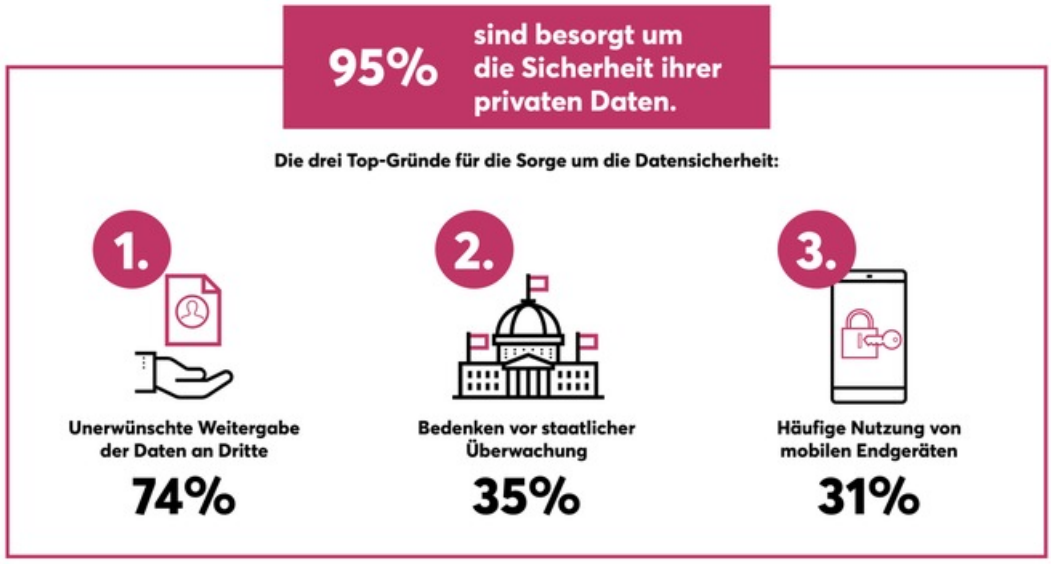
Nevis Security AG

17.08.2021 – 08:00 Uhr

Internet-Nutzer sorgen sich um ihre Daten / Das neue Nevis Sicherheitsbarometer zeigt, wie Konsumenten die Sicherheit ihrer Daten verbessern können und warum Passwörter beim Login ein Risikofaktor sind



28% wurden schon selbst Opfer einer Cyberattacke oder kennen Betroffene aus ihrem unmittelbaren Umfeld.

So reagieren User nach einem Cyber-Angriff:

Verwendung komplexerer Passwörter

66%

Regelmässige Passwortänderung

56%

Nutzung einer Zwei-Faktor-Authentifizierung

41%

Keine Massnahmen

14%

84 Prozent ist eine einfache Bedienung beim Login wichtig oder sehr wichtig

Passwortnutzung für Online-Konten:

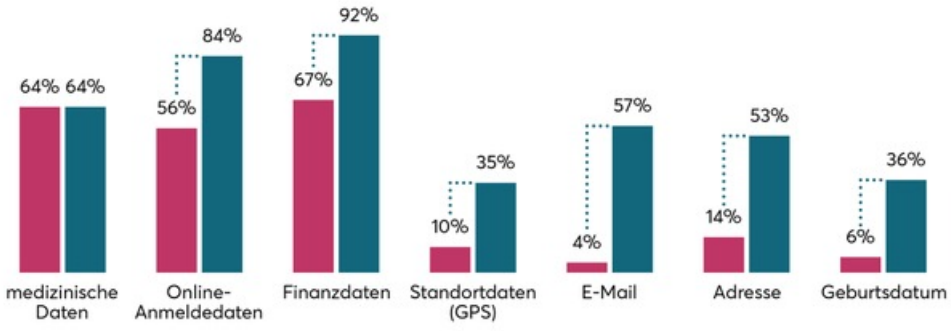
7%
nutzen ausschliesslich ein Passwort für alle Konten

44%
nutzen ein und dasselbe Passwort für mehrere Konten

49%
nutzen nie dasselbe Passwort für mehrere Konten

Security-Gap: Welche Daten sind besonders schützenswert?

Unternehmen unterschätzen das Sicherheitsbedürfnis Ihrer Kunden dramatisch.



nevis®

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

* 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".
** 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.

Zürich (ots) -

Furcht und Leichtsinn liegen bei deutschen Internet-Usern dicht beieinander. Dies geht aus dem Sicherheitsbarometer 2021 von Nevis hervor. Darin deckt der Schweizer Entwickler von Sicherheitslösungen nicht nur auf, dass 95 Prozent der deutschen Verbraucher besorgt um die Sicherheit ihrer privaten Daten sind, sondern auch sehr leichtsinnig im Umgang mit Passwörtern. Zudem zeigt Nevis, wie moderne Technologien den Login-Prozess sicher und höchst komfortabel machen können - nämlich ganz ohne Passwörter.

Für das Sicherheitsbarometer hat Nevis in Zusammenarbeit mit den Meinungsforschungsunternehmen Civey und mo'web research im April 2021 500 deutsche IT-Entscheider und 1.000 deutsche Konsumenten ab 14 Jahren zu Themen wie Passwortsicherheit und Loginverhalten online befragt.

Konsumenten nutzen heute zahlreiche Online-Anwendungen - vom Online-Shopping und -Banking über soziales Networking bis hin zum digitalen Impfausweis - und haben daher zahlreiche Online-Konten. Dabei sind sie sich der Tatsache bewusst, dass ihre sensiblen Daten einem Bedrohungsrisiko unterliegen. Wie die Ergebnisse des Nevis-Sicherheitsbarometers offenbaren, ist zum einen die Sorge um private Informationen groß und zum anderen die Angst vor Hacker-Angriffen. So fürchten rund 93 Prozent der Studienteilnehmer, die bisher noch nicht von einer Attacke betroffen waren, in Zukunft Opfer von Cyber-Kriminellen zu werden.

Risikofaktor Passwort

Im Widerspruch zu dieser Sorge stehen allerdings die Antworten der Befragten beim Thema Login- und Passwortsicherheit. Besonders erschreckend: 14 Prozent der User, die von einem Cyber-Angriff betroffen waren, haben danach nicht die Art und Weise geändert, wie sie ihre Passwörter verwalten und Konten schützen. Werden Maßnahmen ergriffen, liegen Änderungen bei den Passwörtern vor der Nutzung der Zwei-Faktor-Authentifizierung, obwohl dieses Verfahren mehr Sicherheit bietet als der alleinige Einsatz eines Passworts.

Das ist umso bedenklicher, da bei vielen Befragten in Sachen Passwort die Bequemlichkeit über den Sicherheitsaspekt siegt. Mehr als ein Fünftel hat ein Passwort schon einmal mit anderen geteilt. Und die gängige Expertenempfehlung, nie ein und dasselbe Passwort für mehrere Accounts zu verwenden, wird von 44 Prozent der Studienteilnehmer manchmal missachtet. Fällt ein solches Passwort in die falschen Hände, haben Online-Kriminelle es leicht, großen, oft auch finanziellen Schaden anzurichten, indem sie etwa Waren unter falschem Namen bestellen oder die betroffenen Nutzer mit der angedrohten Veröffentlichung sensibler Daten erpressen.

Komfort geht passwortlos

Warum handeln Verbraucher so riskant? Die Erklärung liegt im hohen Stellenwert eines komfortablen Logins: Insgesamt geben 51 Prozent der Studienteilnehmer einer einfachen Bedienung beim Login die Höchstwerte auf einer Zehner-Skala.

Wer allerdings bereits unter Folgen der zunehmenden Cyber-Kriminalität gelitten hat, ist aufgeschlossener gegenüber neuen Technologien. Insgesamt äußern zwar zwei Drittel der Studienteilnehmer Vorbehalte gegenüber Apps, die beim Login hohe Sicherheit bieten und dafür kein Passwort benötigen. Aber 52 Prozent derer, die nach einem Hacker-Angriff ihr Verhalten in puncto Passwortsicherheit geändert haben, würden eine solche App nutzen. Diese Apps erlauben es den Usern beim Login, sich statt mit komplizierten, schwer zu merkenden Passwörtern einfach mit ihren unverwechselbaren biometrischen Daten zu identifizieren. Dazu zählt etwa Face-ID, also die Gesichtserkennung, die auf vielen modernen Geräten bereits funktioniert. Somit sind diese Apps nicht nur sehr sicher, sondern sie vereinfachen den Login, weil das Merken und Eintippen komplizierter Passwörter damit Vergangenheit ist. Auch eliminieren sie das Risiko, dass Verbraucher statt komplexer Passwörter auf einfach zu merkende Kombinationen wie "123456" ausweichen, die für Hacker leicht zu knacken sind.

Moderne Technologien bevorzugen

Angesichts der Tatsache, dass die Verbrauer sich von Unternehmen gleichermaßen Sicherheit und Komfort beim Login wünschen, erstaunt die Skepsis gegenüber passwortlosen Logins. Der Grund dürfte das mangelnde Wissen darüber sein; auch, weil diese Lösungen noch nicht überall Standard sind. "Als User würde ich im eigenen Interesse großen Wert darauf legen, dass mir Unternehmen oder Institutionen, bei denen ich Online-Konten besitze, die modernste Technologie und Sicherheitsverstärker wie die Mehrfaktor-Authentifizierung bieten", erklärt Stephan Schweizer, CEO der Nevis Security AG. "Warum noch auf komplizierte und riskante Passwörter setzen, wenn es doch einfach ginge? Mit unserem Sicherheitsbarometer 2021 möchten wir sowohl auf Verbraucher- als auch auf Unternehmensseite ein Bewusstsein dafür schaffen, dass es unkompliziert zu integrierende passwortlose Login-Systeme gibt, bei denen Sicherheit und Nutzerfreundlichkeit sich nicht ausschließen. Das kommt letztlich Verbrauchern und Unternehmen zugute."

Das Nevis-Sicherheitsbarometer 2021 steht unter folgendem Link zum Download bereit: https://www.nevis.net/de/nevis-sicherheitsbarometer-2021

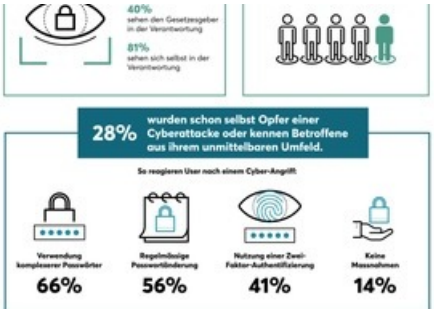
Über Nevis

Nevis entwickelt Sicherheitslösungen für die digitale Welt von morgen: Das Portfolio umfasst passwortfreie Logins, die sich intuitiv bedienen lassen und Nutzerdaten optimal schützen. In der Schweiz ist Nevis Marktführer für Identity und Access Management und sichert über 80 Prozent aller E-Banking-Transaktionen. Weltweit setzen Behörden sowie führende Dienstleistungs- und Industrieunternehmen auf Lösungen von Nevis. Der Spezialist für Authentifizierung unterhält Standorte in der Schweiz, Deutschland und Ungarn.

Pressekontakt:

LEWIS Communications GmbH
Ingo Geisler
Johannstraße 1
40476 Düsseldorf
+49 (0)211 882 476 07
nevis-security@teamlewis.com

Medieninhalte



Das neue Nevis Sicherheitsbarometer 2021 zeigt, wie Konsumenten die Sicherheit ihrer Daten selbst verbessern können und warum Passwörter beim Login ein echter Risikofaktor sind. / Weiterer Text über ots und www.presseportal.de/nr/157549 / Die Verwendung dieses Bildes ist für redaktionelle Zwecke unter Beachtung ggf. genannter Nutzungsbedingungen honorarfrei. Veröffentlichung bitte mit Bildrechte-Hinweis.