

IT-Sicherheit

Passwort-Vergessen kostet 6 Milliarden Euro

7,8 Minuten jede Woche verbringen Berufstätige damit, ihre Passwörter zu verwalten. Aufs Jahr hoch gerechnet entsteht ein Milliarden-Schaden, so Symantec.



Nachdenken, falsch eintippen, Support anrufen:
Jeder Angestellte verbringt mit der Verwaltung seiner Passwörter fast acht Minuten in der Woche, hat der Marktforscher Yougov errechnet.

Foto: Nikolai Sorokin - Fotolia.com

Die Zahl ist beeindruckend: 6,14 Milliarden Euro gehen deutschen Unternehmen jedes Jahr verloren - weil Angestellte **Schwierigkeiten mit Passwörtern**¹ haben. Das behauptet zumindest der Kölner Marktforscher Yougov in einer Analyse, die der Sicherheitsanbieter Symantec in Auftrag gegeben hatte.

Die Rechnung basiert auf folgender Überlegung: Jeder Mitarbeiter braucht im Schnitt 7,8 Minuten pro Woche für die Verwaltung seiner Passwörter. Bei einem Stundenlohn von durchschnittlich 22,4 Euro - Yougov bezieht sich nach eigenen Angaben auf Zahlen des Statistischen Bundesamtes - ergeben sich daraus Kosten von 118 Millionen Euro pro Woche und 6,14 Milliarden im Jahr.

» Sachsen und Thüringer erinnern sich am besten

Verwaltung der Passwörter² beinhaltet für die Autoren der Umfrage das Erinnern aktueller Kennwörter und das Kreieren neuer, Anfordern neuer Passwörter, Inanspruchnahme vom Support, weil man sich nicht einloggen kann und ähnliches. Das Eintippen der Passwörter selbst fällt nicht darunter.

Glaubt man den Forschern, dürften Unternehmen in der Region Sachsen und Thüringen am wenigsten Geld verlieren. Hier geben 24 Prozent der mehr als 2.000 Befragten an, überhaupt keine Schwierigkeiten mit dem Verwalten ihrer Kennwörter zu haben. In Hessen, Rheinland-Pfalz und im Saarland sind es dagegen nur 14 Prozent.

Im bundesweiten Durchschnitt nehmen insgesamt 18 Prozent der Befragten für sich in Anspruch, ihre **Passwörter problemlos im Griff**³ zu haben und keine Minute dafür zu verschwenden. Unter den Frauen behauptet das sogar jede Fünfte.

Eine Mehrheit von insgesamt 52 Prozent erklärt, wöchentlich zwischen einer und 15 Minuten für die Passwort-Verwaltung zu brauchen. In der Vorzeige-Region Sachsen und Thüringen sind es 43 Prozent. Im Norden Deutschlands (Schleswig-Holstein, Hamburg, Niedersachsen und Bremen) benötigen dagegen fast zwei Drittel (64 Prozent) so viel Zeit dafür.

» Nur jeder Vierte hat sichere Passwörter

Noch ein Ergebnis der Studie: Offenbar spielt das Alter beim Kennwörter-Management nur eine geringe Rolle. Unter den Befragten, die von sich selbst behaupten, überhaupt keine Schwierigkeiten damit zu haben, stammen jeweils 20 Prozent aus den Altersgruppen 18 bis 24 Jahre und 35 bis 44 Jahre. Lediglich die Gruppe ab 55 Jahren ist mit 15 Prozent unterproportional vertreten. Die Altersstufen dazwischen liegen bei 17 Prozent (25 bis 34 Jahre) und 19 Prozent (45 bis 54 Jahre).

Yougov wollte außerdem wissen, wie die Befragten ihre Benutzerkonten sichern. Fazit: Nur 27 Prozent arbeiten **mit Kennwörtern, die die Studienautoren als "stärker" anerkennen**⁴. Das heißt: Die Passwords

bestehen aus einer zufälligen Buchstaben-/Nummern-Reihenfolge. 29 Prozent verwenden dagegen Kennwörter, die als "leicht zu erraten" beziehungsweise "leicht zu recherchieren" gelten, also zum Beispiel den Namen des Haustieres oder den des Partners. Beliebt sind auch die Heimatstadt und das eigene Geburtsdatum. Solche Daten finden Cyberkriminelle leicht in sozialen Netzwerken.

Über den Tag verteilt müssen die Befragten im Durchschnitt sechsmal ein Passwort eingeben. Um sich das zu erleichtern, verwenden 42 Prozent der Nutzer dasselbe Kennwort für mehrere Konten. Als Auftraggeber der Studie fügt Symantec folgende Tipps für mehr Sicherheit an:

Unternehmen sollten **firmenweit starke Authentifizierung** einführen, und das nicht nur für bestimmte Anwendungen. Ein Unternehmen sei "nur so sicher wie das schwächste Passwort".

» Sicherheits-Trainings für Mitarbeiter anbieten

Open Enterprise-Anwendungen wie Software-as-a-Service- und Partnerzugänge müssen ebenso geschützt werden wie Systeme innerhalb des Unternehmens.

Entscheider sollten sicherstellen, dass Mitarbeiter **starke Passwords benutzen**. Stark heißt: Mindestens acht Zeichen, darunter alphanumerische Elemente und Sonderzeichen. Es ist wichtig, dass Angestellte **unterschiedliche Kennwörter benutzen** und diese regelmäßig wechseln.

Firmenleitungen sollten der Belegschaft die Sicherheitsprobleme erklären und diese **Informationen durch Bildungsprogramme** verstärken.

¹ <http://www.cio.de/knowledgecenter/security/2254125/index.html>

² <http://www.cio.de/knowledgecenter/security/2236957/index.html>

³ <http://www.cio.de/knowledgecenter/security/191957/index.html>

⁴ http://www.cio.de/das_iphone_im_unternehmen/tipps/2265812/index2.html

⁵ <http://www.cio.de/knowledgecenter/security/2240510/index.html>

von Christiane Pütter

IDG Business Media GmbH

Alle Rechte vorbehalten. Jegliche Vervielfältigung oder Weiterverbreitung in jedem Medium in Teilen oder als Ganzes bedarf der schriftlichen Zustimmung der IDG Business Media GmbH. DPA-Texte und Bilder sind urheberrechtlich geschützt und dürfen weder reproduziert noch wiederverwendet oder für gewerbliche Zwecke verwendet werden. Für den Fall, dass in CIO unzutreffende Informationen veröffentlicht oder in Programmen oder Datenbanken Fehler enthalten sein sollten, kommt eine Haftung nur bei grober Fahrlässigkeit des Verlages oder seiner Mitarbeiter in Betracht. Die Redaktion übernimmt keine Haftung für unverlangt eingesandte Manuskripte, Fotos und Illustrationen. Für Inhalte externer Seiten, auf die von CIO aus gelinkt wird, übernimmt die IDG Business Media GmbH keine Verantwortung.