WHITEPAPER #03

Usable Security – *Handlungsfelder menschzentrierter Cybersicherheit*

DIGITALER VERBRAUCHERSCHUTZ

Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Inhaltsverzeichnis

Management Summary 04

1. Einleitung und Ausgangslage 06

2. Vier Handlungsfelder für Usable Security 08

2.1 Gebrauchstauglichkeit 10

2.2 Zugänglichkeit 12

2.3 Transparenz 14

2.4 Akzeptanz 16

3. Fazit und Ausblick 18

Referenzen 19

Impressum

Herausgeber:
Bundesamt für Sicherheit in der Informationstechnik (BSI)
Postfach 20 03 63 | 53133 Bonn
Tel.: 0800 274 1000 | bsi@bsi.bund.de

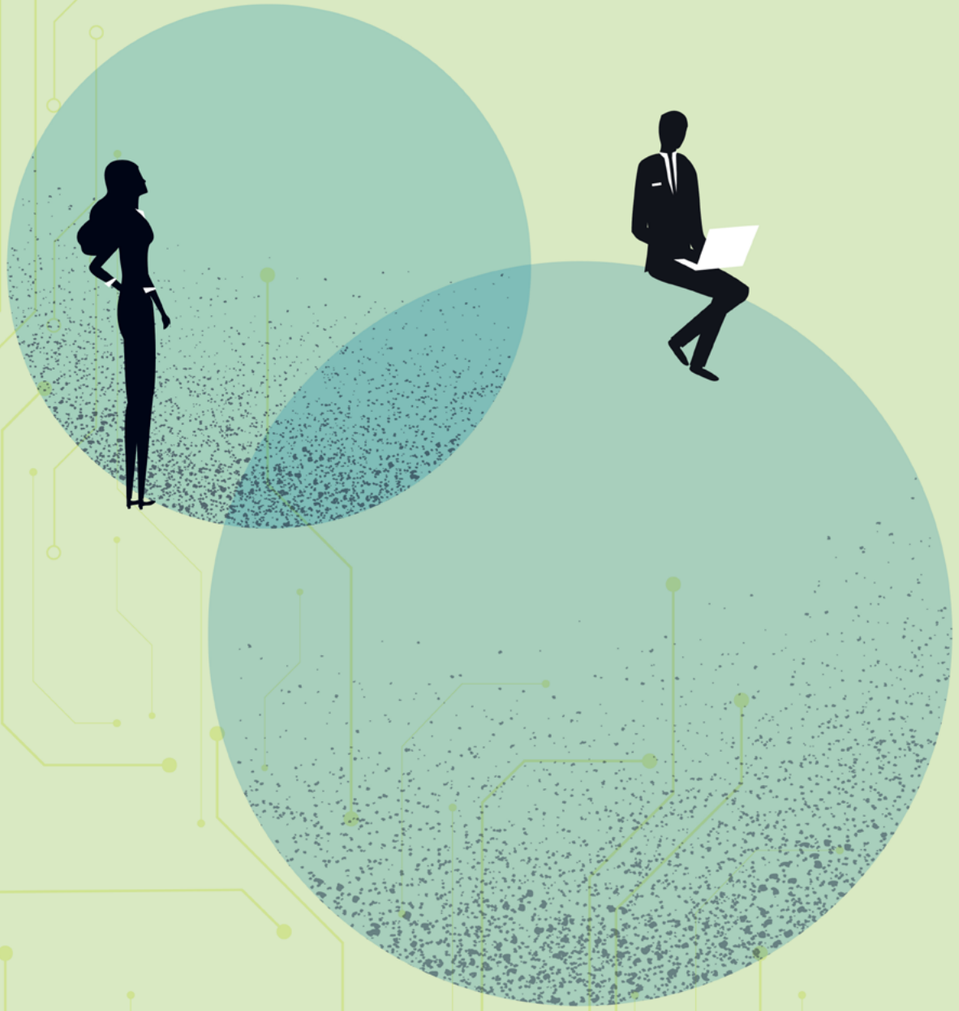
www.bsi.bund.de

Redaktion und Gestaltung: BSI

Stand: August 2025

Bildnachweise: AdobeStock©jozefmicic

Management Summary



In der Cybernation Deutschland müssen wir alle mitnehmen. Cybersicherheit muss für alle gleichermaßen im Alltag gut nutzbar und einfach umsetzbar sein. Dafür müssen Cybersicherheitsmaßnahmen den Grundsätzen menschzentrierter Gestaltung folgen. Cybersicherheitsmaßnahmen, die nicht nutzbar oder nicht verständlich sind, werden nicht akzeptiert und umgangen. Die Folgen sind Nicht-Nutzung, Falsch-Nutzung oder die Nutzung unsicherer Alternativen und damit eine deutliche Schwächung des Sicherheitsniveaus.

In vier zentralen Handlungsfeldern kann die Usable Security über definierte Gestaltungsprinzipien gezielt gesteigert werden:

Sicherheitsmechanismen müssen (1) praktisch und einfach *nutzbar*, (2) für alle leicht *zugänglich* und (3) in ihrer Wirkungsweise *transparent* sein, damit sie (4) von Nutzenden *akzeptiert* und sicher angewendet werden.

(1) Gebrauchstauglichkeit (Usability) orientiert sich an den Handlungszielen, die eine Anwenderin oder ein Anwender mit der Nutzung eines Systems verfolgt. **Cybersicherheit ist dabei in der Regel kein primäres Handlungsziel.** Cybersicherheitsmaßnahmen müssen sich daher gut und einfach in Handlungsabläufe und Nutzungsalltag integrieren lassen und möglichst wenig vom eigentlichen Ziel ablenken. Für ihren Erfolg in der Praxis ist eine bedachte menschzentrierte Gestaltung von Cybersicherheitsmaßnahmen essentiell.

(2) Zugänglichkeit: Der Schutz vor Cyberbedrohungen muss **allen ohne Einschränkung** möglich sein. Cybersicherheitsmechanismen müssen von Menschen mit unterschiedlichsten Bedürfnissen, Fähigkeiten und Ressourcen **gleichermaßen** genutzt werden können.

(3) Transparenz: Nutzende müssen verstehen können, **warum** sie bestimmte Maßnahmen anwenden sollten, aber auch **wie** sie funktionieren, **was** sie bewirken und **wie sie** demnach **anzuwenden sind.** Transparenz stärkt das Vertrauen in Anbieter und Systeme und ermöglicht **sicheres und selbstbestimmtes Handeln.**

(4) Fehlende Akzeptanz äußert sich durch Nicht-Nutzung, Falsch-Nutzung oder Umgehung von Cybersicherheitsmechanismen. Mitunter wird dadurch die Nutzung schwächerer Sicherheitsmechanismen begünstigt, die in der Usability besser abschneiden. **Gebrauchstauglichkeit, Zugänglichkeit und Transparenz sind die Grundlage für Akzeptanz.** Darüber hinaus gibt es jedoch noch weitere dedizierte Akzeptanz-Stellschrauben.

Mit Hilfe der vier Handlungsfelder kann und muss die Gestaltung menschzentrierter Cybersicherheit von Anfang an bei der Entwicklung neuer Cybersicherheitsmechanismen berücksichtigt werden. Bestehende Mechanismen können anhand des Handlungsrahmens überprüft und evaluiert werden.

Cybersicherheit und Usability wirken in eine Richtung – wenn man etwas dafür tut. Cybersicherheitsmaßnahmen, die menschzentriert gestaltet wurden, sind nicht nur einfacher zu nutzen, sondern heben zugleich das Sicherheitsniveau in der Praxis deutlich an. Usable Security ist ein essentieller Baustein wirksamer Cybersicherheit.

Menschzentrierte Gestaltung muss eine Standardanforderung der Regulierung zur Cybersicherheit werden. Cybersicherheit sollte Anforderung an die Anwendbarkeit im Alltag immer enthalten. Regulierungen wie der Cyber Resilience Act müssen stärker nutzerzentrierte Anforderungen integrieren. Usable Security sollte unter anderem in die Normungsaktivitäten zur Ausgestaltung des Cyber Resilience Act Einzug halten und sich letztendlich in Produkten und Diensten am Markt niederschlagen.

Das vorliegende Whitepaper ist eine Einladung zur gemeinsamen Diskussion und Weiterentwicklung dieses Themenfeldes.

1. Einleitung und Ausgangslage

Als Bundesamt für Sicherheit in der Informationstechnik (BSI) stellen wir uns der Herausforderung: wir wollen die digitale Gesellschaft zukunftsfähig und cybersicher gestalten und damit die Cybernation Deutschland aufbauen. Hierfür braucht es alle Stakeholder und gesellschaftlichen Gruppen.

Wie viel können aber die Millionen Verbraucherinnen und Verbraucher zu dieser Gestaltungsaufgabe beitragen? Wie schaffen wir es als Gesellschaft alle Gruppen, auch die besonders vulnerablen und die nicht technologie-affinen Verbraucherinnen und Verbraucher mit ins Boot zu holen? Dies kann nur gelingen, wenn wir Technologien und besonders Sicherheitsmaßnahmen so gestalten, dass sie im Alltag für alle Gruppen gleichermaßen mit wenig Aufwand nutzbar und umsetzbar sind. Die Bedürfnisse und Bedenken von Verbraucherinnen und Verbrauchern sowie von zivilgesellschaftlichen Gruppen sind zu hören und bereits im Technologiedesign auszuräumen, um Akzeptanz für Maßnahmen der Cybersicherheit zu schaffen.

Ein solches menschzentriertes Design von Technologien und Diensten kann die Cybersicherheit stärken und ist aus unserer Sicht unentbehrlich: denn wir müssen Technologien und Dienste sicher und einfach auf die Straße bringen, damit sie tatsächlich in den Lebenswelten von Verbraucherinnen und Verbrauchern ankommen. Das neue passwortlose Authentisierungsverfahren Passkeys dient dabei als Positivbeispiel mit Potential. Es zeigt, dass Cybersicherheitsmaßnahmen die menschzentriert gestaltet wurden, nicht nur einfacher zu bedienen sind als herkömmliche Verfahren, sondern zugleich das Sicherheitsniveau deutlich anheben können.[1]

Andersherum nutzt die sicherste Technologie nichts, wenn sie – weil nicht zugänglich oder akzeptiert – in der Schublade verbleibt, während gleichzeitig eine unsichere Alternative breite Anwendung findet. Auch hierfür gibt es vielfältige Beispiele: Die sicherste Mehrfaktorauthentisierung nutzt nichts, wenn sie durch eine einfache E-Mail aus einem schlecht gesicherten Account zurückgesetzt werden kann.

Mangelnde Usable Security betrifft alle Nutzenden digitaler Technologien. Besonders deutlich zeigt sich das im Bereich der Internetsicherheit. In Deutschland nutzen laut Statistischem Bundesamt 96 % der Bevölkerung das Internet. Gleichzeitig waren allein in den letzten zwölf Monaten 61 % aller Internetnutzenden von Cyberkriminalität betroffen. Ein erheblicher Teil dieser Vorfälle, nämlich 30 %, ist dabei auf Phishing-Angriffe zurückzuführen.[2] Phishing zählt zu den am häufigsten genutzten Methoden von Cyberkriminellen.[3] Ein wesentlicher Grund für die hohe Erfolgsquote solcher Angriffe ist die fehlende Transparenz in digitalen Anwendungen und eine unzureichend nutzungsfreundliche Gestaltung.

Der Usable Security-Ansatz soll Menschen aktivieren, sodass sie ein partizipierender Teil der Sicherheitsstrategie werden. Vorsicht ist aber geboten: Menschen dürfen nicht überfordert werden. Die Last der sicheren Nutzung von Technologien und Diensten darf nicht auf ihnen abgeladen werden. Menschen nutzen Technologien, um gewisse Ziele zu erreichen. Sicherheit ist nicht ihr erstes und oberstes Interesse. Durch gestalterische Maßnahmen müssen wir es also schaffen, dass einerseits ein Basisschutz geschaffen wird, der allen Verbraucherinnen und Verbrauchern ein Mindestmaß an Cybersicherheit garantiert ohne andererseits ihre Handlungssouveränität und freie Entscheidung für Produkte und Dienste einzuschränken.

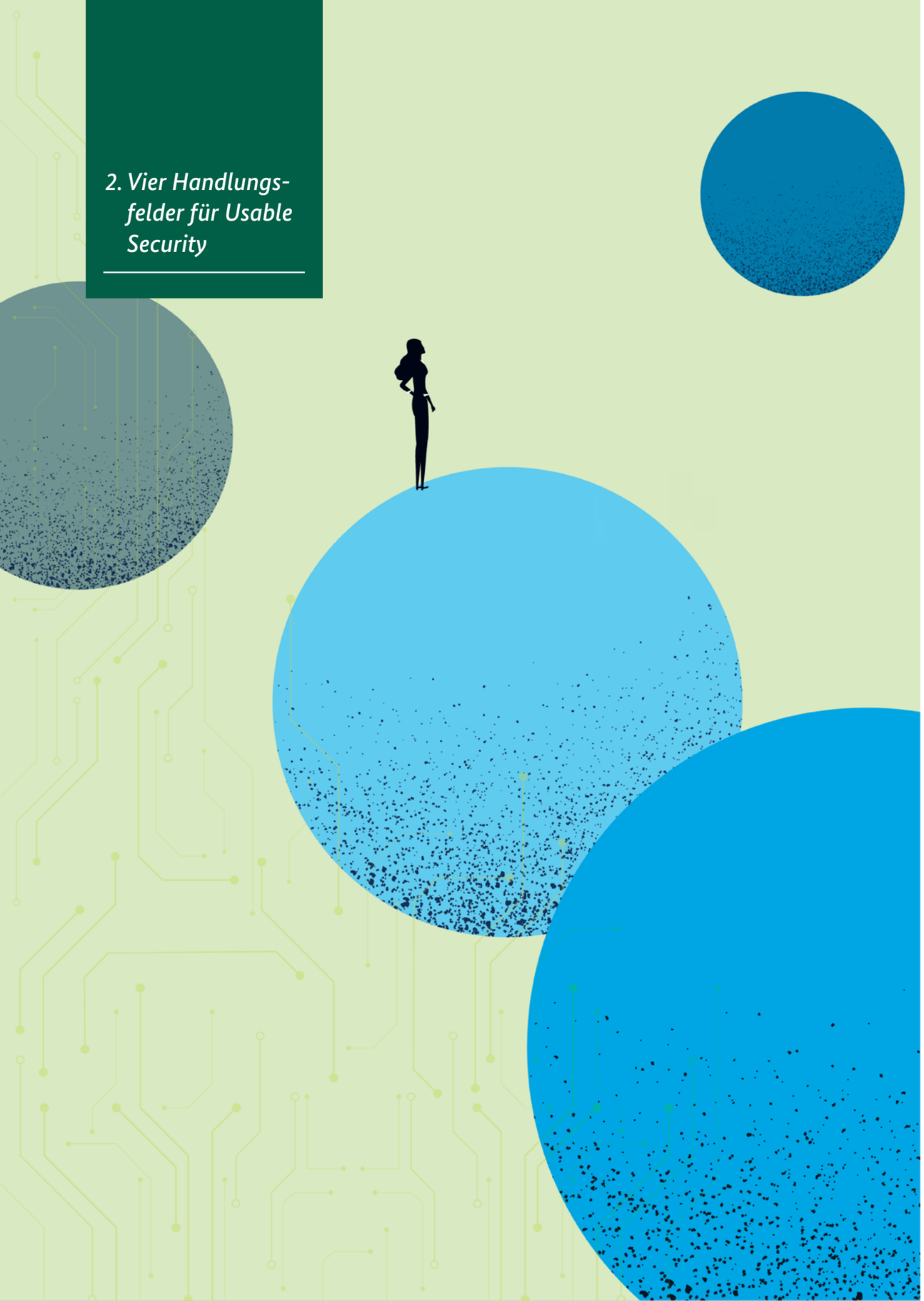
Hier fokussieren wir mit unseren Gestaltungshinweisen entsprechend insbesondere auf Anbieter und Hersteller, die dafür sorgen sollen, dass Verbraucherinnen und Verbrauchern sichere Produkte und Dienste per Design und per Default zur Verfügung gestellt werden, sodass diese im Sinne der Usable Security sicher genutzt werden können. Auch Angebote öffentlicher Stellen sollten als Vorreiter den Prinzipien der Usable Security folgen.

Für Unternehmen führt menschzentrierte Cybersicherheit nicht nur zu einer gesteigerten praktischen Sicherheit ihrer IT-Landschaften und angebotenen Produkte und Dienste. Vielmehr werden durch entsprechende Gestaltungsprozesse Risiken, Kosten und Aufwände reduziert. Ein Mangel an Usable Security birgt Risiken, die mitunter Gefahr für Leib und Leben, Bedrohungen der Hard- und Software-Sicherheit, Datenverlust und Datenschutz, erhöhte Kosten und Arbeitsaufwände, unzufriedene Mitarbeitende und mangelnde Kundenbindung betreffen können. Menschzentrierte Gestaltungs- und Entwicklungsprozesse können diesen Risiken entgegenwirken, sowie Entwicklungskosten und vor allem erhöhte Kosten nachträglicher Anpassungen erheblich senken.

Es bleibt das Problem festzustellen, welche Sicherheitsmechanismen von Nutzenden selber als alltagstauglich wahrgenommen werden. Was findet Akzeptanz, was wird als Einschränkung oder vielleicht sogar als Bevormundung empfunden? Es gibt einige bereits erprobte Methoden und Tools, um ein menschzentriertes Design zu erreichen, beispielsweise: direkte Einbindung von Nutzergruppen in die Gestaltung von Technologien oder Diensten, Nutzungstests, Nutzungsstudien und -befragungen.[4] Auch ohne die direkte Beteiligung von Nutzergruppen ist es schon hilfreich, beim Design auf interdisziplinäre Teams zu bauen und Expertinnen und Experten für User Experience einzubeziehen.

Dieses Whitepaper zeigt auf, welche Handlungsfelder sich im Bereich der Usable Security auftun und welche Stellschrauben betätigt werden können.

2. Vier Handlungsfelder für Usable Security



Usable Security ist ein etabliertes, seit mehreren Dekaden intensiv beforschtes interdisziplinäres Forschungsfeld der angewandten Informatik.[5] Zahlreiche Studien haben gezeigt, dass eine technisch durchdachte, aber gestalterisch mangelhafte bzw. nicht-menschzentrierte Umsetzung von Sicherheitsmechanismen zu unsicherem Verhalten, praktischen Sicherheitslücken und Nutzerfrustration führen. Eine menschzentrierte Gestaltung von Sicherheitsmechanismen hat hingegen in vielen Bereichen bereits Einzug in die Praxis gehalten und dabei im Ergebnis messbar zu mehr Sicherheit geführt – und das in der Regel mit, und auch gerade wegen, einer gleichzeitigen Steigerung der Nutzungszufriedenheit.

So haben beispielsweise Nutzungsstudien dazu geführt, dass Warnungen des Browsers vor unsicheren Webseiten oder Verbindungen heute für Nutzende deutlich verständlicher und im Default sicherer gestaltet sind. Oder: Nutzende moderner Messenger können heute – anders als bei E-Mail – ohne besonderes Zutun per Default Ende-zu-Ende-verschlüsselt kommunizieren.

Die zentralen Erkenntnisse aus Forschung und Praxis zu Usable Security lassen sich auf vier zentrale Handlungsfelder reduzieren:

Sicherheitsmechanismen müssen (1) praktisch und einfach *nutzbar*, (2) für alle leicht *zugänglich* und (3) in ihrer Wirkungsweise *transparent* sein, damit sie (4) von Nutzenden *akzeptiert* und sicher angewendet werden (vgl. Abbildung 1).

Für alle vier Handlungsfelder existieren konkrete Stellschrauben, mit denen sich die Gebrauchstauglichkeit, Zugänglichkeit, Transparenz und Akzeptanz von Cybersicherheitsmaßnahmen gezielt steigern lassen. Diese den vier Handlungsfeldern zugeordneten Prinzipien dienen einerseits der Gestaltung und Entwicklung neuer Sicherheitsmaßnahmen sowie andererseits der Überprüfung und Evaluation bestehender. Sie führen bei systematischer Anwendung zu einer gesteigerten praktischen Nutzbarkeit und Akzeptanz sowie ganzheitlicher Alltagstauglichkeit von Sicherheitsmechanismen.

GEBRAUCHSTAUGLICHKEIT

- Wirksamkeit / Effektivität
- Effizienz
- Robustheit gegenüber Fehlern
- Erlernbarkeit

TRANSPARENZ

- Informationspräsentation
- Selbstbeschreibungsfähigkeit
- Konsistenz / Erwartungskonformität

ZUGÄNGLICHKEIT

- Einfachheit
- Wahrnehmbarkeit
- Anpassbarkeit / Nutzungsflexibilität
- Vermeidung von Stressoren

AKZEPTANZ

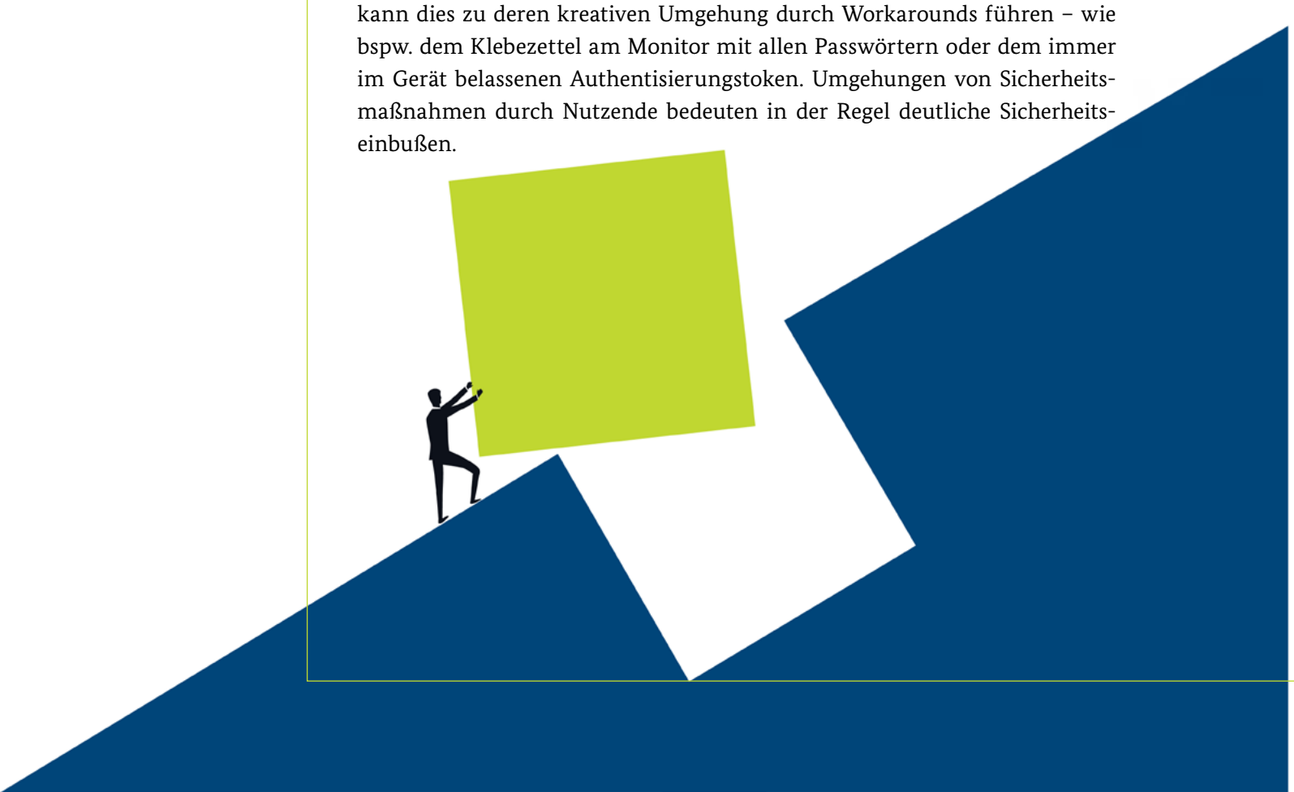
- Vertrauen
- Joy of Use / Freude
- Wahrgenommene Nützlichkeit
- Minimierung von Störungen

Abbildung 1: Vier Handlungsfelder für Usable Security

2.1 Gebrauchstauglichkeit

Die Gebrauchstauglichkeit (auch Usability oder umgangssprachlich Benutzungsfreundlichkeit) orientiert sich an den Handlungszielen, die eine Anwenderin oder ein Anwender mit der Nutzung eines Systems verfolgt. Cybersicherheitsmaßnahmen können ein solches Nutzungsziel darstellen – beispielsweise bei der Absicherung des Bankkontos vor fremdem Zugriff oder dem Einsatz einer Firewall oder einer Anti-Virus-Software. Häufig stellen IT-Sicherheitsziele jedoch Rahmenbedingungen oder untergeordnete Nutzungsziele dar und sind den primären Handlungszielen der Nutzenden nachgeordnet – wie zum Beispiel bei dem Tätigen von Online-Überweisungen. Bei der Gestaltung von Sicherheitsmaßnahmen ist daher besondere Sorgfalt zu leisten, dass diese gut in die Handlungsabläufe und in den Nutzungsalltag integriert werden können und den Anwendenden schlüssig dargeboten werden.

Ohne Zweifel mögen Sicherheitsmaßnahmen das eigentliche Handlungsziel mitunter behindern, sie können (und müssen!) jedoch oft mit Bedacht so gestaltet werden, dass eine Beeinträchtigung gering ausfällt. Usability und Cybersicherheit dürfen nicht gegeneinander ausgespielt werden. Vielmehr sollten erhöhte gestalterische Anstrengungen bei der Usability von (angemessenen) Cybersicherheitsmaßnahmen vorgenommen werden. Werden Sicherheitsmaßnahmen von Nutzenden als lästig oder unnötig wahrgenommen, kann dies zu deren kreativen Umgehung durch Workarounds führen – wie bspw. dem Klebezettel am Monitor mit allen Passwörtern oder dem immer im Gerät belassenen Authentisierungstoken. Umgehungen von Sicherheitsmaßnahmen durch Nutzende bedeuten in der Regel deutliche Sicherheitseinbußen.



Prinzipien im Handlungsfeld Gebrauchstauglichkeit

Wirksamkeit / Effektivität: Anwendende verfolgen mit der Nutzung eines Systems in der Regel ein bestimmtes Ziel – beispielsweise die Erledigung einer Aufgabe. Ein System soll Anwendende dabei unterstützen, dieses Nutzungsziel möglichst vollständig und korrekt zu erreichen. Sicherheitsmaßnahmen müssen angemessen sein und zum intendierten Effekt führen.

Kriterien: Funktionalität; Bedrohungsanalyse; Identifizierbarkeit der unterstützten Aufgaben; Standardauswahlmöglichkeiten

Beispiel: Anwendende werden durch Authentisierung am System nicht vom eigentlichen Aufgabenziel abgebracht, sondern nach erfolgreicher Anmeldung direkt zu den vorher ggf. bereits angestoßenen Aktionen zurückgeführt. Beispielsweise sollen die im Warenkorb eines Online-Shops abgelegten Produkte auch nach Anmeldung dort weiterhin gelistet sein.

Effizienz: Der bei der Nutzung einzubringende, bei Sicherheitsmaßnahmen in der Regel zusätzliche Aufwand ist – neben der Zielerreichung an sich – ein entscheidender Einflussfaktor. Der Nutzungsaufwand soll minimiert werden und verhältnismäßig sein zu den Schutzzielen einerseits und den eigentlichen Nutzungszielen andererseits.

Kriterien: Bearbeitungszeit; Aufwandsoptimierung; Ressourcenverbrauch; Finanzielle Kosten; Notwendigkeit zusätzlicher physischer Objekte

Beispiel: Eine Authentisierung mittels Fingerabdruck oder Gesichtserkennung trägt in der Regel deutlich zur Beschleunigung von Anmeldeprozessen bei.

Robustheit gegenüber Fehlern: Bei der Nutzung von Systemen treten Fehler auf: in Systemkomponenten, durch verbundene Systeme oder durch Nutzende. Auftretende Fehler müssen dabei so behandelt („gemanaged“) werden, dass einerseits die Funktionalität und Integrität des Systems gewahrt bleibt und andererseits Anwendenden ein sicheres und effizientes Nutzen des Systems (ohne Einschränkungen) möglich ist. Systeme sollen so gestaltet sein, dass sie einerseits helfen, vorhersagbare Nutzungsfehler zu vermeiden oder diese automatisch korrigieren und andererseits Nutzende bei der selbstständigen Behebung von Fehlern unterstützen.

Kriterien: Fehleranfälligkeit / Fehlertoleranz; Fehlervermeidung; Fehlerbehebung

Beispiel 1: Sinnvoll gestaltete Formulareingabefelder und Plausibilitätschecks können Nutzungsfehler verhindern.

Beispiel 2: Bei Systemen zur biometrischen Authentisierung kann eine erneute Erfassung der biometrischen Merkmale notwendig sein, wenn die Erkennungsraten des Systems abnehmen und Nutzende fälschlicherweise regelmäßig bei der Authentisierung abweisen.

Erlernbarkeit: Weist ein System eine gute Erlernbarkeit auf, kann es über die Zeit zunehmend effektiver und effizienter genutzt werden. Eine gute Erlernbarkeit schlägt sich sowohl bei der initialen Nutzung nieder, trägt aber auch bei fortwährender Nutzung positiv zur Nutzungseffizienz bei. Gerade in der Cybersicherheit unterstützt der Dreiklang aus Lernen – Üben – Routinisieren die nachhaltige Verwendung von Sicherheitsmechanismen. Insgesamt fördert eine zunehmende Vertrautheit im Umgang mit einem System auch die Nutzungszufriedenheit.

Kriterien: Assistierte Ersteinrichtung; Unterstützung beim Entdecken, Ausprobieren, Erinnern und Wiedererkennen von Bedienfunktionen; Lernen durch wiederholte Anwendung (Routinisierung); Aufrechterhaltung der Nutzbarkeit (Retention); Schulung und Dokumentation

Beispiel: Durch Sensibilisierungsmaßnahmen zu Phishing-Gefahren und dem regelmäßigen Erkennen und Löschen im E-Mail-Postfach erlernen, üben und routinisieren Nutzende den sicheren Umgang mit gefährlichen E-Mails.

2.2 Zugänglichkeit

Es gibt zahlreiche Gründe, warum Menschen keinen sicheren und verlässlichen Zugang zu digitalen Diensten und Technologien haben. Die Hürden können vielfältig sein:

- *Körperliche und kognitive Einschränkungen,* wie die der Motorik, des Seh- oder Hörvermögens, des abstrakten Denkvermögens und Komplexitätsverständnisses oder der Konzentrationsfähigkeit führen bspw. zu Schwierigkeiten bei visuellen Captchas, komplexen Passwortregeln oder auch der feinmotorischen Navigation mit Maus oder Touchscreen. Oft beeinträchtigen zudem schlecht erkennbare Merkmale der Finger oder bei Brillenträgern biometrische Authentisierungsverfahren.

- *Finanzielle, soziale oder geographische Einschränkungen* kommen zum Tragen, wenn bspw. notwendige Geräte oder Dienste Nutzenden nicht oder nur zeitweise zur Verfügung stehen, sich Nutzende diese mit anderen Personen im Haushalt oder an öffentlichen Orten wie Bibliotheken teilen oder sie keinen uneingeschränkten Zugang zum Internet haben.

- *(Sozio-)Emotionale Einschränkungen* ausgelöst durch bspw. Sorgen, Stress, Angst oder Hilflosigkeit können den Aufbau oder die Anwendung von digitalen Kompetenzen beeinträchtigen. Ein mangelndes Selbstvertrauen in Bezug auf die eigenen digitalen Kompetenzen kann bspw. zu einer verminderten Fähigkeit führen, potentielle Cyberangriffe wie Viren und Phishing-Versuche zu erkennen und erfolgreich abzuwehren.

Individuelle Einschränkungen dürfen jedoch nicht dazu führen, dass der Zugang zu Werkzeugen und Hilfsmitteln, die für den Schutz vor Cyberbedrohungen erforderlich sind, ebenfalls eingeschränkt ist. Zugängliche und barrierefreie Cybersicherheit bedeutet also, Sicherheitsmechanismen so zu konzipieren und umzusetzen, dass sie von Menschen mit unterschiedlichsten Bedürfnissen, Fähigkeiten und Ressourcen gleichermaßen genutzt werden können.

Zugänglichkeit muss daher bedeuten, allen Personen der Gesellschaft Zugang zu digitalen Angeboten zu verschaffen, aber auch sicherzustellen, dass diese ohne Angst vor digitalen Bedrohungen und Angriffen genutzt werden können.

Prinzipien im Handlungsfeld Zugänglichkeit

Einfachheit: Die Nutzung eines Systems oder eines Sicherheitsmechanismus soll möglichst wenig zusätzliche mentale, kognitive und motorische Beanspruchung hervorrufen – insbes. über die Erfüllung der eigentlichen Nutzungsziele hinaus – und insgesamt möglichst wenige Interaktionsschritte erfordern.

Kriterien: Kognitive Beanspruchung; Mentale Beanspruchung; Motorische Beanspruchung; Geforderte Interaktionen

Beispiel: Statt komplexen Passwortregeln (mit Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen) wird eine Passphrase oder die Methode Three-Random-Words („hausofenbett“) als Vorgabe für sichere Passwörter verwendet.

Wahrnehmbarkeit: Bereitgestellte Informationen sowie Bedienelemente des Systems sollen z. B. über Darstellungs- und Medienalternativen für verschiedene Wahrnehmungsformen verfügbar sein. Dazu gehören bspw. Optionen für einfache Sprache, vereinfachtes Layout, kontrastreiche Farben und unterschiedliche Schriftgrößen ebenso wie Alternativ-Texte für Bilder und Videos sowie Vorleseoptionen. Die Web Content Accessibility Guidelines (WCAG)[6] geben hier bspw. Leitlinien für Webanwendungen vor. Des Weiteren soll eine Kompatibilität mit assistiven Technologien wie Screenreadern hergestellt werden.

Kriterien: Darstellungsalternativen; Medienalternativen; Unterscheidbarkeit; Kompatibilität mit assistiven Technologien

Beispiel 1: Warnmeldungen wie bspw. Sicherheitswarnungen werden multimedial ausgegeben – z. B. mit Warnton, Warnsymbol, Warnfarbe und Warntext.

Beispiel 2: Als Captcha wird neben einem bildbasierten Rätsel auch ein akustisches Captcha angeboten.

Anpassbarkeit und Nutzungsflexibilität: Vor dem Hintergrund unterschiedlicher Nutzungserfahrungen, digitaler Kompetenzen sowie sozialer und kultureller Hintergründe soll das System an die Bedürfnisse der Nutzenden individuell anpassbar sein. Des Weiteren sollen die Nutzungsmöglichkeiten und möglichen Einsatzzwecke des Systems insofern flexibel sein, als dass es für verschiedene Nutzungsszenarien und in verschiedenen Nutzungskontexten verwendet werden kann. Die unterschiedlichen Kontexte, in denen Nutzende Sicherheitsentscheidungen treffen, müssen berücksichtigt werden.

Kriterien: Allgemeingültigkeit; Steuerbarkeit; Leistungsfähigkeit; Technologiealternativen; Soziale Einbettung; Kompatibilität und Interoperabilität; Skalierbarkeit

Beispiel: Bei der Authentifizierung kann man zwischen verschiedenen Verfahren wählen: z. B. Passkeys oder 2-Faktor-Authentisierung; Fingerabdruck, Gesichtserkennung, PIN oder Entsperrmuster.

Vermeidung von Stressoren: Wenn sich Nutzende unter Druck gesetzt fühlen, kann dies dazu führen, dass ungeeignete Bewältigungsstrategien angewendet oder Sicherheitsmaßnahmen umgangen werden. Das System oder der Sicherheitsmechanismus soll daher möglichst vermeiden, dass unnötige Stressoren wie Zeitdruck, Handlungs- oder Entscheidungserfordernisse, finanzielle Belastung, emotionaler oder sozialer Druck auf die Nutzenden bei oder durch die Verwendung des Systems entstehen.

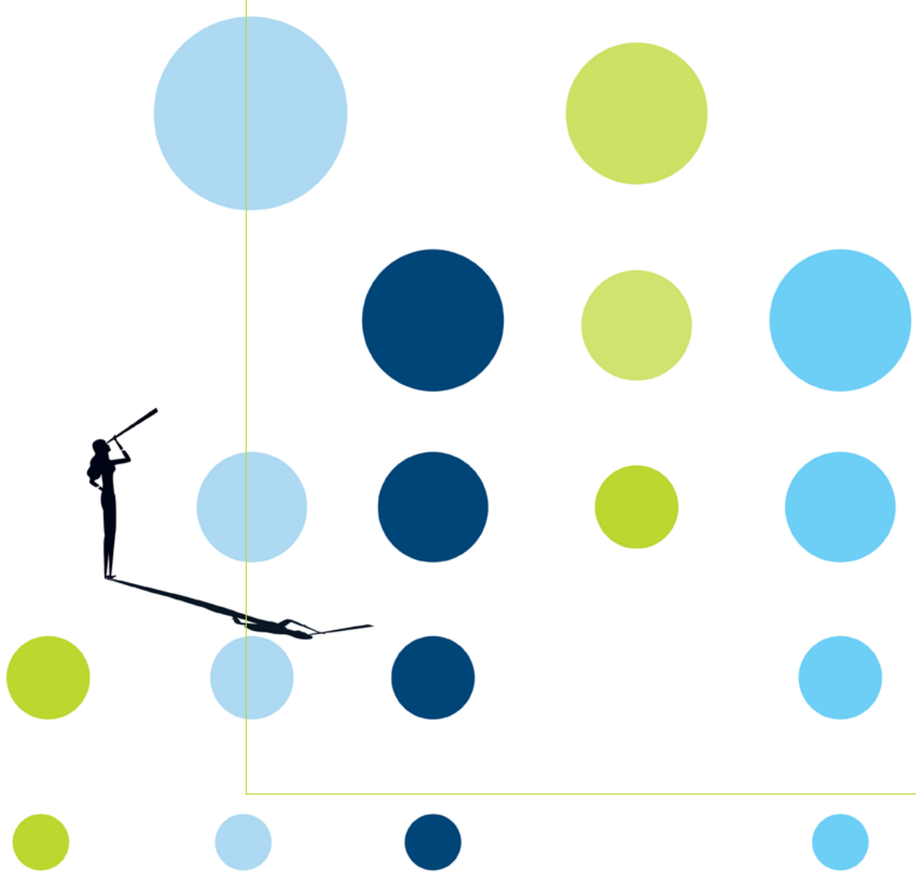
Kriterien: Zeit- bzw. Handlungsdruck; Entscheidungsdruck; Finanzielle Belastung; Emotionaler Druck

Beispiel: Wenn Passwörter im Beisein Dritter eingeben werden müssen (wie z. B. beim Fernsehabend mit Freunden via Bildschirmtastatur), kann dies zu Stress und zur unbeabsichtigter Passwortpreisgabe führen. Automatisierte Authentisierungsverfahren wie Passkeys oder Biometrie umgehen solche Stressoren häufig.

2.3 Transparenz

Die Transparenz des Systems oder der Sicherheitsmaßnahmen ist für Nutzende wesentlich, um einerseits zu verstehen, warum sie bestimmte Maßnahmen anwenden sollen (also deren Notwendigkeit verstehen und akzeptieren), aber auch wie sie funktionieren, was sie bewirken und wie sie demnach anzuwenden sind. Durch Transparenz kann also nicht nur Vertrauen in Anbieter, System und Sicherheitsmechanismus gesteigert werden. Transparenz ist auch notwendig, um die vom System erwarteten Handlungen umsetzen zu können. Sie erlaubt so den Nutzenden einen souveränen und selbstbestimmten Umgang mit dem System und den Sicherheitsmechanismen. Transparenz ist damit eine weitere zentrale Voraussetzung für ein sicheres Verhalten der Nutzenden in der Praxis.

Die Art und Weise der Informationsvermittlung muss dabei an die Nutzenden, an ihre Denkweisen, Mentalen Modelle und Kompetenzen angepasst und ggf. gestuft gestaltet werden.



Prinzipien im Handlungsfeld Transparenz

Informationspräsentation: Die im System angebotenen Informationen zum System und dessen Nutzung sowie die Daten und Informationen zur Aufgabenerledigung sollen so dargestellt werden, dass Nutzende daraus ein Verständnis entwickeln können, was das System leistet, wie es die Daten verarbeitet und wie es Anwendende demzufolge für ihre Ziele nutzen können. Hierzu gehören verständliche, vollständige, gut strukturierte und leicht auffindbare Informationen, die neben Nutzungshinweisen auch Risiken und Gefahren von Systemfunktionen darlegen. Ein System, welches sich den Nutzenden als „black box“ darstellt, kann schnell zu Unverständnis oder Überforderung und damit zu einer geringen Nutzungsakzeptanz führen.

Kriterien: Verständlichkeit; Vollständigkeit; Risiken & Vorteile; Auffindbarkeit / Navigierbarkeit; Inhaltsbezogenheit

Beispiel: Moderne Messenger und Browser zeigen an, wenn verschlüsselt kommuniziert wird und warnen, wenn die Kommunikation unverschlüsselt ist.

Selbstbeschreibungsfähigkeit: Der aktuelle Systemzustand sowie die möglichen Bedienschritte und Aktionen sollen für Nutzende klar erkennbar sein. Das System soll Orientierungspunkte anbieten, damit jederzeit ersichtlich ist, wo man sich im Prozess oder im System befindet und welche Aktionen durch welche Bedienelemente ausgelöst werden. Außerdem soll das System adäquate Rückmeldungen, ggf. Hinweise oder Warnungen geben sowie Hilfen und Dokumentation anbieten.

Kriterien: Orientierung; Beherrschbarkeit; Systemstatus; Rückmeldung und Warnung; Hilfen

Beispiel: Der Status laufender Hintergrundprozesse wie Updates oder Backups wird vom System angezeigt. Der Nutzende wird über das Ergebnis benachrichtigt (Fehler oder Erfolg).

Konsistenz / Erwartungskonformität: Das System soll für Nutzende in Darstellung und Verhalten vorhersagbar und konsistent sein. Die Konsistenz soll sowohl innerhalb des Systems sowie im Vergleich zu anderen (verbreiteten) Systemen gegeben sein. Sie soll auch durch die Einhaltung etablierter Normen und Konventionen erreicht werden. Das System soll so den Erwartungen und Erfahrungen der Nutzenden entsprechen. Ein System oder ein Sicherheitsmechanismus, der sich in vielen Belangen von bisher erlernten Gewohnheiten und gemachten Erfahrungen unterscheidet wird abgelehnt. Neue Interaktionsmuster (Innovationen, Alleinstellungsmerkmale) müssen von Nutzenden hingegen erst erlernt werden (vgl. Erlernbarkeit).

Kriterien: Systemverhalten; Einheitliche Darstellung; Vertrautheit; Konformität

Beispiel 1: Bei den meisten Diensten kann man sein Passwort mittels „Passwort vergessen?“ über eine E-Mail an das persönliche Postfach zurücksetzen. Der Prozess ist für Nutzende dabei häufig sehr ähnlich.

Beispiel 2: Passkeys als neues passwortloses Anmeldeverfahren bricht mit den Erfahrungen der Nutzenden (der Eingabe von Benutzername und Passwort) und daraus abgeleitet ihren Erwartungen an „sichere“ Authentisierung. Obwohl das neue Verfahren einfacher ist und schneller geht als die Anmeldung mit Benutzername und Passwort erfordert dessen Einführung daher erhöhte Anstrengungen auf Seiten der Anbieter.

2.4 Akzeptanz

Die Akzeptanz ist ein wesentlicher Erfolgsfaktor für Sicherheitsmaßnahmen. Projekte scheitern viel zu häufig daran, dass Sicherheitsmaßnahmen von Nutzenden nicht eingesetzt oder adäquat umgesetzt werden, selbst wenn sie noch so gut gestaltet sind und eine hohe Wirksamkeit entfalten. Die vermeintlich weichen Akzeptanzkriterien können dann zu harten Fakten werden und gar zur Ablehnung führen. Umgekehrt kann man feststellen, dass Verbraucherinnen und Verbraucher (manchmal auch weniger wirksame) Sicherheitsmechanismen nutzen, weil sie diesen (scheinbar blind) vertrauen, Freude bei der Nutzung empfinden oder mit diesen ihre Ziele schneller und besser erreichen können.

Verbesserungen in den Handlungsfeldern Gebrauchstauglichkeit, Zugänglichkeit und Transparenz sind die Grundlage, um Akzeptanz bei Nutzenden zu erhöhen, jedoch sind diese allein keine Garantie dafür. Im Handlungsfeld Akzeptanz müssen weitere wesentliche Stellschrauben angepackt werden, um guten Sicherheitsmechanismen letztlich zum Erfolg zu verhelfen.

Prinzipien im Handlungsfeld Akzeptanz

Vertrauen: Akzeptanz kann entstehen, wenn Nutzende dem System sowie dem Anbieter vertrauen, sie sich freiwillig für oder gegen die Nutzung entscheiden können und sich sicher (d.h. geschützt vor Risiken) im Umgang mit dem System fühlen. Vertrauensbildend kann dabei auch die Art und Weise der Einführung, Heranführung und Begleitung eines (neuen) Systems sein (z. B. durch Nutzungsstudien, Nutzendenbeteiligung und technischem Support). Dabei können Partnerorganisationen aus dem Kreis der Nutzenden als Vertrauensanker fungieren.

Kriterien: Empfundene Freiheit von Risiken; Freiwilligkeit der Nutzung; Awareness und Sensibilisierung; Einbeziehung der Nutzenden; Partnerorganisationen als Vertrauensanker; Ethische Aspekte

Beispiel: Eine vertrauenswürdige Stelle, wie bspw. das BSI, empfiehlt den Einsatz eines bestimmten Authentisierungsverfahrens. Das IT-Sicherheitskennzeichen des BSI zeigt Konsumenten auf einen Blick, dass ein digitales Produkt bestimmte Sicherheitsanforderungen erfüllt.

Joy of Use / Freude: Freude bei der Nutzung und andere positive Nutzungserlebnisse unterstützen die Akzeptanz eines Systems oder einer Sicherheitsmaßnahme. Positive Nutzungserlebnisse können z. B. durch die Erfüllung persönlicher Bedürfnisse, der Identifikation mit dem System, durch Motivation und Stimulation oder durch hohen Nutzungskomfort hervorgerufen werden.

Kriterien: Attraktivität des Systems; Individualisierbarkeit; Motivation und Stimulation; Identifikation mit dem System; Bequemlichkeit und Komfort

Beispiel: Das Smartphone gibt bei Authentisierung mittels Fingerabdruck dynamische und visuell ansprechend gestaltete Rückmeldungen. Diese vermitteln nicht nur besser die Funktionsweise biometrischer Authentisierung (bspw. bei der Registrierung neuer Merkmale), sondern sie wirken auch spielerisch.

Wahrgenommene Nützlichkeit und Minimierung von Störungen: Die wahrgenommene Nützlichkeit beschreibt wie zufrieden Nutzende mit der wahrgenommenen Erreichung ihrer pragmatischen Ziele und des dafür eingebrachten Aufwands sind. Dazu zählt auch eine subjektive Bewertung der Ergebnisse und Konsequenzen der Nutzung und inwieweit bspw. eine Sicherheitsmaßnahme als Beeinträchtigung der eigentlichen Aufgabenerledigung wahrgenommen wird.

Kriterien: Aufgabenrelevanz; Workflow-Integration; Re-Authentifikation

Beispiel: Eine umständliche Re-Authentisierung von häufig verwendeten Systemen mit subjektiv begrenztem Nutzen für die eigene Zielerfüllung (bspw. rein administrative Systeme) wird als störend empfunden.

3. Fazit und Ausblick

Die Notwendigkeit menschzentrierter Gestaltung von Sicherheitsmaßnahmen scheint auf der Hand zu liegen: Technologien und Sicherheitsmaßnahmen sollen **in die praktische Anwendung** kommen und dafür müssen sie einfach nutzbar gestaltet werden. Nur so können wir allen Menschen der Cybernation einen sicheren, einfachen und selbstbestimmten Zugang zu den Chancen und Vorteilen der Digitalisierung gewähren. Die Frage ist also nicht das ob, sondern das wie.

IT-Dienstleister sowie Hersteller und Anbieter digitaler Produkte sind in der Pflicht, menschzentriertes Design von Beginn an umzusetzen. Hier unterstützt der vorgestellte Handlungsrahmen mit entsprechenden Kriterien und Empfehlungen. Um für alle Akteure eine gute Grundlage zu bilden, eruiert das BSI derzeit die Möglichkeiten der Standardisierung der Anforderungen an Usable Security – nach Möglichkeit erstellt im Konsensverfahren und zeitnah verfügbar für einen internationalen Anwenderkreis.

Die Forderung nach menschzentriertem Design hat bereits Einzug gehalten in wesentliche Positionspapiere.[7] Besonders im Bereich der Regulierung muss aber noch nachgeschärft werden. Menschzentriertes Design muss eine **Standardanforderung der Regulierungen zur Cybersicherheit** werden – hierfür muss der Gesetzgeber sorgen. Cybersicherheit muss Anforderungen an die Anwendbarkeit im Alltag immer inkludieren.

Der Cyber Resilience Act[8] beispielsweise wird in naher Zukunft Märkte für vernetzte Produkte bzw. Produkte mit digitalen Elementen regulieren. Im Text der Regulierung wird das menschzentrierte Design nur an wenigen Stellen – zumeist lediglich in Bezug auf die Transparenz – genannt. Hier ist eine Lücke entstanden, die durch die **Gestaltung der horizontalen und vertikalen Normung** geschlossen werden kann. Beispielsweise bei produktspezifischen Normen zu smartem Spielzeug oder bei Wearables muss darauf geachtet werden, dass Anforderungen an die Sicherheit der Funktionalität und der einfachen Anwendung sich einander nicht entgegenstehen.

Ein weiterer Weg, um langfristig nutzungsfreundliche Märkte zu gestalten, ist es, die Aspekte und Kriterien der Usable Security in **Beschaffungs- und Vergabeprozessen** zu berücksichtigen. In der Regel ist die Barrierefreiheit bereits als Anforderung in solchen Prozessen gesetzt. Hier muss noch mehr geschehen. Das menschzentrierte Design nach im Konsens aufgestellten Kriterien sollte bei allen Designprozessen zu einem wesentlichen Bestandteil werden. Die öffentliche Hand muss hier als Vorbild voran gehen. Das fehlende Akzeptanz zum Scheitern von Technologieprojekten führen kann, wird uns immer wieder eindrücklich an großen und kleinen Projekten vor Augen geführt. Notwendig ist daher eine Berücksichtigung von menschzentrierten Erfolgskriterien von Beginn an, also per Design – damit sich Usable Security letztlich in Produkten und Diensten am Cybermarkt Deutschland stärker niederschlägt.

Zivilgesellschaftliche Akteure können die Rechte von Verbraucherinnen und Verbrauchern stärken, indem sie die Forderung nach menschzentrierter Gestaltung unterstützen und an Politik und Wirtschaft herantragen.

Alle Akteure sind eingeladen, sich im Dialog zur Weiterentwicklung dieses wichtigen Themenfeldes zu beteiligen.

4. Referenzen

[1] Bundesamt für Sicherheit in der Informationstechnik (BSI). Schafft die Passwörter ab?! – Anmelden ohne Passwort mit Passkey. https://www.bsi.bund.de/dok/1107470

zurück zum Text, Seite 6

[2] bitkom (2025). Cybercrime-Bilanz: 6 von 10 Internetnutzern sind betroffen. https://www.bitkom.org/Presse/Presseinformation/Cybercrime-Bilanz-6-von-10-Internetnutzern-betroffen

zurück zum Text, Seite 6

[3] Bundeskriminalamt (2025). Bundeslagebild Cybercrime 2024. https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/Lagebilder/Cybercrime/2024/CC_2024.html?nn=28110

zurück zum Text, Seite 6

[4] Arbeitskreis „Usable Security & Privacy“ der German UPA (2019). Usable Security & Privacy: Nutzerzentrierter Schutz sensibler Daten. https://germanupa.de/arbeitskreise/arbeitskreis-usable-security-privacy/fachschrift

zurück zum Text, Seite 7

[5] Siehe bspw. Garfinkel, S. & Lipford, H.R. (2014). Usable Security – History, Themes, and Challenges. Morgan & Claypool. http://dx.doi.org/10.2200/S00594ED-1V01Y201408SPT011

zurück zum Text, Seite 9

[6] Web Content Accessibility Guidelines (WCAG) 2.2 (2024). W3C Recommendation. Abrufbar unter: https://www.w3.org/TR/WCAG22/ (Deutsche Übersetzung der Vorversion (2.1) abrufbar unter: https://outline-rocks.github.io/wcag/translations/WCAG21-de/

zurück zum Text, Seite 13

[7] TeleTrust (2025). Positionspapier Cyber-Nation V 2.0. https://www.teletrust.de/publikationen/broschueren/cyber-nation/

zurück zum Text, Seite 18

[8] Bundesamt für Sicherheit in der Informationstechnik (BSI). Cyber Resilience Act – Cybersicherheit EU-weit gedacht. https://www.bsi.bund.de/dok/cra

zurück zum Text, Seite 18

Abruf der verzeichneten URLs am 15. Juli 2025.

www.bsi.bund.de