Petition zur minimierung der Sicherheitsrisiken standardisierter E-Mail-Adressformate in europäischen Behörden und Finanzinstitutionen unter Berücksichtigung regulatorischer Rahmenbedingungen

Autor: Alexander Engelbrecht / XelAeriS / Bayern für www.FdBank.org 08.05.2025

1. Executive Summary

Dieser Bericht analysiert die Sicherheitsimplikationen der verbreiteten Nutzung standardisierter, personenbezogener E-Mail-Adressformate, insbesondere des Formats Vorname.Nachname@Domain, in deutschen Behörden und Finanzinstitutionen. Die Analyse ergibt, dass dieses Format, während es in Behörden weniger dominant ist, im Finanzsektor, einschließlich großer Banken, weit verbreitet ist.[1] Diese Standardisierung schafft eine erhebliche und leicht ausnutzbare Angriffsfläche.

Die Vorhersagbarkeit solcher Formate erleichtert Angreifern die Informationsbeschaffung (OSINT), die Durchführung gezielter Phishing- und Social-Engineering-Kampagnen sowie die Ausnutzung von Datenlecks erheblich.[2] Diese Risiken werden durch neue, KI-gestützte Bedrohungen wie automatisiertes Cybersquatting und fortgeschrittenes Reverse Social Engineering weiter verschärft, da diese Techniken von der Kenntnis präziser Zielinformationen profitieren.[4]

Die regulatorische Landschaft, geprägt durch die IT-Sicherheitsanforderungen der BaFin (früher BAIT, nun zunehmend DORA) und die Empfehlungen des BSI, adressiert die IT-Sicherheit umfassend.[6] DORA insbesondere verschärft die Anforderungen an das IKT-Risikomanagement, die Meldung von Vorfällen, Resilienztests und das Management von Drittparteienrisiken.[8] Allerdings fehlt es sowohl in den BaFin-Vorgaben als auch in den BSI-Empfehlungen an einer expliziten Adressierung der spezifischen Risiken, die sich aus der *Standardisierung von E-Mail-Formaten* ergeben. BaFin konzentriert sich in ihren Warnungen primär auf die Abwehr von Betrug durch *gefälschte* Domains, während die Risiken *vorhersagbarer Formate* innerhalb legitimer Domains weniger Beachtung zu finden scheinen.[10]

Die im ursprünglichen Nutzerinteresse erwähnte spezifische Fallkonstellation bezüglich Herrn Engelbrecht und einer BaFin-Warnung konnte anhand der vorliegenden Informationen nicht substanziiert werden.[11] Die zugrundeliegende Besorgnis über eine mögliche Unterschätzung der Risiken durch Domain-Registrierungsstrategien und standardisierte E-Mail-Adressen seitens der Aufsicht erscheint jedoch angesichts der Analyse plausibel.

Zusammenfassend lässt sich feststellen, dass trotz robuster allgemeiner IT-Sicherheitsregularien

eine spezifische Lücke bei der Adressierung der Risiken durch standardisierte E-Mail-Formate besteht. Es werden Empfehlungen zur Diversifizierung von E-Mail-Formaten, verstärkter Überwachung, strenger Authentifizierung, gezielter Schulung und einer proaktiveren Domainstrategie für Institutionen sowie zur Anpassung regulatorischer Leitlinien vorgeschlagen.

2. Introduction

2.1 Kontextualisierung

Die digitale Kommunikation, insbesondere via E-Mail, ist ein integraler Bestandteil der Arbeitsabläufe in deutschen Behörden und im Finanzsektor. Eine gängige Praxis zur Vereinfachung der Verwaltung und Kommunikation ist die Verwendung standardisierter, oft personenbezogener E-Mail-Adressformate, wie beispielsweise Vorname.Nachname@Domain. Diese Konvention wirft jedoch signifikante Fragen hinsichtlich der Cybersicherheit auf, die den Kern dieses Berichts bilden. Die Untersuchung konzentriert sich auf die potenziellen Schwachstellen, die aus dieser Standardisierung in kritischen Sektoren wie dem Justizwesen, der Polizei und der Finanzindustrie resultieren.

2.2 Problem Statement

Das zentrale Problem standardisierter E-Mail-Formate liegt in ihrer Vorhersagbarkeit. Während sie internen Nutzern die Kontaktaufnahme erleichtern, bieten sie externen Akteuren mit böswilligen Absichten einen entscheidenden Vorteil. Angreifer können mit geringem Aufwand valide E-Mail-Adressen von Mitarbeitern generieren, sobald das verwendete Muster bekannt ist. Dies senkt die Hürde für die initiale Informationsbeschaffung (Open Source Intelligence, OSINT) und ermöglicht die Erstellung hochgradig personalisierter Angriffsvektoren wie Spear-Phishing und Social Engineering.2 Die Kenntnis von Namen, Arbeitgeber und E-Mail-Struktur liefert Angreifern wertvolle Informationen, die für gezielte Manipulationen genutzt werden können. Verschärft wird diese Problematik durch die zunehmende Verfügbarkeit und Leistungsfähigkeit von Künstlicher Intelligenz (KI), die zur Automatisierung und Skalierung von Angriffen wie Cybersquatting und Reverse Social Engineering eingesetzt wird, welche wiederum von präzisen Zielinformationen profitieren.4

2.3 Regulatory Nexus

Die IT-Sicherheit und Kommunikationsstandards in den betroffenen Sektoren unterliegen der Aufsicht und den Vorgaben maßgeblicher regulatorischer Instanzen. Für den Finanzsektor ist primär die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) zuständig, deren Anforderungen an die IT (z.B. BAIT, nun übergehend in die EU-Verordnung DORA) die Institute zu implementieren haben.6 Das Bundesamt für Sicherheit in der Informationstechnik (BSI) gibt darüber hinaus allgemeine und spezifische Empfehlungen zur IT-Sicherheit heraus, die auch für Behörden relevant sind.7 Eine zentrale Frage, die auch im Nutzerinteresse anklingt, ist, inwieweit diese regulatorischen Rahmenwerke die spezifischen Risiken adressieren, die von standardisierten E-Mail-Formaten und potenziell uneindeutigen Domainnamen ausgehen. Es besteht die Sorge, dass insbesondere die BaFin diese spezifischen Risiken unterschätzt oder in ihrer Regulierung nicht ausreichend berücksichtigt.

2.4 Report Objective & Scope

Ziel dieses Berichts ist eine fundierte Analyse der Verbreitung des Formats Vorname.Nachname@Domain und ähnlicher Strukturen in deutschen Behörden (Polizei, Justiz) und Finanzinstitutionen (Banken, BaFin, Verbände). Es werden die damit verbundenen Sicherheitsrisiken – einschließlich OSINT, Phishing, Social Engineering und der Rolle von KI-gestützten Angriffen –

detailliert untersucht. Weiterhin wird die relevante regulatorische Landschaft (BaFin, BSI, DORA) beleuchtet und kritisch bewertet, inwieweit die aktuellen Aufsichtsmechanismen geeignet sind, die identifizierten Schwachstellen zu mitigieren. Der Bericht strebt eine expertenbasierte Einschätzung an, die die Zusammenhänge zwischen E-Mail-Formatierungspraxis, Sicherheitslücken, neuen Bedrohungen und regulatorischer Effektivität darlegt.

3. Email Address Formatting Conventions in German Authorities and Financial Institutions

3.1 Financial Sector (Banks, BaFin, Associations)

Die Analyse der E-Mail-Formatierungskonventionen im deutschen Finanzsektor zeigt eine deutliche Tendenz zur Standardisierung, insbesondere zur Verwendung personenbezogener Formate.

- **Prevalence of Vorname.Nachname:** Die verfügbaren Daten deuten darauf hin, dass das Format Vorname.Nachname@Domain oder sehr ähnliche Varianten im Finanzsektor weit verbreitet sind. Ein markantes Beispiel ist die Deutsche Bank, bei der das Format {first}.{last}@db.com für einen überwältigenden Anteil von über 92% der E-Mail-Adressen genutzt werden soll.[1] Allgemeine Empfehlungen für professionelle E-Mail-Adressen nennen dieses Format ebenfalls als gängigsten und bevorzugten Standard, neben Variationen wie Initialen in Kombination mit dem Nachnamen.[17] Diese hohe Prävalenz schafft eine große, vorhersagbare und homogene Angriffsfläche in einem kritischen Sektor. Die Bequemlichkeit für die interne Kommunikation steht hier im direkten Widerspruch zu den Sicherheitsimplikationen, da die Standardisierung die Aufklärung (Reconnaissance) für Angreifer erheblich vereinfacht. Sobald das Muster einer Organisation bekannt ist, können potenziell Tausende gültige E-Mail-Adressen samt zugehöriger Namen generiert werden, was den Aufwand für OSINT und die Erstellung von Spear-Phishing-Listen drastisch reduziert.
- **BaFin's Own Practices & Warnings:** Die BaFin selbst kommuniziert eine klare Linie bezüglich ihrer eigenen E-Mail-Domäne. Sie versendet E-Mails ausschließlich über die Domain @bafin.de (sowie eine spezifische Domain für Newsletter: BaFinWebDE@newsletter.gsb.bund.de).[10] Die Behörde warnt aktiv und wiederholt vor betrügerischen E-Mails, die ähnliche, aber inkorrekte Domains verwenden (z.B. @bafin.com oder bafin@marketcontactgroup.online).[10] Als Beispiel für einen korrekten Absender wird poststelle@bafin.de genannt, was auf die Nutzung funktionaler Adressen hindeutet.[10] Gleichzeitig weisen die Kontaktformulare der BaFin, die Felder für Vor- und Nachnamen sowie die E-Mail-Adresse erfordern, darauf hin, dass auch die BaFin personenbezogene Daten im Kontext von E-Mail-Kommunikation erhebt.[19] Die öffentlichen Warnungen der BaFin konzentrieren sich jedoch primär auf die Abwehr direkter Imitation durch *falsche* Domains und auf Spoofing (Fälschung des Absenders auch bei korrekter Domain), insbesondere bei unaufgeforderter Kontaktaufnahme.[10] Die inhärenten Risiken, die sich aus der *Vorhersagbarkeit von Adressformaten innerhalb der legitimen @bafin.de-Domain* ergeben könnten, werden in diesen Warnungen nicht explizit thematisiert. Dies

deutet auf eine mögliche Lücke in der öffentlichen Risikokommunikation hin, die genau die vom Nutzer angesprochene Schwachstelle betrifft: Der Fokus liegt auf externen Bedrohungen, die die Domain nachahmen, nicht auf den potenziellen Risiken interner Formatierungsstandards.

- **Bank Associations & Other Institutions:** Auch bei anderen Akteuren im Finanzumfeld ist die Verknüpfung von Personendaten mit E-Mail-Adressen üblich. Beispielsweise erfordern Registrierungsformulare für Newsletter oder Veranstaltungen beim Verband deutscher Pfandbriefbanken (vdp) die Angabe von Anrede, Vorname, Nachname, Unternehmen und E-Mail-Adresse.[21] Ebenso folgen Kontaktformulare von Banken wie der VR Bank diesem Muster.[18] Dies unterstreicht die gängige Praxis, E-Mail-Adressen direkt mit identifizierbaren Personendaten zu koppeln.

3.2 German Authorities (Police, Justice, etc.)

Im Gegensatz zum Finanzsektor scheint die Nutzung standardisierter, personenbezogener E-Mail-Formate für die offizielle externe Kommunikation bei deutschen Behörden, insbesondere im Justiz- und Polizeiwesen, weniger verbreitet zu sein.

- **Justice System Communication:** Für den rechtlich verbindlichen elektronischen Rechtsverkehr sind normale E-Mails explizit nicht zugelassen.[22] Stattdessen kommen sichere, dedizierte Kommunikationsplattformen wie das Elektronische Gerichts- und Verwaltungspostfach (EGVP) oder De-Mail zum Einsatz.[22] Diese Systeme stellen Authentizität und Integrität sicher, umgehen aber die typischen E-Mail-Infrastrukturen und deren Formatierungskonventionen für den kritischen Austausch.
- **Email Formats in Justice/Administration:** Wo Standard-E-Mail dennoch genutzt wird, etwa für allgemeine Anfragen oder interne Zwecke, dominieren oft funktionale Adressen. Beispiele hierfür sind poststelle@bmj.bund.de (Bundesministerium der Justiz), aumiau@bfj.bund.de oder datenschutz@bmj.bund.de (Bundesamt für Justiz).[27] Kontaktformulare sammeln zwar Namen und E-Mail-Adressen [32], aber die Struktur der dahinterliegenden oder für Mitarbeiter verwendeten Adressen wird nicht durchgängig offengelegt. Dokumente zeigen teils Platzhalter für individuelle E-Mails ohne Formatangabe.[28] Das Niedersächsische Landesamt für Bezüge und Versorgung (NLBV) nutzt ebenfalls funktionale Adressen wie NLBVZIBHa@nlbv.niedersachsen.de oder PoststelleNLBVHannover@nlbv.niedersachsen.de, erwähnt aber auch die Existenz von Personen-E-Mails.[33] Die österreichische Justiz lehnt E-Mails für Verfahrensangelegenheiten explizit ab.[34]
- **Police Communication:** Die Kontaktaufnahme mit der Polizei wird häufig über Webformulare oder zentrale, funktionale E-Mail-Adressen wie gst.internet@polizei.bayern.de (Bayerisches Innenministerium) oder pp-

obn.herrsching.pi@polizei.bayern.de (Polizeiinspektion Herrsching) kanalisiert.[36] Von der Nutzung direkter E-Mail für Notrufe oder die Erstattung von Anzeigen wird explizit abgeraten.[36] Zwar werden für die Anzeigenaufnahme vollständige Personalien benötigt [40], eine direkte Verknüpfung mit einem standardisierten E-Mail-Format für Beamte ist aus den vorliegenden Informationen jedoch nicht ersichtlich.

Diese Beobachtungen legen nahe, dass deutsche Behörden, insbesondere im Justizbereich, für ihre kritische externe Kommunikation weniger auf standardisierte, personenbezogene E-Mail-Formate angewiesen sind als der Finanzsektor. Der häufigere Einsatz funktionaler Adressen und sicherer Plattformen wie EGVP reduziert potenziell die Angriffsfläche, die sich aus leicht vorhersagbaren persönlichen E-Mail-Formaten ergibt. Dies impliziert ein potenziell höheres Maß an inhärenter Sicherheit gegen formatbasierte Aufklärung im öffentlichen Sektor, obwohl interne Kommunikationsmuster möglicherweise dennoch standardisiert sein könnten.

3.3 Table: Overview of Email Format Patterns
Die folgende Tabelle fasst die beobachteten Muster der E-Mail-Formatierung in den untersuchten Sektoren zusammen:

Sektor	**Verbreitete Formate**	**Prävalenz (Vorname.Nachname)**	**Prävalenz (Funktional/Plattform)**	**Unterstützende Quellen**
Finanzinstitute (Banken)	Vorname.Nachname@..., Initialen-basiert	Hoch	Mittel (für Support etc.)	1
BaFin	@bafin.de, Funktionale Adressen (poststelle@...), Newsletter-Adresse	Unbekannt (intern)	Hoch (extern sichtbar)	10
Justizsystem	EGVP, De-Mail, Funktionale Adressen (poststelle@..., aumiau@...,	Gering (extern sichtbar)	Hoch	22

	xbfj@...)			
Polizei	Webformulare, Funktionale Adressen (gst.internet@..., pi@...), Notruf (Telefon)	Gering (extern sichtbar)	Hoch	[36]
Allgemeine Behörden	Funktionale Adressen (...ZIB...@..., Poststelle...@...), De-Mail, Personen-Adressen	Mittel (variiert)	Hoch	[25]

Hinweis: Die Prävalenzschätzungen basieren auf den analysierten Quellen und beziehen sich primär auf extern sichtbare oder explizit genannte Formate. Interne Konventionen können abweichen.

Diese Übersicht verdeutlicht die unterschiedlichen Ansätze und unterstreicht die hohe Konzentration des potenziellen Risikos durch das Vorname.Nachname-Format im Finanzsektor, was die nachfolgende Risikoanalyse besonders relevant macht.

4. Inherent Security Vulnerabilities of Standardized Email Formats

Die Verwendung standardisierter und somit vorhersagbarer E-Mail-Adressformate birgt inhärente Sicherheitsrisiken, die von Angreifern systematisch ausgenutzt werden können.

4.1 Facilitation of OSINT and Reconnaissance

Standardisierte Formate wie Vorname.Nachname@Domain oder Initial.Nachname@Domain sind trivial zu erraten, sobald das verwendete Muster einer Organisation bekannt ist.2 Angreifer können öffentlich zugängliche Informationen, wie Mitarbeiterlisten auf Unternehmenswebseiten oder Profile auf beruflichen Netzwerken wie LinkedIn, nutzen, um Namenslisten zu erstellen. In Kombination mit der bekannten Domain und dem vermuteten E-Mail-Format lässt sich eine große Anzahl potenziell gültiger E-Mail-Adressen systematisch generieren.2

Die Validierung dieser generierten Adressen kann oft ohne direkte Interaktion mit den Zielservern erfolgen (passive Validierung), beispielsweise durch die Analyse von Mail Exchange (MX)-Einträgen oder SPF/DKIM/DMARC-Konfigurationen.[2] Aktive Methoden, wie das Senden von Test-E-Mails oder die Nutzung spezialisierter Verifizierungsdienste (z.B. EmailHippo, ZeroBounce), sind ebenfalls möglich, bergen jedoch das Risiko, entdeckt zu werden.[2] Zahlreiche

OSINT-Werkzeuge wie theHarvester, Hunter.io, Phonebook.cz, Epieos sowie Skripte oder sogar KI-Modelle wie ChatGPT können diesen Prozess der Adressgenerierung und -validierung automatisieren und skalieren.[2]

Eine erfolgreich validierte E-Mail-Adresse bestätigt nicht nur die Existenz eines Mitarbeiters und dessen Zugehörigkeit zur Organisation, sondern liefert oft auch den vollen Namen und potenziell das Geschlecht. Diese Informationen dienen als Ausgangspunkt für weitere OSINT-Aktivitäten, wie die Suche nach zugehörigen Profilen in sozialen Netzwerken oder Einträgen in Datenbanken über Datenlecks.[2] Die Leichtigkeit, mit der standardisierte E-Mail-Formate vorhergesagt und validiert werden können, verwandelt somit selbst semi-öffentliche Mitarbeiterverzeichnisse (wie LinkedIn) in direkt nutzbare Ziellisten für Cyberangriffe. Dies senkt die initiale Hürde für die Aufklärung durch Angreifer signifikant, da sie nicht erst auf geleakte E-Mail-Listen angewiesen sind, um gezielte Kampagnen zu starten.

4.2 Increased Susceptibility to Phishing, Spear Phishing, and BEC

Die Kenntnis der korrekten E-Mail-Adresse und des zugehörigen Namens eines Mitarbeiters ist ein entscheidender Faktor für den Erfolg von gezielten Phishing-Angriffen. Angreifer können diese Informationen nutzen, um hochgradig personalisierte Spear-Phishing-E-Mails zu erstellen.3 Solche E-Mails, die den Empfänger korrekt ansprechen und möglicherweise auf interne Gegebenheiten Bezug nehmen, wirken weitaus legitimer als generische Phishing-Versuche und haben eine deutlich höhere Erfolgswahrscheinlichkeit, den Empfänger zum Klicken auf einen bösartigen Link, zum Öffnen eines infizierten Anhangs oder zur Preisgabe sensibler Daten zu verleiten.

Insbesondere bei Business Email Compromise (BEC)-Angriffen ist die Kenntnis der E-Mail-Adressen von Schlüsselpersonen (z.B. Geschäftsführer, Finanzleiter) essenziell. Angreifer können sich überzeugender als diese Personen ausgeben, wenn sie deren tatsächliche E-Mail-Adresse verwenden (oder eine sehr ähnliche, gefälschte Adresse), um beispielsweise betrügerische Überweisungen zu veranlassen oder vertrauliche Unternehmensdaten zu erlangen.[3]

Der psychologische Effekt ist nicht zu unterschätzen: Eine E-Mail, die scheinbar von einem bekannten Kollegen mit der korrekten Adresse (vorname.nachname@legitime-domain.de) stammt, wird mit einer höheren Wahrscheinlichkeit als vertrauenswürdig eingestuft.[3] Selbst wenn der Inhalt ungewöhnlich ist, kann die bekannte Absenderadresse die Wachsamkeit des

Empfängers herabsetzen. Das BSI warnt explizit davor, dass Absenderadressen leicht gefälscht werden können (Spoofing) [53], doch die initiale Glaubwürdigkeit wird durch das korrekte Format erhöht. Standardisierte E-Mail-Formate wirken somit als Multiplikator für die Effektivität von Phishing. Indem sie das Raten von Zieladressen und Namen eliminieren, können Angreifer ihre Ressourcen auf die Erstellung überzeugenderer, personalisierter Köder konzentrieren und so sowohl technische Filter als auch die menschliche Wachsamkeit mit höherer Wahrscheinlichkeit umgehen.

4.3 Enabling Social Engineering and Reverse Social Engineering

Die durch OSINT aus standardisierten E-Mail-Formaten gewonnenen Informationen (Name, Arbeitgeber, potenziell Rolle/Abteilung) sind wertvolle Bausteine für Social-Engineering-Angriffe. Angreifer können diese Daten nutzen, um glaubwürdigere Vorwände (Pretexts) für eine Kontaktaufnahme oder Interaktion zu konstruieren.3 Eine Anfrage, die den Namen und die Zugehörigkeit des Opfers korrekt nennt, wirkt sofort weniger verdächtig.

Im Kontext von Reverse Social Engineering (RSE) können diese Informationen ebenfalls entscheidend sein. Bei RSE manipuliert der Angreifer die Situation so, dass das Opfer von sich aus den Angreifer kontaktiert, meist in der Annahme, legitime Hilfe zu erhalten.[5] Ein Angreifer könnte beispielsweise gezielt ein Systemproblem bei einem bestimmten Mitarbeiter verursachen (Sabotage) und sich dann als IT-Support (Advertising) ausgeben, wobei die Kenntnis der E-Mail-Struktur und der Namen hilft, die Kommunikation authentisch wirken zu lassen oder die richtigen Personen zu impersonieren.[5] Da das Opfer den Kontakt initiiert, ist das Vertrauensverhältnis von Beginn an höher.[5]

Vorhersagbare E-Mail-Formate tragen somit zur Erosion des "Misstrauens gegenüber Unbekannten" in der digitalen Kommunikation bei. Wenn Angreifer mühelos korrekte Namen und Zugehörigkeiten ermitteln und verwenden können, fühlen sich ihre Interaktionsversuche (Phishing, Social Engineering, RSE-Köder) weniger wie unaufgeforderte Kontaktaufnahmen von Fremden an, sondern ähneln eher legitimer interner oder geschäftlicher Kommunikation. Dies spielt menschlichen Vorurteilen zugunsten von Vertrauen und Autorität in die Hände und macht Opfer anfälliger für Manipulationen, etwa durch gefälschten IT-Support oder von vermeintlichen Kollegen.

4.4 Amplification of Risk from Data Breaches

Datenlecks bei Online-Diensten sind eine häufige Quelle kompromittierter Zugangsdaten (E-Mail/Passwort-Kombinationen).2 Wenn Mitarbeiter für externe Dienste E-Mail-Adressen verwenden, die dem standardisierten Format ihres Arbeitgebers ähneln oder gar identisch sind, entsteht eine direkte Verbindung zwischen externen Sicherheitsvorfällen und der internen Unternehmenssicherheit.

Wird eine Liste mit E-Mails im Format Vorname.Nachname@... aus einem Datenleck bekannt, verknüpft dies sofort volle Namen und die (oft aus der Domain ableitbare) Organisation mit den

kompromittierten Adressen.[2] Angreifer nutzen solche Listen gezielt für Credential-Stuffing-Angriffe: Sie probieren die geleakten E-Mail/Passwort-Paare bei anderen Diensten aus, einschließlich der Logins für Unternehmensnetzwerke oder Cloud-Dienste.[2] Die Kenntnis des standardisierten Formats der Unternehmens-E-Mails erleichtert es Angreifern, die Logins gezielt mit extern erbeuteten Zugangsdaten anzugreifen, insbesondere wenn Mitarbeiter Passwörter wiederverwenden – eine bekannte Schwachstelle.[60]

Darüber hinaus können Informationen aus Datenlecks (prüfbar über Dienste wie HaveIBeenPwned, die auch vom BSI empfohlen oder genutzt wurden [60]) mit weiteren OSINT-Ergebnissen kombiniert werden, um ein detaillierteres Profil des Ziels zu erstellen und Angriffe noch gezielter zu gestalten.[2] Standardisierte E-Mail-Formate schaffen somit eine gefährliche Brücke zwischen der persönlichen Online-Identität und der Unternehmenssicherheit. Ein Datenleck auf einer externen, möglicherweise schlecht gesicherten Webseite, bei der ein Mitarbeiter eine E-Mail-Adresse im Stil seiner Arbeitsadresse verwendet hat, kann Angreifern direkt Zugangsdaten oder Informationen liefern, um dessen Unternehmenskonto anzugreifen und so die eigentlichen Unternehmenssicherheitsmaßnahmen zu umgehen.

5. The Role of AI in Exacerbating Threats: Cybersquatting and Reverse Social Engineering

Künstliche Intelligenz (KI) entwickelt sich zu einem potenten Werkzeug für Cyberkriminelle, das bestehende Bedrohungen wie Cybersquatting und Reverse Social Engineering (RSE) verstärken und skalieren kann.

5.1 AI-Powered Cybersquatting

Cybersquatting (oder Domain Squatting) bezeichnet die Praxis, Domainnamen zu registrieren, die identisch oder verwechselbar ähnlich zu existierenden Marken, Unternehmen oder bekannten Namen sind, mit der böswilligen Absicht, davon zu profitieren.4 Dies geschieht oft, um Nutzer fehlzuleiten, die sich vertippen oder die Marke suchen.

- **Techniken und Ziele:** Gängige Techniken umfassen Typosquatting (Ausnutzung von Tippfehlern, z.B. gogle.com statt google.com), Combosquatting (Kombination der Marke mit Schlüsselwörtern wie "payment", "login", "security", z.B. netflix-payments.com), Level-Squatting (Manipulation von Subdomains), Bitsquatting (Änderung eines Bits im Domainnamen), Homograph-Angriffe (Nutzung ähnlich aussehender Zeichen) und das Registrieren abgelaufener Domains (Expiration Date Exploitation).[4] Die Ziele sind vielfältig: Verbreitung von Malware, Durchführung von Phishing-Kampagnen, Verkauf gefälschter Waren, Anzeige von Werbung (Pay-per-Click), Rufschädigung der Originalmarke oder der Verkauf der Domain an den Markeninhaber zu einem überhöhten Preis.[4] E-Mails, die von solchen Domains gesendet werden, sind oft Teil des Betrugsschemas.[64]
- **AI Amplification:** Die zunehmende Verfügbarkeit von KI und Automatisierungstools befeuert das Cybersquatting.[4] KI-Modelle können eingesetzt werden, um massenhaft

überzeugende Domain-Variationen (Typos, Combos, Homographen) zu generieren, die menschliche Kreativität und Kapazität bei weitem übersteigen. KI kann potenziell auch den Prozess der Domainregistrierung und die Einrichtung der zugehörigen (oft betrügerischen) Webseiten oder E-Mail-Infrastrukturen automatisieren. Dies ermöglicht eine Industrialisierung des Cybersquattings. Darüber hinaus kann KI zur Erstellung überzeugenderer Phishing-Inhalte für E-Mails verwendet werden, die von diesen gefälschten Domains gesendet werden.

- **Relevanz für E-Mail-Formate:** Obwohl Cybersquatting primär ein Domain-Problem ist, schafft es die Infrastruktur für E-Mail-basierte Angriffe. Die Kenntnis legitimer E-Mail-Formate (Vorname.Nachname@...) kann Angreifern helfen, effektivere Combosquatting-Domains zu entwerfen (z.B. vorname.nachname-login@falschebank.com) oder Phishing-E-Mails von Typosquatting-Domains gezielter an Individuen zu richten. KI-gestütztes Cybersquatting stellt somit einen Übergang von manueller, opportunistischer Domainregistrierung hin zur potenziell industriell skalierten Erstellung von Infrastrukturen für Markenimitation dar. Dies erhöht das Volumen und die Raffinesse von ähnlich aussehenden Domains, die für Phishing und Betrug genutzt werden können, und macht die Domainüberwachung sowie die E-Mail-Filterung für Organisationen erheblich anspruchsvoller.

5.2 AI-Enhanced Reverse Social Engineering (RSE)

Reverse Social Engineering (RSE) ist eine raffinierte Angriffstechnik, bei der das Opfer dazu gebracht wird, den Angreifer zu kontaktieren.5 Der typische Ablauf umfasst drei Phasen: Sabotage (der Angreifer verursacht ein Problem oder suggeriert dessen Existenz), Advertising (der Angreifer positioniert sich als Problemlöser, z.B. als IT-Support) und Assistance (das Opfer nimmt Kontakt auf und gibt dabei unwissentlich Informationen preis oder gewährt Zugriff).5

- **AI's Role in RSE:** KI kann RSE-Angriffe auf mehreren Ebenen verstärken:
  - *Erstellung überzeugender Köder:* KI kann hochgradig realistische gefälschte Fehlermeldungen, Systemwarnungen, Pop-ups oder Phishing-E-Mails generieren, die legitime IT-Support-Benachrichtigungen oder Sicherheitswarnungen imitieren. Diese werden in der "Advertising"-Phase eingesetzt, um das Opfer zur Kontaktaufnahme zu bewegen.[5]
  - *Automatisierte Interaktion:* KI-gesteuerte Chatbots könnten potenziell die erste Kontaktaufnahme durch das Opfer (die "Assistance"-Phase) bearbeiten. Sie könnten überzeugend Support-Mitarbeiter imitieren, erste Informationen sammeln oder das Opfer anleiten, bevor möglicherweise ein menschlicher Angreifer übernimmt.[5]
  - *Personalisierung und Targeting:* KI könnte OSINT-Daten analysieren – die möglicherweise durch Kenntnis standardisierter E-Mail-Formate gesammelt wurden –

um besonders anfällige Individuen zu identifizieren oder die Sabotage- und Advertising-Phasen stärker auf das spezifische Opfer zuzuschneiden.

- **Connection to Email Formats:** Die Kenntnis vorhersagbarer E-Mail-Formate und der damit verbundenen Namen und potenziellen Rollen liefert die Basisdaten, die eine KI nutzen kann, um RSE-Köder zu personalisieren oder interne Supportstrukturen glaubwürdiger zu imitieren. Eine gefälschte Support-E-Mail, die vom scheinbar korrekten internen Format (it-support@firma.de) kommt und den Nutzer mit Namen anspricht, wirkt überzeugender. KI droht somit, RSE-Angriffe skalierbarer und überzeugender zu machen, indem sie die Erstellung raffinierter Köder automatisiert und potenziell die initiale Opferinteraktion übernimmt. Dies senkt die erforderliche Qualifikation für Angreifer und erhöht die Wahrscheinlichkeit, dass Mitarbeiter auf gefälschte Support-Angebote hereinfallen, insbesondere in Umgebungen, in denen legitime IT-Kommunikationsmuster (und möglicherweise standardisierte Formate) bekannt sind.

6. Regulatory Frameworks and Official Guidance

Die IT-Sicherheit und Kommunikationspraktiken im deutschen Finanzsektor und bei Behörden werden durch verschiedene regulatorische Rahmenwerke und Empfehlungen gesteuert, allen voran durch die Vorgaben der BaFin und des BSI.

6.1 BaFin's IT Security Mandates (BAIT/VAIT/KAIT to DORA)

Die BaFin hat traditionell sektorspezifische Anforderungen an die IT-Sicherheit formuliert, die nun zunehmend durch die europäische DORA-Verordnung abgelöst werden.

- **BAIT/VAIT/KAIT Overview:** Die Bankaufsichtlichen Anforderungen an die IT (BAIT), die Versicherungsaufsichtlichen Anforderungen an die IT (VAIT) und die Kapitalverwaltungsaufsichtlichen Anforderungen an die IT (KAIT) waren Rundschreiben der BaFin, die die gesetzlichen Vorgaben (wie §25a KWG, VAG) konkretisierten.[14] Sie deckten zentrale Bereiche ab, darunter IT-Strategie, IT-Governance, Informationsrisikomanagement, Informationssicherheitsmanagement (inklusive der Rolle eines Informationssicherheitsbeauftragten), Identitäts- und Rechtemanagement, IT-Projekte und Anwendungsentwicklung, IT-Betrieb sowie das Management von Ausgliederungen (Outsourcing).[68] Ein Kernanliegen war es, das Bewusstsein für IT-Risiken auf Managementebene zu schärfen und ein angemessenes Risikomanagement sicherzustellen.[14]
- **Transition to DORA:** Der Digital Operational Resilience Act (DORA), eine EU-Verordnung, ist seit dem 17. Januar 2025 anzuwenden und ersetzt bzw. harmonisiert die bisherigen nationalen IT-Aufsichtsanforderungen im Finanzsektor, um Doppelregulierungen zu vermeiden.[6] Die Rundschreiben KAIT, VAIT und ZAIT wurden mit Ablauf des 16. Januar 2025 aufgehoben. Die BAIT werden schrittweise außer Kraft gesetzt: Sie gelten nur noch für Institute, die (noch) nicht unter DORA fallen, und werden spätestens zum 31. Dezember 2026 vollständig aufgehoben, wenn durch das Finanzmarktdigitalisierungsgesetz

(FinmadiG) weitere Institute in den Anwendungsbereich von DORA fallen.[6]

- **BAIT/DORA Relevance to Email/Domain Security:** Obwohl die BAIT bereits robuste IT-Governance, Risikomanagement und Identitäts- und Zugriffsverwaltung forderten [69], enthielten sie keine expliziten Vorschriften zu E-Mail-Formatierungsstandards oder Domain-Namensrichtlinien. DORA setzt diesen Fokus auf ein umfassendes Management von Informations- und Kommunikationstechnologie (IKT)-Risiken fort und erweitert ihn.[8] E-Mail-Sicherheit ist integraler Bestandteil von DORA, insbesondere in den Bereichen Risikomanagement (Abwehr von Phishing, Malware), Meldung von IKT-Vorfällen, Resilienztests und Management von Drittparteienrisiken (z.B. Cloud-E-Mail-Anbieter).[8] DORA verlangt explizit Maßnahmen zur Sicherstellung der Vertraulichkeit, Integrität und Verfügbarkeit von Daten, einschließlich Verschlüsselung während der Übertragung und im Ruhezustand, sowie Schutz vor unbefugtem Zugriff.[74] Technologien wie DMARC zur E-Mail-Authentifizierung unterstützen die Ziele von DORA.[52] Der Übergang von nationalen Regelungen wie BAIT zu DORA stellt eine signifikante Verschärfung und Präzisierung der Anforderungen an die IKT-Resilienz dar. Auch wenn DORA keine spezifischen E-Mail-Formate vorschreibt, zwingt die starke Betonung des umfassenden IKT-Risikomanagements, der Vorfallmeldung, der Tests und insbesondere des Drittparteienrisikos [8] die Finanzinstitute implizit dazu, ihre E-Mail-Sicherheitspraktiken – einschließlich Authentifizierung, Verschlüsselung und Bedrohungserkennung – weitaus genauer zu überprüfen und zu verbessern.
- **BaFin's Enforcement & Oversight:** Die BaFin führt IT-Prüfungen bei den beaufsichtigten Instituten durch und erwartet die Behebung festgestellter Schwachstellen.[14] Durch das Finanzmarktintegritätsstärkungsgesetz (FISG) wurden die Befugnisse der BaFin zur direkten Prüfung von wesentlichen Auslagerungsunternehmen gestärkt.[85] Die BaFin betont wiederholt, dass IT-Sicherheit höchste Priorität auf Vorstandsebene haben muss.[14]

6.2 BSI Recommendations on Email Security

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) stellt umfangreiche Empfehlungen zur E-Mail-Sicherheit für Unternehmen, Behörden und Privatnutzer bereit.7

- **Technical Measures:** Das BSI rät zur Nutzung sicherer Übertragungsprotokolle (wie POP3S, IMAPS, SMTPS) und empfiehlt, auf die Anzeige von E-Mails im HTML-Format zu verzichten oder diese zumindest standardmäßig zu deaktivieren, um das automatische Nachladen externer Inhalte (Bilder, Tracking-Pixel) und die Ausführung von schädlichem Code zu verhindern.[7] Eingehende und ausgehende E-Mails sollten auf Schadsoftware gescannt werden.[87] Der Einsatz von Ende-zu-Ende-Verschlüsselung wird empfohlen, wo immer möglich und sinnvoll.[53] Ebenso wird die Implementierung von Spam- und Phishing-Filtern nahegelegt, was implizit auch E-Mail-Authentifizierungsstandards wie SPF, DKIM und DMARC einschließt.[87]
- **User Awareness:** Ein zentraler Punkt der BSI-Empfehlungen ist die Sensibilisierung der Nutzer. Der "3-Sekunden-Sicherheits-Check" (Prüfung von Absender, Betreff, Anhang auf

Plausibilität) soll zur Routine werden.[7] Nutzer sollen lernen, Absenderadressen kritisch zu prüfen (z.B. durch Überfahren mit der Maus, um die tatsächliche Adresse anzuzeigen, oder Prüfung des E-Mail-Headers), misstrauisch bei unerwarteten E-Mails, dringenden Handlungsaufforderungen oder generischen Anreden zu sein und auf schlechte Grammatik oder Rechtschreibung zu achten.[7] Links sollten vor dem Klicken überprüft werden (z.B. durch Hovern), und auf Spam-Mails sollte keinesfalls geantwortet werden.[53]

- **Password Security:** Das BSI gibt auch Empfehlungen für starke, einzigartige Passwörter und den möglichen Einsatz von Passwort-Managern.[94] Es weist auf die Wichtigkeit hin, Passwörter geheim zu halten und nicht unverschlüsselt zu übertragen oder zu speichern.[94] Die Überprüfung auf Kompromittierung in Datenlecks wird ebenfalls unterstützt bzw. empfohlen.[60] Die Empfehlungen des BSI konzentrieren sich stark auf die Abwehr von Bedrohungen, die *über* den E-Mail-Kanal verbreitet werden (Malware, Phishing, Spoofing), und auf das richtige Verhalten der Nutzer im Umgang mit E-Mails. Sie bieten jedoch weniger explizite strategische Anleitung zur Wahl von *E-Mail-Adressformaten* als präventive Maßnahme gegen Aufklärung und gezielte Angriffe. Obwohl die technischen Ratschläge fundiert sind, adressiert dieser Fokus möglicherweise nicht vollständig die vom Nutzer hervorgehobene grundlegende Schwachstelle der Formatstandardisierung.

6.3 BaFin's Stance on Domain Management and Phishing

Die BaFin nimmt eine aktive Rolle bei der Bekämpfung von Betrug und Missbrauch im Zusammenhang mit Domains im Finanzsektor ein.

- **Active Warnings:** Die Behörde veröffentlicht regelmäßig und zeitnah Warnmeldungen über betrügerische Webseiten und E-Mail-Domains, die vorgeben, von der BaFin selbst oder von lizenzierten Finanzinstituten zu stammen.[10] Dies umfasst Fälle von Phishing, unerlaubten Geschäften und Identitätsdiebstahl, bei denen Betrüger den Namen legitimer Unternehmen auf gefälschten Domains missbrauchen.[12] Diese Praxis zeigt eine proaktive Überwachung und einen klaren Fokus auf den Verbraucherschutz.
- **Domain Blocking Powers:** Gemäß § 37 Kreditwesengesetz (KWG) verfügt die BaFin über die rechtliche Befugnis, Internet Service Provider (ISPs) anzuweisen, den Zugang zu Domains zu sperren (DNS-Sperren), über die unerlaubte Finanzdienstleistungen angeboten werden.[98] Die Rechtmäßigkeit und Verhältnismäßigkeit solcher Sperren kann jedoch gerichtlich überprüft werden, wie ein Urteil des VG Frankfurt/Main zeigt, das eine spezifische DNS-Sperre als unverhältnismäßig aufhob, aber die grundsätzliche Zulässigkeit der Maßnahme bestätigte.[98]
- **Focus on Illegitimate Domains:** Die dokumentierten Maßnahmen und Warnungen der BaFin richten sich überwiegend gegen die Nutzung *illegitimer*, *betrügerischer* oder *nicht lizenzierter* Domains.[12] Der Fokus liegt auf der Bekämpfung von illegalen Aktivitäten und der Täuschung von Verbrauchern.
- **Ambiguous Domains (User Concern):** Die spezifische Sorge des Nutzers, dass die BaFin die Verwendung "uneindeutiger" (ambiguous) Domainnamen durch *legitime* Banken

zulasse, findet in den vorliegenden Dokumenten keine direkte Bestätigung oder Widerlegung. Die BaFin-Regularien (BAIT/DORA) und Warnungen scheinen sich nicht explizit mit der *Klarheit* oder *Eindeutigkeit* der von beaufsichtigten Instituten gewählten legitimen Domainnamen zu befassen, solange diese nicht für illegale Zwecke missbraucht werden. Die BaFin demonstriert eine klare Fähigkeit und Bereitschaft, gegen *betrügerische* Domainnutzung vorzugehen, *nachdem* diese erkannt wurde (Warnungen, DNS-Sperren). Es gibt jedoch weniger Hinweise auf proaktive regulatorische Maßnahmen, die die *Eigenschaften* (z.B. Klarheit, Eindeutigkeit, Resistenz gegen Typosquatting) von Domainnamen festlegen, die von *legitimen*, beaufsichtigten Instituten gewählt werden. Dies könnte die Lücke sein, die der Nutzer als potenzielles "Sicherheits-Versäumnis" wahrnimmt. Der regulatorische Fokus scheint eher auf der Verhinderung von Betrug *mittels* Domains zu liegen als auf der präventiven Regulierung der Namensgebungspraktiken legitimer Domains selbst.

7. Critical Assessment of Regulatory Oversight and Practices

Eine kritische Bewertung der aktuellen regulatorischen Aufsicht und der gängigen Praktiken im Hinblick auf die Risiken standardisierter E-Mail-Formate ergibt ein differenziertes Bild.

7.1 Adequacy of BAIT/DORA and BSI Guidance

Die regulatorischen Rahmenwerke und Leitlinien bieten eine solide Grundlage für die allgemeine IT-Sicherheit, weisen jedoch Lücken bei der Adressierung der spezifischen untersuchten Problematik auf.

- **Strengths:** Die bisherigen BAIT und insbesondere die neue DORA-Verordnung schaffen einen umfassenden und harmonisierten Rahmen für die digitale operationale Resilienz im Finanzsektor.[8] Die Anforderungen an IKT-Risikomanagement, Sicherheitstests (einschließlich Penetrationstests), Incident Management und das Management von Drittparteienrisiken sind streng und detailliert.[8] Diese Maßnahmen stärken indirekt auch die E-Mail-Sicherheit, da E-Mail ein kritischer Geschäftsprozess und ein häufiger Angriffsvektor ist.[8] Die Empfehlungen des BSI bieten wertvolle technische und verhaltensbezogene Anleitungen zur Abwehr gängiger E-Mail-Bedrohungen wie Malware und Phishing und zur Sensibilisierung der Nutzer.[7]
- **Potential Gaps:** Trotz dieser Stärken adressieren weder die BaFin-Regularien (BAIT/DORA, basierend auf den vorliegenden Informationen) noch die BSI-Leitlinien explizit das systemische Risiko, das durch die *Standardisierung vorhersagbarer E-Mail-Adressformate* entsteht. Während das Identitäts- und Rechtemanagement ein Thema ist [70], wird die Wahl des Adressformats selbst nicht als eigenständiger Risikofaktor in den formalen Anforderungen oder Empfehlungen hervorgehoben. Die Gefahr, dass diese Formate OSINT und gezielte Angriffe erleichtern, scheint in der Regulierung unterrepräsentiert zu sein. Ebenso fehlt eine klare regulatorische Positionierung zur Nutzerkritik bezüglich potenziell "uneindeutiger", aber legitimer Domainnamen, die von

Banken verwendet werden könnten. Es besteht somit eine Diskrepanz zwischen der in der Cybersicherheits- und OSINT-Community erkannten Schwachstelle vorhersagbarer E-Mail-Formate (siehe Abschnitt 4) und dem expliziten Fokus der deutschen Finanzregulierung und der BSI-Leitlinien. Die Vorschriften fordern robuste Sicherheit *um* die Kommunikationskanäle herum, scheinen aber über die inhärenten Risiken des gewählten *Adressierungsschemas* selbst zu schweigen. Dies deutet darauf hin, dass dieser spezifische Angriffsvektor – das Format selbst – derzeit kein primärer Fokus der überprüften regulatorischen Dokumente ist.

7.2 BaFin's Enforcement and Domain Security Approach

Die BaFin agiert im Bereich der Domain-Sicherheit sichtbar, jedoch primär reaktiv.

- **Reactive Strength:** Die Behörde überwacht den Markt aktiv auf betrügerische Aktivitäten und warnt regelmäßig vor spezifischen Domains und E-Mail-Adressen, die für illegale Finanzgeschäfte oder Phishing genutzt werden.[11] Sie besitzt zudem das Instrument der DNS-Sperre, um gegen nicht lizenzierte Anbieter vorzugehen, auch wenn dessen Einsatz rechtlich komplex sein kann.[98]
- **Proactive Limitation?:** Der Fokus liegt klar auf der Bekämpfung *illegaler* Domainnutzung. Es gibt keine Anzeichen dafür, dass die BaFin proaktiv Standards für die Namensgebung oder E-Mail-Formatierungsrichtlinien bei *legitimen*, beaufsichtigten Instituten vorschreibt oder prüft. Die Wirksamkeit des Ansatzes beruht somit stark auf der Erkennung von Missbrauch, weniger auf präventiven Richtlinien zur Minimierung der Angriffsfläche durch Namenskonventionen.

7.3 The "Engelbrecht Case" Context

Der vom Nutzer angeführte spezifische Fall "Engelbrecht" konnte nicht verifiziert werden.

- **Lack of Evidence:** Die zur Verfügung gestellten Rechercheergebnisse enthalten keine Informationen, die einen Fall mit "Herrn Engelbrecht", bestimmten Domainregistrierungen und einer daraus resultierenden BaFin-Warnung im Kontext unterschätzter E-Mail-Risiken belegen.[11] Eine direkte Analyse oder Bestätigung der Nutzerwahrnehmung zu diesem spezifischen Fall ist daher nicht möglich.
- **Addressing the Underlying Concern:** Unabhängig von der Verifizierbarkeit des Einzelfalls ist die *zugrundeliegende Sorge* des Nutzers – dass die BaFin die Risiken im Zusammenhang mit Domainstrategien und E-Mail-Formaten unterschätzen könnte – nachvollziehbar. Wie in Abschnitt 7.1 dargelegt, fokussieren sich die expliziten regulatorischen Texte und öffentlichen Warnungen der BaFin stark auf die Abwehr von Betrug und illegalen Aktivitäten [11] und weniger auf die präventive Steuerung von Risiken, die aus legitimen, aber potenziell unsicheren Praktiken wie der Standardisierung von E-Mail-Formaten resultieren. Während die BaFin zweifellos Domain-bezogene Bedrohungen erkennt, scheint der spezifische Angriffsvektor der Formatstandardisierung in ihrer öffentlichen Kommunikation und möglicherweise auch in der Tiefe ihrer Regulierung

weniger prominent zu sein. Obwohl der konkrete Fall nicht belegt werden kann, stützt die Analyse die Plausibilität der Kernkritik des Nutzers. Die reaktive Haltung der BaFin bei der Bekämpfung *betrügerischer* Domains, kombiniert mit dem Fehlen expliziter Regeln für *legitime* Domain- und E-Mail-Formatierungsstrategien, nährt die Besorgnis, dass präventive Maßnahmen gegen die inhärenten Risiken vorhersagbarer Formate und potenziell mehrdeutiger Domains im aktuellen Regulierungsrahmen unterentwickelt sein könnten.

8. Conclusion and Strategic Recommendations

8.1 Synthesis of Findings

Die Analyse der Sicherheitsrisiken standardisierter E-Mail-Adressformate in deutschen Behörden und Finanzinstitutionen führt zu folgenden zentralen Schlussfolgerungen:

- **Verbreitung und Risiko:** Vorhersagbare E-Mail-Formate, insbesondere Vorname.Nachname@Domain, sind im deutschen Finanzsektor weit verbreitet [1], während Behörden tendenziell stärker auf funktionale Adressen und sichere Plattformen setzen.[27] Diese Standardisierung im Finanzsektor schafft eine signifikante, leicht ausnutzbare Angriffsfläche.
- **Erhöhte Anfälligkeit:** Solche Formate erleichtern Angreifern nachweislich die Informationsbeschaffung (OSINT), die Durchführung gezielter Phishing- und Social-Engineering-Angriffe (inkl. BEC) und erhöhen das Risiko bei Datenlecks durch die direkte Verknüpfung von Identitäten.[2]
- **KI als Verstärker:** KI-gestützte Bedrohungen wie automatisiertes Cybersquatting und fortgeschrittenes Reverse Social Engineering können diese Schwachstellen nutzen und deren Auswirkungen potenzieren, indem sie Angriffe skalieren und personalisieren.[4]
- **Regulatorische Lücke:** Bestehende IT-Sicherheitsregularien (BAIT/DORA) und BSI-Empfehlungen sind zwar umfassend, adressieren jedoch nicht explizit das spezifische Risiko, das von der *Standardisierung der E-Mail-Formate* selbst ausgeht.[7] Der Fokus liegt auf der Absicherung der Infrastruktur und der Abwehr eingehender Bedrohungen, nicht auf der präventiven Gestaltung der Adressierungsschemata.
- **BaFin's Fokus:** Die BaFin bekämpft aktiv betrügerische Domainnutzung [10], scheint aber weniger präventiv auf die Gestaltung legitimer Domain- und E-Mail-Praktiken bei beaufsichtigten Instituten einzuwirken.
- **Validität der Kernsorge:** Die spezifische Nutzererwähnung eines "Engelbrecht-Falls" konnte nicht verifiziert werden.[11] Die zugrundeliegende Sorge einer möglichen Unterschätzung der Risiken durch standardisierte Formate und Domainstrategien, erscheint jedoch angesichts der festgestellten Lücke zwischen bekannten Schwachstellen und explizitem regulatorischem Fokus plausibel.

8.2 Recommendations for Authorities and Financial Institutions

Basierend auf den Ergebnissen werden folgende strategische Empfehlungen für Behörden und Finanzinstitute abgeleitet:

- **Email Format Diversification:** Es sollte geprüft werden, inwieweit weniger vorhersagbare E-Mail-Formate eingeführt werden können, insbesondere für Mitarbeiter in sicherheitskritischen Bereichen oder mit hoher externer Sichtbarkeit. Alternativen könnten rollenbasierte Adressen (buchhaltung@...), die Verwendung von Initialen in anderer Kombination (v.nachname@..., vorname.n@...) oder sogar teilweise randomisierte Elemente sein.[17] Hierbei muss eine Balance zwischen erhöhter Sicherheit und Nutzerfreundlichkeit gefunden werden.
- **Enhanced Monitoring & Detection:** Implementierung fortschrittlicher Überwachungssysteme ist ratsam. Diese sollten nicht nur auf bekannte Malware oder Phishing-Indikatoren achten, sondern auch auf Muster, die auf systematische Reconnaissance hindeuten (z.B. sequenzielle Abfragen von Adressvarianten). Der Einsatz von E-Mail-Authentifizierung (DMARC p=reject) und Advanced Threat Protection (ATP) zur Erkennung raffinierter Angriffe ist essenziell.[8] Ebenso wichtig ist die Überwachung auf potenzielle Cybersquatting-Versuche gegen die eigene Marke.
- **Strengthened Authentication:** Die konsequente Durchsetzung von Multi-Faktor-Authentifizierung (MFA) für den Zugriff auf E-Mail-Konten und zugehörige Systeme ist unerlässlich und entspricht dem Geist von DORA [74] und den BSI-Empfehlungen.
- **Targeted User Training:** Schulungsmaßnahmen sollten über allgemeine Phishing-Warnungen hinausgehen und spezifisch die Risiken von OSINT durch vorhersagbare Formate, die Mechanismen von Spear Phishing, BEC und RSE sowie die Bedeutung von Passwort-Hygiene thematisieren. Dies verstärkt die BSI-Leitlinien [7] und DORA's Forderung nach Sicherheitsbewusstsein.[82]
- **Domain Strategy Review:** Organisationen sollten eine proaktive Domainstrategie verfolgen. Dies beinhaltet die defensive Registrierung relevanter Domain-Variationen (Tippfehler, gängige TLDs), um Cybersquatting vorzubeugen.[4] Bei der Wahl primärer Domains sollte auf Klarheit und Eindeutigkeit geachtet werden, um Verwechslungen und Missbrauch zu erschweren.

8.3 Recommendations for Regulatory Bodies (BaFin, BSI)

Für die zuständigen Aufsichtsbehörden und Standardisierungsgremien ergeben sich folgende Handlungsempfehlungen:

- **Update Guidance:** Es sollte erwogen werden, die Sicherheitsimplikationen der Standardisierung von E-Mail-Adressformaten und die Bedeutung klarer Domain-Namenskonventionen explizit in die relevanten Leitlinien aufzunehmen – sei es im Rahmen der Auslegung von DORA durch die BaFin oder in den allgemeinen Empfehlungen des BSI.
- **Promote Best Practices:** Neben den technischen Sicherheitsanforderungen sollten aktiv Best Practices für eine sicherere E-Mail-Formatierung (z.B. Diversifizierung) und defensive

Domainregistrierungsstrategien kommuniziert und gefördert werden.

- **Risk Assessment Focus:** Im Rahmen der DORA-Anforderungen an das IKT-Risikomanagement [8] sollten beaufsichtigte Institute explizit dazu angehalten werden, die spezifischen Risiken ihrer gewählten E-Mail-Formatierungsstruktur und ihrer Domainnamen zu bewerten, zu dokumentieren und gegebenenfalls zu mitigieren.
- **Information Sharing:** Der durch DORA geförderte Informationsaustausch [9] sollte nicht nur aktuelle Bedrohungen umfassen, sondern auch den Austausch über effektive präventive Strategien, einschließlich sicherer E-Mail-Formatierung und Domain-Management-Praktiken, einschließen.

Durch die Umsetzung dieser Empfehlungen könnte die Resilienz deutscher und europäischer Behörden und Finanzinstitutionen gegenüber gezielten Cyberangriffen, die auf der Vorhersagbarkeit von Kommunikationsstrukturen aufbauen, signifikant erhöht werden.

Referenzen

1. Most common email formats of Deutsche Bank | Find verified ..., Zugriff am April 26, 2025, https://mailmo.io/email-patterns/email-address-format-of-deutsche-bank
2. OSINT: Mastering Email Address Investigation | CyberQuizzer Blog, Zugriff am April 26, 2025, https://www.cyberquizzer.com/blog/osint-email-address-investigation
3. Recognizing email threats and social engineering | J.P. Morgan Private Bank U.S., Zugriff am April 26, 2025, https://privatebank.jpmorgan.com/nam/en/insights/wealth-planning/recognizing-email-threats-and-social-engineering
4. 6 Things to Know About Domain Squatting in 2024 - CybelAngel, Zugriff am April 26, 2025, https://cybelangel.com/6-things-to-know-about-domain-squatting-in-2024/
5. Understanding Reverse Social Engineering Tactics - SafeAeon Inc., Zugriff am April 26, 2025, https://www.safeaeon.com/security-blog/reverse-social-engineering/
6. geändert am 09.04.2025 DORA - Digital Operational Resilience Act - BaFin, Zugriff am April 26, 2025, https://www.bafin.de/DE/Aufsicht/DORA/DORA_node.html
7. Nutzen Sie die E-Mail wirklich sicher? - BSI, Zugriff am April 26, 2025, https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Onlinekommunikation/E-Mail-Sicherheit/e-mail-sicherheit_node.html
8. DORA (Digital Operational Resilience Act): Ensuring secure financial communication - Retarus Corporate Blog - EN, Zugriff am April 26, 2025, https://www.retarus.com/blog/en/dora-ensuring-secure-financial-communicationikation-sicher-gestalten/
9. Digital Operational Resilience Act (DORA) - EIOPA - European Union, Zugriff am April 26, 2025, https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en
10. Warnungen & Aktuelles - Finanzaufsicht nutzt die E-Mail-Domain @bafin.de, Zugriff am April 26, 2025, https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Verbrauchermitteilung/weitere/2024/meldung_2024_03_05_Finanzaufsicht_E-Mail_Domain.html

11. Warnung vor gefälschten BaFin-E-Mails, Zugriff am April 26, 2025, https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Verbrauchermitteilung/weitere/2024/meldung_2024_24072024_gefaelschte_BaFin_Mails.html
12. Identitätsdiebstahl: BaFin warnt vor der Webseite investment-vermittlungen.de, Zugriff am April 26, 2025, https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Verbrauchermitteilung/unerlaubte/2024/meldung_2024_07_22_investment_vermittlungen_de.html
13. Reverse Social Engineering: Explaining a Potent Threat - Pureversity, Zugriff am April 26, 2025, https://www.pureversity.com/blog/reverse-social-engineering
14. IT-Aufsicht bei Banken und Versicherern - Jahresbericht 2018 - BaFin, Zugriff am April 26, 2025, https://www.bafin.de/DE/PublikationenDaten/Jahresbericht/Jahresbericht2018/Kapitel1/Kapitel1_5/Kapitel1_5_1/kapitel1_5_1_artikel.html
15. Von BAIT zu DORA: Neue Anforderungen an die IT-Regulierung im ..., Zugriff am April 26, 2025, https://casis-wp.de/von-bait-zu-dora-neue-anforderungen-an-die-it-regulierung-im-finanzsektor/
16. E-Mail Sicherheit - BSI - Bund.de, Zugriff am April 26, 2025, https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Buero/E-Mail-Sicherheit/e-mail-sicherheit_node.html
17. So erstellen Sie eine professionelle E-Mail-Adresse, Zugriff am April 26, 2025, https://sparkmailapp.com/de/blog/create-professional-email-address-format-examples
18. Phishing-Mail: BaFin warnt vor falschen Webseiten und E-Mails im Namen der BaFin, Zugriff am April 26, 2025, https://www.vrbanking.de/banking-service/sicherheit/phishing-warnungen/bafin-falsche-webseiten-emails.html
19. General contact form - BaFin, Zugriff am April 26, 2025, https://www.bafin.de/EN/DieBaFin/Kontakt/Kontaktformular/form_node.html
20. Support form - BaFin, Zugriff am April 26, 2025, https://www.bafin.de/EN/DieBaFin/Kontakt/Supportformular/supportformular_node.html
21. Datenschutz - vdp - Verband Deutscher Pfandbriefbanken, Zugriff am April 26, 2025, https://www.pfandbrief.de/site/de/vdp/footer/datenschutz.html
22. Elektronischer Rechtsverkehr | justiz.hessen.de, Zugriff am April 26, 2025, https://justizministerium.hessen.de/buergerservice/online-dienstleistungen/elektronischer-rechtsverkehr
23. Elektronischer Rechtsverkehr mit der Justiz Leitfaden, Zugriff am April 26, 2025, https://justiz.de/ervvoe/leitfaden_erv_pdf.pdf;jsessionid=4E3BBDFA1A0477A73F8DB234B73FDA42
24. Elektronischer Rechtsverkehr | Nds. Landesjustizportal - Portal Niedersachsen, Zugriff am April 26, 2025, https://justizportal.niedersachsen.de/startseite/burgerservice/elektronischer_rechtsverkehr/elektronischer-rechtsverkehr-202993.html
25. BMI - De-Mail - Bundesministerium des Innern und für Heimat, Zugriff am April 26, 2025, https://www.bmi.bund.de/DE/themen/moderne-verwaltung/e-government/de-mail/de-mail-node.html
26. BfJ - Elektronischer Rechtsverkehr - Bundesamt für Justiz, Zugriff am April 26, 2025, https://www.bundesjustizamt.de/DE/DasBfJ/Kontakt/Rechtsverkehr/Rechtsverkehr_node.

html
27. Anmeldeformular für das automatische Mitteilungs- und Auskunftsverfahren bei der Registerbehörde (AuMiAu) - Bundesamt für Justiz, Zugriff am April 26, 2025, https://www.bundesjustizamt.de/SharedDocs/Downloads/DE/ZentraleRegister/AuMiAu-Formular.pdf?__blob=publicationFile&v=10
28. Muster Nummer 1 Begleitschreiben bei eingehenden Ersuchen (zu Nummer 11 Absatz 1 Buchstabe a - REVOSax, Zugriff am April 26, 2025, https://www.revosax.sachsen.de/attachments/29302
29. BMJ - Kontakt - Bundesministerium der Justiz, Zugriff am April 26, 2025, https://www.bmj.de/DE/service/kontakt/kontakt_node.html
30. BMJ - Impressum - Bundesministerium der Justiz, Zugriff am April 26, 2025, https://www.bmj.de/DE/service/impressum/impressum_node.html
31. Datenschutzerklärung zum Beratungstelefon - hilfe-info.de, Zugriff am April 26, 2025, https://www.hilfe-info.de/Webs/hilfeinfo/DE/HilfeUndBeratung/AnsprechpartnerUndBeratungsstellen/BundUndLaender/Datenschutzerkl%C3%A4rung_Beratungstelefon.html
32. BfJ - Kontakt - Bundesamt für Justiz, Zugriff am April 26, 2025, https://www.bundesjustizamt.de/DE/DasBfJ/Kontakt/Kontakt_node.html
33. Kontakt | Niedersächsisches Landesamt für Bezüge und Versorgung (NLBV), Zugriff am April 26, 2025, https://www.nlbv.niedersachsen.de/wir_ueber_uns/kontakt/kontakt-68514.html
34. Kontakt - BMJ, Zugriff am April 26, 2025, https://www.bmj.gv.at/uebersicht_startseite/veroeffentlichungsangaben/kontakt.html
35. Kontakt - Die österreichische Justiz, Zugriff am April 26, 2025, https://justiz.gv.at/kontakt.1ab.de.html
36. Impressum - Die Bayerische Polizei, Zugriff am April 26, 2025, https://www.polizei.bayern.de/wir-ueber-uns/impressum/index.html
37. Polizeiinspektion Herrsching, Zugriff am April 26, 2025, https://www.lk-starnberg.de/showobject.phtml?object=tx|613.4096.1&ModID=9&FID=603.2190.1&title=
38. Die Bayerische Polizei - Die Bayerische Polizei - Ihr Garant für die ..., Zugriff am April 26, 2025, https://www.polizei.bayern.de/index.html
39. Kontakt - Die Bayerische Polizei, Zugriff am April 26, 2025, https://www.polizei.bayern.de/kontakt/index.html
40. So erstatten Sie Anzeige bei der Polizei | Verbraucherzentrale.de, Zugriff am April 26, 2025, https://www.verbraucherzentrale.de/wissen/vertraege-reklamation/kundenrechte/so-erstatten-sie-anzeige-bei-der-polizei-90897
41. Strafanzeige bei der Polizei; Erstattung - BayernPortal, Zugriff am April 26, 2025, https://www.bayernportal.de/dokumente/leistung/081865799498
42. Username/Email | s0cm0nkey's Security Reference Guide - GitBook, Zugriff am April 26, 2025, https://s0cm0nkey.gitbook.io/s0cm0nkeys-security-reference-guide/cyber-intelligence/osint/username-email
43. Leveraging OSINT techniques for email investigations - Authentic8 Silo, Zugriff am April 26, 2025, https://www.authentic8.com/blog/osint-techniques-email-investigations
44. Investigating Email Addresses with OSINT - OSINT Combine, Zugriff am April 26, 2025, https://www.osintcombine.com/post/investigating-email-addresses-with-osint

45. Review OSINT tool for social engineering - PMC, Zugriff am April 26, 2025, https://pmc.ncbi.nlm.nih.gov/articles/PMC10504660/
46. What does your email reveal? An ultimate mailbox investigation guide - OSINT Team, Zugriff am April 26, 2025, https://osintteam.com/learn-to-investigate-email-addresses/
47. Phishing and Social Engineering - Grand Valley State University, Zugriff am April 26, 2025, https://services.gvsu.edu/TDClient/60/Portal/KB/ArticleDet?ID=575
48. Your guide to identifying social engineering scams and cyber threats - Mastercard, Zugriff am April 26, 2025, https://www.mastercard.com/news/perspectives/2024/your-guide-to-identifying-social-engineering-scams-and-cyber-threats/
49. Don't Take the Bait! Phishing and Other Social Engineering Attacks | NJCCIC, Zugriff am April 26, 2025, https://www.cyber.nj.gov/guidance-and-best-practices/email-security/phishing-and-other-social-engineering-attacks
50. Avoiding Social Engineering and Phishing Attacks | CISA, Zugriff am April 26, 2025, https://www.cisa.gov/news-events/news/avoiding-social-engineering-and-phishing-attacks
51. Social Engineering - How to Secure Business Emails. - Guardian Digital, Zugriff am April 26, 2025, https://guardiandigital.com/email-threat/social-engineering
52. 3 ways the Digital Operational Resilience Act relates to email and domain security, Zugriff am April 26, 2025, https://blog.redsift.com/dora/3-ways-the-digital-operational-resilience-act-relates-to-email-and-domain-security/
53. E-Mail-Sicherheit: Mythen im Faktencheck - BSI - Bund.de, Zugriff am April 26, 2025, https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Sicherheitsirrtuemer/irrtuemer-e-mail-sicherheit.html
54. Das BSI informiert – 4 Sicherheitsirrtümer bei E-Mails - Projekt 29, Zugriff am April 26, 2025, https://projekt29.de/das-bsi-informiert-4-sicherheitsirrtuemer-bei-e-mails/
55. How Social Engineering Phishing Works: My Real-Life Encounter - Ran The Builder, Zugriff am April 26, 2025, https://www.ranthebuilder.cloud/post/social-engineering-phishing-my-experience
56. Reverse Social Engineering Attacks in Online Social Networks - S3@Eurecom, Zugriff am April 26, 2025, https://s3.eurecom.fr/docs/dimva11_reverse.pdf
57. What is Reverse Social Engineering? And How Does It Work? - Aware EC-Council, Zugriff am April 26, 2025, https://aware.eccouncil.org/what-is-reverse-social-engineering.html
58. What Is Reverse Social Engineering & How to Mitigate Risks - Trustifi, Zugriff am April 26, 2025, https://trustifi.com/blog/reverse-social-engineering-prevention-strategy/
59. Reverse Social Engineering: Preying On Role Reversal - Keystrike, Zugriff am April 26, 2025, https://www.keystrike.com/blogs/reverse-social-engineering-preying-on-role-reversal
60. BSI Sicherheitstest nutzen - so geht's - CHIP Praxistipps, Zugriff am April 26, 2025, https://praxistipps.chip.de/bsi-sicherheitstest-nutzen-so-gehts_24236
61. Sicherheitstest Ihrer Mailadresse durch das BSI - fox-on Datenschutz GmbH, Zugriff am April 26, 2025, https://fox-on.com/sicherheitstest-ihrer-mailadresse-durch-das-bsi/
62. What Is Cybersquatting and How to Deal With It | Trademark Engine, Zugriff am April 26, 2025, https://www.trademarkengine.com/blog/what-is-cybersquatting/
63. Cybersquatting: Attackers Mimicking Domains of Major Brands Including Facebook,

Apple, Amazon and Netflix to Scam Consumers, Zugriff am April 26, 2025, https://unit42.paloaltonetworks.com/cybersquatting/
64. 10 Interesting Cybersquatting Examples to Learn From - InfoSec Insights - Sectigo, Zugriff am April 26, 2025, https://sectigostore.com/blog/cybersquatting-examples/
65. Cybersquatting: How to Recognize it and Take Appropriate Action, Zugriff am April 26, 2025, https://nyplaw.com/cybersquatting-how-to-recognize-it-and-take-appropriate-action/
66. Latest trends in cybersquatting | Infosec, Zugriff am April 26, 2025, https://www.infosecinstitute.com/resources/phishing/latest-trends-in-cybersquatting/
67. As NFT's Popularity Grows, So Does Cybersquatting - Cybercrime Magazine, Zugriff am April 26, 2025, https://cybersecurityventures.com/as-nfts-popularity-grows-so-does-cybersquatting/
68. BAIT, VAIT, KAIT: IT-Sicherheit in der Finanzwirtschaft | Endpoint Protector Blog, Zugriff am April 26, 2025, https://www.endpointprotector.de/blog/bait-vait-kait-it-sicherheit-in-der-finanzwirtschaft/
69. Bankaufsichtliche Anforderungen an die IT (BAIT): Die 7 wichtigsten Fragen - usd AG, Zugriff am April 26, 2025, https://www.usd.de/7-fragen-zu-bait/
70. Versicherungsaufsichtliche Anforderungen an die IT - Wikipedia, Zugriff am April 26, 2025, https://de.wikipedia.org/wiki/Versicherungsaufsichtliche_Anforderungen_an_die_IT
71. BAIT: Diese Anforderungen stellt die Bankaufsicht an die IT - bayoosoft, Zugriff am April 26, 2025, https://www.bayoosoft.com/beitraege/anforderungen-bankaufsicht-an-die-it-von-banken/
72. Aktuelle Themen - IT-Sicherheit: Erwartungen der Bankenaufsicht - BaFin, Zugriff am April 26, 2025, https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Fachartikel/2013/fa_bj_2013_11_it_sicherheit.html
73. 10.01.2025 DORA kommt: Änderungen bei den aufsichtlichen Anforderungen an die IT, Zugriff am April 26, 2025, https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Meldung/2025/meldung_2025_01_09_DORA.html
74. DORA compliance for Email | Zivver, Zugriff am April 26, 2025, https://www.zivver.com/solutions/dora-compliance
75. DORA Regulation and Compliance - Mimecast, Zugriff am April 26, 2025, https://www.mimecast.com/content/dora/
76. DORA Regulation - Tenable documentation, Zugriff am April 26, 2025, https://docs.tenable.com/cyber-exposure-studies/dora/Content/overview.htm
77. Digital Operational Resilience Act (DORA) | Updates, Compliance, Training, Zugriff am April 26, 2025, https://www.digital-operational-resilience-act.com/
78. DORA User's Guide to Compliance - Sonatype, Zugriff am April 26, 2025, https://www.sonatype.com/resources/guides/dora-compliance-guide
79. What is DORA, and How Will It Impact You? Demystifying The Digital Operational Resilience Act | Mitratech, Zugriff am April 26, 2025, https://mitratech.com/resource-hub/blog/what-is-dora/
80. How DORA regulates email security: Your DORA compliance checklist - Zivver, Zugriff am April 26, 2025, https://www.zivver.com/blog/how-dora-regulates-email-security-your-dora-compliance-checklist
81. The intersection of DORA and DMARC, Zugriff am April 26, 2025,

https://dmarcreport.com/blog/the-intersection-of-dora-and-dmarc/
82. Navigating DORA and Ensuring Email Security Compliance - Cofense, Zugriff am April 26, 2025, https://cofense.com/blog/navigating-dora-and-ensuring-email-security-compliance
83. DORA Regulation and Why You Should Invest in Email Encryption - Kiteworks, Zugriff am April 26, 2025, https://www.kiteworks.com/regulatory-compliance/dora-regulation-email-encryption/
84. Data Security Compliance with the Digital Operational Resilience Act – DORA - Thales CPL, Zugriff am April 26, 2025, https://cpl.thalesgroup.com/compliance/emea/data-security-compliance-dora-resilience-act
85. Aktuelle Themen - IT-Aufsicht bei Banken - BaFin, Zugriff am April 26, 2025, https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Fachartikel/2021/fa_bj_2110_IT_Aufsicht.html
86. Pressemitteilungen - BaFin richtet Fokus zunehmend auf IT-Risiken, Zugriff am April 26, 2025, https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Pressemitteilung/2024/pm_2024_01_23_PK_Risiken_im_Fokus.html
87. E-Mail-Sicherheit: Handlungsempfehlungen für Internet-Service-Provider - Allianz für Cyber-Sicherheit, Zugriff am April 26, 2025, https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_098.pdf?__blob=publicationFile&v=1
88. Drei Sekunden für mehr E-Mail-Sicherheit - Allianz für Cyber-Sicherheit, Zugriff am April 26, 2025, https://www.allianz-fuer-cybersicherheit.de/Webs/ACS/DE/Netzwerk-Formate/Medien/Video/E_Mail_Sicherheitscheck/E_Mail_Sicherheitscheck_node.html
89. Safer Internet Day: BSI und DsiN räumen mit Mythen zu E-Mail-Sicherheit auf, Zugriff am April 26, 2025, https://www.sicher-im-netz.de/safer-internet-day-bsi-und-dsin-raeumen-mit-mythen-zu-e-mail-sicherheit-auf/
90. BSI warnt vor E-Mails mit gefälschtem BSI-Absender - manage it, Zugriff am April 26, 2025, https://ap-verlag.de/bsi-warnt-vor-e-mails-mit-gefaelschtem-bsi-absender/40168/
91. BSI und DsiN räumen mit Mythen zu E-Mail-Sicherheit auf - Infopoint Security, Zugriff am April 26, 2025, https://www.infopoint-security.de/bsi-und-dsin-raeumen-mit-mythen-zu-e-mail-sicherheit-auf/a39726/
92. Drei Checkpunkte für mehr E-Mail-Sicherheit | BSI - YouTube, Zugriff am April 26, 2025, https://www.youtube.com/watch?v=8H678AuWetQ
93. BSI verschärft Anforderungen an E-Mail-Sicherheitslösungen - SinCera Tech GmbH, Zugriff am April 26, 2025, https://www.sincera-tech.com/post/cyber-sicherheit-blog-4
94. Empfehlungen des BSI für starke Passwörter im Unternehmen: Kontrolle ist überlebenswichtig! - Specops Software, Zugriff am April 26, 2025, https://specopssoft.com/de/blog/empfehlungen-des-bsi-fur-starke-passworter-im-unternehmen-kontrolle-ist-uberlebenswichtig/
95. Warnungen & Aktuelles - QuantumAI: BaFin warnt vor Domain quantumtrade-app.live, Zugriff am April 26, 2025, https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Verbrauchermitteilung/unerlaubte/2024/meldung_2024_11_29_QuantumAI.html
96. FdCoin und FdBank: BaFin warnt vor Websites und weist auf Identitätsmissbrauch hin, Zugriff am April 26, 2025,

https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Verbrauchermitteilung/unerlaubte/2025/meldung_2025_04_24_FdCoin_FdBank.html
97. Kryptobetrug: Geld zurückholen nach Verlust über Euro Pro Markets (europromarkets.net) – BaFin warnt! - Anwalt.de, Zugriff am April 26, 2025, https://www.anwalt.de/rechtstipps/kryptobetrug-geld-zurueckholen-nach-verlust-ueber-euro-pro-markets-europromarkets-net-bafin-warnt-243505.html
98. Laut einem aktuellen Urteil kann die BaFin DNS-Sperren anordnen - domain-recht.de, Zugriff am April 26, 2025, https://domain-recht.de/internet-politik/websperren/vg-frankfurt-m-laut-einem-aktuellen-urteil-kann-die-bafin-dns-sperren-anordnen-69695.html
99. How Salt Communications Supports Compliance with DORA Regulations, Zugriff am April 26, 2025, https://saltcommunications.com/news/how-salt-communications-supports-compliance-with-dora-regulations/