Handelsblatt

NACH DEM HACKERANGRIFF AUF YAHOO

Wenn Passwörter nicht mehr schützen

von: Christof Kerkmann
Datum: 27.09.2016 16:00 Uhr

Es ist der nächste große Datendiebstahl: Hacker haben bei Yahoo Informationen über 500 Millionen Nutzer erbeutet. Mit jedem Vorfall wird das Prinzip Passwort geschwächt. Welche Gefahren drohen - und was noch hilft.

Passwort geknackt

Passwörter wie „123456“ oder „dadada“ sind nicht sicher. Kriminelle und Spione können sie in kürzester Zeit knacken.

(Foto: dpa)

Millionen Nutzer haben letzte Woche eine schlechte Nachricht in ihrem E-Mail-Postfach vorgefunden: Angreifer sind in die Systeme von Yahoo eingedrungen und haben 500 Millionen Datensätze samt verschlüsselter Passwörter kopiert - der Internetriese rät nun dazu, die Zugangsdaten schleunigst zu ändern und nach „verdächtigen Aktivitäten“ Ausschau zu halten.

Das Ausmaß des Schadens ist zwar rekordverdächtig, doch der Datendiebstahl an sich kein Einzelfall. In den vergangenen Jahren gelang es Angreifern wiederholt, Millionen von Datensätzen zu stehlen. Jedes Mal müssen die Nutzer fürchten, dass Hacker und Spione sie bestehlen und ausschnüffeln. Und jedes Mal wird deutlich, wie schwach die Absicherung durch Passwörter eigentlich ist.

GROSSE HACKER-ANGRIFFE DER VERGANGENEN JAHRE

Yahoo

Es ist der wahrscheinlich größte Datendiebstahl bei einem einzigen Unternehmen bislang: Mindestens eine halbe Milliarde Nutzer des US-Internetkonzerns Yahoo sind Opfer eines Hackerangriffs geworden. Die Kriminellen erbeuteten E-Mail-Adressen, Geburtsdaten, Telefonnummern, Passwörter und auch unverschlüsselte Sicherheitsfragen, wie Yahoo am Donnerstag mitteilte. Der Angriff ereignete sich schon Ende 2014, im August 2016 wurden 200 Millionen Daten im Netz zum Kauf angeboten – für umgerechnet 1700 Euro.

Ebay

Bei der im Mai 2014 bekanntgewordenen Attacke verschafften sich die Hacker Zugang zu Daten von rund 145 Millionen Kunden, darunter E-Mail- und Wohnadressen sowie Login-Informationen. Die Handelsplattform leitete einen groß angelegten Passwort-Wechsel ein.

Target

Ein Hack der Kassensysteme des US-Supermarkt-Betreibers machte Kreditkarten-Daten von 110 Millionen Kunden zur Beute. Die Angreifer konnten sich einige Zeit unbemerkt im Netz bewegen, die Verkäufe von Target sackten nach Bekanntgabe im Dezember 2013 ab, weil Kunden die Läden mieden.

Home Depot

Beim Angriff auf die amerikanische Baumarkt-Kette gelangten Kreditkarten-Daten von 56 Millionen Kunden in die Hände unbekannter Hacker, wie im September 2014 mitgeteilt wurde. Später räumte Home Depot ein, dass auch über 50 Millionen E-Mail-Adressen betroffen waren.

JP Morgan

Die Hacker erbeuteten bei der im August 2014 bekanntgewordenen Attacke auf die US-Großbank die E-Mail- und Postadressen von 76 Millionen Haushalten und sieben Millionen Unternehmen.

Sony Pictures

Ein Angriff, hinter dem Hacker aus Nordkorea vermutet wurden, legte für Wochen das gesamte Computernetz des Filmstudios lahm. Zudem wurde die E-Mail-Korrespondenz aus mehreren Jahren erbeutet. Die Veröffentlichung vertraulicher Nachrichten sorgte für höchst unangenehme Momente für mehrere Hollywood-Player.

Ashley Madison

Eine Hacker-Gruppe stahl im Juli 2015 Daten von rund 37 Millionen Kunden des Dating-Portals. Da Ashley Madison den Nutzern besondere Vertraulichkeit beim Fremdgehen versprach, waren die Enthüllungen für viele Kunden schockierend.

V-Tech

Der Spezialist für Lernspielzeug räumte den Hacker-Angriff im November 2015 ein. Später wurde bekannt, dass fast 6,4 Millionen Kinder-Profile mit Namen und Geburtsdatum betroffen waren, davon gut 500.000 in Deutschland.

Das Passwort steht schon länger in der Kritik. Es sei „das schlechteste Authentifizierungsverfahren, das wir haben“, sagt Arno Wacker, Professor für angewandte Informationssicherheit an der Uni Kassel. „Aber es ist nun mal das einfachste und billigste - deswegen wird es weiter eingesetzt.“ Dabei spielt die Zeit gegen das Verfahren. Denn Hacker finden immer effizientere Methoden, um Passwörter zu knacken. Wir erklären, wie Nutzer sich damit arrangieren können.

Riskantes „dadada“

E-Mails, soziale Netzwerke, PC, Kreditkarte, und und und: Der normalvernetzte Mensch muss sind mindestens ein halbes Dutzend Passwörter und Codes merken, wenn nicht deutlich mehr. Das macht vielen zu schaffen. Nach einer Umfrage des Hightech-Verbands Bitkom fühlt sich jeder Dritte

(36 Prozent) mit der großen Menge an Passwörter überfordert.

Um damit klarzukommen, setzen viele Nutzer auf eine riskante Vereinfachung: Zum einen verwenden sie ihre Zugangsdaten mehrfach. Wenn Cyberkriminelle diese erbeuten, haben es sie leicht, auch in andere Websites einzudringen - etwa beim Online-Händler Amazon oder dem Netzwerk Facebook .

IT-SICHERHEIT GEHT ANDERS
Die dümmsten Passwörter der Welt

Bild 1 von 19

Hacker

Obwohl Daten- und Identitätsdiebstähle ständig Schlagzeilen machen, benutzen viele Internetnutzer weiterhin unsichere Passwörter. Das beliebteste Passwort der Welt sei nach wie vor „123456", teilte das Potsdamer Hasso-Plattner-Institut für Softwaresystemtechnik (HPI) am Dienstag auf Grundlage einer Analyse gestohlener Datensätze mit. Die HPI-Forscher stützten ihre Angaben auf die Analyse von mehr als 215 Millionen geraubten Identitätsdaten, die sie seit 2011 im Netz entdeckt hatten. Allein in diesem Jahr untersuchten sie nach eigenen Angaben fast 35 Millionen Datensätze, die von Cyberkriminellen in speziellen Internetforen veröffentlicht wurden. Diese Daten stammten demnach aus 15 verschiedenen Quellen, darunter einem Hackerangriff auf das Seitensprungportal Ashley Madison. (Foto: dpa)

Zum anderen verwenden sie einfache Zeichenketten: Das beliebteste Passwort der Welt lautet „123456", gefolgt von „password" und „qwerty", nach der Abfolge der Buchstaben auf der englischen Tastatur. Dass selbst Facebook-Chef Mark Zuckerberg den Begriff „dadada" für sicher genug hielt, um seine Nutzerkonten bei Twitter und Pinterest abzusichern, macht nicht gerade Hoffnung für den Durchschnittsnutzer.

Das mag zwar einige Zeit gut gehen, wie der Fall Zuckerberg zeigt. Doch sobald Hacker wie bei Yahoo persönliche Daten kopieren, werden einfache Passwörter zum Problem. Selbst, wenn diese verschlüsselt sind. Warum das so ist, lesen Sie auf der nächsten Seite.

Es klingt halbwegs beruhigend, was Yahoo in seiner E-Mail an die Nutzer schreibt: Unter den gestohlenen Informationen seien keine „ungeschützten Passwörter" - diese Daten sind also nicht im Klartext vermerkt, sondern unkenntlich gemacht. Was der Konzern verschweigt: Auch derart verschlüsselte Daten lassen sich rekonstruieren, wenn die Hacker nur ausreichend Zeit und Ressourcen haben.

Die von Yahoo eingesetzte Technik ist heute Standard. Experten bezeichnen sie als Hash, englisch

für zerhacken. Das Passwort wird dabei mit einem mathematischen Verfahren in eine lange Buchstaben- und Zahlenkette umgerechnet - wenn Nutzer sich anmelden, überprüft der Anbieter lediglich, ob ihre Zugangsdaten denselben Code produzieren. Ein Beispiel: Der Algorithmus MD5 zerhäckselt das Passwort „123456“ zum Hash-Wert „e10adc3949ba59abbe56e057f20f883e“.

SCHUTZ GEGEN DATENDIEBE

Passwörter gut schützen

Es klingt offensichtlich: Nutzer sollten ihre Passwörter gut schützen. Doch nicht wenige kleben ein Post-it mit Zugangsdaten an den Monitor oder speichern sie gar in einer Datei auf dem Rechner. Beides ist riskant – wenn Eindringlinge ins Büro oder auf den Rechner gelangen, können sie auch auf die E-Mails oder das Content Management System zugreifen.

Erst lesen, dann klicken

Es ist der Klassiker: In der E-Mail wird ein lustiges Katzenbild oder ein sensationelles Video angekündigt. Lädt man den Anhang herunter oder klickt auf den Link, fängt man sich aber einen Virus ein. Daher gilt nach wie vor die Regel, Anhänge und Links kritisch zu prüfen, ebenso Nachrichten von unbekannten Absendern.

Vorsicht mit USB-Sticks

Eine beliebte Angriffsmethode: Hacker lassen präparierte USB-Sticks auf dem Parkplatz oder in der Kantine liegen – und hoffen darauf, dass arglose Mitarbeiter das Gerät an den PC anschließen. Diese Masche funktioniert erschreckend gut. Die Lehre daraus: Nutzer sollten mit unbekannten Speichermedien extrem vorsichtig umgehen.

WLAN nur mit Verschlüsselung

Ob im Café oder am Flughafen: Wer mit seinem Smartphone oder Notebook ein öffentliches WLAN-Netzwerk nutzt, geht ein Risiko ein. Wenn man vertrauliche Daten abrufen will, sollte man das beispielsweise möglichst nur mit einer SSL-Verbindung tun. Weitere Tipps gibt das Bundesamt für Sicherheit in der Informationstechnik (BSI).

Schutz gegen Mitleser

In der Bahn oder im Flugzeug können Mitreisende ohne Probleme einen Blick auf das Notebook oder Smartphone erhaschen – und bekommen so möglicherweise sensible Informationen mit. Sicherheitsexperten raten daher, sich nach sogenannten Schultersurfern umzusehen und im Zweifelsfall die Datei geschlossen zu lassen. Zudem raten sie dringend davon ab, das Gerät auch nur kurz aus dem Auge zu lassen.

Gesunde Skepsis bei Apps

Apps können das Leben leichter machen, aber auch unsicherer: Viele Anwendungen fragen Informationen ab, die die Nutzer vermutlich nicht weitergeben wollen. Gerade Android-Nutzer sollten genau überprüfen, welche Berechtigungen ein Programm einfordert und im Zweifelsfall lieber die Finger davon lassen. Gleiches gilt für PC-Nutzer, die Programme aus dem Nutzer herunterladen und installieren. Besonders illegale Kopien sind häufig verseucht.

Code fürs Smartphone

Es mag zwar vielleicht nerven, wenn man jedes Mal einen Code eingeben muss, bevor man das Smartphone nutzen kann. Doch eine Sperre ist höchst nützlich, wenn das Gerät verloren geht oder gestohlen wird. Viele Firmen schreiben eine solche physische Absicherung vor. Im Büro kann es durchaus sinnvoll sein, den Rechner zu sperren, während man eine Besprechung hat oder in die Mittagspause geht.

Software aktuell halten

Auch dieser Tipp ist bekannt, er wird aber trotzdem oft nicht beherzigt: Nutzer sollten die Software auf ihrem Rechner immer aktuell halten. Das gilt nicht nur für den Virenscanner, sondern auch das Betriebssystem und Anwendungsprogramme wie Browser oder Textverarbeitung. Potentiell können Angreifer viele Lücken ausnutzen, um schädliche Software auf das Gerät zu schleusen.

Doch auch so eine Verschlüsselung lässt sich knacken. Denn mit einer Kopie der Datenbank können die Einbrecher in Ruhe Millionen von Varianten ausprobieren: Sie verschlüsseln die Passwörter mit demselben Verfahren wie der Internetdienst - stimmt das Ergebnis mit dem Hash-Wert in der Datenbank überein, haben sie den Schlüssel in der Hand.

„Die professionellen Gruppen haben in der Regel einen Pool von Rechnern, auf denen sie die viele Anfragen parallel laufen lassen“, sagt Arno Wacker von der Universität Kassel. Dabei setzen sie - quasi als intelligenten Dietrich -Programme wie „John the Ripper“ ein. Die Software gibt zunächst typische Passwörter wie „123456“ und „password“ ein, dann versucht sie es mit Begriffen aus dem Wörterbuch und wandelt sie leicht ab. Mit der Zeit probiert sie immer komplexere Kombinationen. „Das ist ein Massenangriff, der auf die schwächsten Glieder der Kette zielt“, sagt Wacker.

IT-SICHERHEITSGESETZ
Das müssen Unternehmen nach einem Störfall melden

Systematische Analyse

Seit Ende Juli 2015 sind Unternehmen, die kritische Infrastrukturen betreiben, dazu verpflichtet, Störungen in ihrer IT-Infrastruktur an das Bundesamt für Sicherheit in der Informationstechnik (BSI) zu melden. Dieses sammelt die anonymisierten Berichte und wertet sie azs. Auf diese Weise, so heißt es in einem Fachartikel im Magazin „Markt und Mittelstand“, lassen sich etwa bundesweite Hacker-Angriffe systematisch analysieren, um später noch besser gegen solche Attacken gewappnet zu sein.
(Foto: Getty Images)

Die Erfolgsquote hängt von der Verschlüsselungstechnik ab. Das Hash-Verfahren Bcrypt, das Yahoo nach eigenen Angaben überwiegend eingesetzt hat, gilt unter Experten als vergleichsweise sicher - um ein komplexes Passwort zu rekonstruieren, müssen die Angreifer einen deutlich höheren Rechenaufwand betreiben als bei älteren Verfahren wie MD5. Das hilft allerdings nicht, wenn Nutzer einfache Passwörter wie „123456“ oder „Mama“ verwenden: Diese erkennt die Software binnen Minuten.

Ihr Wissen über die Marotten der Menschen verfeinern die Angreifer mit jedem Datensatz. „Sie nutzen aus, dass die Menschen bei Passwörtern gewisse Schemata verwenden“, sagt Thorsten Holz, Professor für Systemsicherheit an der Ruhr-Universität Bochum. So lasse sich ablesen, nach welchen Mechanismen Nutzer ihre Passwörter wählen, womöglich in Abhängigkeit von den Regeln, die der

Onlinedienst dafür vorgibt. „Man kommt weg vom naiven Raten." Das gilt auch für den aktuellen Fall: 500 Millionen Datensätze bieten eine Menge Lernstoff.

Der Hackerangriff auf Yahoo zeigt einmal mehr: Der Schutz mit E-Mail-Adresse und Passwort lässt sich leicht aushebeln. Längst bieten Gerätehersteller und Online-Dienste daher zusätzliche Absicherungen an. Dabei helfen SMS mit Codes genauso wie Fingerabdruck- und Irisscanner.

Erstere sind Mittel für die sogenannte Zwei-Faktor-Authentifizierung: Zum Passwort tritt ein zweiter Faktor, der die Sicherheit gewährleisten soll. Das kann etwa ein Code sein, den Nutzer per SMS erhalten oder auf einer App ablesen können. Oder ein kleiner Stecker, der an die USB-Schnittstelle angeschlossen wird und damit den Nutzer zusätzlich identifiziert.

Das Konzept ist schon Jahrzehnte alt und von Bankgeschäften hinlänglich bekannt – wer am Automaten Geld abholt, muss sowohl die Bankkarte besitzen als auch den Code kennen. Dass es sich erst jetzt auch bei Internetdiensten durchsetzt, hat nach Ansicht von Arno Wacker mit der Verbreitung von mobilen Geräten zu tun. „Früher brauchte man für das Verfahren zusätzliche Hardware wie eine Smartcard", sagt der Informatiker. „Heute kann man davon ausgehen, dass jeder ein Smartphone hat." Damit sei das Verfahren einfach und erschwinglich geworden.

ZEHN TIPPS FÜR MEHR IT-SICHERHEIT

Quelle
Schluss mit dem Silodenken: Geht es nach den Experten von Dell, sollten Mittelständler ihre Sicherheitsstrategie im Rahmen eines abteilungsübergreifenden Projekts auf einheitliche Füße stellen - und zwar mit folgenden zehn Schritten (erschienen im Magazin creditreform 06/2006):
Geschäftsleitung involvieren
Oft beschneidet das Management aus Renditegründen das Budget. Daher: Informieren und sicherstellen, dass die Firmenlenker die Tragweite des Sicherheitsprojekts erkennen.
Bestandsanalyse durchführen
Geräte und Lösungen sowie ihre Eignung für die Abwehr von Cyberattacken katalogisieren - ebenso Rechteverwaltung, Sicherheitsbewusstsein sowie interne und externe Gefahren.
Einsatzteam aufbauen
Eine zentrale Abteilung stimmt alle sicherheitsrelevanten Punkte aufeinander ab. Silos sind wenig effizient und übersehen Sicherheitslücken. Ratsam: einen Chief Information Security Officers ernennen.
Sicherheitsstrategie entwickeln
Wie viel darf welche Sicherheitsmaßnahme kosten, welche Risiken werden in Kauf genommen? Anschließend Budget- und Personal-Szenarien entwerfen.
Budgets verhandeln
Je früher Führungskräfte in das IT-Sicherheitsprojekt eingebunden sind, desto besser können sie nötige Ausgaben nachvollziehen - und desto konstruktiver gestalten sich Verhandlungen.
Sicherheitsrichtlinien ausarbeiten

Und zwar unternehmensweit: Diese sollten auch alle notwendigen Compliance- und sonstigen gesetzgeberischen Aspekte berücksichtigen.

Systeme und Updates installieren

Nicht nur moderne Systeme und Lösungen, die es mit fortschrittlichen Attacken aufnehmen, sind essenziell - aktuelle Updates sind es ebenfalls.

Schulungen vorsehen

Auf Basis eines mittelfristigen Schulungsplans festlegen: Wer wird wie oft zu welchen Themen aus- beziehungsweise fortgebildet?

Der Geschäftsleitung berichten

Dann bleibt sie dem Sicherheitsprojekt gewogen. Eine grafische Aufbereitung der Sicherheitslogs sensibilisiert nachhaltig.

Kontrollschleife einbeziehen

Regelmäßig die Effizienz neuer Maßnahmen und Strukturen durchleuchten. Dabei neue Gefahren, Lösungen am Markt sowie Organisationsveränderungen berücksichtigen.

Da das E-Mail-Konto der Zentralschlüssel zum digitalen Leben ist, sollten Nutzer es unbedingt doppelt absichern. Auch Yahoo weist nach dem Hackerangriff auf diesen Mechanismus hin. Bei vielen anderen Diensten ist es ebenfalls überlegenswert, etwa Apples iCloud, in der viele Nutzer private Daten wie Fotos speichern.

Bequem, aber nicht sehr sicher

Ein anderes Mittel zur Absicherung ist der eigene Körper. Ob per Fingerabdruck oder Irisscan: Zur Absicherung von Smartphones und PCs kommen immer häufiger biometrische Verfahren zum Einsatz. Apple setzte 2013 mit der TouchID-Technologie den Trend, inzwischen haben selbst Mittelklassetelefone einen Sensor. Und mit Windows 10 bietet Microsoft eine Technik zur Entsperrung des Gerätes per Fingerabdruck-, Gesichts- oder Iriserkennung, die allerdings aktuelle Hardware braucht.

DATENSCHUTZ IN UNTERNEHMEN
Acht IT-Sicherheitsregeln, die Chefs beachten sollten

Bild 1 von 11

Als Mittelstand uninteressant?

Hacker haben es doch nur auf die ganz großen Konzerne abgesehen? Das ist ein gefährlicher Irrglaube. Wenn Sie so oder so ähnlich argumentieren, sobald Sie auf die Sicherheit Ihrer hauseigenen IT-Systeme angesprochen werden, ist es um die Sicherheit in Ihrem Unternehmen möglicherweise nicht gut bestellt.
(Foto: Getty Images)

Aufgrund der Geschwindigkeit seien diese Verfahren nutzerfreundlich, urteilt IT-Sicherheitsexperte Thorsten Holz von der Ruhr-Universität Bochum. Allerdings gebe es ein grundsätzliches Problem: „Man kann dieses Passwort nicht ändern." Die Struktur des Fingerabdrucks oder der Iris bleibt ein Leben lang gleich. Wenn Hacker sich darauf Zugriff verschaffen, ist Biometrie nicht mehr sicher, betont der Professor für Systemsicherheit.

WIE DIE HACKER ZUM ZIEL KOMMEN

Eine einzige Schwachstelle reicht

Wenn kriminelle Angreifer in ein Computersystem eindringen wollen, haben sie einen Vorteil: Sie müssen womöglich nur eine einzige Schwachstelle finden, um einen Rechner zu kompromittieren. Einige ausgewählte Angriffsmethoden.

Verspätetes Update

Es gibt praktisch keine fehlerlose Software – wenn Sicherheitslücken entdeckt werden, sollte sie der Hersteller mit einem Update schließen. Viele Firmen lassen sich jedoch Zeit, diese zu installieren und öffnen Angreifern somit Tür und Tor.

Angriff auf die Neugier

Der Mensch ist neugierig - das machen sich kriminelle Hacker zunutze: Sie verfassen fingierte E-Mails, die wichtige Dokumente oder ein lustiges Video versprechen, aber nebenbei die Zugangsdaten eines Mitarbeiters stehlen. Phishing wird diese Methode genannt.

Gutgläubigkeit als Einfallstor

„Hier ist die IT-Abteilung. Wir brauchen mal Ihr Passwort": Nicht selten gelangen Angreifer mit einem dreisten Anruf an die Zugangsdaten eines Mitarbeiters. Wer gutgläubig ist, fällt auf diese Masche rein – obwohl die IT-Fachleute aus dem eigenen Haus nie so eine Frage stellen würden.

Ein Passwort, das nicht sicher ist

Ob Router oder Drucker: Viele Geräte werden mit einem Standardpasswort ausgeliefert. Wenn die IT-Abteilung es nicht verändert, haben Angreifer leichtes Spiel. „Die Handbücher mit dem Passwort stehen oft im Internet", sagt Joachim Müller, Chef für IT-Sicherheit beim Dienstleister Ceyoniq Consulting.

Ein schwaches Glied

Angreifer suchen das schwächste Glied in der Kette, häufig alte Systeme. Zudem kennen professionelle Angreifer – neben Kriminellen auch Geheimdienste – oft Sicherheitslücken, die den Herstellern der Software noch nicht bekannt sind. Gegen solche Zero-Day-Exploits kann man sich kaum schützen.

Dass die Sensoren sich überwinden lassen, haben Fachleute mehrfach demonstriert, unter anderem 2013 Hacker des Chaos Computer Clubs (CCC): Sie fotografierten einen Fingerabdruck von einer

Glasoberfläche ab und imitierten ihn mit Holzleim - das reichte, um das iPhone 5s zu überwinden. Dafür ist es noch nicht einmal nötig, das Glas selbst in die Hand zu bekommen, eine gängige Digitalkamera reicht dafür aus.

„Biometrie bedeutet mehr Bequemlichkeit, nicht mehr Sicherheit“, sagt Arno Wacker von der Uni Kassel. Trotzdem sei die biometrische Absicherung sinnvoll - als zusätzlicher Schutz. Denn zahlreiche Nutzer sperren ihr Smartphone überhaupt nicht. Sein Fazit: „Gegen den Gelegenheitsdieb hilft der Fingerabdrucksensor, gegen die NSA vermutlich nicht.“ Immerhin.

GEHACKTE WEBCAMS IN SHODAN
Das Internet der unsicheren Dinge

Eine Mischung aus verschiedenen Faktoren will Google einsetzen, um auf Geräten mit dem eigenen Betriebssystem Android Passwörter ganz zu ersetzen. Dazu zählen der Aufenthaltsort, Gesichtserkennung und typische Verhaltensweisen beim Tippen - daraus errechnet die Software einen Vertrauenswert. Biometrie kommt dabei also zum Einsatz, aber nicht allein. App-Entwickler sollen bis Jahresende auf die Trust API genannte Technologie zugreifen können.

@ckerkmann folgen