HISCOX

KI & Cyber:
Gamechanger für die Versicherungsbranche?!

Ihre Referenten

Klemens Lemke

Underwriting Manager Cyber,
Hiscox

Unser Gast:

Daniel Schätzle

Rechtsanwalt und Partner,
HÄRTING Rechtsanwälte
PartGmbB

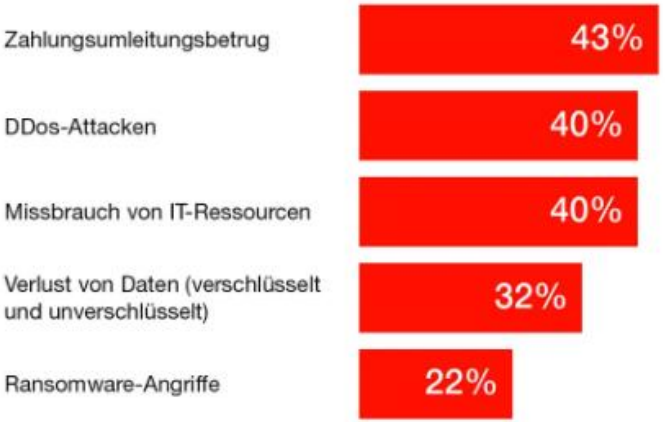
Hiscox Cyber Readiness Report 2025
Studiendesign

- Zum Report: In Zusammenarbeit mit dem Marktforschungsinstitut Wakefield Research wurden weltweit 5.750 kleine und mittlere Unternehmen (KMU)
- Befragt wurden Repräsentanten und Experten aus: Deutschland, USA, Großbritannien, Irland, Frankreich, Spanien, Belgien und den Niederlanden (1.000 davon aus Deutschland)
- Repräsentative Auswahl von Unternehmen in unserem präferierten Kundensegmenten
- Erstmals konkret auch KI thematisiert
- Zum Report: https://www.hiscox.de/research/hiscox-cyber-readiness-report/

Erkenntnisse Hiscox Cyber Readiness Report 2025
Angriffsvarianten

Cyber-Kriminelle nutzen multiple Angriffsvarianten

Top 5 der Cyber-Schäden:

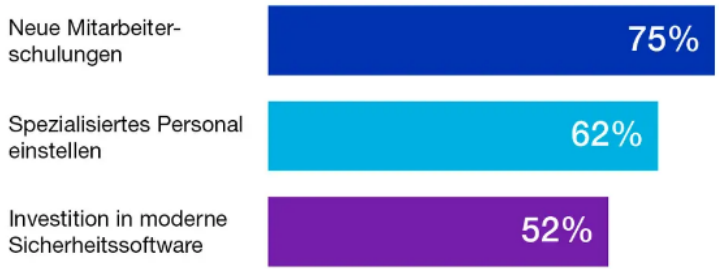


Quelle: Hiscox Cyber Readiness Report 2025 (www.hiscox.de/crr2025)

Erkenntnisse Hiscox Cyber Readiness Report 2025
Cyber-Resilienz

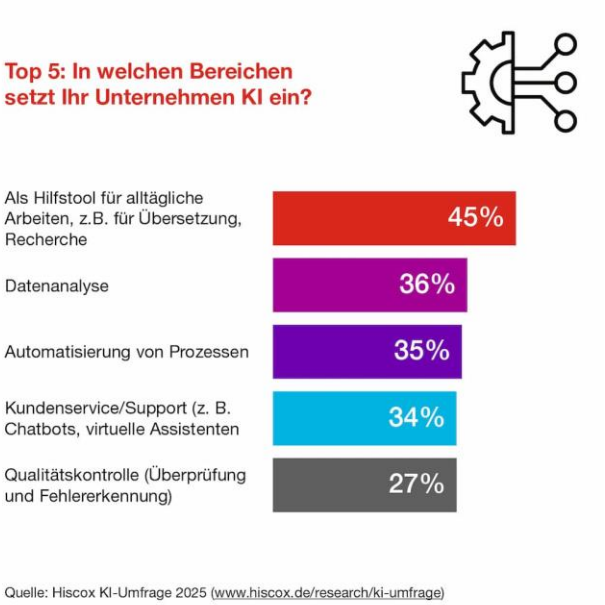
Investition in präventive Maßnahmen für mehr Cyber-Resilienz

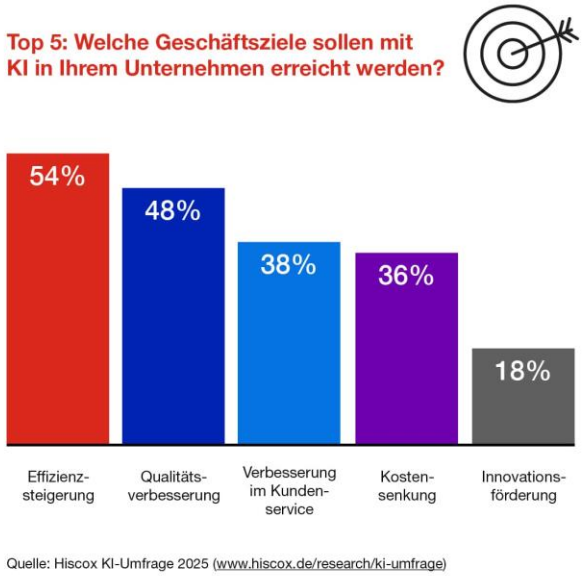
Folgendes haben die befragten Unternehmen konkret geplant:



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

Erkenntnisse Hiscox Cyber Readiness Report 2025
Anwendung von KI





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

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.

Ein Blick in die Schaden-Praxis
Wir übergeben das Wort
an Daniel Schätzle…

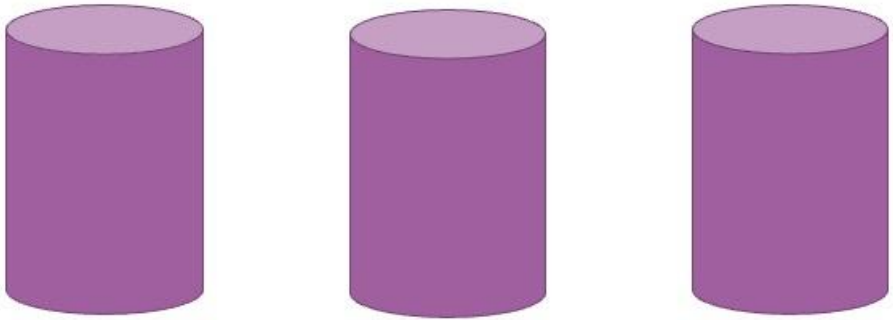
HÄRTING

KI & Cyberrecht

Hiscox IDD-Days ´26

RA Daniel Schätzle | HÄRTING Rechtsanwälte

Die drei Säulen des IT-Sicherheitsrechts in der Beratungspraxis



Prävention

Incident-Handling

Schadens-abwehr

KI-Einsatzszenarien

„Normaler“ Einsatz von KI im Unternehmen

IT-Sicherheitsstruktur setzt KI zur Angriffserkennung und Abwehr ein

Entwicklung von KI-Lösungen

Angreifer nutzen KI

HÄRTING

Cyber & KI
Compliance-Anforderungen

AI Act – Risikobasierter Ansatz

Hochrisiko KI

- **Sicherheitsregulierte Produkte & deren Sicherheitsbauteile**
  - **z.B. Spielzeug, Aufzüge, Funkanlagen, Schutzausrüstungen, Medizinprodukte**
- **Verwendung in Hochrisikobereichen**
  - **z.B. Biometrie, kritische Infrastruktur, Arbeits- und Personalmanagement**
- **Pflichten für Anbieter, u.a.**
  - **Risikomanagementsysteme**
  - **Dokumentation**
  - **Cybersicherheit**
- **Pflichten für Betreiber, u.a.**
  - **angemessene technische und organisatorische Maßnahmen (TOMs), um den sicheren und ordnungsgemäßen Betrieb des KI-Systems zu gewährleisten**

NIS2

- **Umsetzung in Deutschland seit 12/25**
- **BSI-Gesetz maßgeblich**
- **Anwendbarkeit für mittlere und große Unternehmen**
  - **Mitarbeiterzahlen / Umsatzzahlen maßgeblich**
- **sowie im Bereich KRITIS**
- **Nur für bestimmte Sektoren**

NIS2 - Sektoren

Besonders wichtige Einrichtungen	Wichtige Einrichtungen	
Große Unternehmen	**Mittlere Unternehmen**	**Große u. mittlere Unternehmen**
Energie (Versorgung mit Strom, Fernwärme, Kraftstoff, Heizöl und Gas)		Transport u. Verkehr (Post/Kurierdienste)
Transport und Verkehr (Luft, Schiene, Schiff, Straßen)		Abfallbewirtschaftung
Finanzwesen (Bankwesen und Finanzmarktinfrastrukturen)		Produktion, Herstellung, Handel (Chemie)
Gesundheit		Produktion, Verarbeitung, Vertrieb (Food)
Wasser (Trinkwasser, Abwasser)		Verarbeitendes Gewerbe/Warenhersteller
Digitale Infrastruktur (z.B. RZ-Betreiber, Cloud-Computing-Dienste)		Anbieter digitaler Dienste
Weltraum		Forschung

NIS2 - Pflichtenüberblick

Pflicht	Norm	Besonders wichtige Einrichtungen	Wichtige Einrichtungen
Risikomanagement	§ 30	X	X
Meldepflichten	§ 32	X	X
Registrierungspflicht	§ 33	X	X
Unterrichtungspflicht	§ 35	X	X
Umsetzungspflicht der Geschäftsleitung	§ 38	X	X
Informationsaustausch mit dem BSI	§ 6	X	X
Nachweispflicht (auf Verdacht)	§ 63 (§ 64)	X	(X)

Maßnahmen Risikomanagement, § 30 BSIG

- **präventive TOMs ergreifen, um Auswirkungen von Sicherheitsvorfällen möglichst gering zu halten**
  - **Verhältnismäßigkeitsbewertung erforderlich**
  - **Dokumentationspflicht**
- **Mindestanforderungen in § 30 Abs. 2 aufgelistet**
  - **Stand der Technik**
  - **Einschlägige europäische und internationale Normen berücksichtigen**
  - **Gefahrübergreifender Ansatz**
- **Ggf. weitere Spezifizierung aufgrund zukünftiger Durchführungsrechtsakte und nationaler Rechtsverordnungen**
  - **DURCHFÜHRUNGSVERORDNUNG (EU) 2024/2690 DER KOMMISSION vom 17. Oktober 2024**

Maßnahmen Risikomanagement, § 30

1. Konzepte in Bezug auf die Risikoanalyse und auf die Sicherheit in der Informationstechnik,
2. Bewältigung von Sicherheitsvorfällen,
3. Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement,
4. Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Diensteanbietern,
5. Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von informationstechnischen Systemen, Komponenten und Prozessen, einschließlich Management und Offenlegung von Schwachstellen,
6. Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Sicherheit in der Informationstechnik,
7. grundlegende Verfahren im Bereich der Cyberhygiene und Schulungen im Bereich der Sicherheit in der Informationstechnik,
8. Konzepte und Verfahren für den Einsatz von Kryptografie und Verschlüsselung,
9. Sicherheit des Personals, Konzepte für die Zugriffskontrolle und für das Management von Anlagen,
10. Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung.

DSGVO

- **Datensicherheit als Teil der IT-Sicherheit**
- **Sicherheit der Verarbeitung, Art. 32 DSGVO**
  - **TOMs nach Stand der Technik**
  - **Art, Umfang, Umstände und Zwecke der Verarbeitung beachten**
  - **Eintrittswahrscheinlichkeit für Datenschutzverletzung**

DSGVO

- **Datensicherheit als Teil der IT-Sicherheit**
- **Sicherheit der Verarbeitung, Art. 32 DSGVO**
  - **TOMs nach Stand der Technik**
  - **Art, Umfang, Umstände und Zwecke der Verarbeitung beachten**
  - **Eintrittswahrscheinlichkeit für Datenschutzverletzung**

Pflichten für die Hersteller *(Art. 13 CRA)*

1. **Cybersicherheit schon in der Produktentwicklung beachten**
2. **Schwachstellen offenlegen**
3. **Supportzeitraum aufrechterhalten**
4. **Konformität mit den Anforderungen nachweisen**

Sicherheitsstufen

Einstufung	Norm	Beispiele
Standard	Art. 3 Nr. 1 CRA	Drucker, Bildbearbeitungssoftware
Wichtige Produkte Klasse I	Art. 7, Anhang III CRA	Browser, Passwort-Manager, Anti-Viren Software, Betriebssysteme, intelligente Türschlösser
Wichtige Produkte Klasse II	Art. 7, Anhang III CRA	Browser, Passwort-Manager, Anti-Viren Software, Betriebssysteme, intelligente Türschlösser
Kritische Produkte	**Art. 8 Anhang, IV CRA**	**Smartcards, Sicherheitsboxen, Smart-Meter-Gateways in intelligenten Zählern**

Bedeutung für die Cyberversicherung?

1. **Erfüllung von Maßnahmen als Voraussetzung für Abschluss**
2. **Angebote zur Prävention**
3. **Deckung trotz Verstoß gegen (neue) gesetzliche Vorgaben?**

HÄRTING

Angriffsszenarien mittels KI

Spear-Phishing

- **Gezielte Phishing E-Mail, die mittels KI erstellt wurde**
- **Nachricht enthält bösartigen Link**
- **Beispiel:**
  - **E-Mail-Account wird kompromittiert**
  - **KI überwacht über Wochen E-Mail-Kommunikation, u.a. zur Freigabe von Transaktionen**
  - **KI übernimmt Kommunikation**
  - **Folge: Freigabe von mehr als 1 Mio. Euro**

CEO-Fraud

- **Freigabe durch persönliche Bestätigung auf Führungsebene**
  - **Klassische Telefonanruf**
  - **Video-Call**

- **KI simuliert persönliche Freigabe**

Zero-Day-Exploits

- **KI gestütztes Scannen einer IT-Infrastruktur auf Schwachstellen mit Höchstgeschwindigkeit**
- **IT hat kaum eine Chance Schwachstellen selbst zu erkennen und zu schließen**
- **Beispiel:**
  - **Anbieter einer Cloud-Computing-Lösung übersieht nach einem (fehlerhaften) Server-Update eine Schwachstelle, die Zugangsmöglichkeiten eröffnet**
  - **KI nutzt Schwachstelle und verbreitet darüber Schadsoftware auf den einzelnen Kundeninstanzen**
  - **Nach Ausführung der Schadsoftware werden sämtliche Server-Instanzen, auch die der Kunden, gesperrt**
  - **Entsperrung gegen Zahlung von Bitcoin**
  - **Zuvor Datensammlung zur weitergehenden Erpressung**

Zugriff über einfache Verschlüsselung

- **(Remote-)Arbeitsplatzumgebungen sind nur einfach verschlüsselt**
- **Algorithmus durchläuft in Sekunden mögliche Passwörter und erhält dadurch Zugriff**
- **Ransomware-Angriff auf IT-Systeme**
  - **Wartung von Flugzeugen**
  - **Stillstandzeiten sind kritisch (und teuer)**
- **Problem**
  - **Keine Multi-Faktor-Authentifizierung**
  - **Obliegenheitsverletzung?**

HÄRTING

Umgang mit KI & Cyberrecht

Risikomanagement managen!

- **Wo wird KI im Unternehmen eingesetzt?**
- **Welche IT-sicherheitsrechtlichen Gesetzte sind zu beachten (AI Act, DSGVO, CRA, NIS2, DORA etc.)?**
- **Maßnahmen umsetzen und optimieren!**
- **Dokumentation!**
- **Angebote der Versicherer nutzen**
- **Obliegenheiten beachten**
- **Versicherer in Prozessen zum Incident-Handling einbeziehen**

HÄRTING

RA Daniel Schätzle

IT Recht, IT-Sicherheit, Software, Litigation

schaetzle@haerting.de

HÄRTING.fm

https://haerting.de/podcast/

HÄRTING Rechtsanwälte | www.haerting.de

Chausseestr. 13, 10115 Berlin | Tel. +49 30 28 30 57 40 | Fax. +49 30 28 30 57 44

Chancen durch KI:
Beispiele für konkrete Einsatzgebiete

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

Wie agieren in einer KI-unterstützten Bedrohungslage?

- Konsequente MFA-Nutzung und Kennzeichnung externer Kommunikation
- 4-Augenprizip 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-LLM´s

HISCOX

Vielen Dank für Ihre Aufmerksamkeit