

Das Passwort-Dilemma und wie Sie es umgehen können

Herrsching, 22.05.2014

„Bitte ändern Sie Ihre Passwörter!“

Hinweise wie diese haben wir in den vergangenen Wochen oft gelesen. Erst kam das Thema „Heart-bleed“ auf den Tisch. Dabei wurde bekannt, dass durch eine Sicherheitslücke in der Verschlüsselungssoftware OpenSSL möglicherweise unzählige Kundenkonten verschiedenster Anbieter von Online-Plattformen kompromittiert wurden. Die allgemeine Empfehlung: Passwörter ändern. Gerade heute wurde bekannt, dass Hacker erfolgreich Kundendaten von Ebay abgezogen haben. Und wieder heißt es: ändern Sie Ihre Passwörter!

Diese Empfehlung ist mit Sicherheit richtig. Insbesondere dann, wenn Sie das gleiche Passwort ggf. sogar in Verbindung mit der gleichen Email-Adresse als Zugangsdaten für mehrere Onlineshops oder Serviceplattformen nutzen, wird es gefährlich. Hat jemand Ihre Zugangsdaten für Ebay in der Hand, liegt es nahe, diese auch bei Amazon, Facebook oder sogar auf Onlineplattformen von Behörden zu testen.

Wetten, dass Sie Ihre Passwörter nicht ändern?

Das trifft zumindest auf die meisten Internet-Nutzer zu und hat ganz einfache Ursachen. Sie können sich so viele Passwörter nicht merken. Oder Ihnen fallen gar keine sicheren Passwörter ein, und die meisten Plattformen lassen die „einfachen“ Passwörter, die bisher oft zum Einsatz kommen, bei Neuhinterlegung gar nicht mehr zu.

Wie denke ich mir ein sicheres Passwort aus?

Unter einem im normalen Gebrauch sicheren Passwort versteht man heute ein Passwort mit mindestens 12 Stellen, das aus einer Kombination von Zahlen, Buchstaben in Groß- und Kleinschreibung und Sonderzeichen besteht. Es sollte kein Wort aus dem Wörterbuch enthalten, keine Eigennamen, Geburtstage und ähnliche leicht herauszufindende Inhalte.

Das können Sie sich tatsächlich ganz leicht zusammenstellen und auch wirklich merken, wenn Sie einen einfachen Tipp beherzigen. Arbeiten Sie mit einem Merksatz. Aus den Wörtern dieses Merksatzes nehmen Sie die Anfangsbuchstaben, reichern den Satz um ein Satzzeichen an (Sonderzeichen) und achten darauf, dass der Satz eine Zahl enthält.

Hier ein Beispiel:

Abends um 17 Uhr läuft Werbung von Amazon im Radio!

Das Passwort:

Au17UIWvAiR!

Die reine Zahlen- und Buchstabenkombination könnten Sie sich ganz sicher nicht merken. Mit Hilfe des Merksatzes ist das kein Problem, und Sie haben ein wirklich sicheres Passwort zur Hand.

Mit diesem Trick lösen Sie auch die Herausforderung, sich für jedes Benutzerkonto ein eigenes Passwort zu merken. Wie das funktioniert haben Sie wahrscheinlich schon selbst entdeckt: Sie ersetzen in Ihrem Merksatz einfach den Anbieter.

Beispiel:

Abends um 17 Uhr läuft Werbung von Zalando im Radio!

Tun Sie uns jetzt noch einen kleinen Gefallen: nutzen Sie auf keinen Fall diesen Beispielsatz!

Haben Sie an die Benutzerkonten Ihrer Kanzlei gedacht?

Wenn wir Hinweise wie „Bitte ändern Sie Ihr Ebay-Passwort“ lesen, denken wir in der Regel erst einmal an private Belange. Achten Sie darauf, dass auch die Kunden-Zugänge, die Sie für Ihre Kanzlei bei den Lieferanten angelegt haben, geändert werden. Eventuell bestellen Sie auch für die Kanzlei bei Amazon oder bei Lieferanten für Büromaterial und ähnliches online.

Auch Online-Administratorenzugänge müssen beachtet werden. Wenn Sie die Inhalte Ihrer Kanzlei-Homepage selbst pflegen und dafür einen Zugang zum ContentManagementSystem haben, müssen Sie unbedingt auf ein sicheres Passwort achten. Es wäre sicher sehr unangenehm, wenn jemand den Zugang zu Ihrer Homepage knackt und diese beispielsweise zur Verbreitung illegaler Inhalte nutzt. So etwas kommt regelmäßig vor.

Das gilt nicht nur für's Internet.

Passwörter sind im Alltag Ihrer Kanzlei ein ganz wesentlicher Sicherheitsfaktor hinsichtlich der Zugangs- und Zugriffskontrolle Ihrer EDV-Systeme. Passwörter, die jeder kennt, die unter der Schreiberunterlage liegen oder die aus zu einfachen Kombinationen bestehen, beeinträchtigen Ihr Datenschutzniveau in essentieller Weise. Das gilt auch dann, wenn Sie Mandanten den Zugriff von außen auf bestimmte Systeme gewähren und hier nicht sicherstellen, dass der Passwortschutz ausreichend gewährleistet ist oder zu schwache Passwörter vorgeben.

Verwenden Sie den Passwort-Merksatz daher am Besten auch in der Kanzlei, z.B. zur Bildung Ihrer Windows-Passwörter, für Banking-Zugänge etc. und für die Festlegung von Passwörtern Ihrer Mandanten.

Mehr Informationen zum Thema Datenschutz erhalten Sie hier:

<http://www.munker.info/datenschutzberatung>

Xing: <https://www.xing.com/companies/munker%25257Cunternehmensberatung>

Facebook: <https://www.facebook.com/MunkerUnternehmensberatung>

Twitter: <https://twitter.com/MunkerDS>