Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

IT-Sicherheitsmanagement in Haushalten (ISiH)

Risiken, Problemstellungen, Lösungsansätze

erstellt von
Certitude Consulting GmbH

Abschlussbericht zum Projekt ISiH im Auftrag des Bundesamts für Sicherheit in der Informationstechnik (BSI)

Herausgeber:
Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn

E-Mail: bsi@bsi.bund.de
Internet: https://www.bsi.bund.de

Durchführung der Studie:
Certitude Consulting GmbH
Werner Riegler
Marc Nimmerrichter
Wolfgang Ettlinger
Barichgasse 40-42, Top 101 B40
1030 Wien
office@certitude.consulting

unter Mitarbeit von Thomas Fischer, Hassan Mohammad, Alexander Hurbean

Abschlussdatum:
November 2025

Inhalt

1 Management Summary

1.1 Ausgangslage und Zielsetzung des Projekts

Das Projekt „IT-Sicherheitsmanagement in Haushalten: Risiken, Problemstellungen, Lösungsansätze“ (ISiH) verfolgte das Ziel, ein tragfähiges, praxisnahes und nachvollziehbares Konzept zu entwickeln, das zeigt, wie IT-Sicherheit für Mehrpersonenhaushalte systematisch analysiert und realistisch gestaltet werden kann. Während Informationssicherheit in Unternehmen und Behörden auf etablierten Standards, formalen Prozessen und klaren Zuständigkeiten beruht, ist sie in privaten Mehrpersonenhaushalten bislang weitgehend ungeregelt. Dennoch steigt gerade dort die digitale Abhängigkeit rapide. Online-Dienste, mobile Anwendungen, vernetzte Geräte und Cloud-Speicher, wobei manches von dem Genannten gegebenenfalls von mehreren Personen im Haushalt genutzt wird, sind zu festen Bestandteilen des Alltags geworden. Daraus resultiert ein wachsender Bedarf an Schutzmechanismen gegen böswillige interne und externe Akteure die sowohl technisch wirksam als auch für Laien umsetzbar sind.

Vor diesem Hintergrund zielte das Projekt darauf ab, grundlegende Prinzipien des Informationssicherheitsmanagements auf den privaten Kontext zu übertragen. Der Fokus lag dabei auf den Möglichkeiten zur Umsetzung eines Berechtigungsmanagements. Die diesbezüglichen Voraussetzungen unterscheiden sich naturgemäß bei Mehrpersonenhaushalten wesentlich von jenen der Unternehmen. Der Ansatz war bewusst interdisziplinär gewählt und verband insbesondere technische und organisatorische Perspektiven. Im Laufe des Projekts wurde diesbezüglich der Bogen auf psychologische und gesellschaftliche Aspekte gespannt. Das Projekt verfolgte dabei nicht das Ziel, neue Sicherheitstechnologien zu entwickeln, sondern bewährte technische und organisatorische Maßnahmen auf seine Übertragbarkeit, Verständlichkeit und Anwendbarkeit zu prüfen. Informationssicherheit in privaten Mehrpersonenhaushalten wurde im Projektverständnis schlussendlich als sozio-technisches System begriffen, also als Zusammenwirken von Technik, Organisation und Mensch.

Der gesamte Projektverlauf war inhaltlich und methodisch so aufgebaut, dass die einzelnen Arbeitspakete aufeinander aufbauten und sich gegenseitig ergänzten. Im Mittelpunkt stand die schrittweise Entwicklung eines an privaten Mehrpersonenhaushalten angepassten IT-Sicherheitsmanagements: Ausgehend

- von der Sammlung und Bewertung bestehender Maßnahmen über
- die Entwicklung einer systematischen Risikoanalyse für Privathaushalte,
- der Abhaltung eines Expertenworkshops zur Identifikation von Risiken und Diskussion von Verantwortlichkeiten bis hin
- zur Erarbeitung konzeptioneller Szenarien und Handlungsempfehlungen.

Durch die abgestimmte Struktur konnte ein geschlossener Erkenntnisprozess etabliert werden, der die Ergebnisse aufeinander bezieht und die Nachvollziehbarkeit gewährleistet.

1.2 Zentrale Erkenntnisse des Projekts

Die Ergebnisse des Projekts verdeutlichen, dass IT-Sicherheit in Privathaushalten ein vielschichtiges Phänomen ist, das technische, soziale und organisatorische Dimensionen untrennbar miteinander verbindet.

Ein erster zentraler Befund betrifft die Übertragbarkeit bestehender Standards auf den privaten Kontext. Zwar lassen sich viele Best Practices aus dem Unternehmensbereich grundsätzlich anwenden, sowohl ihre Wirksamkeit sowie Anwendbarkeit hängt jedoch stark von den Rahmenbedingungen ab. Maßnahmen, die in Organisationen auf klare Rollenverteilungen und institutionelle Kontrolle treffen, scheitern im privaten Umfeld oft an fehlendem Bewusstsein für Zuständigkeiten, eingeschränkter Kompetenz oder begrenzten Ressourcen. Daher müssen Empfehlungen an die Lebensrealität der Haushalte angepasst werden. Mit der bereits verfügbaren Literatur hinsichtlich Best Practices für Privatpersonen kann zumindest ein

umfassender Katalog an Maßnahmen erstellt werden. Sie unterscheiden sich jedoch erheblich in ihrer potenziellen Anwendbarkeit und dem Nutzen-Aufwand-Verhältnis. Dieser Umstand schränkt die Handlungsmöglichkeiten seitens Privatpersonen für die Umsetzung von IT-Sicherheitsmaßnahmen grundsätzlich ein, da eine Implementierung nicht immer ein realistisches Szenario darstellt.

Die entwickelte Risikoanalyse zeigte, dass Privathaushalte einer Vielzahl von Bedrohungen ausgesetzt sind, die sich teilweise erheblich von Informationssicherheitsrisiken für Unternehmen unterscheiden. Neben externen Angriffen spielen interne Risiken, etwa durch gemeinsam genutzte Geräte, geteilte Passwörter oder familiäre Machtverhältnisse eine zentrale Rolle. Besonders bedeutsam sind Risiken, die aus der ungleichen Verteilung technischer Zuständigkeiten resultieren. Der Ausfall oder das Fehlverhalten einer einzigen Person kann erhebliche Auswirkungen auf den gesamten Haushalt haben.

Der Expertenworkshop ergänzte diese technischen und methodischen Erkenntnisse um sozialwissenschaftliche Perspektiven. Die Diskussionen machten deutlich, dass Sicherheitsverhalten immer in sozialen Kontexten stattfindet. Vertrauen, Abhängigkeiten zu anderen Personen, Wissensgefälle und Machtverhältnisse beeinflussen maßgeblich, wie Sicherheitsmaßnahmen wahrgenommen und umgesetzt werden. Den Erfahrungen der Fachpersonen nach ist die Rollenverteilung in Privataushalten häufig geschlechtsspezifisch geprägt. Dieser Umstand kann als Ausdruck des sogenannten „*Digital Gender Gap*“ gedeutet werden. Im Rahmen des Expertenworkshops wurde zudem eine Hypothese aufgestellt, die vier grundlegende Voraussetzungen für die Akzeptanz und Umsetzung von Sicherheitsmaßnahmen festlegt: Wissen, Zeit, Geld und Motivation. Um ungleich verteiltes Wissen in der breiten Gesellschaft hinsichtlich Informationssicherheit entgegenzuwirken, wurde ein deutlicher Bedarf an niederschwelliger, verständlicher Information identifiziert. Die Fachpersonen sahen es als Notwendigkeit an, dass das Bewusstsein über Bedrohungen im digitalen Raum bereits im Schulalter geschaffen werden muss. Eine weitere Erkenntnis aus dem Expertenworkshop war die Heterogenität von Privathaushalten, mit welcher individuelle Anforderungen hinsichtlich der Gewichtung von Budget und verfügbarer Zeit einhergehen.

Ein weiterer Befund betrifft den Zusammenhang zwischen Anwendbarkeit und Sicherheit, insbesondere im Bereich des Berechtigungsmanagements. Maßnahmen, die zu komplex oder zu aufwändig sind, werden in der Praxis kaum umgesetzt. Daraus ergibt sich die Notwendigkeit, technische Schutzmaßnahmen, welche lediglich von den Herstellern digitaler Produkte umsetzbar sind, so zu gestalten, dass sie ohne vertiefte Fachkenntnis genutzt werden können. Eine entsprechende Nutzung seitens der Privatanwender findet idealerweise automatisiert, mit klarer Rückmeldung und minimaler Interaktion statt.

Schließlich zeigten die drei in Arbeitspaket (AP) 05 untersuchten Szenarien, dass IT-Sicherheit im privaten Umfeld nur dann nachhaltig erreicht werden kann, wenn Verantwortung und Handlungsspielräume klar verteilt sind. Haushalte können durch bewusste Verhaltensänderungen und Routinen einen wichtigen Beitrag leisten, doch sie dürfen mit dieser Aufgabe nicht allein gelassen werden. Hersteller tragen die Verantwortung, Produkte so zu gestalten, dass sie standardmäßig sicher konfiguriert an den Kunden geliefert werden und zugleich benutzbar sind. Für die Bewertung der Anwendbarkeit von IT-Sicherheitsfunktionen kann das Konzept der „*Usable Security*“ (BSI, 2025b) herangezogen werden. Dazu muss die Politik allerdings den Rahmen schaffen, indem Sicherheit zur Standardanforderung und nicht zum freiwilligen Zusatz wird.

1.3 Handlungsorientierte Schlussfolgerungen

Aus den Projektergebnissen lässt sich ableiten, dass IT-Sicherheit in Privathaushalten auf drei Ebenen gleichzeitig gedacht werden muss. Jede der individuellen (Person), der technischen (Hersteller) und der regulatorischen Ebenen (Gesetzgeber) trägt auf eigene Weise zur Gesamtsicherheit bei, wobei keine Ebene für sich die anderen vollständig ersetzen kann, sondern gegenseitig voneinander abhängig sind.

Auf der individuellen Ebene kommt es darauf an, Verantwortlichkeiten im Haushalt zu klären und Sicherheitsmaßnahmen als wiederkehrende Routinen zu etablieren. Passwörter, Datensicherungen, Updates und Zugriffsrechte sollten regelmäßig überprüft werden. Insbesondere bei gemeinschaftlich genutzten Geräten und Diensten ist ein angemessenes Berechtigungsmanagement vorzusehen. So bietet

beispielsweise die Anlage eines zweiten Administratorkontos auf diesen Geräten die Möglichkeit, einen potenziellen Ausfall der hauptverantwortlichen Person zu kompensieren.

Aufgrund der Heterogenität von Privathaushalten und damit einhergehenden spezifischen Anforderungen ist ein risikobasierter Ansatz notwendig, um zielgerichtet Maßnahmenempfehlungen an die Haushalte weitergeben zu können. Mit einem systematischen Risikoanalyseprozess, wie er in diesem Projekt entwickelt wurde, besteht grundsätzlich die Möglichkeit für die Identifikation und Priorisierung von effektiven Maßnahmen unter Berücksichtigung individueller Rahmenbedingungen.

Auf der technischen Ebene müssen Hersteller und Anbieter ihre Produkte nach den Prinzipien *security by design*[1], *security by default*[2] und *„Usable Security“* (BSI, 2025b) gestalten. Sicherheit darf nicht von der Eigeninitiative der Nutzenden abhängen, sondern muss integraler Bestandteil der technischen Architektur sein. Dazu gehören sichere Voreinstellungen, automatische Aktualisierungen, moderne Verschlüsselungsstandards und klare Rechteverwaltung. Transparente Benutzerführung und barrierefreie Gestaltung erhöhen nicht nur die Benutzerfreundlichkeit, sondern auch die Akzeptanz und Effektivität von Sicherheitsfunktionen.

Schließlich ist auf der regulatorischen Ebene der Gesetzgeber gefordert, Mindeststandards festzulegen und deren Einhaltung zu überwachen. Einheitliche Zertifizierungen und transparente Kennzeichnungen können Privatpersonen eine Orientierung bei ihrer Kaufentscheidung bieten und das Vertrauen in digitale Produkte stärken. Ergänzend sollte die Politik Bildung und Forschung fördern, um langfristig digitale Selbstschutzkompetenz in der Bevölkerung aufzubauen.

1.4 Gesamtbewertung und Ausblick

Die entwickelten Instrumente, insbesondere die Maßnahmentabelle und die Risikoanalyse, bieten eine strukturierte Grundlage für die Identifizierung, Erkennung und Bewertung von Risiken eines Privathaushalts. Gleichzeitig verdeutlicht das Projekt, dass technische Lösungen nur dann wirken, wenn sie in ein organisatorisches und soziales Gefüge eingebettet sind.

Die Ergebnisse sind damit nicht allein als theoretischer Beitrag zu verstehen, sondern als Ausgangspunkt für praxisorientierte Weiterentwicklungen. Sie können in der Verbraucherbildung, in der Produktentwicklung sowie in politischen Initiativen zur Förderung von IT-Sicherheitskompetenz eingesetzt werden. Besonders vielversprechend erscheint die Weiterentwicklung des Risikoanalyse-Tools zu einem interaktiven, web- oder appbasierten Instrument, welches Haushalte durch die Eingabe von wenigen Daten, beispielsweise der verwendeten Assets und der Haushaltszusammensetzung, gezielt Maßnahmen zur Erhöhung der IT-Sicherheit vorschlägt.

Langfristig leistet das Projekt einen Beitrag dazu, IT-Sicherheit als gemeinsame gesellschaftliche Aufgabe zu etablieren. Die im Projekt gewonnenen Erkenntnisse und Empfehlungen sind hilfreich für künftige Strategien, Fördermaßnahmen und Forschungsprogramme, die darauf abzielen, Privathaushalte zu befähigen, ihre digitale Umgebung sicher, selbstbestimmt und nachhaltig zu gestalten.

[1] „security by design“ gewährleistet, dass bereits im Zuge der Konzeption und Entwicklung die Sicherheit in Systemen und Diensten integriert wird.

[2] „security by default“ gewährleistet die standardmäßig sichere Konfiguration von Systemen und Diensten.

2 Einleitung

Die fortschreitende Digitalisierung prägt zunehmend alle Lebensbereiche. Digitale Technologien sind längst nicht mehr nur in Arbeits- und Unternehmenskontexten allgegenwärtig, sondern haben den privaten Lebensraum in einem hohen Maß durchdrungen. Smartphones, Smarthome-Systeme, Cloud-Dienste, Online-Banking und vernetzte Haushaltsgeräte bestimmen den Alltag vieler Menschen und bilden ein dichtes Netz aus Informationsflüssen, personenbezogenen Daten und Kommunikationsschnittstellen.

Diese Entwicklung eröffnet einerseits neue Formen von Komfort, Flexibilität und gesellschaftlicher Teilhabe, andererseits entsteht eine wachsende Abhängigkeit von digitalen Systemen, die auch im häuslichen Umfeld mit Risiken verbunden ist, insbesondere wenn es sich dabei um Mehrpersonenhaushalten handelt.

Während Unternehmen und Behörden längst über formal geregelte Prozesse des Informationssicherheitsmanagements verfügen, fehlen in privaten Mehrpersonenhaushalten häufig vergleichbare Strukturen. Schutzmaßnahmen werden dort meist reaktiv, situativ, intuitiv oder gar nicht umgesetzt. Hinzu kommt, dass technische Kenntnisse, Sicherheitsbewusstsein und Risikowahrnehmung innerhalb eines Haushalts stark variieren können. Dadurch entstehen organisatorische Lücken und Verantwortungsdiffusion, die Angreifern, sowohl von extern als auch intern, neue Angriffspunkte bieten.

Vor diesem Hintergrund gewinnt die Frage an Bedeutung, wie sich ein IT-Sicherheitsmanagement auch im privaten Bereich systematisch, methodisch nachvollziehbar und alltagstauglich gestalten lässt.

Das Projekt „IT-Sicherheitsmanagement in Haushalten: Risiken, Problemstellungen, Lösungsansätze“ (ISiH) setzte genau an dieser Fragestellung an. Es untersuchte, welche Methoden, Werkzeuge und Konzepte erforderlich sind, um die Prinzipien des Informationssicherheitsmanagements aus der Privatwirtschaft und dem behördlichen Bereich in den häuslichen Kontext zu übertragen. Dabei stand weniger die Entwicklung technischer Innovationen im Vordergrund als vielmehr die Übertragbarkeit bestehender Modelle auf reale, soziale Strukturen innerhalb von privaten Mehrpersonenhaushalten. Der Fokus lag dabei auf der möglichen Umsetzung eines Berechtigungsmanagements innerhalb von Privathaushalten, um insbesondere spezifischen Risiken bei der gemeinschaftlichen Nutzung von Geräten und digitalen Diensten zu begegnen.

Informationssicherheit wurde somit nicht rein als technisches Konstrukt, sondern als ein Zusammenspiel aus Technik, Verhalten, Organisation und Verantwortung betrachtet.

2.1 Projektinhalte und Arbeitspakete

Das Projekt gliederte sich in vier zentrale Arbeitspakete. Jedes Paket stellte eine inhaltliche und methodische Weiterentwicklung des vorherigen dar und erweiterte die Perspektive auf IT-Sicherheit im privaten Raum. Im Mittelpunkt stand die schrittweise Entwicklung eines an privaten Mehrpersonenhaushalten angepassten IT-Sicherheitsmanagements, welches insbesondere die Anforderungen für ein Berechtigungsmanagement behandelt und abdeckt.

In Arbeitspaket (AP) 02 „Best Practices“ wurde die Identifikation, Kategorisierung und Bewertung bewährter Sicherheitsmaßnahmen vorgenommen. Eine Literaturrecherche nationaler und internationaler Quellen diente als Grundlage für das Arbeitspaket. Aus den analysierten Dokumenten wurden 52 konkrete Maßnahmen extrahiert und fünf zentralen Themenbereichen zugeordnet: Accountsicherheit und Authentisierung, Benutzergeräte, Heimnetzwerk, Datensicherheit & Privatsphäre und IoT / Smarthome. Die Maßnahmen wurden hinsichtlich Vor- und Nachteile, ihrer Anwendbarkeit sowie ihres Verhältnisses von Nutzen zu Aufwand bewertet. Um eine praxisnahe Beurteilung zu ermöglichen, wurde ein fiktiver „Beispiel-Haushalt“ entworfen, welcher verschiedene Altersgruppen, technische Fähigkeiten und Nutzungsszenarien für digitale Produkte repräsentierte. Bei der Definition dieses fiktiven Haushalts wurden die Aussagen von

Personen aus Interviews eines vorangegangenen BSI-Projekts[3] herangezogen. Als Referenzmodell bildete der definierte Haushalt in der Folge den Ausgangspunkt für die Risikoanalyse und alle nachfolgenden Projektphasen.

Das darauf aufbauende Arbeitspaket „Risikoanalyse für Privathaushalte“ (AP03) hatte das Ziel, bewährte Verfahren der Risikoanalyse, wie etwa jene der ISO/IEC 27005 oder des BSI-Standards 200-3 an die spezifischen Gegebenheiten von privaten Mehrpersonenhaushalte anzupassen. Das Ergebnis war ein vereinfachter, aber nachvollziehbarer Prozess zur Identifikation, Bewertung und Behandlung von Risiken. Der systematische Ansatz dieses Risikoanalysekonzepts bietet die Möglichkeit zur Implementierung von Automatismen, welche wiederum eine toolgestützte und effiziente Umsetzung ermöglichen. Dies wurde anhand einer durchgeführten Risikoanalyse anhand des Beispiel-Haushalts im Rahmen des Projekts demonstriert.

Im Rahmen des Arbeitspakets „Organisation von IT-Sicherheit in Privathaushalten“ (AP04) wurde ein Expertenworkshop abgehalten, um die theoretischen Annahmen der Risikoanalyse mit praktischen Erfahrungen aus der Lebensrealität unterschiedlicher Zielgruppen abzugleichen. Acht Fachpersonen aus den Bereichen Verbraucherschutz, Gleichstellung, inklusive Digitalisierung, Pflege, finanzielle Bildung und Verbrechensopferhilfe diskutierten aktuelle Sicherheitspraktiken, Herausforderungen bei der Umsetzung von Sicherheitsmaßnahmen, die Heterogenität von Privathaushalten und deren spezifischen Anforderungen sowie Verantwortlichkeiten im häuslichen Umfeld. Basierend auf den Erkenntnissen des Expertenworkshops wurden konkrete Anwendungsfälle und Bedrohungen für Mehrpersonenhaushalte abgeleitet, welche die Notwendigkeit eines Berechtigungsmanagement verdeutlichen.

Im abschließenden Arbeitspaket „Konzeptentwicklung“ (AP05) wurden unterschiedliche Handlungsperspektiven für ein IT-Sicherheitsmanagement in Privathaushalten aus drei verschiedenen Blickwinkeln entwickelt und bewertet. Dabei wurden die Möglichkeiten und Grenzen zur Umsetzung eines IT-Sicherheitsmanagements durch die Haushalte, Hersteller und Anbieter von digitalen Produkten sowie dem Gesetzgeber isoliert untersucht. Die Analyse konnte nachvollziehbar zeigen, dass bei einer einseitigen Umsetzung von Sicherheitsmaßnahmen wesentliche Restrisiken verbleiben. Erst durch das Zusammenspiel von Verhalten, Technik und Regulierung kann ein andauerndes und angemessen wirksames Sicherheitsniveau für private Mehrpersonenhaushalte erreicht werden.

Durch diese aufeinander abgestimmte Projektstruktur konnte ein geschlossener Erkenntnisprozess etabliert werden, der die Ergebnisse aufeinander bezieht und die Nachvollziehbarkeit gewährleistet.

2.2 Berichtsstruktur

Die nachfolgenden Kapitel im vorliegenden Bericht spiegeln den projektumspannenden Bogen in Form der Arbeitspakete wider. Zunächst werden in Kapitel 3 die methodischen Grundlagen und Ergebnisse der Best-Practice-Analyse vorgestellt, die den Maßnahmenkatalog für die restlichen Arbeitspakete bildet. Kapitel 4 beschreibt die Entwicklung und Anwendung eines Risikoanalysekonzepts für Privathaushalte, das die Grundlage für alle weiteren Arbeiten schafft. Kapitel 5 widmet sich den empirischen Erkenntnissen aus dem Expertenworkshop und stellt aufgrund dessen Erkenntnisse die wichtigsten sozialen Einflussfaktoren auf IT-Sicherheitsverhalten dar. Darauf aufbauend beschreibt Kapitel 6 anhand typischer Anwendungsfälle, wie ein Berechtigungsmanagement in Mehrpersonenhaushalten funktionieren könnte. Kapitel 7 präsentiert schließlich die aus allen Arbeitspaketen abgeleiteten Konzepte und Szenarien für ein IT-Sicherheitsmanagement im privaten Bereich, bevor Kapitel 8 die wesentlichen Empfehlungen für Privathaushalte, Hersteller und Anbieter sowie Politik zusammenführt.

Jedes dieser Kapitel ist grundsätzlich in folgende Abschnitte gegliedert:

[3] Eine Zusammenfassung des BSI-Projektes ist hier zu finden: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/DVS-Berichte/Studie_Haushaltsbefragung.html

1. Zielsetzung und Ausgangslage
2. Methodisches Vorgehen
3. Ergebnisse
4. Diskussion der Ergebnisse und Fazit

Der vorliegende Bericht enthält eine konsistente Argumentationslinie, die von der Analyse über die Anwendung bis hin zur Handlungsempfehlung reicht. Er liefert nicht nur Einzelergebnisse, sondern zeigt, wie diese miteinander verknüpft sind und sich gegenseitig ergänzen: von der Frage

- *„Welche Maßnahmen sind im privaten Kontext grundsätzlich sinnvoll?“* (AP02), über
- *„Welche Risiken bestehen für private Haushalte und wie lassen sich diese systematisch analysieren, bewerten und behandeln?“* (AP03), bis hin zu
- *„Wie können Privatpersonen, Hersteller und Politik gemeinsam zu einer sicheren digitalen Lebenswelt beitragen?“* (AP05).

Damit versteht sich dieser Abschlussbericht nicht lediglich als Ergebnisdokumentation, sondern als konzeptioneller Beitrag zur Weiterentwicklung des Verständnisses von IT-Sicherheit im privaten Raum mit dem Ziel, langfristig Strukturen zu schaffen, die den Schutz im digitalen Raum zu einer selbstverständlichen und sozial verankerten Alltagsaufgabe machen.

3 Ergebnisse aus AP02: Best Practices

3.1 Zielsetzung und Ausgangslage

Dieses Arbeitspaket bildete die methodische und inhaltliche Grundlage für die weiteren Arbeitspakete des Projekts „IT-Sicherheitsmanagement in Haushalten“ (ISiH). Ziel war die Identifikation, Strukturierung und Bewertung bestehender, bewährter Praktiken („Best Practices“) im Bereich des IT-Sicherheitsmanagements, die sich auf den spezifischen Kontext von Privathaushalten übertragen lassen.

Während für Organisationen und Unternehmen bereits eine Vielzahl von Standards, Normen und Handlungsempfehlungen existieren (beispielsweise ISO/IEC 27001, BSI IT-Grundschutz), fehlen vergleichbar systematische Ansätze für private Haushalte. Diese Lücke sollte durch die Erarbeitung einer strukturierten Maßnahmenbasis geschlossen werden, die sich in späteren Arbeitspaketen für den Risikoanalyseprozess und die Entwicklung von Konzepten für ein IT-Sicherheitsmanagement nutzen lässt.

Das Arbeitspaket verfolgte somit die folgenden Teilziele:

- Durchführung einer Literaturrecherche und Analyse vorhandener Leitfäden und Empfehlungen
- Ableitung und Beschreibung von Best Practices, die für Privathaushalte anwendbar sind
- Bewertung dieser Maßnahmen anhand von Kriterien zur Anwendbarkeit und zum „Nutzen-Aufwand-Verhältnis“
- Kategorisierung der Maßnahmen in praxisnahe Themenfelder
- Definition eines „Beispiel-Haushalts“ als Referenzmodell zur späteren Anwendung und Bewertung der Maßnahmen in realistischen Nutzungsszenarien

Die Ergebnisse aus diesem Arbeitspaket dienten in den nachfolgenden Projektphasen als zentrale Grundlage zur Behandlung konkreter Risiken (AP03), zur Diskussion im Expertenworkshop (AP04) sowie zur Entwicklung von Konzepten für ein IT-Sicherheitsmanagement für Privathaushalte (AP05).

3.2 Methodisches Vorgehen

Zur Erhebung der Best Practices wurde eine Literaturrecherche durchgeführt. Die Recherche umfasste sowohl nationale als auch internationale Quellen, die Empfehlungen zur IT-Sicherheit im privaten Umfeld bereitstellen. Zu den **primären** Quellen zählten insbesondere:

- **Bundesamt für Sicherheit in der Informationstechnik (BSI):** Veröffentlichungen und Informationsangebote für Verbraucherinnen und Verbraucher (unter anderem: Cybersicherheitsmonitor (BSI, 2024a), Tipps für Smarthome & IoT-Geräte (BSI, 2025c), Empfehlungen zur Passwortgestaltung (BSI, 2025f))
- **A-SIT Zentrum für sichere Informationstechnologie – Austria**: Inhalte der Plattform *onlinesicherheit.gv.at* des österreichischen Bundeskanzleramts, insbesondere die Bereiche „Prävention“ und „Sicherheitstipps“ (BKA und A-SIT, 2025).
- **National Security Agency (NSA, USA)**: kompakter Leitfaden “*Best Practices for Securing Your Home Network*” (NSA, 2023).
- **Wissenschaftliche Publikationen**: *Cyber Security @ Home: The Effect of Home User Perceptions of Personal Security Performance on Household IoT Security Intentions* (Mitchell, 2020).

Aus diesen und weiteren Quellen wurden relevante Maßnahmen extrahiert, zusammengeführt und inhaltlich harmonisiert. Ergänzend erfolgte die Einbindung bestehender Praxiserfahrungen der Projektmitarbeitenden sowohl seitens des Auftraggebers als auch des Auftragnehmers.

Zur Strukturierung der Ergebnisse wurde eine Maßnahmentabelle erstellt, die sämtliche identifizierten Maßnahmen in einer einheitlichen Form dokumentiert. Die Tabelle enthält für jede Maßnahme:

- eine Kurzbeschreibung,
- identifizierte Vor- und Nachteile,
- Einschätzungen zur Anwendbarkeit
- Bewertung des Nutzen-Aufwand-Verhältnisses,
- potenziell geschützte Assets,
- technische Voraussetzungen,
- nicht berücksichtigte Aspekte und offensichtliche Restrisiken sowie
- die Quellen, welche die jeweilige Maßnahme als Best Practice anführen.

Die Tabelle bildete damit das zentrale Werkzeug zur nachvollziehbaren Bewertung der Eignung und Wirksamkeit einzelner Maßnahmen im privaten Umfeld.

3.3 Der Beispiel-Haushalt als Referenzmodell

Zur praxisorientierten Anwendung der Best Practices wurde im Rahmen des Arbeitspakets ein fiktiver „Beispiel-Haushalt“ definiert. Dieser Haushalt sollte ein möglichst realistisches, zugleich aber neutral generalisierbares Abbild typischer digitaler Nutzungssituationen in privaten Mehrpersonenhaushalten darstellen.

Der Beispiel-Haushalt (siehe Tabelle 1) bestand aus fünf fiktiven Personen unterschiedlicher Altersgruppen und technischer Kompetenzen. Für jede Person wurden die persönlichen und gemeinschaftlich genutzten Geräte, deren Nutzungsaktivitäten, Hobbys und Interessen sowie ergänzende Aussagen dokumentiert. Die Aussagen der Personen, deren genutzte Geräte sowie Dienste basierten zum Großteil auf einer durchgeführten Haushaltsbefragung aus einem vorangegangenen BSI-Projekt[4].

Tabelle 1 Übersicht der Personen im „Beispiel-Haushalt“

Bewohner	***Alter***	***Rolle im Haushalt***	***Technische Affinität / Besonderheiten***
Sven	43 Jahre	Vater, berufstätig, technisch versiert	Verantwortlich für Heimnetzwerk und Smarthome; verfügt über ansatzweises Wissen über IT-Sicherheitspraktiken (sicherer Umgang mit Passwörtern)
Birgit	44 Jahre	Mutter, berufstätig	nutzt digitale Produkte hauptsächlich für Kommunikation und Online-Banking
Maja	21 Jahre	Tochter, Studentin	Nutzung sozialer Medien und Streaming-Dienste; Verwendet digitale Produkte für Recherchen, Kommunikation und Gaming
Adrian	12 Jahre	Sohn, Schüler	nutzt digitale Produkte für Gaming, Kommunikation und Streaming; hat nur eingeschränkten Zugriff auf digitale Dienste und ist von diesem Umstand genervt
Franziska	68 Jahre	Großmutter	nutzt ihr Smartphone hauptsächlich für Kommunikation; besitzt eine digitale Notrufuhr, welche ihr aufgrund von Vorerkrankungen ein besseres Gefühl von Sicherheit gibt

[4] Eine Zusammenfassung des BSI-Projektes ist hier zu finden: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/DVS-Berichte/Studie_Haushaltsbefragung.html

Dieses Referenzmodell erlaubte eine konsistente Untersuchung der Anwendbarkeit und Wirksamkeit von Maßnahmen, indem technische und soziale Aspekte der Haushaltsstruktur gleichermaßen berücksichtigt wurden. Der Beispiel-Haushalt diente in allen folgenden-Arbeitspaketen (AP03–AP05) als Referenz, um Vergleichbarkeit und Anschlussfähigkeit der Ergebnisse zu ermöglichen.

3.4 Ergebnisse der Literaturrecherche und Maßnahmenkategorisierung

Insgesamt wurden 52 Maßnahmen identifiziert und in fünf übergeordnete Kategorien eingeordnet. Die Auswahl der Kategorien ergab sich sinngemäß aus der Natur der identifizierten Maßnahmen und sollte zentrale Schutzbereiche des privaten digitalen Umfelds darstellen. Die Kategorisierung und Liste der Maßnahmen fokussieren sich auf die meist genannten Maßnahmen zum Zeitpunkt der Untersuchung und sind nicht abschließend, da sich Sicherheitsempfehlungen individuell am volatilen Markt der Verbraucherprodukte anpassen können. Die nachfolgende Tabelle 2 listet einige beispielhafte Maßnahmen für jede Kategorie auf.

Tabelle 2 Kategorien der Maßnahmen inklusive Beispiele

Kategorie	***Beispiele für Maßnahmen***	***Anzahl der Maßnahmen***
Accountsicherheit & Authentisierung	Multi-Faktor-Authentisierung, Passwortloses Anmelden (Passkeys), Nutzung eines Passwortmanager	6
Benutzergeräte	Software- und Systemupdates, Verteilung von Administrationsberechtigungen auf mehrere Personen, Trennung zwischen Standard-Benutzerkonten und Administrationskonten, Installation einer Anti-Virus-Software	10
Heimnetzwerk	Verwendung von modernen WLAN-Verschlüsselungsstandards, Änderung von Standardpasswörtern, Trennung von Netzwerken	13
Datensicherheit & Privatsphäre	regelmäßige Datensicherung, Zugriffsschutz für Datensicherungen, Verschlüsselung von Daten, Festplatten und Datensicherungen, App- & Programmzugriffsbeschränkungen auf Daten und Dienste, Abdecken von nicht verwendeten Kameras	12
IoT / Smarthome	Keine Verwendung persönlicher Passwörter für Smarthome- oder IoT-Geräte, automatische Installation von Updates, Funktions- und Berechtigungsprofile für Benutzer	11

Etwa zwei Drittel dieser Maßnahmen wurden in mehreren Quellen übereinstimmend als Best Practices genannt, was ihre Relevanz und allgemeine Anerkennung im Bereich der IT-Sicherheit unterstreicht.

Neben der inhaltlichen Zusammenführung wurden die Maßnahmen auf ihre Konsistenz und Aktualität geprüft. Veraltete oder nicht mehr praktikable Empfehlungen (beispielsweise regelmäßige Passwortänderung ohne Anlass) wurden kontextualisiert und gegebenenfalls angepasst.

3.4.1 Bewertungsansatz

Um die Maßnahmen über eine rein qualitative Beschreibung hinaus vergleichbar zu machen, wurde ein standardisiertes Bewertungsverfahren definiert. Dieses umfasst zwei Kernkriterien:

3.4.1.1 Anwendbarkeit

Die Anwendbarkeit wurde anhand von drei Subkriterien bewertet, welche nachfolgend als Fragen formuliert sind und sich am Konzept der „*Usable Security*“ (BSI, 2025b) orientieren:

- **Robustheit gegen Nutzungsfehler**: Ist die Maßnahme robust gegen Fehler beziehungsweise Fehlkonfigurationen, welche in Folge negative Auswirkungen für das System, den Benutzer oder die IT-Sicherheit haben könnte?
- **Erlernbarkeit**: Kann die Umsetzung der Maßnahme schnell erlernt und produktiv umgesetzt werden?
- **Einfachheit**: Ist die Maßnahme ohne größere Beanspruchung der mentalen, kognitiven und motorischen Fähigkeiten umzusetzen?

Jedes Subkriterium der Anwendbarkeit wurde binär bewertet (1 = zutreffend, 0 = nicht zutreffend), sodass sich eine insgesamte Wertung für die Anwendbarkeit zwischen 0 und 3 ergab. Diese wurde wiederum qualitativ, von „schlecht“ bis „sehr gut“, interpretiert.

3.4.1.2 Nutzen-Aufwand-Verhältnis

Für die Einschätzung des Nutzen-Aufwand-Verhältnisses von Maßnahmen wurde eine 3×3-Matrix definiert, auf der beide Dimensionen des Verhältnisses nach einer subjektiven Einschätzung aufgetragen wurden. Die Matrix inklusive Wertebereiche ist nachfolgend abgebildet (siehe Abbildung 1).

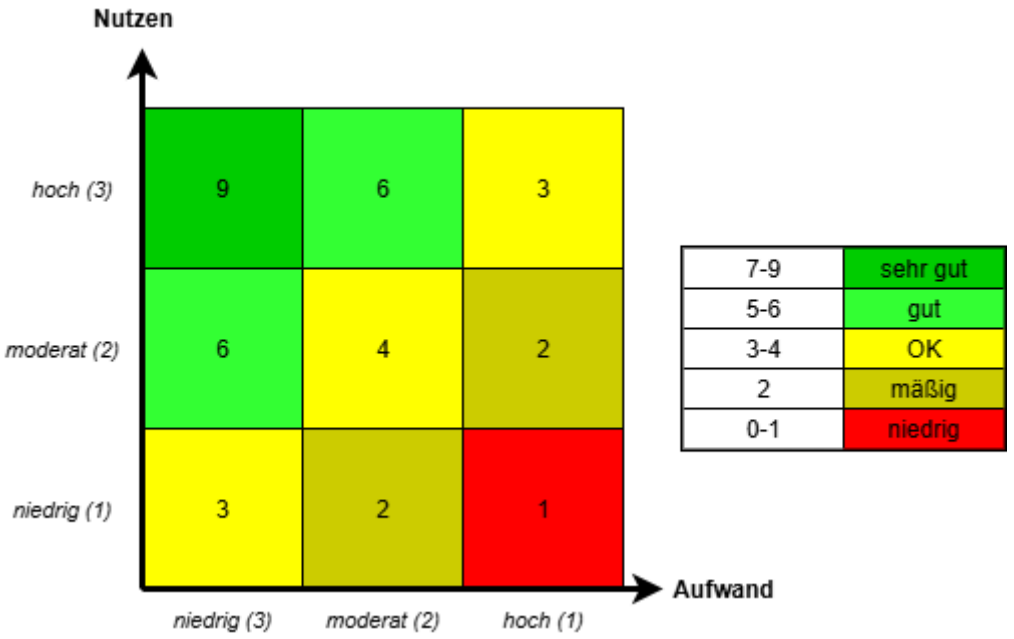

Abbildung 1 Matrix für die Bewertung des Nutzen-Aufwand-Verhältnisses

Auf der X-Achse wird der Aufwand für die initiale und laufende Umsetzung der jeweiligen Maßnahme abgebildet, wobei die Wertigkeit absteigend betrachtet wird (niedrig = 3, hoch = 1). Auf der Y-Achse wird der Sicherheitsnutzen der Maßnahmen mit einer aufsteigenden Wertigkeit (niedrig = 1, hoch = 3) aufgetragen. Das Produkt aus diesen beiden Werten ergibt die quantitative Wertung einer Maßnahme für das Nutzen-Aufwand-Verhältnis. Diese Wertung kann potenziell für die priorisierte Auswahl an Maßnahmen mit hohem Nutzen bei geringem oder moderatem Aufwand herangezogen werden.

Das Bewertungsverfahren wurde im Rahmen gemeinsamer Arbeitstreffen abgestimmt und in der Maßnahmentabelle implementiert. Durch die Kombination aus quantitativer und qualitativer Bewertung konnte ein hohes Maß an Nachvollziehbarkeit erreicht werden, auch wenn die Einschätzung einzelner Parameter notwendigerweise subjektiv blieb.

3.4.2 exemplarische Maßnahme

Die nachfolgende Tabelle 3 zeigt eine exemplarische Maßnahme der Kategorie „IoT / Smarthome“. Die Einträge für „Anwendbarkeit“ und „Nutzen<>Aufwand (Priorisierung)“ ergeben sich aus den jeweiligen Bewertungen gemäß den beschriebenen Methoden aus Abschnitt 3.4.1.

Maßnahmenkategorie: **IoT / Smarthome**

Tabelle 3 exemplarische Maßnahme „Eigene Funktions- und Berechtigungsprofile für jeden Benutzer“ aus der Kategorie „IoT / Smarthome“

Bezeichnung	***Eigene Funktions- und Berechtigungsprofile für jeden Benutzer***
Kurzbeschreibung	Für gemeinsam verwendete Smarthome- und IoT-Geräte sollten Funktionsprofile bzw. Berechtigungsrollen für Benutzer eingerichtet werden. Damit können die persönlichen Daten der Anwendenden vor anderen geschützt werden und die Durchführung von unberechtigten Aktionen gesteuert bzw. verhindert werden. Beispielsweise kann so die Steuerung von kritischen Heimfunktionen (bspw. Heizung, Strom, etc.) geregelt werden oder individuelle Sprachprofile für Smart Speaker und intelligente Assistenzen (bspw. Online-Einkauf über Sprachbefehl) mit einhergehenden Berechtigungen angelegt werden.
Vorteile (+)	• Schutz der persönlichen Daten von Anwendenden • Zugriffsbeschränkung auf kritische Heimfunktionen
Nachteile (-)	• aufwändige Umsetzung und Wartung • potenzieller Interessenskonflikt zwischen den Anwendenden (Berechtigungsvergabe)
Anwendbarkeit	moderat (2)
Nutzen<>Aufwand (Priorisierung)	gut (6)
potenzielle, zu schützende Assets	• kritische Heimfunktionen • persönliche Daten
technische Voraussetzungen	• Geräte müssen über die Möglichkeit zur Definition von Profilen (Funktionen und Berechtigungen) verfügen.
nicht betrachtete Aspekte / potenzielle Risiken	keine
Quelle(n)	• Tipps für den sicheren Umgang mit Smart Speakern (BSI, 2023b) • Understanding and Improving Security and Privacy in Multi-User Smart Homes: A Design Exploration and In-Home User Study. (Zeng, et al., 2019)
Nutzen<>Aufwand: Aufwand (1: hoch - 3: niedrig)"	2
Nutzen<>Aufwand: Nutzen (1: niedrig - 3: hoch)	3
Anwendbarkeit: Robustheit (1: ja, 0: nein)	1
Anwendbarkeit: Erlernbarkeit (1: ja, 0: nein)	1
Anwendbarkeit: Einfachheit (1: ja, 0: nein)	0

Hinweis: Im Anhang A dieses Berichts sind exemplarische Maßnahmen von vier weiteren Maßnahmenkategorien angeführt. Für weiterführende Details kann das BSI kontaktiert werden.

3.5 Diskussion der Ergebnisse & Fazit

Die in AP02 erstellte Maßnahmentabelle und die angewandten Bewertungsmechanismen bilden ein konsistentes Fundament für die Bewertung von IT-Sicherheitsmaßnahmen in Privathaushalten, welche jederzeit erweitert beziehungsweise angepasst werden können. Insbesondere die Methoden zur Bewertung der Anwendbarkeit und des Nutzen-Aufwand-Verhältnisses ermöglichen eine nachvollziehbare Priorisierung von Sicherheitsmaßnahmen, die über rein technische Wirksamkeit hinausgeht und den Faktor Mensch miteinbezieht. Die dafür im Projekt verwendeten Bewertungsschemata bieten die Möglichkeit zur granularen Gestaltung für weiterführende Arbeiten. Die Bewertungen selbst können durch empirisch erhobene Daten im Zuge von weiteren Untersuchungen untermauert und objektiviert werden.

Das Arbeitspaket hat gezeigt, dass viele Best Practices aus publizierten Leitfäden oder Arbeiten für den privaten Bereich relevant sind, jedoch an die spezifischen Rahmenbedingungen von unterschiedlichen Haushaltszusammensetzungen angepasst werden müssen. Unterschiede ergeben sich insbesondere aus:

- der Heterogenität der Nutzergruppen,
- dem Fehlen institutioneller Kontrollmechanismen,
- den unterschiedlichen Wissensständen der Haushaltsmitglieder sowie
- der Abhängigkeit von Geräte- und Dienstanbietern.

Diese Erkenntnisse unterstreichen die Notwendigkeit, technische Sicherheitsmaßnahmen mit benutzerfreundlichen, verständlichen und sozial verträglichen Gestaltungsprinzipien zu kombinieren.

Das umfassende Set an strukturierten, bewerteten und kategorisierten IT-Sicherheitsmaßnahmen diente als Grundlage für die weiteren Projektarbeiten. Die erarbeiteten Bewertungsmechanismen und der Beispiel-Haushalt stellten sicher, dass die Maßnahmen in den folgenden Arbeitspaketen kontextbezogen und konsistent angewendet werden konnten.

Die gewonnenen Erkenntnisse flossen direkt in die Entwicklung eines systematischen Risikoanalyseverfahrens ein, das in AP03 umgesetzt wurde. Dort wurden die in AP02 identifizierten Maßnahmen erstmals in Beziehung zu konkreten Bedrohungsszenarien gesetzt und hinsichtlich ihrer Risikoreduktionswirkung untersucht.

4 Ergebnisse aus Arbeitspaket AP03 – Risikoanalyse für Privathaushalte

4.1 Zielsetzung und Ausgangslage

Dieses Arbeitspaket hatte das Ziel, ein systematisches und methodisch fundiertes Konzept zur Risikoanalyse für Privathaushalte zu entwickeln, das an die spezifischen Rahmenbedingungen von Privathaushalten angepasst ist.

Während sich bestehende Standards wie der BSI-Standard 200-3 oder ISO/IEC 27005 an Organisationen mit klar definierten Prozessen, Rollen und Verantwortlichkeiten richten, sind Privathaushalte durch eine heterogene Zusammensetzung, fehlenden formalen Zuständigkeiten und stark divergierende technische Kompetenzen geprägt.

Vor diesem Hintergrund sollte ein Prozessmodell entworfen werden, das es ermöglicht, Risiken im privaten Umfeld systematisch zu identifizieren, zu analysieren, zu bewerten und zu behandeln. Dabei wurden insbesondere für die Behandlung der Risiken die Erkenntnisse in Form der Maßnahmentabelle aus AP02 berücksichtigt. Das Prozessmodell sollte auch ohne tiefgehende Fachkenntnisse zu Risikomanagementmethoden anwendbar bleiben, um eine spätere praktische Umsetzung in realen Haushalten zu ermöglichen. Darüber hinaus wurde angestrebt, die Risikoanalyse so zu gestalten, dass sie erweiterbar und flexibel bleibt. Das Konzept sollte eine Basis schaffen, auf der spätere Projekte und Untersuchungen aufbauen können. Entsprechend war vorgesehen, den gesamten Prozess nachvollziehbar zu dokumentieren und die Bewertungsschritte möglichst transparent zu gestalten.

Die zentralen Fragestellungen für dieses Arbeitspaket lauteten:

- Wie lässt sich der klassische Risikoanalyseprozess (Identifikation, Analyse, Bewertung, Behandlung) für Privathaushalte vereinfachen, ohne an Aussagekraft zu verlieren?
- Welche Informationswerte und Assets sind im häuslichen Kontext besonders schützenswert?
- Welche typischen Bedrohungen und Angreifertypen lassen sich identifizieren und wie können diese bewertet werden?
- Wie können Maßnahmen aus AP02 in die Risikobehandlung integriert werden?

Damit sollte ein methodisches Bindeglied zwischen den in AP02 erarbeiteten Maßnahmen und den späteren konzeptionellen Szenarien aus AP05 geschaffen werden.

4.2 Methodisches Vorgehen

4.2.1 Definitionen und Begrifflichkeiten

Nachfolgende Begriffe wurden, aufgrund unterschiedlicher Bedeutung in gängigen Normen und Standards, für den Kontext des Arbeitspakets festgelegt.

Risikoanalyse
Der Begriff „Risikoanalyse“ wird entsprechend des BSI-Standards 200-3 als gesamtheitlicher Risikomanagement-Prozess, bestehend aus der Identifikation, der Einstufung und Behandlung von Risikoszenarien verwendet (BSI, 2017 S. 6-7).

IT-Risiko bzw. Risikoszenario
Das „(IT-)Risiko“, „Risikoszenario“, setzt sich gemäß BSI-Standard 200-3 aus einem Asset und einer dafür relevanten Bedrohung zusammen.

Der Unterschied zum „IKT-Risiko“ gem. ISO 27005 besteht darin, dass sich ein IKT-Risiko in der ISO-Norm immer aus einer Schwachstelle, einer Bedrohung und einem IKT-Asset zusammensetzt. Schwachstellen von

Assets werden im Zuge der Risikoanalyse von Privathaushalten zwar berücksichtigt und mitbedacht, allerdings nicht explizit ausgewiesen (ISO/IEC, 2022).

Informationswerte
Informationswerte stellen Kategorien von verarbeiteten oder gespeicherten Daten dar. Der Schutzbedarf von Informationswerten hinsichtlich Vertraulichkeit, Integrität und Verfügbarkeit (= primäre Schutzziele der Informationssicherheit) bestimmen maßgeblich den Schutzbedarf der Assets, welche die jeweiligen Informationswerte verarbeiten oder speichern.

Asset
Der Begriff „Asset" wird im Rahmen der Risikoanalyse für Geräte, Dienste und Anwendungen verwendet und ist von den Informationswerten (Datenkategorien) abzugrenzen. Der Schutzbedarf eines Assets leitet sich aus den verarbeiteten oder gespeicherten Informationswerten ab. Die Kombination aus einem Asset und einer relevanten Bedrohung (je nach gefährdeten Schutzzielen) ergibt ein potenzielles Risikoszenario.

4.2.2 Entwicklung des Risikoanalysekonzepts

Zur Umsetzung der Zielsetzung wurde zunächst ein Konzept erstellt, das die Struktur, die Logik und die einzelnen Schritte der Risikoanalyse beschreibt. Dieses Konzept definiert die methodische Grundlage und enthält alle notwendigen Beschreibungen, die zur Durchführung einer entsprechenden Risikoanalyse benötigt werden. Die darin enthaltenen Prozessschritte orientieren sich in Aufbau und Terminologie an bestehenden Standards, insbesondere am Vorgehensmodell des BSI-Standards 200-3, wurden jedoch deutlich vereinfacht und auf typische Nutzungssituationen in Privathaushalten angepasst. Die Unterschiede sind in Abschnitt 4.2.2.1 zusammengefasst.

Im Mittelpunkt steht ein Prozessmodell, das alle Phasen der Risikoanalyse umfasst, von der Erfassung relevanter Informationswerte und digitalen Produkten bis hin zur Auswahl geeigneter Gegenmaßnahmen zur Reduktion von Risiken (siehe Abbildung 6). Der Ablauf beinhaltet folgende Schritte, welche jeweils in den nachfolgenden Abschnitten näher erläutert werden:

1. **Definition der Rahmenbedingungen**, indem die Schutzbedarfsstufen der Informationssicherheitsziele (Vertraulichkeit, Integrität und Verfügbarkeit), Risikowerte, Schadensszenarien, Risikomatrix, Risikoneigung, kritische Schutzbedarfsgrenzen, Auswirkungs- und Eintrittshäufigkeitsstufen festgelegt werden,
2. **Identifikation & Schutzbedarfsbewertung von Informationswerten und Assets** inklusive Vererbung des Schutzbedarfs von Informationswerten auf Assets, die diese speichern oder verarbeiten,
3. **Identifikation und Bewertung von Bedrohungen sowie Angreifertypen** und die damit einhergehende Bestimmung der gefährdeten Schutzziele durch die jeweilige Bedrohung,
4. **Risikoeinstufung (Bestimmung des Brutto-Risikos)** durch Identifikation und Bewertung von potenziellen Risikoszenarien (Kombination aus Asset und Bedrohung) sowie
5. **Risikobehandlung (Bestimmung des Netto-Risikos)** für relevante Risikoszenarien für den Privathaushalt durch die Auswahl von effektiven Maßnahmen zur Senkung der Auswirkung beziehungsweise Eintrittshäufigkeit eines Risikoszenarios.

Hinweis: Die Abschnitte 4.2.2.1 bis inklusive 4.2.2.6 erläutern das theoretische Fundament und können im Sinne des Leseflusses übersprungen werden. Die Übersichtsgrafik des Risikoanalyseprozesses ist in Abschnitt 4.2.2.7 abgebildet. Die Anwendung auf ein Asset des Beispiel-Haushalts wird in 4.2.2.8 beschrieben.

4.2.2.1 Gegenüberstellung mit dem BSI-Standard 200-3

Die Einbettung der Risikoanalyse in den IT-Sicherheitsprozess gemäß dem BSI-Standard 200-3 ist in der nachfolgenden Abbildung 2 dargestellt:

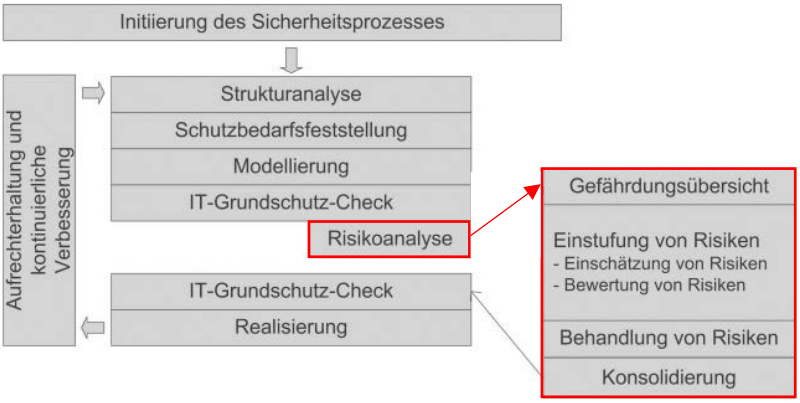

Abbildung 2 Einbettung der Risikoanalyse in den IT-Sicherheitsprozess gemäß BSI-Standard 200-3 (BSI, 2017 S. 7)

Als Datenbasis für den Risikoanalyseprozess setzt der BSI-Standard 200-3 eine Strukturanalyse von Geschäftsprozessen voraus, um Informationswerte und Assets zu modellieren und deren Schutzbedarf zu bestimmen. Für den Risikoanalyseprozess im Kontext von Privathaushalten wurde der Sicherheitsprozess von der Strukturanalyse bis zum Risikoanalyseprozess ähnlich konzipiert (siehe Abbildung 3).

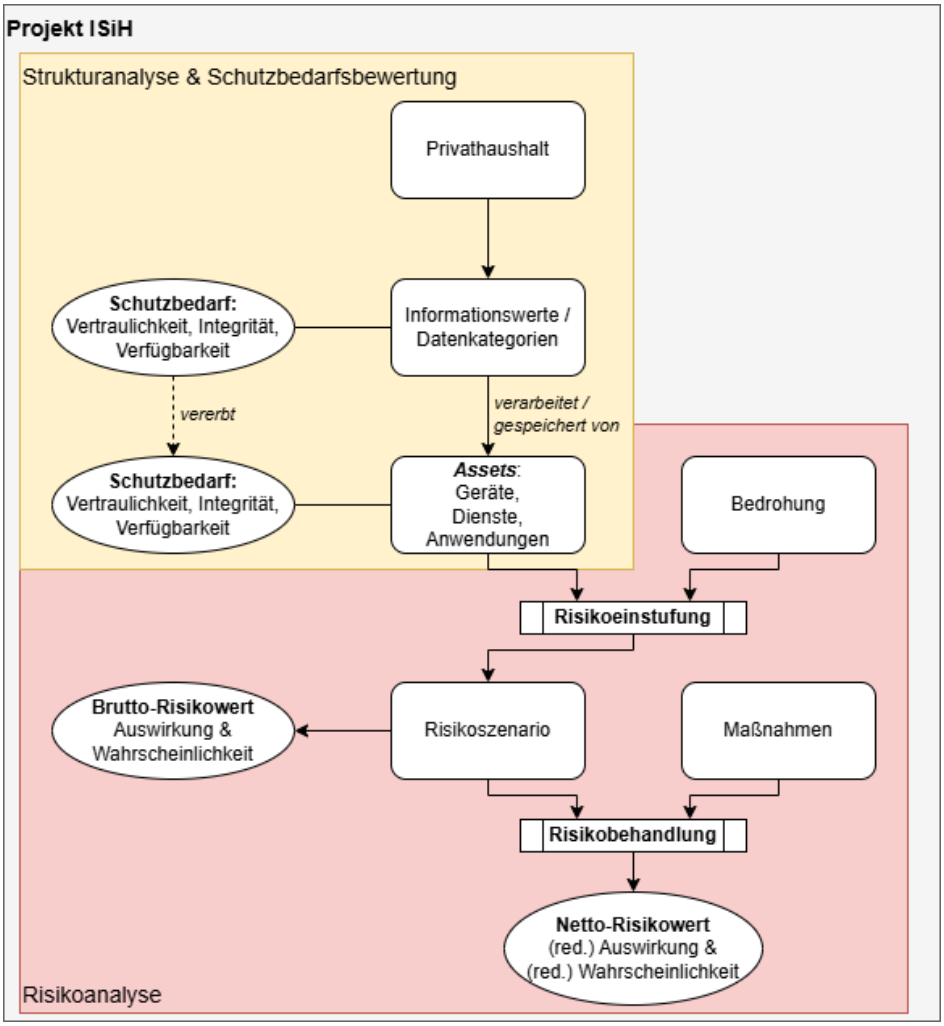

Abbildung 3 Übersicht über die Einbettung der Risikoanalyse in den IT-Sicherheitsprozess für Privathaushalte (eigene Darstellung)

Im Gegensatz zum BSI-Standard 200-3 wurde im Kontext des Projekts ISiH nicht von Geschäftsprozessen ausgegangen, sondern direkt von Informationswerten von Privathaushalten. Diese dienen wie beim BSI-Standard 200-3 als Datengrundlage für die Durchführung einer Risikoanalyse.

4.2.2.2 Definition der Rahmenbedingungen

Um eine einheitliche Risikoanalyse in einem bestimmten Kontext (beispielsweise aufgrund einer spezifischen Verbrauchergruppe) anwenden zu können, sind vorab alle nachfolgend angeführten Rahmenbedingungen zu definieren. Diese Rahmbedingungen wirken sich auf die Menge der zu betrachteten Objekte sowie auf die Ergebnisse des Risikoanalyseprozesses aus. Für die Risikoanalyse im Rahmen des Projekts wurden die in den Tabellen angeführten Werte und Abstufungen verwendet.

Die **Eintrittshäufigkeit** beschreibt die Wahrscheinlichkeit, mit der eine identifizierte Bedrohung tatsächlich eintreten kann. Sie gibt an, wie oft oder mit welcher Regelmäßigkeit ein bestimmtes Risiko unter den gegebenen Rahmenbedingungen realistisch zu erwarten ist.

Tabelle 4 Rahmenbedingungen für den Risikoanalyseprozess: Eintrittshäufigkeit

Eintrittshäufigkeit
Unwahrscheinlich (1)
Gering (2)
Häufig (3)
Sehr häufig (4)

Die **Auswirkung** beschreibt das Schadensausmaß, das durch das Eintreten einer Bedrohung verursacht werden kann. Sie gibt an, wie stark die Beeinträchtigung eines Informationswerts, eines Assets oder des gesamten Haushalts im Falle eines erfolgreichen Angriffs oder einer Störung wäre.

Tabelle 5 Rahmenbedingungen für den Risikoanalyseprozess: Auswirkung

Auswirkung
Niedrig (1)
Mittel (2)
Hoch (3)
Sehr hoch (4)

Der **Risikowert** beschreibt das numerische Ergebnis der Risikobewertung und dient der quantitativen Einordnung einzelner Risiken. Er bildet sowohl für das Brutto- als auch für das Netto-Risiko den zentralen Kennwert der Analyse. Der Risikowert ergibt sich aus dem Produkt der beiden Bewertungsfaktoren Eintrittswahrscheinlichkeit und Auswirkung. Durch die Multiplikation dieser Werte entsteht ein numerischer Score, der die relative Bedeutung eines Risikos im Vergleich zu anderen Szenarien widerspiegelt. Die resultierenden Werte ermöglichen zudem eine Klassifizierung der Risiken in abgestufte Kategorien und können in Form einer Risikomatrix visualisiert werden (siehe Abbildung 4). Diese Darstellung bietet einen schnellen Überblick über die Verteilung und Gewichtung der Risiken und unterstützt die Priorisierung bei der Risikobehandlung.

Tabelle 6 Rahmenbedingungen für den Risikoanalyseprozess: Risikowert

Risikowert
Gering (1-2)
Mittel (3-6)
Hoch (7-11)
Sehr hoch (12-16)

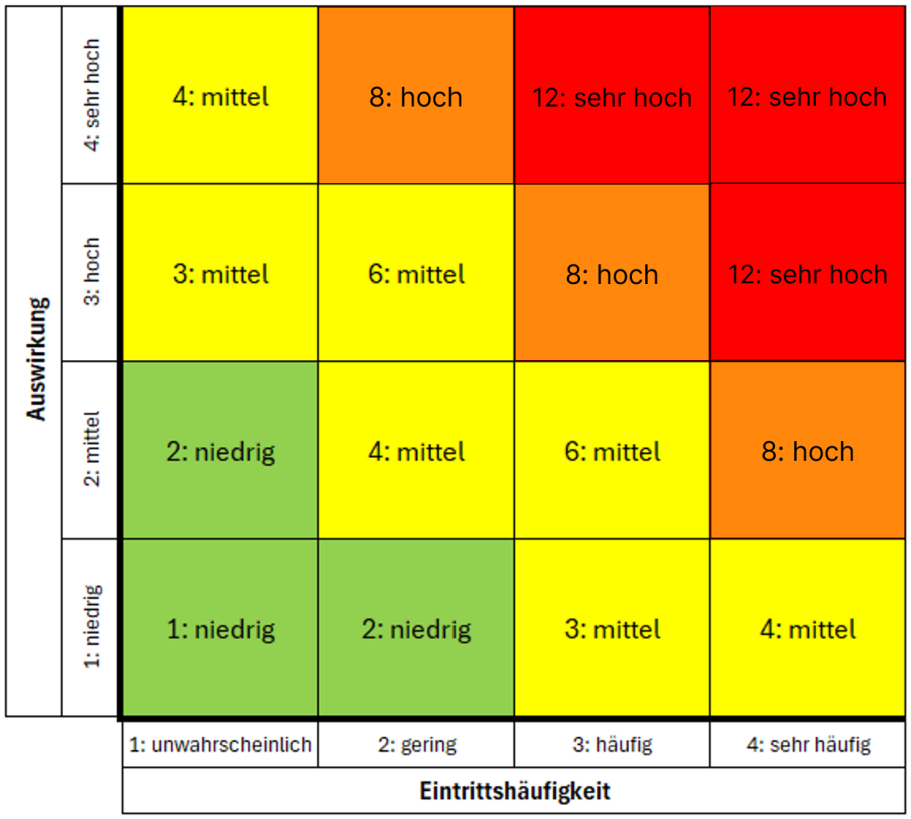

Abbildung 4 Rahmenbedingungen für den Risikoanalyseprozesses: Risikomatrix (eigene Darstellung)

Die **Risikoneigung** beschreibt den Schwellenwert, ab dem ein identifiziertes Risiko als behandlungsbedürftig gilt. Sie dient als Grenze, die festlegt, welcher Risikowert, basierend auf dem berechneten Brutto-Risiko, eine aktive Risikobehandlung erforderlich macht. Wird dieser Schwellenwert erreicht oder überschritten, ist die Anwendung geeigneter Maßnahmen zur Reduzierung des Risikos vorgesehen. Gleichzeitig definiert die Risikoneigung den Zielwert für das verbleibende Restrisiko (Netto-Risiko). Im Verlauf der Risikobehandlung soll das Netto-Risiko so weit gesenkt werden, dass es unterhalb der festgelegten Risikoneigung liegt. Auf diese Weise dient die Risikoneigung sowohl als Entscheidungskriterium für die Notwendigkeit von Maßnahmen als auch als Referenzwert für die Wirksamkeit der Risikobehandlung.

Tabelle 7 Rahmenbedingungen für den Risikoanalyseprozess: Risikoneigung

Risikoneigung
Hoch (7)

Schadensszenarien beschreiben vordefinierte Kategorien von Schäden, die zur Bewertung der potenziellen Schadenshöhen herangezogen werden. Sie dienen dazu, die möglichen Folgen bei Eintritt eines Risikos systematisch zu erfassen und vergleichbar zu machen. Auf Grundlage dieser Szenarien wird auch der Schutzbedarf von Informationswerten und Assets bestimmt.

Tabelle 8 Rahmenbedingungen für den Risikoanalyseprozess: Schadensszenarien

Schadensszenarien
Finanzieller Schaden
Zeitlicher Schaden
Emotionaler Schaden
Rufschädigung

Die **Schadenshöhe** beschreibt die definierten Stufen, mit denen die einzelnen Schadensszenarien bewertet werden. Sie dient der Einschätzung des potenziellen Ausmaßes eines Schadens, der durch das Eintreten einer Bedrohung verursacht werden kann.
Die bewertete Schadenshöhe eines Szenarios bestimmt zugleich den **Schutzbedarf** des betroffenen Informationswerts oder Assets. Für jedes Schutzziel (Vertraulichkeit, Integrität und Verfügbarkeit) werden alle vier Schadensszenarien anhand der entsprechenden Schadenshöhen bewertet. Dabei spielt die Art der Bedrohung keine Rolle, sondern es wird lediglich die potenzielle Schadenshöhe betrachtet, die beim Verlust der Vertraulichkeit, Integrität und Verfügbarkeit eintritt. Der endgültige Schutzbedarf eines für sowohl Vertraulichkeit, Integrität als auch Verfügbarkeit eines Informationswerts ergibt sich nach dem Maximalprinzip aus allen bewerteten Schadensszenarien.
Jede Kombination aus Schadensszenario und Schutzbedarfsstufe beziehungsweise Schadenshöhe wird durch qualitative oder quantitative Kriterien beschrieben, die in einer Schadensmatrix dokumentiert sind (siehe Tabelle 12).

Tabelle 9 Rahmenbedingungen für den Risikoanalyseprozess: Schadenshöhe und Schutzbedarfsstufen

Schadenshöhe und Schutzbedarfsstufen
Unkritisch (1)
Normal (2)
Hoch (3)
Sehr hoch (4)

Die **kritische Schutzbedarfsstufe** legt fest, ab welchem Schutzbedarf eines Schutzziels (Vertraulichkeit, Integrität oder Verfügbarkeit) eine Bedrohung für ein Asset als relevant eingestuft wird. Sie dient damit als Entscheidungskriterium dafür, ob ein Risiko im weiteren Verlauf der Analyse berücksichtigt werden muss. Erreicht oder überschreitet der Schutzbedarf eines Schutzziels für ein Asset die definierte kritische Stufe, wird die entsprechenden Bedrohungen, welche dieses Schutzziel gefährden, in die Risikoanalyse miteinbezogen und bewertet. Im Rahmen des Risikoanalyseprozesses liegt in diesem Fall ein „potenzielles Risikoszenario“ vor. Liegt der Schutzbedarf darunter, gilt das Risiko in diesem Zusammenhang als vernachlässigbar. Tabelle 11 zeigt zwei Beispiele für „Assets“ und in welchen Fällen ein Risikoszenario für die weitere Risikoanalyse relevant wäre.

Tabelle 10 Rahmenbedingungen für den Risikoanalyseprozess: kritische Schutzbedarfsstufe

Kritische Schutzbedarfsstufe
Hoch (7)

Tabelle 11 Rahmenbedingungen für den Risikoanalyseprozess: Beispiel für kritischen Schutzbedarf

Asset (Gerät oder Dienst)	***Schutzbedarf eines Assets (C, I, A)***	***Bedrohung und betroffene Schutzziele (C, I, A)***	***Relevantes Risiko?***
Smartphone (persönlich)	Vertraulichkeit (C): Sehr Hoch (4) Integrität (I): Hoch (3) Verfügbarkeit (A): Hoch (3)	„G 0.14 Ausspähen von Informationen“: Vertraulichkeit (C)	JA
		„G 0.25 Ausfall von Geräten oder Datenträgern“: Verfügbarkeit (A)	JA
Smarthome: Sprachassistenten (gemeinschaftlich)	Vertraulichkeit: Sehr Hoch (4) Integrität: Normal (2) Verfügbarkeit: Normal (2)	„G 0.14 Ausspähen von Informationen“: Vertraulichkeit (C)	JA
		„G 0.25 Ausfall von Geräten oder Datenträgern“: Verfügbarkeit (A)	NEIN

Die Annahmen zur **Schadensmatrix** setzen sich aus der Kombination von Schadensszenarien und Schadenshöhen zusammen, welche jeweils qualitativ oder quantitativ beschreiben werden. Diese Annahmen wurden im Rahmen des Projektes exemplarisch festgelegt.

Tabelle 12 Rahmenbedingungen für den Risikoanalyseprozess: Schadensmatrix

	unkritisch	***normal***	***hoch***	***sehr hoch***
Finanzieller Schaden	Der finanzielle Schaden ist minimal. <2% vom Haushaltseinkommen	Der finanzielle Schaden ist tolerabel. <20% vom Haushaltseinkommen	Der finanzielle Schaden bewirkt beachtliche finanzielle Verluste, ist jedoch nicht existenzbedrohend. <100% vom Haushaltseinkommen	Der finanzielle Schaden ist für die Betroffenen existenzbedrohend und überschreitet 100% vom Haushaltseinkommen.
zeitlicher Schaden	Es entsteht kein nennenswerter, zeitlicher Aufwand für die Betroffenen. (<4 Stunden)	Der zeitliche Schaden beträgt bis zu 24h.	Es ist mit einem Aufwand von bis zu 7 Tagen zu rechnen.	Es ist mit einem zeitlichen Aufwand von mehr als einer Woche zu rechnen.
emotionaler Schaden	Der Vorfall bewirkt keine oder lediglich eine schwache Reaktion der Betroffenen.	Der Vorfall ist peinlich bis ärgerlich, aber verkraftbar.	Der Vorfall bewirkt eine emotionale Schädigung der Betroffenen (Kränkung).	Der Vorfall bewirkt eine langfristige, emotionale Schädigung der Betroffenen (Vertrauensbruch, Angst).
Ruf-schädigung	Das Ansehen der Betroffenen wird nicht beschädigt.	Eine kurzfristige, leichte Schädigung des Ansehens im engsten Kreis der Betroffenen ist zu erwarten.	Das breite Ansehen der Betroffenen ist kurzfristig beschädigt.	Das breite oder ggf. gesellschaftliche Ansehen der Betroffenen ist langfristig beschädigt.

Hinweis: Nach den Erkenntnissen des Expertenworkshops aus AP04 hängt eine sinnvolle Abstufung der Schadenshöhe (insbesondere hinsichtlich finanziellen Schadens) stark vom betrachteten Privathaushalt ab. Für einkommensschwache Haushalte könnte ein finanzieller Schaden von 5 % des Haushaltseinkommens bereits kritisch beziehungsweise nicht tolerierbar sein. Im Rahmen weiterer Forschung müssten diese Werte verifiziert werden. Für die Durchführung der Risikoanalyse in diesem Projekt wurde das monatliche Haushaltsnettoeinkommen des fiktiven Beispiel-Haushalts auf 5.000 € gesetzt.

Die **Bewertung von Maßnahmen** definiert die Stufen für die Senkung der Auswirkung und der Eintrittshäufigkeit, welche für die Bewertung von Maßnahmen zur Reduktion des Brutto-Risikowerts verwendet werden. Die Wertebereiche für beide Faktoren decken sich in diesem Fall mit den beiden Achsen der Risikomatrix (siehe Abbildung 5).

Tabelle 13 Rahmenbedingungen für den Risikoanalyseprozess: Reduktion der Auswirkung

Reduktion der Auswirkung
Keine (0)
Gering (1)
Mittel (2)
Hoch (3)

Tabelle 14 Rahmenbedingungen für den Risikoanalyseprozess: Reduktion der Eintrittshäufigkeit

Reduktion der Eintrittshäufigkeit
Keine (0)
Gering (1)
Mittel (2)
Hoch (3)

4.2.2.3 Identifikation & Schutzbedarfsbewertung von Informationswerten und Assets

Sind alle Rahmenbedingungen festgelegt, folgt im zweiten Schritt der Risikoanalyse die Identifikation der Informationswerte (Datenkategorien) sowie der Assets (Geräte, Dienste und Anwendungen) des Haushalts. Anschließend wird für beide Elemente der jeweilige Schutzbedarf bestimmt. Das Ziel dieses Prozessschritts ist es, sämtliche schützenswerten Informationswerte und die mit ihnen verbundenen Assets im Privathaushalt zu erfassen.

Für jeden Informationswert wird der Schutzbedarf in Bezug auf die drei Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit bewertet. Dabei wird für jedes Schutzziel die Höhe des möglichen Schadens pro Schadenskategorie eingeschätzt, der im Falle einer Beeinträchtigung eintreten kann. Die Art der Bedrohung, welche das Schutzziel gefährden könnte, ist in diesem Schritt noch unerheblich. Der höchste Wert aus den betrachteten Schadensszenarien bestimmt nach dem Maximalprinzip den Schutzbedarf des jeweiligen Schutzziels. Auf diese Weise wird sichergestellt, dass stets der kritischste mögliche Schaden berücksichtigt wird.

Nachdem der Schutzbedarf für alle Informationswerte ermittelt wurde, wird festgestellt, welche der Informationswerte von Assets im Haushalt verarbeitet oder gespeichert werden. Wird ein Informationswert einem Asset zugeordnet, so übernimmt letzteres den entsprechenden Schutzbedarf für jedes Schutzziel. Werden auf einem Asset mehrere Informationswerte verarbeitet, gilt auch hier das Maximalprinzip.

4.2.2.4 Identifikation und Bewertung von Bedrohungen sowie Angreifertypen

Im dritten Schritt der Risikoanalyse werden alle informationssicherheitsrelevanten Bedrohungen identifiziert, die den Privathaushalt gefährden könnten. Das Ziel in diesem Prozessschritt besteht darin, auf Grundlage der identifizierten Bedrohungen alle potenziellen Risikoszenarien zu bestimmen. Risikoszenarien ergeben sich aus der Kombination eines Assets mit einer Bedrohung.

Als Ausgangspunkt für die Identifikation relevanter Bedrohungen ist beispielsweise der Katalog „Elementare Gefährdungen (G 0)“ des Bundesamts für Sicherheit in der Informationstechnik (BSI) sehr nützlich. Dieser Katalog enthält eine umfassende Sammlung definierter Bedrohungen, die ein breites Spektrum an Gefährdungsarten abdecken. Diese reichen von technischen Gefährdungen beziehungsweise Schwachstellen über organisatorische Mängel bis hin zu menschlichen Fehlhandlungen (BSI, 2020). Im Zuge der Bedrohungsidentifikation wurde festgestellt, dass viele dieser Bedrohungen nicht ausschließlich für Unternehmen, sondern auch für Privathaushalte relevant sein können. Der Katalog bietet daher eine fundierte Basis, um jene Bedrohungen zu erfassen, die auch im häuslichen Umfeld auftreten können.

Über den BSI-Katalog hinaus werden weitere Bedrohungen erfasst, die spezifisch für private Mehrpersonenhaushalte gelten. Diese werden aus einer Analyse unterschiedlicher Angreifertypen und deren möglicher Motivationen abgeleitet. Dabei wird untersucht, welche Interessen, Ziele oder Handlungsanreize Angreifer im privaten Kontext haben können, beispielsweise finanzielle Bereicherung,

Kontrolle über Haushaltsmitglieder, Neugier, Machtausübung oder gezielte Manipulation. Im Rahmen der durchgeführten Risikoanalyse auf den fiktiven Beispiel-Haushalt wurden beispielsweise folgende, unterschiedliche Angreifertypen („Threat Actors“) definiert:

Tabelle 15 definierte Threat Actors im Zuge der Risikoanalyse

Threat Actors	***Mögliche Motivation***	***intern/extern***
Anwendende	versehentliche Änderungen an Systemen, Löschung von Daten	intern
Administrierende	Macht & Kontrolle, Eifersucht, Streit	intern
Gäste & Verwandte	Neugierde, Streit	intern
Script-Kiddies	Spaß & Neugierde	beides
Cyberkriminelle	Profit	extern
Dienstleister / Hersteller	Kostensenkung	extern

Aus diesen Motiven ergeben sich zusätzliche Bedrohungsszenarien, die im Katalog nicht in dieser Form abgebildet sind, im Alltag privater Mehrpersonenhaushalte jedoch eine wesentliche Rolle spielen. Darüber hinaus können Bedrohungen aus einschlägigen Studien, Fachliteratur, Umfragen oder Berichten zum Verhalten von Privatpersonen im digitalen Raum berücksichtigt werden. Ebenso können sich neue Bedrohungen aus der sozialen Zusammensetzung des Haushalts, der Rollenverteilung und den individuellen Bedürfnissen von Haushaltmitgliedern ergeben. Beispiele hierfür sind unzureichend gesicherte Zugriffe auf gemeinsam genutzte Geräte, unklare Verantwortlichkeiten für Updates oder Sicherheitskonfigurationen sowie Risiken durch soziale Abhängigkeiten oder digitale Gewalt im häuslichen Umfeld.

Für jede identifizierte Bedrohung wird festgelegt, welche Schutzziele potenziell davon gefährdet sind. Dabei ist eine Mehrfachauswahl möglich, da einzelne Bedrohungen mehrere Schutzziele gleichzeitig betreffen können. Der BSI-Standard 200-3 weist für alle Bedrohungen des Katalogs „elementare Gefährdungen G.0“ bereits entsprechende Schutzziele aus, die im Rahmen des Projekts als Referenz verwendet wurden (BSI, 2017 S. 13-15).

Im nächsten Schritt werden die Bedrohungen mit den betroffenen Assets verknüpft. Eine Bedrohung gilt dann als relevant für ein Asset, wenn zwei Bedingungen erfüllt sind:

1. Der Schutzbedarf eines Schutzziels des Assets entspricht mindestens der definierten kritischen Schutzbedarfsstufe oder übersteigt diese, und
2. die Bedrohung gefährdet eben jenes Schutzziel.

Durch diese systematische Verknüpfung entsteht eine Vielzahl potenzieller Risikoszenarien, die als Grundlage für die nachfolgende Risikobewertung dienen. Ein Risikoszenario wird dabei nach der standardisierten Form *„[Bedrohung X] auf [Asset Y]“* bezeichnet. Diese Namenskonvention gewährleistet die Übersichtlichkeit und Nachvollziehbarkeit im weiteren Bewertungsprozess.

Beispiel: Die Bedrohung „G 0.14 – Ausspähen von Informationen (Spionage)“ gefährdet die Vertraulichkeit von Informationswerten. Das Asset „Smartphone“ speichert und verarbeitet besonders vertrauliche Daten und weist daher einen sehr hohen Schutzbedarf in Bezug auf Vertraulichkeit auf. Da der Schutzbedarf des Assets die definierte kritische Schutzbedarfsstufe überschreitet und die Bedrohung dieses Schutzziel betrifft, ergibt sich das Risikoszenario *„G 0.14 Ausspähen von Informationen (Spionage) auf Smartphone“*.

4.2.2.5 Risikoeinstufung (Bestimmung des Brutto-Risikos)

Im Zuge der Risikoeinstufung wird für jedes potenzielle Risikoszenario der Brutto-Risikowert ermittelt. Dieser Wert beschreibt das Risiko, das besteht, bevor eine Risikobehandlung durch geeignete Maßnahmen erfolgt. Das Ziel der Risikoeinstufung besteht darin, jene Risikoszenarien zu identifizieren, deren Risikowert

nicht ohne weiteres akzeptabel ist und die daher einer Behandlung bedürfen. Die Entscheidung darüber hängt unmittelbar von der zuvor definierten Risikoneigung ab.

Für jedes potenzielle Risikoszenario wird der Brutto-Risikowert aus zwei Bewertungsfaktoren berechnet:

1. Die Eintrittshäufigkeit, bestenfalls basierend auf empirischen Daten und
2. Die Auswirkung, welche sich nach dem Maximalprinzip aus der höchsten, bewerteten Schadensdimension ergibt.

Beide Werte werden miteinander multipliziert, um den numerischen Brutto-Risikowert zu berechnen. Anschließend erfolgt eine Einordnung des Ergebnisses anhand der festgelegten Risikomatrix, die eine Klassifizierung gemäß den festgelegten Stufen (beispielsweise „Gering“, „Mittel“, „Hoch“ oder „Sehr hoch“) vorsieht.

Erreicht oder überschreitet der Brutto-Risikowert den zuvor festgelegten Schwellenwert der Risikoneigung, muss das Risikoszenario durch Maßnahmen behandelt werden. Liegt der Wert unterhalb dieser Grenze, kann es als akzeptabel betrachtet werden und bedarf somit keiner zwingende Behandlung. Auf diese Weise ermöglicht die Risikoeinstufung eine klare Priorisierung der zu behandelnden Risiken und eine effiziente Fokussierung auf die tatsächlich relevanten Bedrohungen.

Zur Steigerung der Effizienz kann die Bewertung der Risiken bereits auf Bedrohungsebene vorgenommen werden. Aufgrund der Vielzahl möglicher Kombinationen zwischen Bedrohungen und Assets (n:m-Beziehung) kann sich eine große Zahl potenzieller Risikoszenarien ergeben. Um den manuellen Bewertungsaufwand zu reduzieren, werden Eintrittshäufigkeit und potenzielle Auswirkung einer Bedrohung vorab festgelegt. Diese vorab definierten Werte bilden einen Mindestrahmen für die Risikobewertung und werden auf alle Risikoszenarien („*Bedrohung X [auf] Asset Y*“) übertragen, in denen die jeweilige Bedrohung vorkommt. Dadurch lässt sich der Aufwand für die Einzelfallbewertung deutlich verringern, ohne dass die Nachvollziehbarkeit der Ergebnisse beeinträchtigt wird.

4.2.2.6 Risikobehandlung (Bestimmung des Netto-Risikos)

In der fünften Phase der Risikoanalyse werden alle Risikoszenarien betrachtet, deren Brutto-Risikowert größer oder gleich der zuvor festgelegten Risikoneigung ist. Das Ziel der Risikobehandlung besteht darin, für jedes relevante Risikoszenario den Risikowert so weit zu senken, dass das daraus resultierende Netto-Risiko unterhalb der definierten Risikoneigung liegt. Auf diese Weise wird erreicht, dass verbleibende Risiken ein akzeptables Maß nicht überschreiten und somit aus Sicht des Haushalts tolerierbar sind.

Zu Beginn der Risikobehandlung wird geprüft, ob jedes potenzielle Risikoszenario tatsächlich im Kontext eines Privathaushalts relevant ist. Szenarien, die keine praktische Bedeutung aufweisen (weil beispielsweise die Bedrohung in der gegebenen Umgebung nicht auftreten kann) werden als nicht relevant gekennzeichnet und dokumentiert. Diese Überprüfung erfolgt zu Beginn des Prozesses, um sicherzustellen, dass der Aufwand der Risikobehandlung auf jene Szenarien konzentriert bleibt, die tatsächlich von Bedeutung sind.

Für die relevanten Risikoszenarien werden anschließend mögliche Maßnahmen zur Risikominderung identifiziert. Als primäre Quelle kann beispielsweise die im Projekt ISiH entwickelte Maßnahmentabelle aus dem vorangegangenen Arbeitspaket 02 dienen. Darüber hinaus können weitere Maßnahmen aus einschlägiger Fachliteratur, insbesondere aus dem BSI IT-Grundschutz-Kompendium, aus wissenschaftlichen Studien, aus Berichten oder direkt aus der Analyse eines konkreten Risikoszenarios abgeleitet werden. Durch diese kombinierte Herangehensweise wird sichergestellt, dass sowohl bewährte Standards als auch kontextspezifische Lösungsansätze berücksichtigt werden.

Für jedes relevante Risikoszenario werden die identifizierten Maßnahmen hinsichtlich ihrer Wirksamkeit bewertet. Dabei wird analysiert, in welchem Umfang sie die beiden Faktoren Eintrittshäufigkeit und Auswirkung des Brutto-Risikos senken können. Beide Faktoren werden in absoluten Zahlenwerten erfasst, die mit den Skalen der Risikomatrix übereinstimmen.

Die Bewertung der Maßnahmen erfolgt in zwei Schritten:

1. Zunächst wird jeweils für die Eintrittshäufigkeit und die Auswirkung individuell geschätzt, um welchen Wert dieser durch die jeweilige Maßnahme reduziert werden kann. Reduziert eine Maßnahme nur die Eintrittshäufigkeit (präventiv) oder nur die Auswirkung (kompensierend), so wird die jeweils andere Dimension mit „0“ bewertet.
2. Anschließend werden die Werte der reduzierten Eintrittswahrscheinlichkeit und Auswirkung miteinander multipliziert. Das Produkt ergibt den neuen Netto-Risikowert des Szenarios.

Werden mehrere Maßnahmen auf dasselbe Risikoszenario angewendet, addieren sich deren Reduktionswerte für die jeweiligen Faktoren. Sollte sich bei der Berechnung ein negativer Wert ergeben, wird der niedrigste positive Wert der Skala (beispielsweise „1“) für die Netto-Eintrittswahrscheinlichkeit oder -Auswirkung verwendet. Dies spiegelt die Annahme wider, dass selbst bei optimaler Umsetzung von Schutzmaßnahmen immer ein Restrisiko verbleibt. Ein vollständig risikofreier Zustand wäre in der Praxis nicht realistisch und würde implizieren, dass die betrachtete Bedrohung für ein Asset keine Relevanz mehr besitzt.

Zur Effizienzsteigerung der Risikobehandlung können bereits auf der Bedrohungsebene generische Gegenmaßnahmen hinterlegt werden. Für jede Bedrohung lassen sich Maßnahmen definieren, die typischerweise zur Reduktion der Eintrittshäufigkeit oder der Auswirkung beitragen. Diese Bewertungen dienen als Richtwerte und erleichtern die Zuordnung in der Risikobehandlung. Trotz dieser Vordefinition ist eine manuelle Überprüfung erforderlich, um die tatsächliche Anwendbarkeit und Wirksamkeit der vorgeschlagenen Maßnahmen im jeweiligen Risikoszenario zu bestätigen oder gegebenenfalls anzupassen.

4.2.2.7 Übersicht über die Abhängigkeiten, Beziehungen und Bewertungsmechanismen im Risikoanalyseprozess

Die nachfolgende Grafik (Abbildung 5) skizziert den oben beschriebenen Risikoanalyseprozess mit allen Abhängigkeiten und Beziehungen zwischen den erläuterten Faktoren, Objekten und Bewertungen.

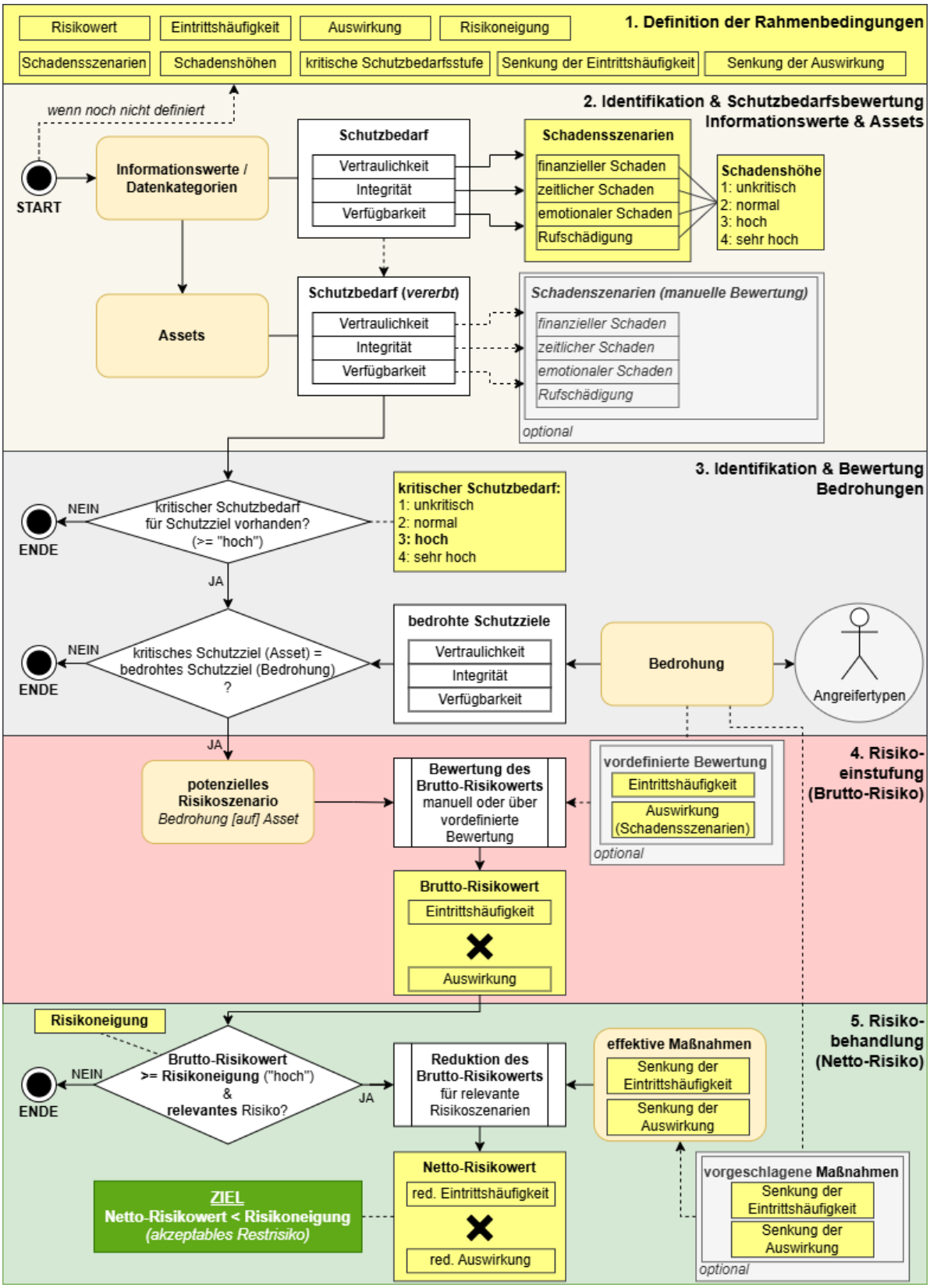

Abbildung 5 Übersicht der Abhängigkeiten, Beziehungen und Bewertungsmechanismen des Risikoanalyseprozesses (eigene Darstellung)

4.2.2.8 Beispielhafte Risikoanalyse auf ein Asset

Hinweis: In Anhang B sind alle Informationswerte, Assets und Bedrohungen der Risikoanalyse angeführt.

Das nachfolgende Beispiel skizziert die Risikoanalyse für das Asset „Heimnetzwerk (WLAN, LAN und Internetzugang)“, wobei die definierten Rahmenbedingungen (Nr. 1 in Abb. 5) aus Abschnitt 4.2.2.2 zu entnehmen sind.

Im Prozessschritt „Identifikation und Schutzbedarfsbewertung“ (Nr. 2 in Abb. 5) wurden die verarbeiteten oder gespeicherten Informationswerte des Assets erhoben, um den Schutzbedarf hinsichtlich Vertraulichkeit, Integrität und Verfügbarkeit zu bewerten. Diese Daten sind in Tabelle 16 und Tabelle 17 dargestellt. Bei der Bestimmung des Schutzbedarfs der Informationswerte sind in Tabelle 16 jene Schadensszenarien angegeben (*kursiv*), welche den Schutzbedarf gemäß Maximalprinzip bestimmten.

Tabelle 16 Beispiel Risikoanalyse: Informationswerte inklusive Schutzbedarfsbewertung

Informationswert	***Schutzbedarf: Vertraulichkeit***	***Schutzbedarf: Integrität***	***Schutzbedarf: Verfügbarkeit***
Sensible Zugangsdaten (Passwort, Passkey, Authenticator-Codes, etc.)	Sehr Hoch (4) *finanzieller Schaden*	Normal (2) *zeitlicher Schaden*	Normal (2) *Zeitlicher Schaden, Emotionaler Schaden*
Private Kommunikation	Hoch (3) *Emotionaler Schaden*	Normal (2) *Zeitlicher Schaden, Emotionaler Schaden, Rufschädigung*	*Normal (2)* *Emotionaler Schaden*
Offizielle Kommunikation m. Behörden, Bank, etc.	Normal (2) *Finanzieller Schaden, emotionaler Schaden, Rufschädigung*	Normal (2) *Finanzieller Schaden, zeitlicher Schaden*	Normal (2) *Zeitlicher Schaden*
Persönliche Dateien (Bilder, Dokumente, etc.)	Hoch (3) *Emotionaler Schaden, Rufschädigung*	Unkritisch (1) *Alle Schadensszenarien*	Hoch (3) *Emotionaler Schaden*
Sensible / nicht-jugendfreie Inhalte	Hoch (3) *Emotionaler Schaden, Rufschädigung*	Unkritisch (1) *Alle Schadensszenarien*	Unkritisch (1) *Alle Schadensszenarien*

Für das Asset „Heimnetzwerk (WLAN, LAN und Internetzugang)“ ergab sich somit folgender Schutzbedarf:

Tabelle 17 Beispiel Risikoanalyse: Schutzbedarf für das Asset „Heimnetzwerk“

Asset	***Schutzbedarf: Vertraulichkeit***	***Schutzbedarf: Integrität***	***Schutzbedarf: Verfügbarkeit***
Heimnetzwerk (WLAN, LAN und Internetzugang)	Sehr Hoch (4)	Normal (2)	Hoch (3)

Im nächsten Prozessschritt „Identifikation und Bewertung von Bedrohungen“ (Nr. 3 in Abb. 5) wurden alle relevanten Bedrohungen für das Asset bestimmt. Dazu wurde der kritische Schutzbedarf für das Asset hinsichtlich Vertraulichkeit und Verfügbarkeit mit den von den Bedrohungen gefährdeten Schutzzielen abgeglichen. Im Falle des Beispiel-Assets ergaben sich dadurch 28 potenzielle Risikoszenarien, unter anderem:

- „G 0.8 Ausfall oder Störung der Stromversorgung auf Heimnetzwerk (WLAN, LAN und Internetzugang)“

- „G 0.14 Ausspähen von Informationen (Spionage) auf Heimnetzwerk (WLAN, LAN und Internetzugang)“

Jedes dieser Risikoszenarien wurde im nächsten Prozessschritt „Risikoeinstufung“ (Nr. 4 in Abb. 5) anhand ihrer potenziellen Auswirkungen (finanzieller Schaden, zeitlicher Schaden, emotionaler Schaden, Rufschädigung) und einer Einschätzung der Eintrittshäufigkeit bewertet. Das Produkt der beiden Bewertungen ergibt den Brutto-Risikowert eines Risikoszenarios. Ist dieser Wert größer oder gleich der Risikoneigung („Hoch“ mit einem Wert ab 7), wird es einer Risikobehandlung unterzogen. Für das Beispiel-Assets „Heimnetzwerk (WLAN, LAN und Internetzugang)“ verblieben nach der Risikoeinstufung 19 zu behandelnde Risikoszenarien. Ein Auszug der Risikoeinstufung für vier konkrete Risikoszenarien wird in Abbildung 6 gezeigt. Von den abgebildeten Risikoszenarien wurde lediglich das Risikoszenario in der letzten Zeile mit einen Brutto-Risikowert größer oder gleich der Risikoneigung bewertet und wird in Folge behandelt.

Risikoszenario	gefährdete Schutzziele	Eintrittshäufigkeit	finanzieller Schaden	zeitlicher Schaden	emotionaler Schaden	Rufschädigung	Auswirkung gesamt	Brutto-Risikowert	zu behandeln?
G 0.8 Ausfall oder Störung der Stromversorgung [auf] Heimnetzwerk (WLAN, LAN und Internetzugang)	A	2: gering	1: unkritisch	3: hoch	2: normal	1: unkritisch	3: hoch	6: mittel	nein
G 0.9 Ausfall oder Störung von Kommunikationsnetzen [auf] Heimnetzwerk (WLAN, LAN und Internetzugang)	A	2: gering	1: unkritisch	2: normal	2: normal	1: unkritisch	2: normal	4: mittel	nein
G 0.11 Ausfall oder Störung von Dienstleistern [auf] Heimnetzwerk (WLAN, LAN und Internetzugang)	C, I, A	2: gering	2: normal	2: normal	2: normal	1: unkritisch	2: normal	4: mittel	nein
G 0.14 Ausspähen von Informationen (Spionage) [auf] Heimnetzwerk (WLAN, LAN und Internetzugang)	C	2: gering	1: unkritisch	1: unkritisch	4: sehr hoch	1: unkritisch	4: sehr hoch	8: hoch	ja

Abbildung 6 Beispiel Risikoanalyse: Auszug aus dem Prozessschritt „Risikoeinstufung“ (eigene Darstellung)

Im letzten Schritt der Risikoanalyse „Risikobehandlung“ (Nr. 5 in Abb. 5) wurden alle Risikoszenarien mit einem Brutto-Risikowert größer oder gleich der Risikoneigung mit geeigneten Maßnahmen versehen. Senken diese Maßnahmen die Eintrittshäufigkeit und Auswirkung in einem Maße, dass das Produkt der reduzierten Werte (der Netto-Risikowert) kleiner ist als die festgelegte Risikoneigung, wurde das Risikoszenario erfolgreich behandelt.

Da der Brutto-Risikowert automatisch berechnet wurde, indem vordefinierte Bewertungen für die Auswirkung und Eintrittshäufigkeit auf Bedrohungsebene angegeben wurden, musste an dieser Stelle noch eine Plausibilisierung vorgenommen werden (siehe Spalte „Relevanz“ in Abbildung 7). Zudem wurden auf Bedrohungsebene im Vorfeld geeignete Maßnahmen aus einem Maßnahmenkatalog angegeben, um die Behandlung durch vorgeschlagene Maßnahmen zu beschleunigen (siehe Abbildung 8). Auch an dieser Stelle musste eine Plausibilisierungsprüfung durchgeführt werden, ob jede automatisch vorgeschlagene Maßnahme tatsächlich für das konkrete Asset anwendbar ist.

	Brutto-Risiko			Relevanz	Netto-Risiko		
Bezeichnung	Brutto-Risikowe	Eintrittshäufigkeit	Auswirkung gesamt	Risiko relevant?	Netto-Risikowe	Eintrittshäufigkeit	Auswirku
G 0.14 Ausspähen von Informationen (Spionage) [auf] Heimnetzwerk (WLAN, LAN)	8: hoch	2: gering	4: sehr hoch	WAHR	1: niedrig	1: unwahrscheinlich	1: niedrig
G 0.17 Verlust von Geräten, Datenträgern oder Dokumenten [auf] Heimnetzwerk (WLAN, LAN)	9: hoch	3: häufig	3: hoch	FALSCH	3: mittel	3: häufig	1: niedrig
G 0.19 Offenlegung schützenswerter Informationen [auf] Heimnetzwerk (WLAN, LAN)	9: hoch	3: häufig	3: hoch	WAHR	4: mittel	2: gering	2: mittel

Abbildung 7 Beispiel Risikoanalyse: Risikobehandlung (Netto-Risiko)

	Maßnahme 1:		(autom. vorgeschlagen)		Maßnahme 2:		(autom. vorgeschlagen)	
Bezeichnung	Bezeichnung	Senkung der Eintrittshäufigkei	Senkung der Auswirkung	anwendbar?	Bezeichnung	Senkung der Eintrittshäufigkei	Senkung der Auswirkung	anwendbar?
G 0.14 Ausspähen von Informationen (Spionage) [auf] Heimnetzwerk (WLAN, LAN)	Sichtschutzfolie für Gerät	2: mittel	0: keine	FALSCH	Dateifreigaben im Netzwerk auf ein Minimum reduzieren	1: gering	1: gering	WAHR
G 0.17 Verlust von Geräten, Datenträgern oder Dokumenten [auf] Heimnetzwerk (WLAN, LAN)	Verschlüsselung von Daten, Festplatten und Datensicherungen				regelmäßige Datensicherungen auf externen Speichermedien			
G 0.19 Offenlegung schützenswerter Informationen [auf] Heimnetzwerk (WLAN, LAN)	Dateifreigaben im Netzwerk auf ein Minimum reduzieren	1: gering	1: gering	WAHR	Deaktivieren der Übermittlung von nicht erforderlichen Daten	2: mittel	0: keine	FALSCH

Abbildung 8 Beispiel Risikoanalyse: Auszug aus Maßnahmen zur Risikobehandlung

4.2.3 Implementierung des Risikoanalysekonzepts

Alle in Abschnitt 4.2.2 beschriebenen Schritte wurden in einem Tabellenkalkulations-Template dargestellt, das die Struktur der Risikoanalyse abbildet und eine teilweise automatisierte Implementierung unterstützt. Das Template diente somit als Werkzeug zur praktischen Anwendung der Risikoanalyse auf den Beispiel-Haushalt und spiegelt die im Konzept beschriebenen Prozessschritte wider. Es enthält dedizierte Arbeitsblätter für die Informationswerte, Assets, Bedrohungen, Maßnahmen und Risikoszenarien, um diese isoliert zu erfassen, zu bewerten und gegebenenfalls nachträglich zu ändern. Mithilfe des Einsatzes von möglichst dynamischen Formeln werden viele Verknüpfungen und Berechnungen automatisiert durchgeführt, was die Anwendung erleichtert, manuelle Eingaben auf ein notwendiges Minimum begrenzt und gleichzeitig die Nachvollziehbarkeit gewährleistet.

Die Risikobewertung erfolgte semiquantitativ. Schadensausmaß und Eintrittswahrscheinlichkeit werden qualitativ bewertet und anschließend in numerische Werte überführt. Auf dieser Grundlage kann das Brutto-Risiko als Zahlenwert berechnet werden, der anschließend durch geeignete Maßnahmen (wiederum mit numerischen Werten hinterlegt) auf einen Netto-Risikowert reduziert wird. Der resultierende Netto-Risikowert kann danach wieder gemäß der definierten Risikomatrix qualitativ eingeordnet werden. Je nach Ergebnis kann das Risikoszenario weiter mit Maßnahmen reduziert werden oder bei einem Risikowert kleiner als die festgelegte Risikoneigung akzeptiert werden.

Nach der Definition der Rahmenbedingungen wurden Informationswerte und Assets für die Risikoanalyse ausgehend vom fiktiven Beispiel-Haushalt identifiziert und deren Schutzbedarf gemäß der vordefinierten Schadensmatrix bewertet. Ergänzend zum herangezogenen Bedrohungskatalog des BSI „elementare Gefährdungen G.0“ wurden haushaltsspezifische Bedrohungen definiert und die davon gefährdeten Schutzziele bestimmt. Die Maßnahmen und deren Bewertung hinsichtlich Risikoreduktion basierten auf den in AP02 definierten Maßnahmen sowie auf der Struktur des fiktiven Beispiel-Haushalts. Für die meisten Bedrohungen konnte zumindest eine potenzielle Maßnahme hinterlegt werden, um den Risikobehandlungsschritt effizient zu gestalten.

Hinweis: Für weiterführende Details zur oben genannten Risikoanalyse-Tabellenkalkulationsdatei kann das BSI kontaktiert werden.

4.3 Ergebnisse der Risikoanalyse

4.3.1 Überblick

Im Rahmen der Risikoanalyse wurden die für den Beispiel-Haushalt relevanten Informationswerte, Assets, Bedrohungen und Risiken identifiziert und bewertet:

1. Zu Beginn wurden die Rahmenbedingungen definiert, welche jenen aus Abschnitt 4.2.2.2 entsprachen.
2. Danach wurde der Schutzbedarf der Informationswerte wurde für jedes Schutzziel (Vertraulichkeit, Integrität und Verfügbarkeit) bewertet.

3. Im nächsten Schritt wurde für jedes Asset angegeben, welche Informationswerte dieses verarbeitet oder speichert. Dadurch ließ sich der Schutzbedarf für die Geräte und Dienste des Beispiel-Haushalts nach dem Maximalprinzip ableiten.
4. Aus dem Katalog „elementare Gefährdungen G.0“ (BSI, 2020) wurden für den Haushalt relevante Bedrohungen identifiziert und um zusätzliche Bedrohungen, basierend auf den Erkenntnissen der Literaturrecherche und relevanten Angreifertypen, ergänzt. Für jede Bedrohung wurden die davon gefährdeten Schutzzielen unter Zuhilfenahme des BSI-Standard 200-3 (BSI, 2017 S. 13-15) festgelegt.
5. Anschließend wurde für alle potenziellen Bedrohungen, die sich aus der Kombination von Asset mit einem kritischen Schutzbedarf und einer entsprechenden Bedrohung ergaben, das Brutto-Risiko (Produkt aus Eintrittshäufigkeit und Auswirkung) bewertet.
6. Risikoszenarien mit einem Brutto-Risikowert größer oder gleich der definierten Risikoneigung („Hoch“) wurden mit Maßnahmen versehen, wodurch das Netto-Risiko berechnet werden konnte.

Die für die Risikoanalyse herangezogenen Informationswerte, Assets und Bedrohungen sind in Anhang B angeführt.

4.3.2 Automatisierungs- und Bewertungsmechanismen

Eine Besonderheit des entwickelten Konzepts liegt in der Möglichkeit einer teilautomatisierten Bewertung. Das im Rahmen des Arbeitspakets erstellte Tabellenkalkulations-Template nutzt Vererbungslogiken und vorgegebene Parameter, um Bewertungen konsistent durchzuführen:

- Der Schutzbedarf eines Assets wird automatisch aus dem höchsten Schutzbedarf der verarbeiteten Informationswerte abgeleitet. Da sich der Schutzbedarf von Informationswerten, verglichen mit der Anzahl und Diversität von möglichen digitalen Produkten, naturgemäß weniger oft ändert, steigert dieser Vererbungsmechanismus die Effizienz der Schutzbedarfsbestimmung.
- Das Brutto-Risiko für ein Risikoszenario ergibt sich aus den vordefinierten Bewertungen hinsichtlich Auswirkung und Eintrittshäufigkeit der Bedrohung. Eine initiale Brutto-Risikobewertung auf Bedrohungsebene erspart somit für laufende und neue Risikoanalysen von Assets Zeit, indem behandelnde Risikoszenarien mit einem Risikowert größer oder gleich der Risikoneigung automatisch identifiziert werden.
- Das Tabellenkalkulation schlägt auf Basis der Bedrohungsebene passende Maßnahmen vor, die aus der in Arbeitspaket 02 entwickelten Maßnahmentabelle einmalig für eine Bedrohung referenziert werden müssen. Die Auswahl der vordefinierten Maßnahmen in der Risikobehandlung bedarf lediglich einer Plausibilisierung hinsichtlich Sinnhaftigkeit und der Risikoreduktionswerte. Damit wird der Prozess der Risikobehandlung beschleunigt, indem in den meisten Fällen die Suche in einer langen Liste nach potenziell wirksamen Maßnahmen außen vor gelassen werden kann.

Die oben beschriebenen Verfahren reduzieren den Aufwand für die Risikoanalyse erheblich. Allerdings bleibt die Einschätzung der Wirksamkeit einzelner Maßnahmen subjektiv; sie kann nur im Zusammenspiel mit Erfahrung und Kontextwissen erfolgen.

4.4 Diskussion der Ergebnisse & Fazit

In diesem Arbeitspaket wurde ein systematisches, nachvollziehbares und praxisnahes Verfahren zur Risikoanalyse für Privathaushalte entwickelt und exemplarisch angewendet.

Das dafür entwickelte Tabellenkalkulations-Template bietet hierfür eine geeignete Basis. Neue Informationswerte, Assets oder Bedrohungen können unkompliziert ergänzt oder adaptiert werden, etwa auf Basis künftiger Erkenntnisse aus empirischen Erhebungen oder Expertenrunden. Die Eintragung von neuen Assets oder Bedrohungen hat zumeist eine automatische Erstellung von Risikoszenarien zur Folge, welche gegebenenfalls behandelt werden müssen. Damit stellt das entwickelte Konzept ein flexibles Instrument zur kontinuierlichen Risikoanalyse im häuslichen Umfeld dar. Es bietet zudem ein hohes Maß

an Transparenz und Nachvollziehbarkeit, erfordert jedoch eine gewisse technische Grundkompetenz. Für den breiten Einsatz müsste eine stärker automatisierte, interaktive Lösung (beispielsweise als Webapplikation oder Smartphone-App) erwogen werden.

Die Ergebnisse der mit dem Tabellenkalkulations-Template durchgeführten Risikoanalyse auf den fiktiven Beispiel-Haushalt zeigen jedenfalls, dass sich Methoden von etablierten Informationssicherheits-Risikobewertung erfolgreich auf den Risikoanalysekonzept für den Privatbereich übertragen lassen, sofern sie um soziale und nutzungsbezogene Dimensionen, beispielsweise durch die Berücksichtigung von emotionalen Schäden und zusätzlichen Bedrohungen im Kontext von privaten Mehrpersonenhaushalte, erweitert beziehungsweise angepasst werden.

Die Risikoanalyse verdeutlichte zudem, dass Privathaushalte mit einer Vielzahl unterschiedlicher Risikoszenarien konfrontiert sind, die sowohl technische als auch soziale Ursachen haben. Für eine effiziente Bewältigung der Identifikation, Analyse, Bewertung und die Priorisierung beziehungsweise der Vorschlag für entsprechende Sicherheitsmaßnahmen, um relevante Risiken zu reduzieren, kann der entwickelte Risikoanalyseprozess vom großen Nutzen sein, da er wertvolle Möglichkeiten zur Automatisierung unterstützt.

Die identifizierten Risiken und Bewertungsergebnisse bildeten die Grundlage für den Expertenworkshop in AP04, der dazu diente, die theoretischen Annahmen durch Erfahrungswissen aus unterschiedlichen Verbrauchergruppen zu validieren und zu erweitern.

5 Ergebnisse aus dem Expertenworkshop (Teil von Arbeitspaket AP04)

5.1 Zielsetzung und Ausgangslage

Der im Rahmen von AP04 durchgeführte Expertenworkshop diente der Validierung der entwickelten Risikoanalyse (AP03) und ihrer zugrunde liegenden Annahmen. Das Ziel des Workshops war, die dort identifizierten Bedrohungen, Risikoszenarien und Bewertungsansätze aus praktischer und interdisziplinärer Perspektive zu überprüfen und um weitere Aspekte zu ergänzen. In weiterer Folge sollten bei diesem Arbeitspaket die neu gewonnenen Erkenntnisse in die Ausarbeitung von Anwendungsfällen für ein Berechtigungsmanagement in Privathaushalten miteinfließen, welche den gesamten Lebenszyklus von digitalen Produkten berücksichtigen. Die Anwendungsfälle aus AP04 werden in Kapitel 6 behandelt.

Der Workshop war somit ein zentraler Baustein, um das methodisch-konzeptionelle Modell aus den vorangegangenen Arbeitspaketen mit qualitativen Erfahrungswerten abzugleichen, die Anwendbarkeit der Analyseergebnisse auf reale Privathaushalte zu prüfen und den Fokus auf das Thema Berechtigungsmanagement zu richten.

5.2 Methodisches Vorgehen

5.2.1 Zusammensetzung der Expertengruppe

Der Workshop fand am 4. Juni 2025 als Videomeeting statt und vereinte acht Expertinnen und Experten aus unterschiedlichen Verbraucher- und Interessengruppen. Es waren Fachpersonen aus folgenden Themenfeldern vertreten:

- Verbraucherschutz (Verbraucherzentralen)
- Pflege & Senioren
- Gleichstellung und Geschlechtergerechtigkeit
- Finanzielle Bildung
- Digitale Gewalt und Opferschutz
- Inklusive Digitalisierung
- Verbrechensopferhilfe

Durch diese Zusammensetzung konnten sowohl technische als auch soziale, psychologische und ökonomische Perspektiven einbezogen werden. Diese breite Expertise an unterschiedlichen Themenfeldern ermöglichte zudem die Berücksichtigung von weiteren, unterschiedlichen Zusammensetzungen von privaten Mehrpersonenhaushalten und deren spezifischen Anforderungen an eine IT-Sicherheitsmanagement.

5.2.2 Aufbau und Ablauf des Workshops

Die inhaltliche Grundlage für den Expertenworkshop bildeten die Ergebnisse der Risikoanalyse (AP03) sowie vorbereitete Leitfragen, die gezielt auf die Überprüfung und Diskussion der dort entwickelten Annahmen ausgerichtet waren. Dabei wurde der Fokus auf das Thema „Berechtigungsmanagement“ gerichtet.

Der Workshop war in fünf thematische Module gegliedert, die in Form von Diskussionsrunden, Online-Whiteboard-Arbeiten und Umfragen durchgeführt wurden und aufeinander aufbauten:

1. **Vorstellungsrunde und Projektüberblick**: Einführung in Zielsetzung, Beispiel-Haushalt und bisherige Projektergebnisse aus AP02 und AP03 im Rahmen des Projekts.

2. **Rollen und Verantwortlichkeiten**: Sammlung typischer Rollen über den gesamten Lebenszyklus digitaler Produkte und Dienste hinweg (Kauf, Wartung, Entsorgung, IT-Sicherheit) mithilfe eines bereitgestellten, interaktiven Online-Whiteboards.
3. **IT-Sicherheit in der Praxis**: Diskussion gängiger Sicherheitspraktiken, Hürden und Wahrnehmungen in den jeweiligen Zielgruppen.
4. **Bewertung von Schadensszenarien, Assets und Bedrohungen**: Durchführung eines Online-Surveys zur Plausibilisierung der Rahmenbedingungen und Bewertungen der durchgeführten Risikoanalyse in AP03.
5. **Abschlussdiskussion**: Verantwortung für IT-Sicherheit im Privatbereich und Feedback zum Projekt ISiH.

Die Ergebnisse der Whiteboard-Sessions und des Online-Surveys wurden im Nachgang aufbereitet.

5.3 Ergebnisse des Expertenworkshops (Kernaussagen)

5.3.1 Rollen und Verantwortlichkeiten

> Zitat aus dem Workshop: „*Der Digital Gender Gap ist ein strukturelles Problem in Privathaushalten. Frauen fehlt es bei einer traditionellen Rollenverteilung schlichtweg an Zeit, um sich mit IT im Haushalt und deren Sicherheit zu beschäftigen.*“

Im ersten inhaltlichen Modul des Expertenworkshops wurde untersucht, wer in den unterschiedlichen Privathaushalten (bezogen auf die berufliche Zielgruppe der Fachpersonen) typischerweise für IT-bezogene Aufgaben verantwortlich ist.

Dazu wurde ein Online-Whiteboard eingesetzt, das die Lebensphasen digitaler Produkte (Kauf, Wartung & Pflege, Entsorgung, IT-Sicherheit) in vier Spalten und Produkttypen (persönliche Geräte, gemeinschaftlich genutzte Geräte, Netzwerk / WLAN, wichtige Online-Dienste) in Zeilen abbildete. Die Teilnehmenden wurden gebeten, basierend auf ihrer beruflichen Expertise und den Erfahrungen mit ihrer jeweiligen Zielgruppe, die Hauptverantwortlichen für jede Lebensphase der Produkttypen zu benennen. Ihnen wurde für die Befüllung des Online-Whiteboards folgende Leitfrage mitgegeben:

Welche „üblichen“ Verantwortlichkeiten bestehen in den unterschiedlichen Konstellationen des Zusammenlebens in Privathaushalten, die den Kauf, die Wartung und die Entsorgung von Geräten und Anwendungen sowie der IT-Sicherheit betreffen?

Für die jeweilige Lebensphase eines digitalen Produkts wurden zusätzlich folgende Fragen im Online-Whiteboard vermerkt:

- *Wer bestimmt, welche Geräte oder Dienste bezogen werden?*
- *Wie verteilen sich die Berechtigungen für den Kauf und die Konfiguration von IT-Geräten und -Diensten in den Haushalten? Wer sind die „typischen“ Administratoren oder Administratorinnen?*
- *Von wem werden die Geräte entsorgt bzw. Dienste gekündigt?*
- *Wer ist für deren Einstellungen und für Maßnahmen zur IT-Sicherheit verantwortlich?*

Diese Fragen wurden für vier unterschiedliche Produktkategorien beantwortet:

- persönliche Geräte, wie etwa Smartphones, Laptops, Smartwatches, etc.
- gemeinschaftlich genutzte Geräte, wie etwa Smart-TV, Digitale Assistenten (Alexa, Google Assistant / Google Nest), Smarthome-Geräte
- Netzwerk & WLAN
- Wichtige Online-Dienste, wie etwa Behördenwege, Banking, etc.

Die Auswertung zeigte ein deutliches Muster:

In nahezu allen Konstellationen wurden männliche Haushaltsmitglieder als Hauptverantwortliche für technische Belange genannt. Dieser Befund wurde von den Teilnehmenden des Expertenworkshops als Ausdruck des sogenannten *Digital Gender Gap* interpretiert. Dabei handelt es sich um ein strukturelles Phänomen, das die ungleiche Verteilung technischer Zuständigkeiten zwischen den Geschlechtern widerspiegelt. Ein damit einhergehendes Problem ist die erhöhte Abhängigkeit und den damit verbundenen Risikoszenarien, wie etwa Machtmissbrauch oder Digitale Gewalt.

Als Gründe dafür wurden unter anderem genannt:

- traditionelle Rollenbilder in Privathaushalten,
- mangelnde Zeitressourcen anderer Haushaltsmitglieder (insbesondere weiblicher Personen) aufgrund familiärer Verpflichtungen,

Sonstige „typische" Verantwortliche, die mehrmals über den gesamten Lebenszyklus von digitalen Produkten genannt wurden, waren die Eltern, der gesetzliche Vormund und Angehörige (Kinder, Eltern, Verwandte). Für die Kategorie „Wichtige Online-Dienste" wurden auch Kinder genannt, für den Fall, dass deren Eltern nicht Deutsch als Muttersprache sprechen. In institutionellen Umgebungen, wie etwa Pflegeeinrichtungen, konnten keine klaren Zuständigkeiten identifiziert werden. Hier variiert die Verantwortung stark und wird teils an Betreiber, externe Dienstleister oder Angehörige ausgelagert.

5.3.2 IT-Sicherheit in der Praxis: Umsetzungsstand und Herausforderungen

> Zitat aus dem Workshop: „*Das Teilen von Passwörtern und Accounts wird zu Beginn einer Beziehung als Liebesbeweis angesehen. Möglichen Konsequenzen zu einem späteren Zeitpunkt werden dabei nicht berücksichtigt.*"

In der anschließenden Diskussion wurden gängige IT-Sicherheitspraktiken und typische Umsetzungsprobleme in den verschiedenen Verbrauchergruppen beleuchtet. Dabei wurden folgende Fragestellungen behandelt:

- *Wie gehen Verbraucherinnen und Verbraucher Ihrer beruflichen Zielgruppe allgemein mit dem Thema IT-Sicherheit um?*
- *Welche internen und externen Risikofaktoren könnten sich für Ihre Zielgruppe aufgrund unzureichender Sicherheitsmaßnahmen ergeben?*
- *Welche Maßnahmen werden bereits umgesetzt oder sind gängige Praxis?*
- *In welchem Ausmaß setzen Verbraucherinnen und Verbraucher auf Vertrauen in andere (Eheleute, Verwandte)?*
- *Gab es in der Vergangenheit konkrete Vorfälle, die mit zusätzlichen IT-Sicherheitsmaßnahmen verhindert werden hätten können?*

Die Expertinnen und Experten bestätigten, dass das Bewusstsein für IT-Sicherheitsmaßnahmen grundsätzlich vorhanden ist, die tatsächliche Umsetzung jedoch häufig ausbleibt.

Als zentrale Ursachen wurden vier mögliche Hauptfaktoren identifiziert:

- **Bequemlichkeit**: Zusätzliche Eingaben (beispielsweise Zwei-Faktor-Authentisierung) oder manuelle Konfigurationen werden als störend empfunden.
- **Angst und Abhängigkeit**: Besonders in Fällen digitaler oder physischer Gewalt können Sicherheitsmaßnahmen (beispielsweise Passwortänderungen) nicht umgesetzt werden, um keine Eskalation zu provozieren.
- **Unterschätzung von Risiken**: Viele Betroffene halten sich für „nicht interessant" für Angriffe oder überschätzen ihre Fähigkeit, Bedrohungen rechtzeitig zu erkennen.

- **Vertrauen / soziale Bindungen**: In engen Beziehungen werden Passwörter oder Geräte häufig geteilt, was potenzielle Sicherheitslücken schafft.

Darüber hinaus wurde eine These zur Umsetzungsvoraussetzung diskutiert, die vier notwendige Faktoren benennt, damit IT-Sicherheitsmaßnahmen tatsächlich realisiert werden können:

- **Wissen**: Das Wissen zur Umsetzung einer Maßnahme muss gegeben sein oder kann sich angeeignet werden.
- **Zeit**: Die Zeit zur Implementierung und Aufrechterhaltung einer Maßnahme muss gegeben sein.
- **Geld**: Das Budget für IT-Sicherheitsmaßnahmen muss gegeben sein. Ein mit IT-Sicherheitsfunktionen ausgestattetes digitales Produkt (beispielsweise mit einer längeren Laufzeit von Updates und Patches) kostet in der Regel mehr als ein Produkt, welches ausschließlich die Funktion für den Einsatzbereich bereitstellt und weniger Augenmerk auf die IT-Sicherheit den Anwendenden legt.
- **Motivation**: Verbraucherinnen und Verbraucher müssen die IT-Sicherheitsmaßnahme umsetzen wollen und nicht durch die oben angeführten Gründe (Bequemlichkeit, Angst und Abhängigkeit, Unterschätzung von Risiken, Vertrauen / soziale Bindungen) daran gehindert werden.

Diese These wurde von allen Teilnehmenden akzeptiert und als hilfreiches Modell zur Beschreibung der Diskrepanz zwischen Bewusstsein und Verhalten bewertet.

Grundsätzlich wurden von den Fachpersonen hinsichtlich gängiger Praktiken Maßnahmen genannt, die auch in der Maßnahmentabelle aus AP02 angeführt wurden. Besonders deutlich traten jedoch Herausforderungen in vulnerablen Gruppen zutage. So berichteten Expertinnen aus dem Bereich „Digitale Gewalt“, dass in Frauenhäusern oder bei Missbrauchsopfern bereits konkrete IT-Schutzmaßnahmen etabliert sind, wie etwa das Ändern von Passwörtern, die Nutzung von Passwortmanagern, das Prüfen von App-Berechtigungen und der Einsatz von Tools zur Erkennung von Bluetooth-Trackern. Betreuende von betroffenen Personen Digitaler Gewalt werden bereits auf gängige IT-Sicherheitspraktiken, wie etwa die oben genannten, geschult. Diese Maßnahmen zeigen, dass IT-Sicherheit im Kontext persönlicher Bedrohung unmittelbar lebenspraktische Relevanz besitzt. Gleichwohl können selbst gut gemeinte Maßnahmen, etwa biometrische Authentisierung, unter Zwang ihre Schutzwirkung verlieren.

Es ist somit nicht auszuschließen, dass für bestimmte, vulnerable Verbrauchergruppen noch andere, spezifische Maßnahmen in der Praxis etabliert oder zumindest bekannt sind. Weiters ließ sich aus der Diskussion ableiten, dass manche „Good Practices“ in gewissen Situationen für bestimmte Verbrauchergruppen nicht den effektiven Schutz gewährleisten, wie man pauschal vielleicht annehmen möchte. Die Diskussion verdeutlichte damit die Grenzen rein technischer Sicherheitsansätze und betonte die Notwendigkeit, psychologische und soziale Dimensionen stärker in Sicherheitskonzepte einzubeziehen.

5.3.3 Bewertung von Schadensszenarien, Assets und Bedrohungen (Online-Survey)

> Zitat aus dem Workshop: „*Besonders kritisch sind emotionale Schäden bis hin zu Suizid. Auch können körperliche Schäden entstehen, wenn digitale Gewalt mit analoger Gewalt verbunden ist.*“

Zur Ergänzung und Überprüfung der in AP03 entwickelten Risikoanalyse wurde die Expertengruppe gebeten, ein vorbereitetes Online-Survey auszufüllen. Das Ziel dieser Erhebung bestand darin, die Annahmen der Risikoanalyse zu plausibilisieren, weitere für Privathaushalte relevante Aspekte zu identifizieren und gegebenenfalls Anpassungen an der Bewertungslogik vorzunehmen.

Die teilnehmenden Expertinnen und Experten bewerteten dabei aus der Perspektive ihrer jeweiligen beruflichen Zielgruppen jene Schadensszenarien, Assets und Bedrohungen, die sie als besonders kritisch für Verbraucherinnen und Verbraucher einschätzten. Mit acht Teilnehmenden handelte es sich dabei nicht um eine repräsentative Umfrage, sondern um eine erste Validierung der Risikoanalyse, deren Ergebnisse als inhaltlicher Input und Kontrollinstrument für die Weiterentwicklung des Modells dienten.

Das Online-Survey gliederte sich in drei Themenbereiche:

1. Bewertung der in der Risikoanalyse verwendeten Schadensszenarien und deren Kritikalität für private Verbraucherinnen und Verbraucher,
2. Einschätzung besonders schutzwürdiger Geräte und Dienste (Assets) und
3. Bewertung von fünf ausgewählten Risikoszenarien aus der Risikoanalyse.

5.3.3.1 Schadensszenarien

> Zitat aus dem Workshop: „*Es benötigt eine regressive Berechnung für die Bewertung von finanziellen Schäden: Arme sind von 2% des monatlichen Haushalts-Nettoeinkommens stärker betroffen als Reiche.*“

Als besonders kritisch wurden von den Expertinnen und Experten vor allem finanzielle und emotionale Schäden eingestuft. Beide Schadensszenarien wurden jeweils von sechs der acht Teilnehmenden als die relevantesten Kategorien bezeichnet. Darüber hinaus wurde angemerkt, dass auch gesundheitliche Schäden infolge physischer Gewalt im Zusammenhang mit digitalen Angriffen als besonders gravierend einzuschätzen wären. Dieser Aspekt wurde damals jedoch bewusst nicht in das Projekt mitaufgenommen.

Bei der Bewertung der kritischen Schadenshöhe zeigten sich deutliche Abweichungen gegenüber den Annahmen der Risikoanalyse. Während dort erst ein Schaden in Höhe von bis zu 100% des monatlichen Haushaltseinkommens als kritisch definiert war, vertraten fünf der acht Teilnehmenden die Auffassung, dass bereits Verluste von bis zu 20% des monatlichen Einkommens für Verbraucherinnen und Verbraucher als nicht tolerierbar gelten sollten. Als Konsequenz wurde vorgeschlagen, die Abstufungen für finanzielle Schäden feiner zu differenzieren. Darüber hinaus wurde angeregt, künftig eine regressive Bewertung einzuführen, da für einkommensschwächere Haushalte bereits ein finanzieller Schaden von wenigen Prozentpunkten des monatlichen Einkommens gravierende Folgen haben könnte, während einkommensstärkere Haushalte denselben Verlust leichter kompensieren würden. Diese Erkenntnis verweist auf die Notwendigkeit, sozioökonomische Unterschiede stärker in der Bewertung finanzieller Risiken zu berücksichtigen.

Bei den übrigen Schadensszenarien (zeitliche Schäden, Ruf- bzw. Imageschäden und emotionale Schäden) deckten sich die Einschätzungen der Expertinnen und Experten weitgehend mit den in der Risikoanalyse angenommenen Kritikalitätsschwellen. Lediglich bei den Imageschäden wurde angemerkt, dass es hierbei zu kulturellen Unterschieden kommen könne, insbesondere im Hinblick auf Ehrvorstellungen oder gesellschaftliche Reputation. Diese Unterschiede sollten bei künftigen Risikoanalysen berücksichtigt werden, da sie die Wahrnehmung und Bewertung von Schäden beeinflussen können.

5.3.3.2 Assets

Unter den physischen Geräten wurde insbesondere das persönliche Smartphone (von 7 der 8 Teilnehmenden genannt) und der persönliche Laptop bzw. PC (6 von 8 Nennungen) als besonders schützenswert eingestuft. Ebenfalls häufig genannt wurden Smarthome-Geräte und digitale Sprachassistenten sowie Netzwerkgeräte (jeweils 5 von 8 Nennungen). Diese Ergebnisse stehen im Einklang mit der Risikoanalyse aus AP03, in der für sämtliche dieser Geräte ein „sehr hoher“ Schutzbedarf ermittelt wurde. Eine Abweichung zeigte sich hingegen bei der Smartwatch. Nur 3 der 8 Teilnehmenden stuften dieses Gerät als besonders schützenswert ein, während in der Risikoanalyse ein sehr hoher Schutzbedarf angenommen worden war. Diese Diskrepanz lässt sich dadurch erklären, dass in der Umfrage nicht explizit darauf hingewiesen wurde, dass Smartwatches biometrische Daten verarbeiten oder für e-Health-Zwecke genutzt werden können. Entsprechend sollte in zukünftigen Risikoanalysen stärker zwischen unterschiedlichen Nutzungszwecken differenziert werden, um die Bewertung anwendungsbezogen präzisieren zu können.

Bei den digitalen Diensten ergab sich ein ähnliches Bild. Als besonders schützenswert wurden von den Teilnehmenden vor allem der Internetzugang bzw. das WLAN (7 von 8 Nennungen), Messenger-Dienste wie etwa WhatsApp, Signal, Telegram oder SMS (ebenfalls 7 von 8 Nennungen) sowie E-Mail-Dienste, Online-

Banking und soziale Medien (jeweils 6 von 8 Nennungen) bewertet. Diese Einschätzungen decken sich weitgehend mit den Bewertungen aus der Risikoanalyse, in der diese Dienste aufgrund der hohen Relevanz für Kommunikation, Identitätsmanagement und finanzielle Transaktionen ebenfalls als kritisch eingestuft wurden. Abweichungen zeigten sich insbesondere bei e-Health-Diensten sowie bei digitalen Behördenportalen. Beide Kategorien wurden jeweils nur von 4 der 8 Teilnehmenden als besonders kritisch bewertet, obwohl die Risikoanalyse für beide Dienste einen sehr hohen Schutzbedarf festgelegt hatte. Dies ist wiederum ein Indiz dafür, dass die Kritikalität von e-Health-Diensten vom konkreten Einsatzbereich abhängen.

5.3.3.3 Bedrohungen

Die Ergebnisse zeigten insgesamt eine grundlegende Übereinstimmung zwischen den Bewertungen der Expertengruppe und den in AP03 ermittelten Risikoeinschätzungen. Dennoch ergaben sich in einzelnen Bereichen Unterschiede, die für die Weiterentwicklung der Risikoanalyse von Bedeutung waren.

Finanzielle Schäden wurden in nahezu allen Bedrohungsszenarien deckungsgleich mit den Annahmen der Risikoanalyse bewertet. Eine Ausnahme bildete das Szenario „Sexuelle Belästigung im Internet, Cyber-Stalking und Sextortion“. Während in der Risikoanalyse ein sehr hoher finanzieller Schaden angenommen wurde, stuften die Expertinnen und Experten diesen im Durschnitt lediglich als „mittel“ ein. Diese Abweichung deutete darauf hin, dass finanzielle Auswirkungen in Fällen digitaler Gewalt zweitrangingen Charakter besitzen und die emotionalen und psychologischen Folgen im Vordergrund stehen.

Bei den zeitlichen Schäden ergaben sich deutlichere Unterschiede. Vier der fünf Bedrohungsszenarien wurden hinsichtlich dieser Schadensdimension eindeutig und mehrheitlich höher bewertet als in der Risikoanalyse. Diese Ergebnisse weisen darauf hin, dass der Faktor Zeitaufwand, wie etwa für Wiederherstellungsmaßnahmen, Neuanschaffungen oder Kommunikationsaufwand nach einem Vorfall, in der Risikoanalyse unterbewertet wurde. Bemerkenswert ist zugleich, dass trotz der höheren Bewertung nur etwa die Hälfte der Expertinnen und Experten zeitliche Schäden als „kritisch“ einstufte. Dies deutete darauf hin, dass der wahrgenommene Aufwand zwar höher eingeschätzt wird, aber nicht in allen Fällen als existenziell relevant galt.

Die emotionalen Schäden wurden von allen Teilnehmenden für sämtliche Bedrohungsszenarien identisch zur Risikoanalyse im Zuge des Projekts bewertet. Dies bestätigt, dass die in AP03 vorgenommenen Annahmen zur psychischen Belastung und emotionalen Betroffenheit offenbar realistische Einschätzungen darstellten.

Ähnlich verhielt es sich bei den Ruf- und Imageschäden, die ebenfalls weitgehend mit den bisherigen Annahmen übereinstimmten. Eine Abweichung zeigte sich beim Szenario „Ausspähen von Informationen bei gemeinschaftlich genutzten Geräten“. Während in der Risikoanalyse dieses Risiko als „unkritisch“ bzw. „niedrig“ eingestuft wurde, bewerteten die Expertinnen und Experten den Schaden in diesem Fall als „hoch“. Diese Neubewertung legte nahe, dass Reputationsverluste, die durch den unbefugten Zugriff innerhalb eines persönlichen oder familiären Umfelds entstehen, stärker berücksichtigt werden sollten als angenommen.

Die Bewertung der Eintrittshäufigkeit von Risikoszenarien ergab insgesamt ein ähnliches Bewertungsniveau wie in der Risikoanalyse. Eine nennenswerte Abweichung zeigte sich jedoch bei Szenarien im Zusammenhang mit Schadsoftware. Hier schätzten die Expertinnen und Experten die Wahrscheinlichkeit eines Befalls als „gering“ ein, während in der Risikoanalyse noch die Einstufung „häufig“ vorgenommen worden war.

Insgesamt lässt sich aus den Ergebnissen ableiten, dass die Risikoanalyse in ihrer Grundstruktur bestätigt wurde, jedoch in einzelnen Bewertungsaspekten präzisiert und kontextsensitiver ausgestaltet werden sollte. Insbesondere die Bewertung der zeitlichen Schäden bedarf einer Anpassung, da dieser Faktor in der Praxis offenbar eine größere Bedeutung hat als angenommen. Zudem sollte geprüft werden, ob die Abstufungen finanzieller Schäden feiner differenziert werden sollten, um unterschiedliche wirtschaftliche Ausgangslagen realistischer abzubilden.

5.3.4 Verantwortlichkeiten und gesellschaftliche Perspektiven

> Zitat aus dem Workshop: „*Awareness für einen angemessenen Umgang mit persönlichen Daten und für Cybersicherheit muss bereits in der Schule geschaffen werden. Mobbing endet nicht am Ende des Unterrichts, sondern setzt sich oft im digitalen Raum nach der Schule fort.*“

In der abschließenden Diskussionsrunde des Workshops wurde das Thema Verantwortlichkeiten noch einmal gezielt aufgegriffen. Im Mittelpunkt standen die Fragen danach, wer für die Sicherheit digitaler Produkte und Dienste verantwortlich sein könnte und welche strukturellen Rahmenbedingungen erforderlich sind, um IT-Sicherheit im privaten Bereich wirksam und nachhaltig zu verankern.

Die Expertinnen und Experten betonten, dass die primäre Verantwortung für IT-sichere Produkte und Dienste bei Herstellern, Anbietern und dem Gesetzgeber liegen müsse. Aktuell werde diese Verantwortung jedoch in weiten Teilen auf die Gruppe der Anwendenden übertragen, die sich selbst um Schutzmechanismen, Datenschutz und Privatsphäre kümmern müssen. Dieses Modell wurde von den Teilnehmenden kritisch bewertet, da es die individuelle Kompetenz und Motivation überfordert und strukturelle Sicherheitsdefizite verdeckt.

Die Teilnehmenden forderten daher eine klare Verpflichtung der Hersteller und Anbieter, die Prinzipien *security by design* und *security by default* konsequent umzusetzen. Diese Prinzipien sollten bei der Entwicklung, Bereitstellung und dem Betrieb digitaler Produkte und Dienste verbindlich berücksichtigt werden. Ergänzend wurde angeregt, gesetzliche Vorgaben zur IT-Sicherheit auch durch ein unabhängiges Kontrollorgan zu überwachen, das die Einhaltung von Mindeststandards prüft und Verstöße sanktioniert.

Ein spezieller Diskussionspunkt betraf Einrichtungen mit betreuendem Charakter, wie etwa Pflegeeinrichtungen oder Seniorenheime. Hier wird die Verantwortung für IT-Sicherheit häufig an externe IT-Dienstleister übertragen. Sind innerhalb der Einrichtung keine ausreichenden Ressourcen oder Kompetenzen vorhanden, verbleibt nur das Vertrauen, dass Dienstleister ihre Systeme nach anerkannten Best Practices implementieren, betreiben und sicher entsorgen. Dieses Abhängigkeitsverhältnis gilt als problematisch, da Einrichtungen oft nicht in der Lage seien, die Qualität oder Sicherheit externer IT-Leistungen selbstständig zu überprüfen.

Neben der Frage institutioneller Verantwortung wurde auch die gesellschaftliche Sensibilisierung als zentrale Voraussetzung für nachhaltige IT-Sicherheit hervorgehoben. Um ein breites Bewusstsein für digitale Risiken und Schutzpraktiken zu schaffen, müsse eine entsprechende Aufklärung bereits im Schulalter beginnen. Die Teilnehmenden sprachen sich dafür aus, IT-Sicherheit als Pflichtbestandteil schulischer Bildung zu verankern, beispielsweise in Form eines eigenständigen Unterrichtsfachs, das digitale Selbstschutzkompetenz, Datenschutz und den verantwortungsvollen Umgang mit Technik vermittelt. Diese Verantwortung liege nach Ansicht der Expertinnen und Experten bei der Bildungspolitik, die entsprechende Vorgaben schaffen müsse.

Darüber hinaus wurde betont, dass auch außerschulische Bildungsangebote ausgebaut werden sollten. Besonders Vereine und gemeinnützige Organisationen könnten hierbei eine wichtige Rolle spielen, indem sie spezifische Verbrauchergruppen gezielt ansprechen und praxisorientierte Formate wie Workshops, Informationsveranstaltungen oder Online-Schulungen anbieten. Die Teilnehmenden plädierten für eine stärkere öffentliche Förderung solcher Initiativen, um Wissen niedrigschwellig und bedarfsgerecht zu vermitteln.

Als potenzielle Herausforderung wurde in diesem Zusammenhang das Stadt-Land-Gefälle benannt. In ländlichen Regionen sei der Zugang zu Informationsveranstaltungen und Weiterbildungsangeboten deutlich eingeschränkter, was gezielte Maßnahmen zur besseren Erreichbarkeit dieser Zielgruppen erforderlich mache.

Im abschließenden Teil des Workshops gaben die Expertinnen und Experten ein direktes Feedback zum Projekt ISiH. Dabei wurde insbesondere der im Rahmen der Risikoanalyse verwendete „Beispiel-Haushalt“

kritisch hinterfragt. Ein einheitliches, allgemeines Haushaltsmodell erschien den Teilnehmenden wenig geeignet, da sich Verbrauchergruppen in vielerlei Hinsicht unterscheiden.

Diese Unterschiede betreffen insbesondere:

- das Haushaltseinkommen,
- die Zusammensetzung der Personen und gegebenenfalls bestehende körperliche oder mentale Beeinträchtigungen,
- die Altersstruktur, die Interessenlage und die Motivation zur Umsetzung von Sicherheitsmaßnahmen,
- sowie kulturelle Hintergründe und Wertehaltungen.

Diese Vielfalt führe dazu, dass IT-Sicherheitsmaßnahmen nicht pauschal angewendet werden können, sondern an die jeweiligen Lebensrealitäten angepasst werden müssen. Ein universelles Haushaltsmodell könne diese Heterogenität nicht angemessen abbilden. Zudem empfahlen die Expertinnen und Experten, bei der Erstellung von Maßnahmenkatalogen und Best-Practice-Listen Barrierefreiheit und digitalen Zwang stärker zu berücksichtigen. Beide Aspekte sollten als Kriterien in die Bewertung der Anwendbarkeit von IT-Sicherheitsmaßnahmen einfließen. Während Barrierefreiheit sicherstellt, dass Maßnahmen für alle Nutzergruppen zugänglich und verständlich sind, verweist der Begriff „digitaler Zwang“ auf Situationen, in denen Menschen digitale Technologien nutzen müssen, ohne ihnen ausweichen zu können. In solchen Fällen sind besonders nutzerfreundliche und sichere Systeme erforderlich, da ein freiwilliger Verzicht auf digitale Dienste praktisch nicht möglich ist.

5.4 Ergebnisdiskussion und Fazit des Expertenworkshops

Der Expertenworkshop stellte eine zentrale Schnittstelle zwischen der theoretisch-modellhaften Risikoanalyse und den späteren konzeptionellen Arbeiten dar.

Die Ergebnisse daraus verdeutlichten, dass IT-Sicherheit in Privathaushalten ein komplexes Zusammenspiel aus technischen, organisatorischen und sozialen Faktoren darstellt. Während die Risikoanalyse aus AP03 eine methodisch-technische Grundlage für die Bewertung von Risiken geschaffen hat, ergänzen die empirischen Befunde aus dem Workshop diese Perspektive um praxisnahe und gesellschaftliche Dimensionen. In der Diskussion zeigte sich, dass viele theoretische Annahmen der Risikoanalyse grundsätzlich bestätigt werden konnten, jedoch in ihrer praktischen Anwendung einer stärkeren Kontextualisierung bedürfen.

Ein zentraler Befund betrifft die Verteilung von Verantwortlichkeiten innerhalb privater Haushalte. Die Diskussionen machten deutlich, dass die Verantwortung für IT-Sicherheitsmaßnahmen häufig auf eine einzelne, meist technisch versiertere Person konzentriert ist. Da diese Person oftmals männlich ist und dieses Phänomen ein strukturelles Problem darstellt, spricht man in diesem Zusammenhang vom *Digital Gender Gap*, welcher Risiken wie Machtmissbrauch und Digitale Gewalt fördert. Diese Struktur führt zu Abhängigkeiten und organisatorischen Schwächen, insbesondere wenn Wissen, Zugänge oder Zuständigkeiten nicht dokumentiert oder geteilt werden. Die Beobachtungen der Expertinnen und Experten bestätigten damit die Annahme, dass fehlende Verantwortlichkeitsstrukturen eines der größten Hindernisse für nachhaltige IT-Sicherheit im häuslichen Umfeld darstellen.

Darüber hinaus wurde deutlich, dass das IT-Sicherheitsverhalten stark von sozialen und individuellen Faktoren abhängt. Kenntnisse, Motivation, verfügbare Zeit und finanzielle Mittel bestimmen maßgeblich, in welchem Umfang Sicherheitsmaßnahmen tatsächlich umgesetzt werden. Die vier Einflussgrößen (Wissen, Zeit, Geld und Motivation) bilden nach Einschätzung der Teilnehmenden die Grundvoraussetzungen für praktikable Sicherheitskonzepte im privaten Bereich. Ist einer dieser Faktoren nicht gegeben, bleibt die Umsetzung selbst einfacher Maßnahmen meist aus.

Die Bewertungen und Diskussionen zu Schadensszenarien und Kritikalität zeigten, dass die in der Risikoanalyse vorgenommenen Einstufungen im Wesentlichen tragfähig sind, jedoch an mehreren Stellen angepasst werden sollten. Besonders der Schadensfaktor „Zeit“ wurde von den Expertinnen und Experten

deutlich höher bewertet als im Modell vorgesehen. Damit wird der Aufwand, der nach einem Sicherheitsvorfall für Wiederherstellung, Kommunikation oder Support erforderlich ist, als realistischeres Maß für Alltagsbelastungen erkannt. Auch die Bewertung finanzieller Schäden sollte differenzierter erfolgen, da Einkommensunterschiede die subjektive Wahrnehmung und Toleranzschwelle stark beeinflussen. Die empirischen Ergebnisse lassen somit daraus schließen, dass Risikobewertungen in Privathaushalten stärker sozioökonomische Unterschiede berücksichtigen müssen.

Bei der Bewertung von Geräten und Diensten (Assets) bestätigte sich die hohe Schutzrelevanz zentraler Kommunikations- und Identifikationssysteme wie etwa Smartphones, Computer, E-Mail-Konten und Messenger-Dienste. Abweichungen zwischen Risikoanalyse und Experteneinschätzungen, wie es beispielsweise bei Smartwatches, e-Health-Diensten oder digitalen Verwaltungsportalen der Fall war, deuteten darauf hin, dass der Einsatzkontext und die Art der gespeicherten Daten entscheidend für die Bewertung des Schutzbedarfs sind. Ein allgemein bewerteter Schutzbedarf reicht nicht aus, wenn sich die Nutzung eines Geräts oder Dienstes je nach Zielgruppe erheblich unterscheidet. Zukünftige Risikoanalysen sollten daher eine kontextsensitive Bewertungssystematik verwenden, die unterschiedliche Einsatzszenarien gezielt abbildet.

Auch die Diskussion der gesellschaftlichen Verantwortung ergab wichtige Impulse. Nach einhelliger Meinung der Teilnehmenden kann die Verantwortung für IT-Sicherheit nicht ausschließlich bei den Verbraucherinnen und Verbrauchern liegen. Herstellern und Anbietern kommt eine wesentliche Rolle zu, indem sie Sicherheit und Datenschutz bereits bei der Entwicklung ihrer Produkte und Dienste nach den Prinzipien *security by design* und *security by default* verankern. Diese Forderung schließt auch den Aufbau geeigneter Kontrollstrukturen ein, um gesetzliche Vorgaben zu überwachen und deren Einhaltung sicherzustellen.

Ergänzend wurde die Bildungspolitik in die Verantwortung genommen, IT-Sicherheitskompetenzen systematisch zu fördern. Insbesondere die Integration digitaler Selbstschutzkompetenz im schulischen Bereich wurde als zentrale Voraussetzung für langfristige gesellschaftliche Wirksamkeit bezeichnet. Darüber hinaus sei der Ausbau außerschulischer Bildungsangebote erforderlich, um bestehende Kompetenzlücken in der Bevölkerung zu schließen und IT-Sicherheit auch außerhalb formaler Bildungseinrichtungen zu verankern.

Der in der Risikoanalyse verwendete „Beispiel-Haushalt“ wurde von mehreren Teilnehmenden kritisch bewertet. Nach Einschätzung der Expertinnen und Experten kann ein einheitliches Haushaltsmodell der Heterogenität realer Lebenssituationen nicht gerecht werden. Unterschiede in Einkommen, Altersstruktur, körperlichen oder mentalen Beeinträchtigungen sowie kulturellen Hintergründen führen zu sehr unterschiedlichen Sicherheitsanforderungen. Künftige Analysen sollten daher stärker differenzierte Haushaltsprofile verwenden, um die Vielfalt realer Nutzungsszenarien abzubilden. Ergänzend wurde empfohlen, bei der Entwicklung von Best-Practice-Listen und Maßnahmenkatalogen Kriterien wie Barrierefreiheit und Digitalen Zwang in die Bewertung der Anwendbarkeit aufzunehmen. Nur so kann gewährleistet werden, dass Sicherheitsmaßnahmen für alle Bevölkerungsgruppen praktikabel und realisierbar sind.

Zusammenfassend lässt sich festhalten, dass der Expertenworkshop die theoretischen Ergebnisse der Risikoanalyse im Kern bestätigt, sie jedoch um wesentliche soziale, ökonomische und organisatorische Perspektiven erweitert hat. Die Diskussionen zeigten, dass technische Sicherheitsmaßnahmen allein nicht ausreichen, um ein angemessenes Schutzniveau in Privathaushalten zu gewährleisten. Effektive IT-Sicherheit entsteht erst im Zusammenspiel zwischen benutzerfreundlicher Technologie, klaren Verantwortlichkeiten, rechtlichen Rahmenbedingungen und einer breiten gesellschaftlichen Sensibilisierung.

Diese Erkenntnisse bilden die Grundlage für die in AP04 entwickelten Anwendungsfälle sowie für die konzeptionellen Szenarien in AP05, die darauf abzielen, IT-Sicherheit im privaten Umfeld als ganzheitliches, sozio-technisches System zu verstehen und zu gestalten.

6 Ergebnisse aus Arbeitspaket AP04 – Organisation von IT-Sicherheit in Privathaushalten

6.1 Zielsetzung und Ausgangslage

Aufbauend auf den Ergebnissen der Risikoanalyse (AP03) und neben den empirischen Erkenntnissen aus dem Expertenworkshop (siehe Kapitel 5) hatte AP04 außerdem das Ziel, vier konkrete Anwendungsfälle, welche ein Berechtigungsmanagement zur Erhöhung der IT-Sicherheit in privaten Mehrpersonenhaushalten erfordern, zu identifizieren. Die technischen und organisatorischen Anforderungen an das Berechtigungsmanagement sollten dabei über den gesamten Lebenszyklus von digitalen Produkten betrachtet werden.

6.2 Methodisches Vorgehen

Die vier Anwendungsfälle wurden von Bedrohungen der Risikoanalyse aus AP03 und den Erkenntnissen des vorangegangenen Expertenworkshops abgeleitet. Jede relevante Bedrohung für einen Anwendungsfall wurde dabei mit den zutreffenden Lebensphasen eines digitalen Produkts, von

1. der Auswahl und dem Kauf, über
2. den Betrieb und der Wartung bis hin
3. zur Entsorgung verknüpft.

Die jeweiligen technischen und organisatorischen Anforderungen eines Anwendungsfalls wurden als konkrete IT-Sicherheitsmaßnahmen definiert und orientierten sich an der Maßnahmentabelle aus AP02.

6.3 Ergebnisse der Anwendungsfälle für ein Berechtigungsmanagement

Für die Ableitung der Anwendungsfälle wurden folgende Bedrohungen herangezogen:

Tabelle 18 herangezogene Bedrohungen aus Risikoanalyse AP03 und Expertenworkshop für die Ableitung von Anwendungsfällen in AP04

Risikoanalyse AP03	***Expertenworkshop***
G 0.14 Ausspähen von Informationen (Spionage)	Digitale Gewalt im Privatbereich, inkl. digitale Überwachung, Kontrolle und Machtmissbrauch
G 0.21 Manipulation von Hard- oder Software	Abhängigkeit aufgrund Digital Gender Gap
G 0.22 Manipulation von Informationen	
G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen	
G 0.31 Fehlerhafte Nutzung oder Administration von Geräten und Systemen	
Problematische Inhalte für Jugendliche und Kinder	
Ausfall des technischen Verantwortlichen	
Machtmissbrauch / Missbrauch von Berechtigungen	

Aus diesen Bedrohungen konnten vier wesentliche Anwendungsfälle für ein Berechtigungsmanagement in Privathaushalten abgeleitet werden, deren technischen und organisatorischen Anforderung in den nachfolgenden Abschnitten beschrieben werden:

1. Zugriffsschutz
2. Jugendschutz

3. Mehrere Administrator-Accounts
4. Vorsorge gegen Machtmissbrauch und Digitale Gewalt

Die Anwendungsfälle #3 „Mehrere Administrator-Accounts“ und #4 „Vorsorge gegen Machtmissbrauch und digitale Gewalt“ setzen jeweils unterschiedliche Schwerpunkte hinsichtlich der zu schützenden Daten und Dienste und sind daher kontextabhängig zu betrachten.

Die Einrichtung mehrerer Administrator-Accounts ist insbesondere dann sinnvoll, wenn es sich um gemeinschaftlich genutzte Geräte oder Datenbestände handelt, beispielsweise bei Netzwerk- oder Smarthome-Komponenten. In solchen Fällen dient ein zweiter administrativer Zugang dazu, die Verfügbarkeit sicherzustellen und den Zugriff auch dann zu ermöglichen, wenn die ursprünglich technisch verantwortliche Person vorübergehend oder dauerhaft ausfällt. Dadurch kann das Risiko eines vollständigen System- oder Datenzugriffsverlustes wirksam reduziert werden.

Im Gegensatz dazu verfolgen Vorsorgemaßnahmen gegen Machtmissbrauch und digitale Gewalt das Ziel, den Schutz persönlicher Geräte und individueller Daten sicherzustellen. In diesen Fällen ist vielmehr die konsequente Trennung von Benutzerkonten, die Nutzung starker Authentisierungsverfahren und die regelmäßige Überprüfung von Berechtigungen entscheidend, um die Integrität und Vertraulichkeit persönlicher Daten zu gewährleisten.

6.3.1 Anwendungsfall #1: Zugriffsschutz

Für den ersten Anwendungsfall wurden folgende potenzielle Bedrohungen (Tabelle 19) zusammengefasst und die daraus resultierenden Anforderungen festgelegt:

Tabelle 19 Anwendungsfall #1: Zugriffsschutz (Bedrohungen und die davon betroffenen Produktlebensphasen)

Bedrohung(en)	***Betroffene Produktlebensphasen***
G 0.14 Ausspähen von Informationen (Spionage)	1. Auswahl & Kauf 2. Betrieb & Wartung 3. Entsorgung
G 0.21 Manipulation von Hard- oder Software	1. Auswahl & Kauf 2. Betrieb & Wartung
G 0.22 Manipulation von Informationen	2. Betrieb & Wartung
G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen	2. Betrieb & Wartung 3. Entsorgung
G 0.31 Fehlerhafte Nutzung oder Administration von Geräten und Systemen	2. Betrieb & Wartung

Ein angemessener Zugriffsschutz regelt den Zugang zu Geräten, Diensten und gespeicherten Daten und trägt maßgeblich dazu bei, unbefugte Zugriffe sowie damit verbundene Bedrohungen zu verhindern und gegebenenfalls zu protokollieren. Durch klar definierte Zugriffsmechanismen wird sichergestellt, dass nur berechtigte Personen auf sensible Funktionen und Daten zugreifen können.

Für die technische Umsetzung in Privathaushalten ergeben sich daraus mehrere Anforderungen an digitale Produkte und Dienste. Diese sollten:

- verschiedene sichere Benutzeranmeldeverfahren unterstützen, etwa Multifaktor-Authentisierung mittels Passkeys, biometrischer Merkmale oder PIN-Verfahren,
- individuelle, nicht öffentlich abrufbare Standard-Anmeldedaten bereitstellen, um identische Zugangsdaten bei Serienprodukten zu vermeiden,
- die Änderbarkeit von voreingestellten Anmeldedaten gewährleisten, etwa durch die Möglichkeit zur Passwortänderung,

- eine Rollen- und Rechteverwaltung für Benutzerkonten unterstützen, die mindestens zwischen regulärer Nutzung und administrativen Tätigkeiten unterscheidet,
- die Absicherung kritischer Funktionen durch PINs oder Passwörter ermöglichen, beispielsweise bei Käufen, Zahlungen oder Änderungen von Systemeinstellungen,
- eine Protokollierung von Zugriffsversuchen und Änderungen mittels schreibgeschützter Audit-Logs vorsehen,
- automatische Benachrichtigungen bei sicherheitsrelevanten Aktivitäten (beispielsweise per E-Mail oder Push-Nachricht auf das Smartphone) unterstützen,
- die Deaktivierung von Benutzerkonten erlauben, um bei Bedarf den Zugriff dauerhaft zu sperren,
- sowie die sichere Löschung von Daten (beispielsweise durch Zurücksetzen auf Werkseinstellungen) ermöglichen, insbesondere vor der Weitergabe oder Entsorgung von Geräten

Neben den technischen Voraussetzungen ist auch eine organisatorische Umsetzung auf Seiten der Anwendenden erforderlich. Dazu zählen Maßnahmen wie die Anlage mehrerer Benutzerkonten mit unterschiedlichen Berechtigungsstufen, der Einsatz sicherer Authentisierungsverfahren, die Änderung von Standardpasswörtern sowie die konsequente Nutzung verfügbarer Sicherheitsfunktionen. Diese organisatorischen Schritte sind als Maßnahmen in der Maßnahmentabelle aus AP02 angeführt.

6.3.2 Anwendungsfall #2: Jugendschutz

Für den zweiten Anwendungsfall wurden folgende potenzielle Bedrohungen (Tabelle 20) zusammengefasst und die daraus resultierenden Anforderungen festgelegt:

Tabelle 20 Anwendungsfall #2: Jugendschutz (Bedrohung und die davon betroffenen Produktlebensphasen)

Bedrohung(en)	***Betroffene Produktlebensphasen***
Problematische Inhalte für Jugendliche und Kinder	1. Auswahl & Kauf 2. Betrieb & Wartung 3. Entsorgung

Die zunehmende Digitalisierung in allen Lebensbereichen führt dazu, dass bereits Kinder und Jugendliche regelmäßig mit potenziell gefährlichen Inhalten oder Akteuren im Internet konfrontiert werden. Gleichzeitig besteht das Risiko, dass Minderjährige unbewusst oder aus Neugier sicherheitsrelevante Änderungen an Geräten vornehmen oder Funktionen nutzen, die mit Kosten verbunden sind oder die IT-Sicherheit und Privatsphäre des Haushalts beeinträchtigen können.

Aus diesen Gründen ist es erforderlich, den Zugriff auf Inhalte sowie die Berechtigungen zum Ausführen bestimmter Funktionen bei digitalen Geräten und Diensten gezielt zu regeln. Technische Schutzmechanismen sollten Eltern und Erziehungsberechtigten ermöglichen, die digitale Nutzung altersgerecht zu gestalten und gleichzeitig die Integrität der Systeme zu wahren.

Für Privathaushalte mit Kindern und Jugendlichen ergeben sich daraus folgende technische Anforderungen an digitale Produkte und Dienste:

- die Möglichkeit, für kritische Funktionen wie Käufe, Bezahlvorgänge oder Änderungen an Einstellungen und Passwörtern eine zusätzliche Authentisierung mittels PIN oder Passwort zu verlangen,
- die Unterstützung von Inhaltsfiltern für Online-Datendienste, Streaming-Plattformen und vergleichbare Anwendungen, um ungeeignete Inhalte zu blockieren,
- die Möglichkeit zur zeitlichen und funktionalen Steuerung der Nutzung, etwa durch Begrenzung der Berechtigungen und Nutzungsdauer einzelner Geräte oder Anwendungen,
- die Unterstützung mehrerer Benutzerkonten oder Profile, um die Trennung von Nutzerrollen innerhalb des Haushalts zu ermöglichen,

- die Implementierung einer Rollen- und Rechteverwaltung, die mindestens zwischen administrativer Steuerung und reiner Nutzung unterscheidet,
- die Bereitstellung von automatischen Benachrichtigungen (beispielsweise per E-Mail oder Push-Mitteilung), wenn sicherheitsrelevante oder kostenpflichtige Aktionen durchgeführt werden,
- sowie die Unterstützung von Verschlüsselungsmechanismen für lokal gespeicherte Daten, beispielsweise durch Festplattenverschlüsselung, um unbefugten Zugriff zu verhindern.

Die zugehörigen organisatorischen Maßnahmen zur praktischen Umsetzung dieser Anforderungen sind in der entwickelten Maßnahmentabelle aus AP02 dokumentiert.

6.3.3 Anwendungsfall #3: Mehrere Administrator-Accounts

Für den dritten Anwendungsfall wurden folgende potenzielle Bedrohungen (Tabelle 21) zusammengefasst und die daraus resultierenden Anforderungen festgelegt:

Tabelle 21 Anwendungsfall #3: Mehrere Administrator-Accounts (Bedrohungen und die davon betroffenen Produktlebensphasen)

Bedrohung(en)	***Betroffene Produktlebensphasen***
Ausfall des technischen Verantwortlichen	1. Auswahl & Kauf 2. Betrieb & Wartung 3. Entsorgung
Abhängigkeit aufgrund *Digital Gender Gap*	1. Auswahl & Kauf 2. Betrieb & Wartung 3. Entsorgung

Der sogenannte *Digital Gender Gap* stellt ein strukturelles und im häuslichen Umfeld weit verbreitetes Phänomen dar. In vielen Privathaushalten übernimmt der männliche Partner üblicherweise die Verantwortung für technische Geräte, Netzwerke und digitale Dienste. Er installiert, konfiguriert und administriert diese Systeme selbstständig. Diese Rollenverteilung führt in der Praxis zu zwei wesentlichen Risiken: Zum einen entsteht eine Abhängigkeit von der technisch verantwortlichen Person, die den Zugriff und die Nutzung digitaler Produkte kontrolliert. Zum anderen besteht bei einem Ausfall dieser Person, beispielsweise durch Abwesenheit, Krankheit oder Trennung, die Gefahr, dass Geräte, Daten oder Dienste für andere Haushaltsmitglieder nicht mehr verfügbar sind.

Zur Reduzierung dieser Abhängigkeiten sollten daher auf gemeinsam genutzten Geräten und Diensten mehrere administrative Benutzerkonten eingerichtet werden. Durch die Existenz eines zweiten oder alternativen Administrator-Accounts bleibt die Möglichkeit erhalten, notwendige administrative Tätigkeiten selbstständig durchzuführen. Dies trägt dazu bei, den Zugang zu digitalen Ressourcen dauerhaft sicherzustellen und die Abhängigkeit von einzelnen Personen, insbesondere im Kontext geschlechtsspezifischer Arbeitsteilung, zu verringern.

Dieser Anwendungsfall ist klar von jenen Geräten und Diensten abzugrenzen, die ausschließlich personenbezogen genutzt werden und besonders schützenswerte Informationen enthalten, wie persönliche Smartphones, Laptops oder Social-Media-Konten. In solchen Fällen wäre ein zusätzlicher administrativer Zugang kontraproduktiv.

Die technischen und organisatorischen Anforderungen zur Implementierung eines zusätzlichen Administrators in Privathaushalten lassen sich wie folgt zusammenfassen:

- Technische Anforderungen:
  - Unterstützung zur Sicherung und Wiederherstellung von Konfigurationsdateien, um Geräteeinstellungen im Bedarfsfall rekonstruieren zu können,
  - Möglichkeit zur Anlage mehrerer Benutzerkonten, einschließlich separater Administrator-Accounts,

- Unterstützung einer Rollen- und Rechteverwaltung, die zwischen Nutzung und Administration unterscheidet,
- Bereitstellung einer Funktion zum Zurücksetzen auf Werkseinstellungen (Factory Reset),
- Möglichkeit zur Deaktivierung von Benutzerkonten, um ungenutzte Zugänge zu sperren,
- sowie Unterstützung einer Protokollierungsfunktion (Audit-Log) zur Nachverfolgung von Zugriffsversuchen und Änderungen, vorzugsweise in schreibgeschützter Form.

- Organisatorische Anforderungen:
  - Einrichtung von mindestens zwei Administrator-Accounts auf gemeinsam genutzten Geräten, um den dauerhaften Zugriff unabhängig von einzelnen Personen zu gewährleisten,
  - sowie Verwendung eines gemeinsamen Passwortmanagers für alle gemeinsam genutzten Geräte und digitalen Dienste (Alternative).

6.3.4 Anwendungsfall #4: Vorsorge gegen Machtmissbrauch & digitale Gewalt

Für den vierten Anwendungsfall wurden folgende potenzielle Bedrohungen (Tabelle 22) zusammengefasst und die daraus resultierenden Anforderungen festgelegt:

Tabelle 22 Anwendungsfall #4: Vorsorge gegen Machtmissbrauch & digitale Gewalt (Bedrohungen und die davon betroffenen Produktlebensphasen)

Bedrohung(en)	***Betroffene Produktlebensphasen***
Machtmissbrauch / Missbrauch von Berechtigungen	1. Auswahl & Kauf 2. Betrieb & Wartung 3. Entsorgung
Digitale Gewalt im Privatbereich, inkl. digitale Überwachung, Kontrolle und Machtmissbrauch	2. Betrieb & Wartung 3. Entsorgung
Abhängigkeit aufgrund Digital Gender Gap	1. Auswahl & Kauf 2. Betrieb & Wartung 3. Entsorgung

Parallel zum Anwendungsfall #3 „Mehrere Administrator-Accounts“, der auf die Sicherstellung der Verfügbarkeit gemeinschaftlich genutzter Geräte und Dienste und Kontrollmöglichkeiten abzielt, befasst sich dieser Anwendungsfall mit dem Berechtigungsmanagement zur Wahrung der Vertraulichkeit und Integrität persönlicher Daten und digitaler Produkte.

Auch in diesem Zusammenhang spielt der *Digital Gender Gap* eine relevante Rolle. Die im häuslichen Umfeld häufig bestehende technische Abhängigkeit von einer (zumeist männlichen) Person kann das Risiko von Machtmissbrauch und digitaler Gewalt erheblich erhöhen.

Ein effektives Berechtigungsmanagement soll daher sicherstellen, dass persönliche Daten, Geräte und Konten nur durch autorisierte Personen genutzt und verwaltet werden können und dass Betroffene jederzeit Kontrolle über ihre digitalen Ressourcen behalten.

Für die Umsetzung dieses Ansatzes ergeben sich folgende technische und organisatorische Anforderungen an Verbraucherinnen und Verbraucher sowie an digitale Produkte und Dienste:

- Technische Anforderungen:
  - Unterstützung automatischer Benachrichtigungen (beispielsweise per E-Mail oder Smartphone), wenn sicherheitsrelevante oder administrative Tätigkeiten ausgeführt werden,
  - Bereitstellung verschiedener sicherer Authentisierungsverfahren, insbesondere Multifaktor-Authentisierung mittels Passkeys, biometrischer Merkmale oder PIN-Verfahren (unter

Berücksichtigung, dass solche Verfahren im Kontext digitaler Gewalt potenziell erzwungen werden können),

- Möglichkeit zum Schutz kritischer Funktionen – etwa Käufe, Bezahlvorgänge oder Änderungen an Systemeinstellungen – durch zusätzliche Authentisierung mittels PIN oder Passwort,
- sowie Unterstützung einer Protokollierung von Zugriffsversuchen und Änderungen über schreibgeschützte Audit-Logs, um Manipulationen nachvollziehen und nachweisen zu können.

- Organisatorische Anforderungen:
  - Einrichtung von mindestens zwei Administrator-Accounts auf gemeinschaftlich genutzten Geräten, um Kontrollverlust bei Ausfall einer Person zu vermeiden,
  - Verwendung individueller, starker Passwörter für persönliche Konten unter Einsatz eines Passwortmanagers,
  - Verschlüsselung und sichere Aufbewahrung sensibler Dateien, beispielsweise durch Cloud-Dienste mit einer standardmäßig eingerichteten Ende-zu-Ende-Verschlüsselung für die Kommunikation,
  - gezielte Steuerung von App- und Systemberechtigungen auf persönlichen Geräten, um Zugriffe auf Daten und Funktionen zu kontrollieren,
  - sowie Nutzung von Multifaktor-Authentisierungsmethoden für besonders sicherheitsrelevante Online-Dienste wie E-Mail- oder Identitätskonten.

6.4 Diskussion & Fazit

Die Anforderungen an ein Berechtigungsmanagement in Privathaushalten lassen sich grundsätzlich in technische und organisatorische Anforderungen unterteilen. Orientiert man sich hierbei an etablierten Good Practices, Standards und Normen aus der Industrie und dem privatwirtschaftlichen Umfeld, so zeigt sich, dass viele dieser Prinzipien in angepasster Form auch auf den privaten Bereich übertragbar sind.

Dies erklärt, warum zahlreiche Anforderungen nicht nur für einzelne, sondern für mehrere oder sogar alle Anwendungsfälle gleichermaßen relevant sind und einen nachhaltigen Mehrwert bieten.

Gleichzeitig bestehen jedoch spezifische Bedrohungslagen und Nutzungssituationen, die ausschließlich im privaten Umfeld auftreten und somit modifizierte oder erweiterte Anforderungen an das Berechtigungsmanagement erforderlich machen.

Besonders die technischen Anforderungen spielen bereits bei der Auswahl und Anschaffung digitaler Produkte eine entscheidende Rolle. Nur wenn Geräte und Dienste grundlegende Sicherheits- und Verwaltungsfunktionen unterstützen, können entsprechende Maßnahmen während des Betriebs, der Wartung sowie bei der Entsorgung oder Deaktivierung wirksam umgesetzt werden. Damit wird deutlich, dass IT-Sicherheit im Privathaushalt nicht erst bei der Nutzung, sondern bereits bei der produktseitigen Gestaltung und Kaufentscheidung ansetzt.

Die in diesem Arbeitspaket definierten organisatorischen Maßnahmen seitens der Haushaltmitglieder und technischen Maßnahmen seitens der Hersteller bilden die Grundlage für die Konzeptentwicklung.

7 Ergebnisse aus Arbeitspaket AP05 – Konzeptentwicklung und Szenarioanalyse

7.1 Zielsetzung und Ausgangslage

Dieses Arbeitspaket hatte zum Ziel, drei unterschiedliche Konzepte für die praktische Umsetzung eines IT-Sicherheitsmanagements in Privathaushalten zu entwickeln. Die drei Konzepte sollten basierend auf spezifischen Szenarien analysiert werden, die jeweils einen unterschiedlichen Blickwinkel auf die Verantwortung zur Umsetzung von IT-Sicherheitsmaßnahmen einnehmen.

Für die Entwicklung und Bewertung dieser Konzepte wurden die Erkenntnisse und Ergebnisse aus den vorangegangenen Arbeitspaketen systematisch einbezogen:

- Best Practices (AP02): Identifizierte Maßnahmen und deren Bewertung hinsichtlich Anwendbarkeit und Wirksamkeit,
- Risikoanalyse (AP03): Kritische Bedrohungen für Privathaushalte und geeignete Maßnahmen zur Risikobehandlung,
- Expertenworkshop (AP04): Einschätzungen und Bewertungen von Fachpersonen zu Bedrohungen, Gegenmaßnahmen und Anforderungen an die praktische Umsetzung von Sicherheitsmaßnahmen sowie Forderungen an Hersteller und Gesetzgeber.
- Anwendungsfälle für ein Berechtigungsmanagement (AP04): organisatorische und technische Maßnahmen anhand der Anforderungen für ein Berechtigungsmanagement, die von Privathaushalten umgesetzt oder von Herstellern unterstützt und implementiert werden müssen.

Der inhaltliche Schwerpunkt der Analysen lag auf der Auswahl und Bewertung jener Bedrohungen und risikomindernden Maßnahmen, die besonders im Kontext eines Berechtigungsmanagement für private Mehrpersonenhaushalte relevant sind.

Für die Untersuchung wurden drei Szenarien vorab definiert, die unterschiedliche Verantwortungs- und Gestaltungsebenen abbilden:

1. Szenario 1 – „**Verhalten ordnet sich unter**“: Dieses Szenario beschreibt organisatorische und verhaltensbezogene Maßnahmen, die unabhängig von technischen Möglichkeiten durch die Haushaltsmitglieder umgesetzt werden können. Die Verantwortung zur Erhöhung der IT-Sicherheit obliegt somit in diesem Szenario alleinig den Haushaltsmitgliedern.
2. Szenario 2 – „**Technik ordnet sich unter**“: Hier steht die technische Umsetzung von Sicherheitsmaßnahmen im Vordergrund, die mit einem geringen Aufwand für die Haushaltsmitglieder verbunden sind und im Wesentlichen durch die Hersteller digitaler Produkte realisiert und forciert wird. In diesem Szenario wird davon ausgegangen, dass ausschließlich die Technik bzw. die Hersteller digitale Produkte „IT-sicher“ machen können.
3. Szenario 3 – „**Vorschriften für Hersteller und Anbieter durch Gesetze und Regularien**“: In diesem Szenario werden regulatorische Ansätze betrachtet, bei denen nationale oder europäische Vorgaben Anforderungen an Hersteller und Anbieter festlegen und vorschreiben, um die IT-Sicherheit und den Datenschutz der Verbraucherinnen und Verbraucher zu gewährleisten.

Im Rahmen der Szenarioanalyse wurde untersucht, wo die Grenzen bei einer einseitigen Betrachtung der Verantwortung zur Umsetzung von IT-Sicherheitsmaßnahmen liegen. Zugleich sollte aufgezeigt werden, wie technologische, organisatorische und gesetzliche Maßnahmen gemeinsam zur Erhöhung der IT-Sicherheit in Privathaushalten beitragen können, indem sich diese Maßnahmen ergänzen oder voneinander abhängen.

7.2 Methodisches Vorgehen

Ausgehend von den in der Risikoanalyse (AP03) und im Expertenworkshop (AP04) identifizierten schwerwiegenden Bedrohungen wurden im Rahmen der drei Szenarien geeignete Maßnahmen abgeleitet, zusammengeführt und bewertet. Dabei bildeten die erstellte Maßnahmentabelle aus AP02 sowie ergänzende Erkenntnisse aus den Diskussionen des Expertenworkshops die zentrale Grundlage für die Auswahl der Maßnahmen.

Alle identifizierten Maßnahmen wurden hinsichtlich ihrer Wirksamkeit, Umsetzbarkeit und Relevanz für den Beispielhaushalt des Projekts geprüft und angewendet. Alle bewerteten Kriterien einer Maßnahme wurden unter dem Begriff „Kosten-Nutzen-Analyse“ angeführt, ähnlich zum „Nutzen-Aufwand-Verhältnis“ aus AP02. Für die Kosten-Nutzen-Analyse in diesem Arbeitspaket wurden jedoch mehrere Aspekte jeder Maßnahme bewertet.

Besonderes Augenmerk lag auf jenen Maßnahmen, die unmittelbar zur Einrichtung und Umsetzung eines Berechtigungsmanagements in Privathaushalten beitragen. Diese wurden im Rahmen der Bewertung entsprechend gekennzeichnet und in spezifische Kategorien eingeordnet, um ihren Beitrag zur organisatorischen und technischen Absicherung nachvollziehbar zu machen.

Im Zuge dieser Analyse wurden die folgenden kritischen Bedrohungen, die sowohl von externen Akteuren als auch von anderen Haushaltsmitgliedern ausgehen können, als besonders relevant identifiziert und in die Szenarien integriert:

Tabelle 23 schwerwiegende Bedrohungen für die Konzeptentwicklung (AP05).

Bedrohungen
Ausspähen von Informationen / Spionage (G 0.14)
Manipulation von Hard- oder Software (G 0.21)
Manipulation von Informationen (G 0.22)
Software-Schwachstellen oder -Fehler (G 0.28)
Unberechtigte Nutzung oder Administration von Geräten und Systemen (G 0.30)
Fehlerhafte Nutzung oder Administration von Geräten und Systemen (G 0.31)
Social Engineering (G 0.42)
Online-Betrug / Cyberkriminalität
sexuelle Belästigung, Cyber-Stalking & Erpressung
problematische Inhalte für Kinder und Jugendliche
Ausfall des technischen Verantwortlichen
Digitale Gewalt im Privatbereich, inkl. digitale Überwachung, Kontrolle und Machtmissbrauch
Abhängigkeit aufgrund Digital Gender Gap

Zur Bewältigung der in Tabelle 23 angeführten Bedrohungen wurden in den nachfolgenden Abschnitten spezifische Maßnahmen für die drei Szenarien entwickelt, beschrieben, bewertet und eine theoretische Umsetzung hinsichtlich Restrisiken untersucht.

Die Maßnahmen in Szenario 1 und Szenario 2 wurden jeweils im Hinblick auf ihr Kosten-Nutzen-Verhältnis bewertet, wobei sich die zugrunde liegenden Bewertungsfaktoren je nach Szenario unterscheiden. Während in Szenario 1 insbesondere die „Anwendbarkeit“ und die These zu den „vier Voraussetzungen“ (Wissen, Zeit, Geld, Motivation) für die Umsetzung von Sicherheitsmaßnahmen im Vordergrund steht, beziehen sich die Bewertungsaspekte in Szenario 2 stärker auf technische Implementierung, Anwendbarkeit und Überprüfbarkeit.

Im Szenario 3 werden ergänzend Vorschläge für regulatorische Vorgaben formuliert, die von Herstellern und Anbietern digitaler Produkte umzusetzen wären. Diese sollen eine rechtliche und normative Grundlage schaffen, um die in Szenario 2 beschriebenen technischen Maßnahmen verbindlich festzulegen und so

zumindest theoretisch ein dauerhaft hohes Sicherheitsniveau für Verbraucherinnen und Verbraucher sicherzustellen.

Die Wirksamkeit der Maßnahmen in allen drei Szenarien wurde anhand der Anwendung auf den fiktiven Beispiel-Haushalt untersucht. Dadurch konnten die jeweiligen Restrisiken identifiziert und die Grenzen der einzelnen Ansätze sichtbar gemacht werden.

7.3 Szenario 1 – Verhalten ordnet sich unter

Im ersten Szenario wurde angenommen, dass sich die bestehenden technischen Rahmenbedingungen nicht verändern bzw. verbessern. Die Verantwortung für die Erhöhung der IT-Sicherheit liegt somit vollständig bei den Haushaltsmitgliedern selbst. Durch organisatorische Maßnahmen und bewusstes Verhalten ist ein angemessenes Sicherheitsniveau herzustellen und ein funktionierendes Berechtigungsmanagement im privaten Umfeld zu etablieren.

Die Bewertung der einzelnen Maßnahmen im Rahmen der Kosten-Nutzen-Analyse orientierte sich an zwei methodischen Grundlagen:

- Zum einen an der in AP02 entwickelten Bewertungsmethodik für die „Anwendbarkeit“ beziehungsweise „Praktikabilität“ gemäß dem Prinzip der „*Usable Security*“. Diese berücksichtigt die Kriterien Robustheit, Erlernbarkeit und Einfachheit (BSI, 2025b).
- Zum anderen orientiert sich die Bewertung an der im Expertenworkshop (AP04) formulierten These der „vier Voraussetzungen zur Umsetzung von IT-Sicherheitsmaßnahmen“: Zeit, Geld, Wissen und Motivation. Der These zufolge bestimmen diese Faktoren maßgeblich, ob und in welchem Umfang Privatpersonen Sicherheitsmaßnahmen tatsächlich umsetzen können.

Aus der Zusammenführung der Ergebnisse aus der Maßnahmentabelle (AP02), der Risikoanalyse (AP03) und den Diskussionen des Expertenworkshops (AP04) ergaben sich für Privathaushalte die nachfolgenden organisatorischen Maßnahmen, die zur Stärkung des Berechtigungsmanagements und zur Erhöhung der IT-Sicherheit beitragen:

- Unterschiedliche Passwörter für unterschiedliche Accounts,
- sichere Passwortwahl,
- Downloads von vertrauenswürdigen Quellen,
- sichere Aufbewahrung von Datensicherungen,
- Abdecken von nicht verwendeten Kameras und Mikrofonen,
- zusätzlicher Admin-Account für gemeinschaftlich genutzte und zentrale Geräte,
- sowie Weiterbildung und Aufklärung bezüglich Gefahren im digitalen Raum.

Zu exemplarischen Zwecken werden in den beiden nachfolgenden Abschnitten zwei der oben genannten Maßnahmen inkl. der Kosten-Nutzen-Analyse und Anwendung auf den Beispiel-Haushalt beschrieben.

Ein Fazit inklusive identifizierte Restrisiken zu Szenario 1 ist am Ende dieses Abschnitts angeführt.

7.3.1 Maßnahme: Unterschiedliche Passwörter für unterschiedliche Accounts

Es sollten für jeden Account unterschiedliche Passwörter verwendet werden, beispielsweise in Kombination mit einem Passwortmanager. Vor allem für kritische Webseiten und Dienste wie Online-Banking-Seiten, Online-Shops, E-Mail-Dienste, digitale Behördengänge oder das hauseigene Drahtlosnetzwerk sollten verschiedene Passwörter gewählt werden, um die Auswirkung eines gestohlenen oder veröffentlichten Passworts zu reduzieren. Wird kein Passwortmanager verwendet, sollten aufgeschriebene Passwörter vor unbefugtem Zugang geschützt werden.

Tabelle 24 Maßnahme aus Szenario 1: „Unterschiedliche Passwörter für unterschiedliche Accounts“ im Rahmen der Konzeptentwicklung

Kosten-Nutzen-Analyse	
Vorteile	• Schadensbegrenzung bei Kompromittierung eines Accounts, sowohl durch interne als auch externe Akteure • in Kombination mit einem Passwortmanager werden Passwörter geschützt bzw. verschlüsselt aufbewahrt
Nachteile	• ohne Passwortmanager müssen Passwörter ggf. aufgeschrieben werden, was wiederum einen unbefugten Zugriff für andere Haushaltsmitglieder erleichtert (internes Risiko).
Zeit	zusätzlicher Zeitaufwand bei jeder Verwendung
Geld	keine zusätzlichen Kosten, da grundsätzlich genügend kostenlose Passwortmanager verfügbar sind
Wissen	Verwendung eines Passwortmanagers erfordert entsprechendes Wissen über dessen Handhabung und sichere Verwendung (bspw. Verschlüsselung, sicheres Master-Passwort zur Entschlüsselung, etc.).
Motivation	Einbußen von Bequemlichkeit könnte hinderlich für die Umsetzung sein
Praktikabilität / Anwendbarkeit	2 von 3 Punkte: Robustheit: ja | Erlernbarkeit: ja | Einfachheit: nein
Kategorie im Berechtigungs-management	Trägt zum **Zugriffsschutz** bei

Verwenden alle Haushaltsmitglieder unterschiedliche Passwörter für ihre Accounts, verringern sich die Auswirkungen eines kompromittierten Accounts. Das gilt sowohl für Fälle, in denen das Passwort für externe Personen offengelegt wurde, als auch jenen Situationen, in denen andere Haushaltsmitglieder ein Passwort erraten oder erlangen. Zudem besteht dadurch die Möglichkeit, einzelne Passwörter gegebenenfalls mit anderen Haushaltsmitgliedern zu teilen.

7.3.2 Maßnahme: zusätzlicher Admin-Account für gemeinschaftlich genutzte und Zentrale Geräte

Eine wesentliche Erkenntnis aus dem Expertenworkshop stellt der *Digital Gender Gap* in Privathaushalten dar: Ein männlicher Mitbewohner bzw. Partner ist oftmals für die Technik im Privathaushalt zuständig. Dadurch ergeben sich unter anderem zwei konkrete Bedrohungen: Die Abhängigkeit vom männlichen Partner zur Nutzung von digitalen Produkten und deren Nicht-Verfügbarkeit bei Ausfall des technischen Verantwortlichen. Es sollten daher mehrere administrative Accounts für jedes Gerät eingerichtet werden, welches von mehreren Haushaltsmitglieder benutzt und nicht ausschließlich für den persönlichen Gebrauch verwendet wird.

Neben der Verbesserung der Verfügbarkeit wird zudem die Möglichkeit geschaffen, eine Art Kontrollinstanz einzuführen, um potenziell böswillige Manipulationen, Einstellungen oder Handlungen zumindest zu hemmen, zu erkennen und gegebenenfalls rückgängig zu machen.

Besteht keine Möglichkeit zur Anlage eines zweiten Admin-Accounts für einen Dienst oder ein Gerät, sollte zumindest der Zugang (bspw. das Passwort) zum Admin-Account zwischen mindestens zwei Personen im Haushalt geteilt werden, beispielsweise über einen gemeinsam genutzten Passwortmanager.

Tabelle 25 Maßnahme aus Szenario 1: „zusätzlicher Admin-Account für gemeinschaftlich genutzte und zentrale Geräte“ im Rahmen der Konzeptentwicklung

Kosten-Nutzen-Analyse	
Vorteile	• erhöhte Verfügbarkeit für gemeinschaftlich genutzte und zentrale Geräte • Möglichkeit zur Kontrolle und Abschwächung der Abhängigkeit einer Person mit Administratorrechten
Nachteile	• gegebenenfalls erhöhtes Konfliktpotenzial bei unterschiedlichen Meinungen und Absichten zwischen Haushaltsmitgliedern mit Administratorrechten (Freischaltungen/Sperren, o.Ä.)
Zeit	Es fällt lediglich initial ein geringer, zusätzlicher Zeitaufwand an.
Geld	Ein zweiter Admin-Account oder ein Teilen der Zugangsdaten zu einem Admin-Account verursachen in der Regel keine zusätzlichen Kosten.
Wissen	Je nach Dienst oder Gerät muss die Einrichtung eines zweiten Admin-Accounts bzw. die Rechtevergabe bekannt sein.
Motivation	Die bewusste Abhängigkeit und Überlassung der Kontrolle, beispielsweise als Liebesbeweis oder aufgrund von Desinteresse für gemeinschaftlich genutzte Geräte oder Dienste kann für die Umsetzung dieser Maßnahme hinderlich sein. Das Risiko einer plötzlichen Nicht-Verfügbarkeit einer zentralen, technischen Ansprechperson oder von mutwilligen, böswilligen Handlungen durch diese Person kann unterschätzt werden.
Praktikabilität / Anwendbarkeit	2 von 3 Punkte: Robustheit: nein | Erlernbarkeit: ja | Einfachheit: ja
Kategorie im Berechtigungs-management	Trägt zur Nachvollziehbarkeit und der Einhaltung eines 4-Augen-Prinzips bei

Ein zweiter Admin-Account auf jedem Gerät, das gemeinschaftlich genutzt wird, teilt die Verantwortung bzw. Kontrolle über das Gerät unter Haushaltsmitgliedern auf. Für den Beispiel-Haushalt würde es sich anbieten, dass die beiden Elternteile bzw. die bereits volljährige Tochter jeweils einen Admin-Account auf diesen Geräten eingerichtet haben. Damit wird die Verfügbarkeit für notwendige Änderungen (beispielsweise Jugendschutzeinstellung) erhöht und kann vom anderen Elternteil jederzeit kontrolliert werden. Außerdem beugt es einem unerkannten Machtmissbrauch vor. Für Geräte, welche die Anlage von zusätzlichen Admin-Accounts nicht unterstützen, könnte das Passwort zwischen den Elternteilen geteilt werden. Dabei ist zu beachten, dass kein persönlich genutztes Passwort eines Elternteils verwendet wird.

7.3.3 Fazit zu Szenario 1 und Restrisiken

Trotz einer Umsetzung von organisatorischen Maßnahmen verblieben für dieses Szenario Restrisiken, die gegebenenfalls durch technische Maßnahmen adressiert werden müssen:

Werden unterschiedliche Passwörter für unterschiedliche Accounts sowie ausschließlich sichere Passwörter von den Haushaltsmitgliedern verwendet, steigt das Risiko, dass diese Passwörter aufgeschrieben werden. In einem Mehr-Personen-Haushalt läuft man somit Gefahr, dass die aufgeschriebenen Passwörter von jemand anderen gefunden und somit offengelegt werden. Als technische Maßnahme würde hier ein Passwortmanager Abhilfe leisten, dessen Handhabung wiederum erlernt werden muss.

Der Bezug von Software von ausschließlich vertrauenswürdigen Quellen kann nicht zu 100% gewährleisten, dass die Software auch tatsächlich sicher ist bzw. erzeugt gegebenenfalls ein Gefühl falscher Sicherheit hinsichtlich Software-Schwachstellen. Die Entscheidung liegt schlussendlich immer bei den Anwendenden selbst, welche Quelle als „vertrauenswürdig“ erachtet wird, was wiederum das Risiko von potenziellen Fehleinschätzungen impliziert. Als technische Gegenmaßnahme bietet sich für diesen Fall eine installierte

bzw. integrierte Anti-Virus-Software an oder die Nutzung eines offiziellen App-Repository wie dem Google Play Store für Android basierte Systeme bzw. App Store für Produkte von Apple. Alternativ können Webdienste dazu verwendet werden, Softwarepakete zu scannen (beispielsweise „virustotal.com“).

Bei der sicheren Aufbewahrung von Datensicherungen hängt das Sicherheitsniveau hinsichtlich Vertraulichkeit vom Schlüssel zur Ver- und Entschlüsselung der Daten ab. Wird dieser Schlüssel nicht angemessen vor unbefugtem Zugang oder Zugriff geschützt, besteht das Risiko einer Offenlegung von Daten weiterhin. Zusätzlich ist die Auswahl von sicheren Verschlüsselungsalgorithmen eine Voraussetzung für den angemessenen Schutz von Datensicherungen. Dies wiederum setzt gewisse technische Fähigkeiten seitens der Haushaltsmitglieder voraus sowie die Unterstützung und der standardmäßige Gebrauch von sicheren Verschlüsselungsalgorithmen seitens der Verschlüsselungssoftware.

Werden mehrere Admin-Accounts bei gemeinschaftlich genutzten Geräten angelegt, reduziert dies die Bedrohung von Digitaler Gewalt nur geringfügig. Wird ein Administrationspasswort geteilt, sind Tätigkeiten über diesen Account nicht mehr eindeutig zuordenbar. Für eine effektive Umsetzung dieser Maßnahme bedarf es zusätzlicher technischer Funktionen, welche das Monitoring und die Kontrolle von Änderungen effizient ermöglichen (Push-Meldungen, E-Mail-Benachrichtigungen, Schutz von anderen Admin-Passwörtern, etc.). Eine sichere Umsetzung setzt außerdem voraus, dass die Admin-Accounts der gemeinschaftlich genutzten Applikation auf dem Gerät nicht den Betriebssystem-internen Accounts mit systemweiten Zugriffsrechten entsprechen wie etwa „root“ bei Unix-basierten Systemen oder „Administrator“[5] auf Windows-Systemen.

Trotz Weiterbildung im Bereich der IT-Sicherheit verbleibt stets ein Restrisiko hinsichtlich Fahrlässigkeit, einem Unterschätzen von Risiken oder schwindender Motivation, beispielsweise aufgrund von Bequemlichkeiten oder deren Verlust bei der Umsetzung von IT-Sicherheitsmaßnahmen. Effektive, technische Sicherheitsmaßnahmen können dabei Abhilfe leisten, unterschiedlichste Risiken zu behandeln und die IT-Sicherheit in Privathaushalten erhöhen.

Der potenzielle Grad einer Reduktion von Bedrohungen bzw. Risiken, durch technische Sicherheitsmaßnahmen, welche ohne großen Zusatzaufwand für Privatpersonen erzeugen, wurde in Szenario 2 untersucht.

7.4 Szenario 2 – Technik ordnet sich unter

In diesem Szenario wurde untersucht, in welchem Umfang Hersteller und Anbieter durch die Umsetzung technischer Maßnahmen in ihren Produkten und Diensten die IT-Sicherheit von Verbraucherinnen und Verbrauchern erhöhen konnten. Im Mittelpunkt stand die Frage, inwieweit technische Systeme den Schutz der Nutzerinnen und Nutzer aktiv unterstützen und diese gleichzeitig von sicherheitsrelevanten Eigenverantwortlichkeiten entlasten konnten.

Die betrachteten Maßnahmen erforderten entweder keine oder nur eine minimale Interaktion seitens der Verbraucherinnen und Verbraucher. Zugleich dienten sie dazu, den in Szenario 1 identifizierten Restrisiken entgegenzuwirken, die aus fehlerhaftem oder unterlassenem sicherheitsbewusstem Verhalten resultierten.

Die Bewertung der Maßnahmen im Rahmen der Kosten-Nutzen-Analyse orientierte sich, wie auch das Szenario 1, an den Prinzipien der „*Usable Security*“ (BSI, 2025b) und demnach an den Kriterien Robustheit, Erlernbarkeit und Einfachheit. Im Sinne des Leitgedankens „Technik ordnet sich unter“ war diesbezüglich anzustreben, dass alle drei Kriterien bei jeder Maßnahme erfüllt waren. War dies nicht der Fall, konnte dies als Hinweis darauf gewertet werden, dass es sich um technisch komplexere Maßnahmen handelte, die mit Restrisiken behaftet waren und eine sorgfältige Umsetzung durch die Hersteller erforderten.

Darüber hinaus wurde eine subjektive Ersteinschätzung der Überprüfbarkeit der Maßnahmen für die Bewertung herangezogen. Diese Überprüfbarkeit bezieht sich auf sowohl externes Fachpersonal, wie etwa

[5] An dieser Stelle ist der „Administrator“-Account gemeint, nicht die Rolle!

Auditorinnen und Auditoren qualifizierter Prüfstellen als auch durch Anwendende ohne besondere technische Vorkenntnisse.

Die Bewertung in dieser Form hatte zum Zweck, eine differenzierte Einschätzung der technischen Umsetzbarkeit, Nachvollziehbarkeit und Transparenz der Maßnahmen für alle relevanten Akteursgruppen zu gewährleisten.

Für das Szenario 2 ergaben wurden folgende Maßnahmen ausgearbeitet:

- standardmäßiger Einsatz aktueller Verschlüsselungsstandards und sicherer Protokolle,
- standardmäßige Aktivierung von automatischen Updates,
- Möglichkeit zur Anlage und Steuerung von Benutzeraccounts,
- Schutz von kritischen Funktionen via PIN oder Passwort,
- Trennung zwischen Standard- und Adminuser (rollenbasierte Berechtigungen),
- rigorose App- & Programmzugriffsbeschränkungen auf Daten und andere Dienste,
- manipulationsgeschütztes Auditlog,
- sowie Zwang zur sicheren Authentisierung.

Zu exemplarischen Zwecken werden in den beiden nachfolgenden Abschnitten zwei der oben genannten Maßnahmen inkl. der Kosten-Nutzen-Analyse und Anwendung auf den Beispiel-Haushalt beschrieben.

Ein Fazit inklusive identifizierte Restrisiken zu Szenario 2 ist am Ende dieses Abschnitts angeführt.

7.4.1 Maßnahme: Möglichkeit zur Anlage und Steuerung von Benutzeraccounts

Als Grundlage für ein benutzerbasiertes Berechtigungsmanagement sollte seitens der Hersteller und Anbieter von digitalen Produkten die Anlage von Benutzeraccounts beziehungsweise Profilen ermöglicht werden, um die Steuerung von Berechtigungen zu ermöglichen. Ein Gerätepasswort, das entweder nur einer Person bekannt ist oder mit mehreren Personen im Haushalt geteilt wird, erhöht unter anderem das Risiko von Machtmissbrauch bzw. nicht-nachvollziehbaren Änderungen durch mehrere Personen.

Systeminterne Benutzer mit systemweiten Zugriffsberechtigungen (beispielsweise „root“ für Unix-basierte Systeme oder „Administrator“ für Windows-Systeme) sollten gut geschützt werden und in der Regel nicht für die Endanwender zur Verfügung stehen.

Tabelle 26 Maßnahme aus Szenario 2: „Möglichkeit zur Anlage und Steuerung von Benutzeraccounts“ im Rahmen der Konzeptentwicklung

Kosten-Nutzen-Analyse	
Vorteile	• Grundlage für die Steuerung von Berechtigungen für mehrere Personen • reduziert das Risiko von Machtmissbrauch und nicht-nachvollziehbaren Änderungen
Nachteile	• Benutzer müssen initial angelegt werden
Praktikabilität/ Anwendbarkeit	3 von 3 Punkte: Robustheit: ja | Erlernbarkeit: ja | Einfachheit: ja
Überprüfbarkeit für externe Fachpersonen gegeben?	ja
Überprüfbarkeit für Endanwender gegeben?	ja
Kategorie im Berechtigungs-management	Grundlage für die Umsetzung einer Zugriffssteuerung auf Benutzerbasis

Die Möglichkeit zur Anlage von separaten Benutzeraccounts- bzw. Profilen auf Geräten und für Anwendungen stellt die technische Grundlage für die Zugriffssteuerung und einem angemessenen Berechtigungsmanagement unter den Haushaltsmitgliedern dar. Jedes Haushaltsmitglied, das einen Dienst oder ein Gerät benutzt, kann für seinen individuellen Userkontext mit gegebenenfalls unterschiedlichen Berechtigungen ausgestattet werden.

7.4.2 Maßnahme: Schutz von kritischen Funktionen via PIN oder Passwort

Bestimmte Funktionen bei Geräten oder Diensten, welche negative Auswirkungen aufgrund einer Ausführung durch Unbefugte zur Folge hätten, sollten durch eine PIN oder ein Passwort geschützt werden. Dabei kann es sich beispielsweise um Funktionen handeln, die zusätzliche Kosten verursachen, die Installation von zusätzlicher Softwarepakete oder das Ändern von Sicherheitsparametern. Als zusätzlichen Schutz der Verfügbarkeit von Diensten und der Vertraulichkeit von Daten sollte diese Maßnahme standardmäßig von den Herstellern oder Anbietern bei ihren Produkten bzw. Diensten umgesetzt werden.

Tabelle 27 Maßnahme aus Szenario 2: „Schutz von kritischen Funktionen via PIN oder Passwort“ im Rahmen der Konzeptentwicklung

Kosten-Nutzen-Analyse	
Vorteile	Schutz vor unberechtigter Ausführung kritischer Funktionen
Nachteile	zusätzliche Authentisierung notwendig
Praktikabilität/ Anwendbarkeit	3 von 3 Punkte: Robustheit: ja | Erlernbarkeit: ja | Einfachheit: ja
Überprüfbarkeit für externe Fachpersonen gegeben?	Ja
Überprüfbarkeit für Endanwender gegeben?	Ja
Kategorie im Berechtigungs-management	trägt zum Zugriffsschutz bei

Werden kritische Funktionen auf Geräten oder in Anwendungen durch die erneute Eingabe eines Passworts oder PINs geschützt, kann damit zumindest ein rudimentäres Berechtigungsmanagement (Passwort oder PIN muss bekannt sein) umgesetzt werden. Als zusätzliche Abfrage neben einer bereits integrierten Zugriffssteuerung durch Profile oder Benutzeraccounts schützt es Endanwender mit erhöhten Rechten vor potenziell unbeabsichtigten Aktionen mit negativen Auswirkungen auf die Sicherheit des Produkts und Daten oder Kosten. Das Passwort könnte im Falle des Beispiel-Haushalts nur den beiden Eltern, der erwachsenen Tochter oder gegebenenfalls der Großmutter bekannt sein.

7.4.3 Fazit zum Szenario 2 und Restrisiken

Auch wenn die angeführten, technischen Maßnahmen einen wesentlichen Beitrag zum Schutz aller Haushaltsmitglieder leisteten, verblieben bestimmte Restrisiken. Diese können in der Regel nicht ausschließlich durch zusätzliche, rein technische Maßnahmen behandelt werden, sondern benötigen mitunter die Awareness und Umsetzung von Maßnahmen durch die Privathaushalte selbst.

Das Passwort für die Entschlüsselung von lokalen Daten (beispielsweise durch Festplattenverschlüsselung) kann vergessen oder offengelegt werden. Eine sichere Aufbewahrung, wie etwa durch Verwendung eines Passwortmanagers, obliegt schlussendlich den Endanwendern selbst.

Wird ein Gerät oder Dienst außerhalb der regulären Nutzungszeiten von Haushaltsmitgliedern benötigt, könnte die Verfügbarkeit durch eine automatische Installation von Updates beeinträchtigt werden. Endanwender mit erhöhten Privilegien müssen selbst dafür Sorge tragen, gegebenenfalls rechtzeitig einzugreifen und den Updatevorgang, wenn notwendig, verschieben.

Solange nur ein Haushaltsmitglied für die Handhabung von Administratorkonten, sowohl für gemeinschaftlich genutzte als auch persönlich Geräte aller Haushaltsmitglieder, nominiert wird, besteht das Risiko von Machtmissbrauch mit potenziell allen negativen Konsequenzen, inklusive einer Nicht-Verfügbarkeit dieser Person. Die Mitglieder eines Haushalts müssen gemeinsam entscheiden, wer auf welchem Gerät und Dienst zusätzlich Administrationsrechte erhält und gegebenenfalls auch nutzt.

Übersteigt die Anzahl an unterschiedlichen Berechtigungen und deren Freigabefrequenz für Anwendungen und Dienste ab einem Punkt die Kapazitäten von Haushaltsmitgliedern mit entsprechenden Privilegien, sowohl mental als auch zeitlich, besteht das Risiko, dass diese ohne weiteres Nachdenken freigegeben werden.

Die technischen Maßnahmen seitens Hersteller und Anbieter verursachen in der Regel höhere Kosten bei der Entwicklung und laufenden Unterstützungsleistungen, wie etwa das Bereitstellen von (Sicherheits-) Updates. Um die Wettbewerbsfähigkeit von digitalen Produkten und Diensten aufgrund dieser Umstände zu wahren, benötigt es mitunter einheitliche Regelungen und Standards, sowohl auf nationaler als auch europäischer Ebene. Diesem Aspekt wird im dritten Szenario Rechnung getragen, indem Vorschläge seitens Verpflichtungen für Hersteller und Anbieter genannt werden, welche die Erhöhung der IT-Sicherheit für und den Schutz der Privatsphäre von Haushaltsmitglieder von Privathaushalten verbessern sollen.

7.5 Szenario 3 – Vorschriften für Hersteller und Anbieter

Dieses Szenario befasste sich mit der Entwicklung von Vorschlägen für regulatorische Vorgaben und Maßnahmen für Hersteller und Anbieter digitaler Produkte, die darauf abzielen, die IT-Sicherheit sowie den Schutz der Privatsphäre von Verbraucherinnen und Verbrauchern zu stärken. Dabei wurde untersucht, in welchem Umfang rechtliche und normative Rahmenbedingungen dazu beitragen könnten, Sicherheitsstandards verbindlich zu gestalten und deren Einhaltung über den gesamten Lebenszyklus digitaler Produkte hinweg sicherzustellen.

Bereits bestehende europäische Regelwerke, insbesondere der Cyber Resilience Act (Verordnung (EU) 2024/2847), legten verbindliche Mindestanforderungen für Produkte mit digitalen Komponenten fest. Diese umfassten sowohl Aspekte der sicheren Entwicklung als auch der laufenden Unterstützungsleistungen (beispielsweise Bereitstellung von Sicherheitsupdates).

Das Szenario knüpfte an diese bestehenden Vorgaben an und zielte darauf ab, zusätzliche Handlungsempfehlungen und Ergänzungen zu identifizieren, die über die regulatorischen Mindeststandards hinausgehen und eine nachhaltige Verbesserung der IT-Sicherheit im privaten Umfeld ermöglichen könnten. Im Mittelpunkt standen vier zentrale Maßnahmen, die sowohl technische als auch regulatorische Aspekte umfassten und sich ergänzend zu den im Szenario 2 beschriebenen technischen Maßnahmen verhielten.

7.5.1 Vorschrift für security by design

Hersteller digitaler Produkte sollten verpflichtet werden, das Prinzip von *security by design* über den gesamten Entwicklungsprozess hinweg umzusetzen. Dieses Prinzip fordert, dass IT-Sicherheitsaspekte bereits von Beginn an in die Produktentwicklung integriert und in allen Produkt-Lebenszyklusphasen hinweg berücksichtigt werden.

Ziel war es, die Angriffsfläche digitaler Systeme zu minimieren und sicherzustellen, dass mögliche Schwachstellen frühzeitig erkannt, behoben und zukünftig vermeidbar gemacht werden konnten.

Der Cyber Resilience Act greift diesen Ansatz bereits auf und schrieb für alle Produkte mit digitalen Komponenten innerhalb der Europäischen Union entsprechende Verpflichtungen für Hersteller und Händler vor.

7.5.2 Vorschrift für security by default

Darüber hinaus sollten Hersteller verpflichtet werden, ihre Produkte bereits bei der Auslieferung mit sicheren Standardeinstellungen zu versehen, um dem Prinzip von *security by default* zu entsprechen.

Dies bedeutet, dass digitale Geräte und Dienste unmittelbar nach der Inbetriebnahme ein angemessenes Schutzniveau bieten müssen, ohne dass die Endanwender zunächst sicherheitsrelevante Konfigurationen vornehmen müssen.

Dadurch könnten Fehlkonfigurationen und daraus resultierende Sicherheitslücken im häuslichen Umfeld deutlich reduziert werden. Auch hierfür sieht der Cyber Resilience Act Regelungen vor.

7.5.3 Kennzeichnung für „IT-sichere“ Produkte und Dienste

Eine weitere Maßnahme sah die Einführung einer einheitlichen Kennzeichnung für IT-sichere Produkte vor. Privatpersonen sollten bereits vor dem Kauf erkennen können, ob ein Produkt bestimmte Mindestanforderungen an Sicherheit und Datenschutz erfüllt oder nicht. Zur Erlangung dieser Kennzeichnung muss das Produkt nachweislich festgelegte Sicherheitsstandards erfüllen, die vor der Markteinführung überprüft werden sollten. Die Kennzeichnung sollte darüber hinaus eindeutig und für potenzielle Käufer offensichtlich angeben, ob die Konformitätsbewertung durch eine unabhängige, qualifizierte Prüfstelle oder durch eine Selbstdeklaration des Herstellers erfolgte.

Der *Cyber Resilience Act* (Verordnung (EU) 2024/2847) sieht bereits eine vergleichbare Regelung vor, indem dieser vorschreibt, dass Produkte mit digitalen Komponenten bei Erfüllung der Anforderungen eine CE-Kennzeichnung erhalten. Für die Kategorie „Standard“, der die meisten Haushaltsprodukte zugeordnet sind, ist jedoch keine verpflichtende unabhängige Prüfung für den Erhalt der CE-Kennzeichnung vorgesehen. Hersteller können hier eine Selbstbewertung durchführen und die Konformität eigenständig bestätigen. Für die Konsumenten ist auf Basis der CE-Kennzeichnung somit allein nicht ersichtlich, ob eine unabhängige Überprüfung stattgefunden hatte oder ob es sich um eine Selbsterklärung des Herstellers handelt. Daher wird empfohlen, eine transparente Erweiterung dieser Kennzeichnung einzuführen, die diesen Unterschied klar erkennbar macht.

7.5.4 Anwendung und Auswirkung der Maßnahmen auf den Beispiel-Haushalt

Mit gesetzlichen Verpflichtungen für Hersteller und Anbieter von digitalen Produkten zur Einhaltung von Prinzipien wie *security by design* und *security by default* könnten die Haushaltsmitglieder bei der Auswahl, der Anschaffung und dem Betrieb darauf vertrauen, dass diese Produkte ein angemessenes Niveau an IT-Sicherheit bereitstellen. Einstellungen zur Übermittlung von optionalen Daten müssten von den Haushaltsmitgliedern bewusst aktiviert und nicht mehr bei der Installation identifiziert und manuell deaktiviert werden. Sie können außerdem den Standardeinstellungen bei der Auslieferung eines Geräts dahingehend vertrauen, dass diese sicher sind.

Eine einheitliche Kennzeichnung für IT-sichere Produkte würde zudem Transparenz schaffen und Kaufentscheidungen vereinfachen. Verbraucherinnen und Verbraucher könnten auf einen Blick erkennen, inwieweit ein Produkt unabhängig geprüft wurde und welchem Sicherheitsniveau es entspricht.

Dies würde nicht nur Vertrauen fördern, sondern auch den zeitlichen und kognitiven Aufwand für Informationsbeschaffung und Konfigurationsentscheidungen deutlich reduzieren.

7.5.5 Fazit zu Szenario 3 und Restrisiken

Die im dritten Szenario vorgeschlagenen gesetzlichen Verpflichtungen für Hersteller und Anbieter zielten im Kern auf dieselben Risiken ab wie die technischen Maßnahmen aus Szenario 2, erweiterten diese jedoch um eine verbindliche regulatorische Dimension. Durch verbindliche Standards und Kennzeichnungen konnten Sicherheitsanforderungen vereinheitlicht und für Endanwender beziehungsweise Konsumenten nachvollziehbar gemacht werden.

Gleichzeitig bleibt ein Restrisiko bestehen: Ein übermäßiges Vertrauen in die Kennzeichnung und in die Eigenverantwortung der Hersteller könnte zu Fahrlässigkeit im Nutzerverhalten führen. Zudem könnte eine Kennzeichnung, insbesondere bei Selbstdeklarationen der Hersteller, keine Garantie für einen umfassenden Schutz vor allen digitalen Bedrohungen bieten.

Um diesem Risiko zu begegnen, wird empfohlen, dass die Überprüfung und Kontrolle solcher Kennzeichnungen durch unabhängige und qualifizierte Stellen erfolgen sollte. Eine zentrale Kontrollinstanz müsste die Ergebnisse der Prüfungen validieren und dokumentieren, um Transparenz und Vertrauen sicherzustellen.

7.6 Diskussion und Fazit zur Konzeptanalyse und -entwicklung

Es konnte gezeigt werden, dass alle drei Konzepte wesentliche Aspekte der IT-Sicherheit und Privatsphäre von privaten Mehrpersonen-Haushalten behandeln. Die jeweils beschriebenen Maßnahmen wirken wesentlichen und schwerwiegenden Bedrohungen, abgeleitet aus der Risikoanalyse und dem Expertenworkshop, entgegen. Wird jedes Szenario für sich betrachtet, verbleiben allerdings nicht zu vernachlässigende Restrisiken für die Endanwender. Aus diesem Grund kann eine einseitige „Verschiebung“ der Verantwortung hin

- zu den Privathaushalten,
- zu den Herstellern und Anbietern von digitalen Produkten oder
- dem Gesetzgeber,

nicht einer effektiven Umsetzung für ein IT-Sicherheitsmanagement in Privathaushalten entsprechen. Um effektiv die IT-Sicherheit für Privathaushalte und deren Haushaltsmitgliedern zu erhöhen, bedarf es der Mitwirkung aller drei genannten Parteien.

Durch die Gesetzgebung muss der Rahmen für einheitliche Standards und Wahrung der Wettbewerbsfähigkeit am Markt für Hersteller und Anbieter geschaffen werden, welche wiederum diese Standards umsetzen müssen und auch nachweisen können. Konsumenten beziehungsweise Endanwender dürfen sich dadurch allerdings nicht in falscher Sicherheit wiegen, sondern müssen dafür Sorge tragen, die technischen Möglichkeiten zum Schutz ihrer IT-Sicherheit und Privatsphäre zu nutzen und unter Haushaltsmitgliedern eine entsprechende Verteilung der Verantwortlichkeiten und Rollen sowie Kontrollmöglichkeiten einführen und aufrechterhalten. Je früher sich Haushaltsmitglieder untereinander auf Rollen und Routinetätigkeiten einigen, desto besser sind sie für zukünftige Entwicklungen und der steigenden Digitalisierung im Privatbereich sowie den potenziell damit einhergehenden Bedrohungen gewachsen und davor geschützt.

8 Empfehlungen und Zukunftsaussichten

8.1 Zusammenspiel der Handlungsebenen

Die im Projekt „IT-Sicherheitsmanagement in Haushalten“ (ISiH) gewonnenen Erkenntnisse verdeutlichen, dass Informationssicherheit im häuslichen Umfeld nur dann nachhaltig gewährleistet werden kann, wenn technische, organisatorische und regulatorische Maßnahmen ineinandergreifen. Die Verantwortung für IT-Sicherheit darf nicht einseitig bei den privaten Haushalten selbst liegen, sondern muss als gemeinschaftliche Aufgabe verstanden werden, an der Individuen, Hersteller und politische Entscheidungsträger gleichermaßen beteiligt sind.

Auf Grundlage der Projektergebnisse ergeben sich daher Empfehlungen für:

1. die **individuelle** Ebene,
2. die **technische** Ebene und
3. die **regulatorische** Ebene.

8.1.1 Individuelle Ebene: Etablierung von Verantwortlichkeiten und Sicherheitsroutinen im Haushalt

Für Privathaushalte ist es essenziell, IT-Sicherheitsmaßnahmen als wiederkehrende Routineaufgaben zu verankern. Dazu gehören beispielsweise regelmäßige Aktualisierungen von Software und Betriebssystemen, die Nutzung starker und unterschiedlicher Passwörter, die Anwendung von Mehrfaktor-Authentisierung, die Anlage von Benutzerkonten, sowie regelmäßige Datensicherungen.

Innerhalb von Mehrpersonenhaushalten müssen Verantwortlichkeiten und Berechtigungen auf zwei Ebenen unterschieden werden:

1. für **persönliche** Geräte und Dienste und
2. für **gemeinschaftlich genutzte** Geräte und Dienste.

Bei persönlichen Geräten, wie etwa Smartphones, Laptops oder individuellen Online-Konten gilt der Grundsatz der Datenhoheit und persönlichen Integrität. Hier ist eine strikte Trennung der Zugriffsrechte erforderlich, sodass keine zweite Person administrative Kontrolle besitzt. Der Schutz persönlicher Konten und Daten dient insbesondere der Wahrung der Privatsphäre und dem Schutz vor Machtmissbrauch oder digitaler Gewalt. Maßnahmen wie starke Authentisierung, der Einsatz von Passwortmanagern und die konsequente Trennung persönlicher und gemeinschaftlicher Nutzung sind hier zentral.

Für gemeinschaftlich genutzte Geräte oder Dienste, wie etwa Netzwerkkomponenten, Smarthome-Systeme oder Familien-Cloudspeicher, gilt hingegen der Grundsatz der geteilten Verantwortung. In diesen Fällen sollten mehrere administrative Zugänge eingerichtet werden, um sowohl die Verfügbarkeit als auch die Nachvollziehbarkeit von Änderungen zu gewährleisten. Durch die Einrichtung mehrerer Administrator-Accounts wird das Risiko verringert, dass eine einzelne Person vollständige Kontrolle über kritische Systeme ausübt oder andere Haushaltsmitglieder von der Nutzung ausschließt. Diese Mehrfach-Administrationsstruktur trägt zur Resilienz des Haushalts bei und wirkt insbesondere Risiken durch Abhängigkeiten oder Machtmissbrauch entgegen.

Daher wird für die individuelle Ebene empfohlen, bereits bei der Anschaffung und Einrichtung digitaler Produkte darauf zu achten, dass diese eine rollenbasierte Benutzerverwaltung unterstützen. Gleichzeitig sollte innerhalb des Haushalts transparent festgelegt werden, welche Personen über administrative Rechte verfügen und in welchem Umfang diese genutzt werden dürfen.

Darüber hinaus sollte die digitale Kompetenz aller Haushaltsmitglieder systematisch gefördert werden. Hierzu zählen nicht nur technische Kenntnisse, sondern auch ein Bewusstsein für die sozialen und organisatorischen Implikationen von IT-Sicherheit. Eine ausgeprägte „Sicherheitskultur im Haushalt“ kann

dazu beitragen, Sicherheitsmaßnahmen als selbstverständlichen Bestandteil des Alltags zu etablieren und die digitale Selbstbestimmung aller Beteiligten zu stärken.

8.1.2 Technische Ebene: Verpflichtung der Hersteller zur Umsetzung von Sicherheitsprinzipien

Hersteller und Anbieter digitaler Produkte tragen maßgeblich zur praktischen Umsetzbarkeit von IT-Sicherheitsmaßnahmen bei. Ihre Verantwortung besteht darin, digitale Produkte und Dienste nach den Prinzipien *security by design*, *security by default* und *„Usable Security"* (BSI, 2025b) zu gestalten:

- *Security by design* verlangt, dass Sicherheitsanforderungen bereits im Entwicklungsprozess berücksichtigt und in der Systemarchitektur verankert werden.
- *Security by default* fordert, dass Geräte und Anwendungen bereits bei der Auslieferung über sichere Standardeinstellungen verfügen, sodass kein sicherheitskritisches Eingreifen durch die Endanwender erforderlich ist.
- *Usable Security* fordert von Sicherheitsmechanismen die Gebrauchstauglichkeit, die Zugänglichkeit für alle Personen sowie eine transparente Wirkungsweise. Diese drei Faktoren werden als Grundlage angesehen, dass Sicherheitsmechanismen akzeptiert und angewendet werden (BSI, 2025b).

Darüber hinaus sollten Hersteller auf benutzerfreundliche und barrierefreie Sicherheitsfunktionen achten. Komplexe Sicherheitskonfigurationen werden von Endanwendern häufig nicht umgesetzt oder fehlerhaft angewendet. Intuitive Benutzeroberflächen, transparente Einstellungen und automatisierte Schutzmechanismen sind daher entscheidend, um Fehlkonfigurationen zu vermeiden.

Empfohlen wird außerdem die Implementierung technischer Schutzmechanismen, die ein rollenbasiertes Berechtigungsmanagement, Audit-Funktionen und mehrstufige Authentisierung unterstützen. Diese Maßnahmen tragen dazu bei, sowohl die Integrität digitaler Systeme als auch die Nachvollziehbarkeit von Änderungen sicherzustellen.

8.1.3 Regulatorische Ebene: Schaffung verbindlicher rechtlicher Rahmenbedingungen

Zur langfristigen Stärkung der IT-Sicherheit in Privathaushalten ist die Politik gefordert, verbindliche Mindeststandards für Hersteller und Anbieter digitaler Produkte festzulegen. Aufbauend auf bestehenden europäischen Regelwerken, insbesondere dem *Cyber Resilience Act* (Verordnung (EU) 2024/2847), sollte der Gesetzgeber ergänzende Regelungen schaffen, die insbesondere folgende Punkte umfassen:

- Verpflichtende Umsetzung der Prinzipien *security by design*, *security by default* und *Usable Security* (BSI, 2025b) für alle Produkte mit digitalen Komponenten,
- Definition von einheitlichen Mindeststandards hinsichtlich zu implementierender IT-Sicherheitsmechanismen für alle digitalen Produkte und Dienste, einschließlich der Möglichkeit zur Umsetzung eines Berechtigungsmanagements (beispielsweise durch die Anlage von Benutzerkonten und vordefinierten Benutzerrollen),
- Weiterentwicklung einer einheitlichen, transparenten Kennzeichnung für IT-sichere Produkte und Dienste, die Verbraucherinnen und Verbrauchern vor dem Kauf signalisiert, ob ein Produkt unabhängig geprüft oder vom Hersteller selbst zertifiziert wurde,
- Förderung von digitaler Bildung als gesellschaftliche Querschnittsaufgabe, um IT-Sicherheitskompetenz bereits im schulischen und außerschulischen Bereich systematisch zu vermitteln.

Diese regulatorischen Maßnahmen schaffen einerseits einheitliche Wettbewerbsbedingungen für Hersteller und Anbieter, andererseits stärken sie das Vertrauen der Verbraucherinnen und Verbraucher in digitale Produkte und Dienste. Sie bilden damit die Grundlage für eine nachhaltige und überprüfbare Qualitätssicherung im digitalen Verbraucherschutz.

8.2 Weiterentwicklung des Risikoanalyse-Konzepts

Ein zentrales Ergebnis des Projekts ist das entwickelte Risikoanalysekonzept aus AP03. Dieses bietet eine systematische und nachvollziehbare Methode, um Risiken in Privathaushalten zu identifizieren, zu bewerten und mit geeigneten Maßnahmen zu behandeln. Besonders hervorzuheben ist, dass das Konzept explizit auf die Heterogenität privater Haushalte ausgelegt ist und somit unterschiedliche technische Ausstattungen, Lebenssituationen und Kompetenzniveaus berücksichtigen kann.

Für die zukünftige Nutzung und zielgerichtete Anwendung dieses Konzepts wird empfohlen, die entwickelte Risikoanalyse in Form einer Webapplikation oder mobilen App bereitzustellen. Endanwenderinnen und Endanwender könnten dabei ihre genutzten Geräte und digitalen Dienste („Assets“) eingeben. Auf Basis dieser Eingaben würde die Anwendung automatisiert eine priorisierte Liste empfohlener Maßnahmen zur Erhöhung der IT-Sicherheit ausgeben.

Eine solche Umsetzung würde nicht nur die Anwendbarkeit des Konzepts erheblich verbessern, sondern auch die Hürden für den praktischen Einsatz in Privathaushalten senken. Durch eine intuitive Benutzeroberfläche, eine adaptive Risikobewertung und regelmäßige Aktualisierung der Maßnahmenkataloge könnte die Anwendung zu einem zentralen Instrument der Verbraucherbildung und Prävention werden.

Darüber hinaus eröffnet ein digitales Risikobewertungstool neue Perspektiven für quantitative empirische Forschung. Die anonymisierte Erfassung realer Nutzungs- und Konfigurationsdaten sowie die Auswertung häufig empfohlener Maßnahmen würden eine datengestützte Analyse des Sicherheitsverhaltens ermöglichen. Dies würde helfen, die im Projekt formulierten Thesen empirisch zu unterlegen, Muster in der digitalen Risikoexposition privater Haushalte zu identifizieren, um somit zukünftige Maßnahmenkataloge evidenzbasiert weiterzuentwickeln.

8.3 Schlussbemerkung

Insgesamt zeigt das Projekt, dass ein wirkungsvolles IT-Sicherheitsmanagement für Privathaushalte nur durch das Zusammenspiel technischer, organisatorischer und regulatorischer Ansätze erreicht werden kann. Die entwickelte Risikoanalyse stellt hierfür einen zentralen methodischen Baustein dar, der die notwendige Differenzierung für heterogene Haushaltsrealitäten ermöglicht. Das Berechtigungsmanagement wiederum bildet einen unverzichtbaren Pfeiler der praktischen Umsetzung, dessen Herausforderungen jedoch besondere Aufmerksamkeit erfordern.

Literaturverzeichnis

BKA und A-SIT. 2025. Prävention - Sicherheitstipps & Tools. [Online] 2025. [Zitat vom: 27. 10 2025.] https://www.onlinesicherheit.gv.at/Themen/Praevention.html.

BSI. 2025a. Basistipps zur IT-Sicherheit. [Online] 10 2025a. [Zitat vom: 27. 10 2025.] https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/cyber-sicherheitsempfehlungen_node.html.

BSI. 2024a. *Befragung zur Cybersicherheit 2024 (CyMon - der Cybersicherheitsmonitor).* 2024a.

BSI. 2017. BSI-Standard 200-3 Version 1.0. [Online] 2017. [Zitat vom: 27. 10 2025.] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_3.pdf?__blob=publicationFile&v=2.

BSI. 2020. Elementare Gefährdungen. [Online] 07. 12 2020. [Zitat vom: 27. 10 2025.] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium/Elementare_Gefaehrdungen.pdf?__blob=publicationFile&v=4.

BSI. 2025f. Schafft die Passwörter ab?! [Online] 2025f. [Zitat vom: 27. 10 2025.] https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Passkeys/passkeys-anmelden-ohne-passwort.html.

BSI. 2025d. Sicherheitstipps im privaten und öffentlichen WLAN. [Online] 2025d. [Zitat vom: 27. 10 2025.] https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Router-WLAN-VPN/Sicherheitstipps-fuer-privates-und-oeffentliches-WLAN/sicherheitstipps-fuer-privates-und-oeffentliches-wlan_nod.

BSI. 2025c. Smarthome – den Wohnraum sicher vernetzen. [Online] 2025c. [Zitat vom: 27. 10 2025.] https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Internet-der-Dinge-Smart-leben/Smart-Home/smart-home_node.html.

BSI. 2023b. Tipps für den sicheren Umgang mit Smart Speakern. [Online] 2023b. [Zitat vom: 27. 10 2025.] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Wegweiser_Checklisten_Flyer/Wegweiser_kompakt_Smart_speaker.pdf?__blob=publicationFile&v=15.

BSI. 2023a. *Tipps für ein sicheres Heimnetzwerk.* 2023a.

BSI. 2025b. Usable Security – Handlungsfelder menschzentrierter Cybersicherheit (Whitepaper #03). 2025b.

ISO/IEC. 2022. ISO/IEC 27005:2022. 4 [Hrsg.] International Organization for Standardization. *Information security, cybersecurity and privacy protection — Guidance on managing information security risks.* s.l. : ISO/IEC JTC 1/SC 27, 2022.

Mitchell, Erica. 2020. *CYBER SECURITY @ HOME: The Effect of Home User Perceptions of Personal Security Performance on Household IoT Security Intentions.* 2020. 1166.

NSA. 2023. BEST PRACTICES FOR SECURING YOUR HOME NETWORK. [Online] 02 2023. [Zitat vom: 27. 10 2025.] https://media.defense.gov/2023/Feb/22/2003165170/-1/-1/0/CSI_BEST_PRACTICES_FOR_SECURING_YOUR_HOME_NETWORK.PDF.

Zeng, Eric und Roesner, Franziska. 2019. Understanding and Improving Security and Privacy in Multi-User Smart Homes: A Design Expoloration and In-Home User Study. [Hrsg.] USENIX Association. *Proceedings of the 28th USENIX Security Symposium.* 08 2019, S. 159-176.

Tabellenverzeichnis

Abbildungsverzeichnis

Anhang A: Exemplarische Maßnahmen aus AP02

In den nachfolgenden Tabellen ist für vier weitere Maßnahmenkategorien eine exemplarische Maßnahme beschrieben, ergänzend zu jenem Beispiel aus Abschnitt 3.4.2.

Maßnahmenkategorie: **Accountsicherheit & Authentisierung**

Tabelle 28 exemplarische Maßnahme „Multi-Faktor-Authentisierung (MFA) – Biometrie“ aus der Kategorie „Accountsicherheit & Authentisierung“

Bezeichnung	***Multi-Faktor-Authentisierung (MFA) - Biometrie***
Kurzbeschreibung	Für den zusätzlichen Faktor für die Authentisierung sollte, wenn verfügbar, ein biometrisches Merkmal verwendet werden. Biometrische Merkmale haben den Vorteil, dass sie nur schwierig zu fälschen sind und nicht verloren werden können. Die Sicherheit des biometrischen Merkmals hängt jedoch vom Schutz des Geräts ab und wie sicher dieses die biometrischen Informationen aufbewahrt.
Vorteile (+)	• Biometrische Merkmale, wie etwa ein Fingerabdruck, sind nur mit erhöhtem Aufwand zu fälschen und können nicht verloren oder erden. • Biometrische Informationen werden üblicherweise in einem gesonderten, sicherheitskritischen Bereich am System geschützt aufbewahrt. • komfortable in der Anwendung
Nachteile (-)	• besonders hoher Schutzbedarf für aufbewahrte biometrische Informationen notwendig • benötigt ein Gerät zum Lesen bzw. Scannen
Anwendbarkeit	sehr gut (3)
Nutzen<>Aufwand (Priorisierung)	sehr gut (9)
potenzielle, zu schützende Assets	• persönliche Daten • kritische Applikationen (Banking, Online-Shopping, digitale Behördengänge) • Finanzen • sonstige Dienste
technische Voraussetzungen	• Gerät für das sichere Aufbewahren • Einrichtung und Lesen/Scannen der biometrischen Merkmale
nicht betrachtete Aspekte / potenzielle Risiken	keine
Quelle(n)	• Basistipps zur IT-Sicherheit (BSI, 2025a) • Schafft die Passwörter ab?! (BSI, 2025f) • BEST PRACTICES FOR SECURING YOUR HOME NETWORK (NSA, 2023)
Nutzen<>Aufwand: Aufwand (1: hoch - 3: niedrig)"	3
Nutzen<>Aufwand: Nutzen (1: niedrig - 3: hoch)	3

Bezeichnung	*Multi-Faktor-Authentisierung (MFA) - Biometrie*
Anwendbarkeit: Robustheit (1: ja, 0: nein)	1
Anwendbarkeit: Erlernbarkeit (1: ja, 0: nein)	1
Anwendbarkeit: Einfachheit (1: ja, 0: nein)	1

Maßnahmenkategorie: **Benutzergeräte**

Tabelle 29 exemplarische Maßnahme „(automatische) Updates für OS und Anwendungen“ aus der Kategorie „Benutzergeräte“

Bezeichnung	*(automatische) Updates für OS und Anwendungen*
Kurzbeschreibung	Aktualisierungen bzw. Patches schließen entdeckte Fehler und Sicherheitslücken in einem Betriebssystem oder Programm und tragen somit zur Erhöhung der Sicherheit bei. Automatische Updates sind, falls möglich, zu aktivieren.
Vorteile (+)	• Schutz vor gängigen und bekannten Angriffsvektoren • Schwachstellen werden geschlossen
Nachteile (-)	• automatische Aktualisierungen können zu fehlerhaften Systemzuständen führen • manuelle Aktualisierungen sollten zeitnah installiert werden, wodurch ein entsprechender Aufwand entsteht
Anwendbarkeit	moderat (2)
Nutzen<>Aufwand (Priorisierung)	gut (6)
potenzielle, zu schützende Assets	• persönliche Geräte
technische Voraussetzungen	• Betriebssystem oder Applikation darf nicht End-Of-Life (ohne Support) sein
nicht betrachtete Aspekte / potenzielle Risiken	• Kompatibilität zu anderen digitalen Produkten
Quelle(n)	• Basistipps zur IT-Sicherheit (BSI, 2025a) • Prävention (BKA und A-SIT, 2025) • BEST PRACTICES FOR SECURING YOUR HOME NETWORK (NSA, 2023)
Nutzen<>Aufwand: Aufwand (1: hoch - 3: niedrig)"	3
Nutzen<>Aufwand: Nutzen (1: niedrig - 3: hoch)	2
Anwendbarkeit: Robustheit (1: ja, 0: nein)	0
Anwendbarkeit: Erlernbarkeit (1: ja, 0: nein)	1
Anwendbarkeit: Einfachheit (1: ja, 0: nein)	1

Maßnahmenkategorie: **Heimnetzwerk /WLAN**

Tabelle 30 exemplarische Maßnahme „Gast-Netzwerk am WLAN Router einrichten“ aus der Kategorie „Heimnetzwerk / WLAN“

Bezeichnung	***Gast-Netzwerk am WLAN-Router einrichten***
Kurzbeschreibung	Mit einem separaten Gast-Netzwerk können Geräte von Gästen von anderen, persönlichen Geräten oder Smart Devices getrennt werden, auf denen sensible Dienste wie Onlinebanking oder Homeoffice-Anwendungen genutzt werden bzw. persönliche Daten geteilt werden.
Vorteile (+)	• Schutz vor Befall mit Schadsoftware auf persönlichen Geräten durch Gast-Geräte • Wahrung der Vertraulichkeit von persönlichen Daten, welche ggf. im Netzwerk verfügbar sind (Segmentierung) • keine Weitergabe des Schlüssels für das gesicherte, private Netzwerk
Nachteile (-)	• Konfiguration auf Router notwendig
Anwendbarkeit	niedrig (1)
Nutzen<>Aufwand (Priorisierung)	gut (6)
potenzielle, zu schützende Assets	• persönliche Daten • Heimnetzwerk und damit verbundene Geräte
technische Voraussetzungen	• Router muss in der Lage sein, zwei Netzwerke/SSIDs parallel zu betreiben.
nicht betrachtete Aspekte / potenzielle Risiken	• Filtermechanismen für Gast-Netzwerke (URL-Filter, freigegebene Ports, etc.)
Quelle(n)	• Tipps für ein sicheres Heimnetzwerk (BSI, 2023a) • Sicherheitstipps im privaten und öffentlichen WLAN (BSI, 2025d) • CYBER SECURITY @ HOME: The Effect of Home User Perceptions of Personal Security Performance on Household IoT Security Intentions (Mitchell, 2020) • BEST PRACTICES FOR SECURING YOUR HOME NETWORK (NSA, 2023)
Nutzen<>Aufwand: Aufwand (1: hoch - 3: niedrig)"	2
Nutzen<>Aufwand: Nutzen (1: niedrig - 3: hoch)	3
Anwendbarkeit: Robustheit (1: ja, 0: nein)	0
Anwendbarkeit: Erlernbarkeit (1: ja, 0: nein)	1
Anwendbarkeit: Einfachheit (1: ja, 0: nein)	0

Maßnahmenkategorie: **Datensicherheit & Privatsphäre**

Tabelle 31 exemplarische Maßnahme „Abdecken von nicht verwendeten Kameras“ aus der Kategorie „Datensicherheit & Privatsphäre“

Bezeichnung	***Abdecken von nicht verwendeten Kameras***
Kurzbeschreibung	Bei Geräten mit Kameras, wie etwa Laptops, Smartphone oder mit dem Netzwerk verbundenen Spielzeug sollte die Kameralinse abgedeckt werden, wenn sie nicht verwendet wird.
Vorteile (+)	• Schutz vor unbemerkten Aufnahmen / der Privatsphäre • reduzierte Auswirkung auf die Privatsphäre von kompromittierten Kameras
Nachteile (-)	keine
Anwendbarkeit	moderat (2)
Nutzen<>Aufwand (Priorisierung)	sehr gut (9)
potenzielle, zu schützende Assets	• persönliche Daten
technische Voraussetzungen	keine
nicht betrachtete Aspekte / potenzielle Risiken	keine
Quelle(n)	• BEST PRACTICES FOR SECURING YOUR HOME NETWORK (NSA, 2023)
Nutzen<>Aufwand: Aufwand (1: hoch - 3: niedrig)"	3
Nutzen<>Aufwand: Nutzen (1: niedrig - 3: hoch)	3
Anwendbarkeit: Robustheit (1: ja, 0: nein)	1
Anwendbarkeit: Erlernbarkeit (1: ja, 0: nein)	1
Anwendbarkeit: Einfachheit (1: ja, 0: nein)	0

Anhang B: Informationswerte, Assets und Bedrohungen der durchgeführten Risikoanalyse

Informationswerte inkl. Schutzbedarfsbewertung:

Tabelle 32 Informationswerte inklusive Schutzbedarf

Informationswerte	*Schutzbedarf: Vertraulichkeit*	*Schutzbedarf: Integrität*	*Schutzbedarf: Verfügbarkeit*
körperliche Merkmale (Name, Alter, Geschlecht, Größe, Gewicht, etc.)	2: normal	2: normal	1: unkritisch
sensible Zugangsdaten (Passwort, Passkey, Authenticator-Codes, etc.)	4: sehr hoch	2: normal	2: normal
Kontaktdaten (E-Mail, Telefon)	2: normal	2: normal	2: normal
besondere Kategorien personenbezogener Daten (biometrische Daten, ethnische Herkunft, politische Meinungen, religiöse Überzeugungen, Gesundheitsdaten)	3: hoch	3: hoch	1: unkritisch
private Kommunikation (Nachrichten)	3: hoch	2: normal	2: normal
offizielle Kommunikation m. Behörden, Bank, etc.	2: normal	2: normal	2: normal
Standortdaten (live & historisch)	3: hoch	2: normal	2: normal
Bezahlungsmethoden	4: sehr hoch	1: unkritisch	1: unkritisch
finanzielle Informationen	2: normal	1: unkritisch	1: unkritisch
persönliche Dateien (Bilder, Dokumente, etc.)	3: hoch	1: unkritisch	3: hoch
persönliche Vorlieben & Interessen	2: normal	2: normal	1: unkritisch
Bild- & Tonaufnahmen	4: sehr hoch	1: unkritisch	1: unkritisch
sensible / nicht-jugendfreie Inhalte	3: hoch	1: unkritisch	1: unkritisch

Assets inklusive Schutzbedarf:

Tabelle 33 Umgesetzte Risikoanalyse: Assets inklusive Schutzbedarf

Asset	*Schutzbedarf: Vertraulichkeit*	*Schutzbedarf: Integrität*	*Schutzbedarf: Verfügbarkeit*
Smartphone	4: sehr hoch	3: hoch	3: hoch
persönlicher Computer (stationärer PC / Laptop)	4: sehr hoch	3: hoch	3: hoch
Tablet	4: sehr hoch	2: normal	2: normal
Smartwatches	3: hoch	4: sehr hoch	4: sehr hoch
Smarthome- und IoT-Geräte	4: sehr hoch	2: normal	1: unkritisch
Netzwerkgeräte: Router, Modem, Accesspoint	4: sehr hoch	2: normal	2: normal
Entertainment-Geräte: Smart-TV, Konsolen	2: normal	2: normal	2: normal
Speichermedien: USB-Sticks, Festplatten	3: hoch	1: unkritisch	3: hoch
Entertainment-Dienste: Streaming (Musik, Video/Filme)	4: sehr hoch	2: normal	1: unkritisch
Recherche	2: normal	2: normal	1: unkritisch
Online-Shopping	4: sehr hoch	2: normal	2: normal
Fitness / e-Health	4: sehr hoch	4: sehr hoch	4: sehr hoch
digitales Banking	4: sehr hoch	2: normal	2: normal
digitale Behördenwege	4: sehr hoch	3: hoch	2: normal
Soziale Medien: Facebook, Instagram, TikTok	4: sehr hoch	2: normal	2: normal
E-Mail-Dienste	4: sehr hoch	2: normal	2: normal
Kommunikations-Dienste / direct Messaging: SMS, Whatsapp, Snapchat	3: hoch	2: normal	2: normal
Spiele / Gaming	4: sehr hoch	2: normal	2: normal
Cloud-Datenspeicherdienste	4: sehr hoch	2: normal	3: hoch
Outdoor-Aktivitäten: Wandern, Reisen	3: hoch	2: normal	2: normal
Smarthome: Sprachassistenten	4: sehr hoch	2: normal	1: unkritisch
Smarthome: zentrale Haussteuerung (lokal & remote)	4: sehr hoch	2: normal	2: normal
Heimnetzwerk (WLAN, LAN)	4: sehr hoch	2: normal	3: hoch

relevante Bedrohungen inkl. betroffener Schutzziele und „*Threat Actor*“:

Tabelle 34 umgesetzte Risikoanalyse: Bedrohungen inklusive gefährdeter Schutzziele

Bedrohung	***Threat Actor***	***Betroffene Schutzziele (C, I, A)***
G 0.8 Ausfall oder Störung der Stromversorgung	Dienstleister / Hersteller	A
G 0.9 Ausfall oder Störung von Kommunikationsnetzen	Dienstleister / Hersteller	A
G 0.11 Ausfall oder Störung von Dienstleistern	Dienstleister / Hersteller	C, I, A
G 0.14 Ausspähen von Informationen (Spionage)	nicht eindeutig eingrenzbar	C
G 0.15 Abhören	Cyberkriminelle	C
G 0.16 Diebstahl von Geräten, Datenträgern oder Dokumenten	nicht eindeutig eingrenzbar	C, A
G 0.17 Verlust von Geräten, Datenträgern oder Dokumenten	nicht eindeutig eingrenzbar	C, A
G 0.19 Offenlegung schützenswerter Informationen	AnwenderInnen	C
G 0.20 Informationen oder Produkte aus unzuverlässiger Quelle	AnwenderInnen	C, I, A
G 0.21 Manipulation von Hard- oder Software	intern allgemein	C, I, A
G 0.22 Manipulation von Informationen	intern allgemein	I
G 0.23 Unbefugtes Eindringen in IT-Systeme	nicht eindeutig eingrenzbar	C, I
G 0.24 Zerstörung von Geräten oder Datenträgern	intern allgemein	A
G 0.25 Ausfall von Geräten oder Systemen	nicht eindeutig eingrenzbar	A
G 0.28 Software-Schwachstellen oder -Fehler	Dienstleister / Hersteller	C, I, A
G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen	intern allgemein	C, I, A
G 0.31 Fehlerhafte Nutzung oder Administration von Geräten und Systemen	AnwenderInnen	C, I, A
G 0.36 Identitätsdiebstahl	Cyberkriminelle	C, I, A
G 0.39 Schadprogramme	extern allgemein	C, I, A
G 0.42 Social Engineering	nicht eindeutig eingrenzbar	C, I
G 0.45 Datenverlust	nicht eindeutig eingrenzbar	A
G 0.47 Schädliche Seiteneffekte IT-gestützter Angriffe	Script-Kiddies	C, I, A
Online-Betrug / Cyberkriminalität	Cyberkriminelle	C, I
Datenspeicherung & Algorithmus gesteuerte Anzeige von Inhalten (Werbung)	Dienstleister / Hersteller	C
sexuelle Belästigung, Cyber-Stalking & Erpressung	Cyberkriminelle	C
problematische Inhalte für Jugendliche und Kinder	nicht eindeutig eingrenzbar	C
Machtmissbrauch (Missbrauch von Berechtigungen)	AdministratorInnen	C, I, A
Ausfall des technischen Verantwortlichen	AdministratorInnen	A
Umgehung von Jugendschutzmaßnahmen und Einschränkungen für Unmündige	Script-Kiddies	C