Cyberversicherung für Privatkunden

Erkenntnisse eines Markteinstiegs von Vertrieb bis Schaden

Debeka

Das **Füreinander** zählt.

Agenda

1. Vorstellung der DEBEKA Gruppe
2. Überblick Versicherungsmarkt
3. Gefahren für Privatkunden
4. Debeka Cyberversicherung
5. Schadensfälle und Rechtsfragen

1.

Vorstellung der Debeka Gruppe

DEBEKA GRUPPE

Hauptverwaltung Koblenz

seit 1905

7,7 Mio.
Mitglieder (2024)

21,7 Mio.
Verträge

16.372
Mitarbeitende

240
Geschäftsstellen

15,5 Mrd. €
Bruttobeiträge (2024)

DEBEKA ALLGEMEINE

Platz 22 unter 211 der deutschen Schaden- und Unfallversicherern

- Unfallversicherung
- Haftpflichtversicherung
- Rechtsschutzversicherung
- Kraftfahrtversicherung
- Fahrradversicherung
- Hausratversicherung
- Glasversicherung
- Wohngebäudeversicherung
- Reiseversicherung
- Gewerbeversicherungen

2.

Überblick Versicherungsmarkt

Marktstatus Cyberversicherung für Privatpersonen

mehr als 50% der Internetnutzer werden Opfer von Cyberkriminalität

nur 14 Versicherer bieten eigenständige Tarife an

viele Produkte unzureichend oder nur als Bausteine

Inhaltliche Orientierung u. a. an einer Analyse von „Franke & Bornberg“

Marktstatus Cyberversicherung für Privatpersonen

Verbraucherschutz und Transparenz

- Produkte oft als Zusatzbaustein konzipiert -> erhöhtes Risiko von Unklarheiten über Umfang und Grenzen des Versicherungsschutzes
- Durch fehlende Transparenz und Unklarheiten wird auch ein eigenständiger Vergleich erschwert
- Keine GDV-einheitlichen Musterbedingungen führen zu heterogenem Marktangebot

Deckungslücken

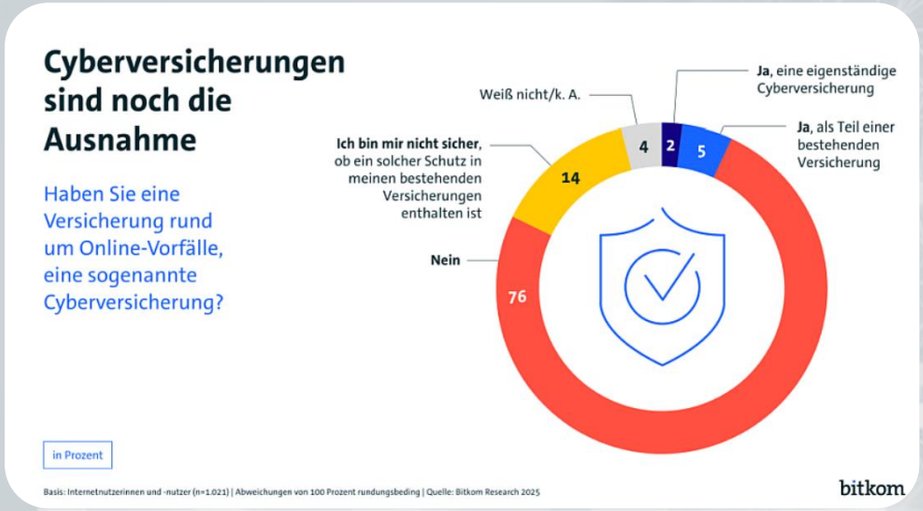
- Risiken oft gar nicht oder mit zu niedrigen Summen versichert
- Deckungslücken im Schadenfall -> höhere finanzielle Belastung für Kunden

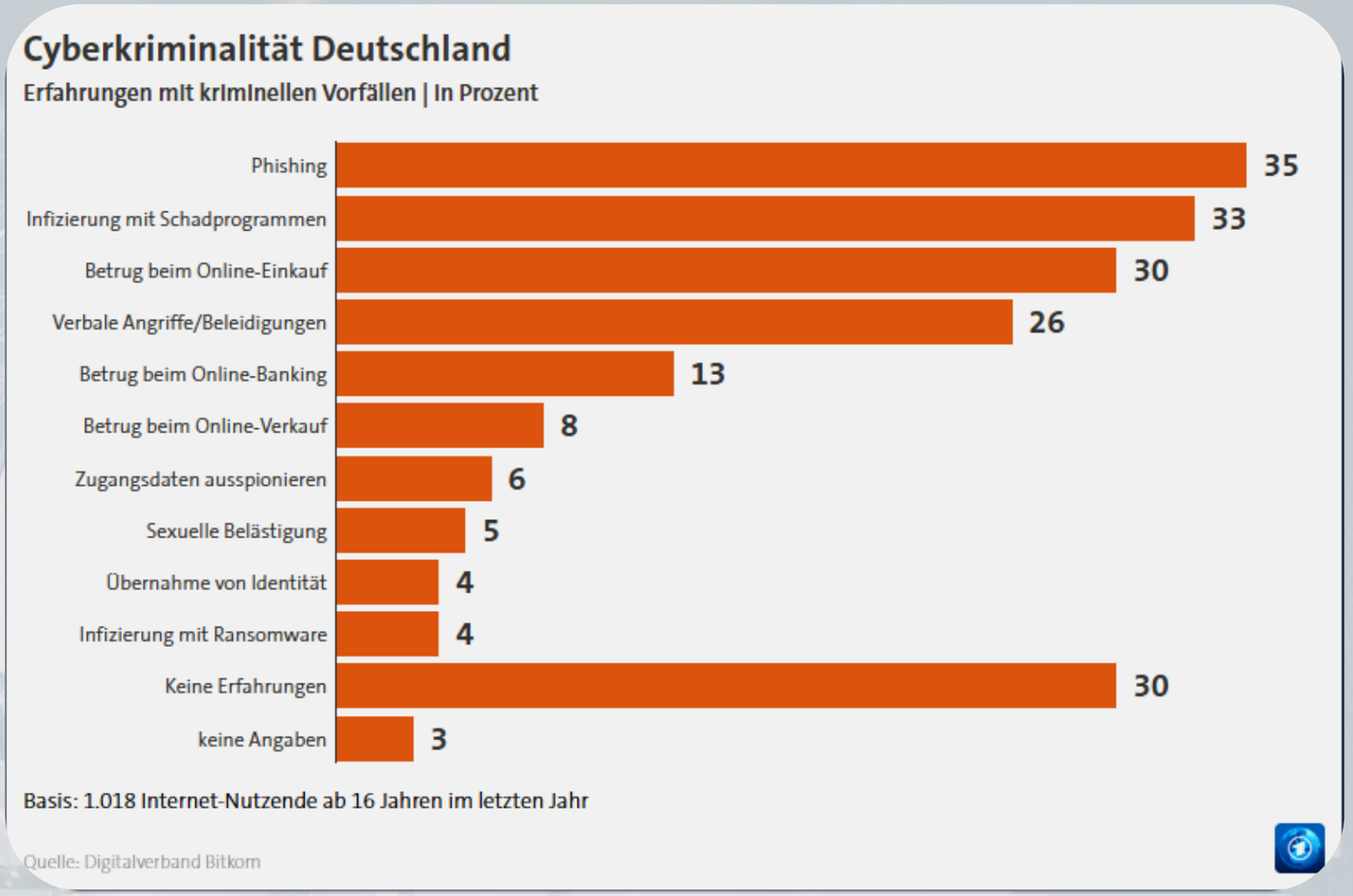
  + Streitigkeiten mit Unternehmen

3.

Gefahren für Privatkunden

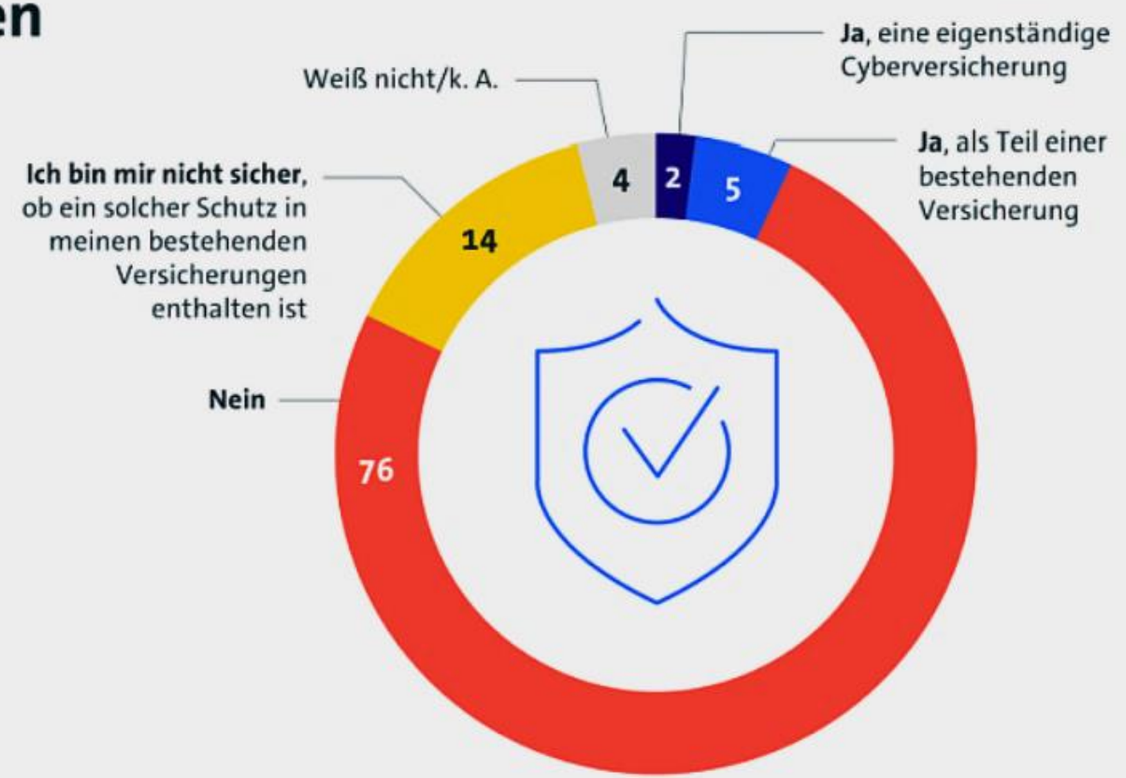
GEFAHREN FÜR PRIVATKUNDEN





Cyberversicherungen sind noch die Ausnahme

Haben Sie eine Versicherung rund um Online-Vorfälle, eine sogenannte Cyberversicherung?



in Prozent

Basis: Internetnutzerinnen und -nutzer (n=1.021) | Abweichungen von 100 Prozent rundungsbeding | Quelle: Bitkom Research 2025

bitkom

Moderne Angriffsmethoden und ihre Risiken

Kaspersky (2025): „Cybersicherheitstrends 2026 – KI-gestützte Angriffe und Verteidigungsmethoden".

Sophos X-Ops (2025): „2025 geht, 2026 kommt – Rück- und Ausblick in Sachen Cyberkriminalität".

Warum es immer gefährlicher wird

KI-gestütztes Phishing

Künstliche Intelligenz erzeugt täuschend echte Nachrichten und Stimmen, wodurch Social Engineering glaubwürdiger wird.

QR-Code-Phishing (Quishing)

Manipulierte QR-Codes auf Alltagsobjekten führen Opfer auf gefälschte Loginseiten zur Datendiebstahl.

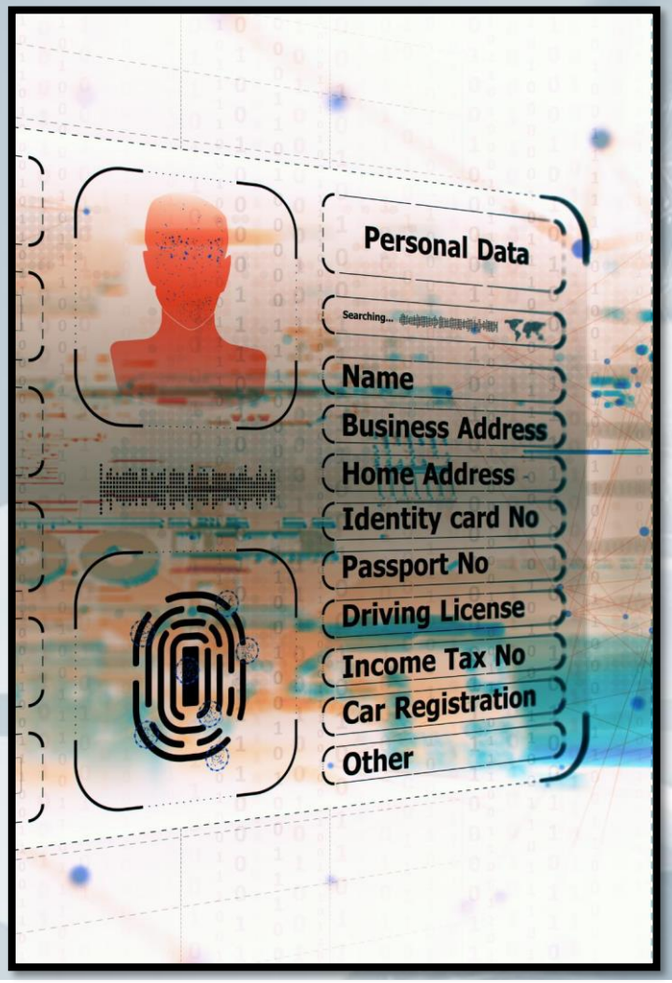
MFA-Müdigkeit

Nutzer werden durch viele Multi-Faktor-Anfragen überflutet und erteilen versehentlich Zugriffsrechte.

Soziale Ingenieurskunst als Dienstleistung

Professionelle Betrüger bieten KI-Stimmimitationen und komplexe Betrugsabläufe als Service an.

Starkiller - Morderne Phishing-Gefahren



Warum Starkiller so gefährlich ist

Phishing-as-a-Service Modell

Starkiller ermöglicht einfachen Zugang zu professionellen Phishing-Angriffen durch ein benutzerfreundliches SaaS-Dashboard mit Support und Updates.

Echtzeit Proxy-Technologie

Starkiller leitet Nutzerinteraktionen direkt über echte Login-Seiten, wodurch keine sichtbaren Fälschungsmerkmale entstehen.

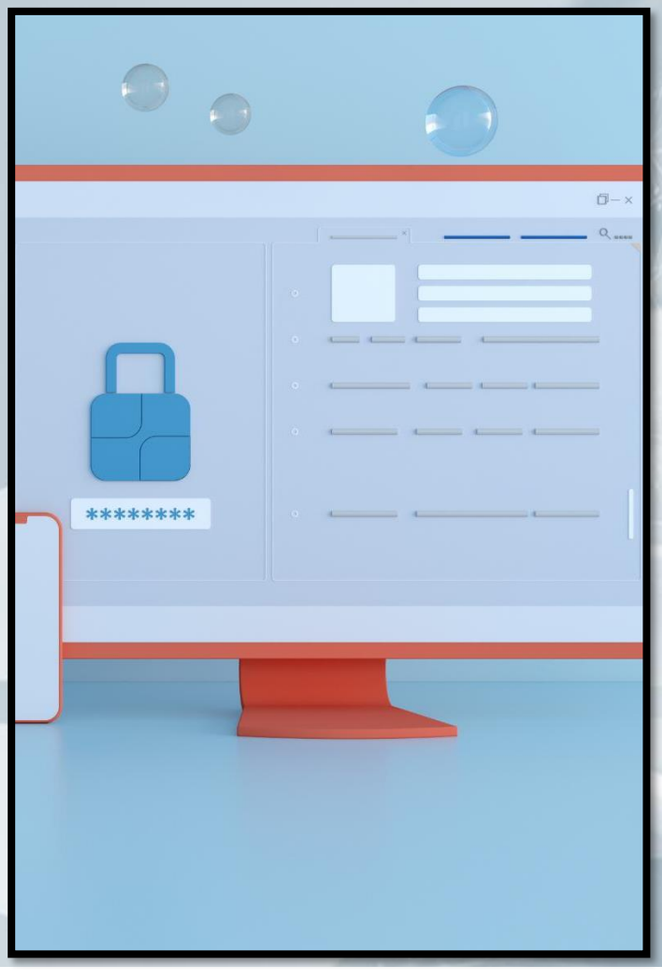
Umgehung der Multi-Faktor-Authentifizierung

Das Toolkit fängt MFA-Codes und Push-Bestätigungen ab, um vollständigen Zugriff auf geschützte Konten zu ermöglichen.

Breite Plattformunterstützung

Starkiller imitiert realistisch große Plattformen wie Microsoft 365, Google und Banken, was Kontenübernahmen erleichtert.

Starkiller - Morderne Phishing-Gefahren



Ablauf eines Angriffs

Täuschend echte Links

Angreifer nutzen gefälschte Links mit legitimen Domainnamen vor dem @-Zeichen, um Opfer zu täuschen.

Live-Proxy und Headless Browser

Ein Reverse-Proxy mit Headless Chrome lädt die echte Website in Echtzeit und zeigt sie dem Opfer.

MFA und Session Hijacking

Der Angreifer fängt MFA-Codes ab und erlangt vollständigen Kontozugriff durch Echtzeit-Weiterleitung.

Keylogging und Live-Monitoring

Starkiller erlaubt das Überwachen aller Eingaben und Interaktionen des Opfers unbemerkt.

Starkiller - Morderne Phishing-Gefahren

Warum Starkiller kaum erkennbar ist und wie man sich schützt

Schwierige Erkennung von Starkiller

Starkiller lädt die echte Login-Seite in Echtzeit, wodurch typische Phishing-Warnsignale verschwinden.

Begrenzte Wirksamkeit von MFA

Multi-Faktor-Authentifizierung schützt kaum, da Angreifer MFA-Codes als Durchlaufposten missbrauchen.

Wichtige Schutzmaßnahmen

Manuelle URL-Eingabe, Passkeys, FIDO2 und Awareness sind entscheidend für den Schutz.

Gesellschaftliche Relevanz

Veränderte Erwartungen durch Privatpersonen durch die fortschreitende Digitalisierung

- Ein Großteil des Alltags findet heute online statt: Shopping, Kommunikation, Banking.

Gesellschaftliches Sicherheitsniveau hält nicht mit der Geschwindigkeit der digitalen Entwicklung mit:

- Deutliche Defizite in der Cyber-Resilienz bei Privatpersonen.

Bedrohung durch Cyberrisiken wächst rasant und viele Menschen wiegen sich in falscher Sicherheit.

- Cybermobbing, Identitätsdiebstahl oder Phishing sind bereits Teil der Lebensrealität.

Cyberkriminalität betrifft uns alle – unabhängig von Alter, Einkommen oder digitaler Kompetenz

Der private Cybermarkt **hinkt** dem tatsächlichen Risiko noch **hinterher**. Es fehlt an **breiten, leistungsfähigen, eigenständigen Tarifen** - trotz stark wachsender Bedrohungslage.

4.

Debeka Cyberversicherung


Cyberversicherung
IHRE DIGITALE SICHERHEIT.
UNSERE PRIORITÄT.
Debeka

LEISTUNGEN DER Debeka CYBERVERSICHERUNG

CYBER-PRÄVENTION
EIGENSCHADENSABSICHERUNG
inkl. umfangreicher Assistance

- ✓ IT-Assistance
- ✓ Digitaler Nachlass
- ✓ Anti-Betrugs-Assistent
- ✓ Cloud zur Datensicherung
- ✓ Datenrettung
- ✓ Online-Shopping
- ✓ Cyber-Mobbing
- ✓ Reputationsschutz
- ✓ Identitätsdiebstahl

CYBER-HAFTPFLICHT
Drittschadensabsicherung - modern und inklusive

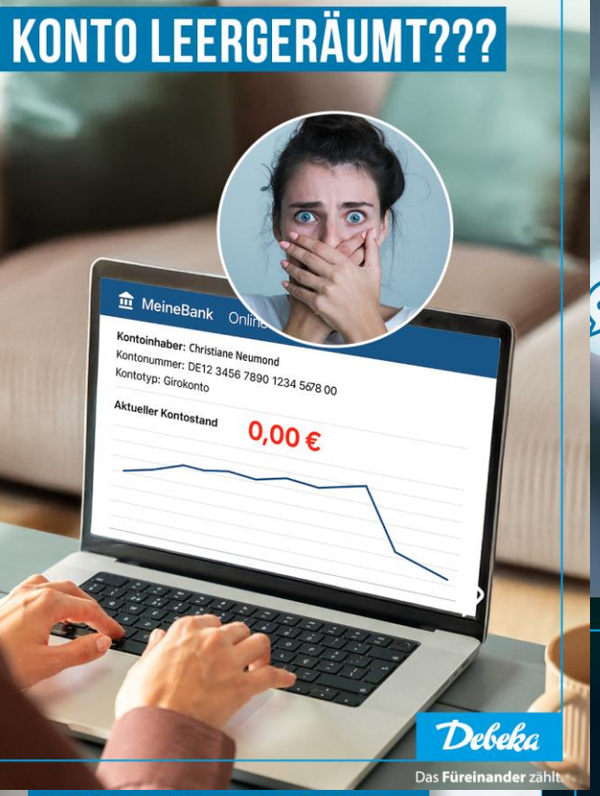
- ✓ Übermittlung von Schadprogrammen
- ✓ Verletzung datenschutzrechtlicher Bestimmungen
- ✓ Verletzung urheberrechtlicher Bestimmungen
- ✓ Vertraulichkeits-/Persönlichkeitsrechtsverletzungen

OPTIONAL

CYBER-RECHTSSCHUTZ
attraktive Zusatzabsicherung

- ✓ Telefonische Rechtsberatung
- ✓ Rechtsschutz im Vertrags- und Sachenrecht
- ✓ Schadensersatz-Rechtsschutz
- ✓ Straf-Rechtsschutz
- ✓ Beratungs-Rechtsschutz bei Urheberrechtsverstößen
- ✓ Aktiver Straf-Rechtsschutz

KONTO LEERGERÄUMT???



Debeka
Das Füreinander zählt

DIGITALE RISIKEN BETREFFEN UNS ALLE:

- Betrug beim Onlineshopping
- Phishing-Attacken
- Cybermobbing
- Datenverlust

WIE KANN ICH MICH DAGEGEN SCHÜTZEN?

2024 GAB ES IN DEUTSCHLAND 131.391 GEMELDETE FÄLLE VON CYBER-KRIMINALITÄT.

DATENKLAU WAS JETZT?!

AUF EINEN FAKE-SHOP REINGEFALLEN??

SCHÜTZE DEIN KIND VOR CYBERMOBBING!

Cyberversicherung

KLEINER KLICK, GROSSES DRA

- Schutz bei Cyberangriffen
- Für dich und deine ganze Famil
- Ersatz bei Online-Betrug und

UNSERE LÖSUNG

Cyber funktioniert, wenn Fachbereich, IT, Marketing und Vertrieb konsequent zusammenarbeiten.

Das Thema Cyber hat eine hohe gesellschaftliche Relevanz.

Debeka
Cyberversicherung

Das zunehmende Schadensvolumen unterstreicht den Absicherungsbedarf.

Es gibt viele Kundenkontaktpunkte und ein hohes Interesse auf Kundenseite.

5.

Schadensfälle und Rechtsfragen

Ich möchte meine wichtigen Daten in einer Cloud speichern können…

Meine Daten wurden über einen Link abgefangen…

Mein Kind wurde Opfer von Cybermobbing…

Mir wird eine Urheberrechtsverletzung vorgeworfen…

Mein WLAN verbindet sich nicht richtig…

Mein Drucker druckt nicht mehr und zeigt eine Fehlermeldung…

Ich habe ein Forderungsschreiben erhalten, obwohl ich bei dem Online Shop nie eingekauft habe…

Ich habe Schulbücher auf eBay verkauft, das Geld aber nie erhalten…

Jemand buchte in meinem Namen online Reisen…

Ist mein Laptop noch sicher, wenn ich keine Updates mehr machen kann?

Ich habe einen Laptop auf Kleinanzeigen gekauft, aber nie erhalten…

Ich habe eine seltsame E-Mail erhalten, kann ich den Anhang öffnen?

Worauf muss ich achten, wenn ich das neue Windows Update mache?

Nachdem mein Handy gehackt wurde, sind viele persönliche Daten verschwunden…

Ich habe in meinem Online Banking komische Abbuchungen entdeckt…

Erste Schadenserfahrungen – Cyber Eigenschaden

- ✓ **Verlust bei Interneteinkäufen**
- Produktkauf über eBay
- Verkäufer abgetaucht, kein Erhalt der Ware
- Nachweise bei Schadensmeldung: Chatverläufe, polizeiliche Anzeige, Zahlungsnachweis

C 1 Schutz bei Interneteinkäufen

C 1.1 Was ist versichert?

Versicherungsschutz besteht für die Nicht- oder Falschlieferung von über das Internet gekauften Waren sowie für den Fall, dass die Ware beschädigt oder zerstört bei Ihnen ankommt.

Dabei versichert sind im Internet gekaufte Waren mit einem Kaufpreis ab 50 Euro pro Bestellung, die dem persönlichen (nicht dem gewerblichen oder beruflichen) Gebrauch dienen. Sie müssen in einem Zahlungsvorgang vollständig bezahlt worden sein (kein Ratenkauf oder Leasing). Als Waren gelten auch Veranstaltungstickets (z. B. Theater-, Musical- oder Konzertkarten). Versichert sind ebenfalls Privatkäufe (z. B. über Kleinanzeigen-Portale).

Erste Schadenserfahrungen – Cyber Eigenschaden

✓ **Kreditkartenmissbrauch (Phishing)**

- Kauf von Schulbüchern über Kleinanzeigen, Bezahlung mit Bezahlfunktion von Kleinanzeigen
- Zusendung eines falschen Links, Abfangen der Kreditkarten Daten
- Daten genutzt für Buchungen „booking.com“

C 3 Finanzschutz nach Identitätsmissbrauch

C 3.1 Was ist versichert?

Versichert ist, wenn ein Dritter unberechtigt Ihre persönlichen Daten erlangt, damit Ihre Identität vortäuscht und Sie dadurch einen Vermögensschaden erleiden.

Versichert ist, im Zusammenhang mit Ihren Privatkonten, z. B. der Missbrauch

- Ihrer privat genutzten Zahlungskarte (z. B. EC-Karte/Girokarte, Debitkarte, Kreditkarte oder Kundenkarte mit Zahlungsfunktion),
- Ihrer Karten-/Kontodaten bei (Online-)Bezahlvorgängen,

beim Online-Banking oder E-Payment (Nutzung sonstiger Online-Bezahlsysteme mit Bank-Funktion, z. B. PayPal, Apple-Pay): Ein Dritter verschafft sich rechtswidrig während Ihres Online-Bankings bzw. Online-Bezahlvorgangs am eigenen Laptop/PC oder mobilen Endgerät (z. B. Tablet, Smartphone) Ihre persönlichen Daten,

durch Pharming: Sie werden auf eine betrügerische Webseite umgeleitet. Dort geben Sie arglos Ihre Daten ein. Ein Dritter erfasst die eingegebenen sensiblen Informationen wie Benutzernamen, Passwörter, Kreditkartendaten etc. Anschließend begeht der Dritte unter Ihrer Identität betrügerische Aktivitäten meist finanzieller Art oder greift auf andere Online-Konten zu. Mehrere Schäden stellen hierbei einen Versicherungsfall dar, wenn sie auf einem Pharming-Angriff beruhen, bei dem der Dritte mehrere Zugangs- und Identifikationsdaten von Ihnen erlangt hat.

Erste Schadenserfahrungen – Cyber Eigenschaden

Finanzschutz nach Identitätsmissbrauch

Ablauf

- Anruf der "Bank" (Abteilung IT-Sicherheit)
- Hinweis auf verdächtige Abbuchungen (**21.900 Euro**)
- Installation angeblicher Antivirensoftware
- Täter überzeugte VN durch persönliche Daten der Ehefrau
- Freigabe per Photo-TAN
- Kein Rückruf, VN entdeckt Schaden
- Konto gesperrt, Anzeige erstattet

Bank lehnt den Schaden wegen autorisiertem Überweisungsauftrag durch den Kunden ab.

Haftungsgrenzen von Banken bei Kontomissbrauch

Einlagensicherungsrichtlinie (2014/49/EU)?

- **§ 675u BGB:** nicht autorisierte Zahlungen müssen erstattet werden
- **§ 675v BGB:** Kunde haftet nur bei grob fahrlässigem Verhalten oder Vorsatz
- **§ 675w BGB:** Beweislast liegt bei der Bank
- **§ 675l BGB:** Schutzpflicht des Nutzers

Rechtssprechung (Phishing / Online-Banking)

1. **BGH – XI ZR 107/22**: *Grundsatzentscheidung zur Beweislast bei unautorisierten Zahlungen*
   - verschiebt Rechtslage zugunsten der Verbraucher
2. **OLG Dresden – 8 U 760/22**: *autorisierte, aber ungewollte Zahlung, Kunde fällt auf „Kontoverifizierung“ rein*
   - keine Erstattung, aufgrund eigenständiger Freigabe
3. **OLG Dresden - 8 U 1482/24**: *autorisierte Zahlung, aber Bank verstößt gegen Sicherheitsvorgaben*
   - Teilhaftung der Bank

Haftungsgrenzen von Banken bei Kontomissbrauch

Bürgerliches Gesetzbuch (BGB)
§ 675w Nachweis der Authentifizierung

Ist die Autorisierung eines ausgeführten Zahlungsvorgangs streitig, hat der Zahlungsdienstleister nachzuweisen, dass eine Authentifizierung erfolgt ist und der Zahlungsvorgang ordnungsgemäß aufgezeichnet, verbucht sowie nicht durch eine Störung beeinträchtigt wurde. Eine Authentifizierung ist erfolgt, wenn der Zahlungsdienstleister die Nutzung eines bestimmten Zahlungsinstruments, einschließlich seiner personalisierten Sicherheitsmerkmale, mit Hilfe eines Verfahrens überprüft hat. Wurde der Zahlungsvorgang mittels eines Zahlungsinstruments ausgelöst, reicht die Aufzeichnung der Nutzung des Zahlungsinstruments einschließlich der Authentifizierung durch den Zahlungsdienstleister und gegebenenfalls einen Zahlungsauslösedienstleister allein nicht notwendigerweise aus, um nachzuweisen, dass der Zahler

1. den Zahlungsvorgang autorisiert,
2. in betrügerischer Absicht gehandelt,
3. eine oder mehrere Pflichten gemäß § 675l Absatz 1 verletzt oder
4. vorsätzlich oder grob fahrlässig gegen eine oder mehrere Bedingungen für die Ausgabe und Nutzung des Zahlungsinstruments verstoßen

hat. Der Zahlungsdienstleister muss unterstützende Beweismittel vorlegen, um Betrug, Vorsatz oder grobe Fahrlässigkeit des Zahlungsdienstnutzers nachzuweisen.

Bürgerliches Gesetzbuch (BGB)
§ 675v Haftung des Zahlers bei missbräuchlicher Nutzung eines Zahlungsinstruments

(3) Abweichend von den Absätzen 1 und 2 ist der Zahler seinem Zahlungsdienstleister zum Ersatz des gesamten Schadens verpflichtet, der infolge eines nicht autorisierten Zahlungsvorgangs entstanden ist, wenn der Zahler

1. in betrügerischer Absicht gehandelt hat oder
2. den Schaden herbeigeführt hat durch vorsätzliche oder grob fahrlässige Verletzung
   a) einer oder mehrerer Pflichten gemäß § 675l Absatz 1 oder
   b) einer oder mehrerer vereinbarter Bedingungen für die Ausgabe und Nutzung des Zahlungsinstruments.

Bürgerliches Gesetzbuch (BGB)
§ 675l Pflichten des Zahlungsdienstnutzers in Bezug auf Zahlungsinstrumente

(1) Der Zahlungsdienstnutzer ist verpflichtet, unmittelbar nach Erhalt eines Zahlungsinstruments alle zumutbaren Vorkehrungen zu treffen, um die personalisierten Sicherheitsmerkmale vor unbefugtem Zugriff zu schützen. Er hat dem Zahlungsdienstleister oder einer von diesem benannten Stelle den Verlust, den Diebstahl, die missbräuchliche Verwendung oder die sonstige nicht autorisierte Nutzung eines Zahlungsinstruments unverzüglich anzuzeigen, nachdem er hiervon Kenntnis erlangt hat. Für den Ersatz eines verlorenen, gestohlenen, missbräuchlich verwendeten oder sonst nicht autorisiert genutzten Zahlungsinstruments darf der Zahlungsdienstleister mit dem Zahlungsdienstnutzer ein Entgelt vereinbaren, das allenfalls die ausschließlich und unmittelbar mit dem Ersatz verbundenen Kosten abdeckt.

Schutzpflicht:
Sicherer Umgang mit dem Zahlungsinstrument

- **Geheimhaltung von PIN/TAN** (keine Weitergabe, auch nicht an angebliche „Bankmitarbeiter“)
- **sichere Verwahrung** von Karte, TAN-Generator etc.
- **keine Aufzeichnung der PIN** zusammen mit der Karte
- **keine Nutzung unsicherer Geräte** für das Online-Banking
- **sofortige Aktualisierung von Sicherheitssoftware**

OLG Dresden – 8 U 760/22

Fall

- ungewollter Zahlungsvorgang nach **Man-in-the-Middle-Attacke** beim ChipTAN-Verfahren
- Kundin überweist „Verifizierungs-Cent“ → Betrüger lösen später Zahlung über 7.572,60 € aus.

▶ **Entscheidung des OLG Dresden:** Klage abgewiesen – Bank muss nichts erstatten.
Zahlung gilt als autorisiert, da Kundin den TAN-Prozess selbst ausgelöst hat.

▶ **Rechtliche Einordnung:**
Autorisierung nach *§ 675j BGB* liegt vor, wenn Kunde TAN aktiv bestätigt
OLG beruft sich insbes. auch auf *§ 675 Abs. 3 Nr. 2b BGB* (Haftung des Zahlers bei grober Fahrlässigkeit)

▶ **Grobe Fahrlässigkeit der Kundin:** Nach Auffassung des Gerichts hätte die Kundin die ungewöhnliche Aufforderung („1-Cent-Verifizierung“) erkennen müssen.

Gericht: **Unachtsamkeit** ermöglichte den Betrug erst.

Deckungskomponenten der Cyber-Haftpflicht

Informationssicherheitsverletzung

- Ungewollte Übermittlung von Schadprogrammen
- Verletzung datenschutzrechtl. Bestimmungen
- Verletzung urheberrechtlicher Bestimmungen
- Vertraulichkeitsverletzung

Erste Schadenserfahrungen – Cyber Haftpflicht

Urheberrechtsverletzung

Schreiben von Anwaltskanzlei – beauftragt von einem großen Medien- und Unterhaltungskonzern

Vorwurf

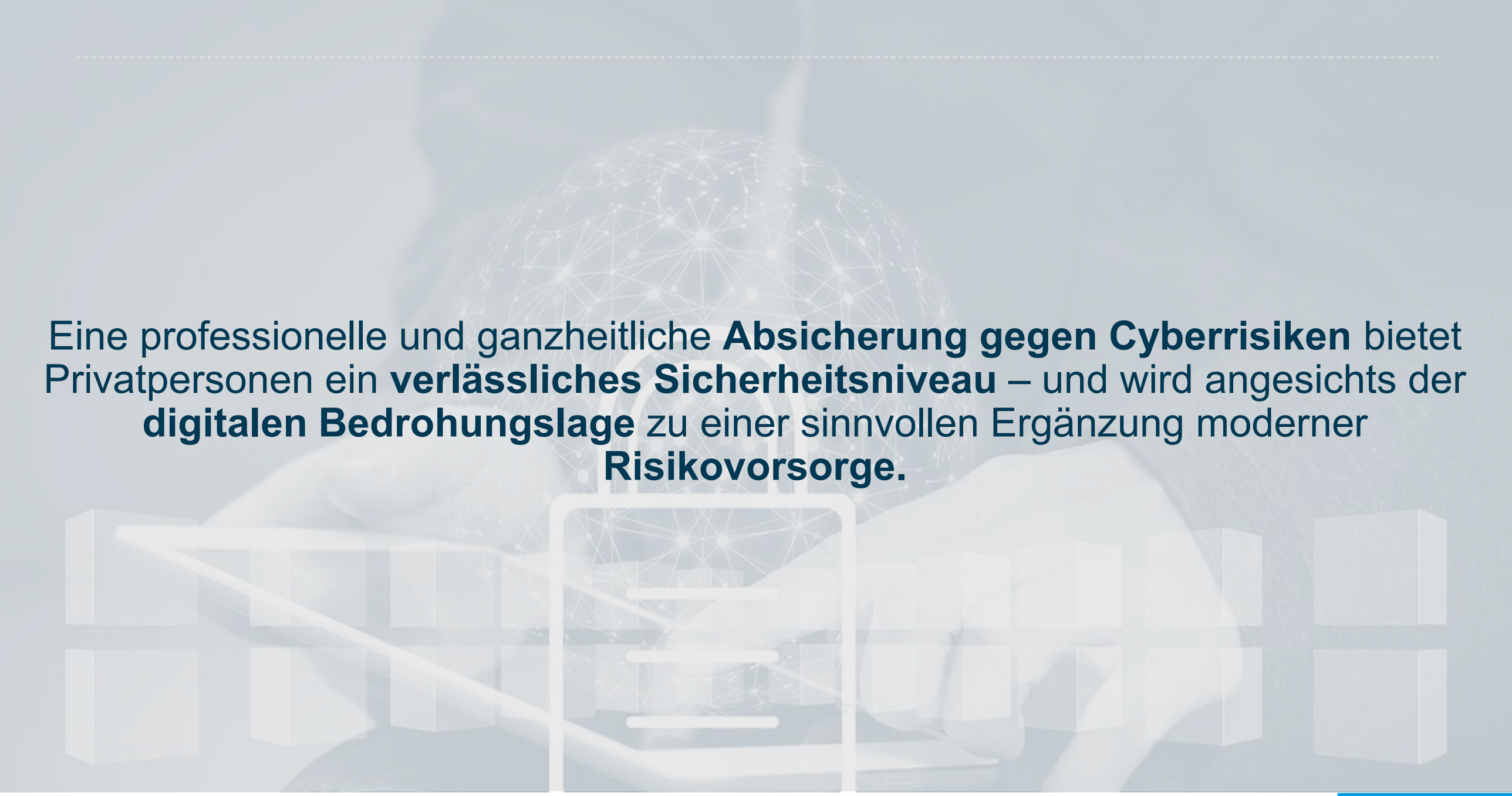
- Illegale Verbreitung eines aktuellen urheberrechtlich geschützten Films
- gerichtliches Auskunftsverfahrens stellt Anschlussinhaber fest

D 2.1.3 Verletzung urheberrechtlicher Bestimmungen

Versichert sind Haftpflichtansprüche, die aus einer unerlaubten Nutzung oder Verwertung von urheberrechtlichen geschützten Werken im Internet entstehen. Dabei übernehmen wir auch die Gebühren einer Abmahnung, mit der ein Anspruch auf Unterlassung oder Widerruf gegen Sie begehrt wird.

Nicht versichert sind hingegen

- Ansprüche, wenn Sie die fehlende Berechtigung zu der Veröffentlichung kannten.
- Vertragsstrafen sowie Bußgelder und Strafen aus einer strafrechtlichen Verfolgung einer Urheberrechtsverletzung.



Eine professionelle und ganzheitliche **Absicherung gegen Cyberrisiken** bietet Privatpersonen ein **verlässliches Sicherheitsniveau** – und wird angesichts der **digitalen Bedrohungslage** zu einer sinnvollen Ergänzung moderner **Risikovorsorge.**

Ihr Ansprechpartner

Debeka

Benjamin Porz

Debeka Campus 2 – 56058 Koblenz
Tel. 0261 498 -3658
Benjamin.Porz@debeka.de

www.debeka.de


DAS FÜREINANDER ZÄHLT.