
HISCOX CYBER READINESS REPORT 2022

KEY FINDINGS

16.05.2022



DIE WICHTIGSTEN ERKENNTNISSE AUS DEM CYBER READINESS REPORT IM ÜBERBLICK

Cyber-Angriffe als Risiko Nummer eins für Unternehmen

Die befragten Experten in sieben von acht Ländern (inklusive **Deutschland**) stufen Cyber-Angriffe als die größte Bedrohung für ihr Unternehmen ein – noch vor Pandemie, Wirtschaftsabschwung und Fachkräftemangel.

Cyber-Angriffe steigen international weiterhin an

Mittlerweile geben 48% aller befragten Unternehmen weltweit an, in den letzten 12 Monaten Opfer mindestens einer Cyber-Attacke geworden zu sein – im Jahr zuvor waren es noch 43%; **in DE: gleichbleibend hohes Niveau wie im Vorjahr bei 46%.**

Mittlere Cyber-Gesamtschadenskosten sind in Deutschland am höchsten

DE: Die mittleren Kosten für Cyber-Attacken liegen weiterhin hierzulande deutlich höher als im internationalen Vergleich (INT: €15.255; DE: €18.712).

Dramatischer Einbruch in der Cyber-Selbsteinschätzung der Unternehmen

International: Cyber-Experten sinken von 20% auf 5%, Hauptgrund ist die große Zahl an Kumul-Attacken wie z. B. Log4j; **in DE: Experten: stark gesunken von 21% auf 3%.**

DIE WICHTIGSTEN ERKENNTNISSE AUS DEM CYBER READINESS REPORT IM ÜBERBLICK

Investitionen in Cyber-Sicherheit seit 2019 um 250% gestiegen

Auch im Vergleich zum Vorjahr ein deutlicher Anstieg der Cyber-Security-Invests gemessen am Gesamt-IT-Budget: International: von 21% in 2021 auf 23% in 2022, **in DE von 20% auf 24% (in 2019 lag dieser in DE erst bei 11%)**.

Cyber-Versicherungen werden immer selbstverständlicher

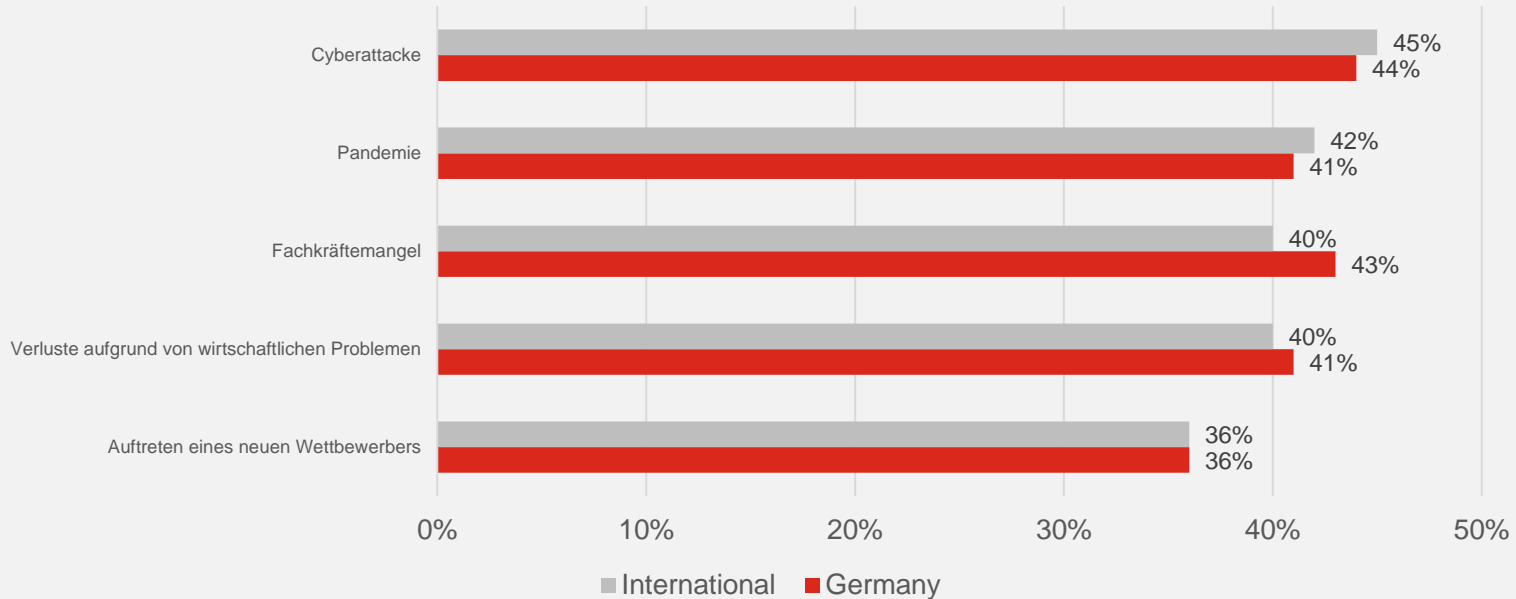
DE: In Deutschland sind 67% der befragten Unternehmen bereits abgesichert – damit liegt DE international ganz vorne; nur noch 11% der in DE Befragten geben an, weder eine Cyber-Absicherung zu haben noch planen, eine abzuschließen (2020 waren das noch 25%).

Einer der häufigsten Eintrittspunkte für Hacker ist u.a. der Corporate Cloud Server

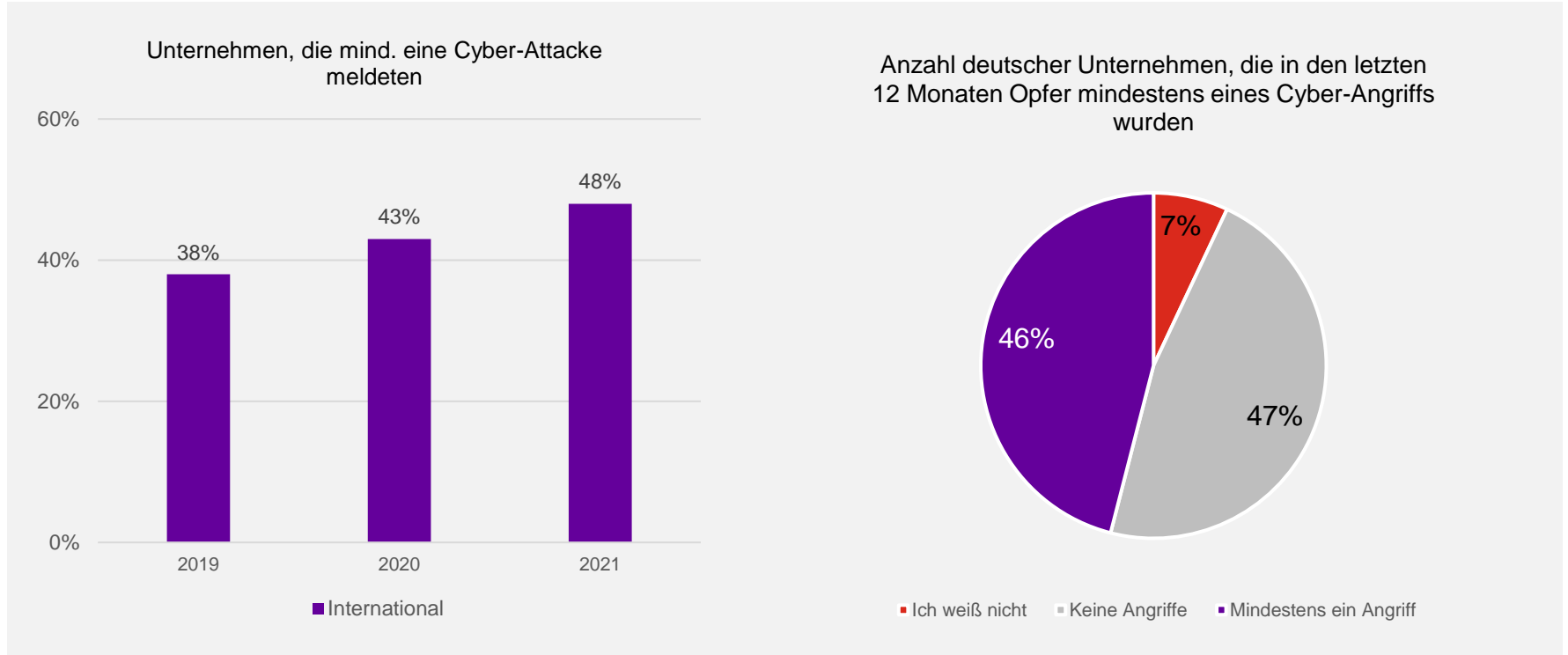
DE: Das ist bei 42% aller Cyber-Schadenfälle in DE der Fall; auf Platz 2 und 3 liegen der physisch in Unternehmen stehende Server (39%) sowie Kompromittierung von Geschäfts-E-Mails (35%).

CYBERANGRIFFE ALS RISIKO NUMMER EINS FÜR UNTERNEHMEN

Wahrnehmung von Unternehmensrisiken



CYBER-ANGRIFFE STEIGEN INTERNATIONAL AN IN DEUTSCHLAND KONSTANT HOCH WIE IM VORJAHR

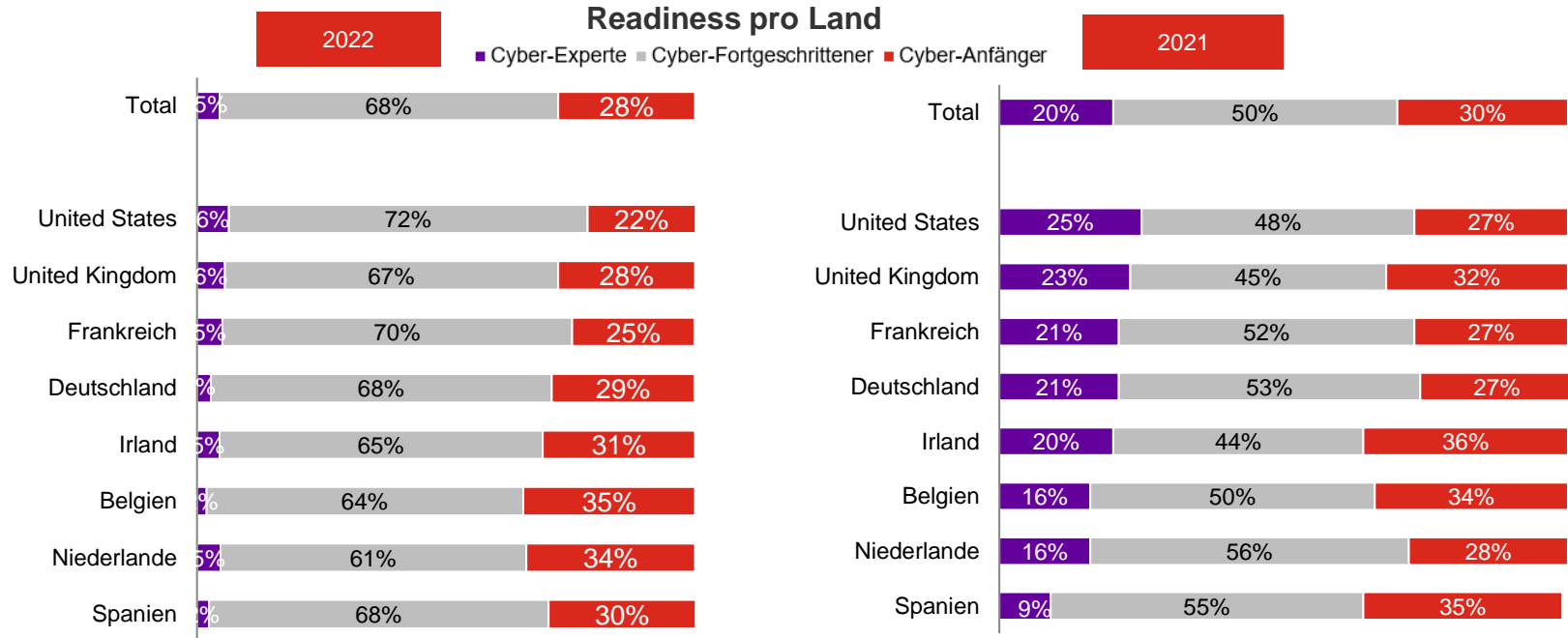


MITTLERE CYBER-GESAMTSCHADENKOSTEN SIND IN DEUTSCHLAND AM HÖCHSTEN

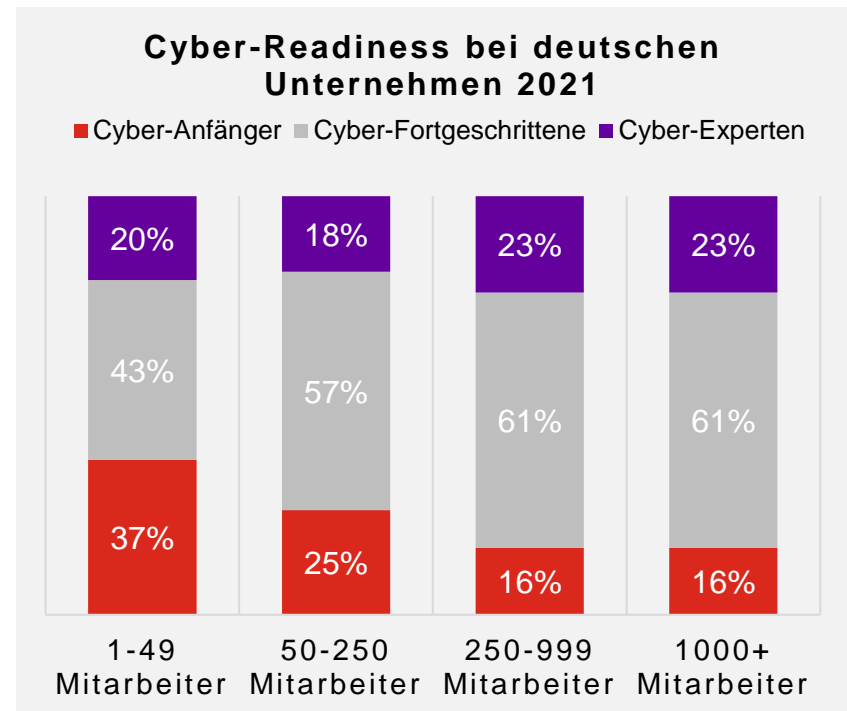
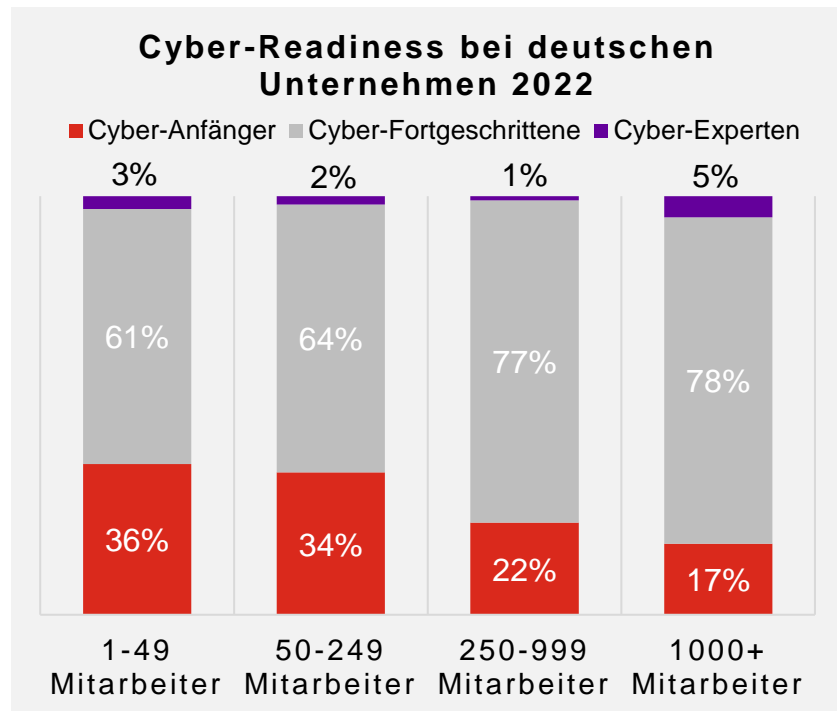
Deutsche Firmen verzeichneten 2022 die **höchsten mittleren Gesamtkosten durch Cyber-Angriffe**



CYBER READINESS MODEL IM JAHRESVERGLEICH (PRO LAND)



DRAMATISCHER EINBRUCH IN DER CYBER SELBSTEINSCHÄTZUNG DER UNTERNEHMEN IN DEUTSCHLAND



WARUM SIND DIE CYBER-EXPERTEN DIESES JAHR VERSCHWUNDEN?

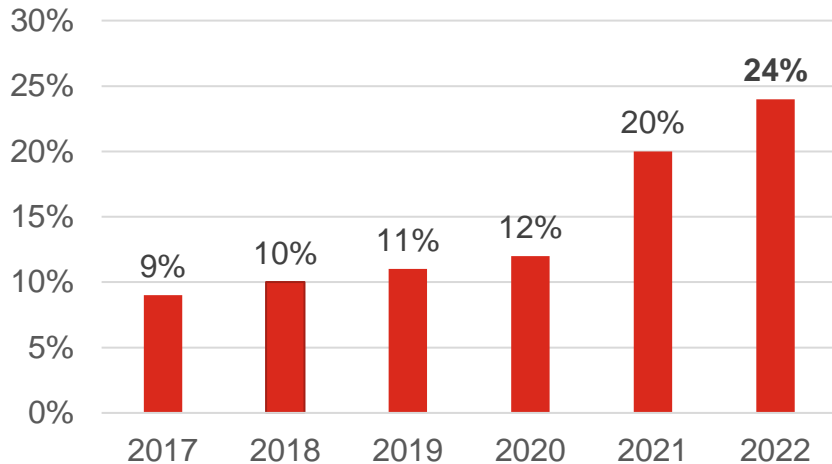
Wir haben eine Theorie...

		Wurde die Umfrage vor dem log4j-Vorfall am 9. Dezember abgeschlossen?			Total
		Vor log4j	Am Tag von log4j	Nach log4j	
Cyber Readiness Level	Cyber-Anfänger	16.6%	26.8%	28.8%	27.5%
	Cyber-Fortgeschrittene	65.3%	68.0%	68.3%	68.0%
	Cyber-Experten	18.1%	5.2%	2.9%	4.5%
Total		100.0%	100.0%	100.0%	100.0%

DEUTSCHE IT-AUSGABEN

AUSGABEN FÜR CYBERSICHERHEIT STEIGEN WEITER AN.

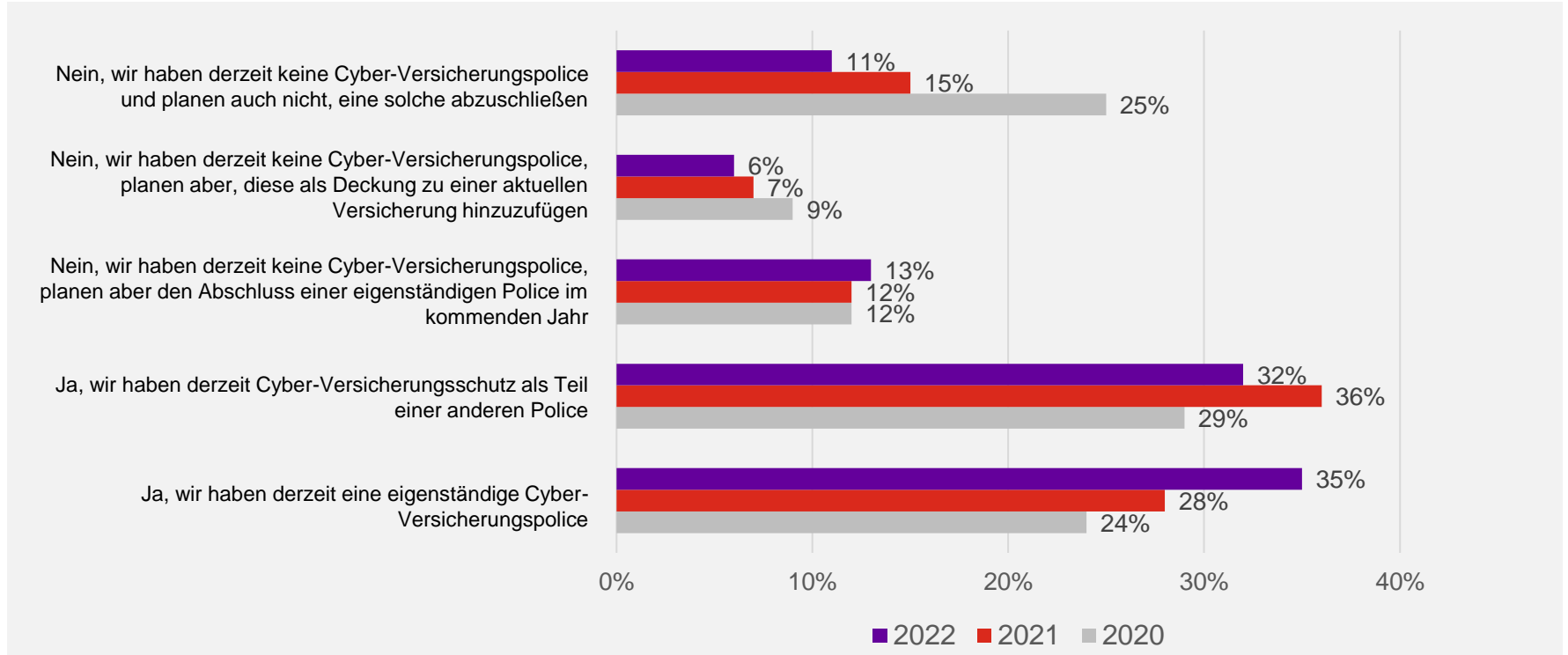
Anteil für Cyber-Sicherheit in Prozent des gesamten IT-Budgets in Deutschland:



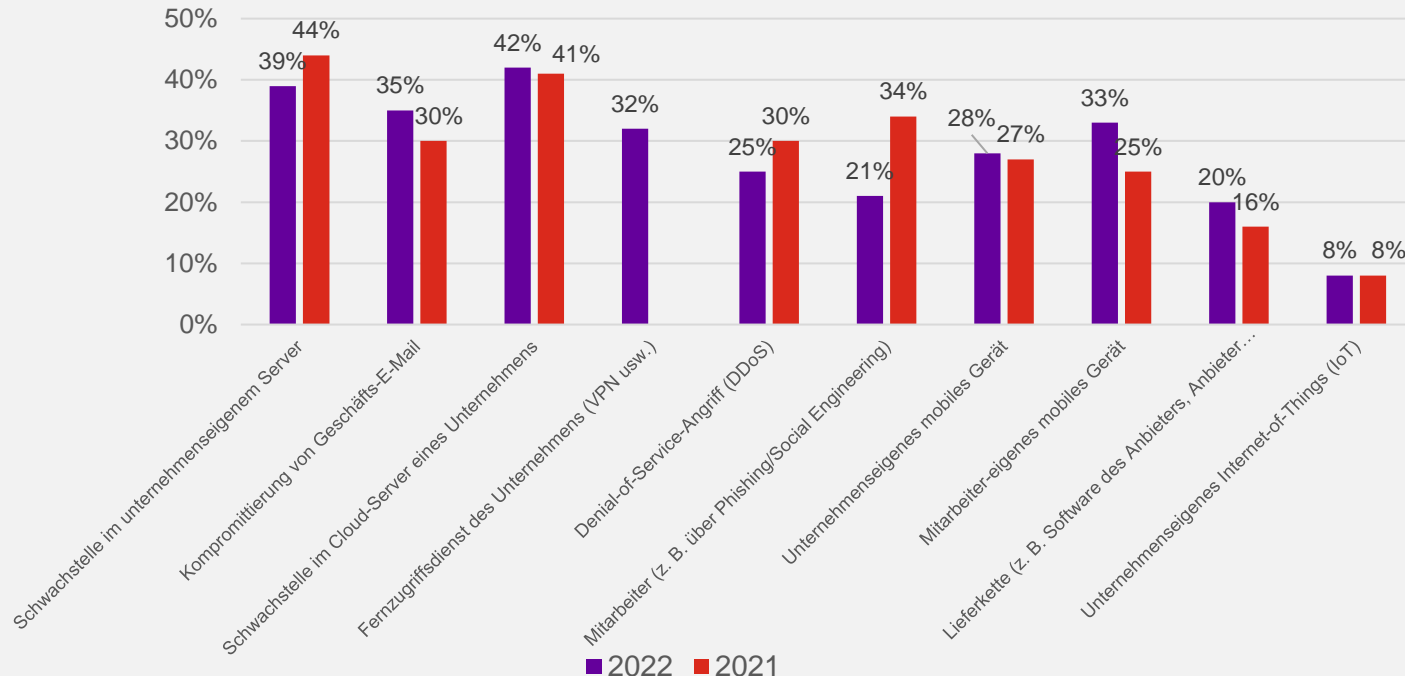
Cybersicherheit in % der IT-Ausgaben:

Jahr	Gesamtdurchschnitt	Deutschland
2022	23%	24%
2021	21%	20%
2020	13%	12%
2019	10%	11%
2018	11%	10%
2017	11%	9%

CYBER-VERSICHERUNGEN WERDEN IMMER SELBSTVERSTÄNDLICHER IN DEUTSCHLAND



HÄUFIGSTER EINTRITTSWEG FÜR HACKER IST CORPORATE CLOUD SERVER



HISCOX CYBER READINESS REPORT 2022

MASSNAHMEN FÜR HOHE CYBER-RESILIENZ



**Erstellung eines
Krisen-
Reaktionsplans für
Cyber-Zwischenfälle**



**Regelmäßige
Simulation eines
Cyberangriffs**



**Regelmäßige
Bewertungen der
Daten- und
Technologie-
infrastruktur eines
Unternehmens**



**Durchführung
wirksamer
Cybersicherheits-
schulungen für die
Mitarbeiter**



**Bessere
Umsetzung von
Cybersicherheits-
prozessen
oder -verfahren, wie
z. B. Patching oder
Pen-Tests**



**Ernennung von
Schlüsselfunktionen
im Bereich der
Cybersicherheit oder
ein verstärktes Team
von Mitarbeitern**

HISCOX CYBER READINESS REPORT 2022

WEITERE ERKENNTNISSE AUS DER PRAXIS

Die Schwachstellen des letzten Jahres zeigen, dass Unternehmen **auch bei guter Prävention Opfer** eines Angriffs zu werden drohen.

Technische Lösungen alleine bieten unzureichenden Schutz, wenn Betriebsprozesse und Organisation nicht auf Sicherheit ausgerichtet sind.

Neben der **Prävention** müssen sich Unternehmen intensiv mit der **Erkennung und Behandlung von Angriffen** auseinandersetzen.

KONTAKT

Hiscox

Leo Molatore

Arnulfstraße 31

80636 München

089/545801566

leo.molatore@hiscox.com

www.hiscox.de/crr2022

LHLK Agentur für Kommunikation

Quirin Löffelmeier

Tegernseer Platz 7

81541 München

089/720187 298

hiscox@lhlk.de

