



Deepfakes & Private Cyber: Wenn digitale Fälschungen zur echten Bedrohung werden



Ihre heutigen Referenten

Alina Sucker



*Product Head Art & Private Clients,
Property & Events – Hiscox Deutschland*

Unser Gast:

Christian Scherg



*Gründer & Geschäftsführender
Gesellschafter – Digital Shelter*

Im Rahmen unserer hochwertigen Hausrat- und Gebäudeversicherung „Haus und Kunst“ bieten wir unsere „Private Cyber“-Deckung an.

Basispaket für **HAUSRAT, KUNST** und **WERTGEGENSTÄNDE**



Zusatzbaustein
GEBÄUDE (Gebäude-Schutz)



Zusatzbaustein
PRIVATE CYBER (Cyber-Schutz)



Zusatzbaustein
FAMILY PROTECTION (Familien-Schutz)



Zusatzbaustein
PRIVATHAFTPFLICHT (Haftpflicht-Schutz)

Versicherte Risiken

1 Cyber-Mobbing

Systematische Verletzung Ihrer Persönlichkeitsrechte im Netz und daraus folgende Reputationsschäden.



2 Netzwerksicherheitsverletzung

Unbefugter Zugriff auf Ihr IT-System – Hacking, Phishing, Viren/Trojaner oder DoS-Angriffe.



3 Cyber-Diebstahl von Zahlungsmitteldaten

Missbrauch gestohlener Zahlungsdaten nach einer Netzwerksicherheitsverletzung.



4 Diebstahl von Kryptowährungen

Unbefugte Übertragung aus Ihrer passwortgeschützten Wallet nach Diebstahl des Private Key.



5 Identitätsmissbrauch & Doxing

Missbrauch personenbezogener Daten und böswillige Veröffentlichung im Netz (inkl. Darknet).



6 Ausbleibende Lieferung

Ware aus einem Online-Einkauf wird trotz Mahnung nicht innerhalb von 14 Tagen geliefert.



7 Urheberrechtsverletzungen

Abmahnung, weil Sie beim Posten oder Teilen unbewusst fremde Urheberrechte verletzt haben.



8 Cyber-Erpressung

Lösegeldforderung nach Blockade Ihres IT-Systems oder Drohung mit Veröffentlichung von Daten.





DIGITAL SHELTER
CYBER & INTERNET SECURITY


HISCOX



Deepfakes
verstehen,
erkennen,
abwehren



DIGITAL SHELTER
CYBER & INTERNET SECURITY



1

Deepfakes verstehen

Was genau ist ein Deepfake?



DIGITAL SHELTER
CYBER & INTERNET SECURITY

HISCOX

KI-generierte oder manipulierte Medieninhalte, die täuschend echt wirken – in vier Formen:



Gesichter und Personen werden realistisch neu erzeugt oder in bestehende Fotos montiert.

Mimik, Gestik und Stimme werden synchron manipuliert oder komplett synthetisch erzeugt.



Stimmen werden geklont – oft reichen wenige Sekunden Originalmaterial.

KI erzeugt Texte, die Stil, Wortwahl und Tonfall einer Person imitieren.



3 Sek. Audio → 85% authentisch wirkender Stimmklon

Typische Einsatzfelder



DIGITAL SHELTER
CYBER & INTERNET SECURITY

HISCOX



Identitätsmissbrauch

Fremde Identität übernehmen – gefälschte Aussagen, Bilder oder Auftritte im Namen einer Person.



Reputationsschäden

Gezielte Rufschädigung durch manipulierte, oft diffamierende Inhalte.



Erpressung/Betrug

Voice-Scams und gefälschte Videocalls zur Erschleichung von Zahlungen.





Warum Deepfakes immer leichter & schneller entstehen

- Frei verfügbare KI-Tools – kaum Vorwissen nötig
- Sinkende Kosten, wenige Sekunden Rohmaterial reichen als Trainingsdaten
- Stimmbasierter KI-Betrug: +1.210% innerhalb eines Jahres



Warum klassische Prüfmechanismen nicht mehr ausreichen

- Menschliches Auge erkennt Fakes kaum besser als der Zufall
- Bewährte Routinen (Rückruf, Augenschein) werden gezielt ausgehebelt
- Deepfake-Identitätsbetrug: erwarteter Anstieg um 495% in 2026



DIGITAL SHELTER
CYBER & INTERNET SECURITY


HISCOX

1.1

Ein Beispiel
aus der Praxis

Der Case



DIGITAL SHELTER
CYBER & INTERNET SECURITY



Ein 17-jähriger Schüler aus einem kleinen Dorf, der u. a. Jungschütze des ortsansässigen Schützenvereins ist, wird Opfer eines Deepfakes.

Eines Morgens tauchen in mehreren WhatsApp-Gruppen und auf Facebook Fotos auf, die ihn scheinbar bei rechtsextremen Demonstrationen zeigen – mitten im Aufmarsch. Die Bilder sind KI-generierte Fälschungen, wirken auf den ersten Blick aber täuschend echt.

Innerhalb weniger Stunden verbreiten sie sich über Facebook, Instagram, TikTok und lokale Nachbarschafts-Chats, werden geteilt, kommentiert und mit empörten Kommentaren versehen.

Am nächsten Tag greift ein lokales Online-Nachrichtenportal das Thema auf und berichtet über „Jungschütze des lokalen Schützenvereins auf Neonazi-Demo gesichtet“ – ohne die Fotos vorher auf ihre Echtheit zu prüfen.



Die Folgen



DIGITAL SHELTER
CYBER & INTERNET SECURITY

HISCOX

Für den 17-jährigen Schüler beginnt eine Welle der Anfeindung, die weit über das Internet hinausgeht.

Online häufen sich Droh- und Hasskommentare in seinen sozialen Netzwerken und den Kanälen seines Schützenvereins, sie werden mit beleidigenden und hasserfüllten Kommentaren überflutet.

Im realen Leben werden er, aber auch seine Eltern und Geschwister auf offener Straße beleidigt und verbal angegriffen. Sein Elternhaus, wie auch das Vereinshaus seines Schützenvereins werden mit Hassparolen beschmiert, Fenster mit Steinen eingeworfen.

Einen „Nazi“ will man in dem Dorf nicht haben.

Der 17-Jährige fürchtet um seinen Ruf, aber auch um seine berufliche Zukunft. Der Handwerksbetrieb, mit dem er bereits einen Ausbildungsvertrag geschlossen hat, hat diesen Vertrag bereits wieder gekündigt.





DIGITAL SHELTER
CYBER & INTERNET SECURITY


HISCOX

2

Deepfakes erkennen



Digitale Sichtbarkeit bewusst steuern

- Bewusst entscheiden, wie viel Foto-, Video- und Audiomaterial von einem selbst öffentlich zugänglich ist – jedes Material kann als Trainingsgrundlage dienen.

Umgang mit Bild- & Tonmaterial



- Vorsicht bei Social Media, Interviews und öffentlichen Videos: Je mehr authentisches Rohmaterial im Umlauf ist, desto leichter lassen sich realistische Fakes erzeugen.



Typische Warnsignale für manipulierte Inhalte

- Unnatürliche Lippen- oder Augenbewegung
- Bildartefakte an Kanten und Übergängen
- Metallisch oder hohl klingende Stimme
- Druck & Geheimhaltung – „sofort überweisen, niemandem sagen“

70%

hielten in einer Studie ein Deepfake-Video für echt – Menschen erkennen Fakes kaum besser als der Zufall.

Verhalten im privaten Umfeld



- Bei sensiblen Anfragen: über eine bekannte Nummer zurückrufen, Vier-Augen-Prinzip anwenden und bei Druck oder Eile misstrauisch bleiben.

Technische & organisatorische Schutzansätze



DIGITAL SHELTER
CYBER & INTERNET SECURITY



Self-Monitoring

- Eigenständige Beobachtung, z. B. über Google Alerts, Rückwärts-Bildsuche und regelmäßige Social-Media-Suche nach dem eigenen Namen.



Professionelles Monitoring

- Systematische Reputations- und Medienbeobachtung durch Expert:innen – frühzeitige Erkennung, bevor sich Inhalte verbreiten.



DIGITAL SHELTER
CYBER & INTERNET SECURITY



3

Deepfakes abwehren

Erste Schritte im Ernstfall



DIGITAL SHELTER
CYBER & INTERNET SECURITY


HISCOX

1

Ruhe bewahren

Nicht in Panik verfallen –
überlegtes Handeln schlägt
Schnelligkeit.

2

Beweise sichern

Screenshots, Links und
Zeitstempel dokumentieren,
bevor Inhalte verändert oder
gelöscht werden.

3

Keine Schnellschüsse

Nicht unüberlegt öffentlich
reagieren – erst Lage
bewerten, dann handeln.

Strategisches Vorgehen



DIGITAL SHELTER
CYBER & INTERNET SECURITY

HISCOX



Bewertung der Lage

Reichweite, Glaubwürdigkeit und Eskalationspotenzial realistisch einschätzen, um die richtige Reaktion zu wählen.



Kommunikation

Bewusst entscheiden, wann reagiert wird – und wann bewusstes Schweigen die klügere Strategie ist, um keine zusätzliche Aufmerksamkeit zu erzeugen.



Zusammenarbeit mit Experten



DIGITAL SHELTER
CYBER & INTERNET SECURITY



Removal-Strategien

- Entfernung aus Suchmaschinen, Social-Media-Plattformen und KI-Tools – als Privatperson kaum durchsetzbar, erfordert Fachwissen und etablierte Kontakte.

Externe Unterstützung



- Zusammenarbeit mit Plattformen und Medien sowie – wo nötig – Einleitung rechtlicher Schritte zur Durchsetzung der Ansprüche.

Darum ist „Private Cyber by Hiscox“ die richtige Lösung für Ihre Kunden



Organisation von Soforthilfe

Schnelle, koordinierte Krisenreaktion – wir steuern die richtigen Schritte vom ersten Moment an.



Zugang zu Expertennetzwerken

IT-Forensik, spezialisierte Anwälte und Kommunikationsberater – abgestimmt aus einer Hand.



Kostenübernahme

Übernahme der versicherten Aufwendungen im Rahmen der vereinbarten Bedingungen.



Cross-Selling: gewerbliche Cyber-Versicherung

Viele unserer Kundinnen und Kunden sind auch unternehmerisch tätig. Die private Cyber-Deckung ist der ideale Anlass, das gewerbliche Cyber-Risiko anzusprechen – und mit Hiscox CyberClear abzusichern.

Teilen Sie uns Ihre Meinung mit!

Feedback zum IDD-Day #3

Feedback geben
& gewinnen!

Die Umfrage dauert nur wenige Minuten, ist vollständig anonym – und als kleines Dankeschön verlosen wir unter allen Feedback-Gebern **drei Eventim-Gutscheine im Wert von je 50 €.**

Jetzt Scannen & teilnehmen →

Vielen Dank!





Vielen
Dank!