Schutz vor Identitätsklau im Internet

16 Millionen gestohlene Zugangsdaten haben Internetnutzer kürzlich aufgeschreckt. Ein Experte gibt Tipps, wie man sich vor solchen kriminellen Attacken schützen kann.

Diebstähle mit enormem Schadenpotenzial

Mitte Januar gab das Bundesamt für Sicherheit in der Informationstechnik (BSI) bekannt, es seien Millionen gekaperter Zugangsdaten zu Online-Konten entdeckt worden.

Zwar ist unklar, was die Kriminellen vorhatten, doch der potenzielle Schaden ist riesig: Wer die Möglichkeit hat, sich in ein fremdes E-Mail-, Shopping- oder Online-Bankkonto einzuloggen, kann auch unkontrolliert darüber verfügen. Betroffene bemerken einen Identitätsdiebstahl oft erst im Nachhinein, etwa wenn ihr Konto leergeräumt oder Waren auf ihre Kosten eingekauft wurden.

Wie können Passwörter und Zugangsdaten überhaupt in fremde Hände gelangen, wie beugt man Identitätsklau am besten vor und was tut man im Schadenfall? Tim Griese, Pressesprecher des BSI, erklärt es.

Experten-Interview I: Wie funktioniert Identitätsklau?

Tim Griese, Pressesprecher des Bundesamts für Sicherheit in der Informationstechnologie (BSI)

Welche Methoden nutzen Kriminelle häufig, um sich persönliche Zugangsdaten von Verbrauchern zu beschaffen?

Im zuletzt bekannt gewordenen Fall der Millionen geraubten Datensätze haben die Täter vermutlich unter anderem auch Schadsoftware eingesetzt. Sie infiziert den Rechner des Nutzers und kann dann alle Tastatureingaben „mitlesen" kann. Wenn der Nutzer sich in seine verschiedenen Online-Accounts einloggt, dann werden auch die Login-Daten (Username und

Passwort) mitgelesen und können von den Online-Kriminellen missbräuchlich genutzt werden.

Eine weitere Methode ist das Phishing. Hierbei wird der Nutzer beispielsweise über einen Link in einer E-Mail auf eine gefälschte Webseite gelockt, die der Webseite bekannter Online-Dienste, Online-Banking-Angebote oder Sozialer Netzwerke täuschend ähnlich sieht.

Wenn dies dem Nutzer nicht auffällt und er versucht, sich dort in seinen vorgeblichen Account einzuloggen, können die Betrüger Nutzername und Passwort abfischen. Damit haben sie den vollen Zugriff auf den Account, können Daten einsehen und ändern, E-Mails verschicken oder im Namen und auf Rechnung des Opfers einkaufen.

Experten-Interview II: Tipps, um Angriffe abzuwehren

Wie kann man sich gegen Identitätsdiebstahl wappnen?

Griese: Neben dem Einsatz eines Virenscanners und einer Firewall ist es wichtig, seinen Rechner sicherheitstechnisch auf dem neuesten Stand zu halten, also Sicherheitsupdates für Betriebssystem, Browser und andere eingesetzte Software rasch einzuspielen. Damit erschwert man das Eindringen einer Schadsoftware. Zudem sollte man für jeden genutzten Online-Dienst (z. B. E-Mail, Online-Banking, Online- Shopping, Soziale Netzwerke) ein separates, möglichst starkes Passwort wählen. Was man dabei beachten sollte, ist nachzulesen bei **„BSI für Bürger".**

Außerdem sollte man vor der Eingabe der Zugangsdaten kontrollieren, ob man sich tatsächlich auf der korrekten Webseite des Online-Angebots befindet, für das man sich anmelden will. Die Webadresse des Angebotes sollte daher stets direkt in den Browser eingegeben oder per angelegtem Lesezeichen aufgerufen werden. Links auf den Online-Dienst, die auf anderen Webseiten gesetzt sind, sollte man nicht folgen, denn diese können unter Umständen auf gefälschte oder manipulierte Webseiten führen.

Auch bei Links, die man in persönlichen Nachrichten in Sozialen Netzwerken oder in E-Mails bekommt, sollte man vorsichtig sein, denn auch dahinter können sich manipulierte Webseiten verstecken. Diese dienen Online-Kriminellen lediglich dazu, die Nutzerdaten zu erhalten und damit den Account und die digitale Identität des Anwenders zu übernehmen.

Experten-Interview III: Verhalten im Schadenfall

Was ist zu tun, wenn die eigenen Zugangsdaten missbraucht wurden?

Griese: Wenn man den Verdacht hat, dass sich jemand in das Online-Konto eingeloggt hat, sollte man sofort das Passwort ändern. Ist auch das

Einloggen selbst nicht mehr möglich, kann man die "Passwort-vergessen-Funktion" nutzen. Der Betreiber des Online-Dienstes sendet dann in der Regel eine E-Mail, die es dem Anwender ermöglicht, das Passwort neu zu setzen und damit das Konto wieder zu übernehmen.

Sollte dieser Weg nicht funktionieren, ist es ratsam, sich umgehend mit dem Kundensupport des Plattformbetreibers in Verbindung setzen. Die entsprechenden Kontaktstellen hat das BSI **hier** aufgelistet.

Noch vor der Passwortänderung ist es unbedingt notwendig, den Rechner mithilfe eines geeigneten Virenprogramms auf Schadsoftware zu überprüfen. Wird eine solche festgestellt, sollte sie entfernt werden. Auch dies übernimmt normalerweise die Antivirensoftware. In manchen Fällen kann es aber auch notwendig sein, den Rechner neu aufzusetzen. Mehr Informationen hierzu gibt das BSI **hier**.

Erstattung des Schadens bei abgeräumtem Konto

Wer Online-Banking betreibt, ist verpflichtet, seine Zugangsdaten, PINs und TANs zu schützen und seine Bank unverzüglich zu informieren, wenn er den Verdacht hat, dass Dritte diese Daten missbrauchen könnten (BGB § 675l). Ob und in welchem Umfang die Bank einen finanziellen Schaden z. B. durch Phishing ersetzt, hängt vom Einzelfall ab. Muss sich der Kunden grobe Fahrlässigkeit vorwerfen lassen, haftet er selbst (BGB § 675v).

Strafanzeige und Schadenersatz

Grundsätzlich kann ein Betrugsopfer bei der Polizei Strafanzeige gegen unbekannt erstatten. Ist der Täter ermittelt und verurteilt, gibt es die Möglichkeit, ihn auf Schadenersatz zu verklagen. Allerdings sollte man sich anwaltlich beraten lassen, ob das im speziellen Fall sinnvoll und aussichtsreich ist. Der Allianz Privat- und Berufs-Rechtsschutz übernimmt die Kosten für die anwaltliche Beratung und Vertretung sowie etwaige Gerichtskosten.

Quelle: Allianz Newsletter 02/2014