Datenschutz und Datensicherheit im Smarthome

Patrick Ney – Projektmanager für Digitalisierung, Digital Scout, Datenschutzkoordinator –

Landeshauptstadt Hannover, Fachbereich Senioren

Datenschutz und Datensicherheit

- Bei der bewussten Weitergabe von Smarthome-Nutzungsdaten sind die Deutschen nach wie vor zurückhaltend
- Bedenken sind in den Altersgruppen unterschiedlich verteilt
- Verbraucher wünschen sich mehr Informationen zu digitaler Sicherheit jedoch nicht zu aktuellen Themen wie Smarthome → Sicherheitsrisiken werden noch nicht bewusst wahrgenommen
- Produkte teils unzureichend in Datenschutzerklärung beschrieben oder die Auffindbarkeit von Privatsphäreeinstellungen ist eingeschränkt
- User-Profiling: Funktionsverlust des Geräts vs. Datenanalyse

Quelle: Deloitte Smart Home Consumer Survey 2018; BSI 2021:Bericht zum Digitalen Verbraucherschutz 2020

Datenschutz und Datensicherheit

- Smarthome Systeme und Geräte aus dem Bereich Internet der Dinge verursachen tendenziell Sicherheitsvorfälle
  - Sicherheitsanalyse zeigen im Jahr 2020 über 7.000 Schwachstellen in sechs zufällig ausgewählten Produkten z.B. in smarten Kinderspielzeug
- Mehrheit der Hersteller von Smart-TVs behebt Sicherheitsmängel erst nach dem Verkauf und bietet ca. 27 Monate Sicherheitsupdates an

Quelle: BSI 2021:Bericht zum Digitalen Verbraucherschutz 2020

Tech Abuse — Smart, Internet-connected devices present new risks for victims of domestic violence & abuse

1 Wearable devices
Could allow perpetrators to track and monitor movements and other behavioural patterns drawing on GPS signals and other collected data.

2 Phones
Could provide perpetrator an access point to control various IoT devices.

3 Laptops and tablets
Accounts between devices are linked and could allow perpetrators to change and review IoT devices' settings via an Internet browser.

4 Remote control of heating, lighting and blinds
Could be used to coerce and intimidate victims by switching systems on or off from afar.

5 Security cameras and TVs
Could facilitate remote monitoring and online stalking; video recording could facilitate image-based abuse (such as revenge porn).

6 Smart security
Could provide access to doors through voice activation, apps, or electronic key codes.

7 Audio recording
Could facilitate remote monitoring and stalking.

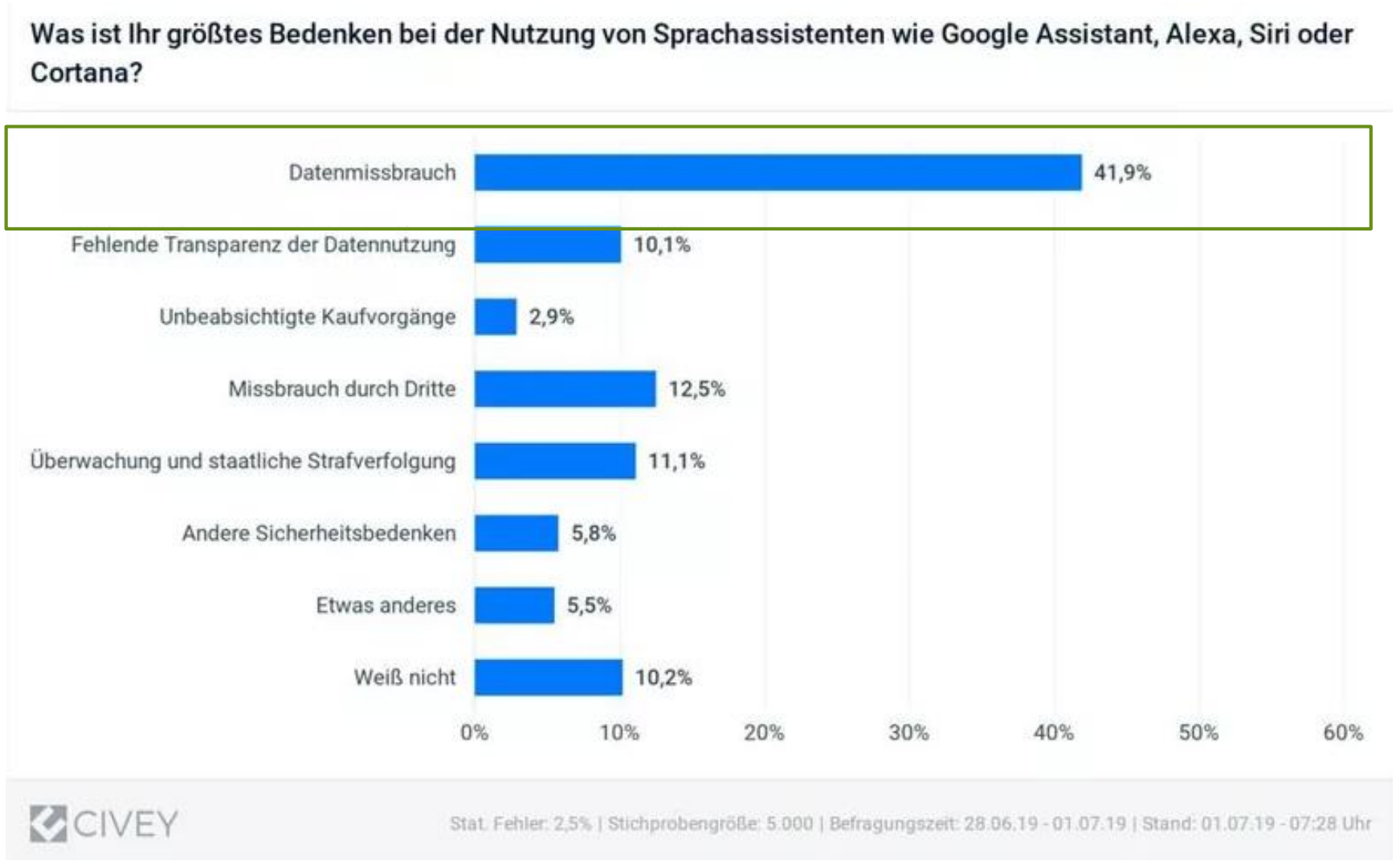
8 Voice control
May enable perpetrators to contact the victim as well as trace and review a person's history of commands and purchases.

9 Router
Connects all smart home devices to the Internet.

DEPARTMENT OF SCIENCE, TECHNOLOGY, ENGINEERING AND PUBLIC POLICY

Quelle:
https://pbs.twimg.com/media/Ds7fJIPWsAA5t7G?format=jpg&name=large, Leonie Tanczer, UCL, London - http://www.csap.cam.ac.uk/network/leonie-tanczer/

Quelle: Eco https://www.security-insider.de/datenschutz-als-schluessel-zur-akzeptanz-von-smart-home-a-863308/



Deshalb: Chancen von künstlicher Intelligenz nutzen unter Berücksichtigung hoher Datenschutzschutzregelungen und Sicherheitsstandards

Datenschutz und Datensicherheit am Beispiel Smart Speaker

1. Ausführung startet durch das Aktivierungswort → Mikrofon ist dauerhaft aktiv jedoch werden keine Daten übertragen
2. Akustisches Signal wird durch künstliche Intelligenz in der Cloud verarbeitet und interpretiert, zusätzlich werden Metadaten wie Uhrzeit, IP-Adresse, verwendete Hard- und Software sowie Diagnose- und Standortdaten gespeichert
3. Optimaler Weise wird der Kontext der Anfrage erkannt
4. Antwort wird an den Smart Speaker geleitet und als Text ausgegeben oder startet eine Aktion

Quelle: https://www.annasleben.de/

Datenschutz und Datensicherheit am Beispiel Smart Speaker

- Datenschutzerklärungen der Anbieter beschreiben allgemein den Zweck der Datenerfassung wie Bereitstellung, Verbesserung der Dienste oder personalisierte Werbung
- Bei der Nutzung von Diensten Dritter tauscht der Anbieter des Smart Speakers diese mit dem Drittanbieter. Damit gelten die Datenschutzbestimmungen des Drittanbieters.
- Nachträglicher Widerruf der Datenspeicherung und Verarbeitung verringert den Funktionsumfang – Geräte sind dann häufig nicht mehr smart

Quelle: https://www.annasleben.de/

Wie können Nutzer*innen Smart Speaker sicher nutzen? I

- Gespeicherte Sprachanfragen können je nach Anbieter eingesehen und gelöscht werden
- Stimmprofile anlegen damit nur Sie Zugriff haben
- Smart Speaker beim Abwesenheit oder Besuch ausschalten
- PIN oder Passwort benutzen für digitale Einkäufe einrichten

Quelle: https://www.annasleben.de/

Wie können Nutzer*innen Smart Speaker sicher nutzen? II

- nur vertrauenswürdige Erweiterungen installieren
- Updates durchführen
- Datenschutzeinstellungen kontrollieren
- Beschränkung auf notwendige Schnittstellen

Quelle: https://www.annasleben.de/

Smarthome Vorteile und Herausforderungen

- mehr Selbstständigkeit für
  - ältere Menschen z. B. durch Staubsaugerroboter
  - Menschen mit Einschränkungen zur Erkennung von Notfallsituationen bei Stürzen und Terminerinnung z.B. bei Tabletten
  - alleinlebende Personen zur Erkennung von Notfallsituationen und automatische Information an Dienstleister
- Energieeinsparung durch Abschaltung von Strom / Heizung bei Abwesenheit
- mehr Sicherheit z.B. Videotürklingeln und Fensterkontaktsensoren
- Smarthome Systeme können bewusst ausgewählt und angepasst werden, bei lokaler Speicherung ohne Cloudfunktionen ist mit Einschränkungen zu rechnen

Quelle: https://www.annasleben.de/ ; Yassein 2019 et. Al. Smart Home Is Not Smart Enough to Protect You - Protocols, Challenges and Open Issues

Smarthome Vorteile und Herausforderungen

- Geräte werden häufig über mehrere unterschiedliche Apps gesteuert
- Verändern sich die Bedürfnisse der Benutzer*innen müssen die Smarthomes neu konfiguriert werden
- hoher Zeit- und Geldaufwand zur Erklärung der Geräte
- zunehmende Komplexität der Datenverarbeitung erschwert Nachvollziehbarkeit, dadurch ist informationelle Selbstbestimmung gefährdet
- für die Funktionen von Smarthomes müssen personenbezogene Daten erhoben werden, dazu wird eine Einwilligung benötigt
- IT-Sicherheit spielt bei Herstellern häufig keine oder nur eine untergeordnete Rolle

Quelle: https://www.annasleben.de/ ; Yassein 2019 et. Al. Smart Home Is Not Smart Enough to Protect You - Protocols, Challenges and Open Issues

10 Regeln - Smarthome sicher nutzen

1. regelmäßig Sicherheitsupdates installieren
2. vorab informieren wie lange Hersteller nach dem Kauf Sicherheitsupdates bereitstellen
3. Aktivierung der Firewall und ändern des voreingestellten Passworts im Router
4. am Router die Einstellung UPnP (Universal Plug and Play) deaktivieren
5. individuelles Passwort mit mind. 18 Zeichen mit Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen für jedes smart Gerät erstellen sowie wenn vorhanden Zwei-Faktor-Authentifizierung aktivieren

Quelle: BSI 2021: Das Internet der Dinge sicher nutzen

10 Regeln - Smarthome sicher nutzen

5. Geräte kaufen die eine verschlüsselte Kommunikation unterstützen
6. kritische Selbstreflexion ob die Geräte über Fernzugriff per Smartphone gesteuert werden müssen
7. zur Datenflusskontrolle VPN (Virtuelles Privates Netzwerk) Verbindung einrichten
8. separates Heimnetz für Smarthome Geräte einrichten
9. physischen Zugriff Fremder auf USB- oder LAN-Ports verhindern
10. Informieren Sie sich über die Datennutzung der Geräte

- Welche Sensoren hat das Gerät?
- Welche Daten werden aufgezeichnet, wo gespeichert oder geteilt?
- Welche Risiken gehe ich mit der Nutzung des Geräts ein?

Quelle: BSI: Das Internet der Dinge sicher nutzen

Auswahl von Datenschutzfreundlichen Smarthome Produkten

ProKNX

KNX Sprachsteuerung mit und ohne Cloud z. B. Aragon oder DIY mit Raspberry Pi & Open Source Anwendungen wie Mozilla DeepSpeech

Digitalstrom

analoge Geräte digital vernetzen über lokalen Server und intelligente Lüsterklemmen

Verschlüsselte Videotürklingel

eufylife

Digitaler Verbraucherschutz

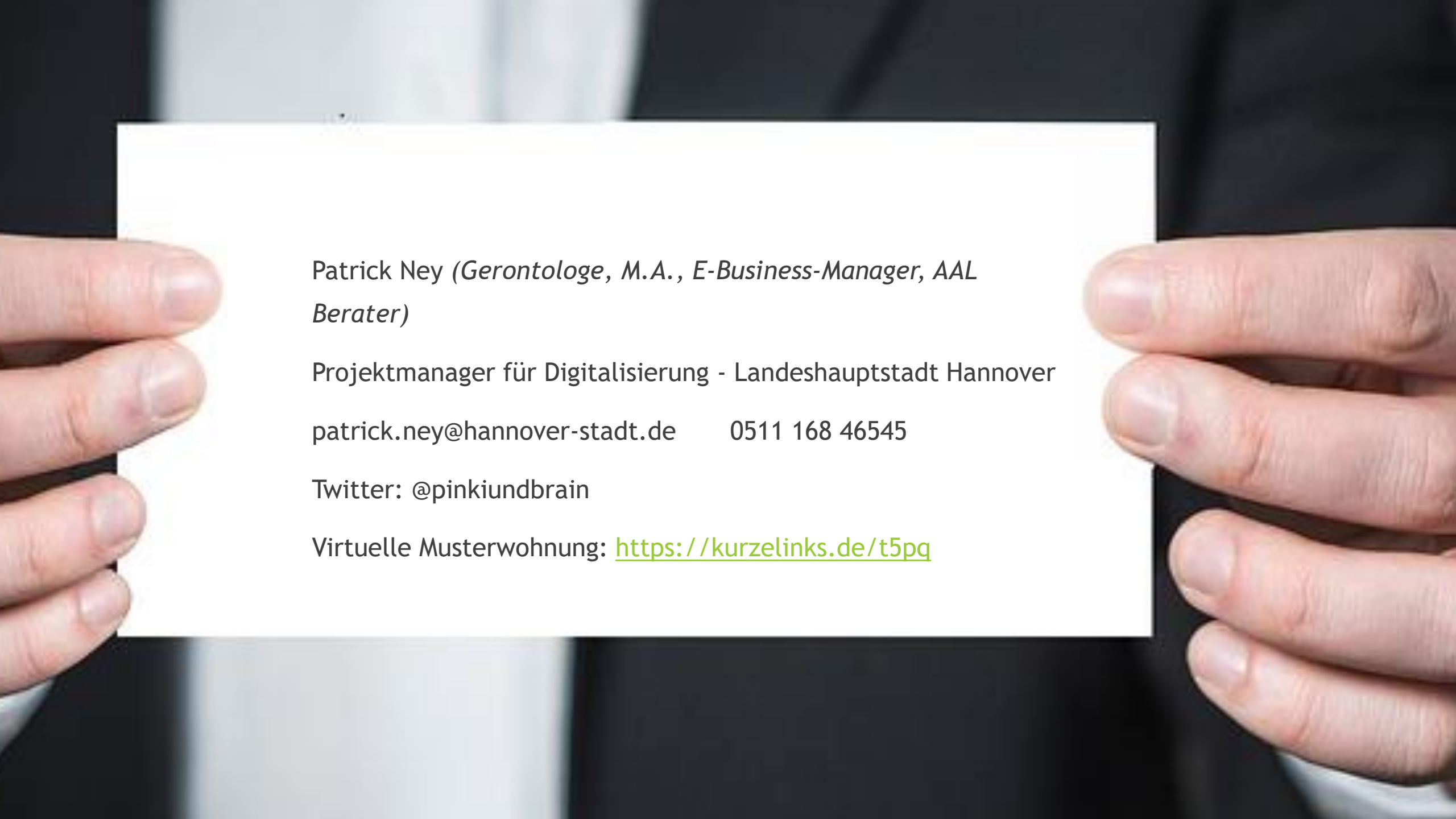
- „Security by Design“ Ansatz durchsetzen
- Verbraucher*innen präventiv über Sicherheitsthemen und Sicherheitsvorfälle informieren
- über Sicherheitssiegel Orientierung bieten
- Data Literacy bei Bürger*innen ausbauen zur Entscheidungsfindung
  - *Data Literacy: Fähigkeit planvoll mit Daten umzugehen und sie im jeweiligen Kontext einzusetzen und hinterfragen zu können*
- Kommunikation über DSGVO ändern - bürgerrechtliche Errungenschaft anstatt bürokratische Last

Quelle: BSI: Das Internet der Dinge sicher nutzen; https://www.stifterverband.org/data-literacy-education

Treffen Sie bewusst Entscheidungen!

Empfehlung von Verbraucherorganisationen und Verbraucherschutzministerien: Informieren Sie sich vorab über verschiedene Anbieter auf dem Markt und vergleichen Sie deren AGB um einen sicheren Anbieter zu wählen.

Was meinen Sie dazu?



Patrick Ney *(Gerontologe, M.A., E-Business-Manager, AAL Berater)*

Projektmanager für Digitalisierung - Landeshauptstadt Hannover

patrick.ney@hannover-stadt.de 0511 168 46545

Twitter: @pinkiundbrain

Virtuelle Musterwohnung: https://kurzelinks.de/t5pq