Die Rolle des Menschen im Kampf gegen Cyberkriminalität

... und warum wir verpflichtet sind Menschen sicherer zu machen

sosafe

ÜBER SOSAFE

Europäischer Marktführer im Human Risk Management

GERRY WEBER · SOS CHILDREN'S VILLAGES · CLARK · WWF · DeepL · ALDI · DAIMLER TRUCK · TUI · ADAC

BAUERFEIND · SCHÜCO · Handelsblatt · VORWERK · DACHSER Intelligent Logistics · CANYON · WAGO

Warum unsere Kunden uns vertrauen

Verhaltenspsychologisch fundiert

Benutzerfreundlich, anpassbar und skalierbar

100 % Compliance mit DSGVO und ISO 27001

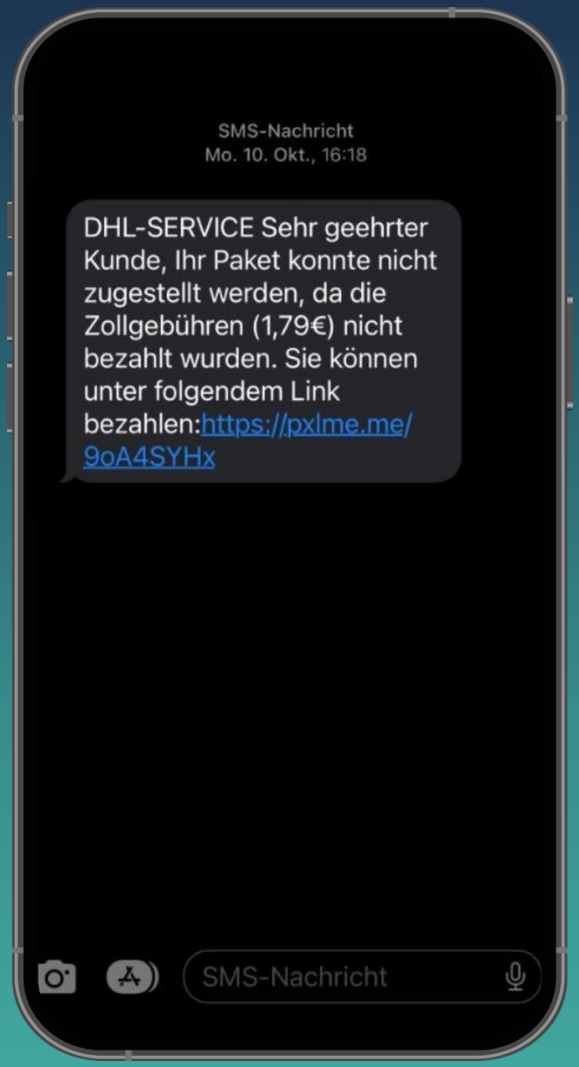
500+
Mitarbeitende vielfältiger Hintergründe

5.000+
Kunden aus verschiedensten Branchen

3.500.000+
Nutzende weltweit

BEVOR WIR STARTEN

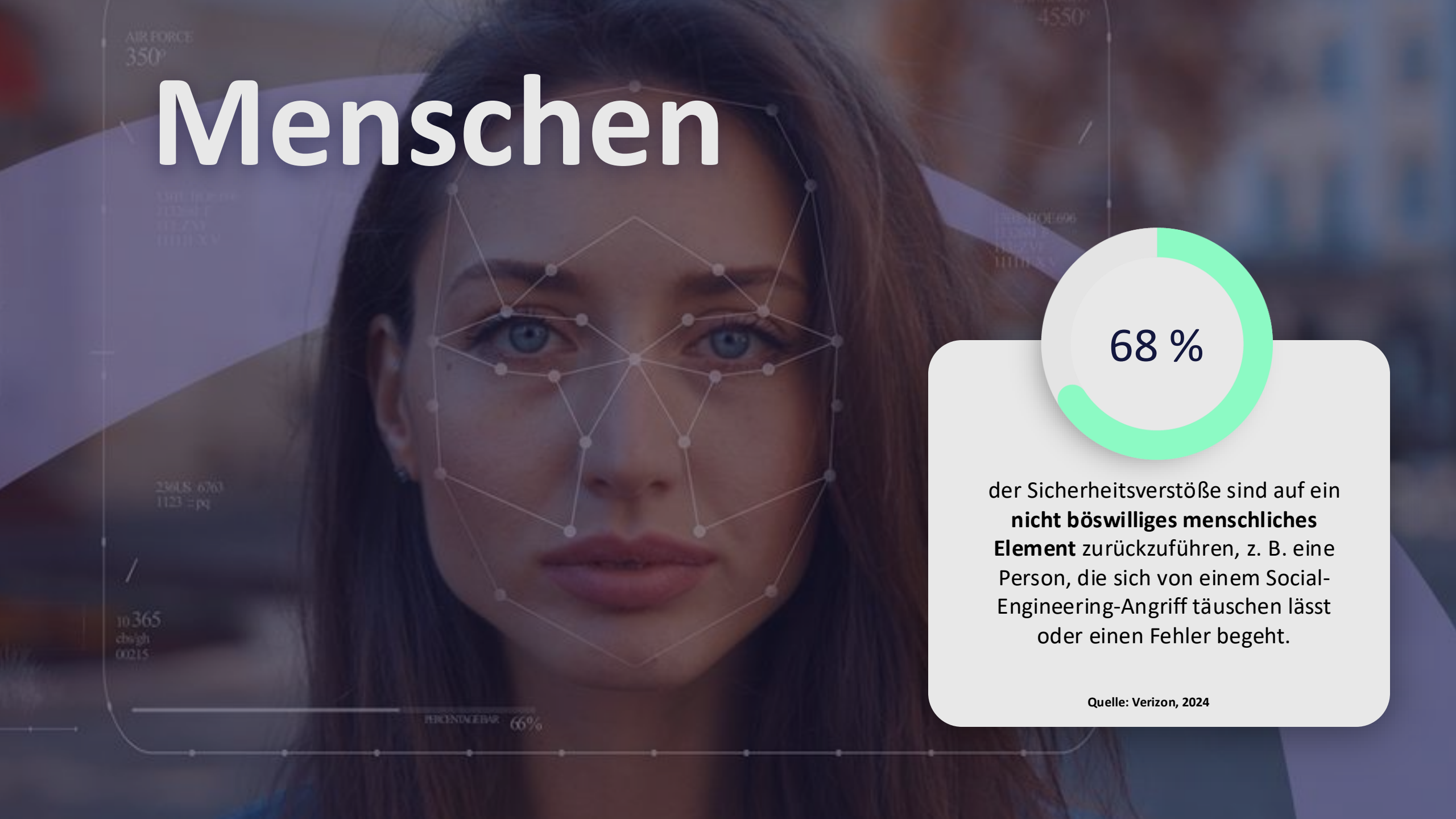
SCHON BEKOMMEN?



FAKT IST:

Cyberkriminelle konzentrieren ihre Angriffe auf ein Hauptziel

Menschen



der Sicherheitsverstöße sind auf ein **nicht böswilliges menschliches Element** zurückzuführen, z. B. eine Person, die sich von einem Social-Engineering-Angriff täuschen lässt oder einen Fehler begeht.

Quelle: Verizon, 2024

UBER HACK

Wie Lapsus$ Psychology genutzt hat um Uber zu hacken

Menschlicher Faktor

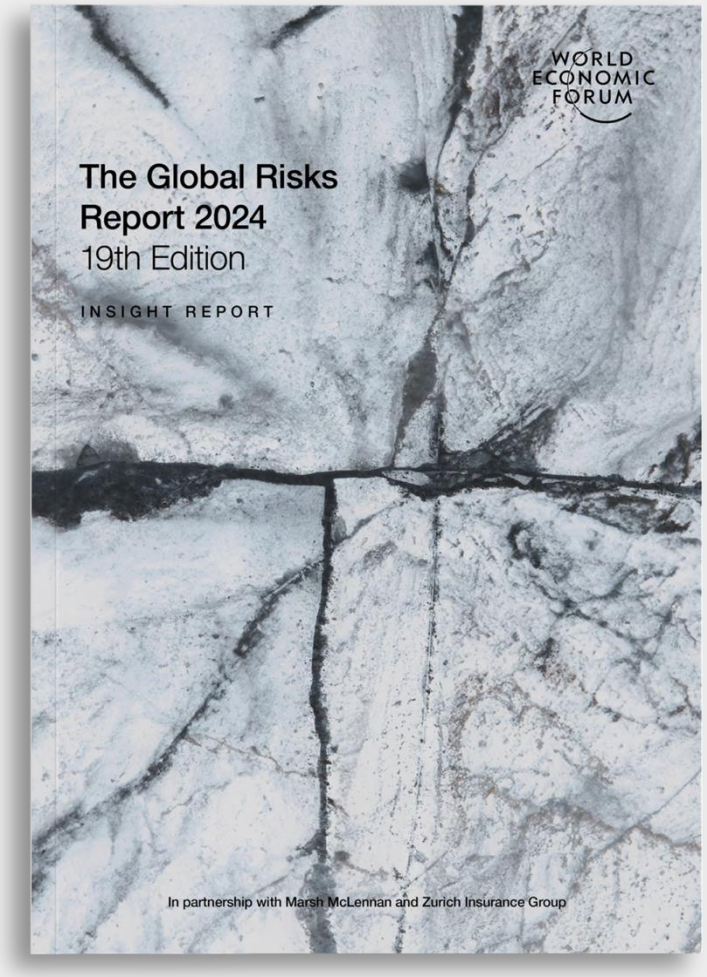
→ Cyber-Kriminelle (Organisationen) **entwickeln sich ständig weiter**
→ Diese Innovationen sind vor allem **psychologischer** Natur

sosafe

Quellen: Cyber Security Drive, 2022, The Hackers News, 2022.

DAS BEDROHUNGSPOTENTIAL STEIGT DRAMATISCH

Zwei der größten Risiken für die Gesellschaft im Jahr 2024 sind KI generierte Desinformationen und Cyberangriffe



Mehr als 32 Mrd. gelöschte Fake- Profile seit 2017

3,4 Mrd. Phishing Mails/Tag

300.000 SMS Angriffe/Minute

sosafe

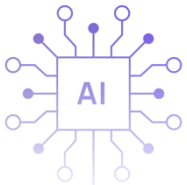
DIE BEDROHUNG WÄCHST

… dahinter stehen drei große Antriebsfaktoren

Neue Technologien

79%

der Security-Verantwortlichen halten den Einsatz generativer KI durch Cyberkriminelle für besorgniserregend, bei Unternehmen mit mehr als 5.000 Mitarbeitern sind es sogar 86 %.



Globale Instabilität

75%

3 von 4 Security-Verantwortliche bestätigen, dass die geopolitische Lage das Sicherheitsrisiko ihrer Organisation erhöht hat.

Vernetzung

80%

der Security-Verantwortlichen erkennen zunehmend die Bedeutung der Lieferkettensicherheit.

Quelle: Human Risk Review, 2024

VERDICT

The state of cybersecurity: AI and geopolitics mean a bigger threat than ever

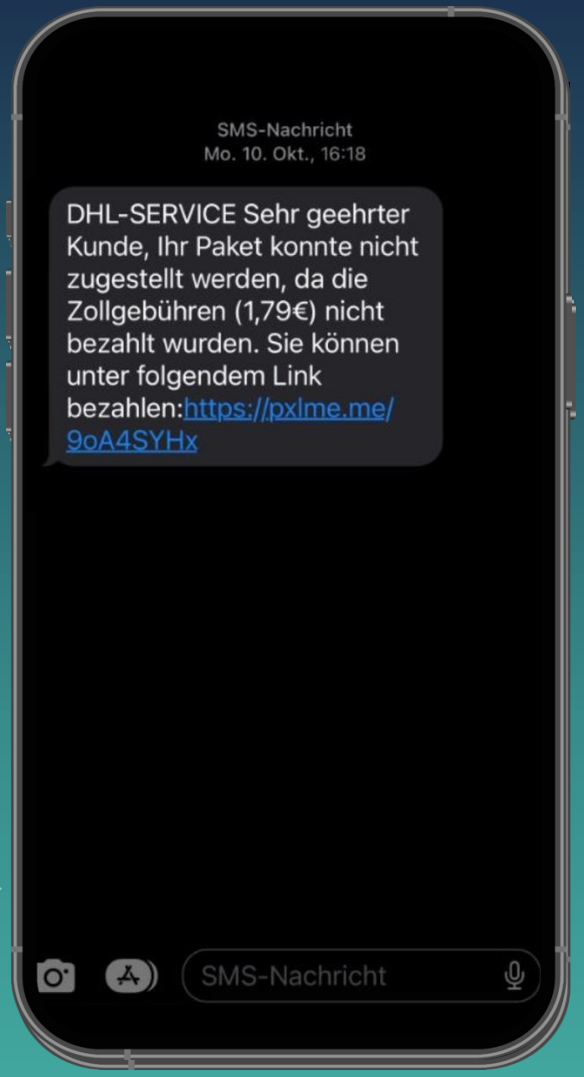
Cyber MAGAZINE

Article • Hacking & Malware

HP: Businesses Fear Physical Supply Chains Pose Cyber Risk

SMISHING EVOLUTION

... Cyberkriminelle lernen schnell



SMISHING VERMEIDEN

5 Tipps:

1. Klicke nicht auf Hyperlinks in Nachrichten von unbekannten oder verdächtigen Absendern.
2. Sei vorsichtig, wenn Du aufgefordert wirst zu zahlen oder vertrauliche Informationen herauszugeben.
3. Reagiere niemals auf SMS von unbekannten oder verdächtigen Nummern - nicht einmal, um sie zu beleidigen.
4. Halte das Betriebssystem und die Apps Deines Handys immer auf dem neuesten Stand.
5. Achte auf Social-Engineering-Kennzeichen, wie z. B. Emotionalisierung.

sosafe

DIESES JAHR KOMMT ES ZUM SHOWDOWN

Die Angriffstrends, die Sie 2024 kennen müssen

Künstliche Intelligenz

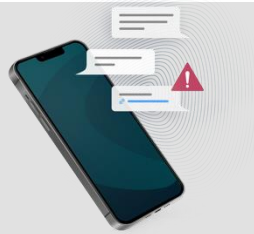
1

Professionalisierung der Cyberkriminalität

2

Pretexting und Multichannel-Strategien

3



Globale Spannungen und Hacktivismus

4

Disinformation-as-a-Service

5

Steigende Burnout-Zahlen

6

Hier herunterladen!

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

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

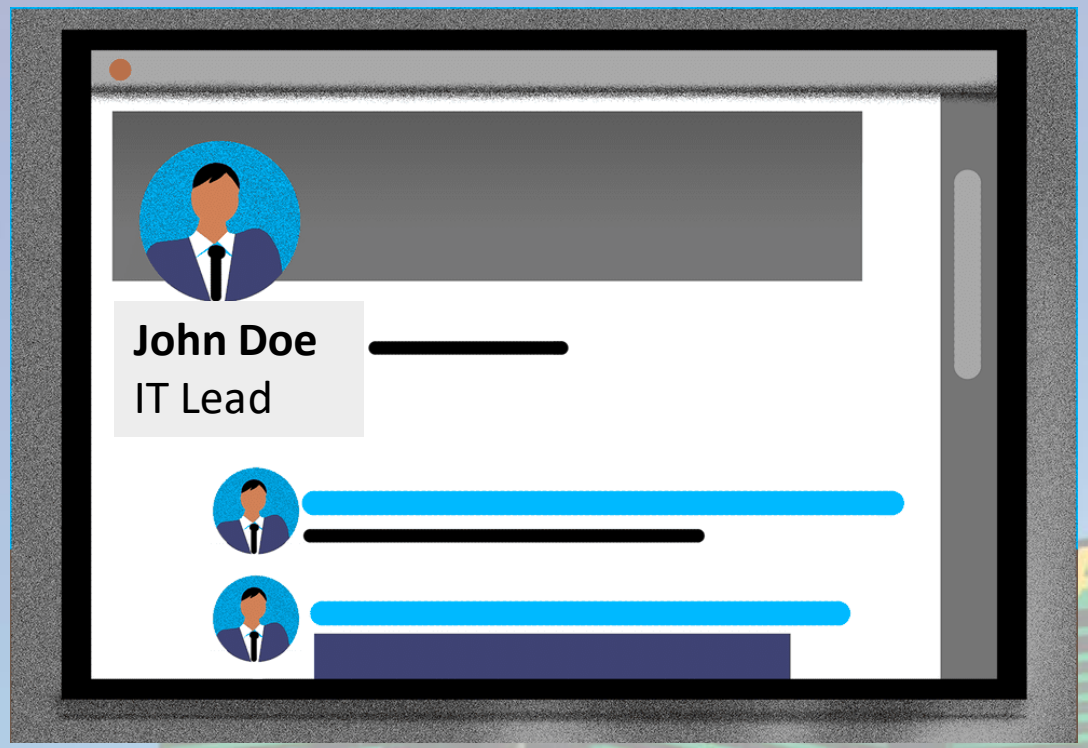
PC-WELT

Kaseya: Erpresser fordern 70 Millionen Dollar Lösegeld

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

When everone is fired up for the concert, but your boss decided the weekend is a great time for a system update…

Helpdesk Worker



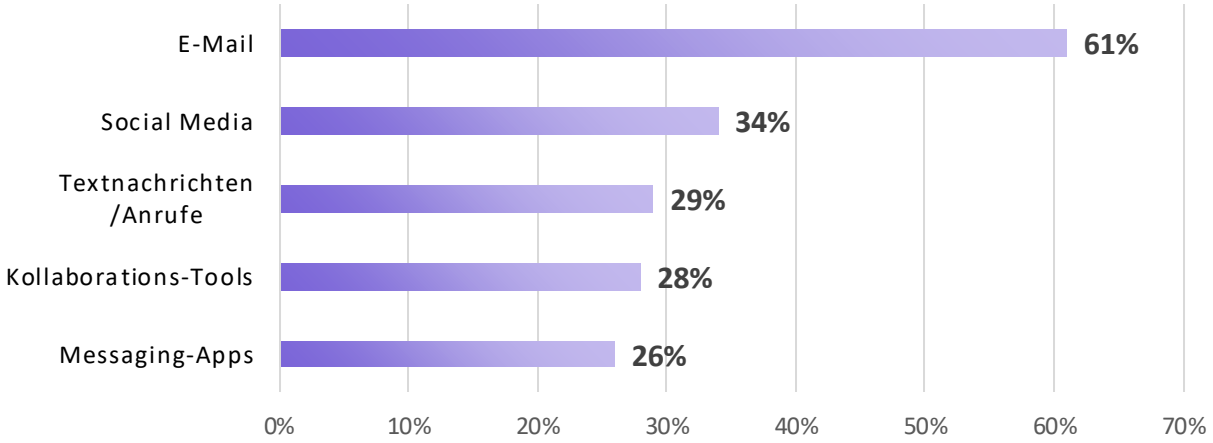
Mitarbeiter IT


MGM
EPICALLY EXTRAORDINARY
KA
CIRQUE DU SOLEIL
MGM GRAND
BRAD GARRETT'S COMEDY CLUB

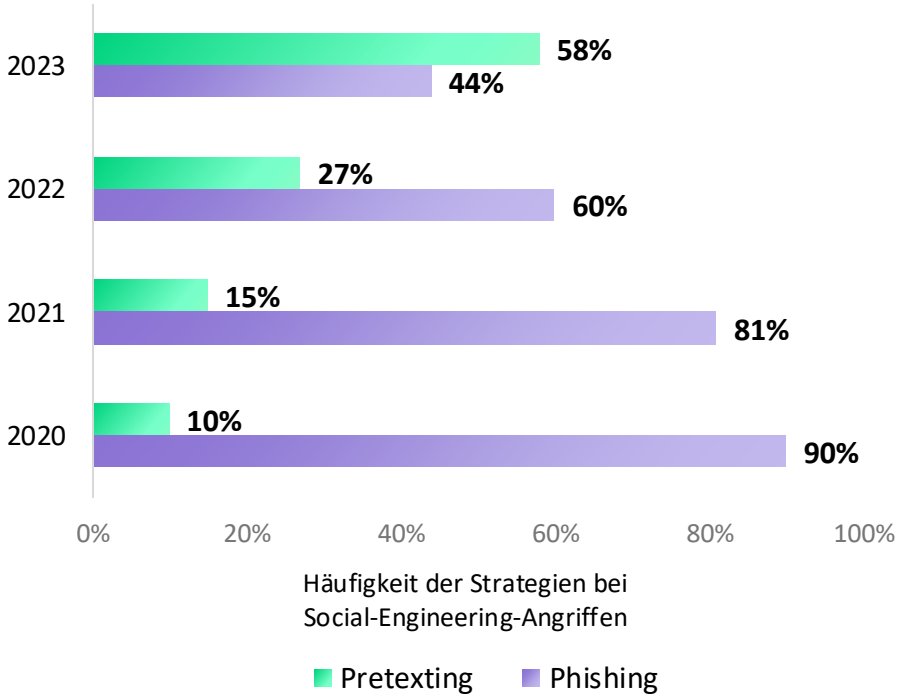

CAESARS PALACE
VIVA MO2 VEGAS
ABSINTHE

Nicht nur wir, auch Cyberkriminelle nutzen neue Kommunikationskanäle

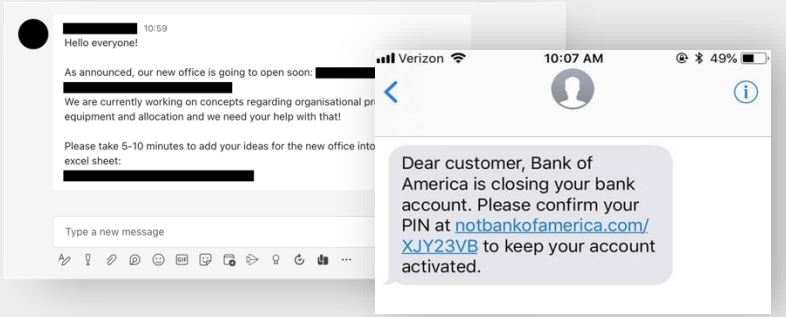
Häufigste Kanäle, über die Organisationen angegriffen werden



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



Scams in Messaging-Apps



Text-nachrichten

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

MULTICHANNEL ANGRIFF

Die Psychologie hinter dem Angriff

Hello Christian,

Great post. Absolutely nailed it. I see it exactly the same way.

Would love to connect.

Search

ort Move Flag Mark as Read Sync Block ...

External [redacted]

JB

To: Dr. Christian Reinhardt

Saturday, 11. May 2024 at 15:40

Hi Christian,

I must take this opportunity to emphasize once again how good your post is!

We are planning a major event on exactly this topic with great speakers. I would like to add you to this lineup.

I have simply planned the same fee as for the others.

Please see if that works for you.

speaker-info

sosafe 2024

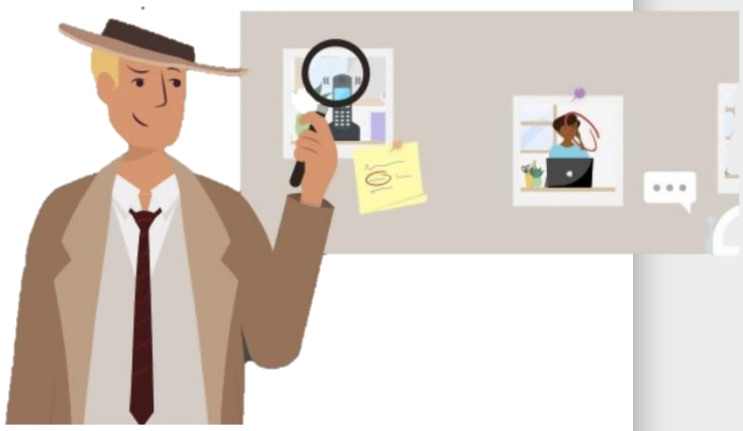
EIN EINFACHER SCHUTZ

3 Lebensretter

Wenn imme eine Nachricht eine starke Emotion auslöst – vorsicht!

1 **Kaffee**

2 **Kollegen**



3 **Recherche**

sosafe

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

BBC

Scammers profit from Turkey-Syria earthquake

Umwelt-katastrophen

Geopolitik

Wirtschaftskrisen und andere globale Ereignisse

tagesschau

Hackerangriff legt ukrainischen Mobilfunkanbieter lahm

heise online

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

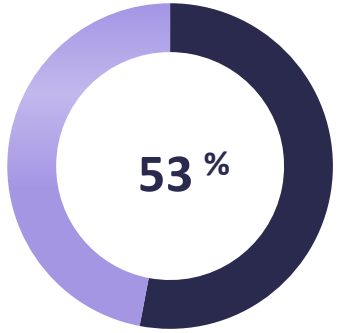
TAGESSPIEGEL

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

KI-getriebene Desinformation ist das größte Kurzzeitrisiko weltweit



2.
KI-gesteuerte Fehl- und Desinformation

WORLD ECONOMIC FORUM

Quelle: Time

WIRED

Slovakia’s Election Deepfakes Show AI Is a Danger to Democracy

“2024 finden in **77 Ländern** Wahlen statt – das betrifft etwa die Hälfte der Weltbevölkerung und knapp **60 %** des globalen Bruttoinlandsprodukts.

J.P.Morgan

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

Wir brauchen mehr Sicherheit bei der Arbeit und nicht mehr Arbeit in der Sicherheit

DIE WELT ETWAS SICHERER MACHEN

Ein Spiel ist nur dann fair, wenn jeder einzelne Spieler seine eigene Verantwortung für Fairness wahrnimmt.

Wir werden nur sicher sein, wenn jeder Einzelne seine eigene Verantwortung für die Sicherheit erkennt und übernimmt.

sosafe

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

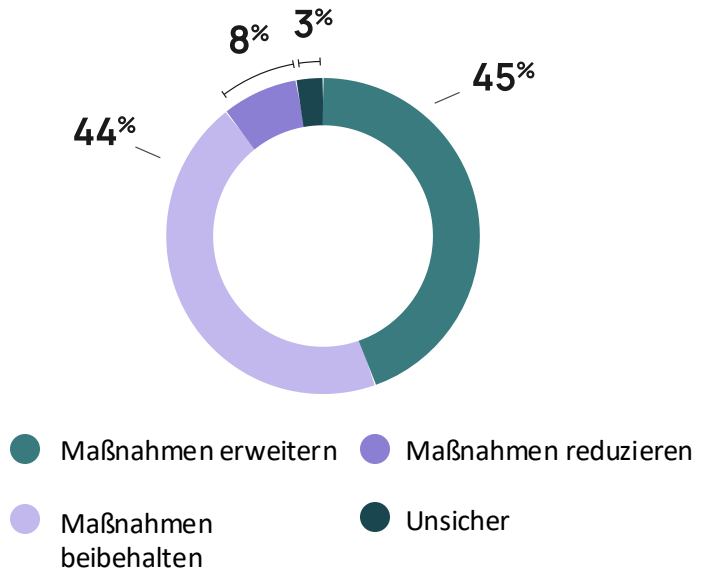
Unsere Sicherheitsmaßnahmen werden erst dann wirklich wirksam, wenn wir uns – genau wie die Angreifenden – auf den Faktor Mensch fokussieren.

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

DIE TRUTHAHN - ILLUSION

Lasst uns nicht auf Thanksgiving warten

powered by sosafe

Human Firewall Conference 2024

Die führende Security-Konferenz
mit Fokus auf dem Faktor Mensch

14.-15. November 2024

Melden Sie sich
zur HuFiCon24 an

Klingt spannend?

Lassen Sie uns diskutieren.

Dr. Christian Reinhardt
Awareness Evangelist
SoSafe

christian.reinhardt@sosafe.de

LinkedIn