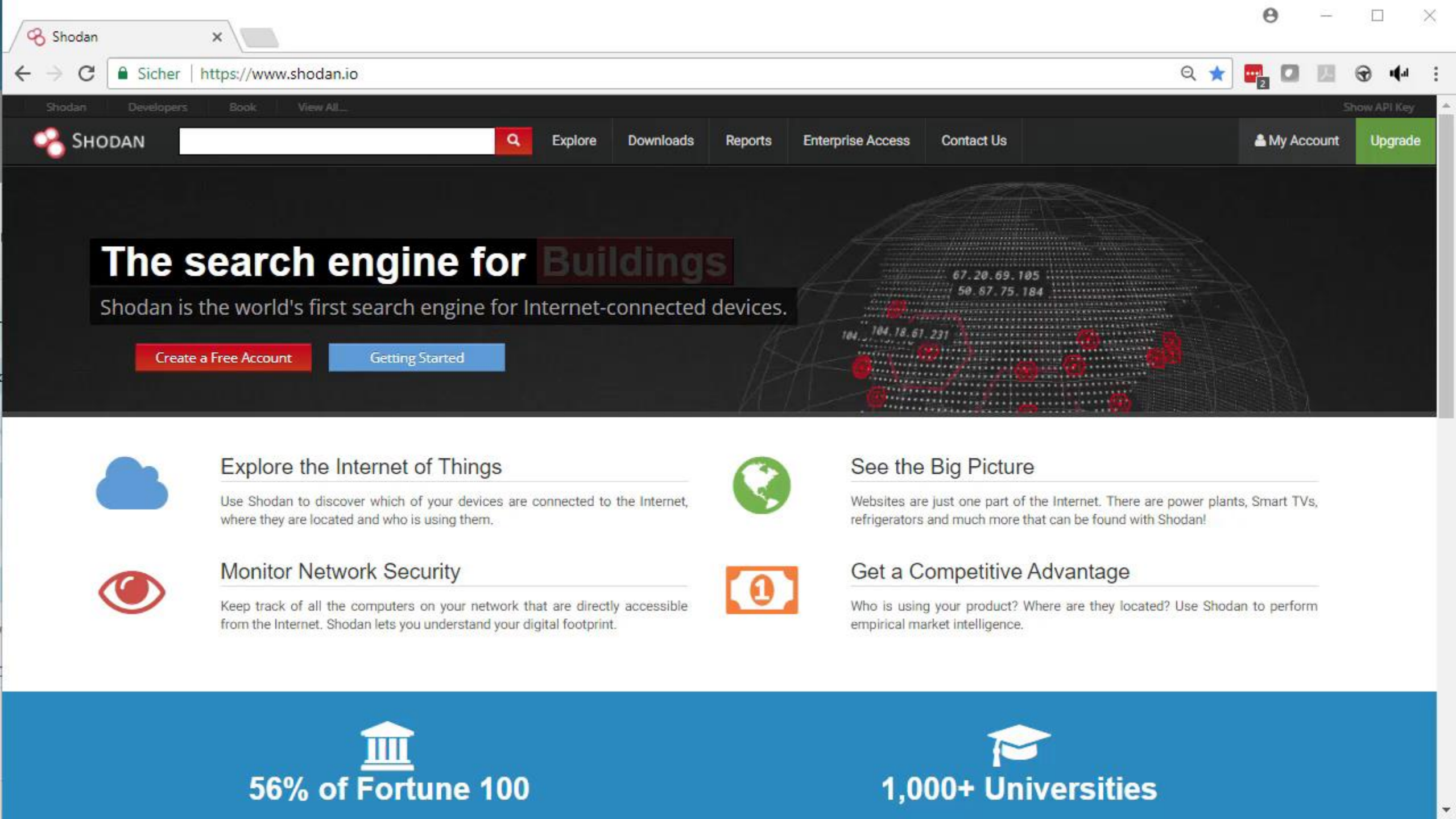
The image shows a Shodan search interface with a search query for Germany and a preview of a webcamXP 5 server interface.

**SHODAN Search Results:**

- Search query: `country:"DE"`
- Navigation: Exploits, Maps, Images, Share Search, Download Results
- TOP COUNTRIES: Germany (26,351,627)
- TOP CITIES:
  - Berlin: 807,172
  - Frankfurt: 405,001
  - Munich: 337,403
  - Hamburg: 333,680
  - Frankfurt Am Main: 185,307
- TOP SERVICES:
  - SIP: 9,218,002
  - Splunk: 4,911,872
  - HTTPS: 2,654,420
  - HTTP: 1,836,653
  - SSH: 855,507

**WebcamXP 5 Server Interface:**

- Page title: **WEBCAMXP 5** - WEBCAMS AND IP CAMERAS SERVER FOR WINDOWS
- Navigation: Home, Multi view, Smartphone, Gallery, Administration
- Status: Not logged in
- Resolution: 320x240
- Two camera feeds are visible:
  - Left feed: Indoor scene with a large potted plant and a white wall.
  - Right feed: Close-up of an orange sofa.
- Footer: POWERED BY WEBCAMXP 5 V5.9.5.0



# The search engine for Buildings

Shodan is the world's first search engine for Internet-connected devices.

Create a Free Account

Getting Started



## Explore the Internet of Things

Use Shodan to discover which of your devices are connected to the Internet, where they are located and who is using them.



## See the Big Picture

Websites are just one part of the Internet. There are power plants, Smart TVs, refrigerators and much more that can be found with Shodan!



## Monitor Network Security

Keep track of all the computers on your network that are directly accessible from the Internet. Shodan lets you understand your digital footprint.



## Get a Competitive Advantage

Who is using your product? Where are they located? Use Shodan to perform empirical market intelligence.



56% of Fortune 100



1,000+ Universities

# Beispiel: Shodan

Shodan Developers Book View All...

SHODAN HTTP-Server v2.0

Exploits Maps Share Search Download Results

TOTAL RESULTS  
**3,703**

TOP COUNTRIES

Germany	3,029
Austria	365
Switzerland	112
Spain	32
Netherlands	27

TOP SERVICES

HTTP (8181)	2,210
HTTP	513
HTTP S	235
Udpxy	197
8081	100

TOP ORGANIZATIONS

Deutsche Telekom AG	1,930
Vodafone DSL	262
Telekom Austria	244
O2 Deutschland	142
Vodafone Kabel Deutschland	125

HomeMatic WebUI

18181/pages/index.htm?sid=@PPA92JAsVk@&client=3

Admin  
Startseite > Status und Bedienung > Räume

Alarmmeldungen (0) Abmelden  
Servicemeldungen (1)

Startseite Status und Bedienung Programme und Verknüpfungen Einstellungen Geräte anlernen Hilfe

Name	Gewerk	Letzte Änderung	Control	
1-Küche				
1-WoZi-Garten-Tuerkontakt:1	Verschluss Batterie betrieben	02.06.2017 09:51:56		
1-Vorzimmer				
1-WoZi-Gartenstrom:1	Licht	21.05.2017 22:21:17	Aus	Ein
1-Wohnzimmer			Temperatur 23.5°C  4.5 °C 30.5 °C Auto Modus Boost Funktion Manu Modus Urlaubs Modus Aus Eco Temperatur Ein Comfort Temperatur	
2-Gäste-WC				
1-WoZi-Heizkoerper:4	Heizung 1-heiz_eg	13.06.2017 11:52:06		
3-Bad				
1-WoZi-Licht	Licht	31.05.2017 20:52:24		

# Beispiel: VNC Keyhole





# Beispiel: VNC Keyhole

The screenshot displays a VNC Keyhole interface for a technical control panel. The main window shows a complex piping system with various valves, pumps, and temperature sensors. A notification box at the top right states: "Jiný uživatel vzdáleně ovládá vaši pracovní plochu" (Another user is remotely controlling your workstation). A "Zadání" (Order) window is open in the bottom left, showing details for a customer order (Zakázka: 000000-000) dated 28.02.2016 06:31:10. The battery status overlay on the right shows a 42% charge for a SONNEN BATTERIE, with 11.2 kWh of Lithium Batterie capacity. It also displays power consumption: Erzeugung (0.0 kW), Aktueller Verbrauch (0.3 kW), and Momentaner Bezug (0.0 kW). The interface includes a "VNC KEYHOLE" logo in the bottom right corner.

Linka Nastavení Databáze

28.02.2016 0

Jiný uživatel vzdáleně ovládá vaši pracovní plochu  
Uživatel na počítači „as27458.net“ vzdáleně ovládá vaši pracovní plochu.

28.02.2016 06:39

SONNEN BATTERIE

42 %

Betriebsart  
Automatikbetrieb

11.2 kWh Lithium Batterie

Entladung 0.4 kW

Erzeugung 0.0 kW

Aktueller Verbrauch 0.3 kW

Momentaner Bezug 0.0 kW

Zadání

Tunel Vsádková pračka 1 Vsádková pračka 2

Zakázka  
000000-000

Datum a čas  
28.02.2016 06:31:10

Program

Váha

Směna Pracovník  
1 0

Zákazník

Oddělení

Sortiment

Datum expedice Poznámka  
26.02.2016

Rep.0 WErr.0[2583478] RErr.998958[2583478] CRCErr.0

VNC KEYHOLE

**Bedrohungen** können  
sich ausbreiten

**SOPHOS**

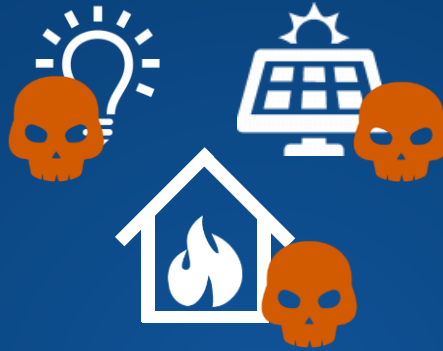
# Der Normalfall - alles in einem Netz



# Ein infiziertes Gerät reicht



Home Office



Licht- und  
Energiesteuerung



Sicherheitstechnik



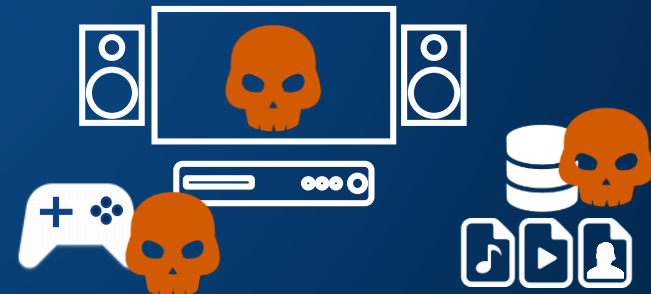
Internet-Router



Gäste-WLAN



Intelligente  
Haushaltsgeräte



Unterhaltungselektronik

# Hacker organisieren IoT-Geräte in Botnetzen

## Großstörung bei der Telekom: Angreifer nutzten Lücke und Botnetz-Code

29.11.2016 16:37 Uhr - Fabian A. Scherschel



Einen Tag nachdem bekannt wurde, dass die großflächige Störung bei der Telekom auf einen – größtenteils missglückten – Hackerangriff zurückzuführen ist, wird klarer, was passiert ist. Die Angreifer zielten mit Botnetz-Code auf eine Sicherheitslücke.

## Neues Botnetz über IoT-Geräte

22.10.2017 12:20 Uhr - Lutz Labs



IoT\_reaper oder IoTroop nennt sich ein neues Botnetz, das sich nach Angaben von Sicherheitsforschern seit September weit verbreitet hat. Die Spezialisten gehen von zwei Millionen Infektionen aus.

Ein Jahr nach dem [Botnetz Mirai](#) greift ein Verwandter um sich: Ein neues Botnetz soll Teile des Mirai-Quellcodes verwenden. Sicherheitsforscher nennen das neue Netz "IoT\_reaper" beziehungsweise "IoTroop". Es nimmt vornehmlich IoT-Geräte ins Visier: Überwachungskameras, NAS-Systeme sowie Videorecorder. Die Geräte stammen den Angaben zufolge vor allem von Netgear, D-Link, Linksys, GoAhead, JAWS, Vacron, AVTECH, MicroTik, TP-Link und Synology.

## Mac&i

7-Tage-News News-Archiv Livetick

News Tipps Artikel Forum Produkte Heft Archiv Abo

Mac & i > News > 2017 > KW 49 > Apples HomeKit: Schwachstelle erlaubte angeblich unerlaubten

## Apples HomeKit: Schwachstelle erlaubte angeblich unerlaubten Fernzugriff

08.12.2017 09:15 Uhr - Leo Becker



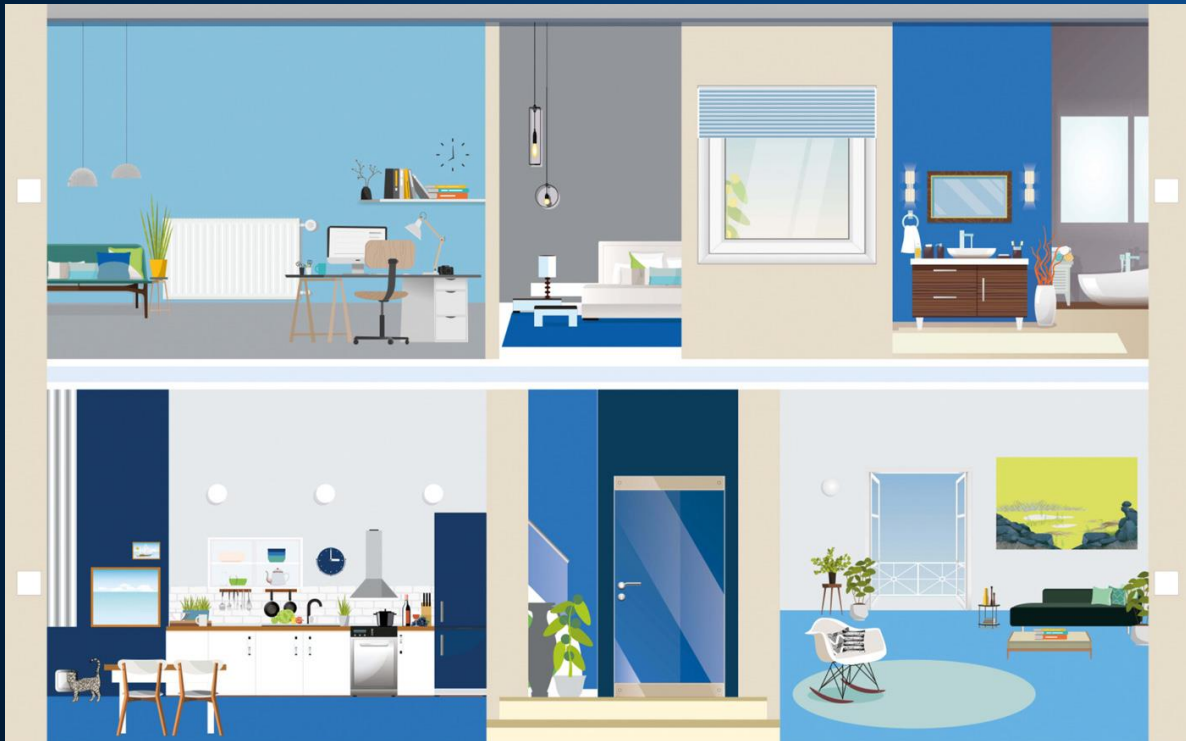
Die Steuerung der HomeKit-Geräte ist mit Apples vorinstallierter Home-App möglich – und per Siri. Für Automatisierung und Fernzugriff erfordern einen Home-Hub wie Apple TV. (Bild: Apple)

Mit Apples HomeKit vernetzte Smart-Home-Geräte – darunter auch Türschlösser – ließen sich einem Bericht zufolge von Unbefugten fernsteuern. Als Gegenmaßnahme hat Apple die Remote-Funktionalität für (berechtigte) Dritte abgedreht.

# Project Haunted House

SOPHOS

# PROJECT HAUNTED HOUSE



# Project Haunted House



## Teil 1 – „Honeypot SmartHome“

- Exponat 4x2,5m mit gängigen SmartHome-Komponenten
  - Nachbildung der Wohnbereiche Arbeitszimmer, Bad, Wohnzimmer, Küche, Eingangsbereich
  - Licht- und Heizungssteuerung, Türschlösser, Rollladensteuerung, Alarmierung, Rauchmelder, Kameras
  - Komponenten von KNX, BACnet, Loxone, HomeMatic, Philips, Amazon
  - Zentrale Steuerung und Vernetzung der SmartHome-Komponenten
- Das SmartHome wird als Honeypot ins Internet gestellt
  - Erreichbarkeit über Standard-Ports
  - Aktuelle Firmware, sichere Passwörter



# Project Haunted House



## Teil 2 – Scan nach Smarthome-Komponenten

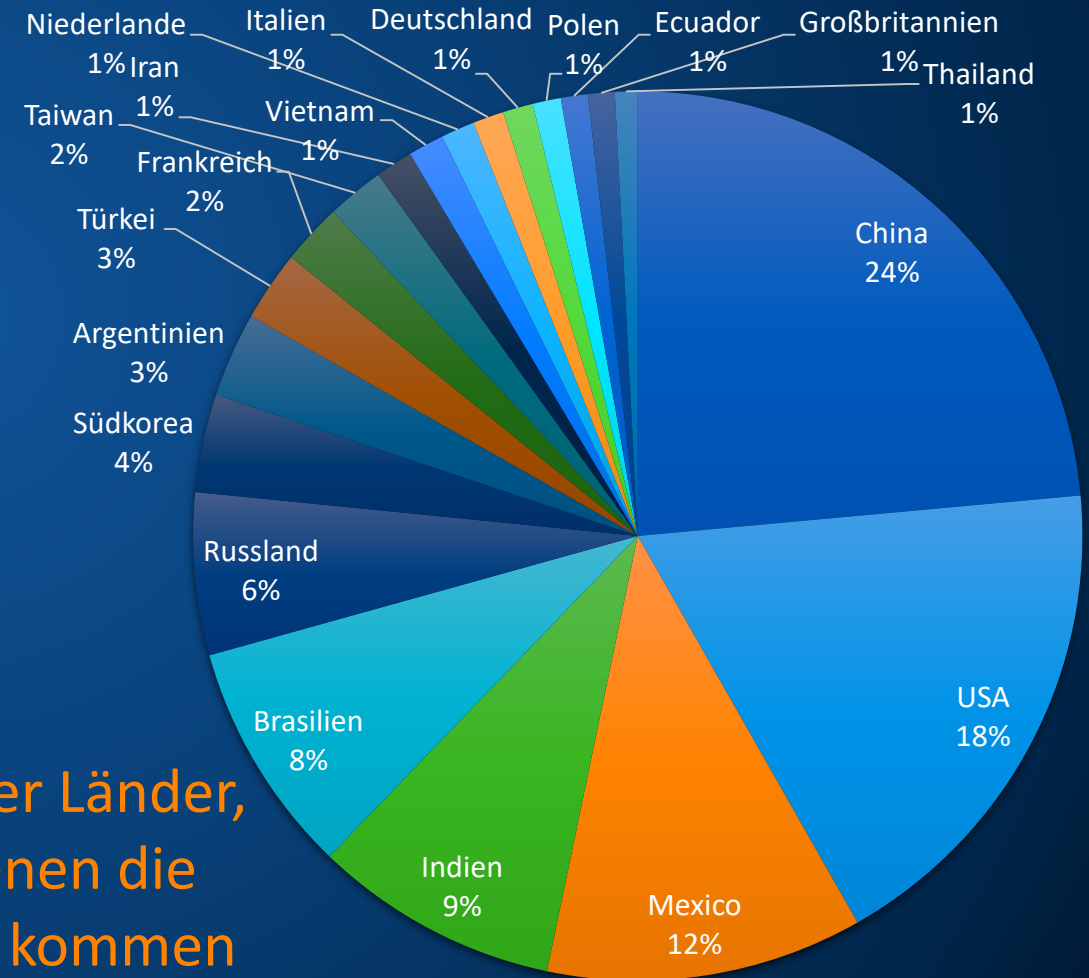
- Kontinuierlicher Scan des Internet nach erreichbaren SmartHome-Komponenten der am weitesten verbreiteten Hersteller
  - KNX
  - BACnet
  - Fox
  - Smart-Home Webserver wie z.B. Homematic, Loxone, OpenHAB usw.
- Aufbereitung der Ergebnisse in Heatmaps

# Erste Ergebnisse

## Honeypot SmartHome

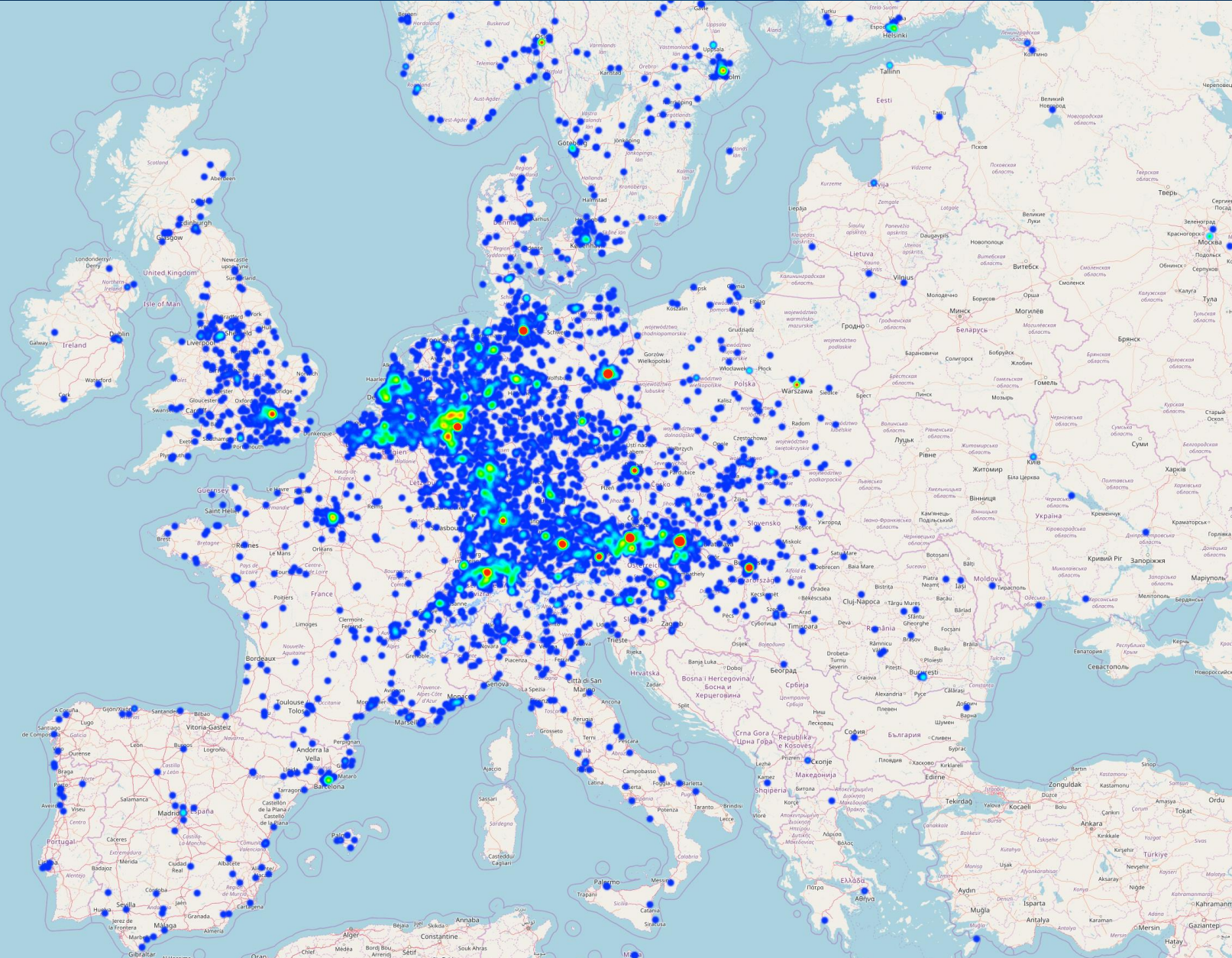
Nach dem Auftauchen in IoT-Suchmaschine „Shodan“

- Durchschnittlich 2.000 bis über 3.300 Zugriffe pro Tag
- Größtenteils automatisierte Anmeldeversuche mit Standardkennwörtern

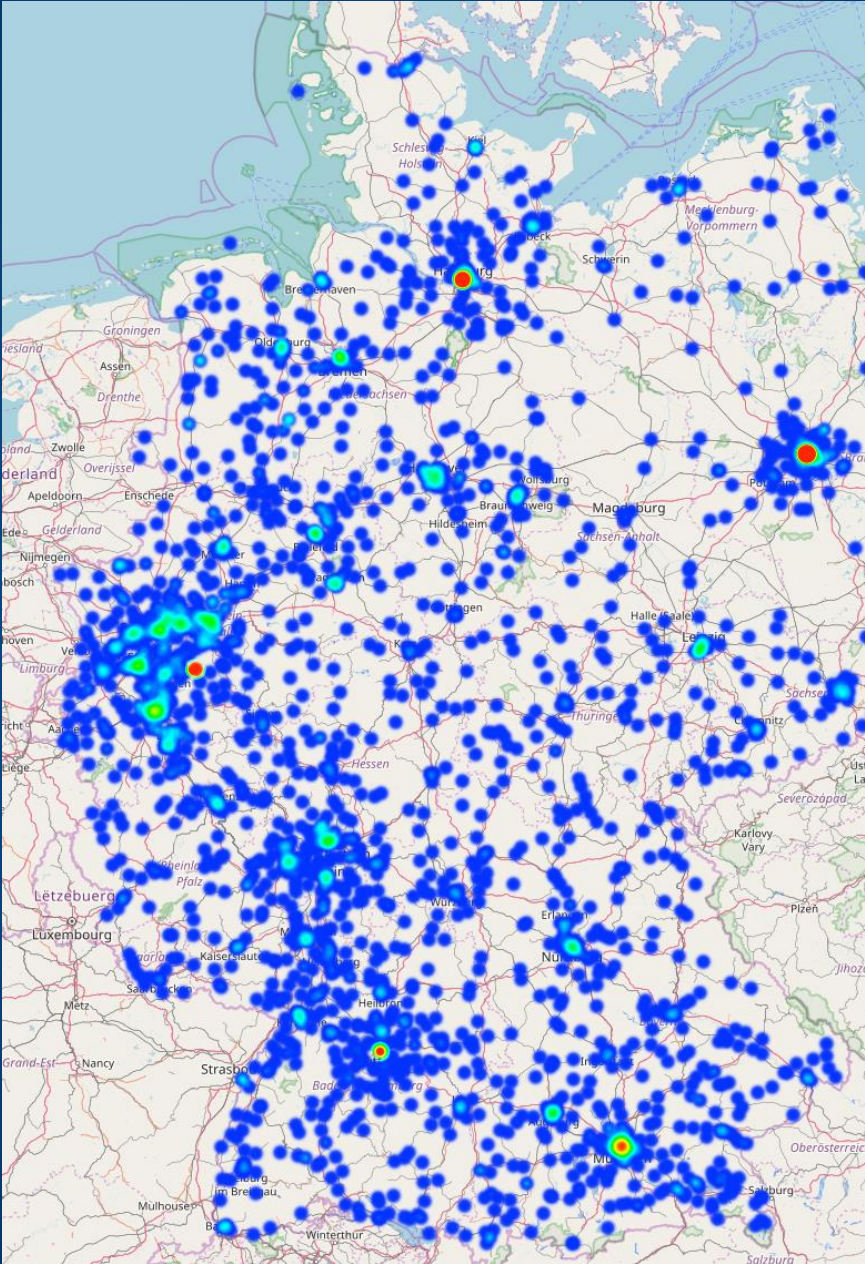


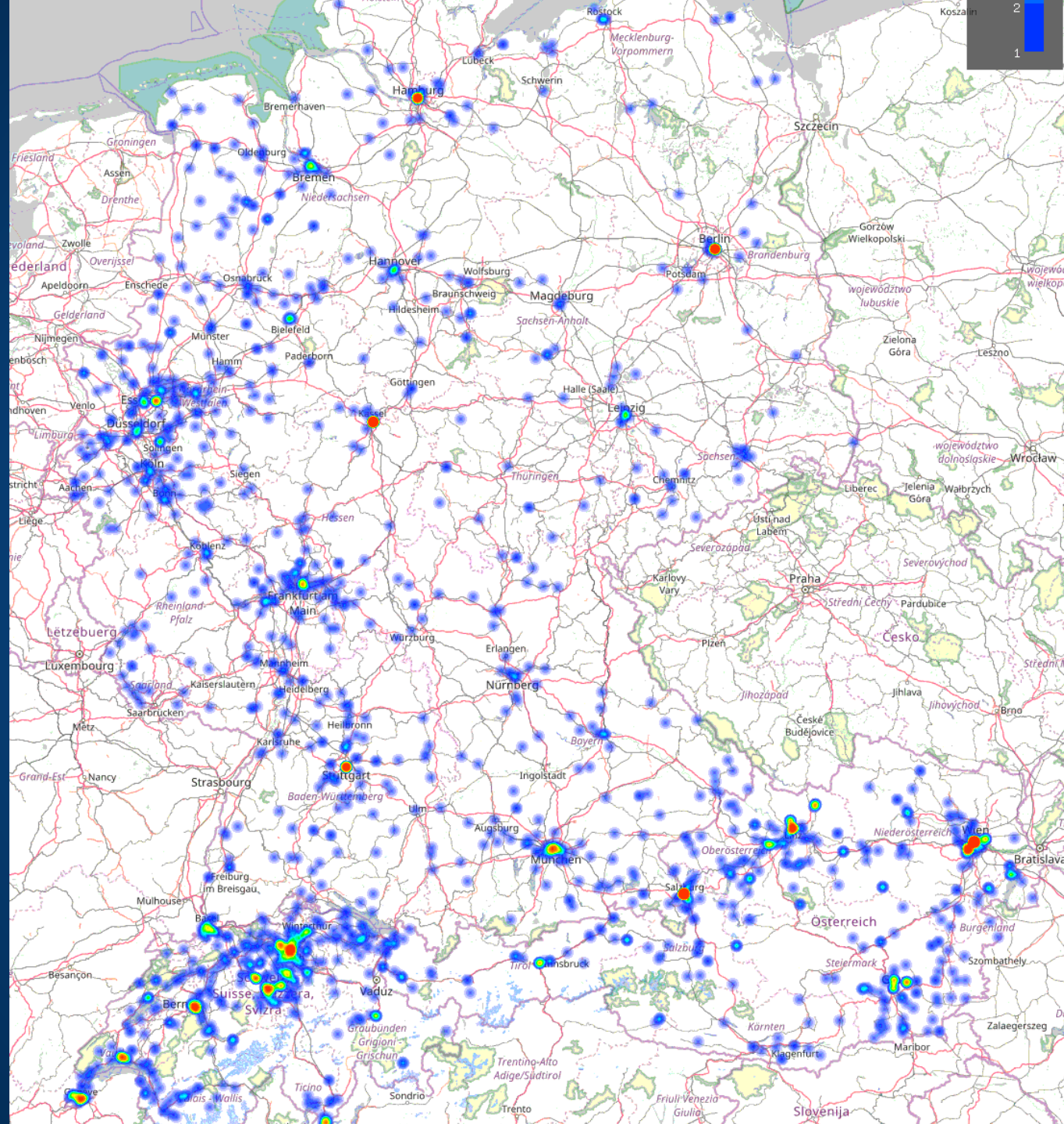
Top20 der Länder, aus denen die Zugriffe kommen

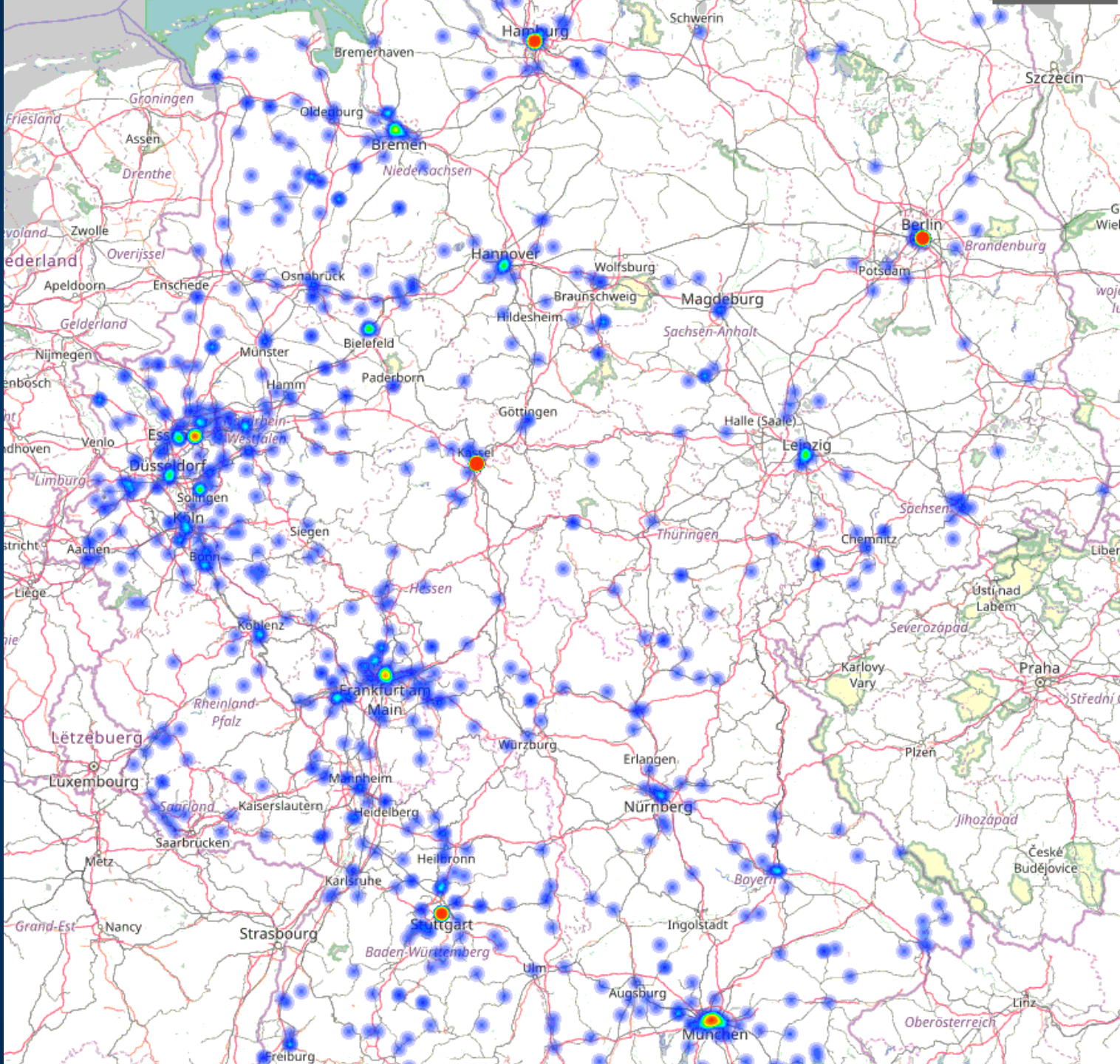
# Aus dem Internet erreichbare SmartHome Systeme von KNX, BACnet und Fox

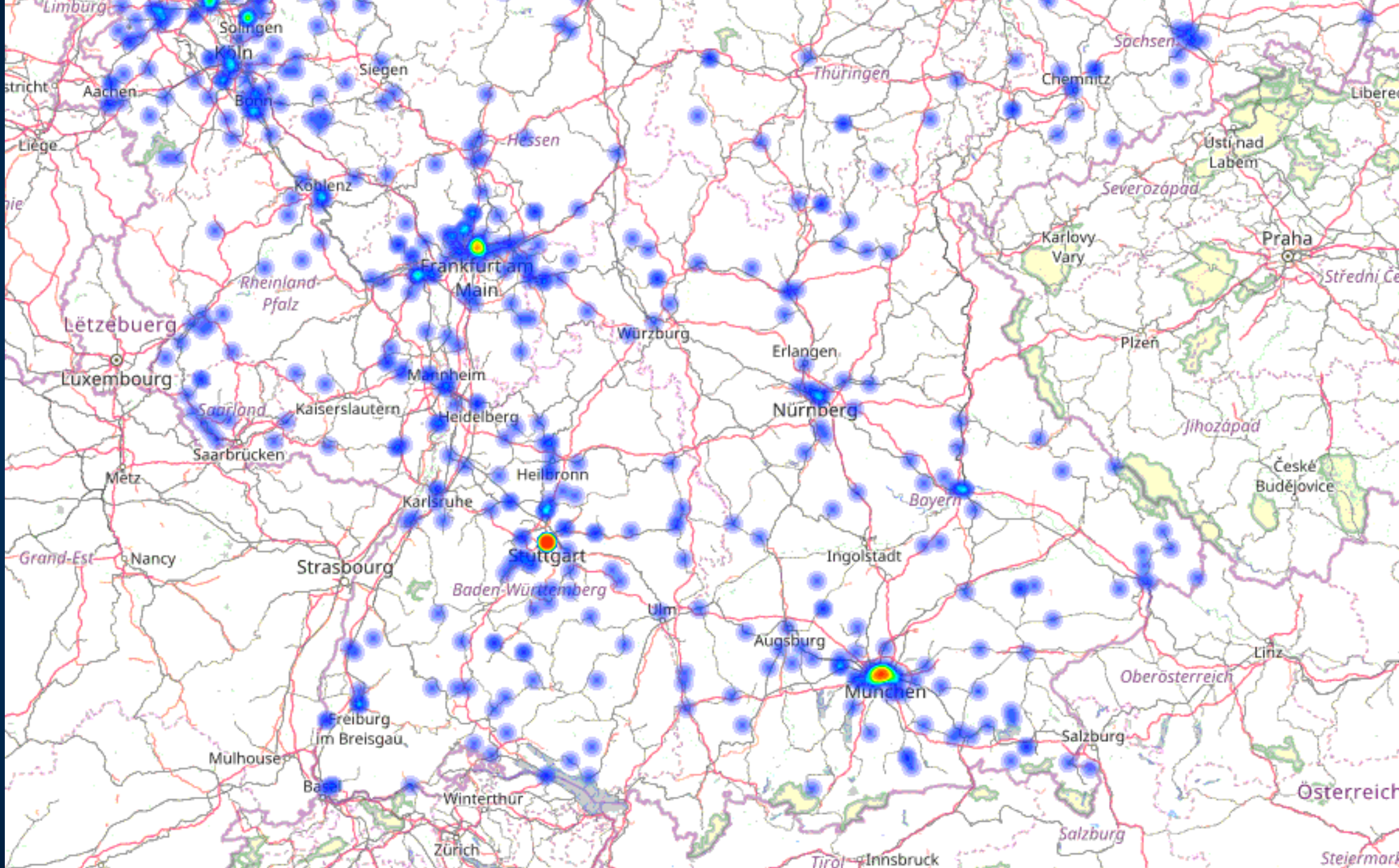


# Aus dem Internet erreichbare SmartHome Systeme von KNX, BACnet und Fox









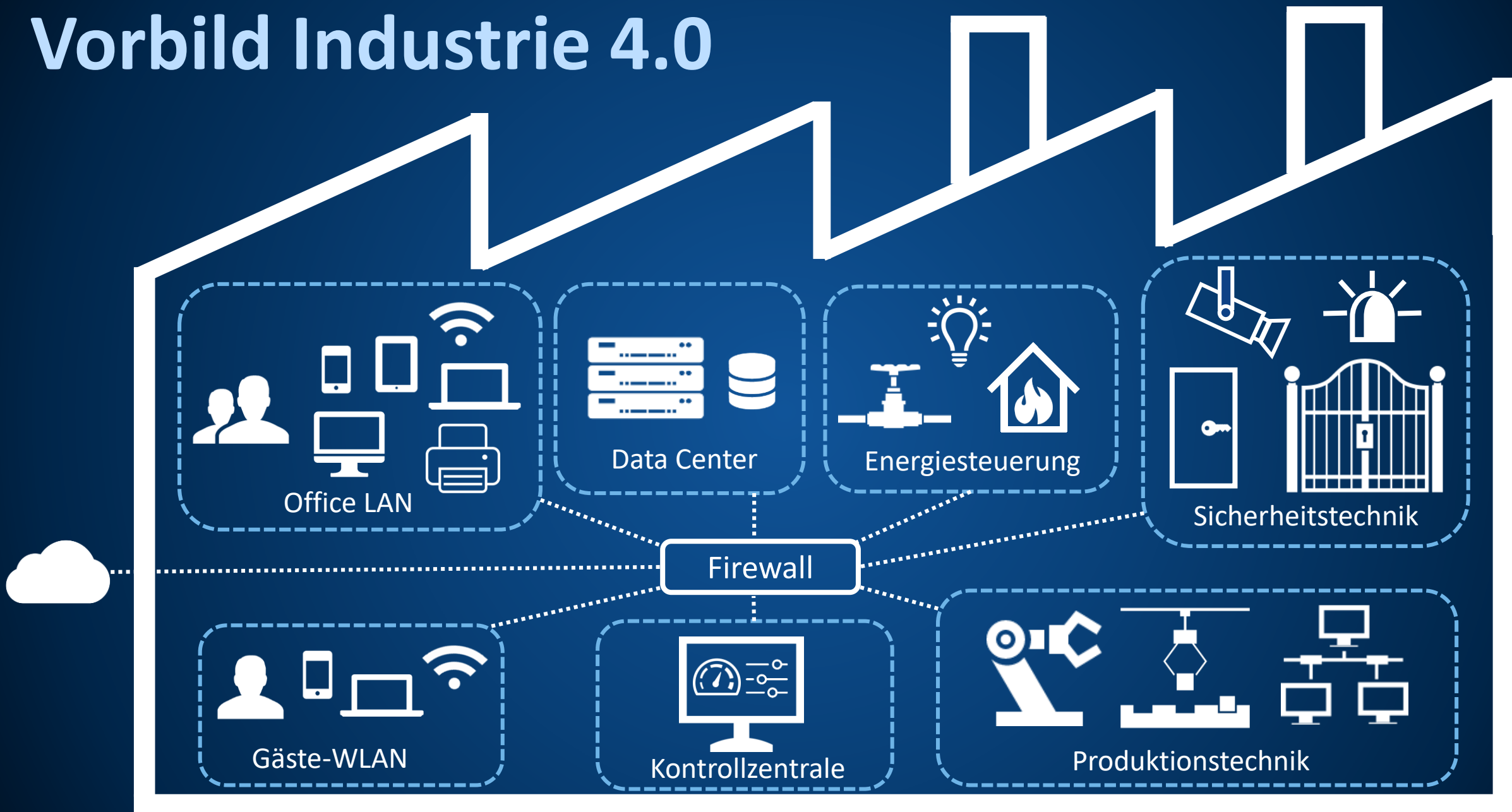
**Was kann ich tun?**

**SOPHOS**

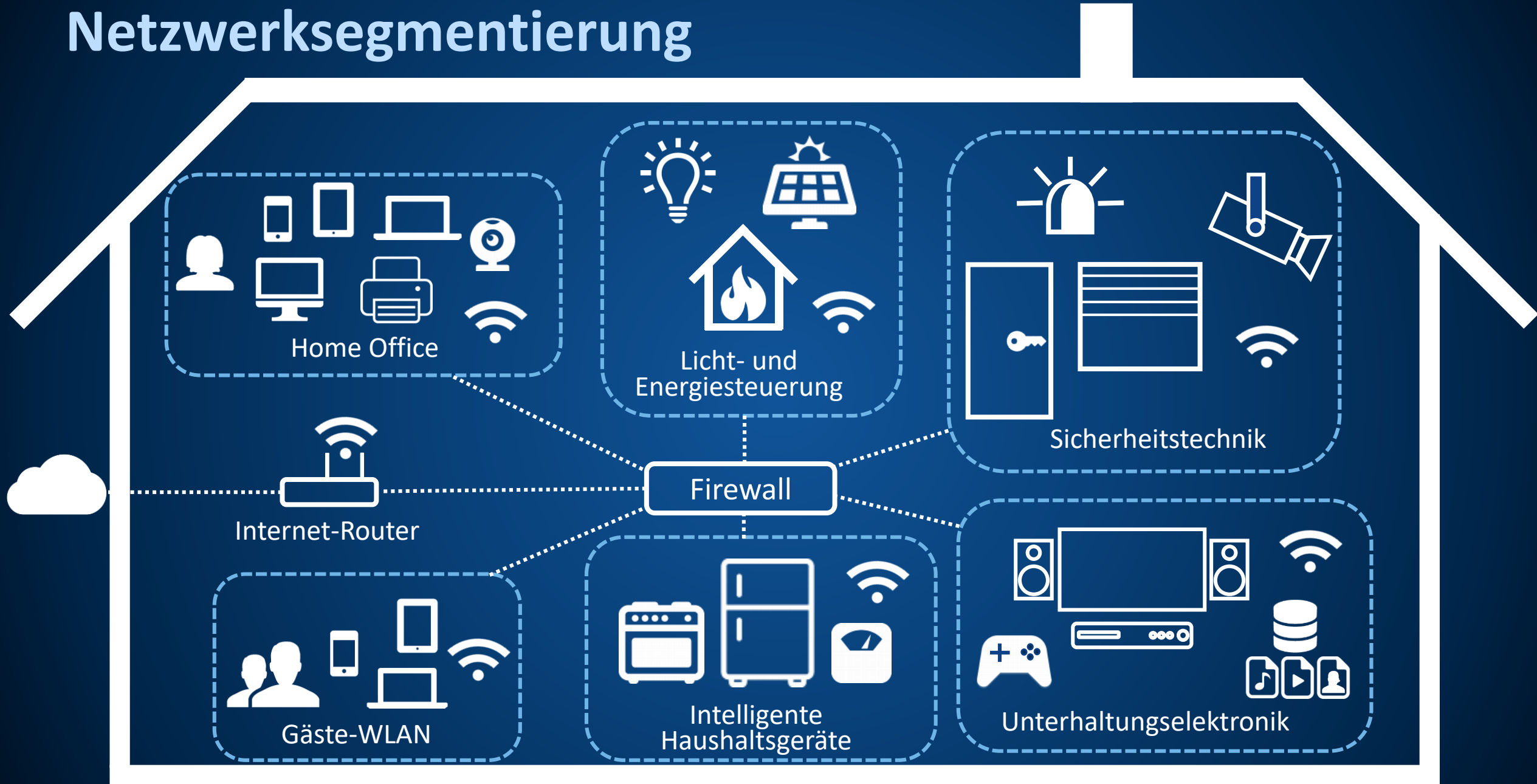


# Maßnahme 1: Segmentierung

# Vorbild Industrie 4.0



# Netzwerksegmentierung



**Maßnahme 2:**  
**Sorgfältige Auswahl von**  
**SmartHome-Komponenten**

# Langfristig denken

- Die Lebensdauer von Smartphone, Fernseher, Webcam und Fitnesswaage liegt bei wenigen Jahren
- Beim SmartHome muss man in Jahrzehnten denken
- Ausfälle von SmartHome-Komponenten bei der Energie- und Hausgerätesteuerung - oder beim SmartCar können massive Folgen haben



# Was muss ich bei Smart Home Komponenten beachten?

- Kann ich das Gerät auch ohne Netzwerkverbindung bedienen?
- Für welchen Zeitraum sichert der Hersteller (Sicherheits-) Updates zu?
- Kann ich lokal, per VPN oder nur über einen Dienst des Herstellers zugreifen?
- Werden Standard-Schnittstellen und Protokolle verwendet? Kann ich einzelne Komponenten ersetzen, wenn es die Lösung oder den Hersteller nicht mehr gibt?



Maßnahme 3:  
Updates, **Updates**, Updates

# Patch early, patch often...

- Updates/Patches für Betriebssysteme und Anwendungen schnellstmöglich einspielen
- Rechner neu starten
- Internet-Router und SmartHome-Komponenten regelmäßig updaten





# Maßnahme 4: Sichere **Passwörter**

# Sichere Passwörter



- Lange + komplexe Kennwörter > 14 Zeichen

Ich esse am liebsten Frankfurter Grüne Soße auf HAWAII  
zusammen mit meinem besten Freund Egon

leaFGSaHzmmbFE

lea!FG\$4H7mmbF3

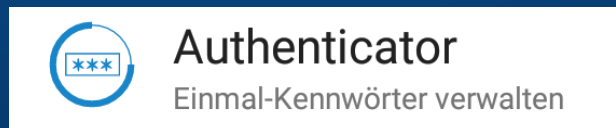
- Pro Dienst/Webseite ein anderes Kennwort

z.B. für Ebay lea!FG\$4HEy7mmbF3

- Passwortmanager nutzen



- 2-Faktor-Authentisierung

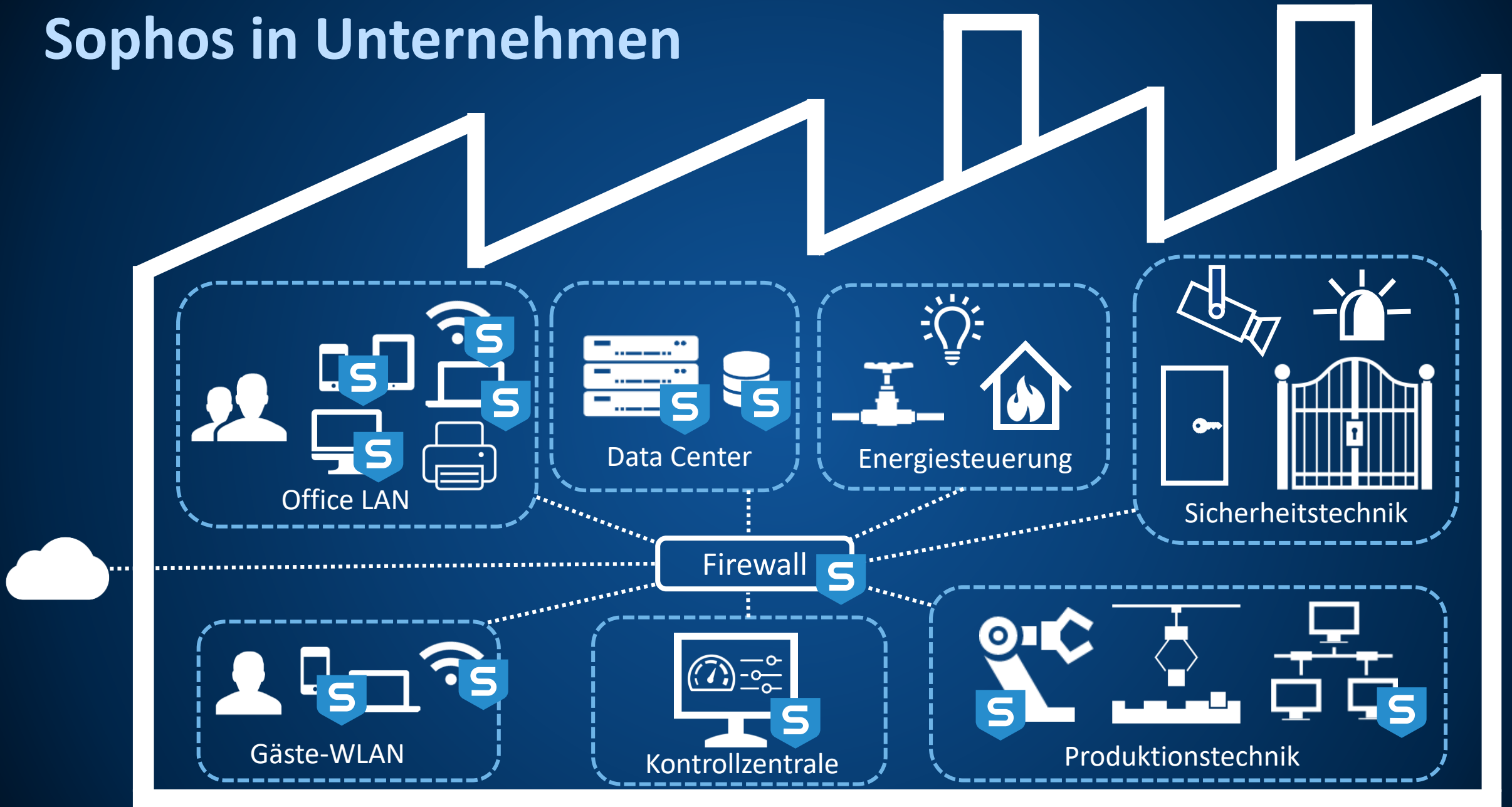


**Maßnahme 5:**  
**Sicherheitssoftware**  
**einsetzen**

# Komplette Unternehmenssicherheit von Sophos



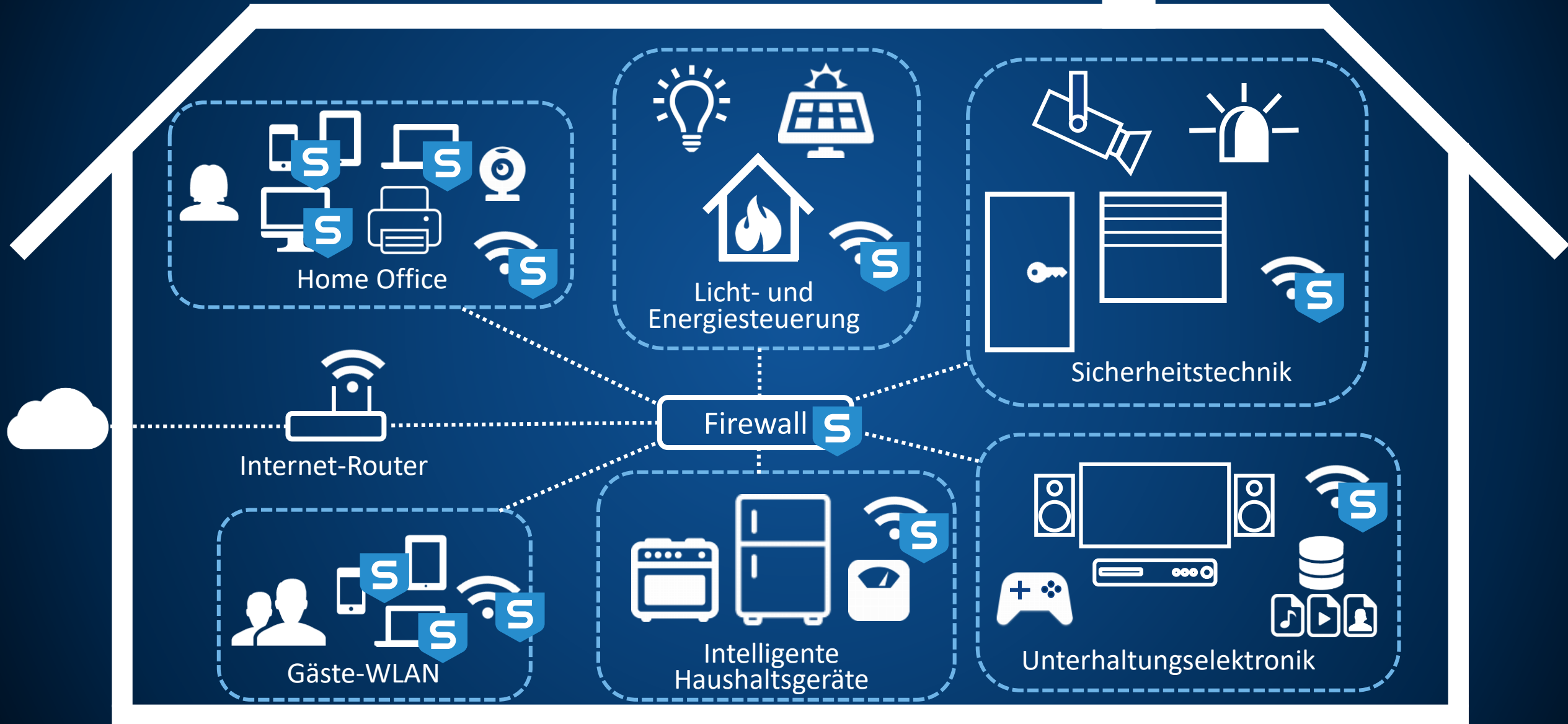
# Sophos in Unternehmen



**Kostenlose**  
Sophos Lösungen  
für **Privatanwender**

**SOPHOS**

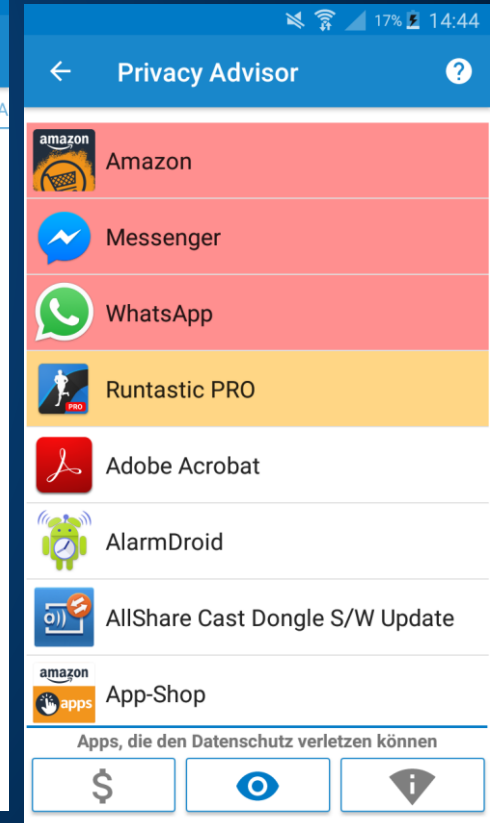
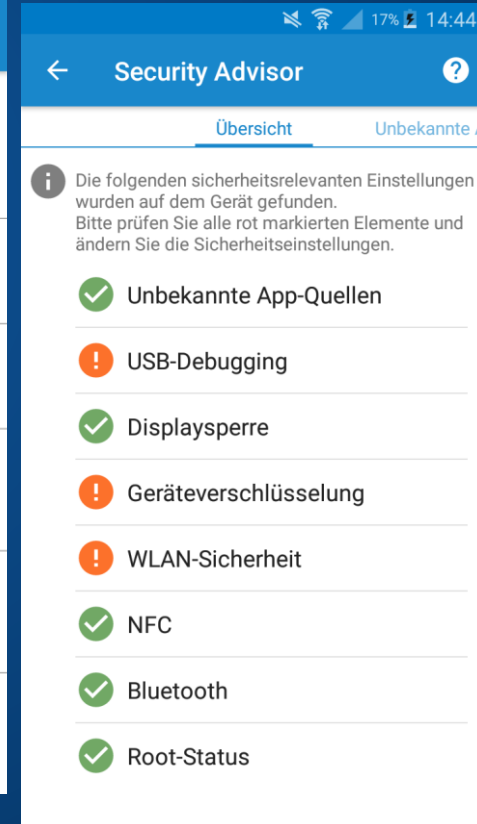
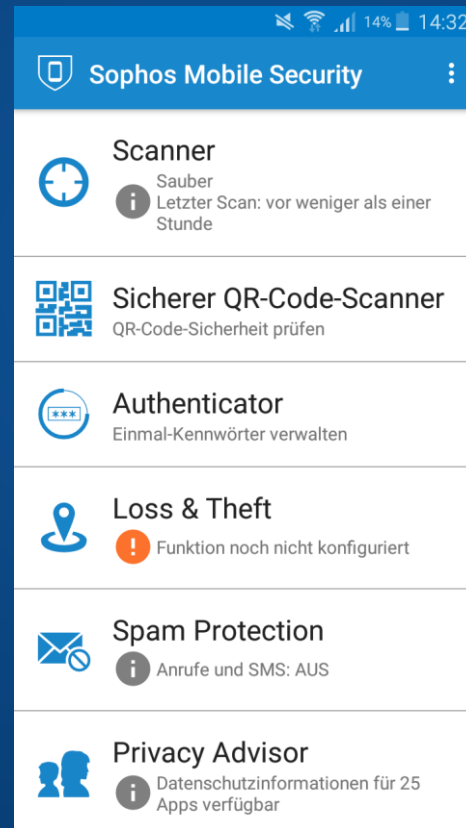
# Sophos Lösungen für Privatanwender



# Sophos Mobile Security für Android



- Kostenlose App für Android
- Malware-Scanner
- Schutz vor Online-Bedrohungen
- Privacy und Security Advisor
- Authentifikator für Multi-Faktor-Authentisierung
- Sicherer QR-Code-Scanner





# Sophos Home für PCs und Mac



- Kostenloser Virenschutz für PCs und Macs auf dem Niveau von Unternehmenslösungen
- Zentrale Verwaltung von bis zu 10 Geräten über Cloud-basiertes Webinterface von überall
- Webfilter und Schutz vor Phishing
- Sperrung unerwünschter Anwendungen

**Secured**  
Automatic Virus Protection is On

Home Dashboard

Full Scan Threats Found: 0

895 of 1237682 items scanned

Protection Exceptions...

- Automatic Virus Protection**  
Checks and protects you in real-time from malware any time a file is accessed. ✓ ON
- Web Protection**  
Blocks websites that are known to have viruses and other threats. ✓ ON
- Potentially Unwanted App Detection**  
Detects potentially unwanted applications in real-time and prevents them from installing or running. ✓ ON

SOPHOS ? Help i About

Web Category ?

Adult & Potentially Inappropriate

	ALLOW	WARN	BLOCK
Adult/Sexually Explicit	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Alcohol & Tobacco	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Criminal Activity	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Hacking	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Illegal Drugs	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Intimate Apparel & Swimwear	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Intolerance & Hate	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Proxies & Translators	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>

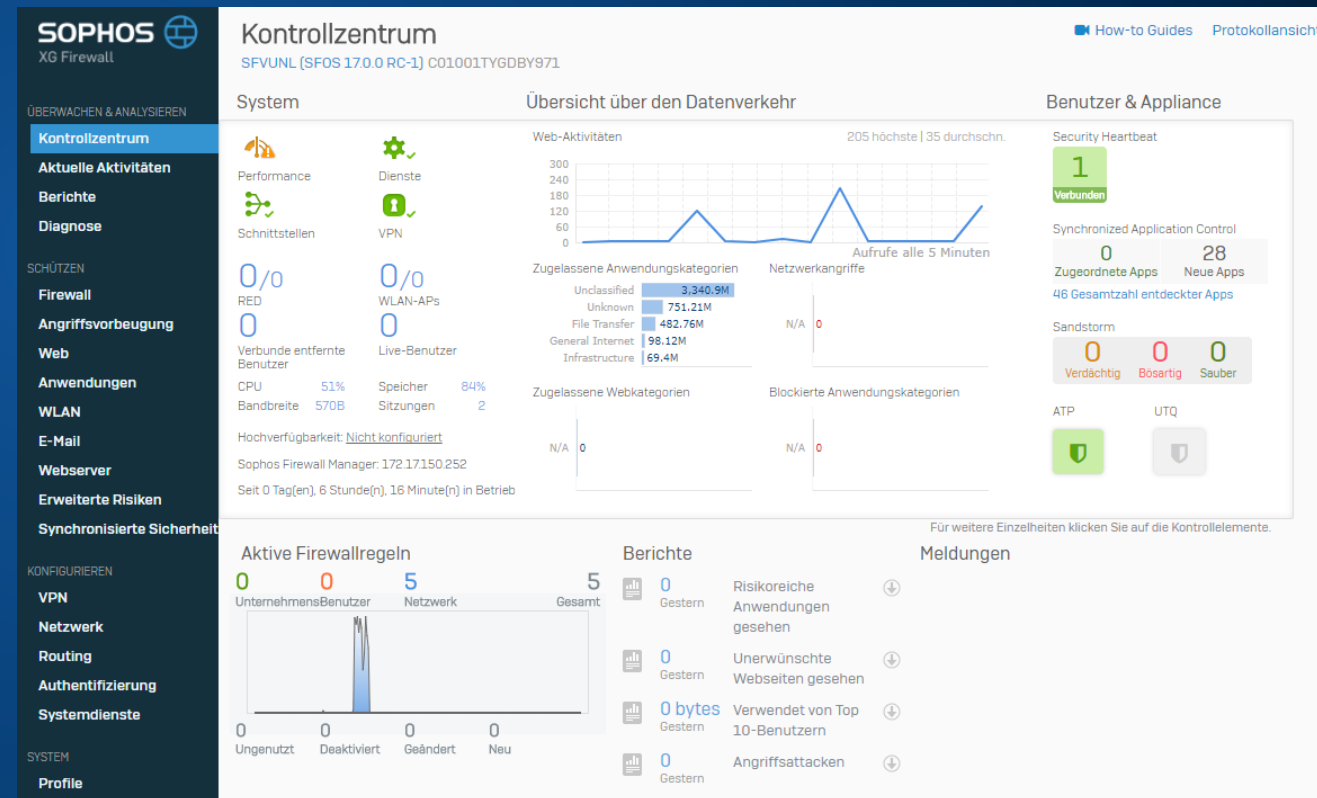
	Threats Cleaned	Websites Blocked	Last Update	
Eintracht-Win10 Secured	No Alerts	0	0	Jun 13, 2017 2:00 AM
Gisela-Win10 Secured	No Alerts	0	0	Feb 9, 2017 8:58 PM
Kathrin-Win10 Secured	No Alerts	0	0	Jun 11, 2017 5:32 PM
Michaels iMac Secured	No Alerts	0	0	Apr 5, 2017 5:19 PM

# IT-Sicherheit auf Unternehmensniveau Einfach. Effektiv. Kostenfrei.



## Sophos XG Firewall Home Edition (Firewall-Software)

- Trennung der Netzwerksegmente (z.B. Internet, Home Office, Gäste-WLAN, SmartHome-Netz, IoT-Netz)
- Web- und Applikationsfilter (kein Zugriff auf gefährliche oder gesperrte Webseiten, Virenschutz)
- Email-Sicherheit (Virenschutz, SPAM-Schutz)
- Sicherer VPN-Zugriff aus dem Internet auf Home Office und SmartHome



# Aktuelle Erkenntnisse und Trends

- Technische Fachbeiträge  
<https://www.sophos.com/de-de/threat-center/technical-papers.aspx>
  - SophosLabs 2018 Malware Forecast
  - Machine Learning: How to Build a Better Threat Detection Model
  - BetaBot Configuration Date Extraction
- Whitepaper, Buyers Guides und Analystenberichte  
<https://www.sophos.com/de-de/security-news-trends/whitepapers.aspx>
  - Exploits in der Falle
  - Mobiler Wahnsinn oder BYOD-Sicherheit
  - Projekte „Honeytrain“ und „Haunted House“
- SophosNews  
<https://news.sophos.com/de-de/>
  - World Wide Western: Coin Miner nehmen Android ins Visier
  - Erster Malware-Star 2018: SkyGoFree attackiert Android-Smartphones
- Youtube Kanäle (z.B. SophosGlobalSupport)

**SOPHOS**  
Security made simple.