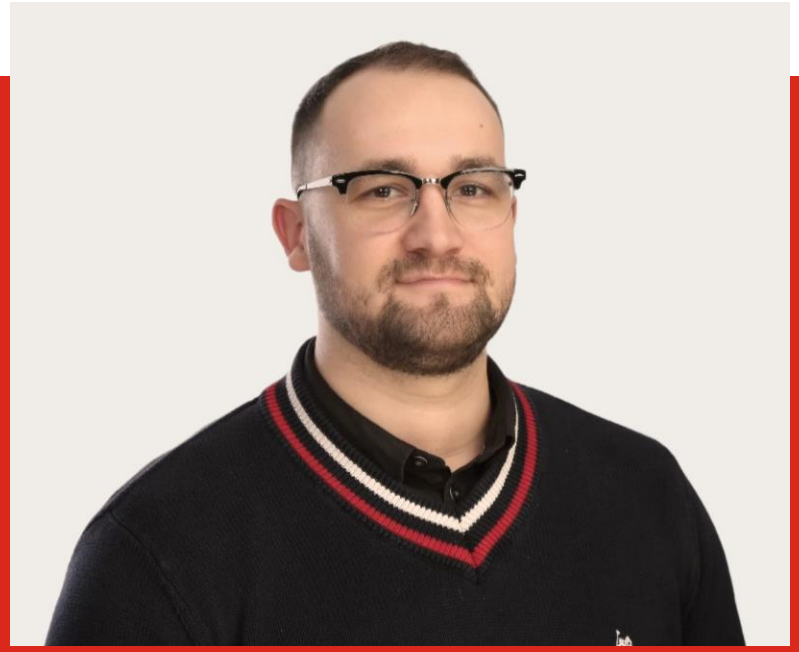
HISCOX

KI & Cyber: Wie neue Technologien die Versicherungswelt verändern

Wir schützen,
was Sie schätzen.

Ihre Referenten

Klemens Lemke



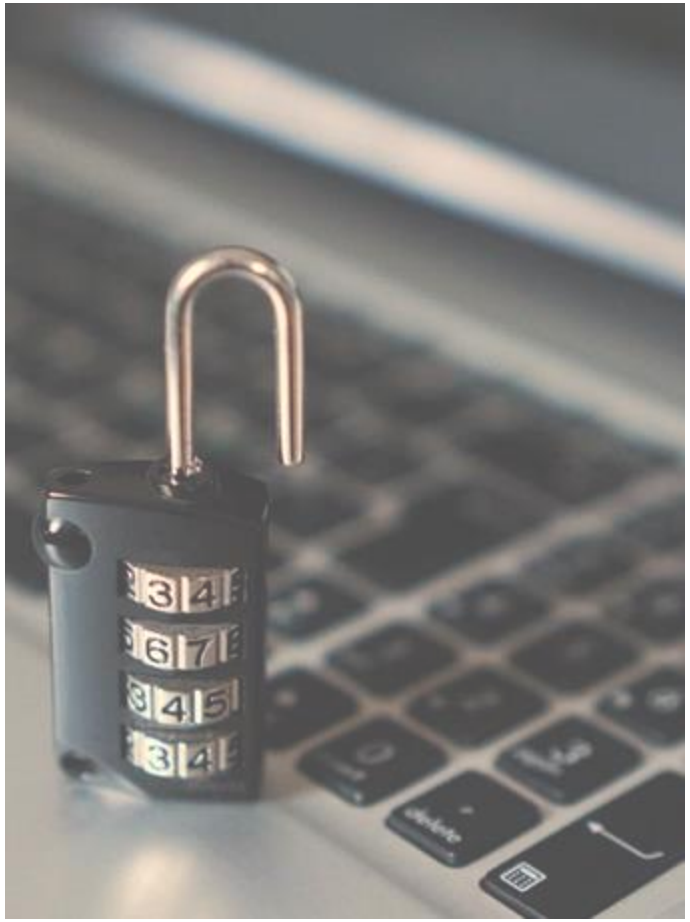
Underwriting Manager Cyber
Hiscox Deutschland

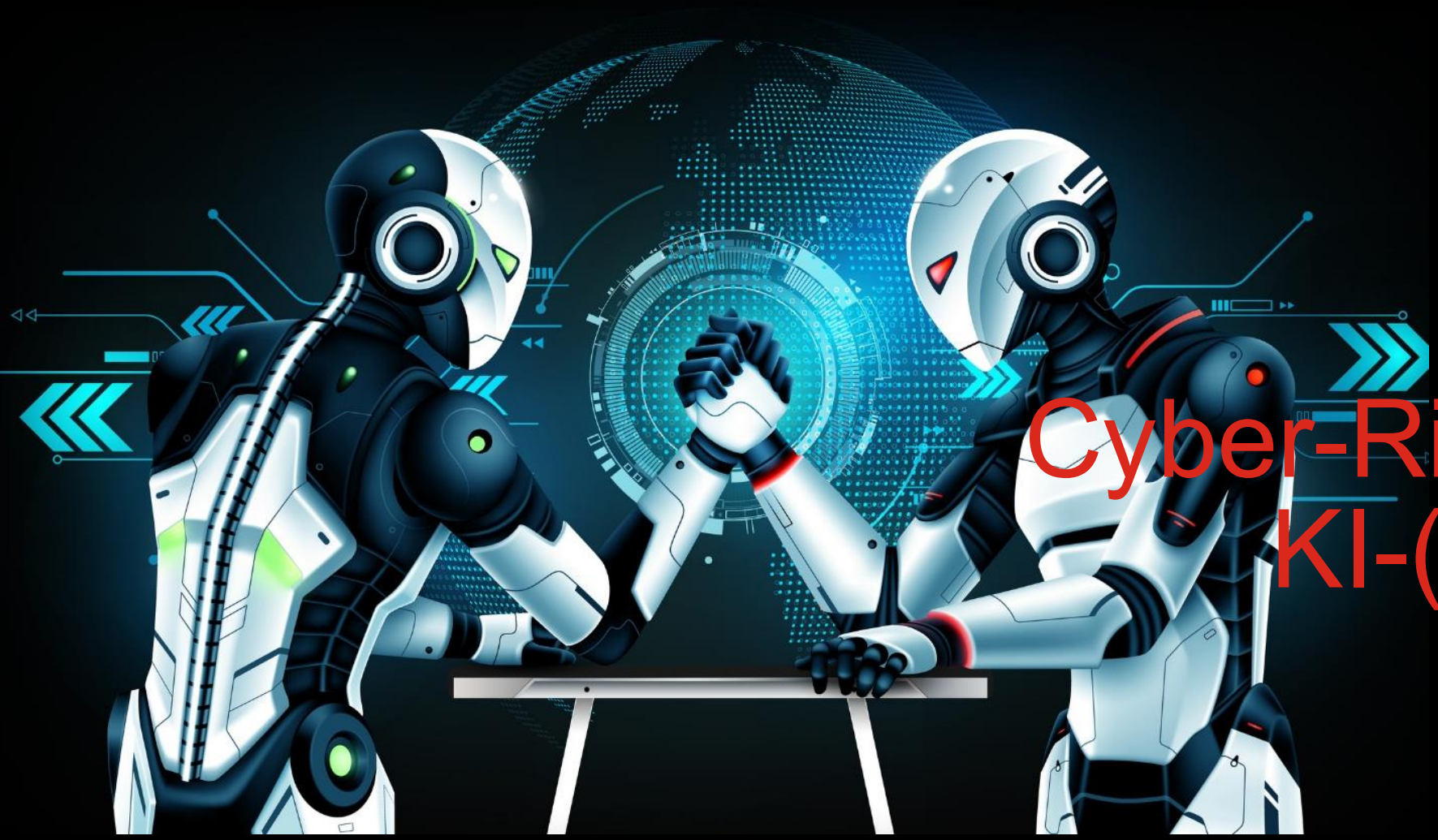
Robin Schröter

Sales & Development Underwriting
Hiscox Deutschland

Agenda

1. Intro: Cyberrisiken in der KI-(R)Evolution
2. Bedrohungen: Schadenszenario eines KI-gestützten Angriffs
3. Chancen: Wie KI in der Prävention & Abwehr hilft
4. Markt-Einblicke: Hiscox KI-Umfrage & Cyber Readiness Report 2025
5. Fazit: Wie agieren in einer KI-gestützten Bedrohungslage?





1. Intro:
Cyber-Risiken in der KI-(R)Evolution

Cyberrisiken in der KI-(R)Evolution:
dynamischere & komplexere Risikolage

HISCOX

1 KI-generierte Phishing-Mails

Erstellung täuschend echter E-Mails im Stil von Vorgesetzten oder Kollegen mittels LLMs

2 Deepfake-Angriffe

Realistische Video- oder Audiodateien, die Kunden, Vorgesetzte oder Behörden simulieren

3 Model Poisoning

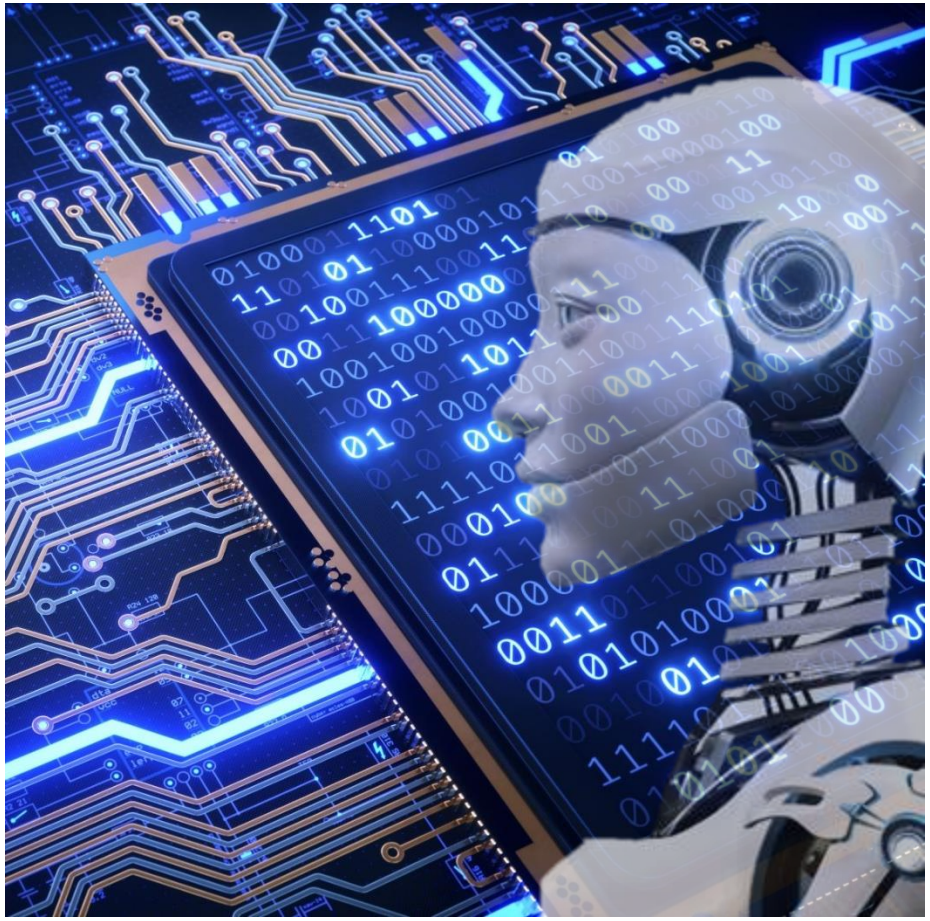
Manipulation von Trainingsdaten von Machine-Learning- Modellen, um gezielt falsche Entscheidungen zu provozieren

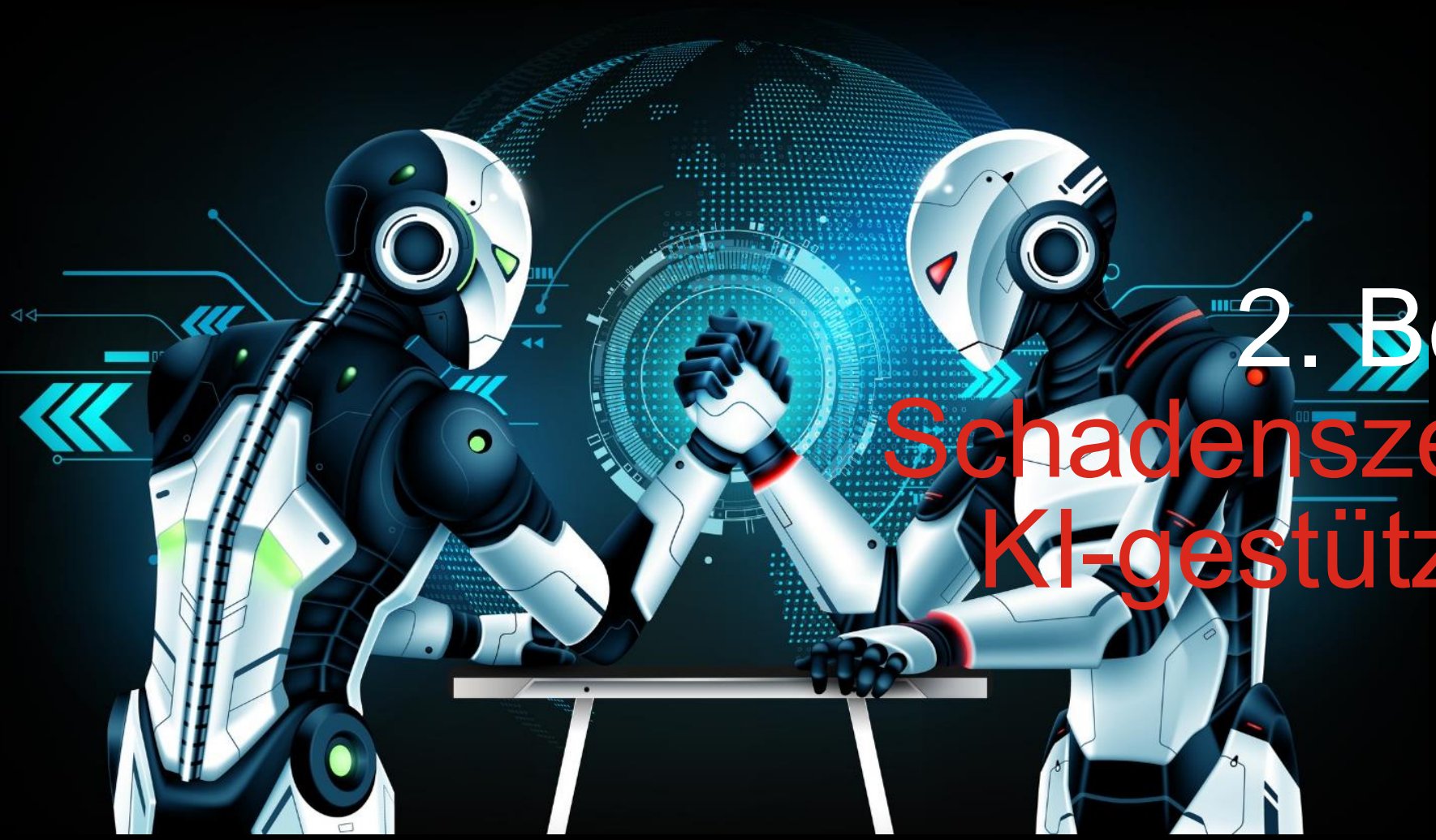
4 Autonome Hacking-Agenten

KI-Agenten führen mehrstufige Angriffe durch – von Spionage über Payload-Generierung bis zur Umgehung von Firewalls –halbautonom und skalierbar

5 KI-generierte Malware

Herstellung von Schadcodes, die sich dynamisch an Sicherheitsmaßnahmen anpassen – z.B. Änderung der Signatur, um Antivirenprogramme zu umgehen.





2. Bedrohungen
Schadenszenario eines KI-gestützten Angriffs

Ein ganz normaler Arbeitstag
Noch!

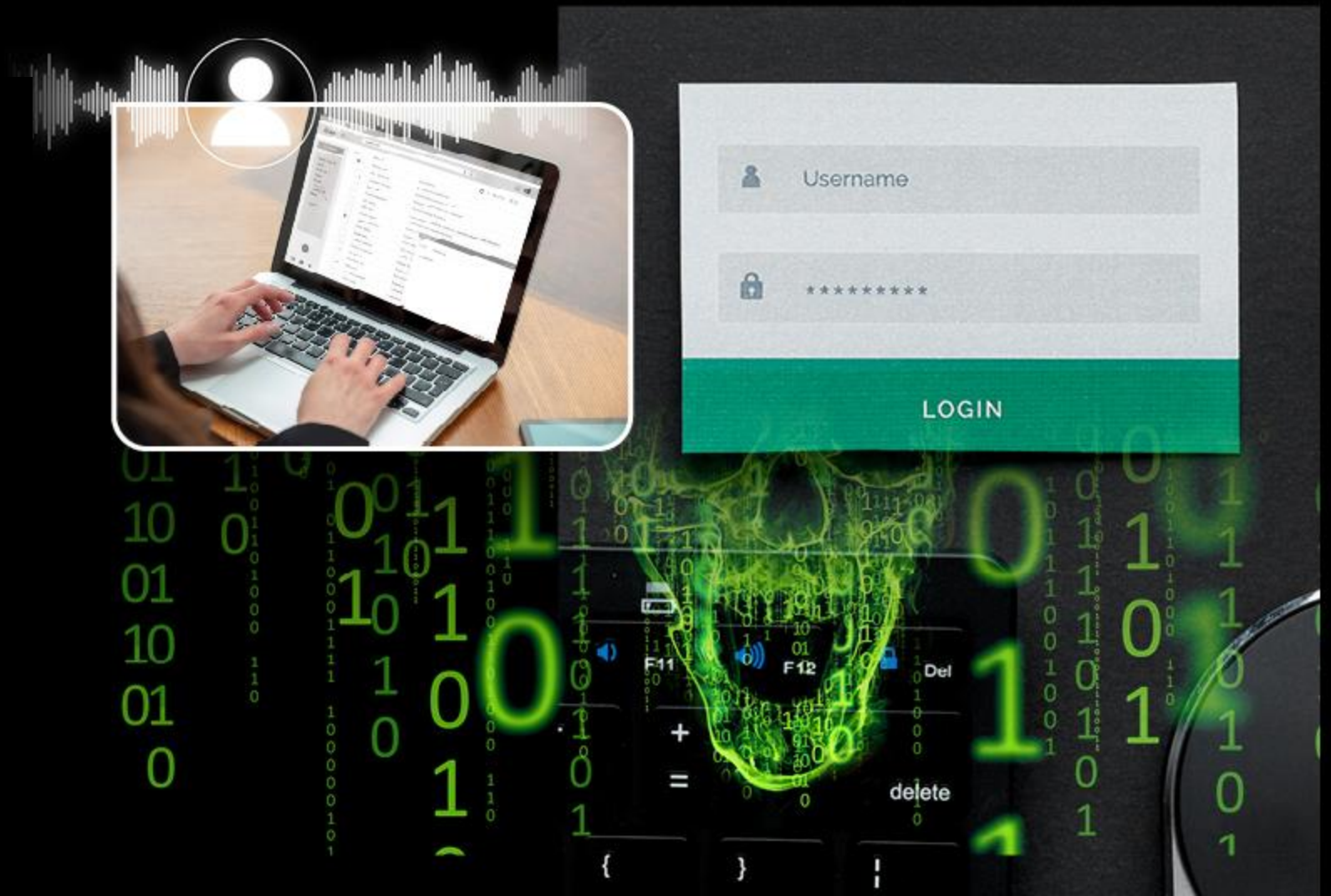
- Mitarbeiter arbeiten konzentriert
- Systeme laufen stabil
- Keine Hinweise auf Bedrohungen
- Doch ein KI-Agent beobachtet
- bereits im Hintergrund

Minute 0 bis 5:
Der Agent scannt das Unternehmen

- Analyse von LinkedIn, Firmenwebseite, Presseartikeln
- Identifikation von Schlüsselpersonen -> Recherche von YouTube- und Schulungs-Videos sowie Vortragsaufzeichnungen der Personen
- Erkennung potenzieller Schwachstellen

Minute 6 bis 10:
Die perfekte Fälschung

- Deepfake-Audio imitiert CTO
- E-Mail mit täuschend echter Sprache und Signatur
- Link führt zu präparierter Website mit Malware

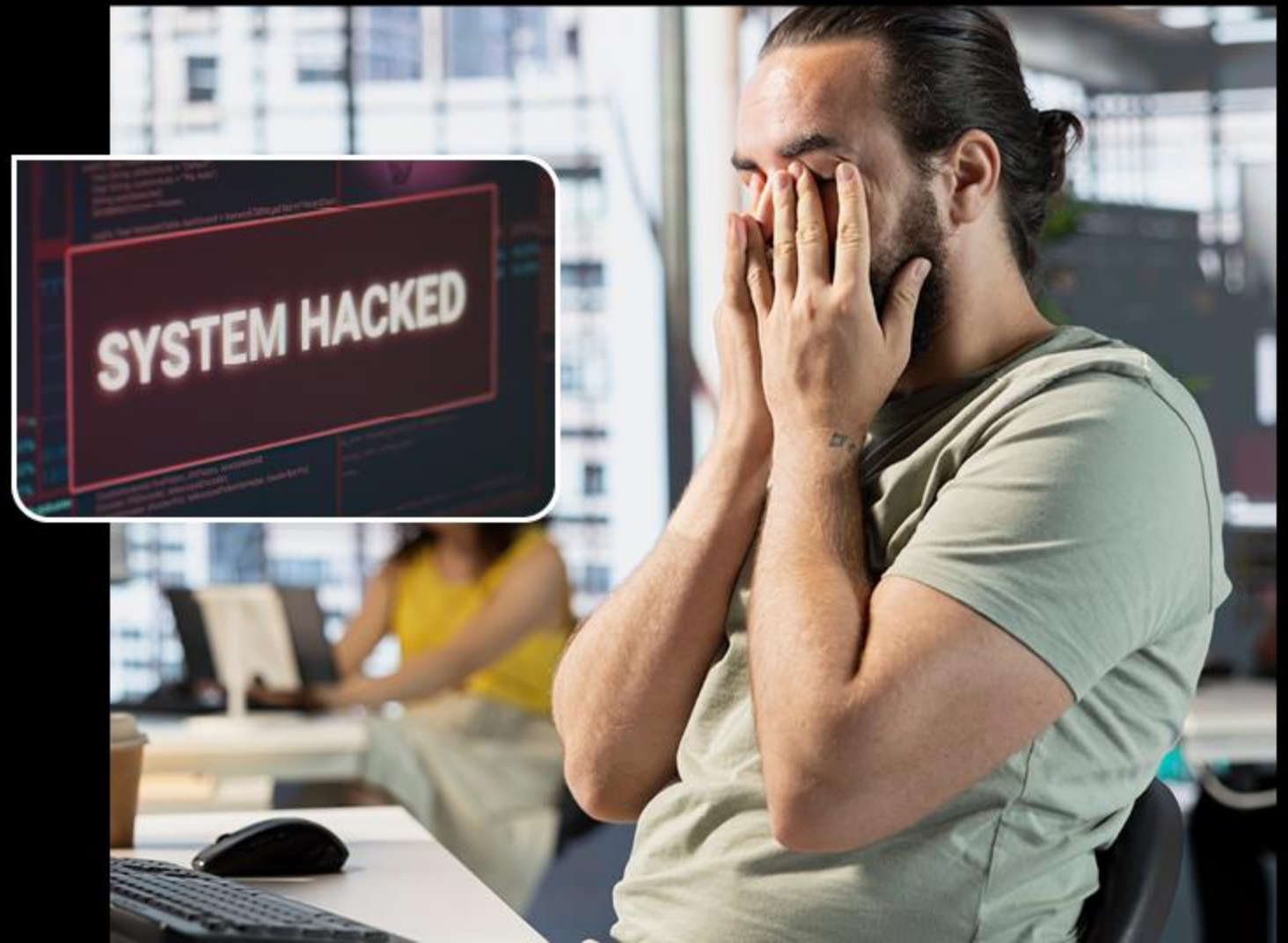


Minute 11 bis 15:
Der Agent übernimmt

- Installation eines Remote Access
- Trojaners Zugriff auf interne Systeme
- Datenexfiltration
- Log-Manipulation
- lateral movement

Zu spät erkannt –
der Schaden ist da

- IT-Mitarbeiter entdecken verdächtige Aktivitäten
- Systeme kompromittiert
- Daten bereits abgeflossen
- Alarm kommt zu spät



3. Chancen

Wie KI in der Prävention & Abwehr hilft

KI als Schutzschild
für mehr Sicherheit

- Frühwarnsysteme
- Automatisierte Reaktionen
- Deepfake-Erkennung
- Cyberresiftzenz beginnt mit intelligentem Schutz

Chancen durch KI:
Beispiele für konkrete Einsatzgebiete I

HISCOX

Bedrohungserkennung & Stream Processing

- Analyse riesiger Datenmengen in Echtzeit und Erkennung von Angriffsmustern
- Identifikation verdächtiger Aktivitäten & Anomalien im Netzwerkverkehr oder ungewöhnliches Nutzerverhalten

Reaktionsautomatisierung

- Automatische Alarmierung & sofortige Einleitung von Gegenmaßnahmen bei erkannter Bedrohung: z. B. Isolieren betroffener Systeme oder Blockieren verdächtiger Zugriffe

Schwachstellenmanagement & Patch-Optimierung

- Identifikation veralteter Softwarekomponenten und gezielte Updates
- Priorisierung der Patches nach Risiko und Angriffs-wahrscheinlichkeit

Chancen durch KI:
Beispiele für konkrete Einsatzgebiete II

HISCOX

Prädiktive Analytik

Vorhersage zukünftiger Angriffe mittels Thread Intelligence, also Auswertung:

- historischer Daten
- bekannter Angriffsmuster & Vorgehensweisen
- genutzter Schwachstellen & adressierte Sektoren
- aktuelle Trends

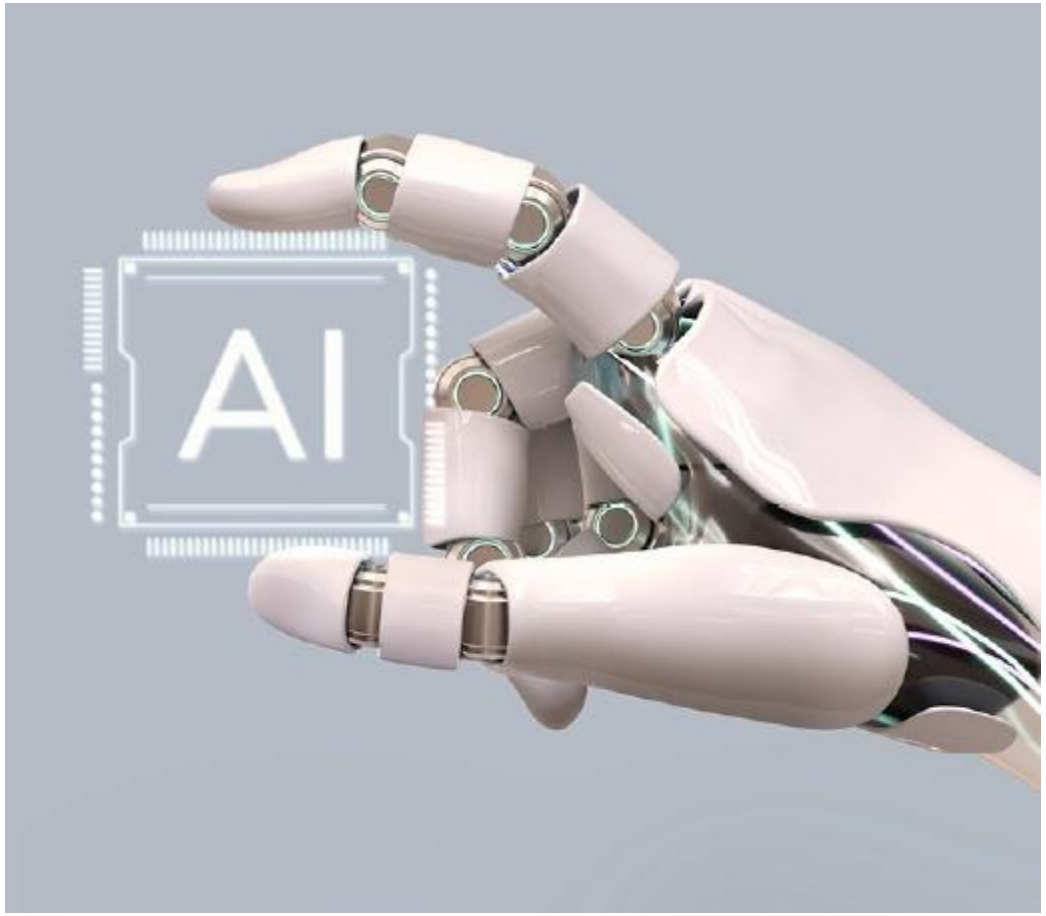
So lassen sich potenzielle Schwachstellen frühzeitig erkennen und absichern

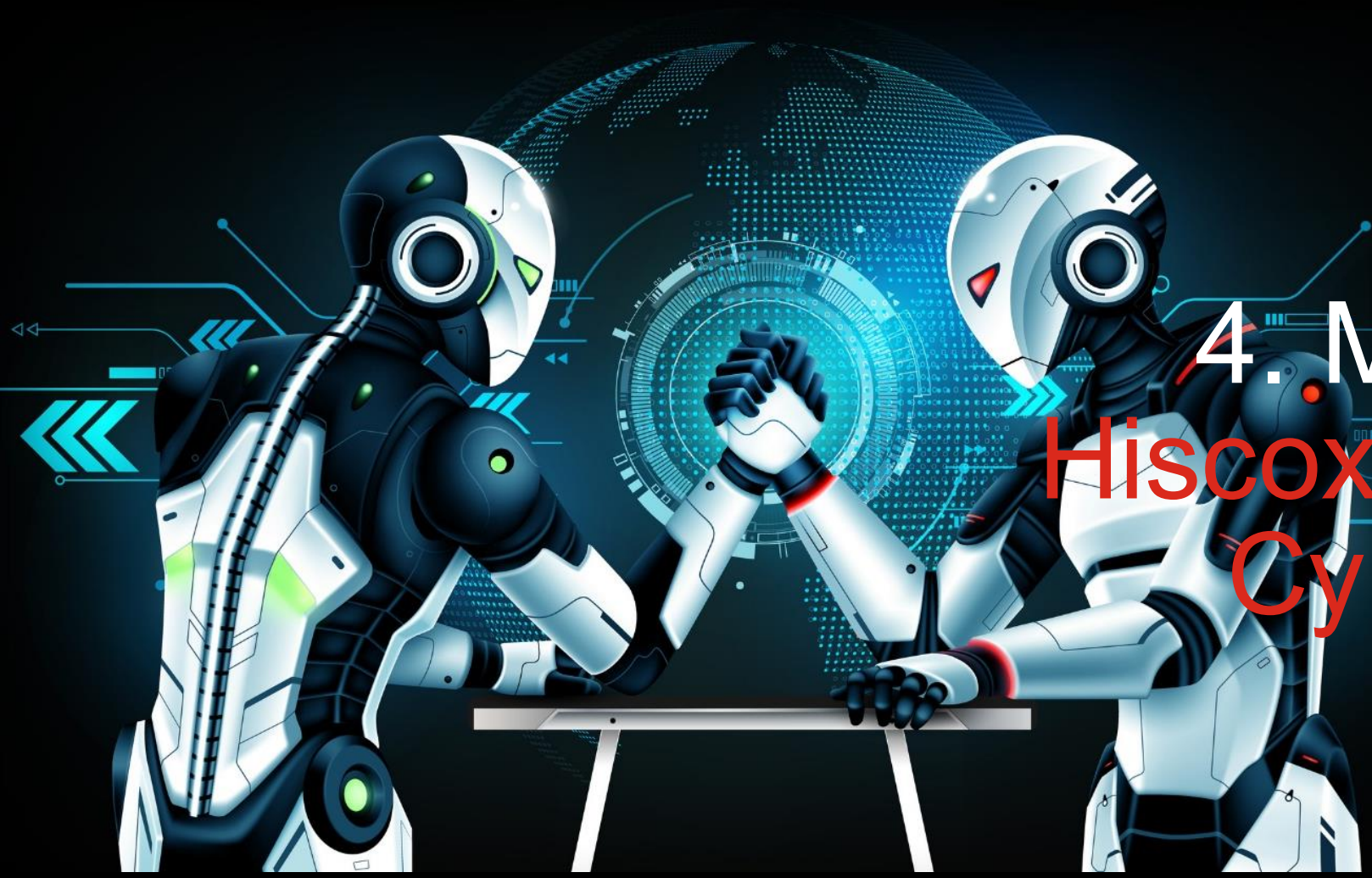
Deepfake-Erkennung

KI erkennt manipulierte Medieninhalte wie gefälschte Videos oder Audiodateien, die für Identitätsdiebstahl oder Social Engineering genutzt werden.

Generative KI für Sicherheits-Playbooks

Erstellung von Sicherheitsrichtlinien, Testfällen -und Reaktions-szenarien für verschiedene Angriffstypen. Das hilft Teams, schneller und strukturierter zu handeln



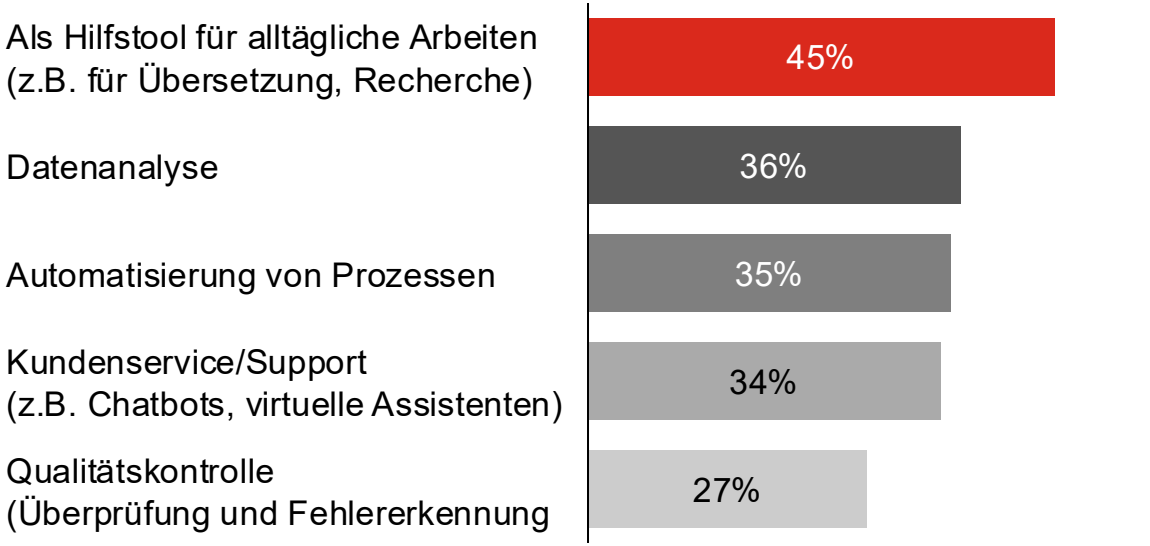


4. Markt-Einblicke

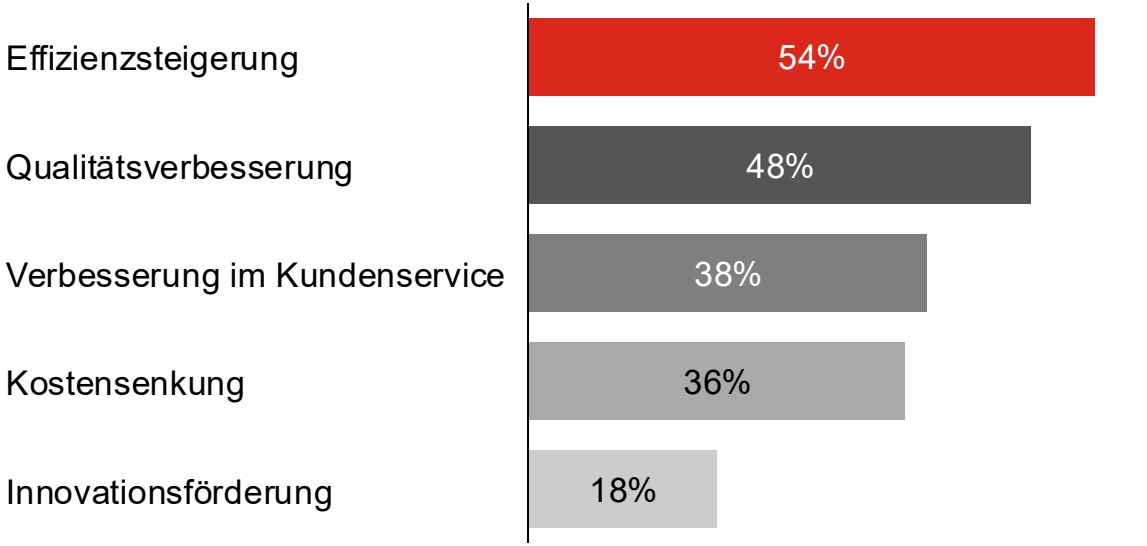
Hiscox KI-Umfrage & Cyber Readiness Report

Spannende Einblicke zu KI:
Die Hiscox KI-Umfrage 2025

Top 5: In welchen Bereichen setzt Ihr Unternehmen KI ein?



Top 5: Welche Geschäftsziele sollen mit KI in Ihrem Unternehmen erreicht werden?

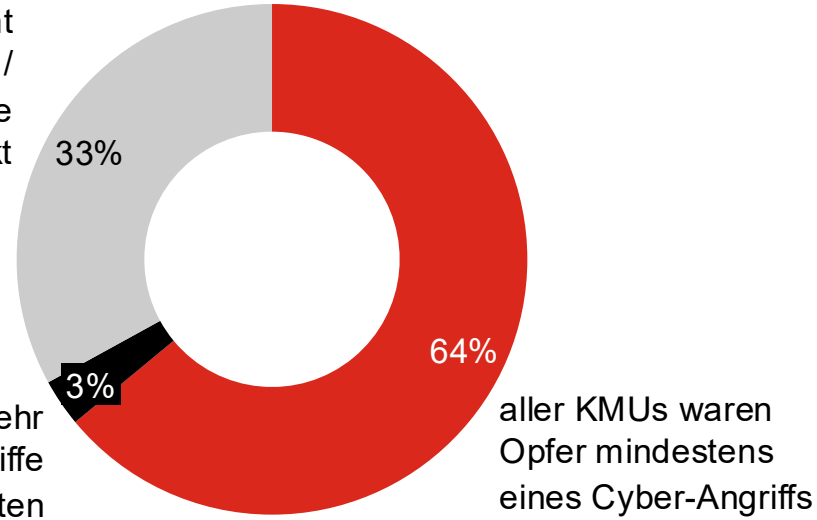


Über 50% der Unternehmen nutzen schon KI, jedoch mit Fokus auf Recherche, Übersetzungen und Effizienzsteigerungen – noch kein Schwerpunkt in Cyber-Sicherheit und -Abwehr

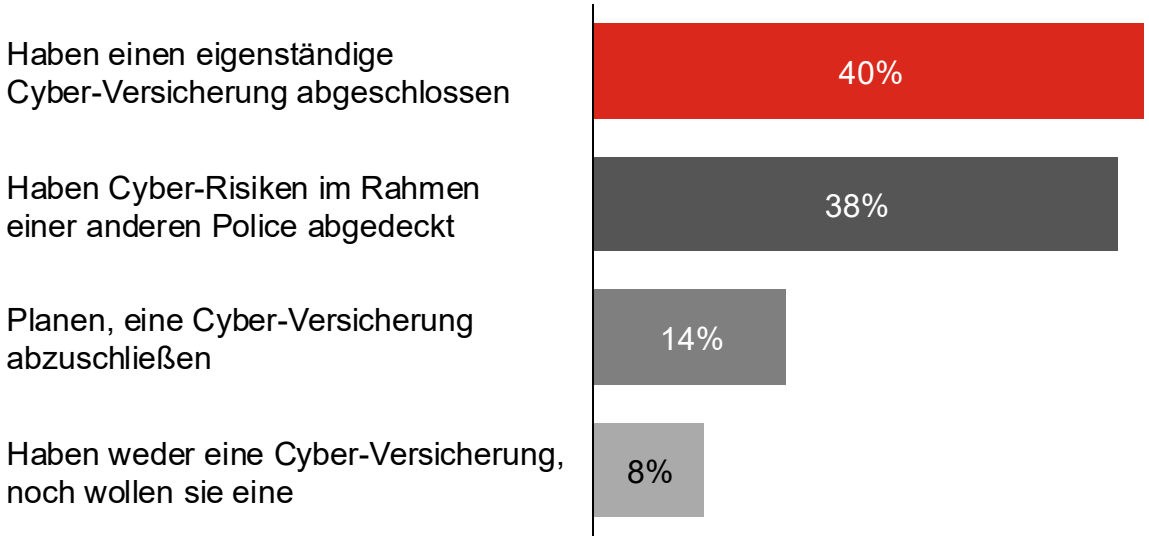
Quelle: Hiscox KI-Umfrage 2025 (www.hiscox.de/research/ki-umfrage)

Spannende Einblicke zu KI & Cyber:
Der Hiscox Cyber Readiness Report 2025 (1/3)

Angespannte Bedrohungslage in Deutschland



6 von 10 der deutschen KMUs sind nicht ausreichend Cyber-versichert

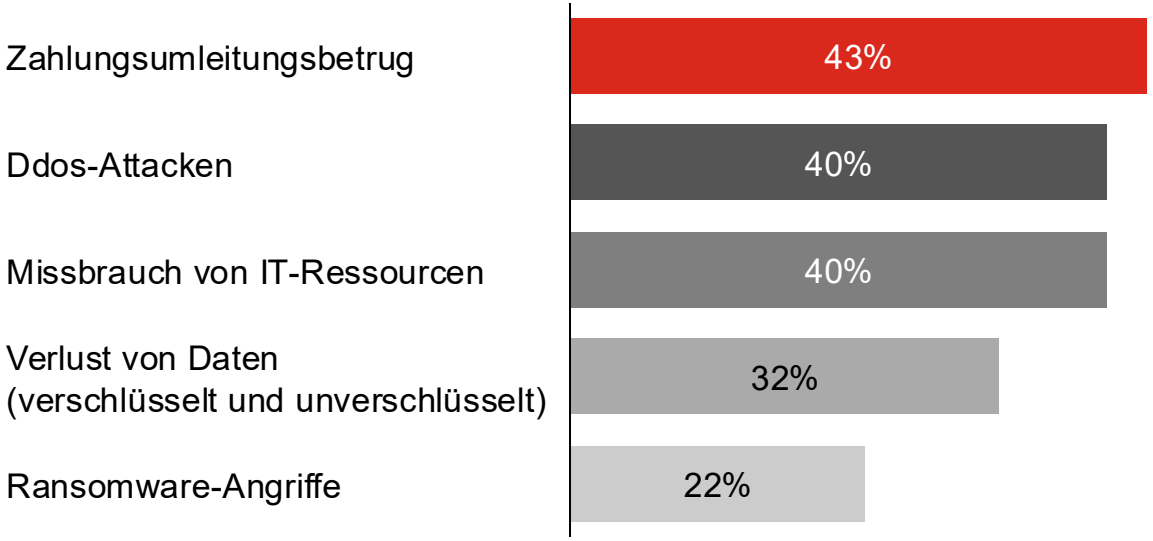


Die Frage ist nicht ob, sondern wann – 6 von 10 deutschen KMUs erlitten mindestens einen Angriff
Cyber-Kriminelle nutzen intensiv KI, was z.B. Phishing-Mails immer schwerer zu erkennen macht
Trotzdem ist die Absicherungssituation oft lückenhaft – nur 4 von 10 sind ausreichend abgesichert

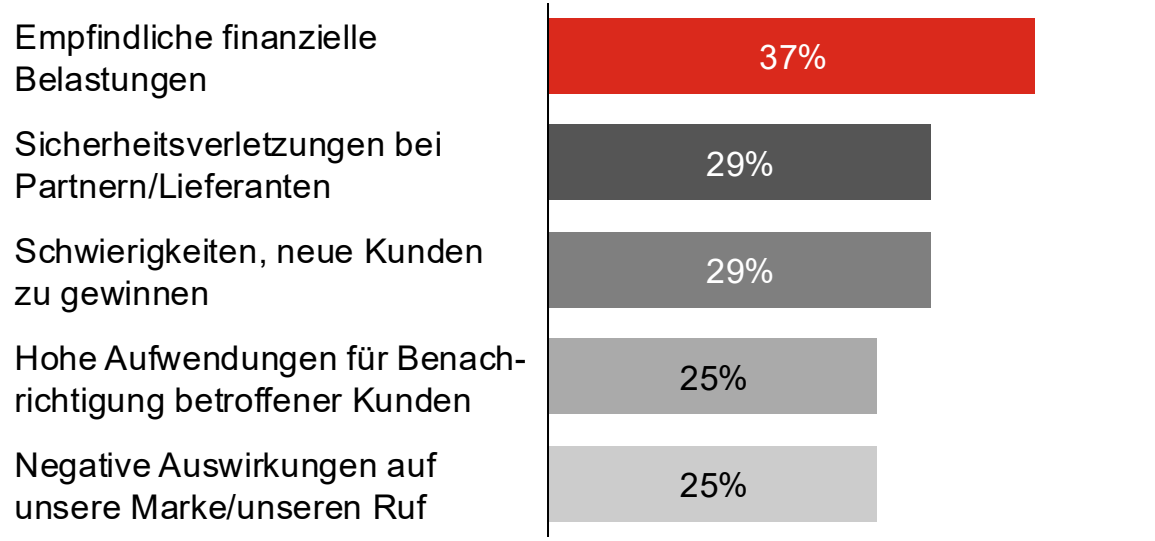
Quelle: Hiscox Cyber Readiness Report 2025 (www.hiscox.de/crr2025)

Spannende Einblicke zu KI & Cyber:
Der Hiscox Cyber Readiness Report 2025 (2/3)

Cyber-Kriminelle nutzen multiple Angriffsvarianten – Top 5 der Cyber-Schäden



Welche Auswirkungen auf das Unternehmen hatten die Cyber-Attacken?



Am schnellsten kommen Cyber-Kriminelle per Zahlungsumleitungsbetrug zum Geld – diese und andere Angriffsvarianten sind häufig KI-gestützt

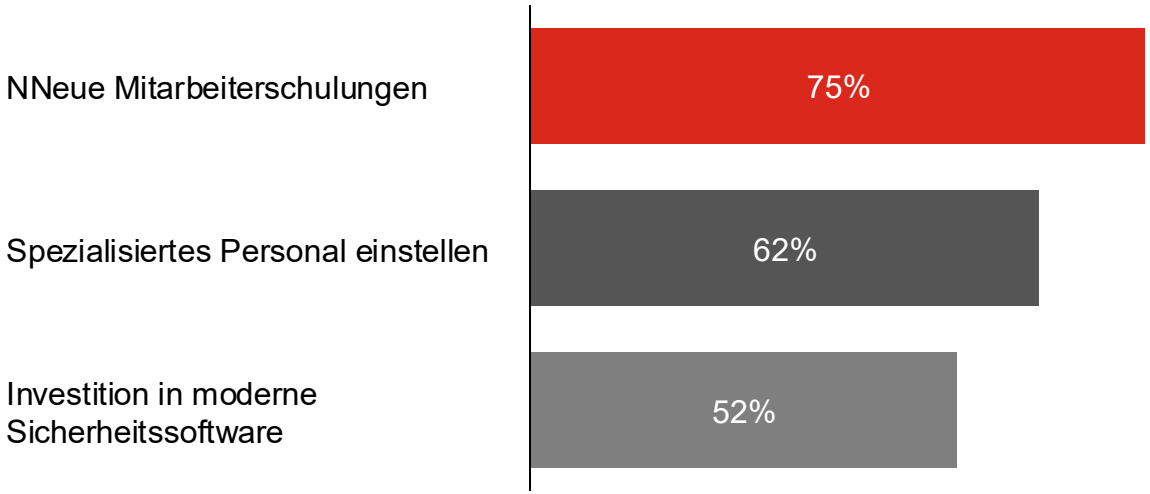
Schwerwiegende Konsequenzen für Unternehmen von finanziellen Verlusten bis Reputationsschäden

Quelle: Hiscox Cyber Readiness Report 2025 (www.hiscox.de/crr2025)

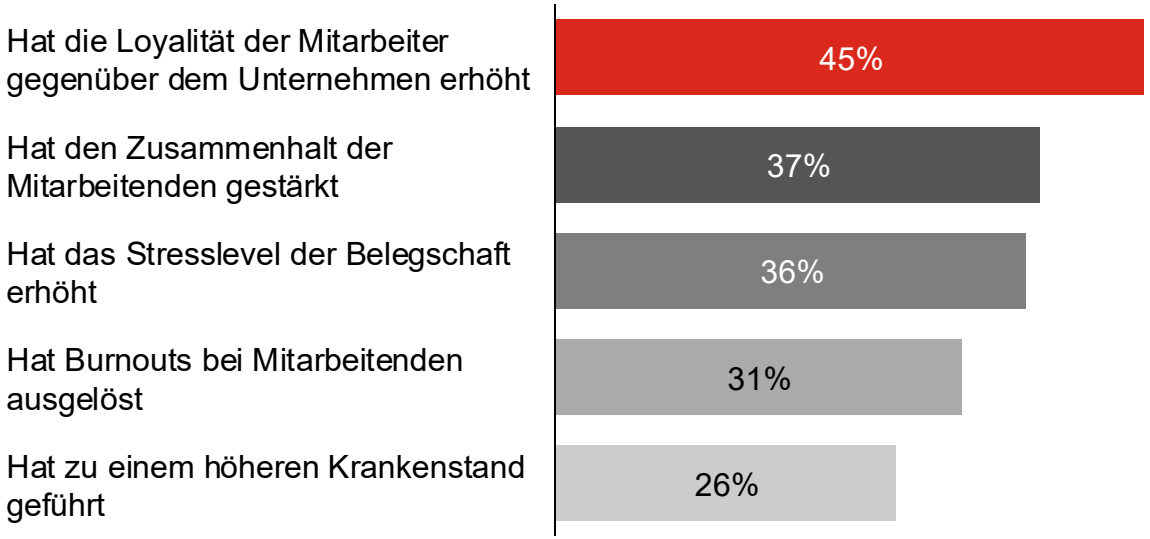
Spannende Einblicke zu KI & Cyber:
Der Hiscox Cyber Readiness Report 2025 (3/3)

Investition in präventive Maßnahmen für mehr Cyber-Resilienz

Folgendes haben die befragten Unternehmen konkret geplant



Was waren die menschlichen Folgen der Cyber-Angriffe?



Positiv: Die Investitionsbereitschaft der KMU für mehr Cyber-Resilienz ist hoch

Häufig übersehen wurden bisher die umfangreichen menschlichen Auswirkungen eines Cyber-Angriffs

Quelle: Hiscox Cyber Readiness Report 2025 (www.hiscox.de/crr2025)

Vertriebsansätze:
KI zwingt zum Handeln!

KI verschärft die Bedrohungslage und das macht Cyber-Versicherung unverzichtbar – Bspw. werden KI-basierte Malware und Phishing zukünftig einer der größten Bedrohungen

Durch die Geschwindigkeit in der KI-Evolution wird Risko noch weniger beherrschbar für Unternehmen – besonders betroffen sind KMU´s!

Es wird immer brandneue Angriffsvektoren geben und erhöht sich die Wahrscheinlichkeit eines auf einen Zero-Day-Exploid

Irrglaube auf Kundenseite:
"Mein Unternehmen ist zu kleine und zu uninteressant für einen Cyber-Angriff"

Hiscox Cyber Readiness Report verdeutlicht, dass das Risiko erkannt wird und die Bereitschaft zur Investition in die Cyber-Sicherheit da ist.

Risiko ist mit einer Cyber-Versicherung versicherbar – Alle KI-Risiken mitversichert.

Unsere Empfehlung:

Jetzt ist die größte Chance auf Cross-Selling bei Ihren Kunden

Vertriebsansätze:
Die USPs der Hiscox Cyber-Versicherung

HISCOX

USPs

Krisendienstleistung im Schaden sind unverzichtbar und können selten von IT-Dienstleistern geleistet werden – **24h Krisenhotline** zu Cyber-Experten

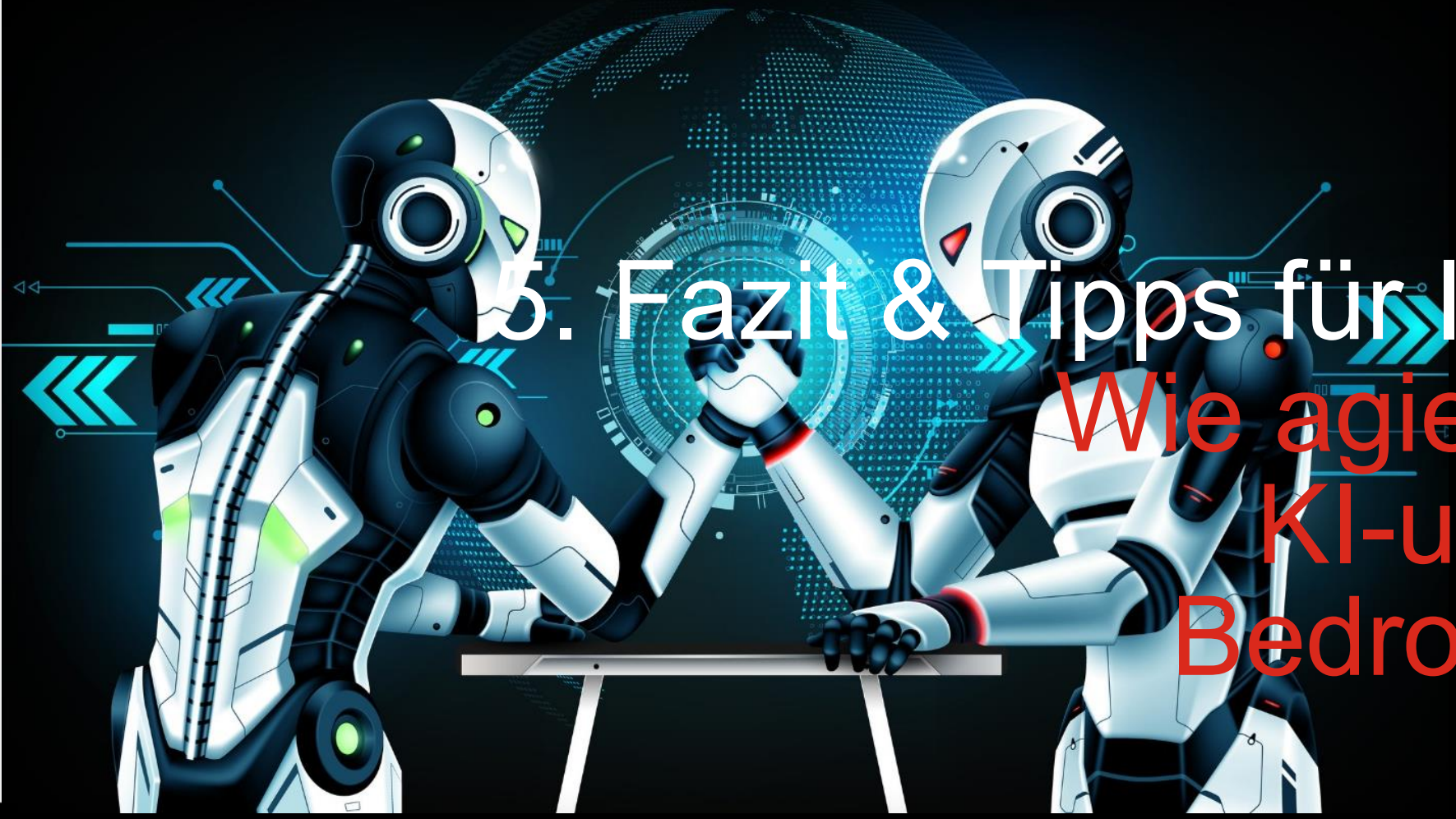
CyberClear: kostenlose Prävention ab dem ersten Tag – Cyber-Training, Phising Simulation, Krisenplan von Experten

norton

CyberClear PLUS – aktiver Support durch Cyber-Sicherheitspaket von Norton

Innovative Deckung mit **Cyber Clear** 01/2026

Optimale Absicherung für Unternehmen und deren digitale Risiken – Führungskräfte stehen im Fokus und müssen der Cyber-Gefahr Rechnung tragen



5. Fazit & Tipps für Ihre Kunden

Wie agieren in einer KI-unterstützten Bedrohungslage?

5. Fazit & Tipps für Ihre Cyber-Kunden:
Wie agieren in einer KI-unterstützten Bedrohungslage?

Konsequente MFA-Nutzung und Kennzeichnung externer Kommunikation

4-Augen-Prinzip bei wichtigen Entscheidungen & Verifizierung wichtiger oder ungewöhnlicher Informationen auf zweitem Kommunikationskanal

KI-Tools unterstützen massiv bei der Angriffserkennung und Sofortmaßnahmen

Sicherstellung von KI-Fachwissen im Unternehmen, insbesondere durch Schulungen der Mitarbeiter

Kontrolle über den „KI-Output“ sicherstellen – KI kann unterstützen, aber sollte nicht unkontrolliert agieren

Regelmäßige Anpassung und Optimierung der IT-Infrastruktur

Klarheit über die Datenbasis der KI-LLMs

Bleiben Sie in Kontakt mit uns!
Auch über profino hinaus

HISCOX

Hiscox Makler News: Abonnieren & gewinnen!

- Stets informiert beraten: Hiscox News & Produktinformationen
- Unterstützung für Ihren Vertrieb: Unterlagen, Studien, digitale Tools
- Profitieren Sie von IDD-Webinaren, exklusive Events & mehr!
- Bei **Neuanmeldung Gewinnchance auf die passende Ausstattung zur Fußball-WM** (1. Preis JBL-Soundbar, 2. & 3. Preis: Fan-Paket)

HISCOX

VIELEN DANK!