SANS SECURITY AWARENESS

OUCH! | Dezember 2017

Der monatliche Security Awareness Newsletter für Jedermann

OUCH!

IN DIESER AUSGABE...

- Passwörter
- Was ist 2-Faktor-Authentisierung
- Funktionsweise

Schutz Ihrer Anmeldeinformationen

Überblick

Gastautor
Tiffany Schoenike ist Leiterin der Kampagnen und Initiativen der National Cyber Security Alliance (**@staysafeonline**). 2016 arbeitete sie mit dem Weissen Haus, der US Regierung und der Industrie an der Entwicklung der Lock Down Your Login Kampagne aus der STOP. THINK. CONNECT.™ Reihe über 2-Faktor-Authentisierung.

Der Prozess der Authentifizierung, d.h. das Nachweisen Ihrer Identität, ist der Schlüssel zum Schutz Ihrer Daten, beispielsweise Ihrer E-Mails, Ihrer Konten in Sozialen Medien oder natürlich Ihrer Bankkonten. Vielleicht wussten Sie noch nicht, dass man drei Arten der Authentifizierung unterscheidet: Etwas, das Sie wissen – wie z.B. Ihr Passwort; etwas, das Sie besitzen – wie z.B. Ihr Führerschein; und Teile Ihrer Identität – wie z.B. ein Fingerabdruck. Jede dieser Methoden hat Vor- und Nachteile. Die gängigste Authentifizierungsmethode sind Passwörter – also etwas, das Sie wissen. Leider stellt sich die alleinige Nutzung von Passwörtern immer mehr als unzureichend heraus. In diesem Newsletter bringen wir Ihnen bei, wie Sie sich schützen können und Ihre Benutzerkonten mit etwas weit Besserem als Passwörtern absichern, mit der sogenannten 2-Faktor-Authentisierung.

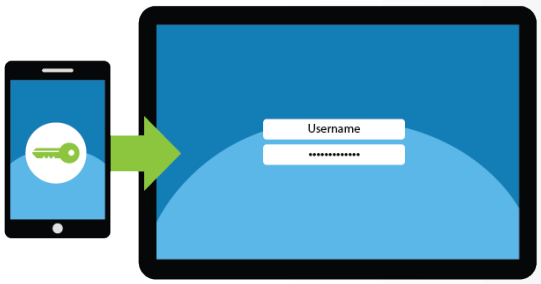
Passwörter reichen nicht mehr aus

Passwörter dienen zum Nachweis Ihrer Identität basierend darauf, dass Sie etwas Bestimmtes wissen. Wenn aber jemand Ihr Passwort erraten oder seiner anders habhaft werden kann, kann er sich für Sie ausgeben und auf all Ihre Daten zugreifen. Kompromittierte Passwörter sind eine der häufigsten Ursachen für gehackte Benutzerkonten. Daher sollten Sie am besten Passwortsätze verwenden die für andere schwer zu erraten sind, für jedes Benutzerkonto ein anderes Passwort wählen und Passwörter nie an andere weitergeben. Diese Tipps haben immer noch ihre Gültigkeit, dennoch sind Passwörter nicht mehr ausreichend sicher. Glücklicherweise gibt es eine einfache und schnell anwendbare Möglichkeit, Ihnen die alleinige Kontrolle über Ihre Daten wieder zu sichern – die 2-Faktor-Authentisierung.

Schutz Ihrer Anmeldeinformationen

Was ist 2-Faktor-Authentisierung?

2-Faktor-Authentisierung (auch 2-Wege-Überprüfung, Mehr-Faktor-Anmeldung oder kurz 2FA genannt) ist viel sicherer als die alleinige Nutzung von Passwörtern. Hierbei wird nicht nur eine Methode zum Nachweis Ihrer Identität gefordert, sondern zwei verschiedene Methoden. Ein gängiges Beispiel ist Ihre Bankkarte. Wenn Sie damit Geld am Automaten abheben, benutzen Sie bereits 2-Faktor-Authentisierung. Sie benötigen zum Abheben 2 Dinge: Ihre Bankkarte (etwas das Sie besitzen), und die passende PIN (etwas das Sie wissen). Wenn Ihre Bankkarte verloren geht oder gestohlen wird, können Dritte damit kein Geld abheben, ohne Ihre PIN zu kennen. Ein Dieb muss über Karte und PIN verfügen um die Karte zu nutzen. 2-Faktor-Authentisierung nutzt genau dieses Konzept.



Sichern Sie Ihre Anmeldung durch die Nutzung von 2-Faktor-Authentisierung ab wann immer das möglich ist, denn dies ist eine der stärksten Methoden für Ihren eigenen Schutz im Internet.

Funktionsweise

2-Faktor-Authentisierung ist weit verbreitet, die meisten Banken, E-Mail-Anbieter, Sozialen Netzwerke und viele andere Seiten bieten es an. Viele dieser Seiten bieten darüber hinaus leicht verständliche Schritt-für-Schritt Anleitungen zum Aktivieren der 2-Faktor-Authentisierung (weitere Details finden Sie unter Weiterführende Informationen am Ende des Newsletters). Wenn Sie 2-Faktor-Authentisierung aktivieren, erfolgt eine Anmeldung von nun an ungefähr wie folgt: Zunächst melden Sie sich an Ihrem Online-Benutzerkonto wie gewohnt mit Benutzername und Passwort an. Das ist der erste der 2 Faktoren – etwas das Sie wissen. Danach erhalten Sie einen Einmalcode, oft per SMS auf Ihr Mobiltelefon. Diesen Code geben Sie nun in die Anmeldemaske ein. Das ist der zweite der beiden Faktoren – Sie müssen etwas (Ihr Telefon) besitzen um den Code zu erhalten. Nun ist Ihr Benutzerkonto wirklich geschützt. Selbst wenn Cyberkriminelle Ihr Passwort stehlen, können sie nicht an Ihr Benutzerkonto, solange sie nicht auch Ihr Telefon haben.

Schutz Ihrer Anmeldeinformationen

Statt den Code per SMS zu erhalten, können Sie auch eine spezielle Authentisierungs-App auf Ihrem Smartphone installieren. Diese App generiert einen einzigartigen Code für jeden Ihrer Anmeldevorgänge. Der Vorteil davon ist eine noch höhere Sicherheit, da der Code direkt auf dem Smartphone erzeugt und nicht noch per SMS übertragen werden muss. Außerdem brauchen Sie keine Verbindung zum Mobilfunknetz um den Code zu erhalten. Die App erzeugt kontinuierlich neue, zeitlich begrenzt gültige Codes für Ihre Online-Anmeldungen.

Anfangs mag 2-Faktor-Anmeldung nach mehr Aufwand aussehen, doch der Schutz Ihrer Daten ist dadurch deutlich höher! Warten Sie nicht, bis Ihre Accounts gehackt werden, schützen Sie Ihre Anmeldung durch das Aktivieren der 2-Faktor-Authentisierung bei wichtigen Benutzerkonten wie E-Mail, Onlinebanking und Sozialen Netzwerken, und entspannen Sie sich in dem Wissen, dass Sie nun deutlich sicherer sind.

Weiterführende Informationen

Passphrasen:	https://securingthehuman.sans.org/ouch/2017#april2017
Webseiten mit 2-Faktor-Authentisierung:	https://twofactorauth.org
Stop|Think|Connect:	https://www.lockdownyourlogin.org
Google 2step:	http://www.google.com/landing/2step/

Informieren Sie Sich

Abonnieren Sie den monatlichen OUCH! Security Awareness Newsletter, greifen Sie auf die OUCH! Archive zu und lernen Sie mehr über SANS Security Awareness Angebote unter securingthehuman.sans.org/ouch/archives.

Deutsche Ausgabe

Diese OUCH! Ausgabe wurde von Marek Kreul und René Wiedewilt aus dem Englischen übersetzt. Beide arbeiten für das CERT eines DAX-Konzerns und haben sich auf IT-Forensik spezialisiert. Sie haben langjährige Erfahrung im Bereich IT-Sicherheit und sind mehrfach GIAC zertifiziert.

Redaktionsleitung: Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley