Der monatliche Security Awareness Newsletter für Computeranwender

OUCH!

IN DIESER AUSGABE...

Zwei-Faktor-Authentifizierung

Überblick

Der Prozess zum Nachweis Ihrer Identität, Authentifizierung genannt, ist der Schlüssel zum Schutz Ihrer Daten. Mit einer starken Authentifizierung können sie sicherstellen, dass nur Sie Zugang zu Ihren Daten erhalten, z.B. zu Ihren E-Mails, Ihren Fotos oder Ihren Bankkonten. Es gibt drei verschiedene Wege um Ihre Identität nachzuweisen. Wissen (z.B. Passwörter), Besitz (z.B. Ihre Fahrerlaubnis) und körperliche Merkmale bzw. Biometrie (z.B. Ihre Fingerabrücke). Jede dieser Methoden hat ihre Vor- und Nachteile. Am verbreitetsten ist der Einsatz von Passwörtern, also Wissen. In diesem Newsletter wollen wir Ihnen die Methode Zwei-Faktor-Authentifizierung näher bringen, welche weit sicherer als die alleinige Nutzung von Passwörtern und darüber hinaus einfach anzuwenden ist. Um die Zwei-Faktor-Authentifizierung besser zu verstehen, müssen wir uns zuerst mit dem Thema Passwörter beschäftigen.

Gastautor

Keith Palmgren hat mehr als 30 Jahre Erfahrung im Bereich Informationssicherheit. Er ist SANS-zertifizierter Trainer und Autor von SANS SEC301, einem fünftägigen Einführungskurs in Informationssicherheit. Wenn er nicht unterrichtet, ist er vorwiegend in den Bereichen Beratung und Projektarbeit tätig. Sie können Keith unter **@kpalmgren** folgen.

Passwörter

Basierend auf der Methode Wissen können Passwörter Ihre Identität beweisen. Passwörter haben jedoch einen gravierenden Schwachpunkt: wenn sie jemand errät oder Zugang zu ihnen erlangt, kann derjenige Ihre Identität annehmen und hat Zugang zu all Ihren Daten, die Sie zuvor mit den Passwörtern gesichert haben. Aus diesem Grund wollen wir Ihnen Wege nahelegen um Ihr Passwort zu schützen. Da wären zum Einen die Nutzung starker, schwer zu erratender Passwörter, des Weiteren die Nutzung unterschiedlicher Passwörter je Account und nicht zuletzt eigene Passwörter mit niemandem zu teilen. Diese Tipps gelten natürlich weiterhin, dennoch haben Passwörter den Zenit ihrer Nützlichkeit überschritten; sie sind in der heutigen Zeit nicht länger effektiv. Durch die neuesten technischen Fortschritte wurde es für Cyberangreifer viel zu leicht Passwörter zu kompromittieren. Wir benötigen daher eine einfach benutzbare, aber sicherere Lösung für starke Authentisierung. Glücklicherweise ist eine solche Lösung bereits verfügbar, in Form der so genannten Zwei-Faktor-Authentifizierung.

Zwei-Faktor-Authentifizierung

Die Zwei-Faktor-Authentifizierung (manchmal auch Zwei-Wege-Anmeldung genannt oder 2FA abgekürzt) ist eine sicherere Anmeldelösung als Passwörter. Sie basiert auf der Nutzung nicht einer, sondern zweier Methoden, um sich zu authentifizieren.

Zwei-Faktor-Authentifizierung

Ein Beispiel ist Ihre EC-Karte. Wenn Sie Geld an einem Geldautomaten abheben wollen, nutzen Sie bereits eine Art der Zwei-Faktor-Authentifizierung. Sie benötigen dafür zwei Dinge, Ihre EC-Karte (Besitz) und die passende PIN (Wissen). Wenn Sie Ihre EC-Karte verlieren ist Ihr Geld noch immer sicher, denn ein Finder kann nicht einfach Geld abheben ohne die PIN zu kennen (solange Sie sie nicht auf Ihre Karte geschrieben haben, was verständlicherweise eine ganz schlechte Idee ist). Gleiches gilt, wenn jemand nur an Ihre PIN gelangt ist, nicht jedoch an Ihre EC-Karte. Ein Angreifer muss über beides verfügen, um Zugriff auf Ihr Konto zu erlangen. Diese Nutzung von zwei Sicherheitsfaktoren macht die Zwei-Wege-Authentifizierung so viel sicherer.

Nutzen Sie Zwei-Faktor-Authentifizierung wann immer sie verfügbar ist. Es ist einer der wichtigsten Schritte zum Schutz Ihrer Informationen.

Nutzung von Zwei-Faktor-Authentifizierung

Zwei-Faktor-Authentifizierung müssen Sie für jedes Ihrer Nutzerkonten separat aktivieren. Viele Onlinedienste unterstützen heutzutage diesen Mechanismus, wobei Google hier eine Vorreiterrolle einnimmt. Google Konten sind ein bevorzugtes Ziel für Cyberangreifer, da Google eine Vielzahl kostenloser Onlinedienste für Millionen Menschen weltweit anbietet. Google sah sich daher gezwungen, stärkere Authentifizierungsformen anzubieten und war eine der ersten Organisationen, die eine Zwei-Faktor-Authentifizierung für den Großteil seiner Dienste verfügbar machte. Wenn Sie verstehen wie Google's Zwei-Faktor-Authentifizierung funktioniert, kennen Sie auch die Funktionsweise bei anderen Diensten wie Twitter, Facebook, Apple, Instagram und die vieler Banken.

Zunächst müssen Sie die Zwei-Faktor-Authentifizierung in Ihrem Google Konto aktivieren und Ihre Handynummer hinterlegen. Sobald das abgeschlossen ist, funktioniert der Prozess wie folgt: Sie melden sich an Ihrem Konto wie gewohnt mit Nutzername und Passwort an. Das ist der erste der beiden Faktoren - etwas das Sie wissen. Google schickt Ihnen anschließend eine Nachricht auf Ihr Mobiltelefon, die einen einzigartigen, sechsstelligen Code enthält. Genau wie Ihr Passwort geben Sie diesen Code auf der Google Seite ein. Das ist der zweite der beiden Faktoren, erlangt durch etwas das Sie besitzen (Ihr Mobiltelefon). Um sich an Ihrem Benutzerkonto anzumelden, müssen Sie also sowohl das Passwort kennen als auch Zugriff auf Ihr Mobiltelefon zum Empfang des Einmalcodes haben. Selbst wenn ein Angreifer Ihr Passwort kennt, kann er nicht auf Ihr Google Benutzerkonto zugreifen, wenn er nicht zugleich auch an Ihr Mobiltelefon kommt. Um zu gewährleisten, dass Ihr Benutzerkonto wirklich sicher ist, schickt Ihnen Google bei jedem Loginvorgang einen neuen Einmalcode.

Zwei-Faktor-Authentifizierung

Bei Google und vielen anderen Diensten gibt es eine weitere Möglichkeit zur Zwei-Faktor-Authentifizierung. Anstelle von Einmalcodes, die per SMS übermittelt werden, können Sie eine Authentifizierungs-App auf Ihrem Smartphone installieren. Die App generiert ständig neue Einmalcodes, die Sie für die Anmeldung benutzen müssen. Der Vorteil liegt darin, dass Sie keinen Mobilfunkempfang benötigen, da das Smartphone die Codes selbst generiert. Der Code kann, da er auf dem Gerät selbst generiert wird, auch nicht im Netzwerk abgefangen werden.

Denken Sie daran, dass Zwei-Faktor-Authentifizierung nicht standardmäßig aktiviert ist, Sie müssen sie immer selbst aktivieren. Auch wenn es anfangs nach einem Mehraufwand aussehen mag, raten wir dringend zur Nutzung dieser Authentifizierungsform wenn immer es möglich ist, insbesondere für kritische Dienste wie Ihren E-Mail Account, Onlinebanking oder Dateiablagen wie Dropbox. Zwei-Faktor-Authentifizierung bietet einfach einen signifikant besseren Schutz für Ihre Informationen, als die alleinige Nutzung von Passwörtern.

Weiterführende Informationen

Passwörter:	http://www.securingthehuman.org/ouch/2015#april2015
Dienste mit Zwei-Faktor-Authentifizierung (engl.):	https://twofactorauth.org
Google Zwei-Faktor-Authentifizierung:	http://www.google.com/landing/2step/
SANS Sicherheitstipp des Tages:	http://www.sans.org/tip_of_the_day.php

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 http://www.securingthehuman.org.

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: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis