FOR DAY SEC

Bayerischer
Forschungsverbund
Sicherheit in der Alltagsdigitalisierung

Cyber-sicherheit im Alltag

Ein Lagebild mit Szenarien, Forschungsperspektiven und Handlungsoptionen

»Die Grenzen zwischen nützlicher Technologie und Datenschutzrisiko verschwimmen zunehmend«

Aktuelle Erkenntnisse aus dem Forschungsverbund ForDaySec

Prof. Dr. Stefan Katzenbeisser

Lehrstuhl für Technische Informatik, Universität Passau

»**Nicht alles kann sicher gebaut werden.** Aber vieles lässt sich sicher integrieren. Dafür brauchen wir Strategien, die mit Unsicherheit rechnen und mit denen wir trotzdem handlungsfähig bleiben.«

Prof. Dr.-Ing. Felix Freiling

Lehrstuhl für Informatik 1 (IT-Sicherheitsinfrastrukturen), FAU Erlangen-Nürnberg

»Datenschutzbehörden, aber auch andere Fachleute aus der Zivilgesellschaft, benötigen dringend **innovative technische Werkzeuge**, um mehr Transparenz im Technologiedschungel des Alltags zu schaffen.«

Prof. Dr. Sabine Pfeiffer

Lehrstuhl für Soziologie mit dem Schwerpunkt Technik – Arbeit – Gesellschaft, FAU Erlangen-Nürnberg

»Cybersicherheit ist zu komplex, um die Bürger damit alleine zu lassen. Wenn immer mehr Menschen, Geräte und Behörden vernetzt sind, braucht es **alltagstaugliche Usability und einen politischen Masterplan,** der alle Ebenen mitdenkt. IT-Sicherheit geht uns alle an!«

Prof. Dr. Johannes Kinder

Lehrstuhl für Programmiersprachen und KI , Ludwig-Maximilians-Universität München

»Wenn allein der Hersteller für Sicherheitsupdates verantwortlich ist, müssen gerade **günstige Smart Devices** im Zweifel sehr schnell aus dem Verkehr gezogen werden. Mit technischen Maßnahmen können wir Updates zu unseren Bedingungen durchsetzen und so auch die Lebensdauer dieser Geräte verlängern.«

Prof. Dr. Dominik Herrmann

Lehrstuhl Privatsphäre und Sicherheit in Informationssystemen, Otto-Friedrich-Universität Bamberg

»**Datenschutz-Compliance nervt? Muss nicht sein.** Wir machen abstrakte Regeln anfassbar. Durch Karten, die man in die Hand nehmen kann, durch interaktive Umgebungen zum Aufspüren von Datenschutzproblemen und durch digitale Lernformate, mit denen Wissen länger hängen bleibt. Damit Datenschutz in Entwicklung und Betrieb nicht mehr nur als lästige Pflichterfüllung abgetan wird.«

Dr. rer. nat. Henrich C. Pöhls

Lehrstuhl für Informatik mit Schwerpunkt IT-Sicherheit, Universität Passau

»**Smarte Alltagsgeräte senden ständig Daten und sind untereinander vernetzt** – ob nötig oder nicht. Wenn man die Netzwerkkommunikation einschränkt oder sogar ganz vom Internet isoliert, schützt man nicht nur seine kritischen Funktionen, sondern kann auch mehr Privatsphäre im digitalen Alltag erreichen. Wir wollen smarte Fähigkeiten auch ›offline‹. «

Dr. Dennis Eckhardt

Lehrstuhl für Soziologie mit dem Schwerpunkt Technik – Arbeit – Gesellschaft, FAU Erlangen-Nürnberg

»**Menschen kümmern sich oft unbeobachtet um digitale Sicherheit:** in Familien, in kleinen Betrieben, im Ehrenamt. Es fehlen allerdings Perspektiven in der Forschung, welche dieses alltägliche Kümmern um Sicherheit untersuchen können. Gesellschaftlich fehlen darüber hinaus Ansätze und Maßnahmen, welche die Menschen auf Augenhöhe mitnehmen, und sie nicht ›nur‹ auf ihre Fehler aufmerksam machen.«

Prof. Dr. Thomas Riehm

Institut für das Recht der digitalen Gesellschaft (IRDG), Universität Passau

»**Digitale Produkte müssen nach dem Kauf weiter betreut werden** – nicht nur, um Fehler zu beheben, sondern um Sicherheit über den gesamten Lebenszyklus zu gewährleisten. Dafür braucht es dringend Rechtssicherheit und klare Leitplanken für Unternehmen und Verbraucher.«

Digitale Sicherheit als Forschungs- und Gesellschaftsaufgabe

Die Digitalisierung des Alltags stellt eine der zentralen Herausforderungen unserer Gesellschaft dar. Vernetzte Systeme durchdringen alle Lebensbereiche – von der Mobilität über die Gesundheitsversorgung bis hin zur Verwaltung. Während in Unternehmen eigene Abteilungen mit Kompetenz im Bereich Digitalisierung und digitaler Sicherheit über die Einführung und Nutzung neuer Technologien wachen, fehlt es in privaten Haushalten oft an Wissen, Ressourcen und struktureller Unterstützung.

Sicherheit im digitalen Alltag ist jedoch der Schlüssel zum Erhalt technologischer Souveränität im Kontext der Wucht, mit der Digitalisierung und künstliche Intelligenz in unsere Welt drängen. Dafür müssen zwei grundlegende Herausforderungen nicht nur bewältigt, sondern in politische Weichenstellungen integriert werden: **die zunehmende Komplexität digitaler Systeme und das menschliche Verhalten im Umgang mit Technik.**

Bruce Schneier warnte bereits 1999:

»The worst enemy of security is complexity.«

Mit jeder neuen vernetzten Komponente steigt die Zahl potenzieller Angriffspunkte, ebenso wie die kognitive Belastung für Nutzende. Sicherheit scheitert selten an fehlender Aufklärung, sondern an psychologischen, menschlichen Mustern. Studien belegen, dass kurzfristige Bequemlichkeit langfristige Sicherheitsziele häufig verdrängt. Hinzu kommen strukturelle Herausforderungen: Die digitale Ausgrenzung älterer Menschen wird mehr und mehr sichtbar.

Die bequeme Lösung, Verantwortung auf Nutzende zu schieben und mehr »Awareness« zu fordern, ist zum Scheitern verurteilt. Sie führt zu kognitiver Überlastung und Entscheidungsmüdigkeit. **Menschen können nicht für jede smarte Glühbirne eine Risikoanalyse durchführen.**

Die Realität zeigt:

Ohne eine gezielte Veränderung von Anreizstrukturen wächst die Komplexitätsfalle weiter.

Deshalb braucht es:

- Transparente Risikokommunikation bereits vor dem Kauf
- Sichere Voreinstellungen als Standard („Security by Default")
- Einen klar regulierenden Staat, der Hersteller in die Verantwortung nimmt
- Offline-fähige Alternativen als Wahlmöglichkeit

Dieses Whitepaper zeichnet ein aktuelles Lagebild zur Cybersicherheit im Alltag, benennt zentrale Trends und zeigt anhand von Entwicklungsszenarien, wie Sicherheit gelingen oder scheitern kann. Es bündelt rechts-, sozial- und technikwissenschaftliche Perspektiven und macht konkrete forschungsbasierte Handlungsoptionen sichtbar, die im Rahmen von *ForDaySec* erarbeitet wurden.

Handlungsdruck, Trends und Perspektiven

Im internationalen Vergleich wird deutlich: **Viele Länder haben begonnen, digitale Sicherheit nicht nur als technologische Herausforderung zu begreifen, sondern als gesamtgesellschaftliche Aufgabe.** Die USA verlagern Verantwortung auf Hersteller, Großbritannien integriert Sicherheit in Technologiepolitik, Singapur belohnt Bürgerbeteiligung. Europa setzt mit der NIS2-Richtlinie und dem Cyber Resilience Act neue Standards – doch die Alltagswirksamkeit bleibt fraglich.

Gleichzeitig steigt der Handlungsdruck in Deutschland. Die Schadensbilanz von Cybercrime ist alarmierend: **267 Milliarden Euro pro Jahr*** verursachen digitale Angriffe in der Wirtschaft, fast 6% des BIP. Im Jahre 2023 waren es noch 206 Milliarden Euro – **ein Anstieg um rund 30% innerhalb nur eines Jahres.**

Auch öffentliche Einrichtungen sind betroffen – vom Flughafen Hamburg bis zur Hochschule Frankfurt. Ein strukturelles Problem verschärft die Lage: Sicherheitskosten werden häufig externalisiert. Der britische Sicherheitsforscher Ross Anderson identifizierte früh diese Fehlanreize: Wer unsichere Produkte verkauft, trägt selten die Folgekosten. Das Resultat ist *Security by Disaster*: Investitionen erfolgen erst nach dem Schadensfall. Die Revolution des Internet of Things (IoT) multipliziert die Risiken: Jede smarte Steckdose, jedes vernetzte Babyphone wird zum potenziellen Einfallstor. **Nutzende werden zu unfreiwilligen Sicherheitsmanagern, ohne Wissen, Zeit oder Ressourcen.**

*Quelle: Bitkom Research 2024

Die Folgen reichen von Datenabfluss bis hin zu Kontrollverlust über wichtige Infrastrukturen, wie etwa Heizung oder Energieversorgung. Eine völlig neue Dimension stellt generative KI dar: Sie erweitert die Angriffsflächen, macht Manipulationen leichter skalierbar und verschärft die Risikolage.

Die Bedarfe sind erkannt und reichen tief in alle gesellschaftlichen Bereiche: In Haushalten verbreiten sich IoT-Geräte zunehmend »durch die Hintertür«, etwa als Geschenke an die Silver Generation. In Betrieben übernehmen Mitarbeitende IT-Sicherheitsaufgaben, für die sie nicht ausgebildet wurden, Verwaltungen sind personell unterbesetzt. **Die Grenzen zwischen nützlicher Technologie und Datenschutzrisiko verschwimmen zunehmend und niemand überblickt mehr die Komplexität der verwendeten Dienste und Geräte,** das heißt: **IT-Sicherheit muss systemisch gedacht werden.**

Mehrere technologische, soziale und politische Trends verändern also derzeit das Ökosystem der digitalen Sicherheit und führen zu einem Paradigmenwechsel: Während IoT-Geräte und KI-Anwendungen exponentiell zunehmen, verschärft sich der Fachkräftemangel und die digitale Spaltung. Gleichzeitig wächst die Erwartung an eine souveräne, gerechte und verlässliche Absicherung des digitalen Alltags – im Privaten wie in öffentlichen Infrastrukturen. Deutschland könnte seine einzigartige Position – starke Industrie und Technologieentwicklung kombiniert mit exzellenter Sozialforschung – in Zukunft noch stärker nutzen, um nutzerzentrierte Ansätze zu entwickeln, denn **wer sich hier gut aufstellt, stärkt nicht nur das Vertrauen der Bevölkerung, sondern schafft auch die Grundlagen für technologische Souveränität im internationalen Wettbewerb.**

Zukunftstrends und ihre Auswirkungen auf die IT-Sicherheit im Alltag

	Generative KI	IoT-Explosion	Demographischer Wandel	Cloud-Migration	Compliance Theater	Digitale Nachhaltigkeit
Beispiel	Persönliche Daten in ChatGPT und täuschend echte Deepfakes	Sehr viele smarte Haushaltsgeräte	Ältere Menschen in digitale Systeme gedrängt	Datenzugriffe ausländischer Behörden	Fokus auf Zertifikate statt echte Sicherheit	Geräte auf Cloud-Dienste und Updates angewiesen
Auswirkungen	Datenverlust, neue Betrugsformen (z. B. Enkeltrick 2.0)	Wachsende Komplexität, neue Angriffsflächen	Digitale Ausgrenzung, Überforderung, Teilhabeverlust	Kontrollverlust, Abhängigkeit, Rechtsunsicherheit	Scheinsicherheit, blinder Fleck für reale Risiken	Kurze Lebenszyklen, mangelnde Update-Fähigkeit, Ressourcenverschwendung

Quelle: Bayerischer Forschungsverbund ForDaySec

Rechtswissenschaftliche Perspektive

Aktualisierungspflichten beim Vertrieb von Software an Verbraucher

Handlungsempfehlungen für den Handel

Mit dem Vertrieb von Software – auch wenn sie in Hardware eingebettet ist – betreten Händler rechtlich anspruchsvolles Terrain. Denn das Gesetz verpflichtet sie im Geschäft (Business-to-Consumer) zur Bereitstellung sogenannter erhaltender Aktualisierungen. Das sind insbesondere Sicherheits-Updates, aber etwa auch Aktualisierungen, die die Kompatibilität mit veränderter Standardsoftware sicherstellen. Die Verpflichtung besteht auch dann, wenn sie die Software nicht selbst entwickelt haben. Zwei Herausforderungen stehen dabei im Mittelpunkt:

- **Pflicht zur Aktualisierung trotz fehlender Kontrolle:** Händler müssen Updates liefern, auch wenn sie weder auf Quellcode noch auf die technische Infrastruktur zugreifen können.

- **Trennung von erhaltenden und erweiternden Updates:** Gesetzlich geschuldet sind nur erhaltende Aktualisierungen. Funktionale Erweiterungen dürfen ohne Zustimmung der Nutzenden nicht „untergemischt" werden.

Falls eine vertragliche Absicherung innerhalb der Lieferkette nicht möglich ist, besteht eine weitere Option in der **transparenten Einschränkung gegenüber Anwendern:** Die Updatepflicht kann durch klare vertragliche Hinweise bereits vor dem Kauf eingeschränkt werden. Nutzende müssen dieser Einschränkung ausdrücklich zustimmen. Ob das rechtlich in jedem Fall Bestand hat, ist derzeit jedoch noch offen. **In jedem Fall gilt:** Bleiben Aktualisierungen aus oder werden falsch umgesetzt, drohen Gewährleistungsansprüche und erhebliche Haftungsrisiken.

Sozialwissenschaftliche Perspektive

Nutzungsverhalten, Vertrauen, Awareness

Sozialwissenschaftliche Perspektive: Sicherheit muss sich an den Lebensrealitäten orientieren

IT-Sicherheit ist kein rein technisches Problem, sondern eine Frage der Alltagslogik. Unsere Forschung zeigt: **Menschen agieren nicht als isolierte „User", sondern in komplexen Haushalts- und Arbeitskontexten.**

Ein Beispiel aus dem Alltag:
Der Vater kauft ein vernetztes Gerät, der Sohn kümmert sich um Updates, die Mutter erhält keine Einweisung. Ein Nutzungs-Bias ist daher schon jetzt Alltag im Wohnalltag. Da sich der Sohn schon um das Device kümmern wird, fehlt oft die Motivation, eigene IT-Sicherheitskompetenz aufzubauen.

Awareness-Kampagnen greifen oft ins Leere, wenn sie an den Lebensrealitäten vorbeigehen.

In Unternehmen ist das Problem nicht kleiner. Besonders im Mittelstand übernehmen Mitarbeitende IT-Sicherheitsaufgaben ohne Ausbildung aus Mangel an Alternativen. Arbeitsüberlastung und fehlende Ressourcen verstärken die **strukturelle Unsicherheit.**

Informatik Perspektive

Wenn Komfort Risiken schafft – wie KI, IoT und Cloud unsere Alltagsinfrastruktur verändern

Die technologische Realität überholt vielerorts die Schutzkonzepte

Eine neue Generation Smart-Home-Anwendungen mit integrierter KI schafft Komfort, aber auch neue Angriffsflächen. Die zunehmende Integration von KI, IoT und Cloud-Diensten im Alltag wirft fundamentale Fragen der Sicherheit auf.

Ein zentrales Problem besteht in der **Intransparenz geschlossener IoT-Ökosysteme.** Proprietäre Schnittstellen erschweren unabhängige Sicherheitsprüfungen und fördern herstellerseitige Abhängigkeiten. Viele Funktionen sind in Cloud-Diensten ausgelagert, häufig bei Anbietern außerhalb der EU. Dadurch entstehen neue datenschutz- und sicherheitsrechtliche Herausforderungen.

Noch komplexer wird es mit der Integration generativer KI-Systeme wie Large Language Models (LLMs). Assistenzdienste mit Zugriff auf Sensoren und Geräte ermöglichen völlig neue Anwendungen, bergen aber das Risiko, dass Nutzende hochsensible Daten preisgeben, oft ohne zu wissen, wo und wie diese verarbeitet werden.

► Handlungsempfehlungen:

Rechtswissenschaft

Updatepflichten sind rechtlich komplex und werden in der Praxis häufig unterschätzt. Händler sollten sich in der Lieferkette unbedingt Updates zusichern lassen und sich rechtzeitig juristischen Rat einholen – nicht zuletzt, um die Sicherheit im digitalen Alltag nachhaltig abzusichern.

Sozialwissenschaft

Man wird es sich in der Zukunft nicht mehr leisten können, an den Menschen vorbeizuforschen. Ein systemisches Verständnis von Verantwortung, Rollen und Alltagslogiken ist Voraussetzung dafür, Sicherheitslösungen wirksam zu gestalten.

Informatik

Sicherheitsfunktionen für den Einsatz von Cloud-basierten KI-Systemen in IoT-Umgebungen lassen sich am zuverlässigsten gestalten, wenn KI-Systeme lokal und dezentral auf Endgeräten betrieben werden – in Kombination mit offenen Standards. So bleibt Kontrolle gewährleistet. Forschung und Hersteller tragen dafür gemeinsam Verantwortung.

HEUTE

Endlose Awareness-Schulungen und Sicherheitstrainings

Komplexe Passwortrichtlinien für dutzende Accounts

Gesetzgeber macht **Einzelperson verantwortlich**

Unüberschaubare Mengen an Geräten und Apps zu verwalten

Ständige Phishing-Warnungen und Verdachtsmeldungen

Jedes Unternehmen hat **eigene Sicherheitsanforderungen**

Permanente Updates und Patches müssen installiert werden

Schuldzuweisungen bei Sicherheitsvorfällen

MORGEN

Systemische Sicherheit – Schutz ist standardmässig in Technologie eingebaut

Regulierung – Unternehmen und Anbieter tragen die Hauptverantwortung für Sicherheit

Geschützte Privatsphäre – Sicher vor Angreifern und Staatstrojanern

Sichtbare Verbände – Kompetente Ansprechpartner für die digitale Sicherheit sind bekannt

Automatisierung – Updates & Patches laufen sicher im Hintergrund

Zielgerichtete Bildung – Relevante Sicherheitskompetenzen statt Missachtung

Sichere Infrastruktur – Resiliente Systeme auf gesellschaftlicher Ebene

Niedrigschwellige Hilfe – Einfache Wege, um Unterstützung zu erhalten

Cybersecurity-Szenarien – Forschungserkenntnisse zur digitalen Sicherheit

Heute ist der digitale Alltag oft von Überforderung geprägt: Menschen und Unternehmen tragen die Hauptverantwortung für ihre Sicherheit, mit komplexen Passwörtern, endlosen Schulungen und ständig neuen Bedrohungen.

Morgen kann Sicherheit systemisch gedacht werden: Verantwortung wird geteilt, Risiken minimiert, Unterstützung leicht zugänglich, und Alltagssicherheit wird so zum Standard.

ForDaySec bringt hier erstmals Forschung aus Informatik, Rechts- und Sozialwissenschaften zusammen, um genau diesen Wandel zu ermöglichen: von individueller Überlastung hin zu einem verlässlich geschützten digitalen Alltag.

Empfehlungen für die Wissenschaftspolitik

Die Forschung im Bereich der digitalen Alltagssicherheit steht vor einer doppelten Herausforderung:
Sie muss technologische Entwicklungen vorausdenken und gleichzeitig alltagsnahe Lösungen ermöglichen. Dafür braucht es gezielte Unterstützung aus der Wissenschaftspolitik. **Bayern vereint starke Industrie, exzellente Forschung und Innovationsmut – ideale Voraussetzungen, um internationale Standards nicht nur zu erfüllen, sondern zu setzen.**

ForDaySec sieht diese Handlungsperspektiven nach internationalem Vorbild, um Bayern als Vorreiterregion zu positionieren:

- Bürgerbeteiligung ermöglichen – nach dem Vorbild von Singapur und den Niederlanden: Programme zur **Einbindung von White-Hat-Hackern** und Sicherheitsforschenden aus der Zivilgesellschaft stärken die gesellschaftliche Verankerung.

- **„Security by Design"** fördern – orientiert an britischen Standards: Die gezielte Berücksichtigung von Sicherheit als Förderkriterium bei der Vergabe von Forschungsmitteln setzt frühzeitig Anreize für praxistaugliche Lösungen.

- Transparenz schaffen – durch regelmäßige Sicherheits-Assessments: Das niederländische Modell **koordinierter Lagebilder** könnte Forschungsverbünden in Deutschland als Vorbild dienen.

Im Freistaat Bayern und auch deutschlandweit kann durch gezielte Förderung nutzerzentrierter Sicherheitslösungen eine Brücke zwischen EU-Regulierung und praktischer Umsetzung geschlagen werden – **Bayern kann damit als Modellregion für andere Bundesländer und Europa dienen.**

Strategie für Unternehmen: Rückrufmanagement neu denken

Smarte Produkte sammeln kontinuierlich Daten über ihren Zustand. Diese Informationen können gezielt genutzt werden, um Gefahren frühzeitig zu erkennen, etwa durch Muster in Telemetriedaten. Gleiches gilt für Social-Media-Daten. Unternehmen bietet sich hier die Chance, ihr Rückrufmanagement an die Gegebenheiten des vernetzten Alltags und Social Media anzupassen und auf zwei Ebenen aktiv zu werden, um Risiken zu minimieren.

Zwei Handlungsebenen für Unternehmen:

Erstens: Informationsgewinnung neu aufstellen

- Monitoring unternehmenseigener Websites, Social-Media-Kanäle und externer Plattformen
- Einsatz von KI-Tools oder spezialisierten Dienstleistern zur Mustererkennung

Zweitens: Gezielt reagieren und kommunizieren

- Warnhinweise direkt auf Produktdisplays
- Fehlerbehebende Updates als Standardmaßnahme
- Fernabschaltungen als ultima ratio

➤ Fazit:

Rückrufmanagement ist Sicherheitsaufgabe. Unternehmen, die vernetzte Produktdaten intelligent auswerten und über digitale Kanäle intervenieren, erhöhen die Produktsicherheit deutlich und minimieren eigene Haftungsrisiken.

Vier zentrale Fragen, die Unternehmen sich strategisch stellen sollten

Unternehmen sollten sich kritisch mit ihrer Verantwortung auseinandersetzen:

1. **Investieren wir in echte Sicherheitsverbesserung – oder nur in Dokumentation und Compliance?**
2. **Wo schieben wir Verantwortung an Verbraucherinnen und Verbraucher ab?**
3. **Welche unserer Produkte müssen bis 2027 die Anforderungen des Cyber Resilience Act erfüllen?**
4. **Wie schaffen wir Transparenz, ohne Geschäftsgeheimnisse preiszugeben?**

Wer diese Fragen offen beantwortet, kann aus regulatorischem Druck einen Wettbewerbsvorteil machen und Vertrauen in einer zunehmend vernetzten Welt aufbauen.

Perspektiven von außen: Expertinnen und Experten aus unserem Netzwerk

Dr. Helene Sigloch

Product Security Officer, BSH Hausgeräte GmbH

»**Das Internet der Dinge ist längst Teil unseres Alltags.** Ein erfolgreicher Hackerangriff kann im Ernstfall bis in unseren Nahbereich, unsere Küchen und Wohnzimmer, eindringen. Deshalb müssen alle gemeinsam für IT-Sicherheit sorgen: Hersteller und Nutzende, Behörden und Wissenschaft.«

Manuel Atug

Principal bei HiSolutions AG

»**Digitale Sicherheit ist Teil der Daseinsvorsorge und genauso unverzichtbar wie Wasser- oder Energieversorgung.** Systeme müssen daher sicher entwickelt, konfiguriert und betrieben werden, um alle Menschen Secure by Design & Default im Alltag zu schützen.«

Caroline Krohn

Fachbereichsleiterin - Digitaler Verbraucherschutz, Bundesamt für Sicherheit in der Informationstechnik BSI

»**IT-Sicherheit muss alltagstauglich sein.** Eine aktuelle BSI-Befragung zur IT-Sicherheit in Privathaushalten zeigt: Menschen wollen sich schützen, scheitern aber oft an unverständlicher Technik. Deshalb ist die konsequente Umsetzung von Usable Security so wichtig.«

Tatjana Halm

Referatsleiterin Recht und Digitales, Verbraucherzentrale Bayern e. V.

»**Der digitale Alltag verlangt ständiges Abwägen zwischen Komfort und Risiko.** Damit IT-Sicherheit nicht zur Zumutung wird, müssen Systeme von Anfang an sicher, verständlich und einfach gestaltet sein – Verantwortung darf nicht allein bei den Verbrauchern und Verbraucherinnen liegen.«

Sie wollen mehr über unsere Arbeit erfahren, Hintergründe kennenlernen und sich mit uns und unseren Expertinnen und Experten vernetzen?

Dann folgen Sie uns auf **LinkedIn** und bleiben Sie über Forschung, Entwicklungen und Veranstaltungen von ForDaySec auf dem Laufenden.

Sie möchten tiefer einsteigen und mehr über unsere Forschung erfahren?

Besuchen Sie uns auf unserer Homepage: **fordaysec.de**

Bayerischer Forschungsverbund **Sicherheit in der Alltagsdigitalisierung**

V.i.S.d.P.
Sabine Toussaint

Universität Passau
Geschäftsstelle ForDaySec
c/o Lehrstuhl Katzenbeisser
Innstraße 43
94032 Passau

fordaysec.de
linkedin.com/company/fordaysec

Kontakt:
fordaysec@uni-passau.de
+49 851 509 6043

Gestaltung:
grafikcafé :: feines design

gefördert durch:

Bayerisches Staatsministerium für Wissenschaft und Kunst

LMU Ludwig-Maximilians-Universität München
FAU Friedrich-Alexander-Universität Erlangen-Nürnberg
Otto-Friedrich-Universität Bamberg
Universität Passau
Technische Universität München