nevis®
Making security an experience.

Sicherheits-barometer #2

Wie unterschiedlich Konsumenten und IT-Entscheider zur IT-Sicherheit stehen

Stephan Schweizer, CEO Nevis Security

Anerkannte Qualität: **Unsere Kunden**

BRACK.CH

die Mobiliar

EQUATEX

PostFinance

GENERALI

QUILVEST

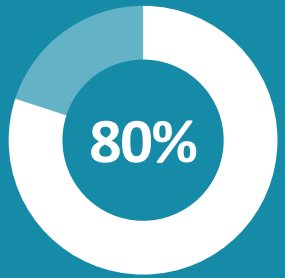
helvetia

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Kanton Zug

HIN

Nevis protects



of all Swiss e-banking transactions

SFS

ETAT DE FRIBOURG
STAAT FREIBURG

SIX

Helsana

swisscom

ne.ch
RÉPUBLIQUE ET CANTON DE NEUCHÂTEL

UBS

ZURICH

VIESMANN

MediData

Gartner: CX Wins!

“Jeder 5. Kunde wechselt nach einem einzigen schlechten Erlebnis **sofort den Anbieter.”**

Quelle: Gartner CX Summit London

19%

Wie die Resultate erhoben wurden

Systematik und Methoden der Studie

Für den Sicherheitsbarometer wurden zwei spezifische Studien durchgeführt, um die Sicht von IT-Entscheidern und Privatpersonen analysieren und vergleichen zu können.

Befragung von IT-Entscheidern
Das Meinungsforschungsunternehmen Civey hat im Auftrag der Nevis Security AG 500 IT-Entscheider zwischen dem 19. Juli bis 12. August 2022 befragt. Die Ergebnisse sind repräsentativ für diese Gruppe. Der statistische Fehler der Gesamtergebnisse liegt bei circa 7,3 Prozent.

Befragung von Privatpersonen
Das Onlinemarktforschungs-Institut mo'web research hat für die Nevis Security AG Ende Juli eine Online-Marktforschungsstudie zum Thema «Das Sicherheitsbarometer 2022» mit der Befragung von 1000 Konsumenten in Deutschland durchgeführt.

Wie häufig sind Cyberangriffe?

IT-Entscheider: Anstieg spürbar

Nicht nur in den Medien, sondern auch in der Wahrnehmung vieler IT-Entscheider gewinnt die Cyberkriminalität an Bedeutung. Mehr als die Hälfte der befragten IT-Entscheider wurde auch tatsächlich schon einmal angegriffen.

Wie entwickelt sich die Cyberkriminalität?

Über

57%

der befragen IT-Entscheider in der Privatwirtschaft haben im letzten Jahr in ihrem beruflichen Umfeld einen Anstieg der Cyberkriminalität wahrgenommen. Rund 39 Prozent geben an, keinen Anstieg gespürt zu haben.

Wie häufig sind Cyberangriffe?

Ungewissheit bei Privatpersonen

Von den befragten Privatpersonen sind lediglich 17 Prozent sicher, dass sie nicht Opfer einer Cyber-Attacke geworden sind. 18 Prozent sind sicher, dass sie nicht verschont geblieben sind. Beim großen Rest überwiegt hingegen die Ungewissheit.

Waren Sie schon einmal Opfer eines Cyberangriffes?

Von den befragten IT-Entscheidern berichten rund 54% von Cyberangriffen auf ihr Unternehmen.

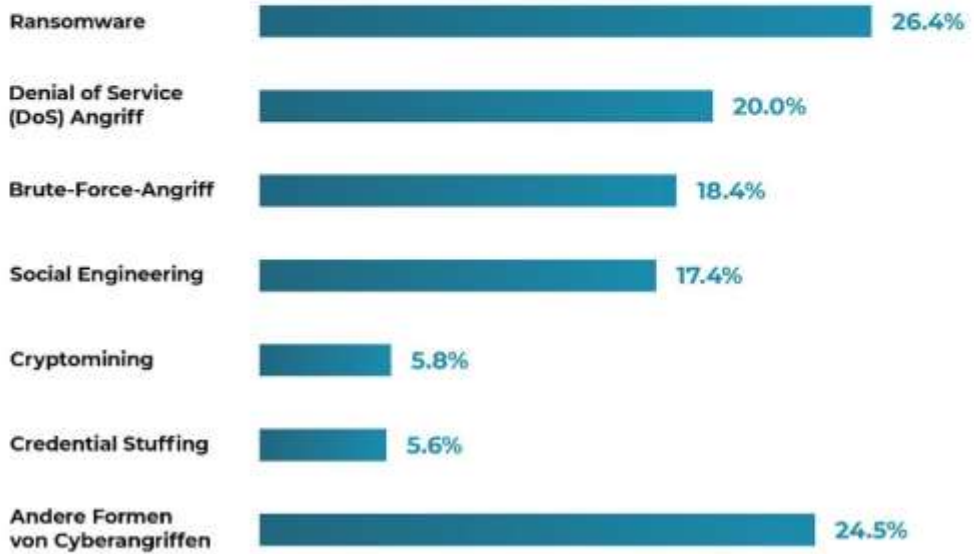
Im Bewusstsein der Privatperson sieht die Situation mit 18% deutlich anders aus.

Wie häufig sind Cyberangriffe?

Bei rund einem Viertel der Angriffe handelte es sich um Ransomware.

Credential Stuffing wird häufig nicht erkannt, da ja mit den «korrekten Daten» eingeloggt wird.

Häufige Angriffsvektoren (Mehrfachnennungen möglich)

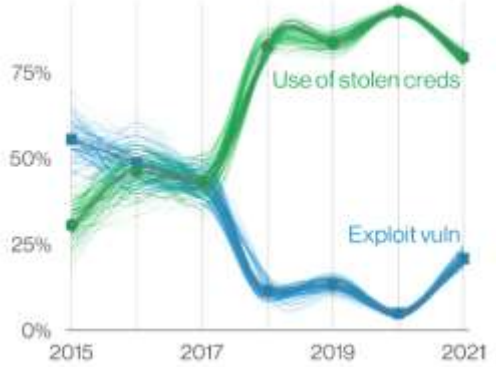


Erfolgsquote: Credential Stuffing ist Nr 1 (!)

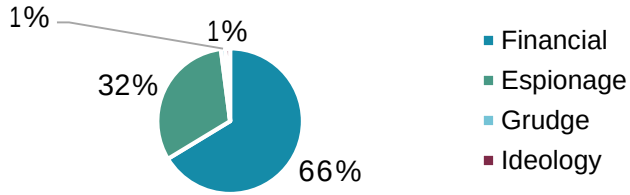
Angriffsziele

Angriffsmetoden

History und Trend



Motivation der Angreifer



Quelle: Verizon Data Breach Investigation Report, 2022

Wie gehen Private mit Passwörtern um?

Mehr als die Hälfte der Befragten benutzt zum Teil identische Passwörter.

Nutzen Sie ein und dasselbe Passwort für verschiedene Online-Konten?

Ja

Nein

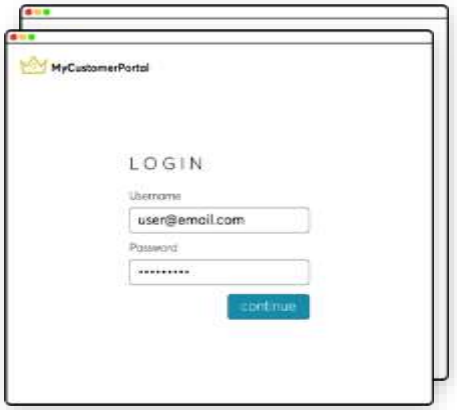
Credential Stuffing in der Praxis

1 Mio Accounts

Combolist

Erfolgsrate 0.5 – 3%

Kompromitierte Accounts: 5'000 – 30'000



Gestohlene Passwörter
- Pishing- oder Malware
- Data leaks (e.g Marriot, Equifax, etc.)
- Can be baught in the darknet
- Often used passwords

Optimierte Tools für spezifische Ziele
- Bank Accounts
- Cloud Storage
- Gaming, Betting and Gambling
- Airlines and Hotels
- Dating Portale
- E-Commerce Accounts

Attackierte Websites
- Bank Accounts
- Cloud Storage
- Gaming, Betting and Gambling
- Airlines and Hotels
- Dating Portals
- etc...

03

Wie informiert sind IT-Entscheider?

Erschreckende Defizite

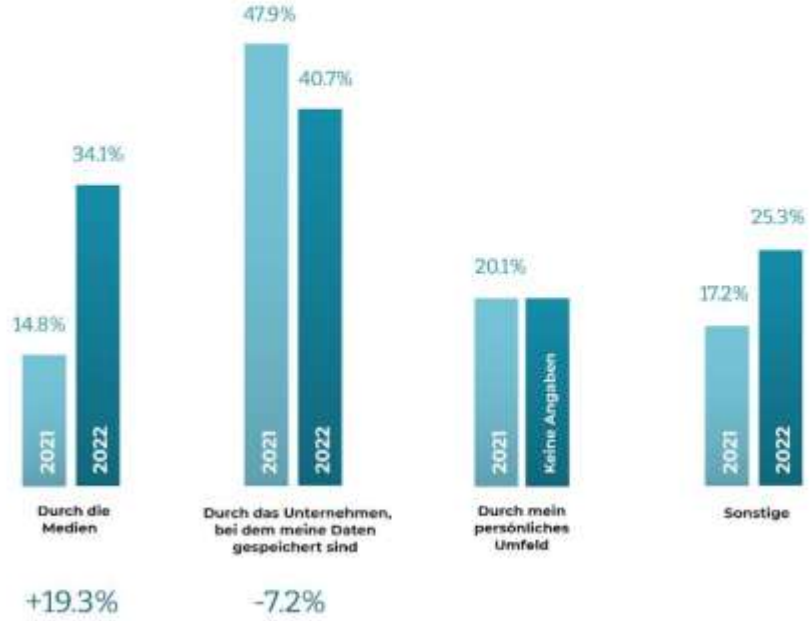
Wie gut wissen IT-Experten, wie man den Gefahren der Cyberkriminalität begegnen kann? Die Wissenslücken sind leider nach wie vor groß.

Wie reagiert man auf Cyberangriffe?

Eigentlich wären die Unternehmen bei Cyberangriffen in der Pflicht, umgehend zu informieren.
Die Realität sieht erschreckend anders aus. Die Informationsbereitschaft der Unternehmen hat im Vergleich zur letzten Befragung sogar um 7,2 % abgenommen.

Mehr als die Hälfte der Unternehmen verschweigt, dass ein Cyberangriff stattgefunden hat.

Wie haben Sie vom Cyberangriff erfahren?



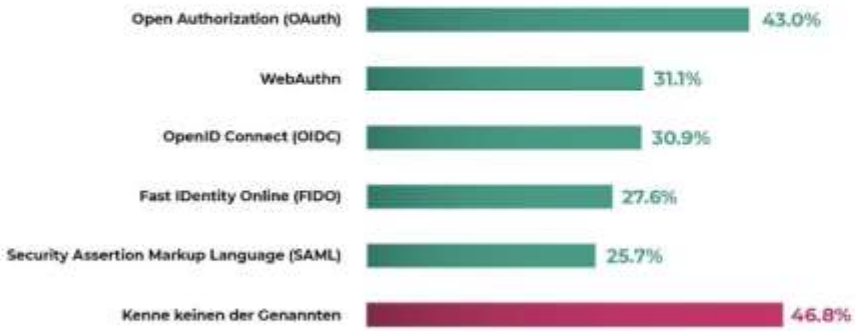
Wie gut sind IT-Entscheider informiert?

Erschreckend große Wissenslücken

Cybersecurity-Standards wie FIDO, Oauth oder WebAuthn sorgen für verlässliche Leitplanken in Bezug auf den Datenschutz. Doch sehr viele Entscheider in den Unternehmen wissen gar nicht, dass es sie gibt.

Fast die Hälfte der befragten Cybersecurity-Entscheider kennt keinen der gebräuchlichen Cybersecurity-Standards.

Welche Cybersecurity-Standards kennen Sie?



Denken Kunden und IT-Entscheider ähnlich?

Beträchtliche Unterschiede

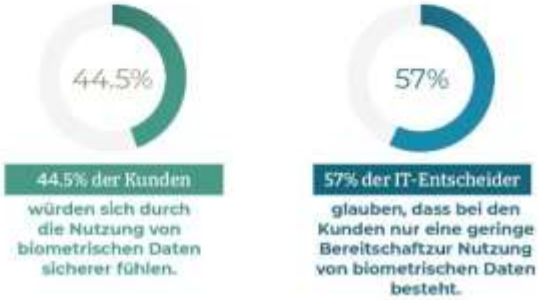
Dass Unternehmen und ihre Kunden nicht immer gleich denken, ist keine Überraschung. Beim Einsatz von Methoden für mehr Datensicherheit ist das Gefälle jedoch eklatant.

Nutzung von Zwei-Faktor-Authentifizierung

Noch weiter klafft die Lücke bei der Zwei-Faktor-Authentifizierung auseinander. Nur 4% der IT-Entscheider sehen darin ein Kundenbedürfnis. Doch satte 64% der Kunden wünschen sich den Einsatz der Zwei-Faktor-Authentifizierung.

Nutzung von biometrischen Daten

Bei der Nutzung von biometrischen Daten scheinen die Unternehmen ihre Kunden nicht allzu gut zu kennen. Sie attestieren ihnen nämlich nur eine sehr geringe Bereitschaft, ihre biometrischen Daten zur Verfügung zu stellen. Fast die Hälfte der Kunden würde sich dadurch aber sicherer fühlen, ein Viertel weiß es nicht genau.



Aktiv für mehr Datensicherheit

Tipps für optimierte IT-Security

IT-Sicherheit ist kein Buch mit sieben Siegeln. Eigentlich ist sie sogar ziemlich einfach.

01

Nutzen Sie CIAM

Das Customer Identity und Access Management sorgt für maximale Sicherheit

02

Werden Sie passwortfrei

Multi-Faktor-Authentisierung mit biometrischen Verfahren machen Logins einfach und sicher

03

Optimieren Sie den Datenschutz

Ein CIAM-System bietet einen datenschutzkonformen digitalen Zugang mit hoher Sicherheit und Kundenorientierung.

Agenda Nevis Kongress

Mittwoch, 26. Oktober
14:30 bis 17:30 Uhr im NCC Ost, Raum Oslo

Registrieren Sie sich gleich hier:

itsa EXPO CONGRESS

14:30 - 15:15

Der neue Nevis Sicherheitsbarometer: Informationsdefizite bei IT-Entscheidern?

Stephan Schweizer, CEO, Nevis Security

Gehen wir in puncto Sicherheit unnötige Risiken ein? Wir präsentieren die Ergebnisse der Studie unter 500 IT-Entscheidern und 1.000 Konsumenten.

15:25 - 15:55

Die Wahrheit über die (Un)Sicherheit von Autoident-Verfahren.

Elmar Reif, Head of Product, PXL Vision

Wie sicher sind nicht-physische Identitätsprüfungen und können sie als zuverlässiges Instrument für digitales Onboarding genutzt werden?

16:00 - 16:25

Digitale Identitäten: Smart, benutzerfreundlich und trotzdem sicher?

Holger Hinzmann, Head of Channel Sales Europe, Nevis Security

Wie mithilfe einer sicheren, biometrischen Authentifizierung die Souveränität und die Kontrolle über die eigenen Daten zurück in die Hände der Anwender gegeben werden kann.

16:35 - 17.25

Account Takeovers – und wie viel Geld verlieren Sie?

Stephan Schweizer, CEO, Nevis Security

Auswirkungen von Credential Stuffing und Kontoübernahmen für den B2C Sektor. Wir zeigen Ihnen, dass die Folgen erfolgreicher Kontoübernahmen mittlerweile über bloße „Geschäftskosten" hinaus gehen und zu einem wesentlichen finanziellen Geschäftsrisiko werden.

DANKE.

Bitte am Ausgang mitnehmen – mit Download-Link zur Studie

+41 43 508 05 92

Birmensdorferstrasse 94
8003 Zürich

info@nevis.net

www.nevis.net