

CYBER-BOOTCAMP AM 16. OKTOBER | 11:30 BIS 12:15 UHR

Gehackt. Erpresst. Stillstand. Was hilft im Ernstfall?



**ANASTASIOS
KAPETANOS**

Claims Underwriter
Hiscox



KLEMENS LEMKE

Underwriter Manager Cyber
Hiscox

Klick. Krise. Kontrollverlust?

Was der Cyber Readiness Report 2026 zeigt

32%

der deutschen KMU
haben im vergangenen
Jahr mindestens
1 Angriff festgestellt

33%

der Betroffenen sahen
Zahlungsfähigkeit oder
Existenz erheblich
gefährdet

41,7 Std.

durchschnittlicher
Betriebsstillstand –
global sind es
31,6 Stunden

29%

der deutschen KMU
haben derzeit keinerlei
Cyber-Versicherungs-
schutz

Basis: Hiscox Cyber Readiness Report 2026 – Wakefield Research befragte vom 5. bis 17. Juni 2026 insgesamt 6.800 Cybersecurity-Verantwortliche in zehn Ländern, alle aus Unternehmen mit weniger als 250 Mitarbeitenden.



Fazit: Cyber ist kein IT-Thema, sondern ein betriebswirtschaftliches Risiko.
Im Ernstfall entscheiden Liquidität, Wiederanlauf und schnelle Expertenhilfe.

Zwischen Angriff und Annahme

Wo Unternehmen wirklich getroffen werden

Angriffe treffen den Kern des Geschäfts

- 45% Finanzbetrug durch Payment Diversion
- 42% DDoS-Attacken
- 40% Missbrauch der eigenen IT-Ressourcen

Getroffen werden Zahlungsströme, Datenbestände und der laufende Betrieb also genau das, was das Tagesgeschäft trägt.

Wahrnehmung trifft auf Realität

48% fürchten vor allem Reputationsschäden.
25% der Betroffenen berichten tatsächlich von negativer Öffentlichkeitswirkung.

Die Außenwirkung wird überschätzt, wirtschaftliche und operative Folgen wiegen deutlich schwerer.

Cyber-Resilienz heißt nicht nur abwehren, sondern im Ernstfall handlungsfähig bleiben.

KI verschärft die Risikolage

Die größten KI-Bedrohungen der nächsten fünf Jahre

45%

Data Poisoning: Die Manipulation von Trainingsdaten

44%

Schwachstellen durch Dritt-KI-Tools wie ChatGPT

43%

Zu große Abhängigkeit, nachlassende menschliche Kontrolle

43%

Kontrollverlust über eigene Unternehmensdaten

Vom Modellrisiko zum Einfallstor: KI macht Angriffe billiger, schneller und glaubwürdiger

- Generative KI senkt die Einstiegshürde für Kriminelle: Phishing-Mails ohne Sprachfehler, passgenau auf Anlass, Branche und Ansprechpartner zugeschnitten.
- Erkennungsmerkmale von früher – schlechtes Deutsch, plumpe Anrede, kruder Absender – funktionieren nicht mehr zuverlässig.
- Gleichzeitig steigt die Abhängigkeit: 97% ergreifen Maßnahmen, aber 58% investieren jährlich weniger als rund 8.700 Euro in Cyber-Resilienz, 12% gar nichts.

Ein Klick genügt

Beispiel einer professionell gemachten Phishing-Mail

Ihr Zugang: Masterclass zur Cyber-Versicherung | Cyber-Bootcamp

Von: Hiscox Cyber-Bootcamp <cyber-bootcamp@hiscox.com>
An: k.lemke@musterfirma.de
Datum: Montag, 12.10.2026, 08:12



Sehr geehrter Herr Lemke,

vielen Dank für Ihre Anmeldung zur Masterclass beim Cyber-Bootcamp am 16.10. Ihr persönlicher Teilnehmerbereich mit Agenda, Unterlagen und IDD-Weiterbildungsnachweis ist ab sofort freigeschaltet.

Aus Sicherheitsgründen haben wir das Anmeldeverfahren umgestellt. Bitte bestätigen Sie Ihren Zugang bis Mittwoch, 14.10.2026, 17:00 Uhr – andernfalls verfällt Ihr Teilnehmerplatz und wird nachrückenden Interessenten zugeteilt.

Zugang jetzt bestätigen >

Mit freundlichen Grüßen
Ihr Hiscox Cyber-Bootcamp Team
Diese Nachricht wurde automatisch erstellt. Bitte antworten Sie nicht auf diese E-Mail.

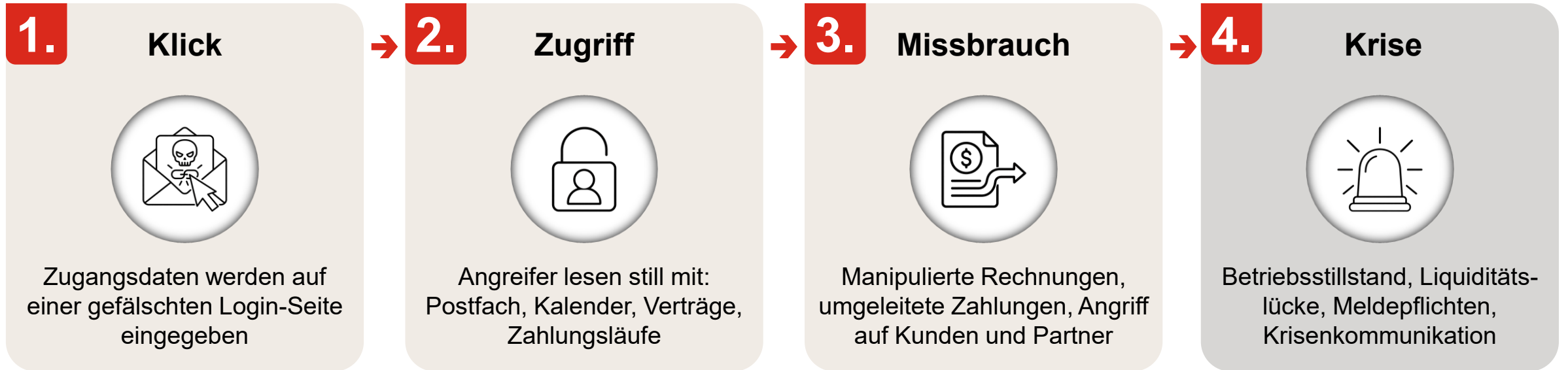
Warum diese Mail funktioniert

- Echter Anlass: Sie sind zum Cyber-Bootcamp angemeldet – die Mail passt exakt in den Erwartungshorizont.
- Hiscox-Absender, Logo und fehlerfreies Deutsch – klassische Warnzeichen fehlen, Absenderadressen lassen sich aber fälschen.
- Verlustangst: Verfall des Platzes.
- Zeitdruck mit konkreter Frist verhindert Rückfragen beim Veranstalter oder in der IT.
- Das Ziel ist nicht die Anmeldung, sondern Ihr Passwort: Die Zielseite ist eine Kopie der Login-Maske.

Prüfen: Nicht nur dem Absender trauen – Link-Ziel vor dem Klick checken und im Zweifel über den bekannten Weg selbst anmelden.

Vom Klick zur Krise

Wie aus einer E-Mail ein Betriebs- und Finanzrisiko wird



Was daraus werden kann, die Schadenpraxis

- Payment Diversion ist mit 45 % die häufigste erfolgreiche Angriffsart, der Schaden entsteht ohne jede Verschlüsselung.
- 41,7 Stunden Stillstand im Schnitt: Jede Stunde ohne Systeme kostet Umsatz, Vertrauen und Nerven.
- Jedes dritte betroffene Unternehmen (33 %) sah Zahlungsfähigkeit oder Existenz erheblich gefährdet.
- Und der Blick nach innen: Stress, Überlastung und Ausfälle in der Belegschaft nach einem Vorfall.

Schadenbeispiel 1 aus der Praxis

Zahlungsumleitungsbetrug (CEO-Fraud)

Der Fall



- Eine Buchhalterin erhält eine E-Mail vom vermeintlichen Geschäftsführer mit der dringenden Bitte um eine Überweisung
- 90.000 € sollen auf ein Konto in der Schweiz fließen – Absender, Signatur und Stil wirken authentisch
- Zeitdruck verhindert die übliche Rückfrage – erst später fällt der Betrug auf

Der Schaden



- Fehlüberweisung durch Zahlungsumleitungsbetrug: 90.000 €
- Psychologische Betreuung der betroffenen Mitarbeiterin: 8 Sitzungen à 150 €
- Schaden gesamt: 91.200 €

Die Hiscox-Lösung



- Netzwerksicherheitsverletzung, da der E-Mail-Account des Geschäftsführers gehackt wurde
- Cyber-Eigenschaden übernimmt die Fehlüberweisung sowie die Organisation der Soforthilfe
- Psychologische Unterstützung aus dem Experten-Netzwerk der Cyber-Versicherung



Zahlungsumleitungsbetrug ist mit 45% die häufigste erfolgreiche Angriffsart – ein gehackter E-Mail-Account genügt für einen sechsstelligen Schaden.

Schadenbeispiel 2 aus der Praxis

DDoS-Attacke auf einen Onlineshop

Der Fall



- Ein Fashion-Onlineshop erzielt einen Großteil seines Umsatzes über den eigenen Webshop
- Kurz vor dem Weihnachtsgeschäft bricht der Zugriff auf die Website plötzlich zusammen
- Ursache: eine gezielte DDoS-Attacke überlastet die Server mit automatisierten Anfragen

Der Schaden



- Cyber-Betriebsausfall durch den mehrstündigen Shop-Ausfall: 15.000 €
- IT-Forensik zur Analyse der Attacke sowie Stabilisierung der Server-Infrastruktur: 9.000 €
- Schaden gesamt: 24.000 €

Die Hiscox-Lösung



- Cyber-Betriebsunterbrechung deckt den Ausfall des wichtigsten Vertriebskanals
- Sofortige Einschaltung von Spezialisten zur Analyse und schnellen Wiederherstellung
- IT-forensische Analyse und Stabilisierungskosten vollständig übernommen

 **DDoS-Attacken zählen mit 42% zu den häufigsten Angriffen auf digitale Geschäftsmodelle – besonders vor umsatzstarken Verkaufszeiträumen.**

Schadenbeispiel 3 aus der Praxis

Ransomware mit Cyber-Erpressung

Der Fall



- Ein Schulungszentrum wird Opfer eines Verschlüsselungstrojaners mit anschließender Lösegeldforderung
- Sämtliche Schulungsinhalte sind nur digital gespeichert – der gesamte Betrieb steht still
- Das vorhandene Daten-Backup ist fehlerhaft und lässt sich nicht zurückspielen

Der Schaden



- Soforthilfe, IT-Forensik und Datenwiederherstellung durch den Krisendienstleister
- Mehrtägige Betriebsunterbrechung des gesamten Schulungsbetriebs
- Gesamtkosten: 520.000 €

Die Hiscox-Lösung



- Netzwerksicherheitsverletzung und Cyber-Erpressung sind versicherte Ereignisse
- Krisendienstleister vor Ort – Daten werden von Forensikern schnellstmöglich wiederhergestellt
- Ransomware zählt aus der Hiscox-Schadenpraxis zu den teuersten Cyber-Schadenfällen



Ransomware gehört zu den teuersten Cyber-Schadenfällen – ohne funktionierendes Backup wird jede Minute Stillstand teuer.

Cyber-Angriff? Das Risiko lässt sich absichern!

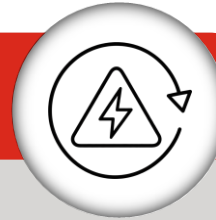
Allround-Cyber-Versicherung von Hiscox

Vor dem Angriff



- **Cyber-Training & Phishing-Test:** Mitarbeitende sensibilisieren, Risiko minimieren
- **Cyber-Sicherheits-Scan:** Schwachstellen erkennen und schließen
- **Norton-Schutzpaket:** umfassender Schutz für Geräte und Daten
(Optional abschließbar mit CyberClear Plus)

Im Ernstfall



- **Krisenplan:** Roter Faden im Ernstfall – vorher geübt, nicht erst im Vorfall gelesen
- **Soforthilfe 24/7:** führende IT-Forensiker als Partner statt Suche nach Ansprechpartnern
- **Expertennetzwerk:** Fachanwälte und PR-Krisenberater aus einer Hand

Danach



- **Haftpflicht:** Abwehr und Erfüllung, inkl. Medienhaftpflicht
- **Eigenschäden:** nur bei Hiscox Forderungsausfalldeckung bei manipulierten Zahlungsdaten
- **Betriebsunterbrechung:** nur bei Hiscox Tagessatzentschädigung ohne komplizierten Nachweis des Ertragsausfalls



**Der beste Schaden ist der, der gar nicht entsteht.
Der zweitbeste ist der, bei dem sofort jemand ans Telefon geht.**

Sicher im Alltag

Praktische Tipps für jeden – auch im Umgang mit KI

E-Mails & Links



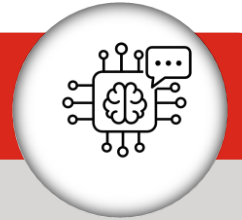
- **Erst denken, dann klicken:** Zeitdruck, Drohung oder Belohnung sind Warnsignale
- **Link prüfen:** Mauszeiger draufhalten, Adresse lesen, im Zweifel Seite selbst aufrufen
- **Rückruf statt Antwort:** Bei Zahlungs- oder Kontoänderungen über die bekannte Nummer nachfragen

Passwörter & Geräte



- **Zweiter Faktor (MFA):** schützt, auch wenn das Passwort geklaut wurde
- **Passwort-Manager:** für jeden Dienst ein eigenes, langes Passwort
- **Updates & Backups:** Updates sofort installieren, Daten regelmäßig und getrennt sichern

KI sicher nutzen



- **Keine sensiblen Daten:** Kundendaten, Verträge und Passwörter gehören nicht in öffentliche KI-Tools
- **Ergebnisse prüfen:** KI klingt überzeugend, kann sich aber irren
- **Echt oder Fake?** Stimmen und Videos lassen sich täuschend echt fälschen – Codewort für Notfälle vereinbaren

**Gesunder Menschenverstand ist die beste Prävention.
Im Zweifel: kurz innehalten, nachfragen, gegenprüfen.**



Vielen Dank für
Ihre Aufmerksamkeit

