



Wenn die Firewall fällt-
Ein Blick in die Hiscox
Cyber -Schadenwelt



Vorstellung und Agenda

Özgün Habenstein



Syndikusrechtsanwältin
– Head of Claims Commercial Lines –

Bastian Lutz



– Team Leader Underwriting –

Vorstellung und Agenda

AGENDA

KI und ihre Auswirkungen

Einblick in Praxisfälle

Fazit und Handlungsempfehlungen

Zahlen, Daten, Fakten

Warum dieses Thema?

Cyberangriffe verändern sich – und KI mischt vorne mit, bei Hackern wie bei Unternehmen

Steigende Komplexität und Geschwindigkeit von Angriffen

Zunehmende Rolle generativer und lernender Systeme

Neue Anforderungen an die Schadenbearbeitung



Warum KI die Cyberwelt grundlegend verändert

„Cyber-Schäden: Klassisch vs. KI-gestützt“

Klassische Szenarien:

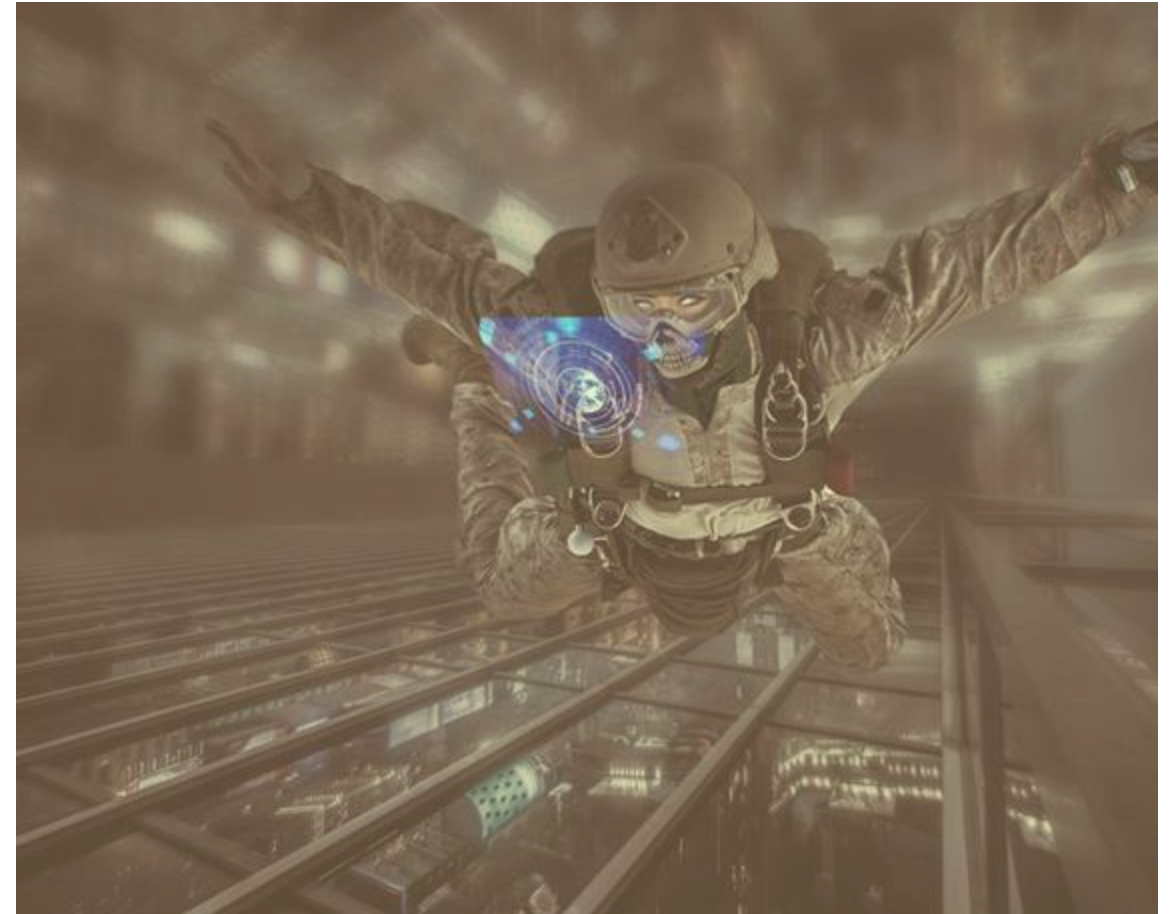
Phishing, Ransomware, DDoS

Neue Dimensionen:

Deepfakes, adaptive Malware, AI-Phishing

Fazit:

KI verstärkt bekannte Angriffsarten signifikant
Deepfakes, KI-Phishing, automatisierte Angriffe
Höhere Schäden, komplexere Prüfung, neue
Unsicherheiten



Schadenfälle – wenn KI der Auslöser ist

Beispiele:

Fake-President-Angriff per Deepfake-Anruf via Zugriff auf die IT Systeme

⇒ Millionenüberweisung

KI-generierter Phishing-Link

⇒ Datenabfluss

⇒ Datenschutzverstoß

Ransomware-Angriff mit KI-Optimierung

⇒ komplette Verschlüsselung



Zahlen / Daten / Fakten

KI verändert die Cyber-Bedrohungslandschaft
(Quelle: CISO-Report 2025)

53 % der CISOs (Chief Information Security Officers) sehen KI als Vorteil für Angreifer
(2023 noch 70 %)

Gleichzeitige Chancen für Verteidiger durch
Automatisierung & Effizienz



Wichtigste KI-basierte Bedrohungen laut CISOs

Realistic Phishing	57 %
Neue Malware-Varianten	44 %
Adaptives Social Engineering	40 %
Exploitation von AI-Tools im Unternehmen	40 %
Automatisierte Angriffe	38 %
Schnellere Brute-Force-Attacken	33 %
Realistische Voice/Deepfakes	30 %



Praxisfall 1:

Legal aber fatal- das Passwort war „kanzlei123!“



Verschlüsselte Daten in einer Anwaltskanzlei

Schadenhöhe: 75.000,00 EUR

Was ist passiert?

Über schwache Passwörter drang Schadsoftware in das Computersystem einer Rechtsanwaltskanzlei ein und verschlüsselte sämtliche Dateien mit der Endung .locked und .readme_txt. Die Kanzlei-Mitarbeitenden konnten nicht mehr auf die Dateien zugreifen und somit nur sehr eingeschränkt arbeiten.

Besonders perfide:

Die Schadsoftware wurde mithilfe von KI entwickelt und gesteuert. KI ermöglichte es den Angreifern, Passwörter gezielt zu erraten und Sicherheitslücken auszunutzen.

Praxisfall 1:

Legal aber Fatal: das Passwort war „kanzlei123!“

Wie half die Cyberversicherung?

Sofortige Unterstützung durch IT-Forensiker

Schadsoftware wurde isoliert und entfernt

Daten wurde mit Hilfe von Spezialisten
wiederhergestellt

Neue Sicherheitsrichtlinien eingeführt



Praxisfall 1:

Legal aber Fatal: das Passwort war „kanzlei123!“

Die Rolle von KI im Angriff

KI-basierte Passwort Cracking Tools analysieren öffentlich verfügbare Daten und kombinieren sie intelligent – Schwachstellen wie einfache Passwörter werden so sekundenschnell erkannt und ausgenutzt.



Praxisfall 2: Zimmer gebucht – Virus mitgebracht: Ein Trojaner auf Urlaubsreise



Hacking

Schadenhöhe: 25.000,00 EUR

Was ist passiert?

Was ist passiert? Ein Hotelmitarbeiter öffnete versehentlich einen E-Mail-Anhang mit einem Trojaner. Die Schadsoftware manipulierte den Hotelserver und versendete über die IT-Infrastruktur Spam-E-Mails.

Schadsoftware war mit KI-Funktionen ausgestattet.

Angriff blieb länger unentdeckt, da die KI den normalen Mailbetrieb imitierte und die Malware geschickt tarnte.

Praxisfall 2: Zimmer gebucht – Virus mitgebracht: Ein Trojaner auf Urlaubsreise

Wie half die Cyberversicherung?

Sie stellte dem Hotel IT-Sicherheitsexperten zur Seite, die das System von dem Trojaner bereinigten.

KI als "stille Mitreisende": Schadsoftware und Phishingsmails werden immer häufiger mit Hilfe von KI erstellt **und operieren häufig auch mit KI.**



Praxisfall 3:

Wenn Hacker shoppen gehen



Datenklau

Schadenhöhe: 60.000,00 EUR

Was ist passiert?

Ein Unternehmen der Onlinebranche wurde aufgrund eines Hacker-Angriffs Opfer von Datenmissbrauch. Über mehrere Wochen hatten Hacker Zugang zu dem streng gesicherten Online-Bezahlsystem. Sie kopierten und nutzten über 250.000 Kundendaten.

Die Angreifer nutzten KI, um Schwachstellen im System automatisiert zu identifizieren und Sicherheitsmaßnahmen zu umgehen. Mittels KI-gestützter Social-Engineering-Techniken (z.B. Audio-Nachrichten, die täuschend echt wie die Stimme des Vorgesetzten klangen) wurden Zugangsdaten von Mitarbeitenden erschlichen und anschließend systematisch ausgenutzt.

Praxisfall 3:

Wenn Hacker shoppen gehen

Wie half die Cyberversicherung?

Sie übernahm die Kosten für IT-Forensik, die rechtliche Beratung in Bezug auf die Sicherstellung der Benachrichtigungs- und Compliance- Richtlinien sowie die rechtliche Beratung.

Künstliche Intelligenz wird zunehmend eingesetzt, um automatisiert Schwachstellen auszuspähen, Passwörter zu knacken oder Phishing-E-Mails, Audio-Nachrichten oder sogar Videos täuschend echt zu verfassen. Die Angriffe werden dadurch präziser – und der Schaden potenziell größer.

Auch KI-basierte Angriffe sind mitversichert – durch spezialisierte Partner für KI-Forensik, Bedrohungsanalyse und angepasste Compliance-Maßnahmen.



Die Auswirkungen auf die Schadenbearbeitung

- ▶ Was KI-Schäden für unsere Arbeit bedeuten
- ▶ Technische Prüfung wird komplexer (z. B. Deepfake-Erkennung)
- ▶ Deckungsprüfung bei „Betrugsschaden“ oft juristisch anspruchsvoll
- ▶ Schnelligkeit & Krisenmanagement sind entscheidend



Rolle der Cyberversicherung heute

Cyberversicherung: mehr als nur Kostenerstattung

Kombination aus Risikotransfer und Krisenhilfe

Zugang zu IT-Forensik, Rechtsberatung,
Krisen-PR-Hilfe



Was hilft Unternehmen im Ernstfall wirklich?

Awareness-Schulungen



4-Augen-Prinzip bei Zahlungen



Firewalls, MFA, Ransomware-sichere Backups,
Segmentierung



Herausforderungen für Versicherer



Kalkulierbarkeit im
KI-Zeitalter – ein
Balanceakt



Dynamische
Risikolage, kaum
historische Daten



Systemische Risiken
(z. B. Lieferketten-
Cyberangriff)



Prämiensteigerung
vs. Marktwachstum



Der Markt wächst – trotz Risiken



Cyber als Zukunftsmarkt – aber kein Selbstläufer

16 % jährliches Wachstum (Europa)

Ziel: 8,3 Mrd. Euro Prämienvolumen bis 2030

Aber:

Schadenquoten von bis zu 124 %

⇒ hohes Risiko

Fazit & Handlungsempfehlungen

Unser Job ist wichtiger denn je

Wir brauchen technisches Know-how im Schadenbereich

Enge Zusammenarbeit mit IT-Forensik und Legal wird essenziell

Klarheit in den Bedingungen, schneller Service im Ernstfall





Vielen Dank für
Ihre Aufmerksamkeit

