Axel Kossel

Risiko Identitätsklau

Wenn Geld und guter Ruf in Gefahr geraten

Im richtigen Leben belegt der Personalausweis unsere Identität. Seit zwei Jahren kann er das auch in der virtuellen Online-Welt, doch seine eID-Funktion wird kaum genutzt. Stattdessen verlässt man sich im Internet meist auf das einfache System aus Benutzername und Passwort – und wird dadurch leicht zum Opfer von Identitätsdieben.

Passieren kann es jedem. Zur Nachricht wird es aber erst, wenn es einem Politiker passiert oder einem Fußballstar. Oder einem Journalisten wie Mat Honan, der seine Erfahrung auf Wired.com so zusammenfasst: „Innerhalb von nur einer Stunde wurde mein gesamtes digitales Leben zerstört." Hacker hatten sein Google-Konto gekapert und gelöscht, über seinen Twitter-Account rassistische und homophobe Statements verbreitet – und über Apples Remote-Wipe-Funktion sogar sein iPhone, iPad und MacBook ferngelöscht.

Möglich wurde dieser breit angelegte Angriff durch die ungeschickte Verkettung der Teile, die Honans digitale Identität ausmachten. Der genaue Vorgang ließ sich mit Hilfe einer Person rekonstruieren, die mit Honan später Kontakt aufnahm und sich als einer der Hacker zu erkennen gab. Sie schrieb, das einzige Ziel der Aktion sei der prominente Twitter-Account des Journalisten gewesen. Mit dem Löschen des E-Mail-Verkehrs aus acht Jahren im Gmail-Konto und der gesamten privaten wie beruflichen Daten auf den Geräten habe man nur verhindern wol-

len, dass Honan allzu schnell die Kontrolle zurückerlangt.

Das Kurzprofil des begehrten Twitter-Accounts führte die Hacker zu Honans Website. Dort fanden sie seine Google-Adresse „mhonan@gmail.com“. Die Passwort-vergessen-Funktion von Twitter bestätigte den Angreifern, dass diese Adresse mit dem Account des Kurznachrichtendienstes verbunden war. Bei Google erfuhren die Hacker wiederum, dass die Wiederherstellungsadresse des Kontos „m:*:*:*:*n@me.com“ lautete. Es war unschwer zu erraten, dass sich hinter den Sternchen der Name aus der Gmail-Adresse verbarg.

Offene Flanke

Damit hatten die Hacker einen Angriffspunkt gefunden. Denn sie wussten aus Erfahrung, dass sie nur die bei Apple hinterlegte Rechnungsadresse und die letzten vier Ziffern der Kreditkartennummer des Opfers benötigen würden, um das Passwort dieses E-Mail-Kontos zu ändern und es so unter ihre Kontrolle zu bekommen. Apple räumte später ein, dass dies möglich gewesen sei, obwohl für diesen Vorgang Sicherheitsfragen hinterlegt waren. Dabei seien allerdings nicht alle internen Richtlinien vollständig befolgt worden.

Die Anschrift von Honan war im Internet leicht zu beschaffen. Doch um an die letzten vier Ziffern seiner Kreditkarte zu gelangen, bedurfte es eines Umwegs über Amazon. Einer der Hacker rief dort an, gab sich für Honan aus und erklärte, er wolle eine weitere Kreditkarte hinterlegen. Dazu musste er nur den Namen, die Anschrift und die Gmail-Adresse von Honan kennen. In einem zweiten Anruf bat er dann darum, die hinterlegte E-Mail-Adresse zu ändern. Als Sicherheitsabfrage dafür wollte Amazon die vollständige Kreditkartennummer wissen – kein Problem, der Hacker hatte ja gerade selbst eine hinterlegt.

Nun musste er nur noch auf der Amazon-Webseite ein neues Passwort anfordern, das ihm an die neu eingetragene E-Mail-Adresse zugesandt wurde. Damit konnte er sich bei Amazon als Mat Honan anmelden und bekam im Profil das angezeigt, was man bei AppleCare als Sicherheitsmerkmal verlangen würde, um das Passwort für mhonan@me.com zu ändern: die letzten vier Ziffern von Honans echter Kreditkartennummer (die vorderen Stellen wurden nicht angezeigt). Nachdem er das me.com-Konto übernommen hatte, ließ er sich dahin von Google ein neues Passwort senden, um über das Gmail-Konto an ein Passwort für den Twitter-Account zu gelangen – Ziel erreicht.

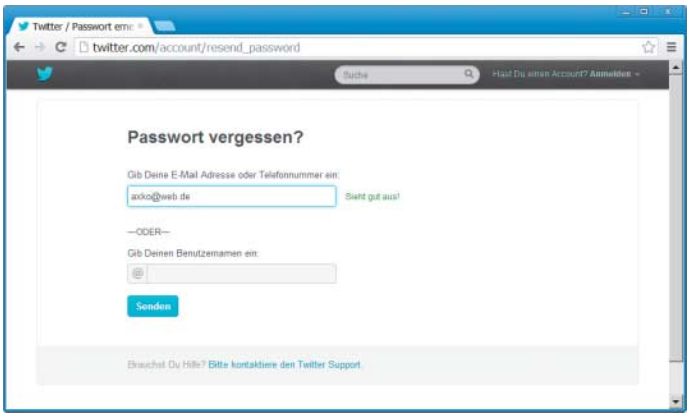
Die Hacker hätten ihrem Opfer auch finanziellen Schaden zufügen können, etwa durch Einkäufe über sein Amazon-Konto. Über die gekaperten E-Mail-Konten hätten sie sich laut Honan sogar Zugriff auf sein Online-Banking oder andere Finanzdienste verschaffen können.

Honan konnte nicht erkennen, welches Sicherheitsrisiko bestand. Amazon zeigte ausgerechnet die letzten vier Ziffern der Kreditkarte an, deren Kenntnis bei Apple wiederum als Beleg für die Identität diente. Für sich gesehen mochte beides der Sicherheit dienen, in Kombination wurde es zur Sicherheitslücke. Apple und Amazon haben mittlerweile nach eigener Aussage diese Mechanismen geändert. Doch Hacker werden andere Dienste finden, deren Eigenschaften geschickt kombiniert Angriffspunkte liefern.

Wunde Punkte

Honans größter Fehler war es, kein Backup der gelöschten Daten angefertigt zu haben. Doch er ist sicherlich nicht der Einzige, der in dieser Hinsicht nachlässig handelt. Ein weiterer Fehler war es, seine öffentlich bekannte Gmail-Adresse und die nur teilweise sichtbare Apple-Adresse so zu wählen, dass man Letztere erraten konnte. Dabei hatte er durch die beiden Accounts bereits einen Vorteil: Es ist nicht unüblich, nur eine E-Mail-Adresse für alles zu nutzen.

Solch öffentliche E-Mail-Adressen, die bei Diensten wie PayPal als Benutzername dienen und bei allen anderen für die Wiederherstellung vergessener Passwörter eingetragen sind, stellen eine große Gefahr dar – einen Single Point of Failure. Lediglich ein einziges Passwort hindert Angreifer am Zugriff auf dieses Konto und damit an der Übernahme der gesamten digitalen Identität. Es kann auf einem ungenügend gegen Schadsoftware abgesicherten System von Keyloggern mitgelesen oder von einem falsch eingestellten E-Mail-Programm unverschlüsselt durchs Netz geschickt werden.



Twitter erleichtert es Identitätsdieben, herauszufinden, mit welcher E-Mail-Adresse sich ihr Opfer angemeldet hat.

Ein weiterer Single Point of Failure ist das Handy, das bei etlichen Diensten wie Google oder Facebook ebenfalls als Recovery-Möglichkeit dient. Auf Smartphones sind darüber hinaus oft noch Clients für diverse Dienste installiert – natürlich mit abgespeicherten Passwörtern, denn die möchte man nicht ständig eintouchen. Der Verlust des Geräts kann daher ebenfalls zur Katastrophe führen.

Bequemlichkeit steht Sicherheit generell entgegen. Bequem sind Single-Sign-on-Dienste, über die man sich mit einem Benutzernamen und einem Passwort bei vielen Diensten anmelden kann. Facebook ist ein prominentes Beispiel dafür: Immer mehr Dienste wickeln die Anmeldungen über das Facebook-Konto ab. Und bei Google gilt ein Konto für alle eigenen und etliche fremde Dienste.

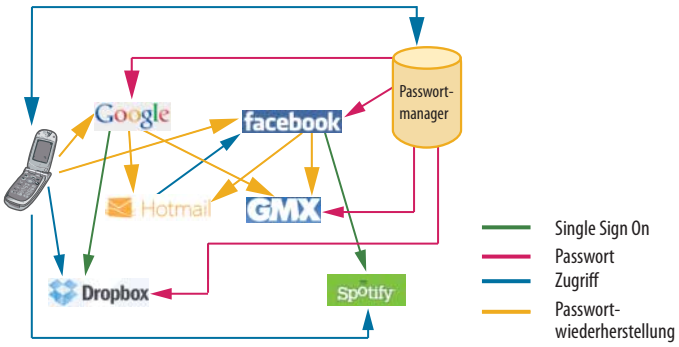
Ebenfalls bequem sind Passwortmanager: Dort hinterlegt man alle Zugangsdaten und schützt sie mit einem Master-Passwort. Diese Sammlung ist dann ein lohnendes Ziel für Angreifer. Der Anwender muss darauf vertrauen, dass sie sicher verschlüsselt ist, besonders wenn sie übers Internet zwischen verschiedenen Geräten synchronisiert wird. So zwang LastPass bereits einmal alle Kunden, ihr Master-Passwort zu ändern, weil der Betreiber „Anomalien im Netzwerkverkehr“ beobachtet hatte. Ob es sich dabei tatsächlich um einen Angriff handelte und ob Kundendaten ausgespäht wurden, hat LastPass nicht verraten.

Der bequemste aller Wege ist es, überall dasselbe Passwort und denselben Benutzernamen zu verwenden. Die Gefahr, die von einem Standardpasswort ausgeht, ist offensichtlich, doch auch den Benutzernamen sollte man variieren. Denn mit Suchmaschinen wie http://namechk.com können Angreifer leicht recherchieren, bei welchen Diensten ein Name noch verwendet wird.

Ausgesperrt

Auch bei einer gut gesicherten Identität kann man Probleme bekommen. Davon berichtet der Blogger Jürgen Vielmeier. Einer seiner Leser hatte sein Google-Konto durch die Option „Bestätigung in zwei Schritten“ geschützt. Dabei bekommt man nach Anmeldung mit Benutzername und Passwort einen Code per SMS oder Anruf auf das Handy übermittelt, dessen Nummer bei Google hinterlegt ist. Eine gute Sache, die Mat Honan vor Schaden hätte bewahren können. Doch für Vielmeiers Leser erwies sie sich als böser Bumerang.

Er wechselte nämlich den Handy-Vertrag und erhielt eine neue Telefonnummer. Dabei vergaß er, bei Google rechtzeitig die neue Nummer zu hinterlegen, da seine Geräte ständig angemeldet waren. Erst nach einiger Zeit bat die Google+-App um eine erneute Anmeldung. Die scheiterte, da kein SMS-Code ankam. Auch misslang es, am PC die neue Telefonnummer einzutragen, da hierfür eine erneute Anmeldung notwendig war.



Die digitale Identität besteht aus vielen Einzelteilen, die miteinander verkettet sind. Das Geflecht birgt für den Anwender kaum erkennbare Sicherheitsrisiken.

Derart ausgesperrt füllte er ein Formular bei Googles Online-Support aus, um den Zugang wieder herzustellen. In mehreren Anläufen scheiterte er an den schwierigen Fragen. Im Support-Forum wurde er nur auf das Formular verwiesen; telefonische Hilfe gab es nicht. Am Ende musste er einsehen, dass Google ihn nicht mehr an seine Daten, unter anderem bei Google Docs erstellte Dokumente, heranlassen würde. Am schlimmsten wird es, wenn man in einem solchen Fall den Zugang zu einem wichtigen E-Mail-Konto verliert: Nicht nur, dass einen wichtige Mails nicht erreichen, auch Profiländerungen sind bei vielen Diensten dann nicht mehr möglich.

Soziale Netze

Nirgendwo zeigen wir mehr von unserer Identität als in den sozialen Netzen. Kein Wunder also, dass dort häufig in Konten eingebrochen wird. Meist wollen die Angreifer, so wie im eingangs geschilderten Fall, eine möglichst prominente Identität nutzen, um Aufmerksamkeit zu erregen. Dazu hacken sie längst nicht immer das Konto des Opfers; oft genügt, unter dessen Namen einen neuen Account anzulegen.

Meist können solche Fälle aufgeklärt werden. So zum Beispiel die Beschimpfungen, die über das Twitter-Profil @piratenOnline im Juni gegen Mesut Özil verbreitet wurden. Schnell wurde klar, dass dies ein Fake-Account war. Pikanterweise untermauerte Innenminister Hans-Peter Friedrich mit diesem Fall seine Forderung nach Vorratsdatenspeicherung, was den Piraten gar nicht schmeckte. Klaus Peukert, Beisitzer im Bundesvorstand der Piratenpartei Deutschland, sagte dazu: „Wir leben lieber damit, dass Spinner in sozialen Netzwerken unter falscher Flagge segeln, statt alle Bürger gleich unter Generalverdacht zu stellen."

Für Privatpersonen können Fake-Einträge böse Folgen haben, etwa strafrechtliche Ermittlungen wegen Äußerungsdelikten oder Ärger mit dem Arbeitgeber. Israel verweigerte 2011 über 300 Besuchern die Einreise, weil diese auf Facebook die Teilnahme an einer pro-palästinensischen Protestaktion angekündigt hatten. Gefälschte Einträge in sozialen Netzen können also auch die Reisepläne des Opfers durcheinanderbringen.

Wie schwierig es sein kann, unerwünschte Inhalte aus dem Netz zu entfernen, davon kann der Jazz-Musiker Bruno Leicht ein Lied singen. Vor rund sechs Jahren hatte er einen Streit mit einem anderen Mitglied in einem US-Forum und wurde daraufhin im Netz mit Schmähungen und retuschierten Fotos verunglimpft. Den Müll von US-Webseiten wie Blogspot und aus Suchmaschinen wie Google entfernen zu lassen, erwies sich als Kampf gegen Windmühlen. Er beauftragte gegen Bezahlung den Dienst „Dein guter Ruf.de", der nach eigenen Angaben Kontakte zu vielen Website-Betreibern weltweit besitzt, über die er Löschanträge stellen kann. Aber auch den Profis gelang es nicht, alles zu beseitigen. Sie versuchen in solchen Fällen, mit positiven Inhalten die Schmähungen von den ersten Trefferseiten der Suchmaschinen zu verdrängen.

Ein gehackter Facebook-Account kann nicht nur dazu dienen, den Ruf des Inhabers zu beschädigen. Gewiefte Betrüger nutzen die darin enthaltenen Informationen, um per Social Engineering an Geld zu kommen. Einen solchen Fall berichtet Franz Patzig in seinem Blog: Eine Bekannte aus den USA kontaktierte ihn via Facebook und berichtete davon, dass sie in London ausgeraubt worden sei und nun festsitze. Ihr Rückflug stehe unmittelbar bevor und sie könne die Hotelrechnung nicht bezahlen.

Patzig hegte keine Zweifel an der Geschichte. Schließlich weiß er, dass seine Bekannte in London studiert hat und gelegentlich dort hinfliegt. Er bot ihr an, mit 150 Euro auszuhelfen, und wies den Betrag per Western Union an. Er rechnete damit, dass sich seine Bekannte nach der Rückkehr bei ihm melden würde. Als die Mail dann kam, enthielt sie eine böse Überraschung: Die Frau warnte alle ihre Kontakte, dass ihr Facebook-Account gehackt worden sei und Betrüger darüber in ihrem Namen um Geld bäten. Patzig erkannte, dass er vor der Zahlung nach einer Information hätte fragen sollen, von der nur er und seine Bekannte wussten und die nicht in Facebook nachzulesen war.

Über die Bestätigung in zwei Schritten kann man die Sicherheit des Google-Kontos stark erhöhen. Diese Google-Funktion, derer sich auch Dropbox bedient, lässt sich über Apps mobil nutzen.

Etwas machtlos

Auch, wenn Sie alles richtig machen, kann Ihre digitale Identität in falsche Hände geraten. Etwa durch eine Sicherheitspanne bei einem Dienst, den Sie nutzen. Sie können Ihre Passwörter noch so hüten, das nützt nichts, wenn durch ein Leck beim Anbieter Millionen Hashes gestohlen werden. Das ist in diesem Sommer bei mehreren Anbietern wie LinkedIn und Last.fm passiert. Und offenbar waren die Hashes so einfach errechnet (ungesalzen), dass sich viele Passwörter daraus gewinnen ließen.

Die Mitarbeiter der Dienste sind nicht vor Fehlern gefeit. Ende Juli musste Dropbox mal wieder ein Datenleck einräumen: Kundendaten wurden aus der Dropbox eines Mitarbeiters entwendet. Der Dieb war demnach über ein geklautes Passwort in den Cloudspeicher eingebrochen. Das hatte er sich auf einer anderen, nicht näher bekannten Website beschafft. Der Diebstahl wurde damit nur möglich, weil der Dropbox-Mitarbeiter dieses Passwort bei mehreren Diensten einsetzte.

Alle Gefahren des Identitätsdiebstahls oder -verlusts lassen sich also nicht bannen. Es gibt aber viele Fehler, die man vermeiden kann. Im Artikel ab Seite 136 finden Sie Strategien und praktische Tipps, um einem Totalverlust der Identität vorzubeugen. Dazu gehören auch Maßnahmen, um die Kontrolle über einen missbrauchten oder gesperrten Account zurückzugewinnen, und das Löschen rufschädigender Inhalte. (ad) c't