

**CYBERSECURITY** – Sind Passwort und Benutzername bekannt, können Unbefugte mit kleinem Aufwand an vertraulichen Informationen gelangen. Für Experten wie Chris Eckert völlig klar. Ein grosser finanzieller Schaden – verbunden mit Ärger, Existenzängsten bis hin zum Reputationsverlust in Ihrem Unternehmen – ist abwendbar, wenn Sie sich nachhaltig mit der Schwachstelle Mensch befassen.

# «Immer wieder ... Passwörter!!!»

Mal ehrlich: Wie oft ertappen Sie sich dabei, beim Erstellen eines neuen Accounts oder beim Bestellen von Produkten oder Dienstleistungen auf einer Onlineplattform, ein bereits bestehendes, sehr simples Passwort zu verwenden? Und machen Sie sich kritische Gedanken darüber, welche negativen Folgen geschäftlich oder privat daraus resultieren können? Ist Ihnen bewusst, dass trotz gutem, technischen Schutz aber aufgrund nachlässigen Verhaltens nur eines Mitarbeitenden eine unbefugte Person oder kriminelle Hacker sich in Ihren IT-Systemen anmelden, die Computeridentität und alle Zugriffsberechtigungen auf Ihre Daten übernehmen können?

Beim Erhalt meines ersten Computers bei der Kantonspolizei Zürich im Jahr 1991 wurde mir eingebläut, keine simplen Passwörter zu verwenden. Es gab damals schon interne Mindestanforderungen, welche erfüllt werden mussten und eine umfassende Instruktion betreffend die Wahl, Länge und Zusammensetzung der Passwörter.

Ich weiss nicht, wie oft in den letzten Jahren Expertenkollegen und ich an Workshops, Vorträgen und Schulungen auf das Thema Passwörter sowie den Umgang damit hingewie-



*Achtung Vorsicht: Der liederlichen Umgang mit Passwörtern kann das Unternehmen teuer zu stehen kommen.*

Bild: 123RF

sen haben. Gefühlt bei Hunderten von Medienbeiträgen, Weiterbildungen und Tagungen war die Passwortproblematik immer wieder ein Kernthema. Nun, 30 Jahre später, sind wir einen Schritt weiter?

## Trugschluss entgegentreten

Die Top 10 der beliebtesten und zugleich dämlichsten Passwörter 2020 (Quelle: Die Welt)

- Platz 10** senha (Portugiesisch für Passwort)
- Platz 9** 1234567890
- Platz 8** 12345
- Platz 7** 123123
- Platz 6** 11111
- Platz 5** 12345678
- Platz 4** password
- Platz 3** picture1
- Platz 2** 123456789
- Platz 1** 123456

Erschreckenderweise, leider kaum. Wir wissen es zwar und haben schon oft darüber gehört und gelesen... Aber das gehört in den Bereich IT und dafür gibt es Zuständige, die sich darum kümmern sollen. Als simpler User bin ich zudem sowieso völlig uninteressant für Hacker. Diesem Trugschluss gilt es entgegenzutreten. Verhindern Sie als Inhaber oder Chef eines Unternehmens, egal in welcher Branche Sie tätig sind, dass es in Ihrem Betrieb zu Identitätsdiebstahl, hervorgerufen durch liederlichen Umgang mit Passwörtern, kommen kann. Denn, Sicherheit ist Chefsache, auch die Cybersecurity gehört dazu.

## Was können Sie tun?

- Instruieren/schulen Sie Ihre Mitarbeitenden regelmässig im Bereich der Informationssicherheit.

Einmalige Informationen bringen nichts!

- Stärken Sie den Mitarbeitenden das Bewusstsein, dass sie selbst für Handlungen geradestehen müssen, welche unter ihrem Benutzernamen erfolgt sind.
- Sorgen Sie dafür, dass Ihr Personal verpflichtet wird, nur starke Passwörter einzusetzen, welche auch regelmässig geändert werden (empfohlener Rhythmus: 2 Monate).
- Ein starkes Passwort hat mehr als 8 Stellen und enthält Zahlen, Sonderzeichen sowie Gross- und Kleinbuchstaben.
- Keine Namen / Vornamen / Geburtsdaten von sich selbst, Verwandten, Freunden und Tieren.
- Generieren Sie starke Passwörter z.B. aus einem Satz, dann erinnern Sie sich eher. Z. B.:

## UNTERNEHMENSCHUTZ

### Neuer Lehrgang

Zugeschnitten auf den umfassenden Unternehmensschutz für KMU in der Schweiz wurde ein neuer Lehrgang erschaffen. Der CAS «Business Protection» an der Hochschule für Wirtschaft HWZ in Zürich startet am 18. Februar 2022 und dauert berufsbegleitend 18 Tage. Es sind noch Studienplätze frei:



- Verwenden Sie einen Passwortsafe für all Ihre unzähligen Passwörter.
- Kontrollieren Sie die Qualität Ihres Passwortes mit einem Online-Passwort-Checker.
- Geben Sie Ihre Passwörter niemals an Dritte weiter, auch nicht an Ihre Stellvertreter.

## DER AUTOR

**Chris Eckert** ist Founding Partner der Swiss Business Protection AG. Er verfügt über mehr als 30 Jahre kriminalistische Erfahrung, erworben bei der Kantonspolizei Zürich sowie der Bundeskriminalpolizei.

[www.swissbp.ch](http://www.swissbp.ch)

Chris Eckert