Neue Art der Passwörter: Bestätigung in 2 Schritten

Haben Sie schon einmal von der *Bestätigung in zwei Schritten*, *Zwei-Faktor-Authentifizierung*, *Zwei-Schritt-Verifizierung* oder *Prüfung in zwei Schritten* gehört?
Diese Begriffe stehen allesamt für ein neues Verfahren rund um Passwörter. Für eben dieses Verfahren gibt es leider keinen einheitlichen Namen. In allen Fällen ist aber das gleiche technische Verfahren gemeint. Es geht dabei um eine zusätzliche (**zweite**) Sicherheitsstufe für verschiedene Internetdienste, bei denen Sie ein Nutzerkonto und Zugangsdaten haben. Diese Sicherheitsstufe wird verwendet, wenn man sich bei einem solchen Dienst anmelden oder beispielsweise die Zugangsdaten ändern möchte. Das Verfahren wird von immer mehr Internetseiten angewendet und wird daher immer wichtiger. Doch wie genau funktioniert es?

Genügt ein Passwort nicht?

Normalerweise haben Sie zum Anmelden für eine Internetseite ein Passwort. Dieses Passwort ist der erste Schritt zur Anmeldung. Das Problem mit Passwörtern ist: Sie können von anderen Personen erraten, gestohlen oder geknackt werden. Gelangt ein Fremder an Ihr Passwort, so könnte er beispielsweise Ihre E-Mails lesen, in Ihrem Namen im Internet einkaufen, auf Ihre Dateien zugreifen oder Ähnliches – abhängig davon, welches Passwort ergaunert wurde. Der Kriminelle könnte sogar Ihr Passwort ändern, sodass Sie das Passwort nicht mehr wissen, er aber!

Die zweite Stufe der Anmeldung

Um das zu verhindern, gehen immer mehr Anbieter von Internetdiensten dazu über, noch einen zweiten Schritt zur Bestätigung hinzuzufügen. Dieser zweite Schritt erfolgt in der Regel über einen Bestätigungscode, den Sie auf ein vertrauenswürdiges Gerät zugesendet bekommen. So wird gewährleistet, dass wirklich nur Sie sich anmelden oder Änderungen an Ihren Zugangsdaten vornehmen können.
Die Bestätigung in zwei Schritten funktioniert also:
1) über etwas, das Sie **kennen** (Ihr Passwort)
2) über etwas, das Sie **besitzen** (Ihr Gerät)
Als Gerät für den zweiten Schritt wird meistens das Smartphone, manchmal der Computer oder das Tablet verwendet. Meist kommt der Bestätigungscode als SMS oder Benachrichtigung. Andere Varianten sind ein Anruf an Ihre Handynummer, bei der ein Bestätigungscode durchgegeben wird oder eine E-Mail mit dem Bestätigungscode an eine vertrauenswürdige Mail-Adresse, die Sie zuvor hinterlegt haben. Manchmal gibt es sogar eine spezielle, zusätzliche App, in der ein Bestätigungscode generiert und angezeigt wird.

Warum bietet das so einen starken Schutz?

Selbst wenn jemand Ihr Passwort für einen solchen Internetdienst herausfinden sollte, so kann diese Person sich trotzdem nicht anmelden, da der Bestätigungscode nur an Sie gesendet wird. Außerdem wären Sie im Angriffsfall gewarnt, wenn jemand versucht, sich in Ihrem Namen anzumelden, da Sie unvermittelt einen Bestätigungscode erhalten, ohne dass Sie sich gerade irgendwo anmelden wollten. Viele Anbieter erkennen sogar, wenn eine Anmeldung plötzlich von einem anderen Gerät oder von einem anderen Ort als üblich erfolgt, und fragen dann zur Sicherheit den Bestätigungscode ab. Wahrscheinlich kennen Sie das Vorgehen so ähnlich auch vom Online-Banking. Möchte man online eine Überweisung tätigen, so muss man sich zunächst mit Passwort anmelden. Beim Ausführen der Überweisung wird dann zusätzlich eine TAN generiert, die man beispielsweise mit einem TAN-Generator entschlüsseln kann oder die man per SMS erhält. Auch hier wird das

zweistufige Verfahren angewendet. Selbst wenn jemand Ihr Passwort für das Online-Banking herausfinden sollte, so kann er keine Überweisung durchführen, weil nur Sie die TAN dafür erhalten, auf einem zweiten Gerät. Bei manchen Banken wird die TAN sogar schon beim ersten Anmelden verlangt und dann noch einmal, wenn man eine Überweisung durchführen möchte. So wird jede Aktion einzeln durch eine zusätzliche Bestätigung geschützt.
Immer mehr große Internetfirmen führen dieses zweistufige Verfahren ein, um die Daten der Kunden besser zu schützen. Bei fast allen Anbietern ist es allerdings (noch) so, dass Sie freiwillig entscheiden können, ob Sie das zweistufige Verfahren verwenden möchten oder nicht. Denn es bietet zwar mehr Schutz, ist aber natürlich auch etwas aufwändiger anzuwenden. Und es kann auch Nachteile haben, nämlich dass Sie sich selbst aussperren.

Vorsicht beim zweistufigen Verfahren
Wenn Sie sich aktiv und freiwillig für das Verfahren zur zweistufigen Anmeldung bei einem Anbieter entscheiden, so müssen Sie sich ganz genau merken, welche Telefonnummer oder welche E-Mail-Adresse Sie zur Anmeldung hinterlegen. Denn wenn Sie diese vergessen oder keinen Zugriff mehr darauf haben, so kann es passieren, dass Sie sich selbst nicht mehr anmelden können. Bei manchen Diensten ist es aus diesem Grund sogar möglich, zur Sicherheit mehrere Nummern oder Adressen zu hinterlegen.

Wer bietet das Verfahren schon an?
Die größten und bekanntesten Internetfirmen bieten die zweistufige Anmeldung alle schon an, jedoch mit unterschiedlichen Namen:
Google: Bestätigung in zwei Schritten
Apple: Zwei-Faktor-Authentifizierung
Microsoft: Prüfung in zwei Schritten
Amazon: Zwei-Schritt-Verifizierung
Facebook: Zweistufige Authentifizierung
Dropbox: Zweistufige Überprüfung
Die zweistufige Anmeldung kann in den Einstellungen des jeweiligen Anbieters aktiviert werden. Bei manchen Anbietern wird der Bestätigungscode bei jeder Anmeldung abgefragt, bei anderen nur von Zeit zu Zeit, oder wenn plötzlich ein Anmeldeversuch von einem neuen Gerät oder von einem anderen Ort aus erfolgt. Außerdem wird der Code in der Regel abgefragt, wenn man Änderungen an den persönlichen Daten vornehmen möchte, zum Beispiel beim Passwort oder Zahlungsinformationen.
Hier geht's zu unserem Kurs "Passwörter":

Passwörter und Passwortmanager

Typisches Praxisbeispiel
Sie alle kennen die Apple-ID und das Google-Konto. (Falls nicht, stöbern Sie mal in unserem Newsletter-Archiv. Dort gibt es einige Beiträge zu Apple-ID und Google-Konto) Das sind die beiden wichtigen "Mitgliederausweise" der beiden Smartphone-Welten von Apple und Google, die am iPhone bzw. bei Android quasi Pflicht sind. Hier sind sehr wichtige Daten hinterlegt und sie müssen besonders gut geschützt werden. Wenn man nun sein eigenes Passwort bei Apple-ID bzw. Google-Konto ändern will, dann kann man nicht einfach so ein neues Passwort eintippen. Sondern man erhält wie oben beschrieben parallel einen Bestätigungscode auf das Handy gesendet. Diesen Bestätigungscode muss man zusätzlich zum neuen Passwort eintippen, nur so kann die Passwortänderung vollzogen werden.

Quelle: https://levato.de/neue-art-der-passwoerter-bestaetigung-in-2-schritten/