nevis®

Sicherheitsbarometer 2021: **Informationsdefizite bei IT-Entscheidern**

In einer repräsentativen Studie* hat Nevis ermittelt, was IT-Entscheider hierzulande für die Sicherheit der eigenen oder der ihnen anvertrauten Daten tun.

Top 4 Hacker-Attacken auf Unternehmen

1. **Brute force** **27%**
2. **Ransomware** **24%**
3. **Social Engineering** **23%**
4. **Credential Stuffing** **12%**

Nur 24 Prozent der Befragten haben bisher noch keinen Angriff erlebt. Problematisch: 27 Prozent wissen nicht, welche Angriffe stattfanden oder haben keine Möglichkeit, dies zu prüfen!

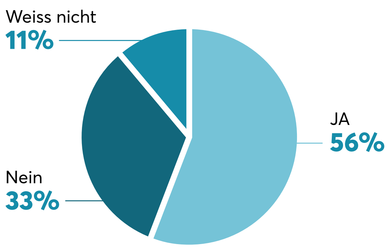
Top Drei Massnahmen für erhöhte IT-Sicherheit

62% Mindestlängen für Passwörter

52% Regelmässige Passwortänderungen

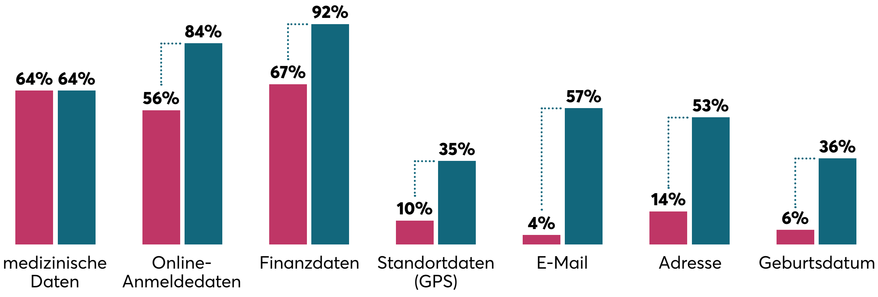
49% Zwei-Faktor-Authentifizierung

Nutzung der Zwei-Faktor-Authentifizierung



Security-Gap: Welche Daten sind besonders schützenswert?

Die Meinungen von IT-Entscheidern* und Benutzern liegen weit auseinander.**



IT-Entscheidungsträger **Benutzer, die Daten als sehr sensibel einstufen**

nevis®

Den detaillierten Überblick zur Studie und Handlungsempfehlungen für mehr Datensicherheit finden Sie im Whitepaper auf: **nevis.net**

* Das Meinungsforschungsunternehmen Civey hat im Auftrag der Nevis Security AG 500 IT-Entscheider zwischen dem 7. April und dem 22. April 2021 befragt. Die Ergebnisse sind repräsentativ für diese Gruppe. Der statistische Fehler der Gesamtergebnisse liegt bei circa 7,3 Prozent.

** mo'web research, das Full-Service-Institut für Onlinemarktforschung in Düsseldorf, hat für das Unternehmen Nevis Security AG im April 2021 eine Online-Marktforschungsstudie zum Thema „Das Sicherheitsbarometer 2021" mit der Befragung von 1.000 Konsumenten in Deutschland durchgeführt. Es ging in dieser Studie hauptsächlich um die „Wertschätzung von persönlichen Daten im Internet".