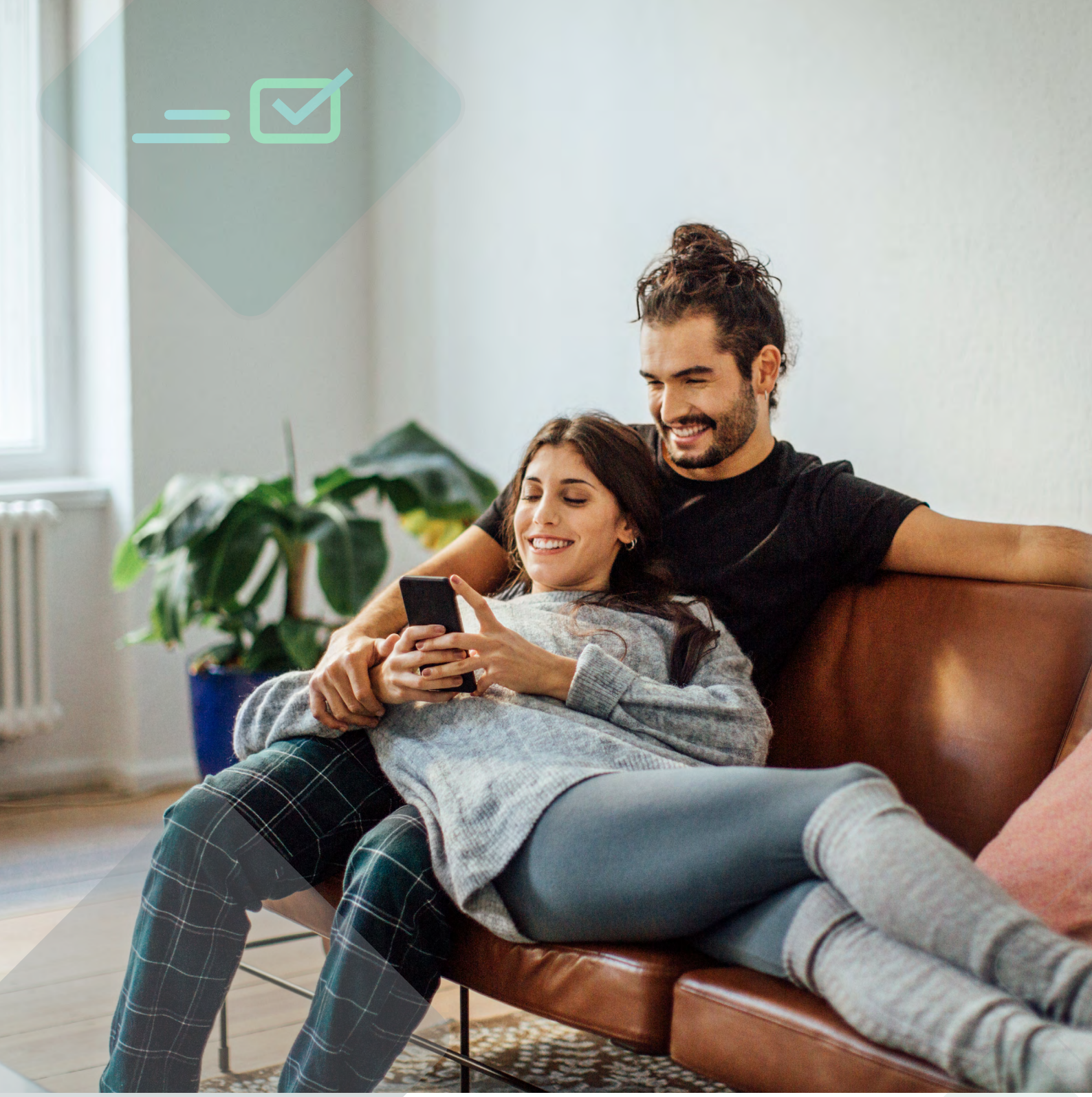
WHITEPAPER #04

Anforderungen an sichere, transparente und benutzerfreundliche Webmail-Dienste

DIGITALER VERBRAUCHERSCHUTZ

Bundesamt
für Sicherheit in der
Informationstechnik

Deine E-Mails,
dein digitales Zuhause.



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: Oktober 2025

Bildnachweise: Titel: GettyImages©Intellson; Seite 2: GettyImages©Luis Alvarez; Seite 3: GettyImages©Intellson; Seite 6: GettyImages©Westend61; Seite: GettyImages©Willie_B.Thomas; Seite 11: GettyImages©Jordi Mora igual; Seite 12: GettyImages©Hinterhaus Productions; Seite 16: GettyImages©Intellson

Inhaltsverzeichnis

Management Summary

E-Mail-Dienste sind ein zentraler Baustein digitaler Kommunikation und Identitätsverwaltung. Doch der Schutz der Verbraucherinnen und Verbraucher vor Sicherheitsrisiken wie Phishing und Identitätsdiebstahl ist bei Webmail-Anbietern teilweise noch lückenhaft umgesetzt. Zudem ist die einfache Anwendung einer Ende-zu-Ende-Verschlüsselung (E2EE) aus dem Webmailer heraus und anbieterübergreifend meist nicht möglich.

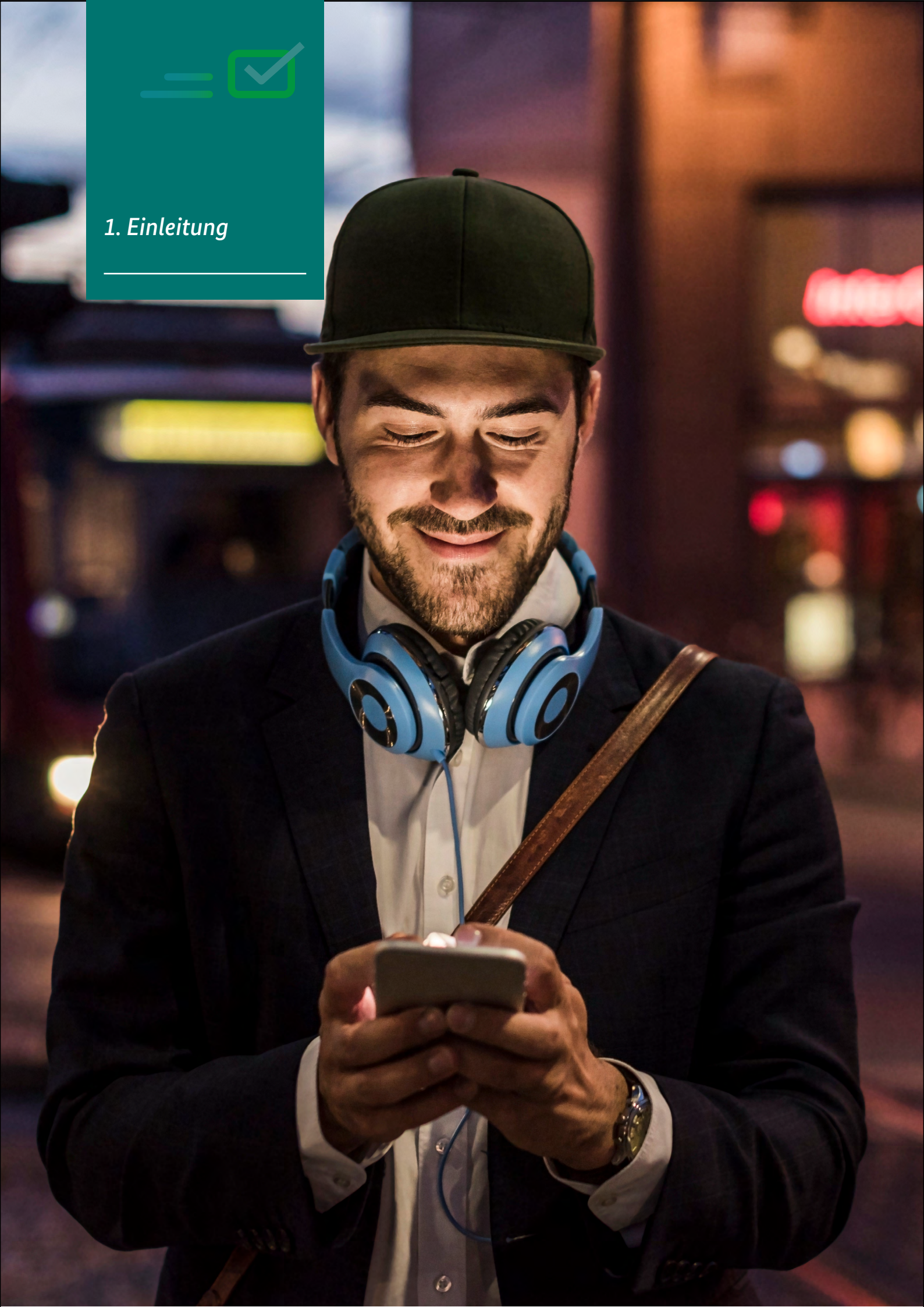
Das vorliegende Whitepaper identifiziert fünf zentrale Handlungsfelder, um den digitalen Verbraucherschutz in diesem Bereich zu stärken – mit besonderem Fokus auf IT-Sicherheit, Transparenz und Usability.

Die zentralen Handlungsfelder lauten:

1. Sichere und benutzerfreundliche Authentifizierungsverfahren – z. B. Zwei-Faktor-Authentisierung und/oder Passskeys als Standard, sichere Passwortregeln nach Stand der Technik, optionale Identitätsverifikation.
2. Einfach nutzbare Ende-zu-Ende-Verschlüsselung – auf Basis offener Standards (OpenPGP, S/MIME), mit automatisierter Schlüsselverwaltung und interoperabler Schlüsselveröffentlichung (z. B. „Web Key Directory“).
3. Effektiver Schutz vor Spam und Phishing – Ergänzung technischer Verfahren im Backend durch konkrete Maßnahmen an der Benutzerschnittstelle (Spam-Melden-Funktion, Melden von False-Positives).
4. Verlässliche Möglichkeiten zur Accountwiederherstellung – insbesondere bei kompromittierten Konten, mit niedrigschwelliger Kommunikation und optionaler Authentifizierung zur Wiederherstellung der Inhaberschaft.
5. Verständliche Sicherheitsprofile und Vertrauensmodelle – Sicherheitsmaßnahmen müssen nachvollziehbar und auffindbar sein, Anbieter sollten Selbstauskünfte zur Sicherheitsarchitektur bereitstellen.

Auf dieser Basis formuliert das Whitepaper konkrete Forderungen an Anbieter von Webmail-Diensten. Nicht zuletzt richtet sich dieses Whitepaper auch an Politik und Zivilgesellschaft, um durch einen gesellschaftlichen Diskurs einen Beitrag zur Stärkung der digitalen Souveränität der Verbraucherinnen und Verbraucher zu leisten.

1. Einleitung



Digitale Kommunikation ist heute ein integraler Bestandteil des Alltagslebens. E-Mail-Dienste – insbesondere browserbasierte Webmailer[1] (Webmail-Dienste, die über einen Webbrowser genutzt werden) – spielen dabei immer noch eine zentrale Rolle. Laut der ARD/ZDF-Medienstudie 2024 nutzen 75 % der Internetnutzerinnen und Nutzer in Deutschland regelmäßig E-Mails, womit die E-Mail immer noch zu den meistgenutzten digitalen Kommunikationskanälen zählt **[1]**. Weltweit werden täglich rund 360 Milliarden E-Mails versendet – Tendenz steigend **[2]**. Ein großer Anteil davon wird über Webmailer abgewickelt. Zunehmende Relevanz gewinnen auch die Apps der Webmail-Anbieter zur Nutzung von E-Mail auf dem Smartphone.

E-Mails dienen nicht nur der privaten und beruflichen Kommunikation, sondern sind oft auch die Schlüsselkomponente zur Verwaltung digitaler Identitäten und zur Wiederherstellung von Accounts. Angesichts dieser zentralen Funktionen und der hohen Verbreitung in der Bevölkerung ist es von erheblicher Bedeutung, dass Webmail-Dienste verlässlich, sicher und nutzerfreundlich gestaltet sind. Verbraucherinnen und Verbraucher müssen sich darauf verlassen können, dass ihre Daten vor unbefugtem Zugriff geschützt, die Identität ihrer Kommunikationspartner überprüfbar und ihre Konten gegen Missbrauch abgesichert sind.

Das vorliegende Whitepaper richtet sich an Anbieter von Webmail-Diensten und formuliert Anforderungen, um die Sicherheit der Verbraucherinnen und Verbraucher in diesem Bereich systematisch und zukunftsorientiert zu erhöhen. Dabei werden nicht nur technische Sicherheitsfunktionen betrachtet, sondern auch Aspekte wie Usability, Transparenz und Vertrauen als wesentliche Bestandteile digitaler Souveränität.

Für eine erfolgreiche Anwendung in der Praxis sind die folgenden Prinzipien unerlässlich:

- Security by Design – Sicherheit wird von Beginn an in die Architektur eines Dienstes integriert, nicht nachträglich ergänzt.
- Security by Default – sichere Voreinstellungen sind Standard, nicht optional.
- Usable Security – Sicherheitsfunktionen müssen für alle Verbraucherinnen und Verbraucher einfach verständlich und handhabbar sein, sonst verlieren sie ihre Wirksamkeit.

Im Fokus dieses Whitepapers stehen fünf zentrale Handlungsfelder, die sich unmittelbar auf die Nutzererfahrung und den Schutz vor digitalen Bedrohungen auswirken:

1. Sichere und benutzerfreundliche Authentifizierungsverfahren
2. Interoperable und einfach nutzbare Ende-zu-Ende-Verschlüsselung
3. Effektive Mechanismen zum Schutz vor Spam und Phishing
4. Niedrigschwellige und gleichzeitig sichere Wege zur Accountwiederherstellung
5. Transparente Sicherheitsprofile und nachvollziehbare Vertrauensmodelle

Aus diesen Handlungsfeldern werden konkrete Forderungen an Anbieter von Webmail-Diensten abgeleitet, um die Sicherheit und Nutzbarkeit ihrer Dienste im Sinne des digitalen Verbraucherschutzes zu verbessern.

Das Whitepaper versteht sich als Beitrag zur aktuellen Debatte um die Rolle von Plattformen und digitaler Souveränität in der Gesellschaft. Es bietet Orientierung für Anbieter, Politik und Fachöffentlichkeit – und möchte zugleich zur weiteren Standardisierung und Verbreitung guter Sicherheitspraktiken animieren.

1 | Dieses Whitepaper betrachtet primär die Benutzerschnittstellen von E-Mail-Diensten. Mit „Webmailer“ ist der Zugriff auf E-Mails über den Browser gemeint. Die Aussagen gelten sinngemäß auch für mobile Apps. Zudem werden Aspekte der Gesamtarchitektur des E-Mail-Dienstes berücksichtigt.

2. Einfache und sichere Authentisierungs-verfahren

Ein wirksamer Verbraucherschutz bei E-Mail-Diensten beginnt mit einer sicheren und gleichzeitig einfach handhabbaren Authentisierung. Der Zugriffsschutz auf das E-Mail-Konto bildet die erste und gleichzeitig wichtigste Verteidigungslinie gegen unbefugte Zugriffe und Missbrauch. Gerade weil E-Mail-Adressen zentrale Schaltstellen der digitalen Identität sind – etwa zur Wiederherstellung anderer Online-Konten – ist ein wirksamer Authentisierungsmechanismus von besonderer Bedeutung.

Trotzdem basiert der Zugang zu vielen E-Mail-Diensten nach wie vor auf Passwörtern, oft ohne weitere Schutzmaßnahmen. Zwei-Faktor-Authentisierung (2FA) wird zwar zunehmend angeboten, ist aber häufig optional und der Prozess zur Einrichtung oft aufwändig. Der aktuelle Cybersicherheitsmonitor legt offen, dass 2FA bei den Internetnutzern generell wenig genutzt wird. Lediglich 34 % der Befragten gaben an, 2FA zu nutzen – Tendenz sinkend [3]. Hier gilt es anzusetzen, um auch im Bereich von Webmailern einfache und sichere Möglichkeiten der 2FA zu implementieren.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat die gängigsten Verfahren der 2FA u. a. hinsichtlich Usable Security und IT-Sicherheit verglichen und die Ergebnisse veröffentlicht [4]. Eine besondere Rolle spielen dabei biometrische Verfahren, welche dafür gesondert betrachtet wurden. Werden Mindestanforderungen u. a. zu einer sicheren Speicherung und Verarbeitung biometrischer Daten sowie einer angemessenen Erkennungsgenauigkeit und Fälschungssicherheit erfüllt, dann bieten biometrische Verfahren für Verbraucherinnen und Verbraucher einen einfachen und sicheren Weg einen E-Mail-Account mittels eines zweiten Faktors abzusichern [5].

Verfahren zur passwortlosen Authentisierung über Passkeys (FIDO2/WebAuthn) sind aktuell noch nicht weit verbreitet, obwohl diese aus Verbrauchersicht sehr einfach anzuwenden sind und gleichzeitig eine hohe Sicherheit mit sich bringen. Eine Verbraucherbefragung des BSI zu Passkeys zeigt, dass Nutzende das Passkey-Verfahren insgesamt sehr positiv bewerten. Insbesondere die unkomplizierte Einrichtung, die schnelle Anmeldung und die hohe Nutzungsfreundlichkeit werden hervorgehoben [6].

Um dem Schutzbedarf gerecht zu werden, sollten Anbieter mehrstufige Authentisierungsverfahren standardmäßig implementieren und aktiv anbieten. 2FA sollte dabei nicht nur als Option im Einstellungsmenü versteckt sein, sondern – im Sinne von Security by Default – standardmäßig aktiviert werden. Dies könnte durch eine automatische Aufforderung zur Aktivierung bei der ersten Anmeldung umgesetzt werden (Opt-out-Mechanismus).

Auch sollten Anbieter bei der initialen Passwortvergabe durch die Nutzerinnen und Nutzer eine entsprechende Passwort-Policy umsetzen. Dabei können Mindestanforderungen für die Erstellung sicherer Passwörter aus dem BSI-Faktenblatt zu sicheren Passwörtern abgeleitet werden [7]. Anbieter sollten zudem eine Prüfung der Passwortstärke bereits bei der Eingabe vornehmen und technische Maßnahmen wie Ratenbegrenzung und IP-Blocking anwenden.

Ein weiterer Ansatz zur Stärkung der Kontensicherheit könnte in der Einführung eines optional nutzbaren Identitätsnachweises bei der Registrierung liegen. Ein solches Verfahren – etwa über ein Postident-Verfahren oder eine eID-Schnittstelle – würde es ermöglichen, die Authentizität des Accountinhabers dauerhaft abzusichern. Im Falle eines späteren Wiederherstellungsbedarfs (z. B. nach Accountübernahme durch Dritte) ließe sich so verlässlich nachweisen, dass der oder die Betroffene tatsächlich die Kontrolle über den Account zurückerhalten sollte. Dies würde nicht nur die Sicherheit erhöhen, sondern auch die Möglichkeiten der Accountwiederherstellung deutlich verbessern. Dieser Service hätte zudem unmittelbare Auswirkungen auf die Authentizität der Nutzer. Ein auf diese Weise registrierter Account könnte für alle Kommunikationspartner als solcher kenntlich gemacht werden. Es wird an dieser Stelle ausdrücklich noch einmal darauf hingewiesen, dass es sich bei diesem Vorschlag um einen freiwilligen Service des Dienstes für seine Nutzerinnen und Nutzer handelt. Die Möglichkeit einen pseudonymen Account zu eröffnen, soll dadurch nicht eingeschränkt werden. Dies sollte weiterhin möglich sein.

Um die Benutzerfreundlichkeit zu gewährleisten, ist die Umsetzung von Usable Security zentral: Die Einrichtung sicherer Verfahren muss niederschwellig, selbsterklärend und für alle Zielgruppen verständlich gestaltet werden. Dies betrifft insbesondere die Einführung in 2FA-Verfahren und Umsetzung von Inhaltsverschlüsselung. Weitere Informationen zu Usable Security finden Sie in dem durch das BSI veröffentlichte Whitepaper „Usable Security – Handlungsfelder menschzentrierter Cybersicherheit“ [8].

3. Interoperable und benutzerfreundliche Verschlüsselung

Ende-zu-Ende-Verschlüsselung (E2EE) ist der zentrale Baustein, um die Vertraulichkeit, Integrität und Authentizität der E-Mail-Kommunikation aus Verbrauchersicht nachhaltig zu schützen. Die Souveränität über die eigenen Daten beim Austausch von E-Mails kann nur durch E2EE erreicht werden. In der Praxis bleibt E2EE im Kontext von E-Mails jedoch ein Nischenthema, das bislang vor allem von technisch versierten Nutzerinnen und Nutzern und meist unter Einsatz eines provider-unabhängigen Clients wie Microsoft Outlook oder Thunderbird umgesetzt wird. Im aktuellen Cybersicherheitsmonitor gaben nur 16 % der Befragten an, E-Mail-Verschlüsselung zu nutzen [3]. Die bisherig angebotenen Verfahren sind durchaus komplex: Schlüsselerzeugung, Austausch und Verwaltung erfordern oft spezielles Vorwissen und manuelle Schritte, die für den Großteil der Anwenderinnen und Anwender eine kaum überwindbare Hürde darstellen [9].

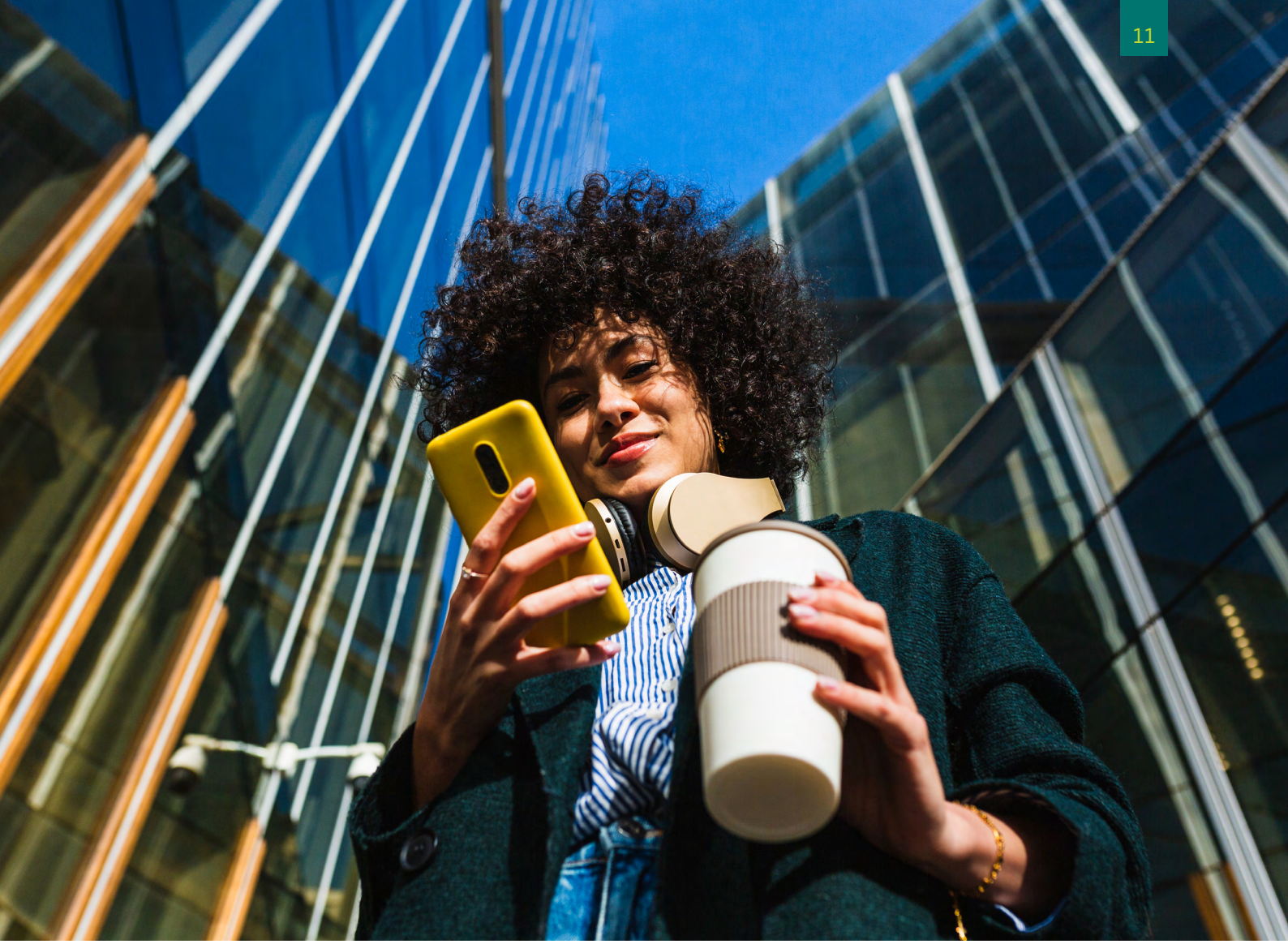
Anbieter von Webmail-Diensten sollten daher sicherstellen, dass Verbraucherinnen und Verbraucher ihre Nachrichten bei Bedarf eigenständig E2EE-geschützt aus dem Webmailer heraus versenden und empfangen können – und zwar ohne hohe Einstiegshürden. Technische Standards wie OpenPGP und S/MIME stellen hierfür etablierte kryptografische Verfahren bereit, die es gilt über einfache und intuitive Anwendungen in Webmail-Diensten umzusetzen. Damit dies gelingt, bedarf es technischer und konzeptioneller Anpassungen seitens der Anbieter.

Dazu gehören vor allem:

- Automatisierte Generierung und Verwaltung von Schlüsselpaaren direkt im Dienst, ohne dass die Nutzerinnen und Nutzer kryptografische Details verstehen oder manuell agieren müssen.
- Unterstützung etablierter offener Standards wie OpenPGP und S/MIME, um die Interoperabilität zwischen verschiedenen Anbietern sicherzustellen und eine langfristige Nutzbarkeit zu gewährleisten.
- Technologieoffenheit: nicht nur auf bekannten Standards verharren, auch neue interoperable Entwicklungen ermöglichen und vorantreiben, die Dienste übergreifend nutzbar sind.
- Niedrigschwellige Veröffentlichung und automatisierter Austausch des öffentlichen Schlüssels, beispielsweise durch das „Web Key Directory“ (WKD), sodass Kommunikationspartner öffentliche Schlüssel leicht finden können, ohne dass zusätzliche Schritte erforderlich sind [10].

Ein entscheidender Erfolgsfaktor dabei ist auch hier Usable Security: Sicherheitsmechanismen sind nur wirksam, wenn sie tatsächlich genutzt werden. Anbieter müssen die Aktivierung und Nutzung von Verschlüsselung so gestalten, dass sie auch für weniger technikaffine Nutzerinnen und Nutzer verständlich bleibt. Das bedeutet:

- Automatische Vorkonfiguration, die eine sichere Grundeinstellung bietet, ohne die Nutzerinnen und Nutzer zu überfordern.
- Klare visuelle Hinweise, wann eine Nachricht verschlüsselt versendet wird (Kenntlichmachung über Symbole wie z. B. Schloss).
- Verständliche Erklärungen in einfacher Sprache, die Transparenz schaffen, ohne in technische Details abzuschweifen.



Darüber hinaus sollten Anbieter ihr Verschlüsselungskonzept offenlegen. Ein transparentes Sicherheitsprofil – leicht auffindbar und in klarer Sprache – stärkt das Vertrauen und hilft Verbraucherinnen und Verbraucher zu verstehen, wie ihre Daten geschützt werden (vgl. Abschnitt 2.5). Dies umfasst Informationen zu verwendeten Protokollen, Schlüssellängen, Speicherorten und Prozessen bei Schlüsselverwaltung (z. B. Nutzung von WKD).

Die Bereitstellung von nutzerfreundlicher Ende-zu-Ende-Verschlüsselung ist nicht nur eine Frage der technischen Umsetzung, sondern ein Beitrag zur digitalen Souveränität der Verbraucherinnen und Verbraucher. Sie versetzt diese in die Lage, vertrauliche Kommunikation eigenständig und ohne zusätzliche Software oder komplizierte Workflows umzusetzen – direkt aus dem gewohnten Webmailer heraus.

Neben E2EE trägt eine Transportverschlüsslung nach aktuellen Standards zur Erhöhung der Vertraulichkeit in der E-Mail-Kommunikation bei. Die Umsetzung der BSI TR-03108 „Sicherer E-Mail-Transport“ [11] mit Technologien zur modernen Transportverschlüsselung wie DANE oder MTA-STS sind ein klares Sicherheitsbekenntnis der Anbieter und entfalten ihre volle Wirkung erst bei einer hohen Verbreitung im Markt. Daher gilt es, diese Technologien in die eigenen Infrastrukturen zu integrieren. Unterstützung bei Fragen zur Umsetzung der Technischen Richtlinie erhalten Anbieter bei der BSI Allianz für Cybersicherheit“ [12].

4. Wirksame und transparente Schutzmechanismen gegen Spam und Phishing

E-Mail-Kommunikation ist nach wie vor eines der bevorzugten Angriffsziele im digitalen Raum. Phishing-Versuche, gefälschte Absenderadressen, Spam mit Schadanhängen oder betrügerische Inhalte – die Bedrohungslage ist vielfältig und höchst dynamisch. Für Verbraucherinnen und Verbraucher sind derartige Angriffe oft schwer zu erkennen und schwerwiegende Folgen wie Identitätsdiebstahl, Datenverlust oder Kontenübernahme durch unberechtigte Dritte keine Seltenheit. Für Anbieter von E-Mail-Diensten ergibt sich daraus die Verpflichtung wirksame, transparente und benutzerfreundliche Schutzmaßnahmen gegen Spam und Phishing zu implementieren. Die Verantwortung für die IT-Sicherheit darf nicht allein auf die Endnutzerinnen und Endnutzer verlagert werden – insbesondere, wenn bereits technische Schutzmechanismen existieren, die automatisiert wirken können.

Das BSI betont, dass ein effektiver Schutz vor Phishing und Spam nur durch ein mehrschichtiges System technischer und organisatorischer Maßnahmen möglich ist [13].

In der Benutzerschnittstelle müssen als Spam markierte Nachrichten eindeutig kenntlich sein. Nutzerinnen und Nutzer sollten zudem die Möglichkeit haben, E-Mails manuell als Spam oder Phishing zu kennzeichnen. Die Differenzierung ist sinnvoll, da Spam in der Regel unerwünschte Werbung darstellt, während Phishing einen direkten Angriff auf Zugangsdaten oder Identitäten bedeutet. Eine getrennte Kennzeichnung verbessert daher sowohl die Präzision der Filtermechanismen als auch die Sicherheit. Ebenso wichtig ist die Option „Kein Spam“ für den Fall von False Positives. Nachrichten des betreffenden Absenders werden anschließend nicht mehr als Spam eingestuft. Auf diese Weise können Nutzerinnen und Nutzer aktiv in den Filterprozess eingreifen. Elementar ist dabei ein transparenter Feedbackloop nach dem Schema: „Danke, diese Nachricht wird nun geprüft“.

Neben diesen Funktionen in der Benutzerschnittstelle sind etablierte Verfahren zur Absenderprüfung und Inhaltsvalidierung im Backend anzuwenden. Die Umsetzung der BSI TR-03182 „E-Mail-Authentifizierung“ [14] trägt dazu bei, den Missbrauch von Identitäten, also das Vortäuschen einer fremden Identität, z. B. für Spoofing- und Phishing-Angriffen zu verhindern – ohne Mehraufwand auf Seiten der Nutzerinnen und Nutzer.

Zentrale Bausteine in diesem Kontext sind:

- SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail) und DMARC zur Prüfung der Authentizität eingehender E-Mails. Diese Verfahren ermöglichen es, gefälschte Absender zuverlässig zu erkennen – etwa durch Abgleich mit den autorisierten Mailservern einer Domain.
- SMTP-Plausibilitätsprüfung, bei der überprüft wird, ob die verwendete Absenderadresse technisch plausibel ist.
- Greylisting: das temporäre Zurückweisen von E-Mails mit der Erwartung, dass nur seriöse Server die Zustellung erneut versuchen. Dies ist besonders wirksam gegen einfache Spam-Bots.
- IP-Reputation-Checks auf Basis von Echtzeit-Blacklists (z. B. Spamhaus), um bekannte Quellen für Spam und Malware frühzeitig zu blockieren.
- Textbasierte Inhaltsfilter, ergänzt durch Virenscanner, um schädliche Anhänge, Links oder typische Betrugsmuster zu identifizieren.
- E2EE leistet auch hier mit digitalen Signaturen einen wichtigen Beitrag.

All diese Maßnahmen wirken vorwiegend im Backend und sind für die Nutzerinnen und Nutzer in der Regel weder sichtbar noch steuerbar. Diese fehlende Transparenz über die Güte und Art der Schutzmechanismen ist aus Perspektive des digitalen Verbraucherschutzes problematisch. Verbraucherinnen und Verbraucher haben kaum eine Möglichkeit zu beurteilen, wie effektiv der Schutz ihres E-Mail-Kontos ist oder nach welchen Kriterien Nachrichten gefiltert, markiert oder blockiert werden. Insbesondere wenn bestimmte Dienste durch maschinelles Inhalts-Scanning besonders hohe Erkennungsraten erreichen, darf der Schutz vor schädlichen Inhalten nicht zu Lasten der Vertraulichkeit oder informationellen Selbstbestimmung gehen.

Hier sind die Anbieter gefordert, die eingesetzten Schutzmaßnahmen zumindest in Grundzügen transparent zu machen.

Dazu gehören:

- Informationen darüber, welche Authentifizierungsverfahren verwendet und ob IP- oder Inhaltsanalysen durchgeführt werden,
- Hinweise darauf, ob und wie Nutzerinnen und Nutzer falsch eingestufte Nachrichten (False Positives) im Webmailer prüfen und freigeben können,
- und klare Kommunikationswege, über die verdächtige Nachrichten gemeldet und überprüft werden können („Spam-Melden“-Funktion).

Darüber hinaus sollten Anbieter regelmäßig prüfen, ob ihre Filtermechanismen dem aktuellen Stand der Technik entsprechen und wie sie im Vergleich zu etablierten Best Practices stehen. Eine öffentlich einsehbare Selbstauskunft – im Rahmen eins Sicherheitsprofils (vgl. Abschnitt 2.5) – könnte hier helfen, Vertrauen aufzubauen und gleichzeitig ein Mindestmaß an Transparenz herzustellen.

Ein wirksamer Schutz vor Spam und Phishing darf nicht allein technischer Selbstzweck sein, sondern muss als integraler Bestandteil digitaler Verbrauchersicherheit verstanden werden.

5. Sichere und nachvollziehbare Wege zur Accountwiederherstellung

Die Wiederherstellung eines E-Mail-Kontos nach einem Verlust des Zugangs – sei es durch vergessene Anmeldedaten oder durch eine Übernahme durch unbefugte Dritte – ist für Verbraucherinnen und Verbraucher ein kritischer Moment. Gerade im Fall eines kompromittierten Kontos sind Nutzerinnen und Nutzer auf schnelle, nachvollziehbare und zugleich sichere Hilfe durch den Anbieter angewiesen. In der Praxis sind diese Prozesse jedoch oft unklar, technisch anspruchsvoll oder mit hohen Hürden verbunden – besonders wenn der Angreifende bereits sicherheitsrelevante Einstellungen verändert hat. Handlungsanweisungen für diese Fälle auf den Webseiten der Anwender existieren oft nicht.

Ein zentrales Problem liegt darin, dass viele Wiederherstellungsverfahren auf Informationen basieren, die nach einer Accountübernahme nicht mehr vertrauenswürdig sind: gespeicherte Backup-E-Mail-Adressen, Telefonnummern oder Sicherheitsfragen können durch Angreifende leicht ersetzt oder manipuliert werden. Deshalb muss schon bei der Registrierung die Möglichkeit geschaffen werden, den legitimen Kontoinhaber später zweifelsfrei identifizieren zu können.

Ein wirksamer Ansatz könnte die optionale Verifikation der Identität bereits im Anmeldeprozess, etwa durch Verfahren wie Postident oder die Verwendung der Online-Ausweisfunktion sein. Dies sollte ausdrücklich als freiwilliger Zusatzdienst angeboten werden – nicht als Voraussetzung für die Nutzung des Dienstes. Ein derart verifizierter Account könnte im Ernstfall einfacher und sicherer wiederhergestellt werden, da der Anbieter auf verlässliche Identitätsmerkmale zurückgreifen kann. Gleichzeitig würde dies auch die Vertrauenswürdigkeit des Absenders gegenüber Dritten stärken.

Neben der Identitätsprüfung müssen auch die regulären Wiederherstellungsprozesse transparent, robust und benutzerfreundlich gestaltet sein.

Dazu gehören:

- Bereitstellung von Informationen zu Möglichkeiten der Wiederherstellung, zum Ablauf und zu erwarteten Bearbeitungszeiten,
- Benennung der Kommunikationskanäle, über die sich Nutzerinnen und Nutzer bei Problemen im Idealfall 24/7 melden können (z. B. E-Mail, Online-Formular, telefonischer Support),
- sowie mehrstufige Verifikationsverfahren, die auch ohne Zugriff auf kompromittierte Daten funktionieren – etwa über gespeicherte Identitätsnachweise, Gerätehistorie oder verifizierte externe Accounts.

Gerade in sensiblen Situationen benötigen Verbraucherinnen und Verbraucher verlässliche Unterstützung auf Augenhöhe. Anbieter müssen den Sonderfall einer Accountübernahme explizit mitdenken und in ihren Prozessen abbilden. Dazu gehört auch eine Priorisierung solcher Fälle im Supportprozess und die Schulung entsprechender Stellen auf Seiten der Anbieter.

Nicht zuletzt ist auch hier die Usability entscheidend: Die Wiederherstellung darf kein Hindernislauf sein, sondern muss klar geführt, verständlich formuliert und im Idealfall auch mobil umsetzbar sein. So lässt sich verhindern, dass Betroffene sich hilflos fühlen. Nicht zuletzt ist der Faktor Zeit an dieser Stelle sehr relevant, da sich unberechtigte Dritte über den E-Mail-Account Zugang zu anderen Diensten verschaffen können, was weitreichende negative Folgen haben könnte. Gute und transparente Prozesse tragen auch zur Kundenbindung bei.

6. Transparente Sicherheitsprofile und nachvollziehbare Vertrauensmodelle

Verbraucherinnen und Verbraucher sind bei der Nutzung von E-Mail-Diensten in erheblichem Maße darauf angewiesen, dass der Anbieter seiner Verantwortung für die Informationssicherheit gerecht wird – gerade weil zentrale Sicherheitsfunktionen wie Spamfilter, Verschlüsselung oder Wiederherstellungsprozesse für Verbraucherinnen und Verbraucher nicht ohne weiteres überprüfbar sind. Das Vertrauen in den Dienst ist häufig nicht durch überprüfbare Fakten, sondern durch Markenimage, Empfehlungen oder Werbung geprägt.

Ein modernes Vertrauensmodell für digitale Dienste muss daher darstellen, warum und in welchem Umfang ein Anbieter als sicher gilt. Dies erfordert nicht nur technische Maßnahmen, sondern auch kommunikative Transparenz über Sicherheitsprozesse, Datenflüsse und Schutzmechanismen. Verbraucherinnen und Verbraucher sollten die Möglichkeit haben, sich ohne technisches Vorwissen einen Eindruck davon zu verschaffen, wie gut ihr Anbieter mit den zentralen Anforderungen der IT-Sicherheit umgeht. Kommen also Anbieter nicht bzw. nicht in geeigneter Weise dem Informationsbedürfnis von Verbraucherinnen und Verbrauchern nach, vergeben sie auch die Möglichkeit, IT-Sicherheit als Kauf- bzw. Nutzungsargument einzusetzen und damit die eigenen Marktchancen zu erhöhen [15].

Ein möglicher Ansatz zur Bereitstellung von verbrauchergerecht aufbereiteten IT-Sicherheitsinformationen[2] im Kontext von Webmail-Diensten ist die Einführung eines öffentlich einsehbaren Sicherheitsprofiles, das leicht verständlich darstellt:

- welche Authentifizierungs- und Verschlüsselungsverfahren implementiert sind,
- wie mit eingehenden Bedrohungen (z. B. Phishing) umgegangen wird,
- wie Prozesse zur Accountwiederherstellung aussehen,
- welche Standards, Zertifizierungen oder Richtlinien (z. B. BSI TR-03108/03182) eingehalten werden und
- wem vertraut der Dienst selbst (Drittanbietern z. B. bei Schlüsselverwaltung).

Dieses Profil sollte faktenbasiert und überprüfbar sein – etwa durch Selbstverpflichtungen, Prüfsiegel oder externe Audits. Vergleichbar mit einem technischen Datenblatt würde es Nutzerinnen und Nutzer ermöglichen, verschiedene Dienste hinsichtlich ihrer Sicherheitspraktiken zu vergleichen, ohne tief technisches Fachwissen zu besitzen.

Derartige Informationen fördern nicht nur die Souveränität der Nutzerinnen und Nutzer, sondern ermöglichen auch eine kritische Auseinandersetzung mit zentralen Fragen digitaler Infrastruktur – etwa zur Speicherung im Ausland, zur Rolle von KI im Spamschutz oder zur Transparenz bei automatisierten Entscheidungen.

Das Sicherheitsprofil sollte sowohl dienstintern (im Webmailer/App leicht auffindbar) als auch öffentlich auf der Website des Anbieters verfügbar sein.

Insgesamt gilt: Vertrauen ist kein statisches Merkmal, sondern ein Ergebnis nachvollziehbarer Sicherheitsentscheidungen und offener Kommunikation. E-Mail-Anbieter, die ihre Schutzmaßnahmen, Abläufe und Standards transparent und verständlich machen, leisten einen aktiven Beitrag zum digitalen Verbraucherschutz und erhöhen ihre eigenen Marktchancen.

2 | Siehe hierzu auch die Studie des BSI „Gute Verbraucherinformationen für IT-sicherheitsbewusste Kaufentscheidungen“ [15], die am Beispiel ausgewählter vernetzter Geräte im Rahmen eines exemplarischen Marktchecks belegt, dass Verbraucherinnen und Verbraucher Schwierigkeiten haben, vor bzw. beim Kauf relevante IT-Sicherheitsinformationen zu finden. Vor diesem Hintergrund untersucht die Studie, wie Verbraucherinnen und Verbraucher besser über IT-Sicherheit informiert werden können und entwickelt Vorschläge zur Darstellung von IT-Sicherheitsinformationen sowie Handlungsempfehlungen für eine Stärkung des Digitalen Verbraucherschutzes.

7. Fazit und abgeleitete Forderungen

Sichere E-Mail-Kommunikation ist eine Grundvoraussetzung für digitale Teilhabe und Selbstbestimmung. Verbraucherinnen und Verbraucher müssen darauf vertrauen können, dass ihre digitale Identität geschützt, ihre Kommunikation vertraulich bleibt und ihre Daten nicht missbraucht werden. Webmail-Dienste übernehmen dabei eine infrastrukturelle Schlüsselfunktion.

Doch in der Praxis ist der digitale Verbraucherschutz bislang nicht systematisch verankert: Sicherheitsfunktionen wie Ende-zu-Ende-Verschlüsselung oder Zwei-Faktor-Authentisierung werden teils zwar angeboten, sind aber oft nicht standardmäßig aktiviert, schwer auffindbar oder nicht interoperabel. Gleichzeitig mangelt es an Transparenz über Sicherheitsprozesse, über Prozesse für Wiederherstellungsmöglichkeiten bei Kompromittierung sowie nachvollziehbare Informationen zur Vertrauenswürdigkeit von Anbietern.

Um diese Lücke zu schließen, braucht es mehr als technische Weiterentwicklungen: Es braucht verbindliche Rahmenbedingungen, einen gesellschaftlichen Konsens über Schutzstandards und gezielte politische Impulse. Die folgenden Forderungen richten sich daher an Wirtschaft, Politik und Zivilgesellschaft gleichermaßen.

KONKRETE FORDERUNGEN DES BSI:

1. Verankerung verbindlicher Sicherheitsstandards

E-Mail-Anbieter sollten technische Mindeststandards umsetzen – insbesondere bei Authentisierung, Verschlüsselung, Spam-Schutz und Accountwiederherstellung. Die BSI-Technischen Richtlinien (z. B. TR-03182 für E-Mail-Authentifizierung) bieten hier eine bewährte Grundlage.

2. Förderung interoperabler Ende-zu-Ende-Verschlüsselung

Die Entwicklung, Integration und Standardisierung nutzerfreundlicher Ende-zu-Ende-Verschlüsselung im Webmailer sollte aktiv unterstützt werden – durch Förderprogramme, Open-Source-Initiativen und Standardisierungsgremien. Interoperabilität (z. B. über OpenPGP, S/MIME, WKD) muss dabei gewährleistet sein.

3. Einführung transparenter Sicherheitsprofile

Diese Profile sollten einfach nachvollziehbar sein und auf überprüfbaren Kriterien basieren.

4. Bereitstellung verbrauchergerechter Informationen zur IT-Sicherheit

Informationen müssen auch für technisch weniger affine Personen verständlich formuliert, dargestellt und leicht auffindbar sein.

5. Unterstützung bei Accountwiederherstellung

Die Wiederherstellung darf kein Hindernislauf sein, sondern muss klar geführt, verständlich-beschrieben und im Idealfall auch mobil 24/7 umsetzbar sein.

Webmailer stellen für viele Verbraucherinnen und Verbraucher die Schlüsselfunktion für die Kommunikation und Accountsicherheit dar. Damit geht ein hohes Maß an Verantwortung für Anbieter einher, dieses wichtige Produkt einfach und sicher abzubilden.

Anbieter haben jetzt die Chance mit der Umsetzung der in diesem Whitepaper aufgeführten konkreten Maßnahmen per freiwilliger Selbstverpflichtung sichtbar Vertrauen aufzubauen. Zugleich können Sie sich damit als verlässlicher Partner in einer insbesondere für Verbraucherinnen und Verbraucher immer komplexer werdenden Welt positionieren. Im Sinne einer ganzheitlich gedachten Unternehmensverantwortung sind die Bedürfnisse der E-Mail-Kundinnen und -Kunden nach Transparenz und Sicherheit aktiv zu berücksichtigen und dadurch ebenso zukünftige gesetzliche Verpflichtungen vorwegzunehmen, um sich so nicht zuletzt einen Wettbewerbsvorteil zu verschaffen.

Quellen

[1] ARD/ZDF (2024): Medienstudie 2024. Online unter: https://archiv.ard-zdf-medienstudie.de/files/Download-Archiv/Medienstudie_2024/Basispraesentation_ARD-ZDF-Medienstudie_2024.pdf

[2] Statista (2024): Prognose zur Anzahl der täglich versendeten und empfangenen E-Mails weltweit von 2021 bis 2028. Online unter: https://de.statista.com/statistik/daten/studie/252278/umfrage/prognose-zur-zahl-der-taeglich-versendeter-e-mails-weltweit/

[3] BSI (2025): Cybersicherheitsmonitor 2025. Online unter: https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Leistungen-und-Kooperationen/Digitaler-Verbraucherschutz/Digitalbarometer/digitalbarometer_node.html

[4] BSI (o. D.): Technische Betrachtung: Wie sicher sind die verschiedenen Verfahren der 2-Faktor-Authentisierung (2FA)? Online unter: https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Zwei-Faktor-Authentisierung/Bewertung-2FA-Verfahren/bewertung-2fa-verfahren_node.html

[5] BSI (2024): Whitepaper des Digitalen Verbraucherschutzes #1: Bewertung der Usable Security und IT-Sicherheit biometrischer Verfahren in der Zwei-Faktor-Authentisierung. Online unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/DVS-Berichte/white-paper-biometrie-2fa.html?nn=1118316

[6] BSI (2024): Verbraucherbefragung zur passwortlosen Authentisierung mit Passkeys. Online unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/DVS-Berichte/passwortlose-authentisierung-bericht.html?nn=1121960

[7] BSI (o. D.): BSI-Basisschutz: Sichere Passwörter. Online unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Checklisten/sichere_passwoerter_faktenblatt.pdf?__blob=publicationFile&v=4#download=1

[8] BSI (2025): Whitepaper des Digitalen Verbraucherschutzes #3: Usable Security – Handlungsfelder menschzentrierter Cybersicherheit. Online unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/DVS-Berichte/whitepaper-usable-security.html?nn=1118316

zurück zum Text, Seite 7

zurück zum Text, Seite 7

zurück zum Text, Seite 7

zurück zum Text, Seite 9

zurück zum Text, Seite 9

zurück zum Text, Seite 9

zurück zum Text, Seite 9

zurück zum Text, Seite 9

[9] Reuter, A. et al. (2021): Secure Email: A Usability Study. Online unter: https://doi.org/10.48550/arXiv.2110.06019 *zurück zum Text, Seite 10*

[10] BSI (o. D.): BSI-Projekt „EasyGPG“: E-Mail Verschlüsselung vereinfachen. Online unter: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Freie-Software/E-Mail-Verschluesselung/EasyGPG/easygpg_node.html *zurück zum Text, Seite 10*

[11] BSI (o. D.): BSI TR-03108: Sicherer E-Mail-Transport. Online unter: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr03108/tr03108_node.html *zurück zum Text, Seite 11*

[12] BSI (2025): BSI veröffentlicht Empfehlungen zur Verbesserung der E-Mail-Sicherheit in Unternehmen. Online unter: https://www.allianz-fuer-cybersicherheit.de/Webs/ACS/DE/Home/_/infos/20250526_Emailsicherheit.html *zurück zum Text, Seite 11*

[13] BSI (2018): E-Mail-Sicherheit: Handlungsempfehlungen für Internet-Service-Provider v2.0. Online unter: https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_098.html *zurück zum Text, Seite 12*

[14] BSI (o. D.): BSI TR-03182: E-Mail-Authentifizierung. Online unter: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr03182/TR-03182_node.html *zurück zum Text, Seite 12*

[15] BSI (2025): Gute Verbraucherinformationen für IT-sicherheitsbewusste Kaufentscheidungen: Status Quo und Handlungsempfehlungen für produktbezogene Verbraucherinformationen zur IT-Sicherheit am Beispiel vernetzter Geräte. Online unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/DVS-Berichte/Transparenzstudie_Ergebnisse.pdf?__blob=publicationFile&v=4 *zurück zum Text, Seite 15*

Abruf der im Quellenverzeichnis verzeichneten URLs am 15.10.2025.

www.bsi.bund.de

Deine E-Mails,
dein digitales Zuhause.