Sicherheit in der Digitalisierung des Alltags

Definition eines ethnografisch-informatischen Forschungsfeldes für die Lösung alltäglicher Sicherheitsprobleme

Dennis Eckhardt
dennis.eckhardt@fau.de
Friedrich-Alexander-Universität Erlangen-Nürnberg (FAU), Institut für Soziologie

Felix Freiling
felix.freiling@fau.de
Friedrich-Alexander-Universität Erlangen-Nürnberg (FAU), Department Informatik

Dominik Herrmann
dominik.herrmann@uni-bamberg.de
Otto-Friedrich-Universität Bamberg, Fakultät für Wirtschaftsinformatik und angewandte Informatik

Stefan Katzenbeisser
stefan.katzenbeisser@uni-passau.de
Universität Passau, Fakultät für Informatik und Mathematik

Henrich C. Pöhls
hp@sec.uni-passau.de
Universität Passau, Fakultät für Informatik und Mathematik

Abstract: In den vergangenen Jahrzehnten hat es unübersehbar zahlreiche Fortschritte im Bereich der IT-Sicherheitsforschung gegeben, etwa in den Bereichen Systemsicherheit und Kryptographie. Es ist jedoch genauso unübersehbar, dass IT-Sicherheitsprobleme im Alltag der Menschen fortbestehen. Mutmaßlich liegt dies an der Komplexität von Alltagssituationen, in denen Sicherheitsmechanismen und Gerätefunktionalität sowie deren Heterogenität in schwer antizipierbarer Weise mit menschlichem Verständnis und Alltagsgebrauch interagieren. Um die wissenschaftliche Forschung besser auf Menschen und deren IT-Sicherheitsbedürfnisse auszurichten, müssen wir daher den Alltag der Menschen besser verstehen. Das Verständnis von Alltag ist in der Informatik jedoch noch unterentwickelt. Dieser Beitrag möchte das Forschungsfeld "Sicherheit in der Digitalisierung des Alltags" definieren, um Forschenden die Gelegenheit zu geben, ihre Anstrengungen in diesem Bereich zu bündeln. Wir machen dabei Vorschläge einerseits zur inhaltlichen Eingrenzung der informatischen Forschung. Andererseits möchten wir durch die Einbeziehung von Forschungsmethoden aus der Ethnografie, die Erkenntnisse aus der durchaus subjektiven Beobachtung des "Alltags" vieler einzelner Individuen zieht, zur methodischen Weiterentwicklung interdisziplinärer Forschung in diesem Feld beitragen. Die IT-Sicherheitsforschung kann dann Bestehendes gezielt für eine richtige Alltagstauglichkeit optimieren und neue grundlegende Sicherheitsfunktionalitäten für die konkreten Herausforderungen im Alltag entwickeln.

Keywords: Alltagsdigitalisierung, Ethnografie, IT-Sicherheit, Interdisziplinarität

Gefördert durch das Bayerische Staatsministerium für Wissenschaft und Kunst (StMWK) im Bayerischen Forschungsverbund "**ForDaySec — Sicherheit in der Alltagsdigitalisierung**" (https://fordaysec.de).

1 Einleitung

Viele IT-Sicherheitsprobleme haben bisher keine überzeugenden Lösungen, die sich nahtlos in den Alltag der Nutzerinnen und Nutzer integrieren lassen. Ein Beispiel hierfür ist das Management moderner Heim-Netzwerke, in denen oft eine Vielzahl unterschiedlicher Geräte miteinander verbunden ist. Viele Menschen überfordern sichere Einrichtung und Administration ihrer Technik, was zu Fatalismus, Lähmung und Kontrollverlust führen kann. Andererseits entwickeln Menschen heterogene und komplexe Bestandssysteme, die über Jahre wachsen, mit eigensinnigen Bedien-, Update- und Installations-Praktiken, die oft nur dann verständlich sind, wenn man sie von Innen betrachtet.

Dieser Nexus von Problemen wird von der IT-Sicherheitsforschung bislang nicht ausreichend adressiert. Fragen der Benutzbarkeit sicherer Systeme spielen hier zwar immer öfter eine Rolle – Lösungen für die Probleme des Alltags, wie das eingangs skizzierte, gibt es jedoch kaum. Offenbar tut sich die Forschung schwer, die richtigen Fragen zu stellen, die tatsächlichen Herausforderungen der Menschen in ihrem alltäglichen Umfeld ausreichend zu erfassen und Lösungen zu entwickeln, die auf die alltäglichen Bedürfnisse, Praktiken und Erfahrungswerte von Nutzerinnen und Nutzern abgestimmt sind.

Vorhandene Methoden geraten dabei an ihre Grenzen. Methoden, die z.B. das Nutzungsverhalten beobachten oder Menschen befragen, leiden aufgrund von sogenannten Beobachtungseffekten häufig unter eingeschränkter Aussagekraft. Wenn es darauf ankommt, verhalten sich Menschen eben anders als im Experiment.

In diesem Beitrag wird daher angeregt, dass die IT-Sicherheitsforschung ihre methodischen Ansätze um Methoden der Ethnografie erweitern sollte. Durch die Einbettung der Forschenden in den Alltag der Nutzerinnen und Nutzer ermöglicht die Ethnografie wertvolle Einblicke, die zur Entwicklung praxisrelevanter Lösungen beitragen können, die die Bedürfnisse der Menschen in den Vordergrund stellen.

Um den Nutzen einer solchen ko-laborativen Zusammenarbeit zu demonstrieren, stellen wir in diesem Beitrag zunächst ethnografische Vignetten vor, aus denen wir zentrale Aspekte der IT-Sicherheit in der Digitalisierung des Alltags ableiten. Wir zeigen weiterhin, wie diese Aspekte in der bisherigen Forschung adressiert wurden. Auf Basis dieser Problemanalyse stellen wir dann ein ethnografisch-informatisches Forschungsfeld zur Untersuchung von IT-Sicherheit in der Digitalisierung des Alltags vor, das einerseits neue Forschungsfragen aufwirft und andererseits den Kanon der für die IT-Sicherheitsforschung nützlichen Methoden erweitern kann.

2 IT-Sicherheit im Alltag

In vier ethnografischen Vignetten – also selektiv gewählten Ausschnitten aus einer Feldforschung – zeigen wir empirische Beispiele, die nach den folgenden Aspekten gruppiert sind: “Alltag selbst digitalisieren und absichern” (Abschnitt 2.1), “Alltag von anderen digitalisieren und absichern” (Abschnitt 2.2.) und “Im Alltag Digitalisierung und Sicherheit aushandeln” (Abschnitt 2.3). Diese Aspekte werden in der Problemanalyse in Abschnitt 3 auf fünf Charakteristika erweitert, auf deren Grundlage wir das neue Forschungsfeld entwickeln. Die Vignetten entstammen der ethnografischen Feldforschung von Dennis Eckhardt zu Smart Homes, die zum Zeitpunkt des Verfassens des Artikels zehn Haushalte umfasste. Die Haushalte wurden im Schneeballsystem für die Forschung gewonnen: Im privaten und beruflichen Umfeld wurden Anfragen zu Smart-Home-Haushalten gestellt. Dadurch ließen sich Haushalte außerhalb des eigenen Kontaktkreises ermitteln, und es konnten weitere Freunde, Nachbarn oder Arbeitskollegen sowie deren Haushalte für die Forschung gewonnen werden. Die Haushalte wurden mit ethnografischen Methoden untersucht: die forschende Person ging in die Haushalte und sprach dort vor Ort mit den Menschen, ließ sich durch die Wohnung führen und reflektierte gemeinsam über ihren Umgang mit Technik. Die Gespräche wurden teilweise mit Rekorder aufgezeichnet, transkribiert und hier zitiert, oder durch feldnotierende Methoden (siehe 4.1) in indirekter Rede aufgezeichnet. Wenn hier von der Ich-Person die Rede ist, so meint dies Dennis Eckhardt als Ethnografen.

2.1 Alltag selbst digitalisieren und absichern

„*Das war, ja, ich glaube, das war so ein bisschen die klassische Corona Langeweile. Genau, irgendwann in den letzten zwei Jahren ging das dann los, da bin ich dann, ja, wahrscheinlich über YouTube, auf dieses System oder auf Home Assistant gekommen. Und da gibt es ein paar YouTuber, die halt alles abdecken, die Tutorials vom Zusammenbau des Raspberry Pis bis eben zum Einrichten von der Software haben, und da habe ich mich dann halt mal ein, zwei Wochen ein bisschen reingesteigert, habe mir alles durchgeschaut und parallel dazu irgendwie mein System da aufgebaut.*“ [Interview mit Haushalt 3 vom 26.04.2023]

Das Interview, aus dem das angeführte Zitat stammt, wurde im Wohnzimmer des Feldforschungspartners durchgeführt. Im Interview, das nicht standardisierten Fragen folgte, befragte ich ihn danach, welches System von IoT-Geräten er sich zuhause selbst aufgebaut hatte. Wie das Zitat nahelegt, brachte er sich den Großteil selbst bei, indem er YouTube-Videos anschaute, einen Raspberry Pi bestellte und selbst programmierte, Geräte miteinander verband und letztlich mit dem Home Assistant zu einem System integrierte. Alles fing mit der Kaffeemaschine an, die er mittels smarter Steckdose automatisierte. Mittlerweile ist daraus ein selbst zusammengebautes System erwachsen, mit dem sich auch smarte Glühbirnen und andere Haushaltsgeräte ansteuern lassen. Dies legt nahe, wie viel sich Akteure im Feld selbst an Wissen über Installation und Wartung beibringen, und damit selbst Systeme aufbauen. In Bezug auf Sicherheit wird dies besonders relevant, da der Feldforschungspartner sich einen VPN-Zugang auf dem Smartphone einrichtete, aber sich nicht mehr sicher war, was er dort genau getan hat:

„*Ich glaube nämlich, von außerhalb [, wenn ich unterwegs bin,] greife ich auch eh über eine VPN darauf zu. Ja, ich habe da mal irgendwas eingerichtet, aber ich weiß nicht mehr was. (beide lachen) Das war eben auch so ein YouTube-Video, wie man auf das System von außerhalb*

zugreift, dass das trotzdem sicher ist, und da habe ich einfach diesem Tutorial gefolgt. Und ich glaube, ich habe da so eine VPN eingerichtet, dass es eben sicher ist und auch von außen nicht angreifbar ist. Also genau, ich mache das immer strikt nach Anleitung, ohne genau zu wissen, was man macht, und hoffe einfach, dass es funktioniert. Ja, da habe ich jetzt auch nicht so die große Angst, dass jetzt gerade der Raspberry Pi hackbar ist.“ [Interview mit Haushalt 3 vom 26.04.2023]

Auch wenn er sich nicht mehr genau daran erinnern kann, was er eingerichtet hat, weil er es auch nicht verstehend nachvollzog, sondern nur nachahmte, richtete er Sicherheitsmechanismen in seinen Alltag ein. Da er als selbstständiger Künstler auf digitale Daten angewiesen ist, die seine Werke sind, hat er zuhause diese Daten auf einem Synology-Server gespeichert, der mit Zwei-Faktor-Authentifizierung abgesichert ist. Hier zeigt sich, welche Unterschiede in der Installation im eigenen Alltag gemacht werden: Der Server wird mit hohen Sicherheitsmechanismen versehen, während andere Geräte in der Smarthome-Umgebung mit einem VPN zum Smartphone verbunden sind, woran er sich aber nicht genau erinnern kann.

In einem anderen Haushalt, wurde ich stattdessen mit einem sehr komplexen Arrangement von mehreren Rechnern konfrontiert, die alle monofunktional eingesetzt wurden. Im Haushalt 7 von einem Rentnerpaar gab es im Heizkeller einen alten PC, der früher der Tochter gehörte und – wie es der Ehemann bei der Führung für mich ausdrückte – ‘doch noch gut sei’: “*Damals teuer, er schmeiße nichts weg, auf keinen Fall, dafür sei das doch noch gut!*“ [Feldnotiz vom 14.07.2023, Haushalt 7] Im gesamten Haus hatten sich dadurch mehrere Rechner angesammelt, die alle unterschiedlich genutzt wurden: Der alte Rechner der Tochter im Heizkeller, auf dem allerdings keine sensiblen Daten gespeichert wurden, und der nur für das Abspielen von YouTube genutzt wurde; einen Rechner im alten Kinderzimmer, auf dem Kinderfotos und -videos lagerten, der auch noch Updates erhielt; zwei Laptops im Dachgeschoss, wobei einer genutzt wurde, um Fotos von einer Speicherkarte zu transferieren (allerdings nur, weil dieser Laptop der einzige war, der eine vom Hersteller eingebaute Schnittstelle hatte) und der andere Laptop, um über Ebay und mit PayPal Dinge einzukaufen (meist Rasierer oder Bohrmaschinen als Geschenke). Die Ehefrau nutzte stattdessen ein Tablet (System und Marke wurden leider nicht erhoben), um damit zu surfen, aber auch auf die Webcam zuzugreifen, die der im Ausland lebende Sohn bei sich im Garten installierte. Außerdem waren im Haus zwei Saugroboter, die allerdings selten genutzt wurden.

2.2 Alltag von anderen digitalisieren und absichern lassen

Im nächsten Haushalt traf ich auf einen Bastler, der als studierter Wirtschaftsinformatiker selbst viel mit Geräten hantiert: Saugroboter werden hier auch aufgeschraubt, und wenn sie als nicht sicher eingestuft werden, erhalten sie ein eigenes segmentiertes Netzwerk, in dem sie dann angemeldet sind. Hier war es allerdings so, dass die Schwiegereltern ihren Mähroboter für den Rasen im Garten über den Schwiegersohn steuern ließen. Bei jenem Schwiegersohn war ich zugegen und erstellte nachfolgende Feldnotiz:

„*Er klickte [auf seinem Rechner] auf eine Karte und man sah die Stadt, in der wir gerade waren, und zwei große gelbe Kreise. Das eine sei das Zuhause, dann die Schule, ein dritter kleiner Kreis weiter oben, das seien die Schwiegereltern, da sei seine Partnerin neulich gewesen, das könne er hier sehen. Ich erinnere mich noch an den Rasenmähroboter, den hätte er ihnen gekauft und eingerichtet. Er hätte sich das schon gedacht, dass das ihnen gefallen müsste, was es auch tat. Normalerweise sei das Ding so programmiert, dass es eben an bestimmten Tagen einfach losfahre und den Rasen mähe. Aber es komme auch mal vor, dass die Schwiegermama dann anrufe und sage, dass er bitte den Roboter mal losschicken solle, es sei gerade trocken, und es solle nachher regnen, das würde jetzt noch passen, was er dann auch mache. Achso?, fragte ich nach. Jaja, die könnten den auch selbst anmachen, aber das laufe dann meist so ab.*“ [Feldnotiz vom 22.08.2023 mit Haushalt 8]

Der Feldforschungspartner hat hier selbst ein hohes Bewusstsein für Sicherheitsprobleme, dass er mit dem Slogan „If you can‘t patch it, you don‘t own it!“ zum Ausdruck brachte. Er zählt sich selbst zur Makers-Community, die selbst baut, lötet und schraubt und sich daher von Hause aus mit Sicherheit auseinandersetzt. Mit dem Mähroboter der Schwiegereltern ist er aber quasi zum delegierten Systems-Admin geworden, und die Software des Roboters ist in zwei Haushalten installiert, sodass er auch von beiden Standorten bedient werden kann. IoT-Geräte können also konträr der möglicherweise eigentlichen Nutzung auch in mehreren Haushalten installiert werden, womit Akteure ein eigenes Netz von Geräten und Verantwortlichkeiten erstellen.

2.3 Im Alltag Digitalisierung und Sicherheit aushandeln

In zwei sehr kurzen weiteren Vignetten wird deutlich, wie im Alltag selbst Digitalisierung, Funktionalität und auch Sicherheit ausgehandelt werden. Daher werden in den folgenden Interviewausschnitten auch mehrere Gesprächspersonen zitiert. In der Interviewsituation selbst kam es zu Momenten der Aushandlung, die hier gezeigt werden.

Im ersten Haushalt wurde ein Saugroboter von einem chinesischen Hersteller bedient. Auf Nachfrage, wie dieser Saugroboter seinen Weg in den Haushalt gefunden hatte, zeigte sich allerdings, dass er kein aktiver Kaufprozess des primären Bedieners war. Im folgenden Interviewausschnitt, in dem sowohl ich als Interviewer als auch das befragte Paar zur Sprache kommen, wird deutlich, dass der Partner seinen Eltern gegenüber lediglich das Interesse für einen solchen Roboter geäußert hatte. Die Eltern verstanden dies allerdings als einen versteckten Hinweis und kauften ihm gemeinsam mit der Partnerin dasselbe Modell, das auch sie selbst benutzten:

„*Partnerin: Du hast ihn ja bei deinen Eltern gesehen.*
Partner: Ich habe ja noch gar nicht gesagt, ich möchte jetzt den [Saugroboter]. Habe ich ja nicht gesagt. Ich habe ja nicht das als spezifischen Weihnachtswunsch ausgegeben oder so, sondern ich habe nur gesagt, dass wäre cool, so einen Roboter zu haben.
Interviewer: Er hat nicht drauf bestanden, aber es war dennoch unvermeidlich. (alle lachen) […]
Partner: Ja. Na ja, sonst hätte ich ...
Partnerin: Das wusste ich gar nicht.
Partner: Sonst hätte ich wahrscheinlich schon recherchiert. Ich mag das schon auch."
[Interview mit Haushalt 4 vom 13.06.2023]

Erst in der Interview-Situation selbst wird auch für die Partnerin deutlich, dass er nicht explizit um den Saugroboter gebeten hat. Nicht jede Technik findet ihren Weg durch klassische Kaufentscheidungsmodelle in die Haushalte, sondern wird verschenkt. Im Alltag muss nun mit der Existenz des Gerätes umgegangen werden. In diesem Fall führt erst die ethnografische Feldforschung zu dieser Reflexion: Die Partnerin gibt an, dass sie – obwohl sie beim Kauf involviert war – dies nicht wusste.

In der zweiten kurzen Vignette wird dagegen deutlich, wie mit Technik umgegangen wird, die nicht alle im Haushalt wirklich wollen. In diesem Haushalt ist der Partner der Technikbegeisterte, der mir als Interviewer voller Freude die Funktionen des Saugroboters zeigte. Währenddessen schaltete sich allerdings mehrfach die Partnerin ein, die wiederholt darum bat, die Kamerafunktion des Roboters auszuschalten. In diesem Interviewausschnitt, in dem wieder mehrere Personen zur Sprache kommen, wird deutlich, dass Funktionalität von Geräten im familiären Alltag ausgehandelt wird: Nicht alles, was ein Gerät kann, oder wozu Nutzende auch in der Lage wären es zu nutzen, wird dann auch tatsächlich genutzt.

„*Partner: (Roboter stoppt) Ich lasse mal weiterfahren und dann –*
Partnerin: Aber es hat gerade gesagt, die Kamera ist an.
Partner: Genau. Und man muss ja noch mal zusätzlich so einen Code aktivieren […]
Partnerin: Können wir die Kamera jetzt wieder ausmachen?
Partner: Es gibt auch den Surveillance-Modus. Also die verkaufen das auch als Surveillance-Modus, […].
Partnerin: So, aber kannst du die Kamera ausmachen, bitte?
Partner: Ja, ich mache sie aus.
Interviewer: Stört dich das?
Partnerin: Ja.
Partner: Der fährt dann wieder […]. Und das ist natürlich, ja, also diese Kamerafunktion –
Partnerin: Sollst du ausmachen, die Kamera.
Partner: Ist aus. Sobald du rausgehst, und wenn ich wieder auf 'Kamera' drücken würde, würde er wieder die Pin abfragen.
Partnerin: Na gut." [Interview mit Haushalt 1 vom 11.04.2023]

3 Problemfelder

Die ethnografischen Vignetten deuten auf eine Vielzahl von Problemfeldern hin. Dazu ziehen wir ein kurzes Fazit, dem eine technische Betrachtung der Problemfelder folgt (Abschnitt 3.1). Wie diese Problemfelder bisher in der Informatik bearbeitet werden und warum daraus ein neues Forschungsfeld erwächst, zeigen wir in Abschnitt 3.2. Zunächst ein Fazit:

In Abschnitt 2.1 zeigte sich, dass Menschen ihre Rechner- oder IoT-Systeme selbst administrieren. Sie eignen sich dafür auch zeitlich begrenzt Fähigkeiten und Wissen – bspw. über YouTube – an, und können Teile davon aber auch wieder vergessen. Obwohl selbst programmiert wurde, erscheinen dann Systeme erneut als eine Black Box. Auch veraltete Rechnersysteme verlassen nach dem Ende ihres Lebenszyklus nicht automatisch einen Haushalt – obwohl dies technisch ratsam wäre. Bewohnende entwickeln eigensinnige Praktiken, wie sie mit obsoleter Technik umgehen (siehe das Beispiel im Heizkeller). Menschen integrieren in ihrem Alltag Technik zu heterogenen und komplexen Bestandssystemen, die selbstgebastelt und mit “Ein-Tool-Lösungen” nicht bearbeitbar sind. In Abschnitt 2.2 zeigt sich wiederum, dass die Ansprechpartner von Technikadministration nicht immer leicht zu identifizieren sind, und dass Menschen Technik auch in verschiedenen Alltagen von anderen einbauen oder warten. Sie delegieren Administration und Wartung an Familienmitglieder – aber auch an andere Menschen und Organisationen. Der letzte Abschnitt 2.3 zeigte ergänzend, dass nicht alles, was technisch möglich ist, auch von Menschen genutzt wird, bzw. Funktionen von Geräten ausgehandelt werden. Mentale Modelle sind – so ist festzuhalten – dynamisch, und werden von Menschen auch untereinander selbst justiert, angepasst, verändert oder sanktioniert (siehe Beispiel des Saugroboters mit Kamerafunktion). Außerdem werden Geräte verschenkt, wodurch Technik Einzug im Alltag hält, die nur partiell erwünscht war. Im Alltag muss dann gelernt werden, mit diesen teils gewünschten, teils unerwünschten Geräten umzugehen.

3.1 Problemfelder und ihre technischen Ursachen

Aus dem vorgeschalteten Fazit kristallisieren sich (sozio-)technische Problemfelder heraus, die für die Informatik relevant sind. Wir haben für dieses Paper die folgenden fünf ausgewählt: (A) Bestandsystem, (B) Heterogenität, (C) Versionierung, (D) Wahrnehmung und (E) Alltagskontext. Die Problemfelder sind weder überlappungsfrei noch decken sie das gesamte Spektrum ab, sie eignen sich aber gut, um grundlegende Ursachen für die in Abschnitt 2 beschriebenen Charakteristika zu benennen. Es folgt unser Verständnis der Problemfelder. Wie diese bereits von der Informatik bearbeitet werden zeigen wir darauffolgend in Abschnitt 3.2.

(A) Als **Bestandssystem** bezeichnen wir ein System von Geräten, bei dem die Geräte bereits gebaut und schon seit einiger Zeit in Betrieb sind, im Gegensatz zu neu entwickelten Geräten, die neu eingerichtet und eingesetzt werden – vergleichbar der Abgrenzung zwischen "Brownfield" und “Greenfield” [So12].

(B) Mit **Heterogenität** bezeichnen wir im Folgenden den Umstand, dass ein System hinsichtlich einzelner technischer System-Parameter (Hardware, Betriebssystem, Software, Protokoll, Netzwerkanbindung) unterschiedliche Ausgestaltung annimmt - bspw. Android und iOS Geräte, Geräte mit WLAN und Geräte mit Bluetooth.

(C) **Versionierung** bezeichnet im Folgenden den Umstand, dass es mehrere Versionen eines Gerätes geben kann, wobei dabei sowohl der Stand der Hardware (andere Komponenten, anderer Hersteller), als auch der Stand der Software eine Rolle spielen.

(D) Als **Wahrnehmung** bezeichnen wir im Folgenden die Art und Weise, wie ein Nutzer oder Teilnehmer ein Gerät, System oder auch die technische Umsetzung beobachtbarer Funktionalität auf der Grundlage seines Wissens betrachtet.

(E) Simplifiziert nehmen wir im Folgenden an, dass der **Alltagskontext** jene Umgebung beschreibt, in der sich menschliches Handeln primär vollzieht.

Diese Problemfelder treten in den vorgestellten ethnografischen Vignetten wie folgt auf:

(1) Die meisten Rechnersysteme werden durch den Besitzer selbst administriert, der oftmals über kein großes Fachwissen verfügt oder dieses sich nur punktuell aneignet, aber auch wieder vergessen kann. (siehe 2.1)

	Bestandsystem	Heterogenität	Versionierung	Wahrnehmung	Alltagskontext

(2) Die eingesetzten Systeme sind über die Jahre ‘gewachsen’ (nichts entsorgen oder auch geschenkt bekommen) und stellen heterogene Bestandssysteme dar. (siehe 2.1, 2.2 und 2.3)

	Bestandsystem	Heterogenität	Versionierung	Wahrnehmung	Alltagskontext

(3) Komponenten werden selten bis gar nicht gewartet – oftmals findet man “liebevoll vernachlässigte Infrastrukturen” vor oder Nutzende sind sich über die Wartung im Unklaren. (siehe 2.1 und 2.3)

	Bestandsystem	Heterogenität	Versionierung	Wahrnehmung	Alltagskontext

(4) Selbst-entwickelte mentale Modelle, was Technik beispielsweise tut, wie man versucht sich selbst Sicherheit zu verschaffen, wozu man Geräte wie benutzt (siehe 2.1 und 2.3)

	Bestandsystem	Heterogenität	Versionierung	Wahrnehmung	Alltagskontext

(5) Einbettung in soziale Gefüge; Situierung von Technik im Alltag: Nutzung wird ausgehandelt, was technisch möglich ist, wird nicht automatisch genutzt. (siehe 2.3)

	Bestandsystem	Heterogenität	Versionierung	Wahrnehmung	Alltagskontext

Die Unterschiedlichkeit der genannten Problemfelder und deren Kombination im Alltag sind ein Indiz für die Komplexität von Sicherheit in der Digitalisierung des Alltags. Im nächsten Abschnitt legen wir dar, wie diese Problemfelder bisher in der Informatik bearbeitet werden.

3.2 Bisheriges Vorgehen der Informatik

Problemfeld (A) Bestandssystem
Bestandssysteme bedeuten zunächst einmal, dass neue und sicherere Technologien nicht oder nur mit Hilfe von Sicherheitsupdates auf dem Gerät/System zur Verfügung stehen. In der Forschung ist es zum einen einfacher ein System mit einer Sicherheitseigenschaft von Grund auf neu zu konzipieren und einzusetzen, es ist sogar ein gutes Beispiel im Sinne des “Security by design” Paradigmas. Die Aufwände ein bestehendes System, gleich welcher Art, umzubauen oder zu erweitern, sind anderer Art [Ax19] und der Aufwand wird meist als ein höherer wahrgenommen. So beschreiben technische Richtlinien, dass die Integration von Altsystemen, zu einer großen Herausforderung wird, wenn die vorhandenen Geräte bereits vor mehreren Jahrzehnten eingesetzt wurden und keine moderne Technologie, insbesondere Software, integrieren können [Etsi19]. Manchmal finden sich auch unvorhergesehen Erweiterungsmöglichkeiten innerhalb bestehender Systeme [Wa23].

Problemfeld (B) Heterogenität
Die technisch orientierte Forschung optimiert Geräte-Merkmale (wie eingesetzte Protokolle, Software, Hardware) für die Einsatzzwecke und entlang des wirtschaftlichen Druckes. Während ein Preisdruck zu einer gewissen Standardisierung und der daraus resultierenden Harmonisierung bestimmter Komponenten (bspw. ESP32 als Hardwarebasis vieler preiswerter, oft leistungsarmer IoT Geräte). Allerdings wirkt die schiere Breite der Produkte (vom Türsensor bis zum Kühlschrank, oder SmartTV) dieser Standardisierung wieder entgegen. Des Weiteren wirken Taktiken zur Nutzerbindung wie Anbieter-Lock-in einer Standardisierung entgegen. Vorstöße wie jüngst “matter” [Cs23] sind die Antwort auf eine Heterogenität, und harmonisiert für eine gesteigerte Interoperabilität das Kommunikationsprotokoll, aber nur solange die Geräte das Protokoll als Update erhalten und über Internet Protokoll (IP) erreichbar sind. Die unter Bestandssytemen diskutierte Problematik, dass man neue Verfahren nur durch neue Geräte einführen kann bedeutet, dass man sich von den alten Geräten trennen müsste, und wenn dies nicht geschieht automatisch zu einer Heterogenität des Gesamtsystemes. Die Forschung bezieht entsprechende Heterogenität mit ein [Bl88] und adressiert dies durch Normung von Protokollen oder Schnittstellen auf höheren Ebenen, so wie dies nun von verschiedenen Herstellern mit großer Anzahl von eigenen Geräten mit dem Protokoll matter passieren soll. Dies führt auf der Ebenen der Benutzerwahrnehmung zu geringerer Heterogenität, da Funktionen einheitlich angesteuert werden können und kann durch entsprechende Software-Updates auch die Integration von Bestandsystemen lösen. Allerdings bleiben unterhalb der Protokolle die Geräte immer noch heterogen, also mit unterschiedlicher Hardware- und Software-Stack und damit weiterhin mit unterschiedlichen IT-Sicherheitsproblemen. Aber auch die Kombination verschiedener Geräte im Alltag ohne das Nutzer im Vorfeld die Auswahlmöglichkeit (z.B. aufgrund fehlender Angebote am Markt oder fehlender technische Expertise) zur Vermeidung von Heterogenität haben, führt zu ebendieser.

Problemfeld (C) Versionierung
Versionierung umfasst hier sowohl sicheres Software Development als auch die sichere Verteilung von Updates. Während letzteres Feld ein weiteres Beispiel für eine große Menge an speziellen Lösungen in speziellen Kontexten darstellt, was gerechtfertigterweise auch den sehr unterschiedlichen technischen Gegebenheiten im jeweiligen technischen Kontext geschuldet ist,

bspw. IoT [Ca23, Mo18]. Hier wurden auch Lösungen speziell für das Update persönlicher Geräte im Alltagsumfeld erforscht [Ch16]. Ersteres Forschungsfeld der sicheren Software Entwicklung ist breiter und es gibt viele Forschungsergebnisse [Kh21] wie den Secure Software Development Life Cycle (SSDLC) process [Gr04] oder Microsoft Software Development Life Cycle (SDL) [Li05]. Diese Prozesse sind aus der Forschung herausgetreten und in Normen wie ISO 27034 [ISO 27034] kodifiziert. Dies scheint gut verstanden zu sein, erfordert aber zusätzlichen Aufwand für die Produktentwicklung. Erst seit kurzem greift die Forschung Fragen der Nutzerwahrnehmung für das Einspielen von Sicherheitsupdates auf [Mo20, Ha23].

Problemfeld (D) Wahrnehmung
Die Untersuchung mentaler Modelle ist seit vielen Jahren Gegenstand der Forschung im Bereich Human-Centered bzw. Usable Security, wo an der Grenze zur und mit Methoden der Kognitions- und Sozialwissenschaft operiert wird, also mit qualitativen und quantitativen Studien. Dabei geht es um die Untersuchung der gedanklichen Mechanismen, mit denen sich Benutzer den Sinn, Zweck und die Funktionsweise eines Systems erklären, um daraus auch Vorhersagen über zukünftiges Systemverhalten abzuleiten [Wa10, Vo13]. Die dort erarbeitete umfangreiche Wissensbasis wurde sehr lange in der Mainstream-Informatik ignoriert und ist auch heute noch vielfach wenig anerkannt. Das Versagen von Sicherheitssystemen wurde ursprünglich “stupid users” (und später “stupid developers”) zugewiesen. Heute gilt diese Ansicht jedoch als widerlegt [Ad99, Gr14, Re19]. Auch wenn sich die hier verwendeten Forschungsmethoden von denen vieler anderer Bereiche der Informatik unterscheiden, liegt auch hier der Fokus stets auf einer bestimmten Sicherheitsaufgabe (wie Passwortmanagement oder verschlüsselte E-Mail), deren Kontext möglichst genau kontrolliert wird, damit beobachtete Effekte dem untersuchten Phänomen zugeschrieben werden können.

Problemfeld (E) Alltagskontext
Die Alltagsprobleme der IT-Sicherheit treten in der etablierten IT-Sicherheitsforschung allenfalls in isolierten Anwendungsdomänen zu Tage. Die öffentliche Wahrnehmung basiert eher auf Ergebnissen von populärwissenschaftlichen Umfragen von Illustrierten und Think Tanks. Im Bereich der Mensch-Maschine-Interaktion gab es jedoch vereinzelt Arbeiten wie Dourish et al. [Do04] und zuletzt auch Fassl und Krombholz [Fa23], die Alltagssitutationen in den Mittelpunkt des Interesses stellen und sich dabei gegenüber ethnografischen Forschungsmethoden geöffnet haben. Trotzdem ist die Betrachtung des menschlichen Alltags im Mainstream der IT-Sicherheitsforschung noch unterbelichtet.

Den Einzug von Computern in den Alltag prognostizierte das 'ubiquitous computing’ [We91] schon 1991 und früher; die Forschung setzte aber zunehmend auf Spezialisierung; hinsichtlich IT-Sicherheit gab [Ku16] und gibt [Ma19] es viele Überlegungen und grundlegende Ansätze zur Lösung dedizierter Probleme, wie den klassischen Ansatz von Stajano und Anderson zur Authentikation von neuen Geräten [St00]. Eine Spezialisierung erfolgte auch in den Anwendungsgebieten, welche sich eben nicht an die Komplexität sicherer alltäglicher Interaktionen heran wagte, sondern eine Fokussierung auf bestimmte der Anwendungs- oder Systemkontexte ergab, etwa für SmartCity [Tr17], smarte Sensorik [Mo17a], smarte Glühbirnen [Mo17b] oder für ganz spezielle Geräte- und Anwendungstypen, beispielsweise implantierbare medizinische Geräte [Ru14], Browser-Nutzung [Pu20] oder Videokonferenzsysteme [We23].

Diese Spezialisierung gilt es zu durchbrechen und den Kontext des Alltages zu erschließen: Auf der Suche nach einer expliziten und harmonisierten Beschreibung des Einsatzes von Geräten des sogenannten Internet der Dinge (Internet of Things, IoT) im Alltag für eine harmonisierte Erforschung sind derzeit auch zwei sich in der Entwicklung befindliche internationale Standards: Der ISO/IEC 27404 [ISO27404] beschreibt die Zertifizierung von sogenannten 'consumer IoT' Produkten und meint damit sowohl IoT-Geräte, IoT-Systeme, oder IoT-Dienste die von natürlichen Personen zu Zwecken, die nicht ihrer gewerblichen, geschäftlichen, handwerklichen oder beruflichen Tätigkeit zugerechnet werden können, benutzt werden. Der voraussichtlich nächstes Jahr erscheinende internationale Standard ISO/IEC 27403 [ISO27403] beschreibt Leitlinien für einen sicheren und datenschutzkonformen Einsatz von Produkten des Internet-der-Dinge im häuslichen Alltag. Dieser verweist ausdrücklich auf Besonderheiten im Alltag und deren gesteigerte Bedeutung für die IT-Sicherheit hin, wodurch sich Schutzbedarf und Sicherheitsprobleme von anderen IoT-Lösungen unterscheiden, z. B. der Tatsache, dass die Nutzer keine Experten sind. Aber auch die gesteigerte Komplexität durch z.B. dynamische Netzwerke, die Variabilität der Geräte hinsichtlich ihrer Ressourcen, hinsichtlich der Kommunikationsprotokolle, hinsichtlich der Hersteller und letztendlich auch die Variabilität in der Interaktionsmöglichkeiten und den Erbrachten und Erwarteten Diensten werden genannt. Diese Systematik sollte man aus technischer Hinsicht entsprechend auf die existierenden Forschungsergebnisse in den verschiedensten technischen Bereichen anwenden.

Wir gehen davon aus, dass zunehmend das Ineinandergreifen dieser Problemfelder im Alltag von Menschen zu einem Sicherheitsproblem wird, und die Informatik daher auch Methoden benötigt, welche diese *eigensinnige Komplexität von Alltag* verstehen kann.

Die bisher gängigen Methoden für die Erforschung von menschlichen Aspekten in der IT-Sicherheit eignen sich dafür nur begrenzt. Neue und bestehende IT-Sicherheitsmechanismen werden zwar in der Forschung oft mit Benutzerstudien evaluiert, allerdings oft unter Laborbedingungen oder in eigens konstruierten Szenarien, die wenig mit der Nutzung im Alltag zu tun haben. Tiefere Einblicke in die Alltagsnutzung erlauben Beobachtungsstudien und Living Labs. Um Verzerrungen durch Beobachtungseffekte zu vermeiden und den Aufwand der Durchführung zu begrenzen, sind solche Studien, beispielsweise [SGP+23], allerdings häufig in eine Beobachtungsphase und eine vor- oder nachgelagerte Befragungsphase aufgeteilt. Sowohl die zeitliche Entkopplung als auch der Mechanismus der Befragung limitieren den möglichen Erkenntnisgewinn, da sich die geäußerten Ansichten und Intentionen nicht immer mit den Handlungen decken.

Daher schlagen wir im Folgenden den Einbezug ethnografischer Methoden vor (4.1), wie man den Begriff 'Alltag' auch für die Informatik nutzbar machen kann (4.2) und wie wir das neue Forschungsfeld verstehen und darin arbeiten wollen (4.3).

4 Ein neues Forschungsfeld

4.1 Der Beitrag der Ethnografie

Die Ethnografie bezeichnet ein Methodenbündel von verschiedenen gegenstandsbezogenen Methoden, die auf das Verstehen ausgelegt sind. Sie ist mit der Beschreibung, Beobachtung und Verstehen von ‘Alltag’ vertraut und hat dafür Erfahrungen mit Methoden gesammelt. Sowohl für das ethnografische Arbeiten, wie auch die qualitative Sozialforschung im Allgemeinen, ist es wichtig, die empirische Forschung zu betonen: „An die Stelle anekdotischen Wissens über soziale Lebenswelten tritt eine empirisch offensive Forschung, die die vordergründigen Betrachtungen von Randbedingungen sozialer Prozesse durch eine detaillierte empirische Analyse ebendieser sozialen Praktiken und Wirklichkeiten, Dynamiken und Details ersetzt.“ [Ka23] Dabei wird allerdings nicht untersucht, wie ‚der deutsche Haushalt‘ typischerweise oder verallgemeinernd mit Sicherheit im digitalen Alltag umgeht, sondern, wie dies konkrete Haushalte tun, wie dies zu verstehen ist, und was daraus auch für größere Zusammenhänge gelernt werden kann. Die Ethnografie ist dabei nicht holistisch, sondern ausdrücklich partiell angelegt [St04]. Sie gewinnt ihre Relevanz eben nicht in Repräsentation von Kultur – also einer Darstellung davon, wie im Alltag ‘typischerweise’ mit IoT-Geräten umgegangen wird –, sondern aus einer Perspektive *von Innen*: Die Feldforschung taucht immersiv und explizit ausschnitthaft in ihr Feld ein, arbeitet mit Feldforschungspartnerinnen und -partnern gemeinsam zusammen, und versucht Beweggründe, Sinnzusammenhänge und Praktiken nachvollziehbar zu machen. Sie kann so rekonstruieren, wie Technik und Sicherheit im Alltag von Menschen *situiert sind und wirken*.

Die Ethnografie wird klassischerweise als ein *Bündel von Methoden* verstanden, die radikal gegenstandsbezogen sind, und die erst in der Praxis erlernt und angepasst werden [KE23]. Je nach Feld oder Forschungsgegenstand werden andere Methoden gewählt, die der Dynamik der untersuchten Alltage auch Rechnung tragen können. Hierbei sind besonders hervorzuheben: (1) Die *Teilnehmende Beobachtung*, bei der Forschende aktiv im Alltag, so weit dies möglich ist, teilnehmen, und aus der Teilnahme heraus Innenperspektiven entwickeln [Ma17; Dw18]. Dabei können unterschiedliche Grade von Teilnahme bestehen, die alle versuchen die forschende Person auch körperlich an das Geschehen nah heranzuführen. (2) Das *Ethnografische Interview*, das ausdrücklich darauf ausgelegt ist, nicht nur O-Töne aus den Befragten heraus zu filtern, sondern, das sich als eine reflexive Ebene versteht, auf der beide Seiten etwas voneinander lernen [Ma17]: “*[I]t is better understood as a process in which interviewer and interviewee are both involved in developing understanding, that is in constructing their knowledge of the social world*” [Da99]. (3) Das *Feldnotieren* als eine notierende Technik in Situationen, in denen das Aufnahmegerät nicht verwendet wird oder auch nicht verwendet werden kann [Ec23; Sa99; BT20]. Hier werden mit Screenshots, Notizbüchern, Sprachnotizen und deren Transkripte Erlebtes, Beobachtetes und teilweise auch erste analysierende Gedanken in Daten aufbereitet – auch im Nachgang von Situationen in Form von Memos. Diese Methoden betonen die *eigene Situierung* im untersuchten Feld. Gerade dann, wenn in der ‘eigenen’ Gesellschaft geforscht wird, ist der Alltag der Forschenden vom Alltag der Beforschten an vielen Stellen ähnlich, vergleichbar oder miteinander verwoben [Ts06]. Die komplexen Einblicke in die Alltage von Menschen entstehen durch die Immersion in ein Feld, das Beobachten eigener (verändernder) Gewohnheiten, und die *dichte Beschreibung* [Ge73; Ho09] von Alltagen, Praktiken, Wissen, Erfahrungen und Akteuren.

4.2 Alltag ethnografisch denken

Der Begriff Alltag wird seit langer Zeit als Forschungsgegenstand von ethnologischen Fächern bearbeitet [Li93]. Darin existiert ein Fokus “Gesellschaft von ihren Lebenswelten und gesellschaftlichen Mikrobereichen her zu denken – im Horizont der Subjekte, ihrer Erfahrungen, der Praxis sinnhafter Aneignung und Herstellung von Welt.“ [Sc20] Im Fokus der Analysen steht Alltag, der nur auf den ersten Blick unproblematisch und wissenschaftlich belanglos erscheint. Die ethnologischen Fächer analysieren das Gewöhnliche, das Alltägliche und das Routinisierte [Je99], indem sie Subjekte mit ihren Erfahrungen und Praktiken in den Mittelpunkt stellen: “Was Alltag für die Kulturanthropologie interessant macht, ist gerade das, was ihn nicht erwähnenswert erscheinen lässt: immer wieder dieselben Zeiten, Räume, Rhythmen, Rituale, Personen, Aktivitäten […]” [Am14]. Das, was Menschen tun, wie sie mit Dingen, Technik oder auch anderen Menschen *umgehen,* wird hierauf aufbauend als Praxis bezeichnet [Sc13; Be97] und als konstitutiv für den Alltag betrachtet. Es geht darum zu fragen, „wie Menschen auf die Welt zugehen und in dieser Welt handeln, auf soziale [aber auch technische] Setzungen, also Strukturen reagieren und diese wiederum gestalten.“ [Ko15]

Dabei ist es jedoch notwendig, dass der Alltag von Menschen nicht als eine reine Beobachtungskategorie verstanden wird, die sich unmittelbar erheben lässt [Cl90]. Alltag ist die von Menschen aktiv gestaltete Lebenswelt, in der sie selbst Technik ‘veralltäglichen’ [Am14]. Menschen integrieren verschiedene Geräte in ihren eigenen Alltag und in den Alltag von anderen (siehe 2.1 und 2.2). Wie sie dies tun, ist mitunter ein Aushandlungsprozess im Alltag der Akteure selbst, die dies reflektieren oder in der Forschungssituation in Reflexion bringen (siehe 2.3). Das Gewöhnliche des Alltags und seine Sinnzusammenhänge sind also „beredet[]“, da sie „Ergebnis von Befragung und Interaktion“ sind [Ts06]: Sie entstehen zumeist erst im Prozess der Forschung – oder in Momenten der Krise und des Nicht-Funktionierens [Am14] – und sind nicht gegebene Daten, die unmittelbar aufgesammelt werden können. Im Gegenteil, sind Feldforschungspartner und -partnerinnen mit ihren Alltagen aktive Gestalter und Gestalterinnen von dem, was erforscht werden kann: „actors have their own theories about what they do; […] actors also have ‚their own theories of actions‘, they are ‚full-blown reflexive and skilful metaphysicians‘ and they have to be taken seriously as intermediaries.“ [Kr09] Den Alltag zu erforschen setzt also voraus, *mit* Alltagen von Menschen forschen zu wollen und die Praktiken, Erfahrungen und Reflexionen von ihnen ebenso wie die von Akteuren ‘selbstgebastelten’ Systeme ernst zu nehmen.

***Sicherheit in der Alltagsdigitalisierung fragt also nach den Praktiken, Erfahrungen und dem angeeigneten Wissen, mit denen Menschen ihren Alltag digitalisieren und sichern*.**

4.3 Das neue ethnografisch-informatische Forschungsfeld

In der Verbindung der Problemfelder und ihrer Komplexität im Alltag, schlagen wir ein neues Forschungsfeld vor. In diesem Forschungsfeld “IT-Sicherheit in der Digitalisierung des Alltags” werden Alltage von Menschen in verschiedenen Lebenswelten untersucht und ihre Komplexität auch technisch beobachtet. Wir möchten ein Verständnis davon entwickeln, wie Menschen Technik im Alltag situieren und welche technischen Probleme daraus entstehen. Dieses Forschungsfeld setzt mit einer Erkundung sozio-kultureller Welten am Anfang an und lagert dies nicht als Experiment in einem labor-ähnlichen Szenario hinten nach. Die Informatik soll die Welt weiterhin technisch ‘verbessern’ und sie zu einem sicheren Ort machen. Die Ethnografie

problematisiert, welche Welt damit eigentlich konkret gemeint ist und *lokalisiert* Alltage mit ihren Praktiken, Akteuren, selbstgebastelten Bestandssystemen, Erfahrungen und Alltagswissen.

Dieses Forschungsfeld lässt sich *ko-laborativ* bearbeiten: Informatische und ethnografische Methoden und sozialwissenschaftliche Fächer arbeiten zusammen, ohne dabei ihre disziplinären Grenzen aufzugeben, noch in der Absicht, dass Informatikerinnen und Informatiker alle ethnografisch arbeiten müssten (oder vice versa). Stattdessen sprechen wir von projektbezogener, zeitlich begrenzter "joint epistemic work" [Bi21], die versucht in einem Modus von "slow science" zu kommen und mit verschiedenen Methoden, Zugängen, Konzepten, aber auch Denkweisen experimentiert [Ni16].

Im Forschungsfeld "IT-Sicherheit in der Digitalisierung des Alltags" arbeiten Informatik und Ethnologie (aber auch anverwandte Fächer) zusammen und richten ihr Tun auf gemeinsame Lernprozesse. Sie treffen sich konzeptionell im Begriff Alltag, der beide Arbeitsbereiche verbinden kann. Die hier angeführten ethnografischen Vignetten (siehe 2.) sind in privaten Haushalten entstanden. Der Begriff Alltag führt das Forschungsfeld aber an die Schnittstellen von Gesellschaft: Alltage in KMUs sind dabei genauso zu untersuchen, wie Alltage in Behörden, Wasserwerken, Busbetrieben, Krankenhäusern oder alltägliches Home Office. Die Informatik kann dadurch die Vorstellung eines 'Users' mit weiteren sozio-kulturellen Ebenen anreichern. Userinnen und User sind in ihrem Alltag selbst Mitarbeitende, die Awareness-Schulungen erhalten, zuhause Geräte miteinander integrieren, oder sich gegenseitig Technik schenken, die sie nie haben wollten.

Die so fokussierten Alltage und Praktiken bieten konzeptionelle Ebenen, die zwischen dem Einzelfall und der einen Lösung für alle liegen. Begrenzt man den technischen Fokus auf vernetzte Bestandssysteme, die nur sporadisch administriert werden und aus heterogenen Geräten und Komponenten bestehen, dann verspricht die Erweiterung des Forschungsinstrumentariums um ethnografische Methoden – also situierte Beobachtungen im Feld und dichte Beschreibungen, die die Subjektivität des Forschenden explizit einbeziehen – einen substantiellen Mehrwert an Erkenntnis. Ob sich dies in bessere Sicherheitslösungen umsetzen lässt, steht für die Autoren außer Frage. Ob aus der Vereinzelung der Beobachtung wieder sinnvoll verallgemeinert werden kann, und schlussendlich wie die gewonnenen Erkenntnisse in ingenieurmäßig-informatische Konstruktionsprozesse integriert werden können, muss weiter ko-laborativ erforscht werden.

Danksagungen

Die Autoren danken Zinaida Benenson, Gaston Pugliese, Marius Momeu, Thomas Riehm und allen anderen Mitgliedern des ForDaySec-Forschungsverbundes für hilfreiche Anmerkungen bei der Entstehung dieses Textes.

Die Arbeit an diesem Text entstand im Rahmen interdisziplinärer Forschung im Bayerischen Forschungsverbund **"ForDaySec — Sicherheit in der Alltagsdigitalisierung"** (https://fordaysec.de), gefördert durch das Bayerische Staatsministerium für Wissenschaft und Kunst (StMWK).

Literaturverzeichnis

[Ad99] Adams, A.; Sasse, M. A.: Users Are Not The Enemy. Commun. ACM 42(12): 40-46 (1999)

[Am14] Amelang, K.: Transplantierte Alltage. Zur Produktion von Normalität nach einer Organtransplantation. Bielefeld: transcript.

[Ax21] Axehill, J.; Herzog, E.; Tingström, J.; Bengtsson, M.: From Brownfield to Greenfield Development - Understanding and Managing the Transition. 31st Annual INCOSE International Symposium, 2021.

[Be22] Benenson, Z.; Freiling, F.; Meyer-Wegener, K.: Soziotechnische Einflussfaktoren auf die "digitale Souveränität" des Individuums. In: Glasze, Georg; Odzuck; Eva; Staples, Ronald (Hrsg.): Was heißt digitale Souveränität? Diskurse, Praktiken und Voraussetzungen "individueller" und "staatlicher Souveränität" im digitalen Zeitalter, Bielefeld: transcript Verlag, S. 61-87 (Politik in der digitalen Gesellschaft), 2022.

[Be97] Beck, S.: Umgang mit Technik. Kulturelle Praxen und kulturwissenschaftliche Forschungskonzepte. Berlin: Akademie Verlag. 1997

[Bl88] Black, A. P.; Lazowska, E. D.; Levy, H. M.; Notkin, D.; Sanislo, J.; Zahorjan, J.: Interconnecting heterogeneous computer systems. Communication of the ACM, ACM.1988

[Bi21] Bieler, P.; Milena D. B.M; Hauer, J.; Klausner, M.; Niewöhner, J.; Schmid, C.; von Peter, S.: Distributing Reflexivity through Co-laborative Ethnography. In: Journal of Contemporary Ethnography 50 (1): 77–98, 2021.

[BT20] Burkholder, C.; Thompson, J.: Fieldnotes in qualitative education and social science research. Routledge, New York, 2020.

[Ca23] Catuogno, L.; Galdi, C. Secure Firmware Update: Challenges and Solutions. Cryptography 2023, 7, 30, 2023.

[Cl90] Clifford, J.: Notes on (Field)notes. In (Sanjek, R.; Hrsg): Fieldnotes: The Makings of Anthropology. Cornell University Press, London, S. 47–70, 1990.

[Ch16] B. -C. Choi, S. -H. Lee, J. -C. Na, J. -H. Lee: Secure firmware validation and update for consumer devices in home networking, in IEEE Transactions on Consumer Electronics, vol. 62, no. 1, pp. 39-44., 2016.

[Cs23] Connectivity Standards Alliance, Online: https://csa-iot.org (Abgerufen Okt. 2023), 2023.

[Da99] Davies, C. A.: Reflexive Ethnography: A Guide to Researching Selves and Others. Routledge, New York, 1999.

[Do04] Dourish, P.; Grinter, R.E.; Delgado de la Flor, J.; Joseph, J.: Security in the wild: user strategies for managing security as an everyday, practical problem. Pers. Ubiquit. Comput. 8, 2004, 391-401.

[Dw18] Daynes, S.; Williams, T.: On Ethnography. Polity Press, Medford, 2018.

[Ec23] Eckhardt, D.: Ethnografisches Feldnotieren in digitalen Feldern: Perspektiven einer Wissens- und Arbeitspraxis. In (Eckhardt, D.; Klausner, M.; Hrsg.): Digital[ität] Ethnografieren. Forschungsmethoden für den digitalen Alltag. Kulturanthropologie Notizen 85, S. 52–77, 2023.

[Etsi19] ETSI TR 103 536 V1.1.2, SmartM2M; Strategic/technical approach on how to achieve interoperability/interworking of existing standardized IoT Platforms, ETSI, 2019.

[Fa23] Fassl, M.; Krombholz, K.: Why I Can't Authenticate - Understanding the Low Adoption of Authentication Ceremonies with Autoethnography. CHI 2023: 72:1-72:15, 2023.

[Ge73] Geertz, C.: Thick Description: Toward an Interpretive Theory of Culture. In (ders.): The Interpretation of Cultures. Selected Essays. Basic Books, New York, 1973.

[Gr04] McGraw, G.: Software security. IEEE Secur. Privacy, vol. 2, no. 2, pp. 80–83, Aug. 2004.

[Gr14] M. Green, M. Smith: Developers are Not the Enemy!: The Need for Usable Security APIs. IEEE Secur. Priv. 14(5): 40-46, 2016.

[Ha23] J. M. Haney, S. M. Furman: User Perceptions and Experiences with Smart Home Updates. IEEE Symposium on Security and Privacy (SP), San Francisco, pp. 2867-2884, 2023.

[Ho09] Horst, C.: Expanding Sites: The Question of 'Depth' Explored. In (Falzon, M.A.; Hrsg.): Multi-sited Ethnography: Theory, Praxis and Locality in Contemporary Research. Routledge, London, 2009.

[ISO27034] ISO/IEC 27034-1 Information technology — Security techniques — Application security — Part 1: Overview and concepts, ISO, Geneva, 2011.

[ISO27403] ISO/IEC DIS 27403 Cybersecurity – IoT security and privacy – Guidelines for IoT-domotics, ISO, Geneva, 2023.

[ISO27404] ISO/IEC WD 27404 Cybersecurity – IoT security and privacy – Cybersecurity labelling framework for consumer IoT, ISO, Geneva, 2023

[Je99] Jeggle, U.: Alltag. In (Bausinger, H.; Jeggle, U.; Korff. G.; Scharfe; M. Hrsg.): Grundzüge der Volkskunde. Wissenschaftliche Buchgesellschaft, Darmstadt, S. 81–126, 4. Auflage, 1993.

[Ka23] Kalthoff, H.: Einleitung: Zur Dialektik von qualitativer Forschung und soziologischer Theoriebildung. In (Kalthoff, H.; Hirschauer, S.; Lindemann, G.; Hrsg.): Theoretische Empirie. Zur Relevanz qualitativer Forschung. Suhrkamp, Frankfurt am Main, S. 8–34, 4. Auflage, 2023.

[KE23] Klausner, M.; Eckhardt, D.: Digitalität und Ethnografie: Eine Einführung in Forschungsmethoden für mehr-als-digitale Felder. In (dies.; Hrsg.): Digital[ität] Ethnografieren. Forschungsmethoden für den digitalen Alltag. Kulturanthropologie Notizen 85, S. 2–19, 2023.

[Kh21] R. A. Khan, S. U. Khan, H. U. Khan and M. Ilyas: Systematic Mapping Study on Security Approaches in Secure Software Engineering, in IEEE Access, vol. 9, pp. 19139-19160, 2021.

[Ko15] Koch, G.: Empirische Kulturanalyse in digitalisierten Lebenswelten. Zeitschrift für Volkskunde 111/2, S. 179–200, 2015.

[Kr09] Krauss, W.; Localizing Climate Change: A Multi-sited Approach. In (Falzon, M.; Hrsg.): Multi-sited Ethnography: Theory, Praxis and Locality in Contemporary Research. Routledge, New York, S. 149–164, 2009.

[Ku16] Kusen, E.; Strembeck, M.: A decade of security research in ubiquitous computing: results of a systematic literature review, International Journal of Pervasive Computing and Communications Vol. 12 No. 2, pp. 216-259, Emerald Group Publishing Limited, 2016.

[Li93] Lipp, C.: Alltagskulturforschung im Grenzbereich von Volkskunde, Soziologie und Geschichte. Aufstieg und Niedergang eines interdisziplinären Forschungskonzepts. Zeitschrift für Volkskunde 89/1, S. 1–33, 1993.

[Li05] Lipner, S.; Michael, H.: The Trustworthy Computing Security Development Lifecycle. [Online]. Available: https://msdn.microsoft.com/en-us/library/ms995349.aspx, 2005

[Ma19] Evandro L. C. Macedo, E.; De Oliveira, E.; Silva, F.; Mello Jr, R.; França, F.; Delicato, F.; Rezende, F.; De Moraes, L.: On the Security Aspects of Internet of Things: A Systematic Literature Review, JOURNAL OF COMMUNICATIONS AND NETWORKS, VOL. 21, NO. 5, OCTOBER 2019.

[Ma17] Madden, R.: Being Ethnographic. A Guide to the Theory and Practice of Ethnography. Sage, London, 2017.

[Mo17a] F. Armknecht, Z. Benenson, P. Morgner, C. Müller, C. Riess: Privacy implications of room climate data. J. Comput. Secur. 27(1): 113-136 (2019)

[Mo17b] P. Morgner, S. Mattejat, Z. Benenson, C. Müller, F. Armknecht: Insecure to the touch: attacking ZigBee 3.0 via touchlink commissioning. WISEC 2017: 230-240

[Mo18] Moran, B.; Brown, D.; Meriac, M.; Tschofenig, H.: A Firmware Update Architecture for Internet of Things Device, 2018.

[Mo20] P. Morgner, C. Mai, N. Koschate-Fischer, F. Freiling and Z. Benenson: Security Update Labels: Establishing Economic Incentives for Security Patching of IoT Consumer Products. IEEE Symposium on Security and Privacy (SP), USA, 2020.

[Ni16] Niewöhner, J.: Co-Laborative Anthropology: Crafting Reflexivities Experimentally. In (Jouhki, J.; Steel, T., Hrsg): Etnologinen tulkinta ja analyysi: Kohti avoimempaa tutkimus- prosessia [Ethnological interpretation and analysis: Towards a transparent research process], Ethnos, S. 81–125, 2016.

[Pö20] H. C. Pöhls and N. Rakotondravony. Dynamic Consent: Physical switches and feedback to adjust consent to IoT data collection. In Proceedings of the 2nd International Conference on HCI for Cybersecurity, Privacy and Trust (HCI-CPT 2020) held in conjunction with the 22nd International Conference on Human Computer Interaction (HCII 2020), pages 322-335, Springer, Jul., 2020.

[Pu20] G. Pugliese, C. Riess, F. Gassmann, Z. Benenson: Long-Term Observation on Browser Fingerprinting: Users' Trackability and Perspective. Proc. Priv. Enhancing Technol. 2020(2): 558-577, 2020.

[Re19] L. Reinfelder, R. Landwirth, Z. Benenson: Security Managers Are Not The Enemy Either. CHI 2019:433, 2019.

[Ru14] M. Rushanan, A. D. Rubin, D. F. Kune and C. M. Swanson: SoK: Security and Privacy in Implantable Medical Devices and Body Area Networks. IEEE Symposium on Security and Privacy, Berkeley, pp. 524-539, 2014.

[Sa99] Sanjek, R.: Fieldnotes. The Making of Anthropology. Cornell University Press, London, 1999.

[Sc13] Schäfer, T.: Die Instabilität der Praxis. Reproduktion und Transformation des Sozialen in der Praxistheorie. Weilerswist: Velbrück Wissenschaft, 2013.

[Sc20] Schmoll, F.: „Volkskunde 70“: 50 Jahre Falkenstein – ein Einordnungsversuch. Zeitschrift für Volkskunde 116/2, S. 217–240, 2020.

[SGP+23] Stöver, A.; Gerber, N.; Pridöhl, H.; Maass, M.; Bretthauer, S.; Spiecker genannt Döhmann, I.; Hollick, M.; Herrmann, D.: How Website Owners Face Privacy Issues: Thematic Analysis of Responses from a Covert Notification Study Reveals Diverse Circumstances and Challenges. Proc. Priv. Enhancing Technol. 2023(2): 251-264, 2023.

[So12] Sommerville, I.: Software Engineering, Ausgabe 9, S. 276, ISBN 978-3-86894-099-2. Pearson, 2012.

[St04] Strathern, M.: Partial Connections. AltaMira, Walnut Creek, 2004.

[St00] Stajano, F. ; Anderson, R.J.: The Resurrecting Duckling: Security Issues in Ad-Hoc Wireless Networks, Proc. Seventh Security Protocols Workshop, Lecture Notes in Computer Science 1796, Springer- Verlag, Berlin, pp. 172–182, 2000.

[Tr17] Tragos, E.; Fragkiadakis, A.; Angelakis, V.; Pöhls, H. C.: Designing Secure IoT Architectures for Smart City Applications. Designing, Developing, and Facilitating Smart Cities, Springer, 2017.

[Ts06] Tschofen, B.: Vom Alltag. Schicksale des Selbstverständlichen in der Europäischen Ethnologie. In (Bockhorn, O.; Schindler, M.; Stadelmann, C.; Hrsg.): Alltagskulturen. Forschungen und Dokumentationen zu östereichischen Alltag seit 1945. Selbstverlags des Vereins für Volkskunde, Wien, S. 91–102, 2006.

[Vo13] Volkamer, M.; Renaud, K.: Mental Models - General Introduction and Review of Their Application to Human-Centred Security. Number Theory and Cryptography 2013: 255-280

[Wa10] Wash, R.: Folk Models of Home Computer Security. SOUPS 2010.

[Wa23] Wagner, E.; Rothaug, N.; Wolsing, K.; Bader, L.; Henze, M.; Wehrle, K.: Retrofitting Integrity Protection into Unused Header Fields of Legacy Industrial Protocols. In 48th IEEE Conference on Local Computer Networks (IEEE LCN'23), 2023.

[We23] L. Weinberger, C. Eichenmüller, Z. Benenson: Interplay of Security, Privacy and Usability in Videoconferencing. CHI Extended Abstracts 2023: 185:1-185:10

[We91] Weiser, M.: The Computer for the 21st century, Scientific American, 1991.