Chillventa Specialist Forums 2022
Chillventa Fachforen 2022

CONNECTING
EXPERTS.

„Cybersicherheit – Der Mensch ist Angriffspunkt Nr. 1“

Michael Piotraschke, Awareness Specialist, SoSafe GmbH

sosafe

Oktober 2022

EINE KURZE VORSTELLUNG

Michael Piotraschke

Awareness Specialist

bei SoSafe Cyber Security Awareness

Fokus

Social Engineering, Integration von Awareness in den Arbeitsalltag

Kontakt

michael.piotraschke@sosafe.de

+49 221 650838-55

STATUS QUO

Die weltweite **Cyber-Bedrohungslage** verschärft sich drastisch

9 von 10

IT- und IT-Sicherheits-verantwortlichen sagen:
Die Cyber-Bedrohungslage hat sich verschärft

Nr. 1

Cybervorfälle gelten als
Nr. 1 Geschäftsrisiko (Allianz)

>1 Billion USD

Immense finanzielle Schäden
in Billionen-Dollar-Höhe

sosafe

Quelle: Human Risk Review 2022, Allianz Risk Barometer 2022

Spektakuläre Opfer

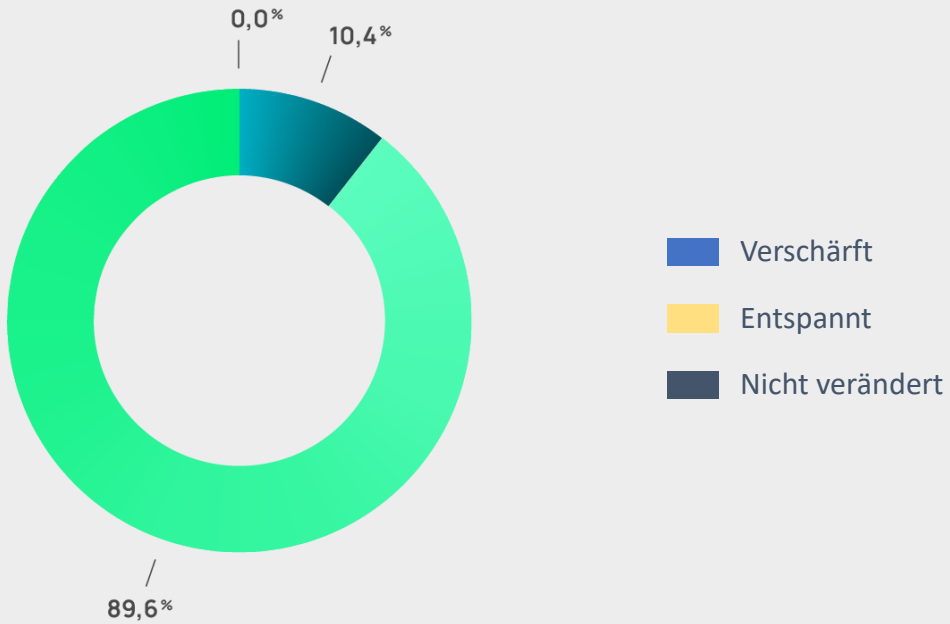
Cybercrime trifft Organisationen jeder Art und Größe

Der Faktor Mensch

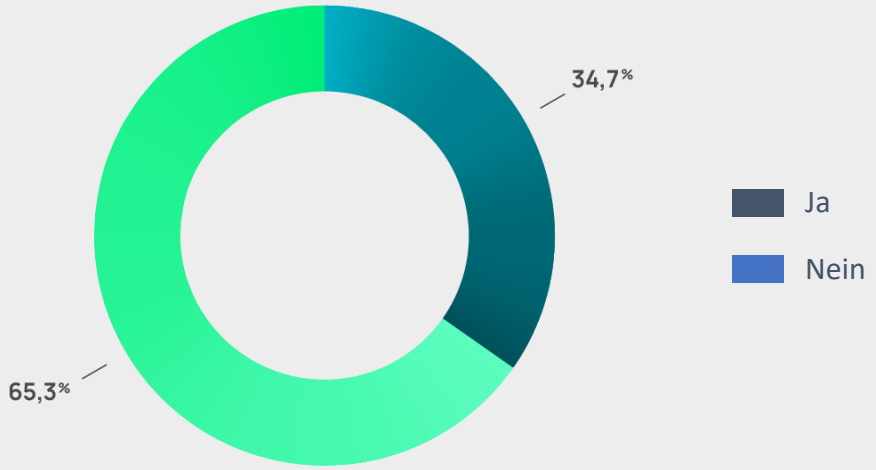
9 von 10 Angriffe starten bei den Mitarbeitenden

Jedes dritte Unternehmen hat 2021 selbst einen Cyberangriff erlebt

Rückblick auf das Jahr 2021: Wie haben Sie die Cyberbedrohungslage wahrgenommen?



Unsere Organisation (oder einer unserer Dienstleister) hat selbst einen Cyberangriff erlebt.



Quelle: Human Risk Review 2022

sosafe

Berichte über Cyberangriffe – und deren kostspielige Folgen – fluten die Nachrichtenspalten weltweit

CSO

UNI WUPPERTAL

Hacker legen Hochschul-Infrastruktur lahm

Keine E-Mails, kein Telefon, keine Online-Plattformen. Die Infrastruktur der Uni Wuppertal ist nach einem Cyberangriff massiv gestört.

BLEEPINGCOMPUTER

Costa Rica declares national emergency after Conti ransomware attacks

tagesschau

500.000 Datensätze betroffen

Rotes Kreuz von Hackern attackiert

Es sind Daten über Flüchtlinge oder vermisste Personen: Bei einem Cyberangriff auf das Internationale Rote Kreuz haben Hacker mehr als 500.000 Informationen über besonders Schutzbedürftige erbeutet.

CPO MAGAZINE

BBC

SpiceJet: Passengers stranded as India airline hit by ransomware attack

sosafe

Quellen: CSO, Bleeping Computer, Tagesschau, CPO Magazine, BBC

Woran liegt das?

Cyberkriminelle nutzen hybride Arbeitsmodelle für Angriffe aus

Was macht dezentral aufgestellte Organisationen zu so attraktiven Zielen für Angriffe?

Fehlende technische Absicherung

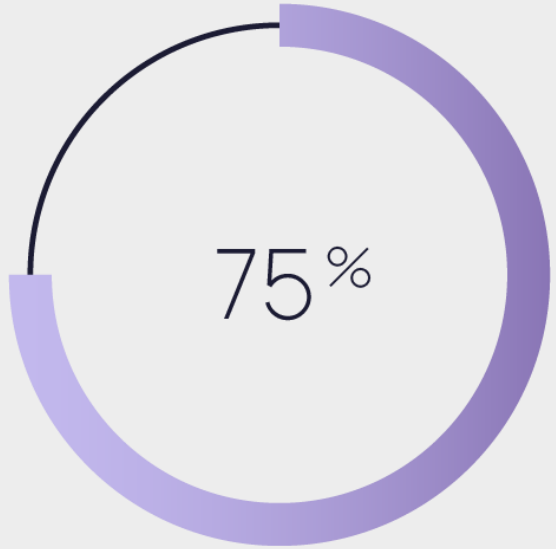
Nur 38 Prozent der Organisationen sichern geschäftliche Geräte per VPN ab.

Neue Angriffskanäle

Neue Kollaborationstools wie Microsoft Teams oder auch Mobiltelefone, bieten neue Angriffsflächen.

Unsicherheit und unzureichende Security Awareness

Von Pandemie und Homeoffice erschöpft, setzen sich Mitarbeitende weniger mit Sicherheit auseinander.



… sagen, dass **hybrides Arbeiten die Wahrscheinlichkeit von Cyberattacken erhöht hat.**

sosafe

Quelle: IW-Kurzbericht, Nr. 54 (2021), Human Risk Review 2022

„Loose lips save(d) ships!“ oder: Flurfunk schützt(e)

Klickrate Phishing-Mails nach Organisationsform

Prä-Corona

Zentral
(1 Standort, kein Remote Work)

12%

30%

Dezentral
(global verteilt, Remote Work)

sosafe

Quelle: Klickraten zweier Kurz-Kampagnen bei zwei Kunden vergleichbarer Größe, aber unterschiedlicher Organisationsform, vergleichbare Templates, Q1 – 2019.

CYBERCRIME-TRENDS 2022

Trendy Phishing: Anlassbezogene Angriffswellen und skrupellose Täuschungen

Phishing ist auf **Allzeithoch**: 1,03 Millionen erfolgreiche Phishing-Angriffe allein in Q1 2022

Cyberkriminelle greifen **aktuelle Themen** und Entwicklungen für zielgenaue Angriffe aus

Emotional manipulative Tricks bringen Menschen dazu, ihre Daten preiszugeben

Quelle: APWG 2022

ANLASSBEZOGENES PHISHING

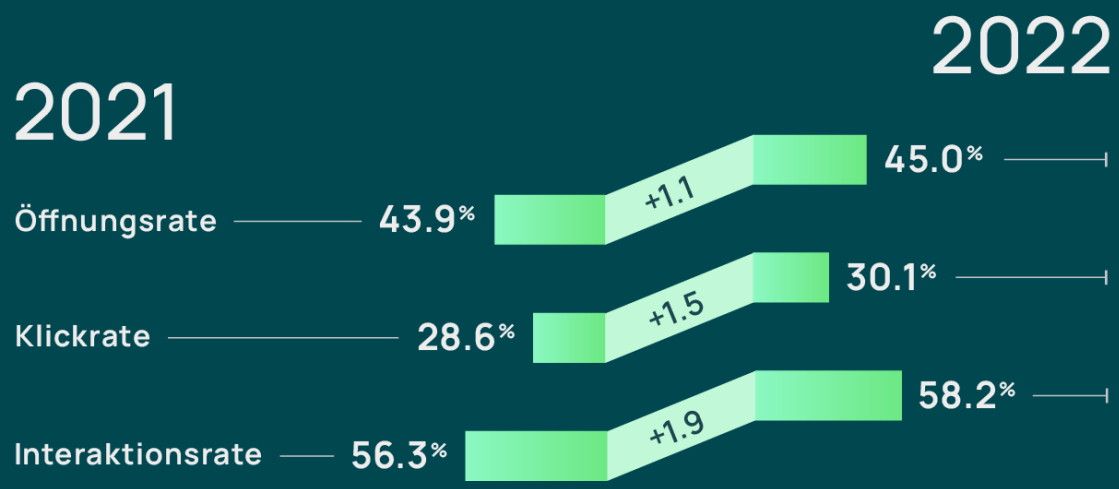
Phishing-Mails mit Bezug zu aktuellem Geschehen gehören mit zu den gefährlichsten

Die Top Phishing-Betreffzeilen 2021/2022

66 %	Folgende Aufgabe ist zu erledigen: Verteilung der Dokumente und Bewertung der Aufgaben
66 %	Sie haben 2 Erwähnungen
57 %	Wichtig: CORONA-Update

Aktueller Bezug + Druck/ Angst

Allgemein erhöhter Social-Engineering-Erfolg



sosafe

Quelle: Human Risk Review 2022

ANLASSBEZOGENES PHISHING

Aktuelle Anlässe bieten Cyberkriminellen genügend Futter

it-daily.net

Dridex-Malware: Geschmacklose Omikron Phishing-Kampagne

Pandemie

INDEPENDENT

Scam warning over fake omicron testing text messages

BSI warnt vor betrügerischen E-Mails in Zusammenhang mit Ukraine-Krieg

heise online

Krieg

ZEIT ONLINE

Phishing-Mails

Russland-Sanktionen: Betrüger zielen auf Bitcoins ab

Energie-/ Wirtschafts-krise

Bundesministerium
Soziales, Gesundheit, Pflege und Konsumentenschutz

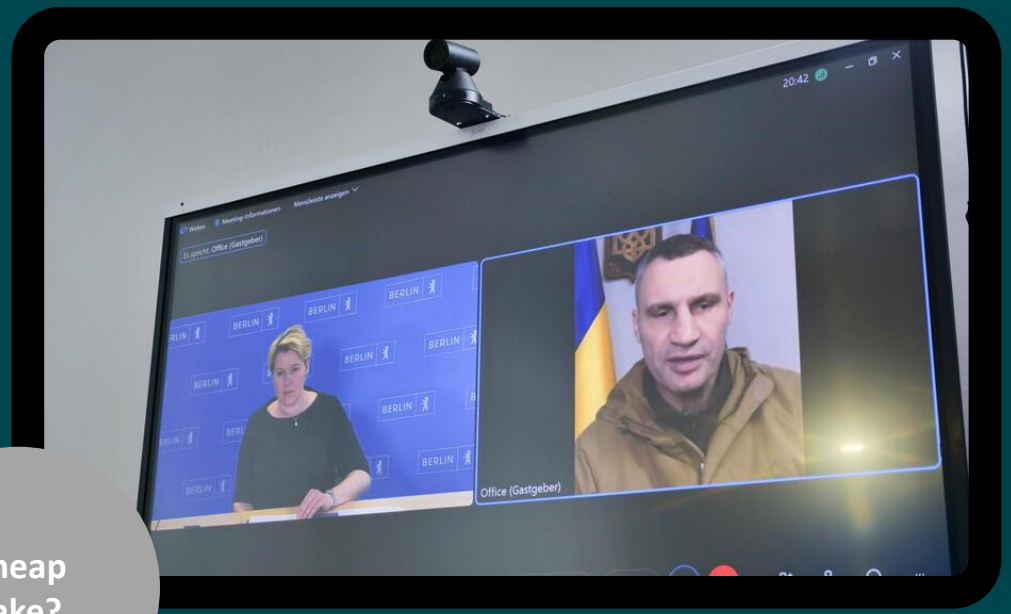
Kriminelle nutzen Energiekrise aus

So schützen Sie sich vor Fake-Onlineshops im Energiesektor

sosafe

Quellen: IT-Daily, The Independent, Die Zeit, Heise Online, BMASK Österreich

Wenn nun Künstliche Intelligenz (KI) ins Spiel kommt…



Cheap Fake?

Deep Fake

Quelle: Handelsblatt 2022

sosafe

… droht Social Engineering 2.0 und die nächste Generation von Phishing

Daten, um die KI zu füttern, und auch entsprechende **KI-as-a-Service-Tools** sind öffentlich immer einfacher zugänglich – auch für Cyberkriminelle

Cyberkriminelle können also bald ohne viel Aufwand KI für ihre Zwecke nutzen, zum Beispiel um

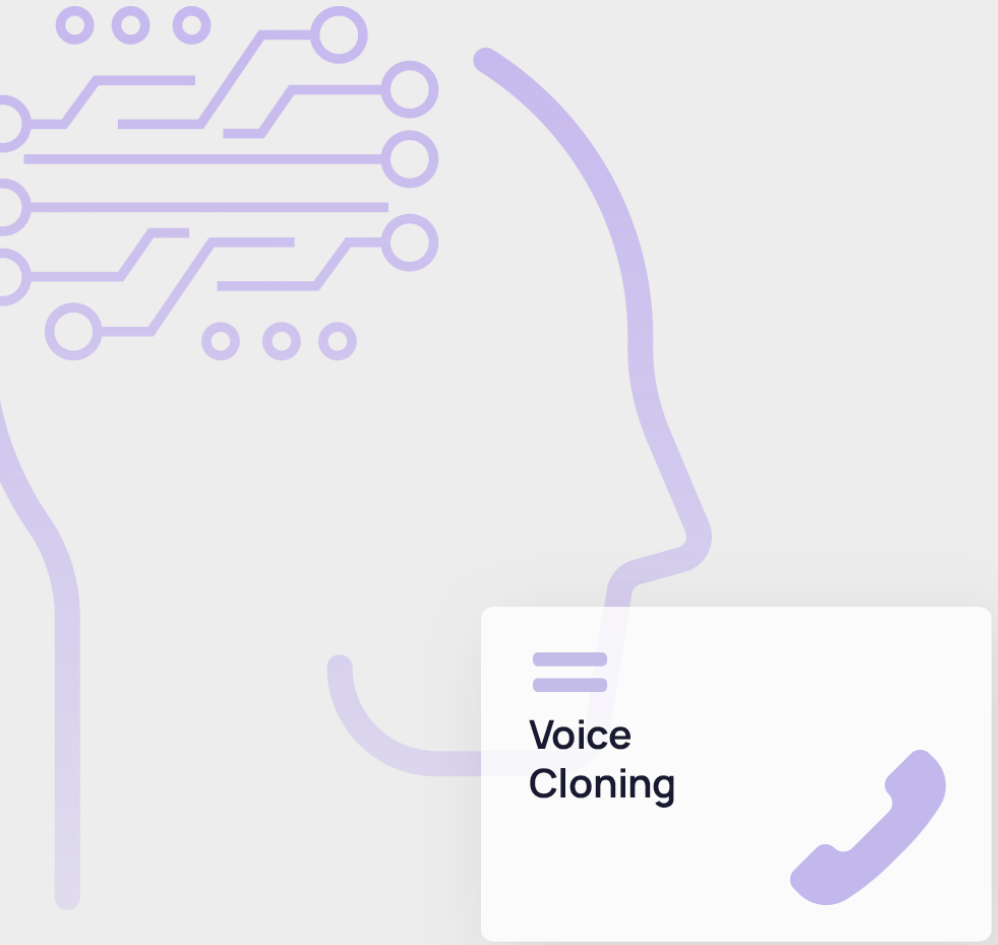
- → ihre Opfer mit realistischen Audio-/Videomaterial noch zielgenauer zu täuschen
- → die öffentliche Meinung zu beeinflussen
- → Spionage zu betreiben, siehe Beispiel Giffey

Quellen: TechCrunch, Reuters, Business Insider

sosafe

DEEPFAKES

KI eröffnet Cyberkriminellen neue Angriffsmethoden – zum Beispiel Voice Cloning



Voice Cloning

Vishing kombiniert mit Deepfakes: Angreifende imitieren die Stimme eines Vorgesetzten künstlich und bringen Mitarbeitende anschließend über einen Anruf dazu, sensible Informationen freizugeben oder Überweisungen zu tätigen

Forbes

Fraudsters Cloned Company Director's Voice In $35 Million Bank Heist, Police Find

Source: Forbes 2021

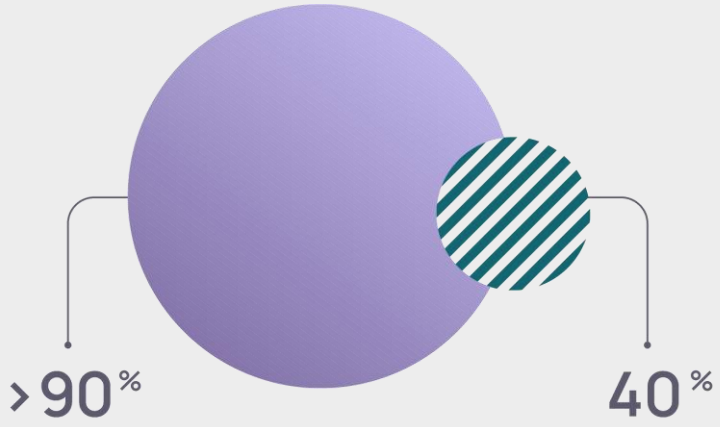
sosafe

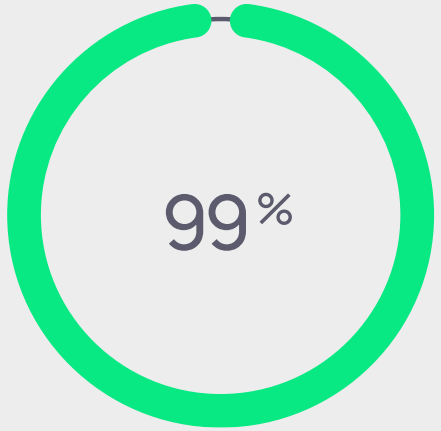
Was tun?

HERAUSFORDERUNG

Die „Security Awareness Gap“: Viele Organisationen sind nicht ausreichend vorbereitet – möchten ihre Sicherheitskultur aber stärken

Mehr als 90 % der IT- und Cybersicherheits-verantwortlichen sagen: Awareness ist wichtig für ihr Unternehmen.





der Befragten sagen, dass sie sich auf die Stärkung der Sicherheitskultur ihres Unternehmens konzentrieren wollen.

“Security Awareness Gap”

Trotzdem wird bei 40 Prozent der Unternehmen, die das Thema für wichtig oder sehr wichtig halten, das Awareness-Level der Mitarbeitenden immer noch als niedrig oder sehr niedrig eingestuft.

Quelle: Human Risk Review 2022

DAS BEHAVIORAL SECURITY MODELL

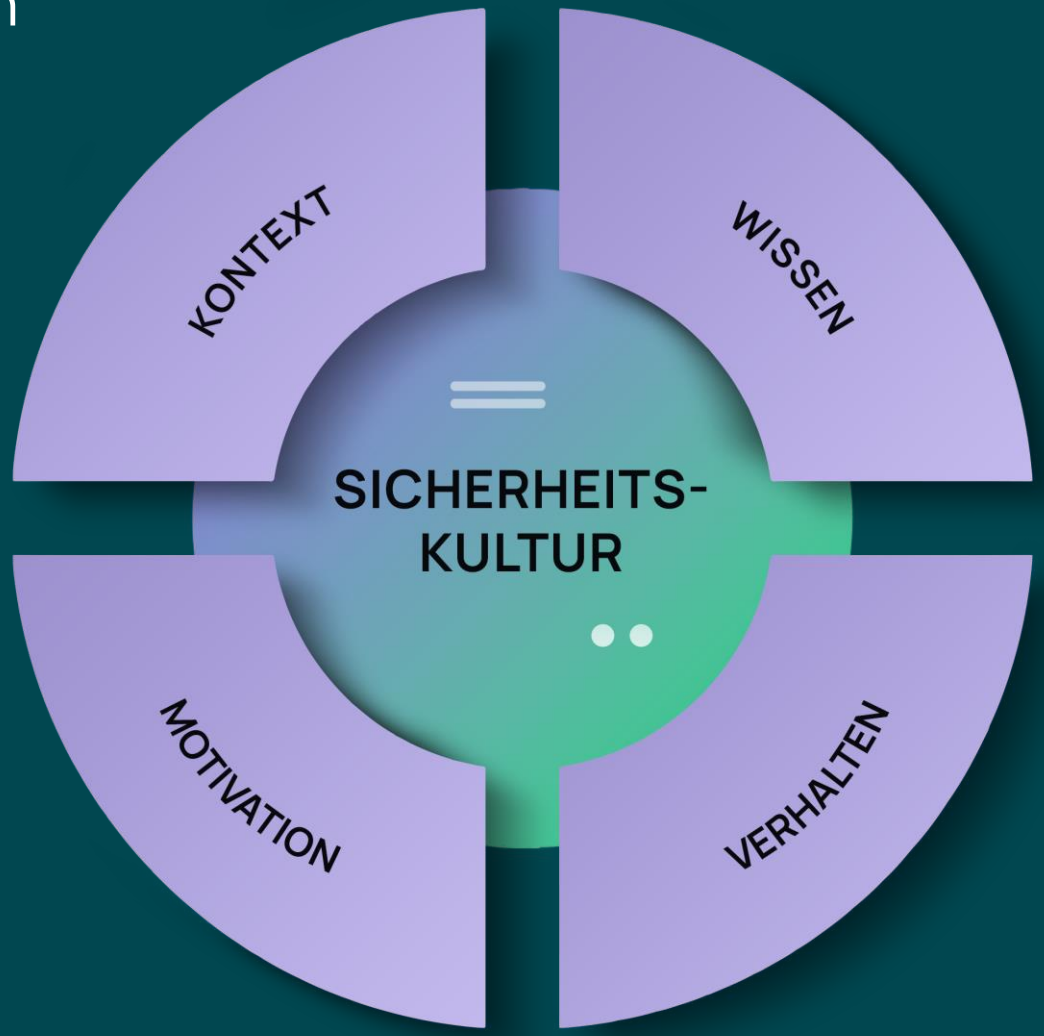
Warum Security Awareness mehr als nur ein Compliance-Thema ist

Security Awareness muss holistischer werden und nachhaltig sicheres Verhalten fördern

→ Anwendung von verhaltenswissenschaftlichen und psychologischen Grundsätzen (z. B. positive Verstärkung)

→ Von einmaligen Maßnahmen hin zur kontinuierlichen Stärkung einer Sicherheitskultur

→ Berücksichtigung weiterer Dimensionen, die sichere Gewohnheiten stärken



sosafe