

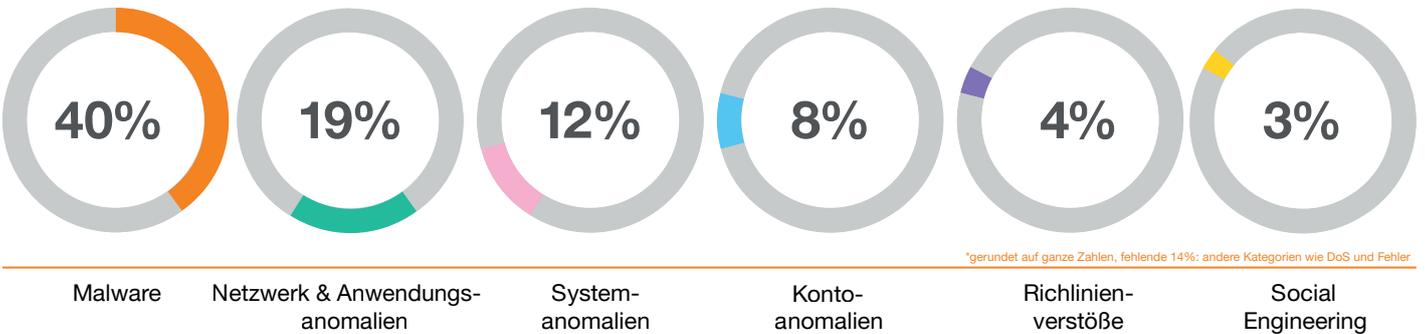
Security Navigator 2023

Research-driven insights
to build a safer digital society



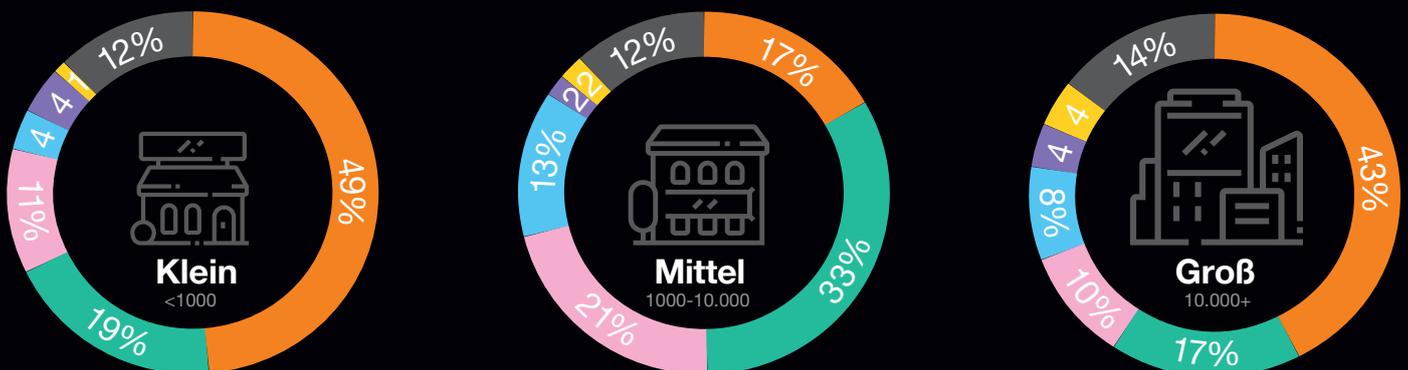
- Verschaffen Sie sich einen Gesamtbild der Cybersecurity-Welt
- 100% der Informationen aus erster Hand, bezogen aus den 17 globalen SOCs und 13 CyberSOCs von Orange Cyberdefense, dem CERT, den Epidemiology Labs, World Watch, Ethical Hacking und Vulnerability Management
- Gewinnen Sie wertvolle Einblicke in die Bedrohungslandschaft
- Expertenberichte und Technologiebewertungen zu Themen wie Ransomware/Cyber-Erpressung, Mobile Security und die Auswirkungen des Krieges in der Ukraine
- Finden Sie Angriffsmuster und Statistiken für Ihre Unternehmensgröße und -vertikalität
- Erfahren Sie, was die folgenschwersten Ereignisse im Jahr 2022 waren und wie sich diese auf die Zukunft auswirken
- Erhalten Sie den vollständigen 120-seitigen Bericht [hier!](#)

Trichter: 99.506 Vorfälle u 29.291 bestätigte Vorfälle



Eine Frage der Größe: Vorfälle nach Unternehmensgröße

■ Malware
 ■ Netzwerk & Anwendung
 ■ System
 ■ Konto
 ■ Richtlinienverstöße
 ■ Social Engineering
 ■ Andere

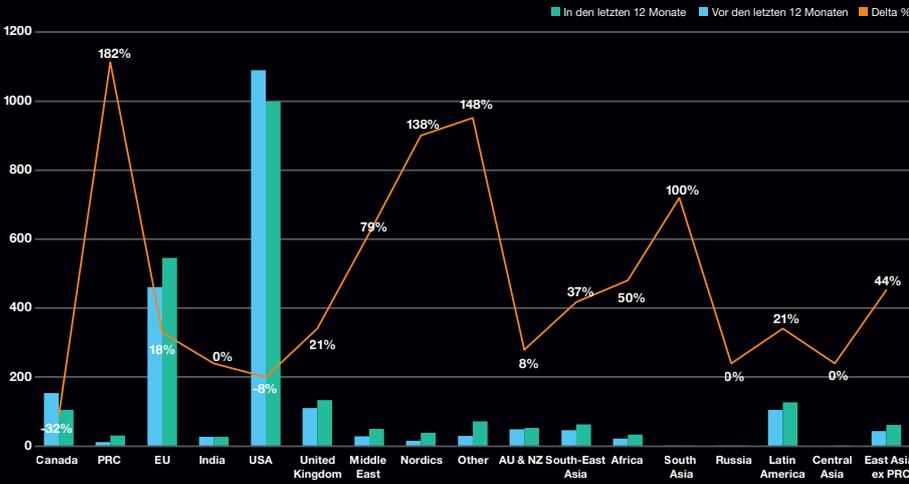


Lesen Sie den vollständigen Report!

Holen Sie sich Ihr kostenloses Exemplar des Security Navigators auf:

[orangecyberdefense.com/de/security-navigator/](https://orange.cyberdefense.com/de/security-navigator/)

Cy-X & Ransomware: Die geografische Entwicklung



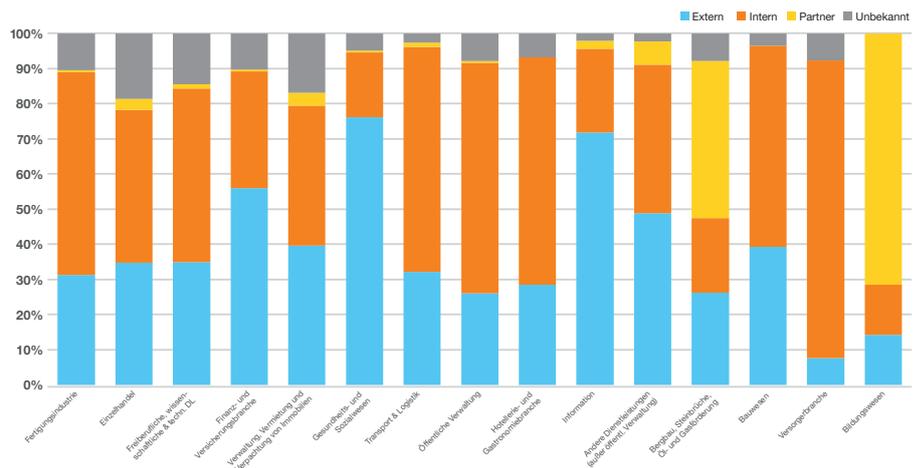
Traditionell waren große, englischsprachige Länder am stärksten von Cyber-Erpressung betroffen. Dies begann sich jedoch im Jahr 2021 zu ändern und hat sich bis 2022 fortgesetzt. Der Standort der Opfer scheint sich zu verlagern – von den USA und Kanada über das Vereinigte Königreich und Westeuropa zum Rest der Welt.

Diese Veränderung beschleunigte sich in den letzten sechs Monaten mit Rückgängen von 34 %, 33 % und 20 % im Vereinigten Königreich, in den USA und in Europa, während Ostasien und Südostasien im gleichen Zeitraum um 30 % und 33 % zulegten.

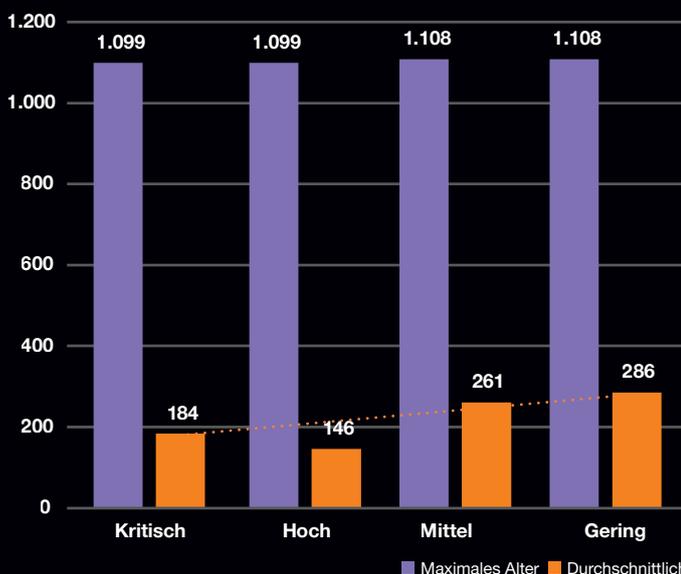
Ein erster Blick auf VERIS: Quellen der Vorfälle

Die Aufschlüsselung auf der rechten Seite zeigt einen Überblick über alle Branchen und die Bedrohungsakteure, die für ihre Vorfälle verantwortlich gemacht werden. Wir sind zwar noch dabei, VERIS zu übernehmen, aber es gibt einen gewissen Einblick in die Arten von Akteuren, mit denen die einzelnen Branchen konfrontiert sind. Natürlich können diese Ergebnisse erheblich von den Erkennungsfähigkeiten der einzelnen Kunden in der jeweiligen Branche beeinflusst werden.

Es ist bemerkenswert, dass es in vielen Branchen offenbar mehr interne als externe 'Akteure' gibt.



Vulnerabilities & Patching



Durchschnittliches/maximales Alter der Findings nach Schweregrad

Wenn wir uns die Werte für die durchschnittliche und die maximale Zeit für verschiedene Kritikalitätswerte genauer ansehen, erhalten wir das Diagramm auf der linken Seite.

Selbst bei kritischen Vulnerabilities dauert es durchschnittlich 6 Monate, bis sie behoben sind, aber das ist zumindest 36 % schneller als die Zeit für weniger schwerwiegende Probleme.

Obwohl wir feststellen, dass kritische Schwachstellen generell überdurchschnittlich schnell geschlossen werden: die Maximalzeit ist konsistent hoch, egal ob kritisch oder nicht.