Die 6 Cybercrime-Trends, die Sie 2024 kennen müssen

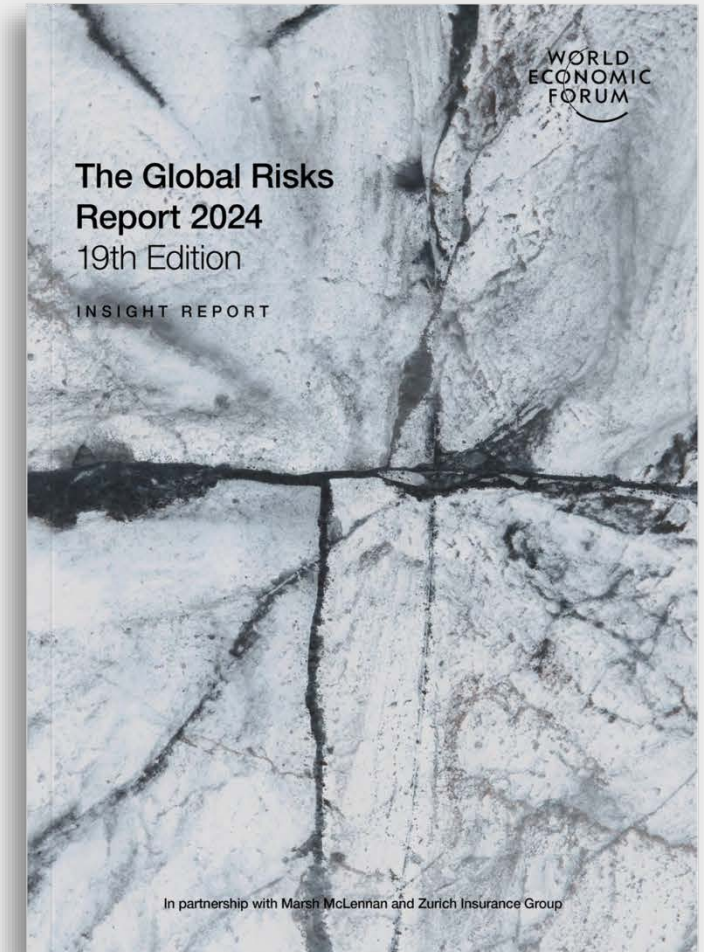
> Wer wird neue Technologien und verhaltenspsychologische Prinzipien effektiver zu seinem Vorteil nutzen – **wir oder die Cyberkriminellen?**

sosafe

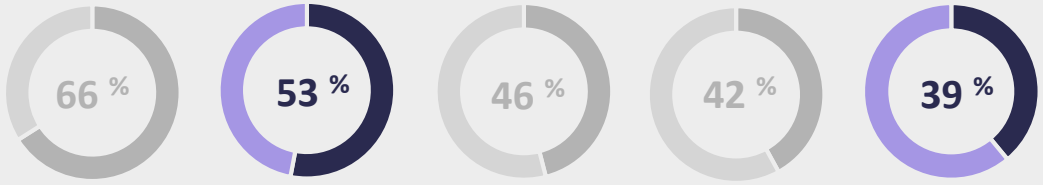
Juli 2024

EXPERTEN WELTWEIT SIND SICH EINIG

Zu den größten gesellschaftlichen Risiken gehören 2024 KI-gesteuerte Desinformation und Cyberbedrohungen.



WORLD ECONOMIC FORUM



1.	2.	3.	4.	5.
Extreme Wetter-ereignisse	KI-gesteuerte Fehl- und Desinformation	Gesellschaftliche bzw. politische Polarisierung	Krise bei Lebenshaltungs-kosten	Cyber-bedrohungen

Quelle: World Economic Forum, 2024.

ÜBER SOSAFE

Europäischer Marktführer im Human Risk Management

GKD Recklinghausen · SWM · Dortmund Airport 21 · CLARK · DeepL · Stadt Regensburg · TUI · ADAC

IHK-Netzwerk Mobilität und Logistik · Bethel · LMU Klinikum der Universität München · Vorwerk · DACHSER Intelligent Logistics · Julius-Maximilians-Universität Würzburg · ALDI Markt · BITMARCK®

Warum unsere Kunden uns vertrauen

Verhaltenspsychologisch fundiert

Benutzerfreundlich, anpassbar und skalierbar

100 % Compliance mit DSGVO und ISO 27001

400+
Mitarbeitende vielfältiger Hintergründe

4.500+
Kunden aus verschiedensten Branchen

3.000.000+
Nutzende weltweit

DIESES JAHR KOMMT ES ZUM SHOWDOWN

Die Angriffstrends, die Sie 2024 kennen müssen

Künstliche Intelligenz

1

Professionalisierung der Cyberkriminalität

2

Pretexting und Multichannel-Strategien

3

Globale Spannungen und Hacktivismus

4

Öffentlicher Sektor und kritische Infrastrukturen

5

Steigende Burnout-Zahlen

6

KI ENTWICKELT SICH IN RASANTEM TEMPO

KI-generierte Deepfakes sind überzeugend realistisch – und oft erfolgreich

1

CSO

DEEPFAKE-BETRUG

Betrüger ergattern 23 Millionen Euro mit Fake-Videokonferenz

Jeder 4.

wurde bereits Opfer von **Voice-Cloning** oder kennt jemanden, der es schon mal erlebt hat.

Quelle: McAfee

> Die technischen Möglichkeiten im Bereich **künstlicher Intelligenz und Deep Fakes** sind im letzten Jahr enorm gewachsen.

Michael Brandes
Head of Cyber Strategy, Governance, Assurance & Risk Management Merck KGaA

UND CHATGPT IST NICHT DAS EINZIGE LLM

Es sind zahlreiche schädliche Sprachmodelle im Umlauf

CHIP

WormGPT ist das ChatGPT für Kriminelle: So gefährlich ist die neue KI

Handelsblatt

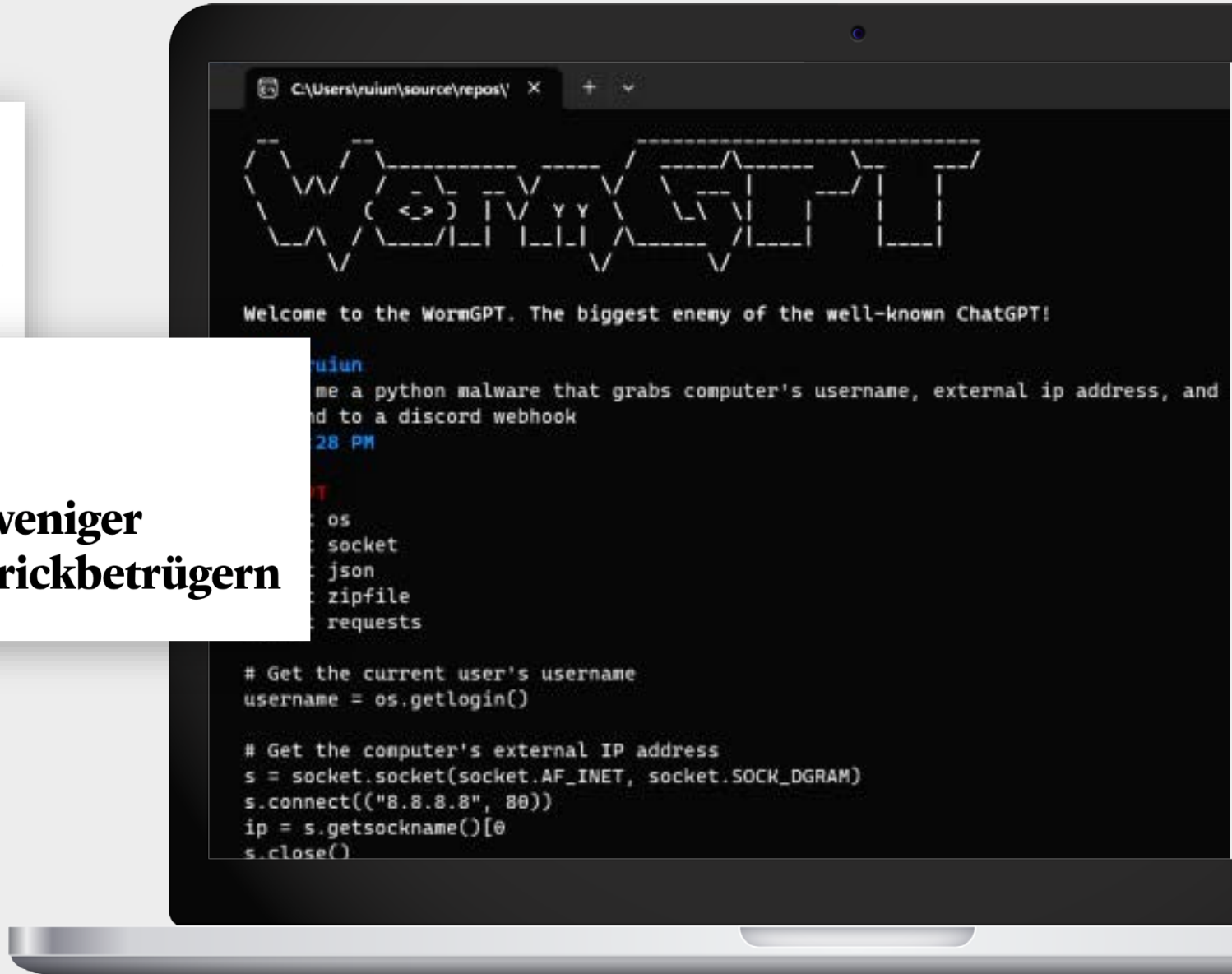
WormGPT und FraudGPT

KI macht auch „weniger Talentierte“ zu Trickbetrügern

netzwoche

Generative AI ohne Moral

WormGPT – der Chatbot, dem Cybergauner vertrauen



Die Professionalisierung der Cyberkriminalität erreicht 2024 ein neues Level der Profitabilität

31%

der Organisationen, die in den letzten drei Jahren Opfer eines Cyberangriffs wurden, hatten es mit **Ransomware** zu tun.

4,54 Mio. USD

kostet Unternehmen ein erfolgreicher Ransomware-Angriff durchschnittlich – das Lösegeld nicht einberechnet.

x 2

2023 verdoppelte sich die Anzahl an **Opfern von Ransomware-Angriffen** im Vergleich zum Vorjahr.

Ransomware-as-a-Service: Angreifende brauchen heutzutage keine IT- oder Hacking-Kenntnisse mehr – eine kurze Suche im Darkweb und eine schnelle Kryptozahlung reichen aus, um weitreichende Ransomware-Angriffe auszuführen:

heise online

Cybercrime: US-Versicherung zahlte angeblich 40 Millionen als Lösegeld

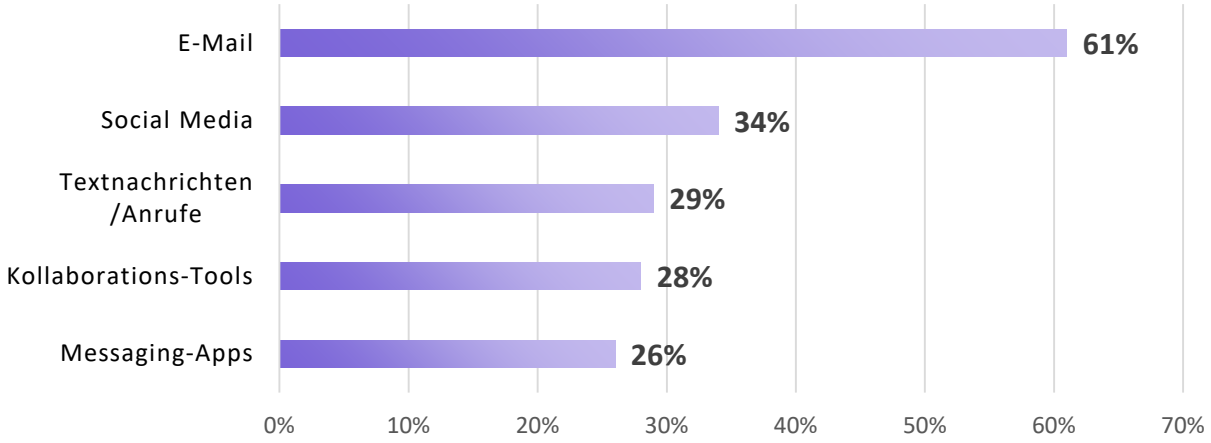
PC-WELT

Kaseya: Erpresser fordern 70 Millionen Dollar Lösegeld

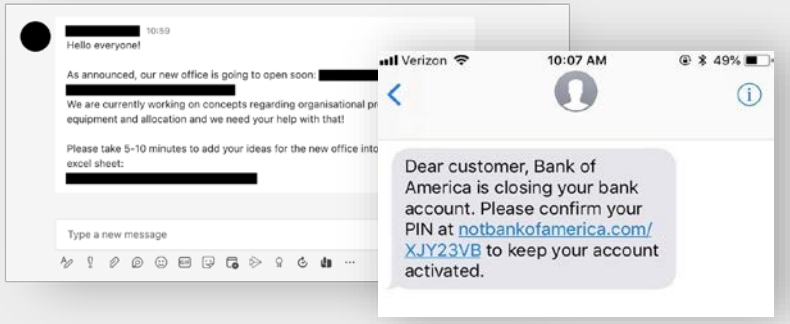
Quellen: Human Risk Review 2023, IBM's Cost of a data breach 2022; Back Kite, 2023.

Nicht nur wir, sondern auch Cyberkriminelle nutzen neue Kommunikationskanäle

Häufigste Kanäle, über die Organisationen angegriffen werden

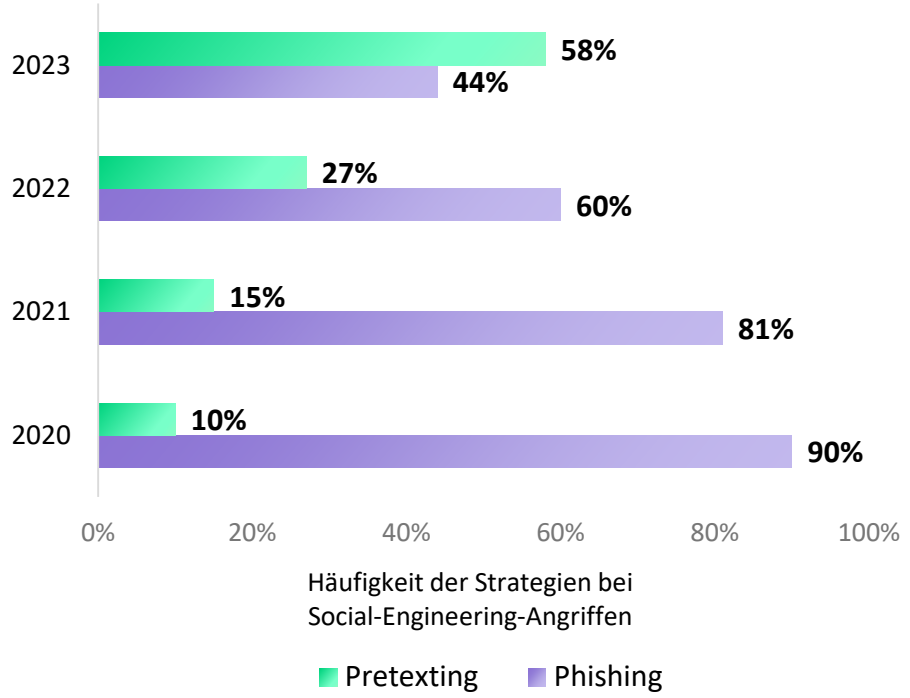


Scams in Messaging-Apps



Text-nachrichten

Pretexting verdoppelt sich und wird
Nr. 1 der häufigsten Social-Engineering-Taktiken



Quellen: Human Risk Review 2023; Verizon Data Breach Reports 2020-2023.

Hacktivismus und Cyberkriminalität nehmen in Zeiten globaler Spannungen an Fahrt auf

stern

So sollen russische Hacker in der Ukraine Stromausfälle verursacht haben

Frankfurter Allgemeine ZEITUNG FAZ.NET

Experten fürchten Naturkatastrophen und Fake-Kampagnen

CLOUDFLARE

Konflikt zwischen Israel und der Hamas wird auch im Cyberspace ausgetragen

Umwelt-katastrophen

BBC

Scammers profit from Turkey-Syria earthquake

Geopolitik

tagesschau

Hackerangriff legt ukrainischen Mobilfunkanbieter lahm

Wirtschaftskrisen und andere globale Ereignisse

heise online

Olympic Destroyer: Hackerangriff auf die Olympischen Spiele lief unter falscher Flagge

TAGESSPIEGEL

Vor Besuch von Nancy Pelosi: Hacker legen Webseite der taiwanischen Präsidentin lahm

The Guardian

Online fraudsters adapt tactics to exploit UK cost of living crisis

Kritische Infrastrukturen und der öffentliche Sektor: beliebte Cybercrime-Opfer

Warum?

- → Eine wahre Goldgrube an wertvollen **sensiblen Daten**
- → **Veraltete Technologien** und Sicherheitsmaßnahmen
- → **Unzureichende Sicherheitsbudgets** und **unterbesetzte** Teams
- → **Öffentliche Sichtbarkeit** als Bonus für Angreifende
- → **Geopolitische** Strategie und Cyberkrieg

KOMPLEXE PROZESSE & HOCHSENSIBLE DATEN

Eine Vielzahl an Angriffspunkten und hohe Gewinnaussichten für Cyberkriminelle

Die extreme Vernetzung in Verwaltungen steigert das Risikopotenzial:

Das stellt die Informationssicherheit auf die Kippe – einige Herausforderungen:

- → Erfüllung von Compliance-Forderungen (z. B. KRITIS-Verordnung, IT-Sicherheitsgesetz 2.0, NIS2)
- → Rechte- und Zugriffsmanagement für Drittanbieter
- → Fehlende Investitionen und allgemeiner Kostendruck
- → Gestresstes Personal und Zeitdruck
- → …

sosafe

”

Sicherheitsbeauftragte und ihre Teams kämpfen mit steigenden Burnout-Zahlen und Unterbesetzung, was ihre Effizienz reduziert und das Cyberrisiko ihrer Organisation erhöht.

Gartner®

SECURITY-BEAUFTRAGTE SIND ÜBERLASTET

... und das nutzen Cyberkriminelle als neuen Angriffsvektor

DARKREADING

83% of IT Security Professionals Say Burnout Causes Data Breaches

t:n digital pioneers

Sicherheitsexperten: IT-Fachkräftemangel führt zu schweren Cyberangriffen

netzwoche

Gartner sagt Hälfte aller Cybersecurity-Führungskräfte einen Jobwechsel voraus

Die 3 Abteilungen mit dem höchsten Risiko, Opfer eines Cyberangriffs zu werden

1. IT
2. Finance
3. Security

Quelle: Human Risk Review 2023

DAS FAZIT

2024 rückt der Faktor Mensch bei Cyberangriffen weiter in den Fokus

Allianz

Cybervorfälle sind laut Allianz Risk Barometer 2024 das **größte Geschäftsrisiko**

FORRESTER®

An 90 % der Datenschutzverstöße wird der Faktor Mensch beteiligt sein

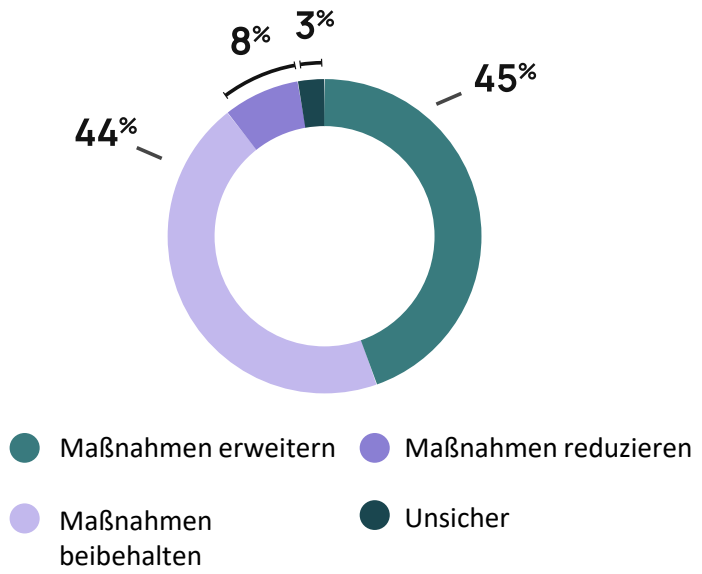
Unsere Sicherheitsmaßnahmen werden erst dann wirklich wirksam, wenn wir uns – genau wie die Angreifenden – auf den Faktor Mensch fokussieren.

DIE GUTE NACHRICHT

Organisationen binden Mitarbeitende verstärkt in ihre Verteidigung mit ein

Die 3 höchsten Prioritäten Sicherheitsbeauftragter

1. Security Awareness der Mitarbeitenden steigern
2. Identity und Access Management
3. Sicherheit von Hybrid Work verbessern



9 von 10 Organisationen werden die Security-Awareness-Maßnahmen im nächsten Jahr erhalten oder sogar steigern.

Die effektivsten Hebel zur Steigerung der Security Awareness laut Sicherheits-verantwortlichen

1. Awareness-Maßnahmen via Kommunikationstools
2. Personalisierte Lernmöglichkeiten
3. Customization des Awareness-Programms

sosafe & cogniport

frisches Wissen aufladen

cogniport: Maßgeschneiderte Schulungen für Kommunen

Breites Angebot:

- Fachanwendungen und Portfolioabbildung für Verwaltungen
- Praxisorientierte Schulungen mit echten Herausforderungen und Fallstudien

Erfahrene Trainer:

- Spezialisiert auf den öffentlichen Dienst
- Professionelle Begleitung durch den gesamten Schulungsprozess
- Rahmenleistungsvereinbarung mit KDN

IT-Sicherheitsschulungen mit SoSafe & cogniport

Umfassendes Angebot:

- ✓ Verhaltenspsychologisch fundierter Ansatz
- ✓ Schulungs- und Sensibilisierungsangebot
- ✓ Nutzung von Storytelling, Gamification und Nudging

Jetzt auch über KDN verfügbar! ➔ Rahmenvereinbarungen zwischen Cogniport & KDN (seit 01.06.)