WISSENSCHAFT • FORSCHUNG
NIEDERÖSTERREICH

Diese Arbeit wird von der Gesellschaft für Forschungsförderung NÖ (GFF) im Rahmen des FTI Call Digitalisierung 2018 kofinanziert. Für den Inhalt dieser Publikation sind die Autor*innen verantwortlich.

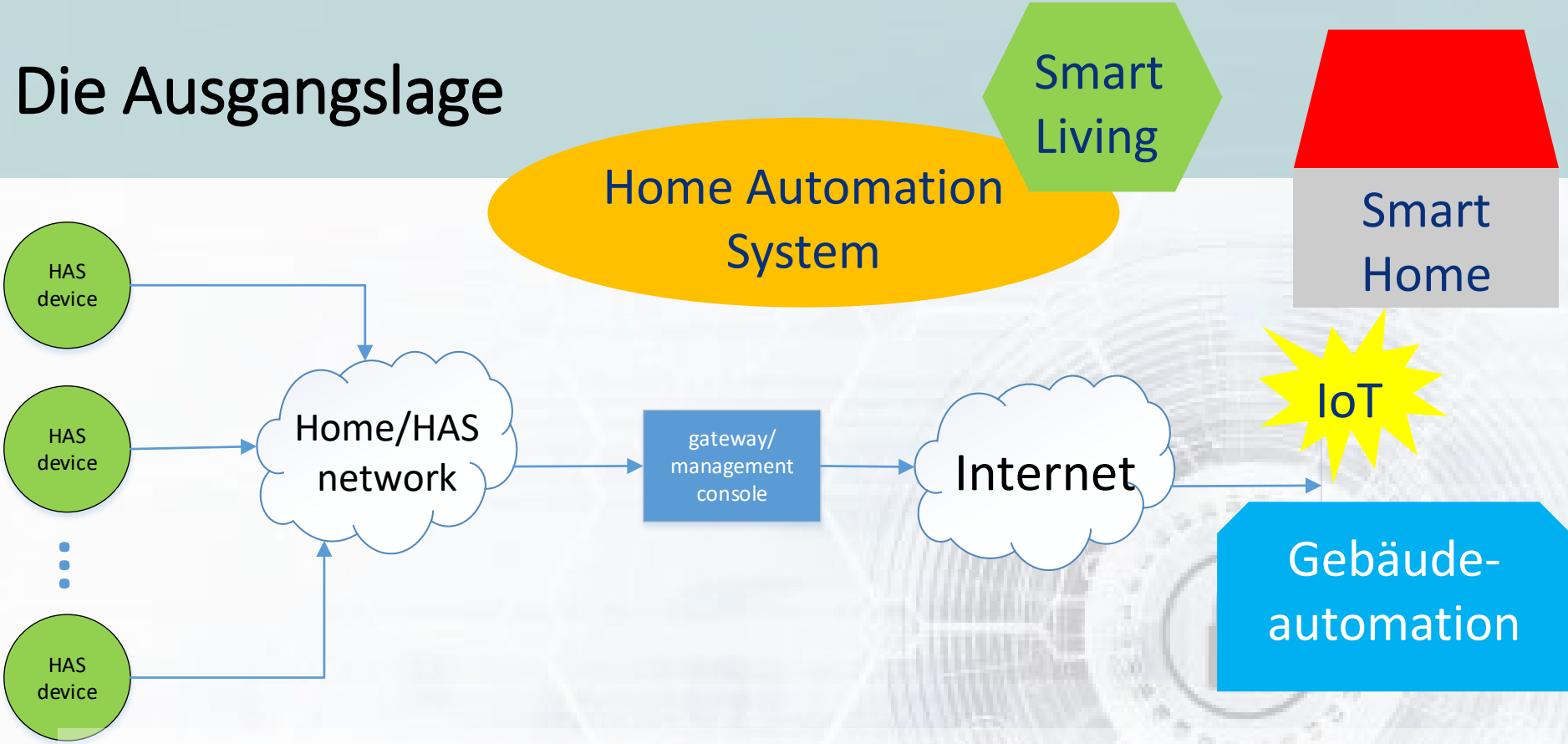
SMART HOMES

NUTZUNG UND SICHERHEIT

Bettina Pospisil / Albert Treytl / Edith Huber / Walter Seböck / Peter Kieseberg

DONAU UNIVERSITÄT KREMS
/fh/// st.pölten
GESELLSCHAFT FÜR FORSCHUNGS FÖRDERUNG NIEDERÖSTERREICH
Haus der Digitalisierung

Die Ausgangslage



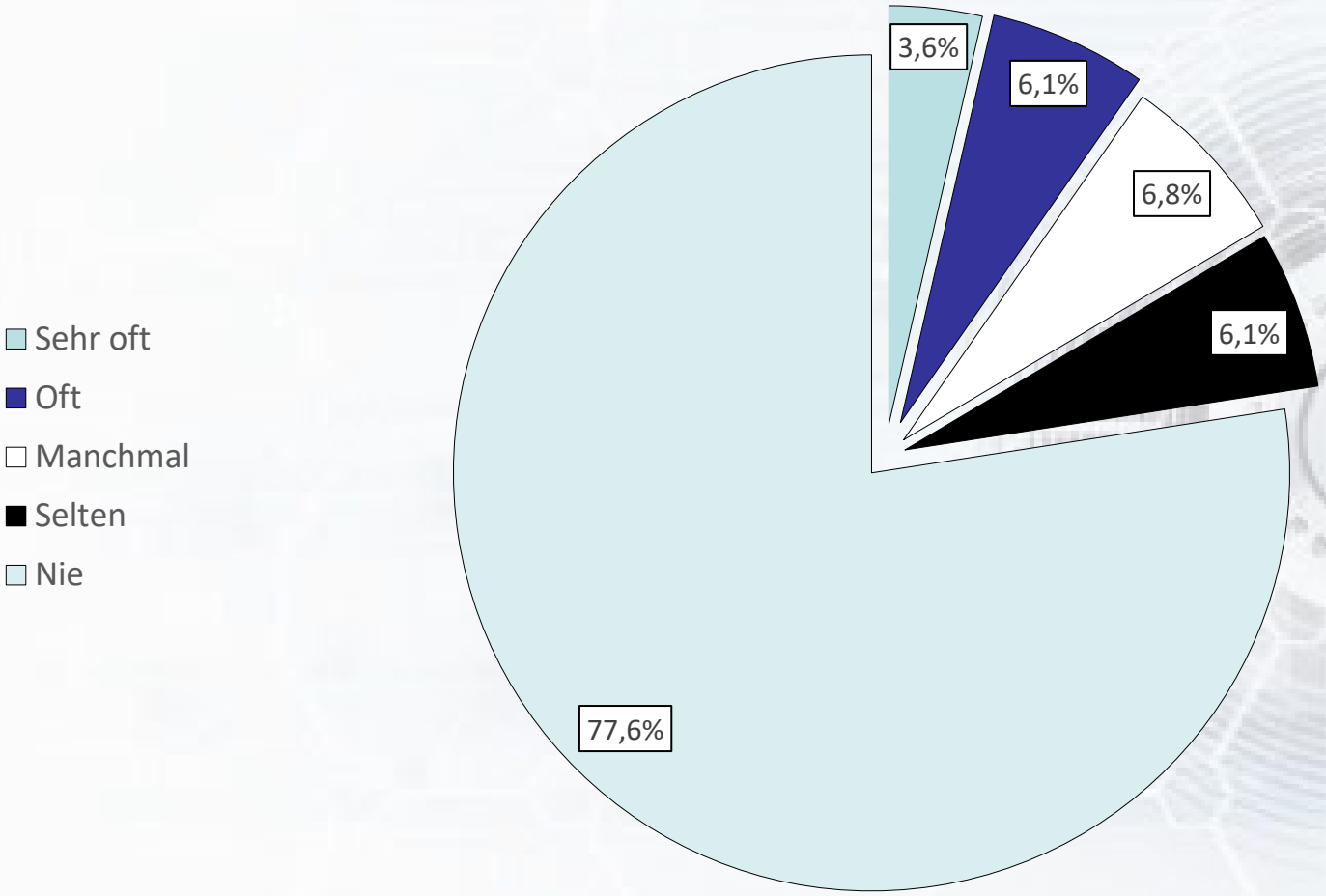
- **Fokus auf Monitoring und Automatisierung von privaten Wohnungen und Häusern**
- Implementierung von hardwarebasierten Sicherheitsmaßnahmen unter Verwendung von Meta-Informationsquellen
- Analyse von Datenströmen in HAS zur Erkennung von Angriffen und zum Schutz der Systeme
- **Aufzeigen des Ist-Zustandes zum Einsatz und zur Nutzung von HAS in privaten Haushalten (Survey)**

Das Forschungsdesign

- Wir wirkt sich das tatsächliche Nutzungsverhalten von HAS auf Sicherheitsüberlegungen aus?
  (1) Wie sieht das Nutzungsverhalten der Österreicher*innen in Bezug auf HAS-Geräte aus?
  (2) Welche Sicherheitsrisiken ergeben sich für österreichische Haushalte durch ihre HAS-Nutzung?
  (3) Wie kann diesen begegnet werden?
- Methodische Umsetzung
  (1) Quantitative Befragung
  (2) Technische Konfiguration zu HAS und Sicherheit generell
  (3) Zusammenführung: Schlussfolgerungen bezüglich Sicherheitsrisiken und Gegenmaßnahmen

DAS NUTZUNGSVERHALTEN

Wie häufig nutzen Sie HAS?



Welche HAS Geräte besitzen Sie?

- Smart TV (583)
- Sprachassistenz-Systeme (299)
- Überwachungskameras (116)
- Beleuchtungssystem (87)
- Alarmsystem (81)
- Steckdosen (80)
- Heizung (70)
- Türglocke (69)
- Staubsauger (65)
- Temperaturmessgeräte (63)
- Bewegungsmelder (61)
- Jalousien (52)
- Türöffner bzw. Schließanlage (43)
- Waschmaschine (43)
- Garage (33)
- Kaffeemaschine (32)
- Rasenmäher (28)
- Pflanzenbewässerung (26)
- Kühlschrank (24)
- Tierfutternapf (24)
- Swimmingpool (16)
- andere (59)

Totalzahlen

Wie wahrscheinlich werden diese genutzt?

- Häufiger genutzt, wenn besessen, werden z.B.
  - Überwachungskameras (78 %)
  - Beleuchtungssysteme (78 %)
  - Heizungssysteme (76 %)
- Durchschnittlich häufig genutzt, wenn besessen, werden z.B.
  - Smart TV (64 %)
  - Sprachassistenten (66 %)
- Selten genutzt, wenn besessen, werden z.B.
  - Tierfutternapf (29 %)
  - Kaffeemaschine (31 %)
  - Waschmaschine (35 %)
  - Kühlschrank (38 %).

Welche Art von HAS ist verbreiteter?

Mobile HAS	Stationäre HAS	Beides möglich
Smart TV	Heizung	Alarmsysteme
Sprachassistenten	Steckdosen	Türglocke und Kamera
Kaffeemaschine	Garage	Bewegungsmelder
Kühlschrank	Jalousien	Temperaturmessgerät
Staubsauger	Beleuchtungssystem	Überwachungskamera
Rasenmäher	Türöffner bzw. Schließanlage	Pflanzenbewässerungs-system
Waschmaschine	Swimmingpool	
Tierfutternapf		

95 %

24 %

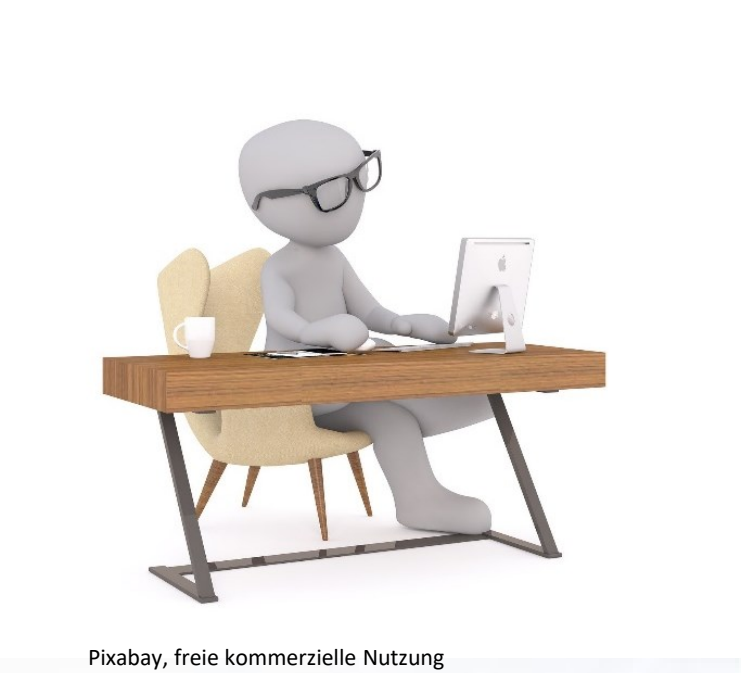
26 %

In welchen Haushalten finden sich mehrere HAS-Geräte?

Pixabay, freie kommerzielle Nutzung

- Haushalte mit höherem Nettoeinkommen
  - Spearman: 0,204**
- Größere Haushalte
  - Spearman: 0,195**
- Haushalte mit Haus im Eigentum
  - Spearman: 0,107**

Wer nutzt HAS-Geräte häufiger?

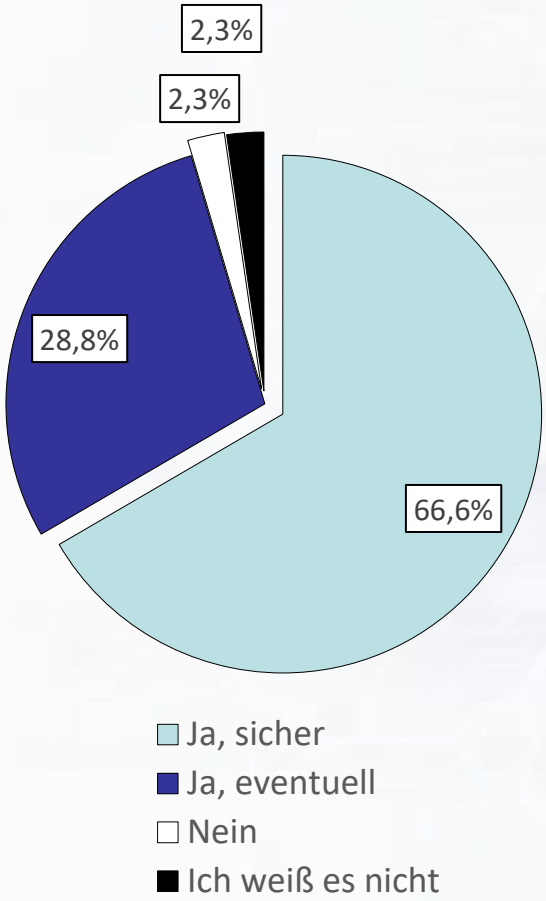


Pixabay, freie kommerzielle Nutzung

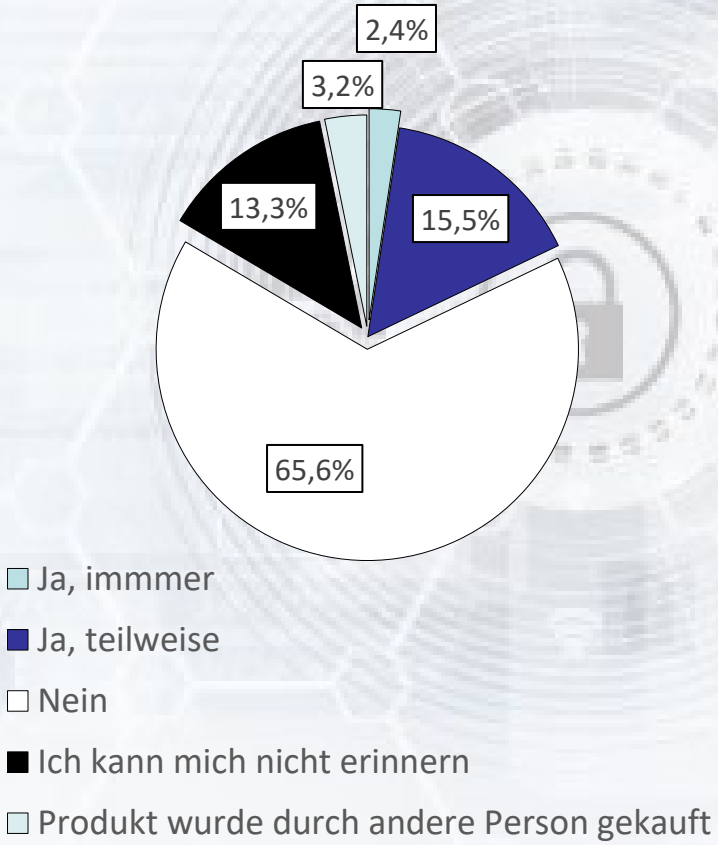
- Jüngere Personen
  - Spearman: 0,194**
- Personen mit IT-Ausbildung
  - Cramer-V: 0,174**
- …Männer?
  - Cramer-V: 0,131**
  - M: Mittelwert=4,39
  - W: Mittelwert=4,57
  - Aber: Geschlecht & Ausbildung im IT-Bereich (Phi: 0,138**)

Sammlung von Nutzungsdaten I

Glauben Sie, dass Ihre Nutzungsdaten gesammelt werden?

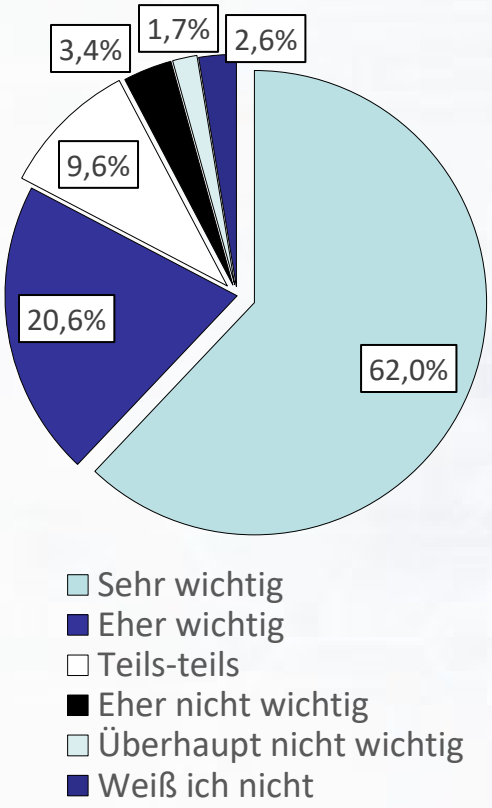


Wurden Sie proaktiv über die Sammlung & Verwendung Ihrer Daten informiert?

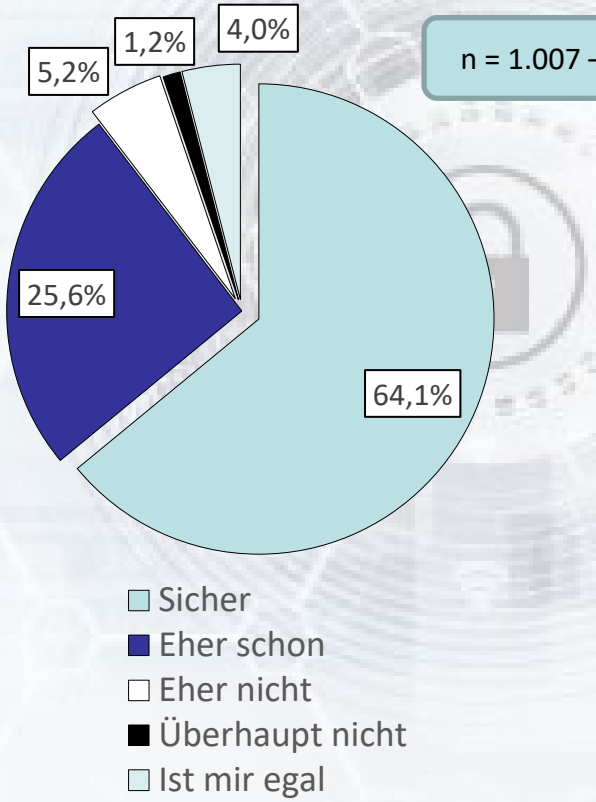


Sammlung von Nutzungsdaten II

Wie wichtig ist Ihnen, dass Sie von Hersteller*innen über die Sammlung & Verwendung Ihrer Daten informiert werden?



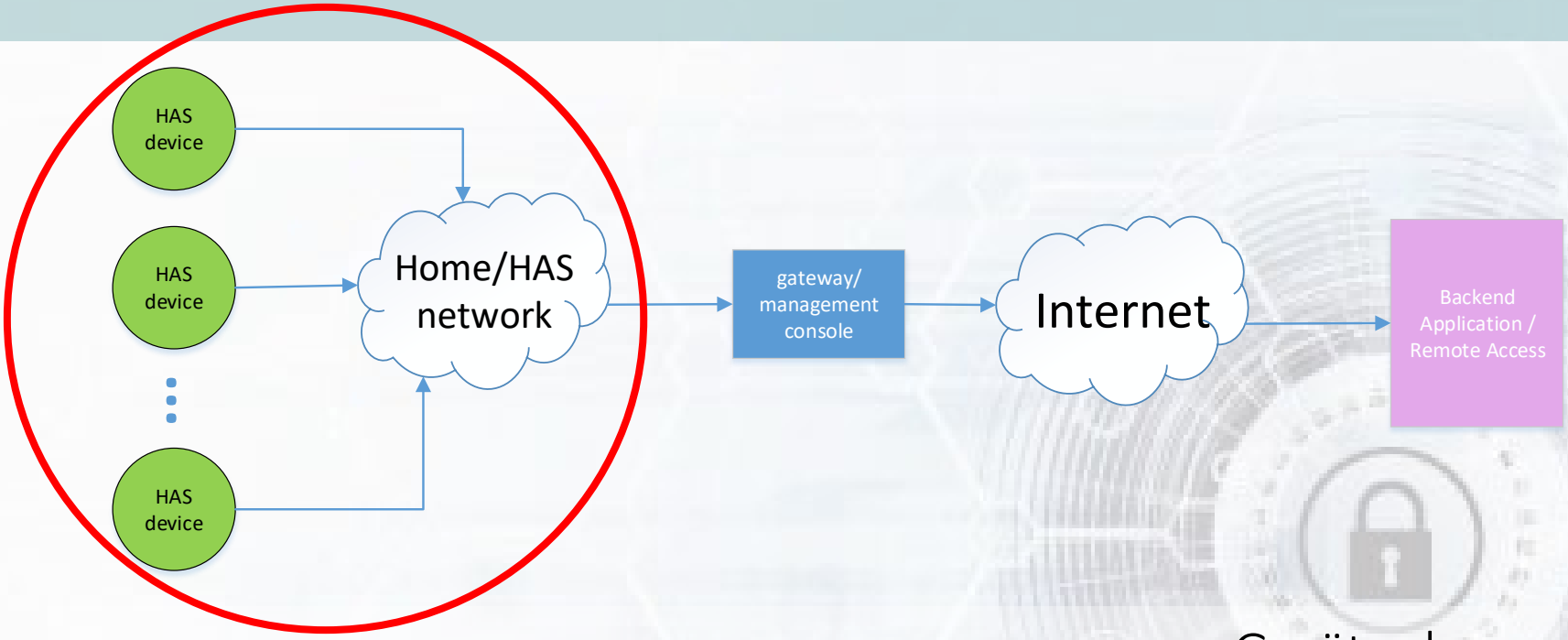
Sollten Hersteller*innen gesetzlich verpflichtet werden, über ihre Sammlung & Verwendung von Daten zu informieren?



n = 1.007 – alle Befragten

HAS UND SICHERHEIT

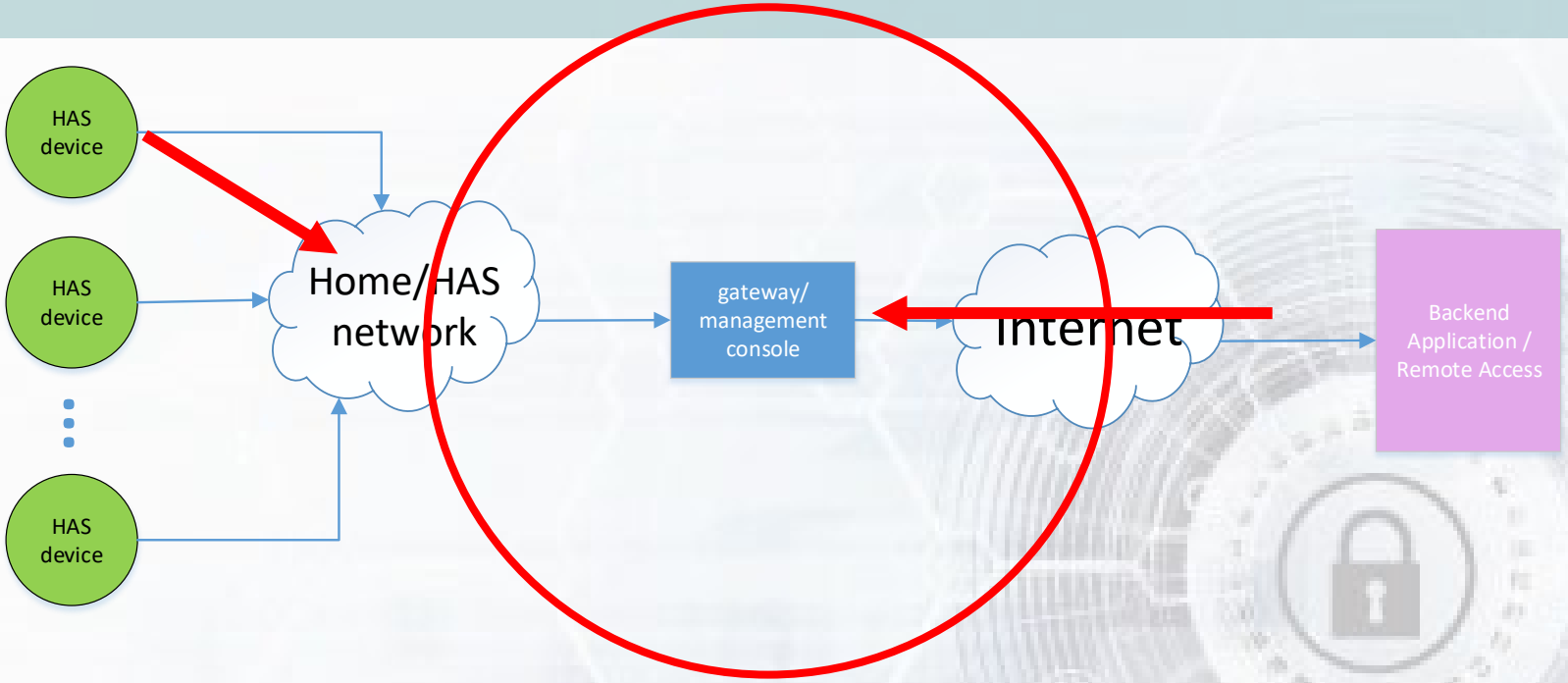
Technische Konfiguration und Angriffsflächen in HAS



Geräteebene

- Kein oder nur schwacher Schutz durch kryptographische Verfahren, Meist schlechtes Schlüsselmanagement
- Problematische Praxis für Sicherheitsupdates auf Grund von mangelnder Bandbreite oder fehlender Wartung.
- Spannungsfeld zwischen direktem physischem Zugang und mangelnder Zugangskontrolle im System.

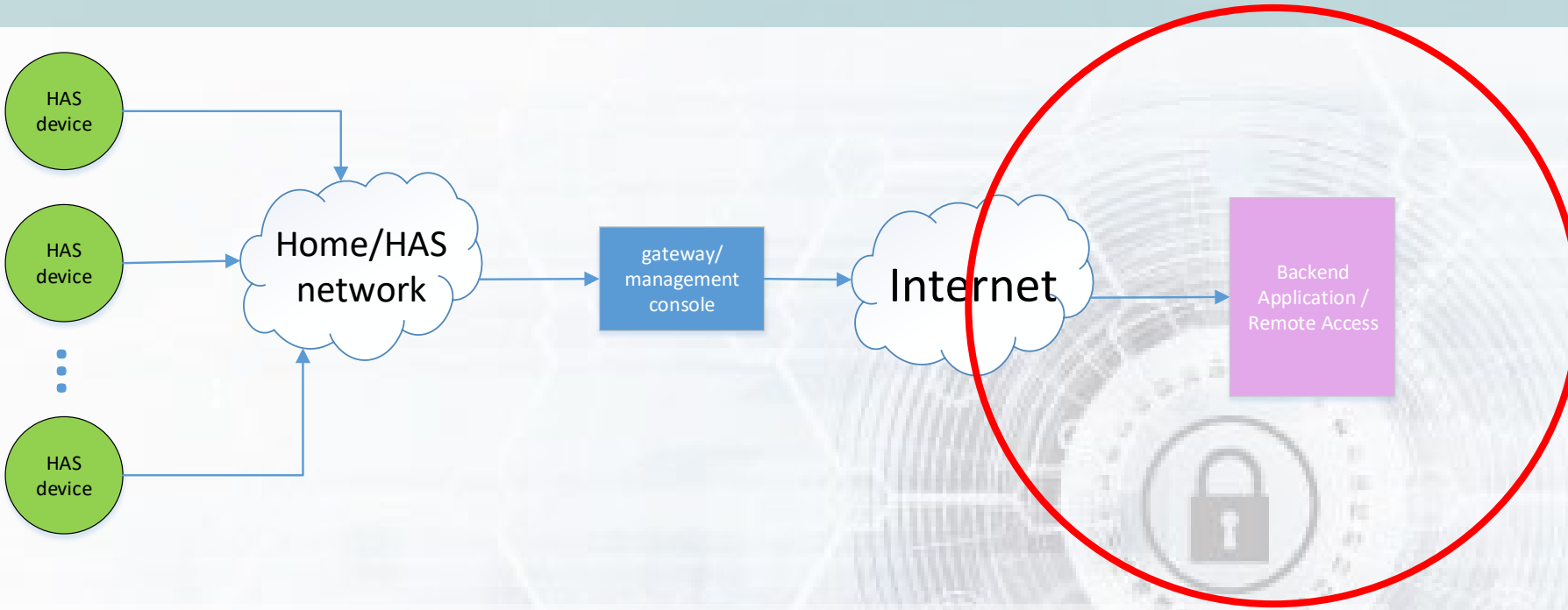
Technische Konfiguration und Angriffsflächen in HAS



Gateway-Ebene

- Zwei Angriffsflächen sowohl aus dem Automatisierungsnetzwerk als auch dem Internet (direkt/indirekt über HAS-Gerät)
- Missbrauch sowohl von Gateways als auch HAS-Geräten als Angriffsplattform
- Direkte Möglichkeit der Manipulation von HAS-Geräten

Technische Konfiguration und Angriffsflächen in HAS



- Applikationsebene/Cloud
  - Schwerwiegende Datenschutzbedenken, da Zugriff auf große Menge an persönliche Daten
  - Offenlegung der Systemkonfiguration
  - Informationen sind ein Katalysator für Pishing, Social Engineering, Erpressung, Stalking, …

CONCLUSIO: SICHERHEITSRISIKEN UND GEGENMAßNAHMEN

Schwachstellen und Risiken für Ö-Haushalte

- Geräte mit direktem Internetzugang -Smart TVs und Sprachassistenten
  - Fehlende Sicherheitsupdates
  - Installationsmöglichkeit für bösartige Apps
  - Steuerung über angegriffene Sprachassistenten
- Schwache Geräte/Nutzer*innen-Authentifizierung
  - Schwache Passwörter (Standardpasswörter, Wiederverwendung,…)
  - HAS werden nicht als IT(OT)-Systeme gesehen
- Systeme für Zugangskontrolle und Überwachung
  - Größtes Wachstumspotential (Statista Smart Home Report 2020)
  - Größte Auswirkung, da Einwirkungen auf die reale Welt

Gegenmaßnahmen & Bedürfnisse der Nutzer*innen

- Weiter- und Bewusstseinsbildung
  - Allg. Bewusstsein (für klassische Computer) vorhanden, aber mangelhafte Kenntnis im Detail bzw. Umsetzung (z.B. Passwortwechsel, Updateverantwortung)
  - Handlungsbedarf für eingebettete, "unsichtbare" Systeme
- Reglementierung der Datenhoheit bzw. -kontrolle
  - Stärkere Verpflichtung von Hersteller*innen (contra Geschäftsmodel mit Nutzer*innen-Daten)
  - Mehr Informationspflichten für Hersteller*innen
  - Starker Wunsch seitens der Nutzer*innen
- Deaktivierung/Schutz von ungenutzten Funktionen
  - Spannungsfeld Besitz, Bewusstsein, Nutzung und, Funktionalität
  - “Hidden Features" müssen abgesichert werden.
  - Aufwand für Aktualisierung von Sicherheitsmaßnahmen

Entwicklung und Herausforderungen

- Stark steigende Anzahl an HAS-Geräten und Systemen
- Wechsel von Entertainment (sichtbar) zu Automatisierung (eingebettet)
- Zunehmende Bedrohung durch eingebettete und mit dem Internet verbundene Geräte
- Große Bedeutung von Sprachassistenten z.B. im Bereich Ambient Assisted Living)

→ Herausforderung: übergangslose Sicherheitsfunktionen
  - Konzepte für Sicherheitsupdates
  - Authentifizierung und Zugriffskontrolle

→ Herausforderung: Datenhoheit und Informationszugriff
  → feinmaschige Zugriffslösungen
  → (gesetzl.) Rahmenwerk

Herzlichen Dank für die Aufmerksamkeit

- Bettina Pospisil, M.A.
  - bettina.pospisil@donau-uni.ac.at
- Dipl. Ing. Albert Treytl
  - albert.treytl@donau-uni.ac.at
- Dr. Edith Huber
  - edith.huber@donau-uni.ac.at
- Ass. Prof. Mag. Dr. Walter Seböck
  - walter.seboeck@donau-uni.ac.at
- Dipl.-Ing. Peter Kieseberg
  - peter.kieseberg@fhstp.ac.at