
Cybercrime Time: Fiktion trifft Wirklichkeit – die Wahrheit hinter “Akte Vakzin”

Autor und Cyberspezialist
Walther Stonet liest aus seinem
2. Brühlsdorf-Krimi



Risiko Cyberraum

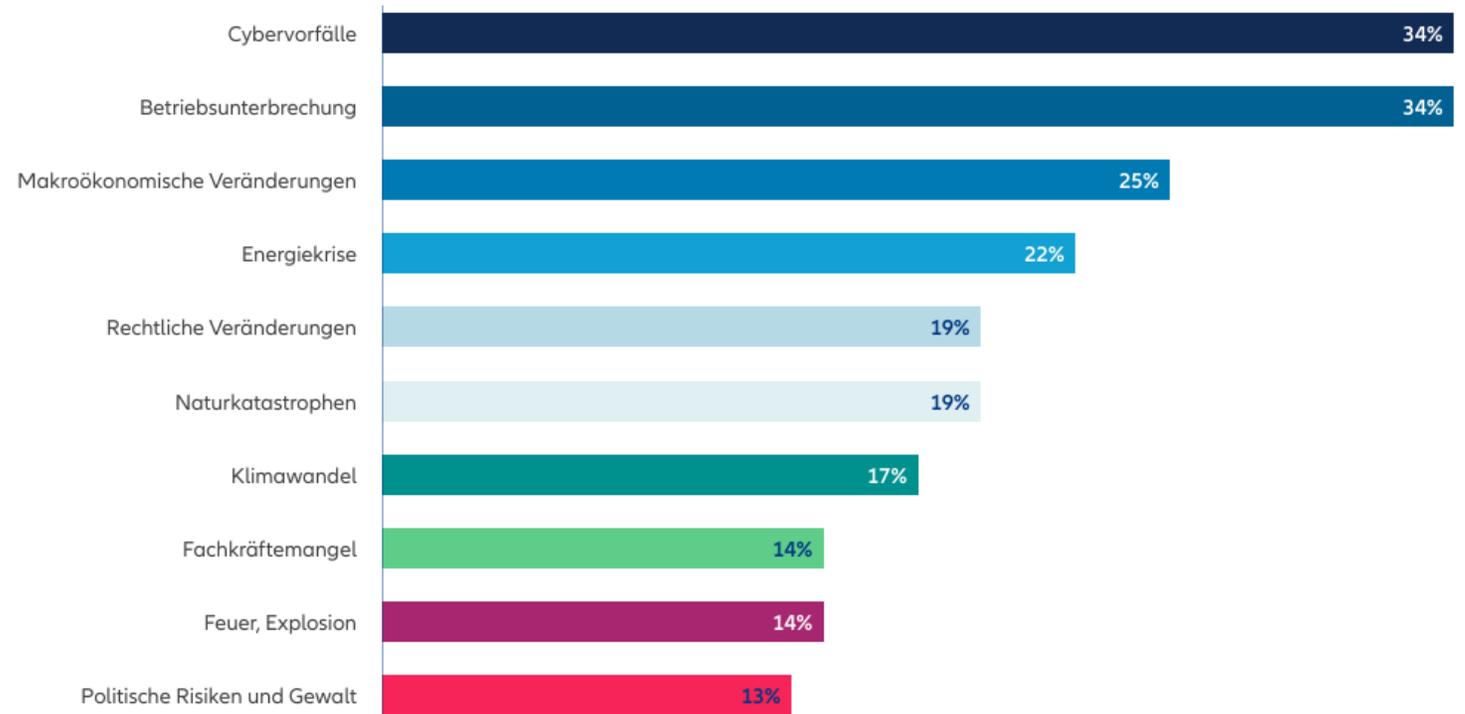
Allianz Risk Report 2023



Top 10 Geschäftsrisiken weltweit in 2023

Allianz Risk Barometer 2023

Basierend auf den Antworten von 2.712 Risikomanagement-Experten aus 94 Ländern und Gebieten (% der Antworten). Die Zahlen ergeben nicht 100%, da jeweils bis zu drei Risiken ausgewählt werden konnten.



Risiko Cyberraum



deutscher Unternehmen waren 2021 von Cyberangriffen betroffen.



war der durchschnittliche Komplettausfall nach einem Angriff

Durchschnittliche Lösegeldsumme



Schaden durch Ransomware in 2021



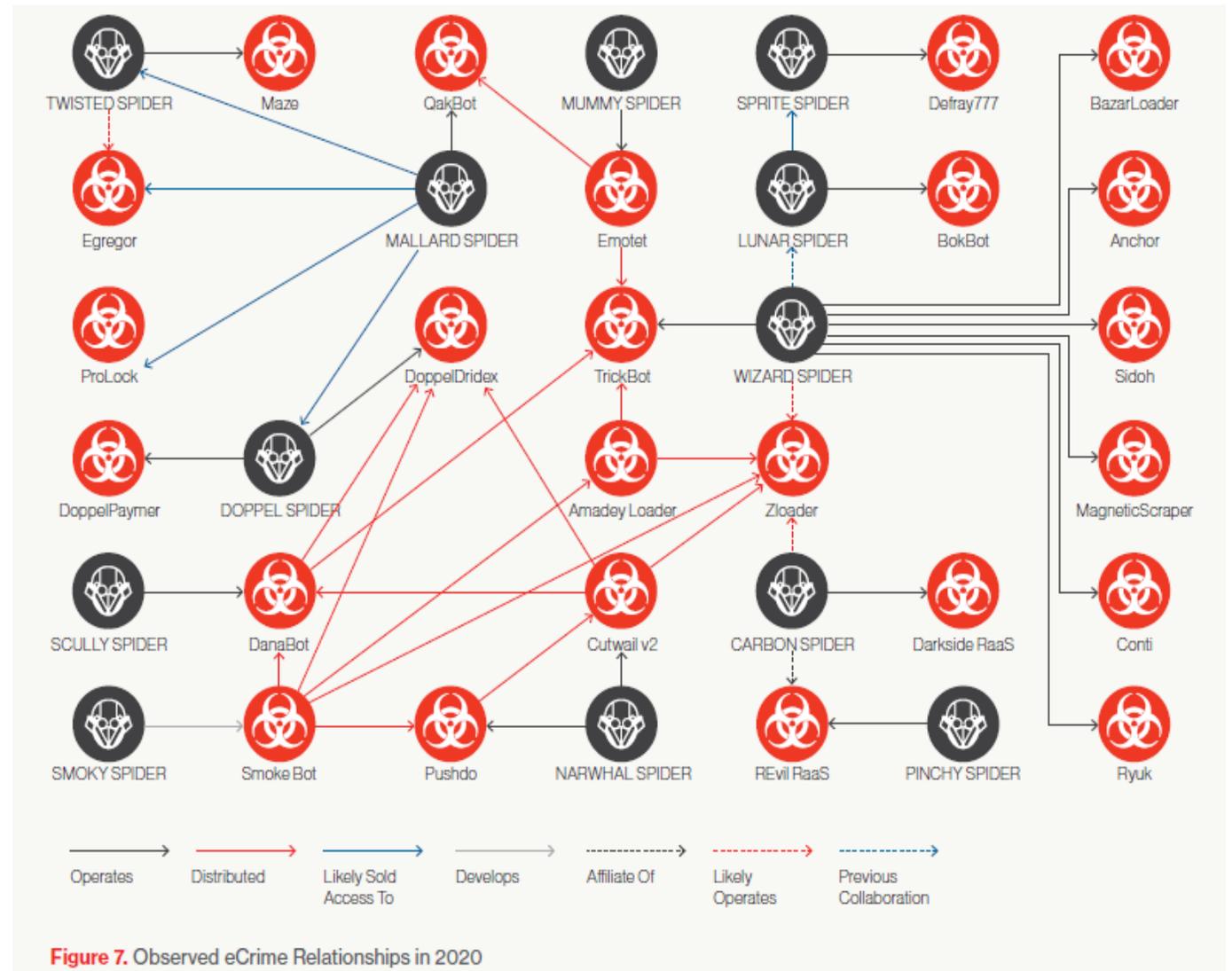
2022 waren Attacken Malware frei und bedienten sich Zugangsdaten oder neuen Schwachstellen.

Das Cybercrime-Geschäft

Alle Berichte und Statements der Spezialisten und Fachbehörden weltweit formulieren deutlich:

„Cyber- oder e-Crime ist ein professionelles Geschäft geworden mit Arbeitsteilung, Preislisten, Marktplätzen und Foren im Darknet.“

„Staaten wie Russland schützen dieses Geschäft vor dem Zugriff durch den Rechtsstaat. Das Risiko ist sehr gering, zur Rechenschaft gezogen zu werden.“





EMA meldet Hackerangriff auf Impfstoffdokumente

„Die Europäische Arzneimittelagentur EMA ist Opfer eines Cyberangriffs geworden. Die Hacker hatten offenbar Zugriff auf Dokumente zu einem Corona-Impfstoff von BioNTech und Pfizer.“

Quelle: DW vom 09.12.2020

<https://www.dw.com/de/europ%C3%A4ische-arzneimittelagentur-meldet-hackerangriff-auf-impfstoffdokumente/a-55889206>

Quelle Foto:

https://de.wikipedia.org/wiki/Europ%C3%A4ische_Arzneimittel-Agentur



Cyberattack Heatmaps

<https://threatmap.checkpoint.com/>

<https://livethreatmap.radware.com/>

<https://www.sicherheitstacho.eu/#/en/tacho>

<https://threatmap.bitdefender.com/>

<https://cyberthreat.thalesgroup.com/>



Was Sie nicht tun sollten...



- Ihr Smartphone aus der Hand geben, damit jemand anderes etwas drauflädt
 - WhatsApp geschäftlich nutzen
 - einfache Passwörter wie 12345, Vornamen oder Orte benutzen
 - seit Jahren das gleiche Passwort benutzen
 - Mitarbeitern Admin-Rechte geben
 - Auf Links in Emails klicken, ohne vorher nachzudenken
-

Passwortsicherheit

- *Länge von Passwörtern entscheidender als Komplexität*
- *Verhindern von Brute-Force Attacken durch Begrenzung von Anmeldungen*
- *Passwörter nur einmal nutzen*
- *Nutzung von Passwortmanagern*

TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD IN 2023

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	1 sec	2 secs	4 secs
8	Instantly	Instantly	28 secs	2 mins	5 mins
9	Instantly	3 secs	24 mins	2 hours	6 hours
10	Instantly	1 min	21 hours	5 days	2 weeks
11	Instantly	32 mins	1 month	10 months	3 years
12	1 sec	14 hours	6 years	53 years	226 years
13	5 secs	2 weeks	332 years	3k years	15k years
14	52 secs	1 year	17k years	202k years	1m years
15	9 mins	27 years	898k years	12m years	77m years
16	1 hour	713 years	46m years	779m years	5bn years
17	14 hours	18k years	2bn years	48bn years	380bn years
18	6 days	481k years	126bn years	2tn years	26tn years

 [Learn how we made this table at hivesystems.io/password](https://hivesystems.io/password)

Damit Sie etwas cybersicherer arbeiten



1. **Passwortspeicher**

<https://bitwarden.com/de-DE/>

Bitwarden – kostenloser Passwortmanager für alle Browser und Smartphones
Kostenlos

2. **Einsatzgebiet**

Generiert und prüft komplexe Passwörter und Phrasen

Managet alle Logins und Zugriffe
plattformübergreifend

Passwörter können schnell geändert und sicher geändert werden

Damit Sie etwas cybersicherer arbeiten

1. Zwei-Faktor-Zugriff
 - Das Smartphone wird zum zweiten Faktor
 - Apps: Google oder Microsoft Authenticator (kostenlos)
2. Aktivieren bei
 - Ihrer Geschäfts-E-Mail
 - Bankkonto im Browser
 - Internet-Shops
 - Arbeiten mit Smartphone oder Tablet



Was Sie mindestens haben sollten...

- Eine professionelle Datensicherung mit Überschreibungsschutz – z.B. in der Cloud
- Eine gemanagete Firewall
- Eine geschützte Webseite, die professionell gehostet ist
- Ein Postfach mit professionellem Schutz vor Spam und Phishing
- Ein Antivirus-Programm auf Ihrem/n Rechner/n



Webseite und Bestellung

Webseite:

<https://bruehlsdorf.com/>

Bestellung im Buchhandel:

[https://www.osiander.de/shop/home/suggestartikel/A1068806239?sq=Akte%20Vakzin&stype=product
Name](https://www.osiander.de/shop/home/suggestartikel/A1068806239?sq=Akte%20Vakzin&stype=productName)

[https://finkeria.shop/shop/item/9783965551534/akt
e-vakzin-von-walter-stonet-kartoniertes-buch](https://finkeria.shop/shop/item/9783965551534/akte-vakzin-von-walter-stonet-kartoniertes-buch)

<https://amzn.eu/d/cBDVOKa>

... und bei mir, dem Autor

