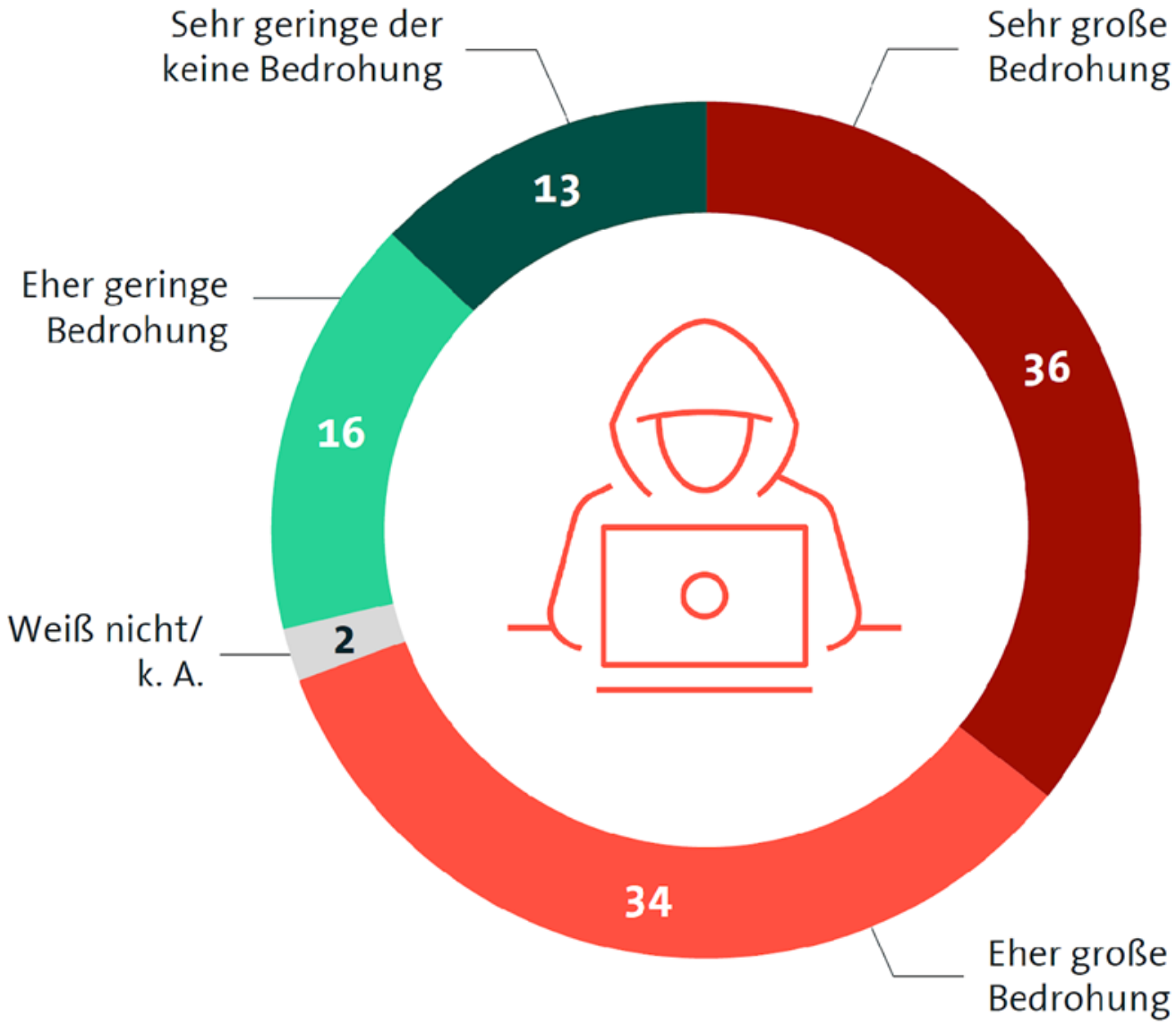

Cyber-Sicherheit
...geht das wieder weg???

7 von 10 Unternehmen fühlen sich stark durch analoge und digitale Angriffe bedroht

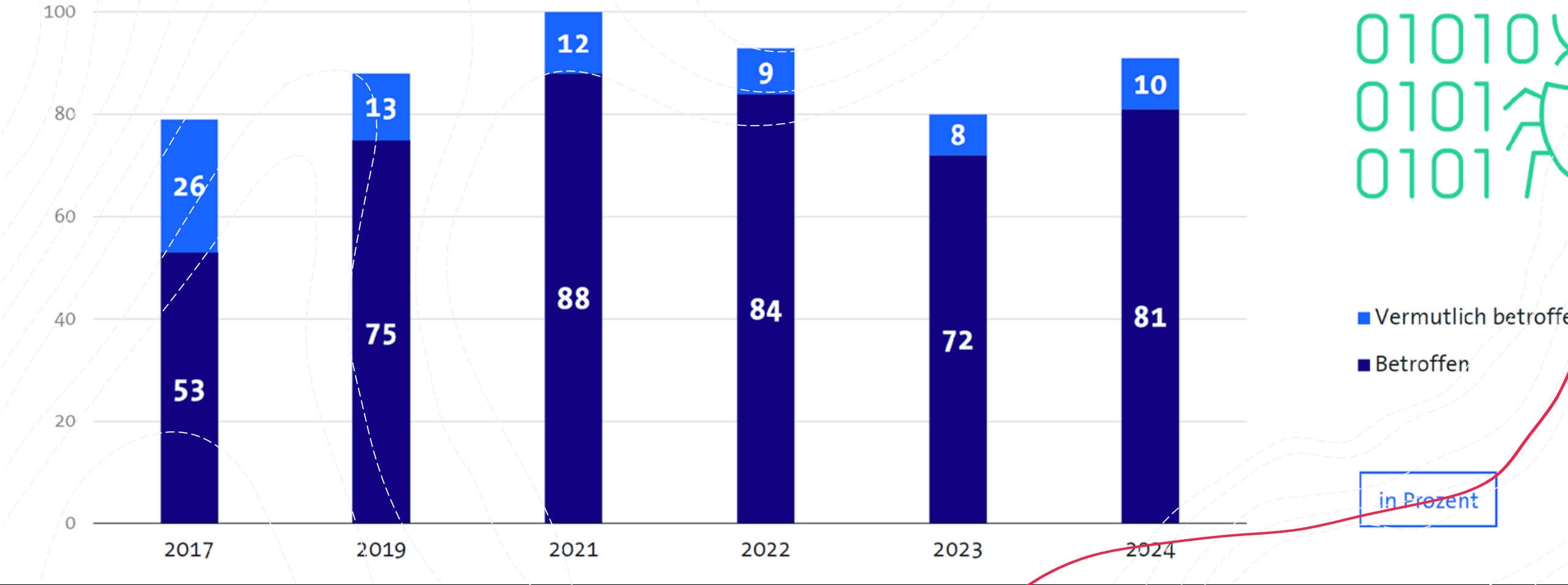
Inwieweit sehen Sie analoge und digitale Angriffe wie Datendiebstahl, Industriespionage und Sabotage als Bedrohung für Ihr Unternehmen?

in Prozent



Wieder mehr Unternehmen von Angriffen betroffen

War Ihr Unternehmen innerhalb der letzten 12 Monate* von Diebstahl, Industrie-spionage oder Sabotage betroffen?



Cyberattacken verursachen zwei Drittel der Schäden

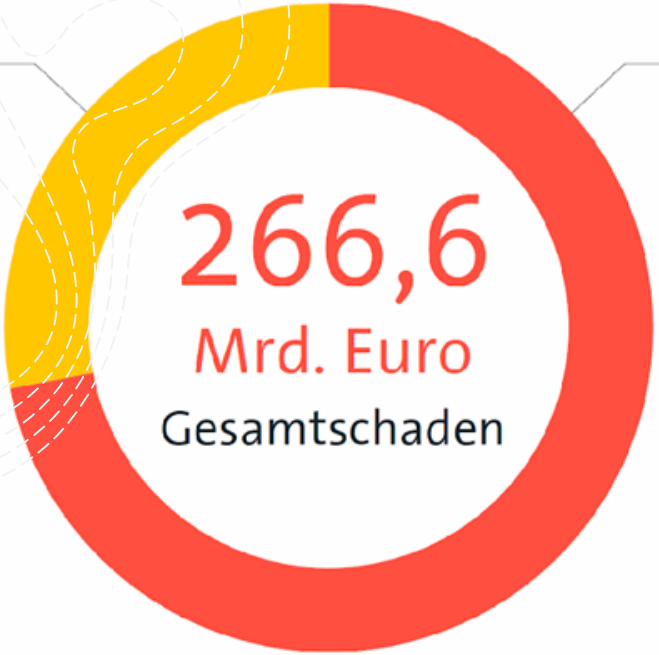
Wie hoch ist der prozentuale Anteil des entstandenen Gesamtschadens, der auf Cyberattacken zurückgeführt werden kann?

33%

88,0 Mrd. Euro

Andere Schäden

(2023: 57,7 Mrd. Euro)



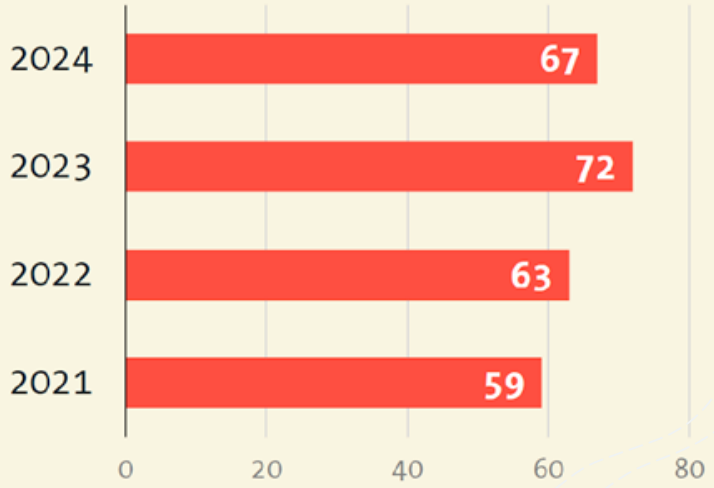
67%

178,6 Mrd. Euro

Cyberattacken

(2023: 148,2 Mrd. Euro)

Anteil Cyberattacken an Gesamtschäden 2021-24



Dora, NIS2UmsuCG, KRITIS-DachG, BDSG, OZG, DSGVO, EnWG, CRA, BSIG, TDDDG, CSA, GeschGehG, eIDAS 2.0, KI-Verordnung, Data Act, EnWG, BGB, TKG, DDG, AtomG, SGB V, RED, KI-Veraordnung, BSI-KRITS-VO

Was ist Cybersicherheit?

- Der Begriff Cybersicherheit bezieht sich auf alle Maßnahmen, die dem Schutz von kritischer IT-Infrastruktur, Netzwerken und Daten vor digitalen Angriffen dienen. Im Fokus der Cybersicherheit oder IT-Sicherheit steht die Abwehr aller digitalen Attacken aus internen oder externen Quellen, die zum Ziel haben, ohne Berechtigung auf Systeme oder Daten von Unternehmen zuzugreifen.

Risikofaktor Cyberkriminalität – Darum ist Cybersicherheit relevant

Die Zeiten, in denen Cyberkriminalität eine eher obskure Gefahr war, sind inzwischen vorbei. Wie aus einer Bitkom-Studie zum Thema Wirtschaftsschutz 2023 hervorgeht, hat sich die Anzahl der Cyberattacken auf Unternehmen zuletzt deutlich erhöht. Erstmals ist eine Mehrheit der befragten Unternehmen (52 %) der Ansicht, dass Cyberattacken ihre geschäftliche Existenz bedrohen. Gleichzeitig erwarten die Teilnehmer – in KRITIS-Sektoren und darüber hinaus – eine deutliche Zunahme an solchen digitalen Angriffen.

Vor dem Hintergrund, dass nicht nur der durch Cyberkriminalität verursachte Schaden, sondern auch der Professionalisierungsgrad der Angreifer kontinuierlich ansteigt, kommt dem Thema Cybersicherheit seit Jahren eine immer wichtigere Bedeutung zu. Dies gilt sowohl für Unternehmen im Bereich der kritischen Infrastruktur als auch für KMUs, die sich gegen potenziell gravierende Attacken von Hackern & Co. absichern möchten.

Wichtige Aspekte einer Cybersicherheitsstrategie

Informationssicherheit Allgemein verbindliche Regelungen innerhalb des Unternehmens, die den Umgang mit (vertraulichen) Informationen festlegen. Dies umfasst auch allgemeine Vorgaben zum Datenschutz oder die konsequente Umsetzung der DSGVO.

Netzwerksicherheit Geeignete Maßnahmen, die darauf abzielen, ein Netzwerk und die darin befindlichen Geräte vor unberechtigtem Zugriff zu schützen. Gesichert werden müssen dabei sowohl kabelgebundene als auch kabellose Netzwerk-Verbindungen.

App-Sicherheit Anwendungen müssen so ausgestaltet sein, dass sie die Sicherheit der Daten, auf die sie Zugriff bieten, nicht gefährden. Dies kann etwa erreicht werden, indem man Software-Anwendungen nach dem „Secure by design"-Leitsatz selbst entwickelt oder explizit hohe Sicherheitsanforderungen an Softwarelösungen Dritter formuliert.

Wichtige Aspekte einer Cybersicherheitsstrategie

Cloudsicherheit Greifen Unternehmen auf moderne (externe) Cloud-Dienste zurück, gelten auch hier identische Sicherheitsanforderungen wie im eigenen Netzwerk. Gerade bei Diensten Dritter müssen Unternehmen auf höchste Standards in Sachen Verschlüsselung setzen. Nur so können Anwendungen und Daten vor Zugriff, Änderung oder Löschung durch unberechtigte Dritte geschützt werden.

Disaster Recovery / BCM Relevante Zwischenfälle, die die IT-Sicherheit eines Unternehmens gefährden, reichen von Bränden im Rechenzentrum über Cyberangriffe bis hin zu Naturkatastrophen aller Größenordnungen. Mit einem Business Continuity & Disaster Recovery Plan werden im Vorfeld klare Leitlinien definiert, die dabei helfen, (digitale) Infrastruktur wiederherzustellen und den Betrieb aufrechtzuerhalten.

Mitarbeiter-Schulung / Awareness

Bei allen Erwägungen rund um das Thema Cybersicherheit nehmen die Endbenutzer eine zentrale Rolle ein. Unternehmen haben ein großes Interesse daran, Benutzer für das Thema zu sensibilisieren. Sie müssen darüber informiert sein, wie sie selbst zur IT-Sicherheit im Unternehmen beitragen können und welche möglichen Risiken sich aus vermeintlich banalen Handlungen (Öffnen eines E-Mail-Anhangs) ergeben können. Dies kann etwa auch im Rahmen eigenständiger Schulungen geschehen.

Arten von Cyberbedrohungen

+ Malware

ist „malicious software“, also Schadsoftware. Abhängig davon, welche Art von Software zum Einsatz kommt, kann diese erhebliche Schäden in der IT verursachen. Die Möglichkeiten reichen von Viren, die Dateien infizieren und beschädigen, über Trojaner, die Systeme von innen heraus schädigen, bis hin zu Spyware, die sich im Netzwerk einnistet und Daten abschöpft.

+ Ransomware

Ransomware (vom englischen Wort „ransom“ für „Lösegeld“) ist eine besonders perfide Art von Malware. Gelangt diese auf ein System, macht sie sich daran, die dort vorhandenen Daten zu verschlüsseln, sodass sie für Unternehmen unbrauchbar werden und nicht mehr zur Verfügung stehen. Ziel dieses Angriffs ist, eine Lösegeldzahlung von den betroffenen Unternehmen zu erpressen.

Arten von Cyberbedrohungen

+ Phishing

Bei Phishing-Versuchen werden Mails an Unternehmen versandt, die den Anschein erwecken sollen, von einem legitimen Absender zu stammen. Dies kann ein Geschäftskunde oder auch ein Dienstleister sein. Phishing zielt darauf ab, Anmeldeinformationen oder andere sensible Daten zu erbeuten, die man anschließend im Darknet verkaufen oder selbst nutzen kann

+ Social Engineering

Beim Social Engineering nutzen Cyberkriminelle Appelle an Mitleid, Angst, Vertrauen und weitere Emotionen, um positiven / negativen Druck auf Betroffene auszuüben. Vielfach werden hierzu auch Details zu den adressierten Einzelpersonen recherchiert, um diese gezielt anzusprechen. Im Fokus steht auch an dieser Stelle, Informationen bzw. sensible Daten von Betroffenen zu erhalten, um diese ggf. damit zu erpressen. Social Engineering ist häufig eine Facette von Phishing-Versuchen.

Volksbanken Raiffeisenbanken

Anpassung des Bankkontos

Sehr geehrte(r) Kunde/Kundin,

Durch den Jahreswechsel hat die Europäische Union uns Finanzinstitute den Auftrag gegeben Ihre Angaben abzugleichen und wenn notwendig zu aktualisieren.

Betroffen davon ist das neue PSD*2 Gesetz was besagt, dass diese jedes Neujahr stichprobenartig neu gewertet werden muss.

Wir Ihre Volks- und Raiffeisenbank sind bereits informiert.

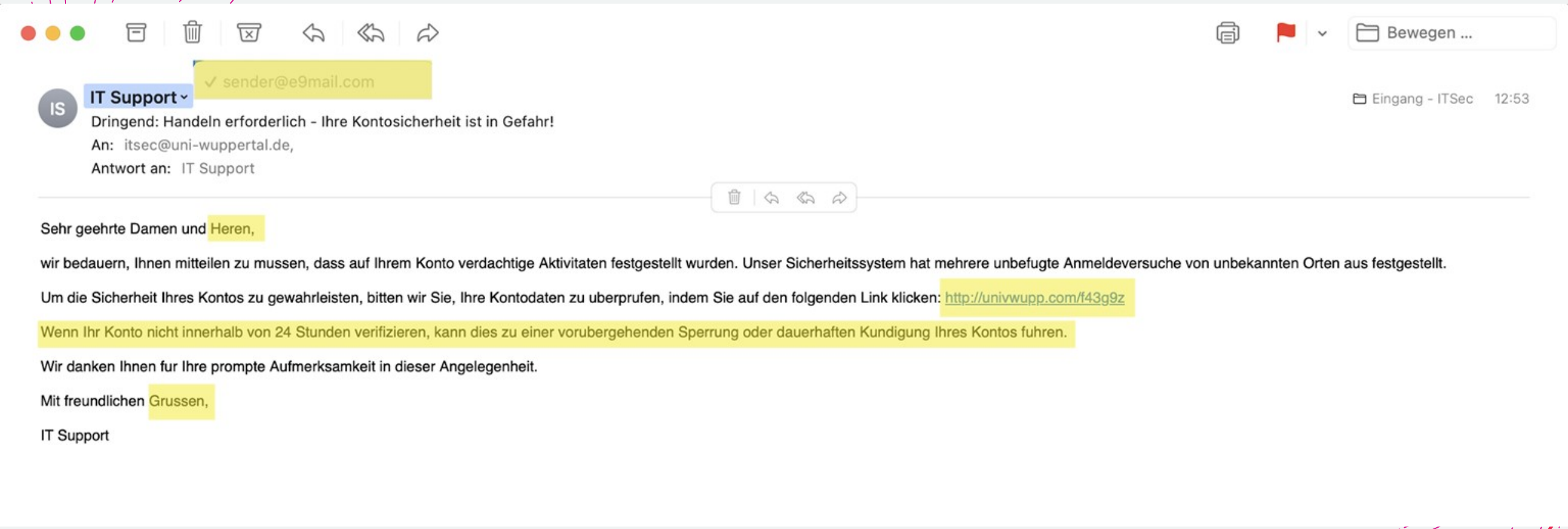
Nun bitten wir sie als wichtiger Kunde Ihre hinterlegten Informationen erneut zu verifizieren, damit unsere Bankmitarbeiter/In Ihre eingegeben Daten prüfen können.

Zur Aktualisierung

Einen schönen Tag noch und beste Grüße Ihr Volksbank-Raiffeisenbank Sicherheits-Services

Viele Grüße und viel Erfolg im neuen Jahr!

Wir danken ihre Zeit und wünschen ihnen Alles Gute!


Bewegen ...
✓ sender@e9mail.com
IS
IT Support
Eingang - ITSec 12:53
Dringend: Handeln erforderlich - Ihre Kontosicherheit ist in Gefahr!
An: itsec@uni-wuppertal.de,
Antwort an: IT Support
Sehr geehrte Damen und Heren,
wir bedauern, Ihnen mitteilen zu mussen, dass auf Ihrem Konto verdachtige Aktivitaten festgestellt wurden. Unser Sicherheitssystem hat mehrere unbefugte Anmeldeversuche von unbekannten Orten aus festgestellt.
Um die Sicherheit Ihres Kontos zu gewahrleisten, bitten wir Sie, Ihre Kontodaten zu uberprufen, indem Sie auf den folgenden Link klicken: http://univwupp.com/f43g9z
Wenn Ihr Konto nicht innerhalb von 24 Stunden verifizieren, kann dies zu einer vorubergehenden Sperrung oder dauerhaften Kundigung Ihres Kontos fuhren.
Wir danken Ihnen fur Ihre prompte Aufmerksamkeit in dieser Angelegenheit.
Mit freundlichen Grussen,
IT Support

Abrufen | Verfassen | Schlagwörter | Schnellfilter

Von noreply@deutschebank.de <dev@tectech.jp>

An [redacted]

Betreff **Neue Informationen. #1423430362**

Deutsche Bank

Sehr geehrter Kunde,

es ist uns aufgefallen, dass Ihnen momentan der Zugriff
auf Ihr Online-Banking-Konto nicht möglich ist.
Um dieses Problem zu beheben, benötigen wir von Ihnen ein Dokument,
das noch fehlt.

Bitte loggen Sie sich in Ihren persönlichen Bereich ein,
indem Sie auf folgenden Link klicken:

Anmelden

Dort finden Sie den Abschnitt zur Dokumentenübermittlung.
Wir benötigen von Ihnen eine Kopie eines fehlenden Dokuments,
um Ihre Identität zu bestätigenund den Zugriff auf Ihr Online-Banking-Konto
wiederherzustellen.

Sobald wir das Dokument von Ihnen erhalten haben, werden wir Ihre Identität
prüfen und Ihnen umgehend den Zugriff auf Ihr Konto wiederherstellen.
Sollten Sie weitere Fragen oder Probleme haben, zögern Sie bitte nicht,
uns zu kontaktieren.

Wir danken Ihnen für Ihre Kooperation und stehen Ihnen gerne zur Verfügung,
falls Sie weitere Unterstützung benötigen.

Mit freundlichen Grüßen,

DEUTSCHE BANK AG

https://kolkokla.s3.amazonaws.com/iksla.html

Hallo [redacted]

Ihre Mithilfe ist erforderlich!

Die neuen Datenschutzgesetze verpflichten uns nun dazu, in regelmäßigen Abständen die Konten unserer Kunden zu überprüfen. Dies dient ausschließlich zu Ihrer eigenen Sicherheit, da in der Vergangerheit immer mehr Vorfälle von Benutzung verschiedener Kundenkonten durch unbefugte Personen entstanden sind.

Um daher wie gewohnt weiterhin Ihr Konto bei uns nutzen zu können, ist Ihre aktive Mitwirkung erforderlich. Dies wird vom Gesetzgeber so verlangt.

Nachdem Sie sich über den Bestätigungsbutton angemeldet haben, werden Ihnen detailiert alle weiteren notwendigen Schritte erklärt.

Bestätigen

Bei Misachtung oder Verweigerung ist ganz klar eine Schließung des Kundenkontos vorgesehen. Der Gesetzgeber fordert in so einem Fall dazu auf.

Vielen Dank im voraus für Ihre Mitwirkung und Ihr Verständnis!

Mit freundlichen Grüßen
Ihr PayPal Kundensupport

Rechnung fehlgeschlagen - Konto gesperrt

NETFLLIX

Hi [redacted]

Wir haben Probleme mit Ihren aktuellen Rechnungsinformationen. Wir werden es erneut versuchen, aber in der Zwischenzeit möchten Sie möglicherweise Ihre MASTERCARD in Ihren Zahlungsdetails aktualisieren.

JETZT KONTO AKTUALISIEREN

Wir sind hier, um Ihnen zu helfen, wenn Sie es brauchen. Besuche den Hilfezentrum für mehr info oder kontaktiere uns.

Deine Freunde bei Netflix


Cyber-Sicherheit
...und nun?

Tipps zur Umsetzung

- **Updates** Veraltete Software kann einen wesentlichen Risikofaktor für die Cybersicherheit von Unternehmen darstellen. Häufig fehlen hier wichtige Sicherheitsupdates, was eine ideale Angriffsfläche für Kriminelle bietet. Besonders Virenschutzprogramme sollten immer über die neueste Software-Version verfügen, damit Schadsoftware zuverlässig sowie schnell erkannt und beseitigt werden kann. Ein gern genutztes Modell ist hier das Hosting – wesentliche Updates werden direkt bereitgestellt und kritische Updates erfolgen automatisch.
- **MFA / Passkeys** Passwörter, die etwa aus einfachen Begriffen oder kurzen Zahlenfolgen bestehen, stellen ein erhebliches Sicherheitsrisiko dar. Passwörter sollten angemessen komplex sein und dabei einen Mix aus Groß- und Kleinschreibung, Zahlen sowie Sonderzeichen enthalten. Lösen Sie wo möglich die Anmeldung durch MFA oder Passkeys

Tipps zur Umsetzung

- **E-Mails** sind häufig das Einfallstor für alle Arten von Cyberangriffen. Daher sollten Mails, gerade solche von unbekannten Absendern, immer mit Vorsicht und Skepsis gehandhabt werden. E-Mail-Anhänge sollten nur dann geöffnet werden, wenn Sicherheit über die Identität des Absenders besteht. Gleiches gilt für das Anklicken von Links. Im Interesse der Cybersicherheit ist es im Zweifel ratsam, direkten Kontakt mit dem vermeintlichen Absender aufzunehmen, um die Echtheit der Mail zu verifizieren.
- **Trends kennen** Um Angriffen auf die Unternehmens-IT vorzubeugen, ist es sinnvoll, sich über „Trends“ im Bereich der Cyberkriminalität zu informieren. Welche Arten von Angriffen finden aktuell besonders häufig statt, vielleicht auch in Bezug auf eine bestimmte Branche? Dies umfasst explizit auch, wesentliche Informationen zu möglichen Cyberangriff-Szenarien unternehmensweit bekannt zu machen.