Executive Summary

9 von 10 IT-Experten und IT-Sicherheitsverantwortliche sagen:

Die Cyber-Bedrohungslage hat sich verschärft. Jede dritte Organisation hat 2021 selbst einen erfolgreichen Cyberangriff erlebt.

Die erfolgreichsten Phishing-Betreffzeilen 2021...

...setzen auf die Thematisierung hybrider Arbeitsprozesse und Emotionen wie Druck und Autorität:

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

Die Top 5 Cybercrime-Trends 2022

01 3 von 4 Befragten geben an, dass sich durch hybride Arbeitsmodelle die Angriffsmöglichkeiten und Erfolgschancen von Cyberkriminellen erweitert haben. Mehr als 80 % sehen eine Kombination technischer und organisatorischer Maßnahmen als Lösung.

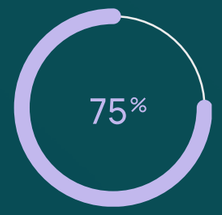
02 Die ENISA spricht von der „goldenen Ära für Ransomware“. Komplexe Angriffstaktiken wie Mehrfacherpressungen erhöhen dabei die Gefahr von Datenmissbrauch um knapp 800 %. Auch die Menge an Malware erreichte laut AV-Test 2021 einen neuen Höhepunkt – mehr als 150 Millionen Schadprogramm-Varianten wurden erkannt, davon 59 % Trojaner.

03 Groß angelegte Supply-Chain-Angriffe zielen auf schwache Glieder in Lieferketten und legen ganze Versorgungssysteme lahm.

04 Der Ausbau von KI-as-a-Service-Angeboten ermöglicht Cyberkriminellen tückische, neue Angriffstaktiken wie Deepfakes, Voice Cloning und automatisiertes und damit massentaugliches Spear Phishing.

05 Phishing und Social Engineering bleiben Dauerbrenner unter den Angriffsmethoden und werden anlassbezogen weiterentwickelt. Fast jede dritte Person klickt auf schädliche Inhalte in Phishing-Mails.

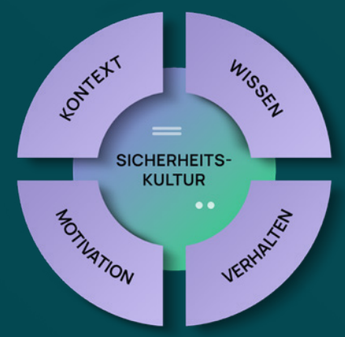
Europaweit verschärfte Cyber-Security-Regularien erhöhen die Haftungsrisiken für Führungskräfte.



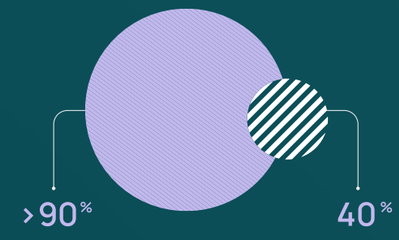
Gartner geht davon aus, dass bei cyber-physischen Vorfällen schon bis 2024 75 % der CEOs persönlich haften werden.

> “Der Mensch ist definitiv der wichtigste Faktor für die Cyberresilienz von Organisationen.”
>
> **Vivien Bilquez,** Principal Cyber Risk Engineer bei Zurich Resilience Solutions

Das Behavioral Security-Modell: Psychologisch fundierte Awareness-Maßnahmen minimieren menschliche Risiken um bis zu 90 %.



Mehr als 90 % der IT-Experten und IT-Sicherheitsverantwortlichen sagen:



Awareness sei wichtig in ihrer Organisation. Doch 40 % dieser Organisationen geben an, das Awareness-Level der Mitarbeitenden sei niedrig. Mehr als zwei Drittel der Befragten planen deshalb, ihre Awareness-Maßnahmen im kommenden Jahr auszuweiten.

Nahezu einstimmig geben 99 % der Befragten an, dass im nächsten Jahr das Stärken der organisationseigenen Sicherheitskultur wichtig sein wird.

> „Es braucht entscheidungsfreudige und leitende Hand auf Führungsebene.“
>
> **Achim Berg,** Präsident des Bitkom