Antworten

Leser fragen, die Redaktion recherchiert

Großer Hackerangriff – Russischen Hackern ist es gelungen, über eine Milliarde Datensätze zu entwenden. Warum sie es auf Passwörter abgesehen haben, erklärt Andre Dolle (links). Philipp Engel hat sich mit der Cookie-Problematik beschäftigt.

Rosetta ist am Ziel – Die Kometenjägerin mit Braunschweiger Technik an Bord hat ihr Ziel erreicht. Der Komet „Chury". Cornelia Steiner ist Rosetta auf der Spur.

Das Wort „Password" steht zwischen Zeichen des Binärcodes auf einem Computerbildschirm. Der aktuelle Fall aus Russland mit über einer Milliarde gestohlener Datensätze lässt aufhorchen. Foto: dpa

Passwort-Diebstahl erschüttert das Netz

Der Fall aus Russland sprengt Grenzen. Auch Ermittler hierzulande haben es schwer, Cyberkriminelle zu fassen.

Unser Leser
Franz Albert
aus Wolfenbüttel fragt:

Ist es nicht endlich Zeit, die ausufernde Kriminalität im Internet wirksam zu bekämpfen?

Die Antwort recherchierte
Andre Dolle

Braunschweig. Die Dimensionen des jüngsten Datenklaus einer russischen Hackergruppe sind gigantisch: Nach Angaben der Sicherheitsfirma Hold Security wurden 1,2 Milliarden Login-Daten gestohlen. Die Frage unseres Lesers ist also berechtigt.

Matthias Möhring, Leiter der Zentralstelle Internet-Kriminalität beim LKA in Hannover, aber sagt: „Wir sind nicht hoffnungslos, was den Kampf gegen die Internetkriminalität angeht." Er fügt aber hinzu: „Wie bei jedem Delikt können wir nur reagieren, nicht agieren." Man könne eine Straftat nun mal nicht vorhersehen. Das gelte für sämtliche Delikte. Möhring führt ein Team von rund 20 Mitarbeitern. Es handelt sich um Spezialisten, die konkret zu bekannt gewordenen Straftaten ermitteln oder im Internet „auf Streife" unterwegs sind.

Liegen Hinweise auf Straftaten vor, versuchen die Beamten, die Kriminellen im Netz aus ihrer Anonymität zu holen, das heißt, Tatverdächtige zu identifizieren. Häufig ist dies mit Beschlüssen von Staatsanwälten verbunden, oft in Form von Rechtshilfeersuchen, die an das Ausland gerichtet werden. Die LKA-Spezialisten sichern auf Servern und Computern gelagerte Daten und analysieren diese, sie werten Hinweise auf E-Mail-Adressen oder genutzte Pseudonyme bei sozialen Netzwerken aus. Trotz der Arbeit seiner Abteilung und der Polizeibeamten im Land sagt Möhring: „Die Wahrscheinlichkeit, dass Unternehmen und Privatleute gehackt werden, die steigt."

> **„Die Wahrscheinlichkeit, dass Unternehmen und Privatleute gehackt werden, die steigt."**
>
> **Matthias Möhring,** Leiter der Zentralstelle Internet-Kriminalität beim LKA

Umso mehr komme es darauf an, dass sich jeder, der im Netz unterwegs ist, schützt. Das sagt Hans-Joachim Allgaier, Sprecher des Potsdamer Hasso-Plattner-Instituts für Softwaresystemtechnik (Tipps des Instituts siehe Text unten). Allgaier ist sicher: „Wer sämtliche Tipps umsetzt, ist gut geschützt." Es gelte das Grundprinzip: Je mehr Sicherheit der Nutzer will, umso unbequemer wird es für ihn. Denn Passwörter müssen regelmäßig geändert werden, sie müssen verschieden sein.

Für die Ermittler ist es schwer, Cyberkriminelle zu enttarnen. „Die operieren aus dem Dunkeln heraus, vernebeln, woher sie stammen, verschleiern ihre Identität, hinterlassen kaum Spuren", sagt Allgaier.

LKA-Spezialist Möhring sagt: „Viele Server, die die Kriminellen nutzen, liegen im Ausland. Oft arbeiten sie sogar mit mehreren Servern, um Spuren zu verwischen."

Gerade beim Phishing, dem Versuch, über gefälschte Webseiten oder E-Mails an persönliche Daten des Internet-Nutzers zu gelangen, steht das LKA vor einer großen Aufgabe. „Wir können in diesem Wettkampf nur hinterherlaufen", sagt Möhring. Phishing-Wellen reichen meist nur über wenige Tage. Danach sind die Antiviren-Programme aktualisiert.

Für Unmut sorgt im aktuellen Fall eine Ankündigung der US-Sicherheitsfirma Hold Security. Die Amerikaner versuchen nun, mit dem Hinweis auf den Mega-Hack aus Russland für die eigenen Dienste zu werben und Kasse zu machen. Für eine Jahresgebühr von 120 Dollar bietet das Unternehmen den Betreibern von Websites einen Test an, bei dem sie feststellen können, ob sie auch betroffen sind. Den Netz-Nutzern will Hold Security in den kommenden 60 Tagen einen „Identity Protection Service" anbieten. Wer eine Voranmeldung für den Abo-Dienst ausfüllt, soll auch erfahren, ob er persönlich von dem Datenklau betroffen ist.

Allgaier hält das für unredlich. „Internetsicherheit darf nicht kommerziellen Interessen unterworfen werden", sagt der HPI-Sprecher. „Das darf keine Frage des Geldbeutels sein."

Und Möhring vom LKA mutmaßt: „Das Unternehmen aus den USA hat offenbar großes wirtschaftliches Interesse an der Veröffentlichung des Datenklaus aus Russland." Er hält die Zahl von 1,2 Milliarden Datensätzen daher bewusst für übertrieben. „Da sind sicher auch veraltete Datensätze und doppelte Datensätze dabei", sagt Möhring.

Da der LKA-Experte es für unmöglich hält, jegliche Art von Internet-Kriminalität restlos zu verhindern, sagt er: „Der Clou wird künftig darin liegen, Anomalien zu erkennen und diesen mit Hilfe von Behörden und Unternehmen, die entsprechende Software anbieten, zu begegnen."

So schützen Sie persönliche Daten im Internet

Jeder kann durch sein eigenes Verhalten dazu beitragen, den Diebstahl von Daten zu verhindern.

Braunschweig. Wieder gibt es Schlagzeilen über den Diebstahl von Profildaten im Internet. Doch jeder kann dafür sorgen, dass seine Daten besser geschützt sind. Doch mit dem Passwortwechsel zum Beispiel ist es wie mit vielen guten Vorsätzen: In der Praxis setzt sich der innere Schweinehund durch. So wechseln die meisten Nutzer viel zu selten ihre Zugangsdaten für E-Mail-Konten, Online-Banking und Co. Und nicht selten nutzen sie ein und dasselbe Passwort für all diese Dienste. 60 Prozent wählen nach Zahlen des Hasso-Plattner-Instituts Potsdam (HPI) für ihre Konten zudem unsichere Passwörter. Das weltweit am meisten verbreitete Passwort lautet demnach „123456" – und ist in Sekunden zu knacken.

Werden Nutzer Opfer von Datendieben, kann der Schaden groß sein. Denn schlimmstenfalls haben die Diebe dann den Schlüssel zu sensiblen Daten von allen möglichen Konten. 100-prozentigen Schutz vor solchen Attacken gibt es nicht. Doch jeder Nutzer kann durch richtiges Verhalten im Netz sein persönliches Risiko verringern. Darauf sollten Sie achten:

1 Lange Passwörter: „Ein gutes Passwort sollte nicht zu kurz sein", sagt Prof. Christoph Meinel vom HPI. Mindestens acht, besser zwölf Zeichen sollte man wählen. Es gilt: Je länger, desto sicherer.

2 Unsinnige Passwörter: „Das Passwort sollte keine sinnvollen Worte enthalten", sagt Meinel. Diese können per Computer schnell ermittelt werden. Außerdem sollten Sonderzeichen und Zahlen enthalten sein. Auch Namen von Ehegatten, Kindern oder KFZ-Kennzeichen lassen sich leicht ermitteln.

3 Verschiedene Passwörter: Jedes Passwort sollte nach Möglichkeit nur für ein Nutzerkonto gebraucht werden. Auf keinen Fall sollten die Passwörter für das E-Mail-Konto und andere Dienste identisch sein. So erhalten Kriminelle durch das Knacken eines Kontos Zugriff auf alle weiteren mit dem selben Passwort.

4 Kennwörter wechseln: „Anwender, die sichergehen wollen, sollten ihr Passwort ändern. Und generell sollten sie das regelmäßig tun", rät Thorsten Urbanski vom Sicherheitsdienstleister GData. Der IT-Verband Bitkom rät, ein Passwort spätestens nach drei Monaten zu ändern. Sollten Profildaten schon gestohlen worden sein, wird der Datensatz für Kriminelle durch einen Passwortwechsel unbrauchbar.

5 Passwort-Manager: Lange und komplizierte Passwörter sind schwer zu merken. Christoph Meinel empfiehlt den Einsatz von Passwort-Managern. Diese speichern verschiedene Passwörter zentral auf dem Computer, so dass man sich nur noch ein Master-Passwort merken muss.

> **„Das Passwort sollte keine sinnvollen Worte enthalten."**
>
> **Christoph Meinel,** Professor am Hasso-Plattner-Institut

6 Weitere Sicherungsverfahren: Einige Dienste wie Online-Banking, soziale Netzwerke oder Online-Shops bieten die sogenannte Zwei-Schritte-Authentifizierung an. Dabei wird zusätzlich zum Passwort beispielsweise noch ein Code auf das Mobiltelefon gesandt, der abgefragt wird. „Das bietet eine erhöhte Sicherheit, sobald Sie zwei Geräte verwenden", sagt Christoph Meinel. Um alle Informationen abzugreifen, müssten Hacker beide Geräte überwachen. Wer sein Online-Banking per Smartphone erledigt und auf dem gleichen Gerät seine Tan-Nummern empfängt, ist nicht unbedingt sicherer. „Da hat es schon Angriffe gegeben", sagt Meinel.

7 Sparsam mit Daten sein: „Man sollte überlegen, ob man Daten wirklich abgeben will", rät Meinel. Nutzer sollten sich immer die Frage stellen, ob sie einen Dienst wirklich brauchen. Je mehr Konten man eröffne, umso höher sei die Chance, dass eines geknackt werde.

8 Selber prüfen: Ob die eigenen Daten schon im Netz kursieren, kann zum Beispiel ein kostenloser Test des HPI zeigen. Das Institut forscht fortlaufend nach gestohlenen Nutzerdaten. Wer auf der HPI-Webseite seine E-Mail-Adresse eingibt, erfährt, ob die eigenen Daten an einschlägigen Stellen im Web kursieren. *dpa*

Cookies löschen reicht nicht mehr

Neue Technologien sammeln Daten im Netz.

Von Philipp Engel

Braunschweig. Mit einer neuen Methode sammeln Firmen im Internet Daten der Nutzer. Das Ziel: Profile mit Informationen über das Surfverhalten sollten personalisierte Werbung ermöglichen.

Das funktionierte bislang über Cookies: kleine Programme, die von Webseiten lokal auf dem Computer gespeichert werden. Über sie wurde nachvollziehbar, welche Inhalte auf welchen Seiten ein einzelner Nutzer interessant fand. Viele Nutzer löschen aus diesem Grund regelmäßig die Cookies oder lassen sie erst gar nicht zu.

Nutzer haben keine Kontrolle mehr

Eine neue Methode verfolgt das gleiche Ziel, geht dabei aber anders vor – und entzieht sich weitgehend der Kontrolle durch den Nutzer. Auf tausenden beliebten Webseiten findet sich die Technologie namens „Canvas Fingerprinting", wie Forscher aus Belgien und den USA feststellten.

„Im Gegensatz zu klassischen Cookies werden dabei keine Daten beim Benutzer gespeichert, sondern das Verhalten des Browsers beim Anzeigen der Webseite analysiert", erklärt Steffen Arntz vom Computerverein „Stratum 0 e.V." in Braunschweig. „Da jeder Computer und Browser ein bisschen anders konfiguriert ist, etwa bei Schriftarten, Bildschirm- oder Fenster-Größen, ergeben sich Unterschiede, durch die ein Nutzer identifiziert werden kann."

Das „Canvassing" ist unsichtbar. Weil die Informationen nicht auf dem heimischen Computer gespeichert werden, sondern auf fremden Servern, kann der Benutzer sie auch nicht mehr löschen.

Wer sich schützen will, muss auf Funktionen verzichten

Doch es gibt Möglichkeiten, sich zu schützen, sagen die Experten. Das ist allerdings meist mit Einschränkungen beim Surfen verbunden. Arvid Grimm von „Stratum 0" rät, schon den Verbindungsaufbau zu einem Canvassing-Dienstleister zu unterbinden, damit er seine Techniken gar nicht erst in Aktion bringen kann. Dabei hilft etwa ein Browser-Addon, wie AdBlock. Ebenfalls als Zusatzprogramm für den Browser kommt „NoScript" infrage, ein Programm, das nur auf bestimmten Seiten die Ausführung von Java-Scripten erlaubt. Nachteil: Auf Seiten, wo es nicht erlaubt ist, funktionieren einige Angebote womöglich nicht mehr.

„Das ist sehr ärgerlich", sagt Grimm. Denn gerade unversierte Nutzer müssten entscheiden: Lasse ich mich tracken oder verzichte ich komplett auf bestimmte Webdienste? Doch es gibt Hoffnung: „Die Community, die hinter den bisherigen Browser-AddOns steht, macht sich seit dem flächendeckenden Einsatz der eigentlich nicht ganz neuen Techniken immer mehr Gedanken über deren Abwehr."