



Cyber Risiken zum Weihnachtsgeschäft: Axa warnt vor zunehmenden Online-Bedrohungen

Michael Fiedler

Ob Black Friday oder Cyber Monday: Axa weist darauf hin, dass Online-Betrug und Datenkriminalität in der Vorweihnachtszeit deutlich zunehmen. Laut Axa Future Risks Report unterschätzen viele Deutsche diese Risiken weiterhin – obwohl Täter zunehmend mit KI-gestützten Methoden arbeiten.

Cyber Risiken steigen zum Jahresende deutlich an

Online-Einkäufe rund um Black Friday, Cyber Monday und das Weihnachtsgeschäft gehören inzwischen zum Alltag. Laut der Axa steigen in genau dieser Phase jedoch auch die Risiken für Cyberangriffe auf Privatanutzer. Täter nutzen zunehmend professionelle Methoden, darunter KI-generierte Inhalte, um an Daten zu gelangen oder betrügerische Transaktionen auszulösen. Die möglichen Folgen sind gravierend: Identitätsdiebstahl, missbräuchliche Einkäufe, Datenmissbrauch oder der Zugriff auf private Konten.

Future Risks Report 2025: Bevölkerung unterschätzt Cybergefahren

Der Axa Future Risks Report 2025 zeigt eine deutliche Diskrepanz zwischen Experteneinschätzungen und der Wahrnehmung in der Bevölkerung.

- Experten sehen Cyber Risiken unter den Top-Risiken der nächsten fünf bis zehn Jahre.
- In der deutschen Bevölkerung liegen sie deutlich weiter hinten und erreichen nur Platz zehn.

Auch Risiken durch KI und Big Data werden von Verbrauchern seltener als relevante Gefahren bewertet. Axa interpretiert dies als Hinweis darauf, dass viele Nutzer trotz zunehmender Bedrohungslage nur unzureichend auf Cyberangriffe vorbereitet sind.

Schutzmaßnahmen für Verbraucher: Axa nennt konkrete Empfehlungen

Axa gibt eine Reihe von Hinweisen für sicheres Online-Shopping in der Weihnachtszeit:

Sichere Passwörter verwenden Einfache oder gängige Passwörter wie „123456“ oder „Passwort“ vermeiden. Stattdessen Passwörter wählen, die mindestens 12 Zeichen lang sind, eine Mischung aus Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen enthalten. Für jeden Dienst ein

eigenes Passwort verwenden. Ein Merksatz kann helfen, komplexe Passwörter zu erstellen, z.B.: „Jedes 3. Eis in diesem Sommer ist Schokolade plus Vanille“ = J3EidSiSch+V. Regelmäßig Passwörter ändern Passwörter alle drei bis vier Monate aktualisieren. Passwort-Manager erleichtern die sichere Verwaltung von Zugangsdaten. Vorsicht beim Umgang mit persönlichen Daten Im Internet nur die nötigsten Informationen teilen und auf vertrauenswürdige Shops und Plattformen achten. Eine SSL-Verschlüsselung (<https://> in der URL) bietet mehr Sicherheit beim Einkauf. Aktuelle Sicherheitssoftware nutzen Anti-Viren-Programme installieren und diese stets auf dem neuesten Stand halten. Firewall-Funktion des Betriebssystems nutzen. Vorsicht bei E-Mails und Links Phishing-E-mails sind eine der häufigsten Methoden, um an Daten zu gelangen. Keine verdächtigen Anhänge oder Links öffnen und die Absenderadresse genau prüfen. Zwei-Faktor-Authentifizierung aktivieren Wo immer möglich, die Zwei-Faktor-Authentifizierung aktivieren, um zusätzlichen Schutz für Konten zu gewährleisten. Beim Online-Shopping auf vertrauenswürdige Anbieter setzen Auf Bewertungen, Gütesiegel und klare Kontaktinformationen achten. Nur bekannte Plattformen nutzen und Angebote vermeiden, die zu schön sind, um wahr zu sein. Vorsicht beim Teilen von Fotos und persönlichen Informationen in sozialen Netzwerken Kriminelle nutzen diese Daten für gezielte Betrugsversuche.

Vorgehen bei Verdacht auf einen Cyberangriff

Laut Axa sollten Betroffene bei einem möglichen Angriff sofort handeln: Passwörter ändern, die Polizei informieren, Auskunfteien wie Schufa prüfen und den Versicherer kontaktieren. Axa verweist dabei auf ihren Internetschutz-Baustein der Hausratversicherung, der Hilfe bei Cybermobbing, Identitätsdiebstahl und Betrugsfällen umfasst.

Versicherungs- und Finanznachrichten

expertenReport



<https://www.experten.de/id/4947177/Cyberisiken-zum-Weihnachtsgeschaeft-Axa-warnt-vor-zunehmenden-Online-Bedrohungen/>