Datenklau – na und?

◢ Massenhacks, Identitätsdiebstahl, verhökerte Passwörter – immer wieder schrecken Medienberichte über **geknackte Nutzerkonten** die Öffentlichkeit auf. Die wirtschaftlichen Folgen für die betroffenen Unternehmen müssten eigentlich immens sein. Doch weit gefehlt – der **Aufregung** folgt schnell gefährliche Gelassenheit. ›

◢ Auf Paste Sites, Sharing-Seiten und Online-Marktplätzen finden sich umfangreiche Listen mit gestohlenen Zugangsdaten, sie werden gehandelt und geteilt. Jüngst sorgte das Internetportal Yahoo für Schlagzeilen, als es zugeben musste, dass 500 Millionen seiner Nutzerkonten bereits 2014 kompromittiert worden waren. Das könnte als größter Datendiebstahl in die Geschichte des kommerziellen Internets eingehen. Die Angreifer lasen Namen, Mailadressen, Geburtsdaten, Telefonnummern und Passwörter in verschlüsselter Form aus. Wahrscheinlich werden die Hacker versuchen, mit diesen Informationen in weitere Kennungen der Betroffenen einzudringen. Dass das funktioniert, haben frühere Hacks in sozialen Netzwerken bereits gezeigt. Natürlich ist Yahoo kein Einzelfall. Angriffe auf Millionen von Nutzerkonten gelangen bei LinkedIn, Adobe, Dropbox und MySpace. Oft wurde das erst Jahre später publik. Trotz solcher Vorfälle leiden die betroffenen Anbieter nicht unter großen Abwanderungsverlusten. Die Zahl der Kunden, die aus Ärger über möglicherweise unzureichende IT-Sicherheitsmaßnahmen zur Konkurrenz wechseln, gilt als gering. Immer noch ändern viele nicht einmal ihre Passwörter, um sich gegen künftige Angriffe besser zu wappnen. Warum ist das so? Legen die Nutzer womöglich weitaus weniger Wert auf die Sicherheit ihrer Daten als allgemein angenommen? Ist sie ihnen gar egal oder trügt dieser Eindruck? Die Redaktion von business impact debattiert das Pro und Kontra.

Fotos: Shutterstock/Rob Kints, Claus Dick

Pro:

Die Provider tragen keine Schuld

Von Ralf Bretting

◢ Es ist kein halbes Jahr her, da brachte der Report „Compromised Credentials“ eine traurige Wahrheit ans Licht. Der IT-Security-Dienstleister Digital Shadows hatte die 1000 größten Unternehmen der Forbes-Global-2000-Liste auf kompromittierte Authentifizierungsdaten überprüft. Das Ergebnis überraschte sogar Experten: Insgesamt wurden mehr als fünfeinhalb Millionen gehackte E-Mail- und Passwortkombinationen entdeckt. Betroffen waren 97 Prozent der untersuchten Firmen über alle Branchen hinweg. Durchschnittlich fanden sich pro Unternehmen 706 geleakte Login-Daten online. Quintessenz: Mitarbeiter, die ihre Mailadressen und vor allem die dazugehörigen Passwörter nicht regelmäßig ändern, setzen sich einem hohen Risiko aus. Das gilt für jeden von uns, der sich in der digitalen Welt bewegt – und die meisten wissen das. Gehackte Webseiten mit systemtechnischen Schwachstellen, Spear-Phishing-Mails im Posteingang, Schnüffel-Apps auf dem Smartphone – die Bedrohungen lauern überall. Und sie nehmen zu, je vernetzter wir unser Leben gestalten. Deshalb ist Eigenschutz unabdingbar. In einem freien Netz trägt zunächst einmal jeder selbst die Verantwortung dafür, dass seine Daten geschützt sind. Persönliche Dateien, die ich als sensibel einstufe, stelle ich grundsätzlich nur über eine spezielle Verschlüsselungssoftware in die Cloud. Passwörter generiere ich mit

Weiter auf Seite 58 ➟

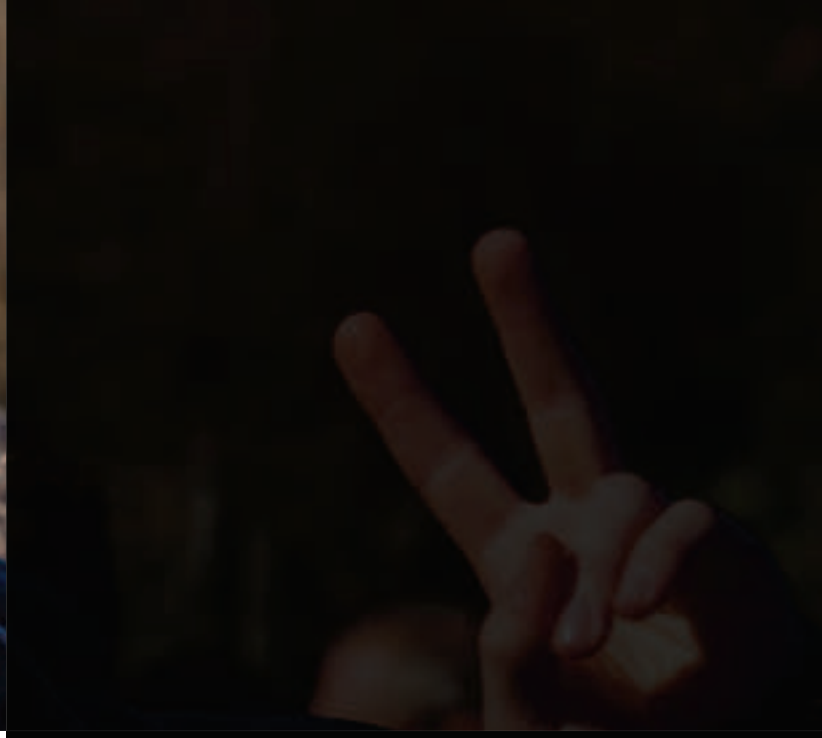
Kontra:

Nutzern ist der Datenklau nicht egal

Von Ulrich Hottelet

◢ Allzu viele Nutzer ziehen keine oder zu wenig Konsequenzen aus einem Datenklau. Das ist bedauerlich und schädlich – sowohl für sie selbst als auch letztlich für uns alle. Denn wer in einem solchen Fall nicht einmal sein Passwort ändert, muss sich nicht wundern, wenn er demnächst wieder Opfer eines Datendiebstahls wird. Wer ein- und dasselbe Passwort gar für mehrere Webseiten nutzt – eine weit verbreitete Praxis, vor der immer wieder gewarnt wird –, erleidet bei der nächsten Attacke möglicherweise einen noch größeren Schaden. Wenn sich selbst bei gravierenden Sicherheitsverstößen nur wenige Kunden dazu durchringen können, ihrem Anbieter die rote Karte zu zeigen und zur Konkurrenz zu wechseln, dann steigert das nicht die Motivation der fahrlässigen Unternehmen, künftig ein größeres Augenmerk auf Datensicherheit zu legen. Im Umkehrschluss aber anzunehmen, den Nutzern sei es regelrecht egal, wenn ihre Daten gehackt werden, ist eindeutig zu kurz gegriffen. Erstens wissen viele nichts davon, wenn sie von ihrem Anbieter nicht auf die Ausspähung aufmerksam gemacht werden. Das gilt für viele selbst dann, wenn die Publikumsmedien über einen Datenklau berichten, was ohnehin nur bei Massenhacks der Fall ist. Zweitens haben manche einfach vor der Gefahr kapituliert. Allzu oft wurden IT-Riesen, Online-Händler und soziale Medien schon von Datenraubzügen heimgesucht. Drittens sollte man die menschliche Trägheit nie unterschätzen. Es ist einfach bequemer, beim alten Anbieter zu bleiben, als sich über Alternativen zu in

Weiter auf Seite 58 ➟



einer speziellen App. Sie sind mindestens 20 Zeichen lang und eine wilde Kombination aus Buchstaben, Zahlen und Sonderzeichen, die sich niemand merken kann. Auf jeder Webseite, auf der ich mich einloggen muss, verwende ich ein anderes Kennwort und ersetze es nach drei Monaten durch ein neues. Beide Lösungen, die mich und meine Daten schützen, gibt es nicht umsonst. Aber die knapp 50 Euro, die ich dafür pro Jahr bezahle, sind gut angelegt und geben mir das Gefühl von Sicherheit. Deshalb habe ich kein Problem, Facebook, Dropbox, Evernote, Gmail und Co. beruflich wie privat zu nutzen. In mehr als 25 Jahren Online-Aktivität ist mir nichts abhanden gekommen und niemand hat meine digitale Identität missbraucht. Es gab keine Erpressungsversuche, kein Credential Stuffing. Ein Freischein für die Zukunft ist das natürlich nicht. Aber selbst wenn mich eines Tages der Verdacht beschleichen sollte, etwas sei nicht in Ordnung, würde ich darin keinen Grund sehen, Hals über Kopf nach alternativen Serviceanbietern am Markt zu suchen. Ich würde einfach ein neues kompliziertes Passwort für meinen Account generieren – und fertig. Die Erwartung, dass allein ein Provider für den Schutz der Privatsphäre verantwortlich zeichnet, ist mir völlig fremd. Für den verkehrssicheren Zustand eines Autos im Betrieb müssen ja auch Halter und Fahrer sorgen, nicht der Hersteller. Wer Sicherheit möchte, muss auch bereit sein, etwas dafür zu tun. Das gilt für alle Lebensbereiche, nicht nur in der Online-Welt.

formieren und neu zu registrieren. Das heißt aber nicht, dass es die Kunden nicht vorziehen würden, von fremdem Zugriff auf ihre gespeicherten Informationen verschont zu bleiben. Viertens sind genaue Zahlen über Nutzerwechsel kaum bekannt – die Anbieter haben kein Interesse, den Rückgang ihrer Kundschaft publik zu machen. Und fünftens lassen sich die Gründe nur vermuten, warum jemand einen bestimmten Anbieter wählt und behält. Der Preis ist bei Kaufentscheidungen oft das wichtigste Kriterium. Angenommen ein anderes Unternehmen bietet mehr Sicherheit, fordert aber einen höheren Preis dafür, so wird es im Markt schwer sein, dem billigeren Wettbewerber die Kunden abzujagen. Weitere wichtige Entscheidungskriterien im Internet sind die Funktionalität des Portals, seine Bedienfreundlichkeit, ein ansprechendes Design, der Unterhaltungsfaktor und eine hohe Nutzerzahl, insbesondere in sozialen Netzwerken. Mit all dem punkten gerade die großen amerikanischen Anbieter. Ihre deutschen, meist viel kleineren Konkurrenten verweisen zwar oft auf ein besseres Niveau bei Sicherheit und Datenschutz, können aber vielfach in den anderen Bereichen nicht Paroli bieten. „The winner takes it all“, heißt es im Internet. Heißt: Der Marktführer ist nur schwer aus seiner Position zu verdrängen. Daraus aber zu folgern, den Nutzern sei es ziemlich egal, wenn ihre Daten geklaut werden, ist ein Trugschluss. Er hätte im Übrigen die höchst unerfreuliche Konsequenz, dass sich die Unternehmen nicht um mehr Sicherheit bemühen müssten, schließlich bleiben ihnen die Kunden ja sowieso erhalten. Und das ist so ziemlich das Letzte, was wir Nutzer uns von Anbietern wünschen könnten.