

So erstellen Sie ein sicheres Passwort

Damit sich eine Person gegenüber Diensten, wie zum Beispiel dem Online-Banking, als diejenige ausgeben kann, die sie wirklich ist, ist der Nachweis einer Identität erforderlich. Man spricht in diesem Falle von der so genannten Authentifizierung. Häufig authentifiziert sich eine Person bei Online-Diensten mit Benutzernamen und Passwort. Dabei entspricht der Benutzername nicht immer den gleichen Regeln (mal ist es die Kontonummer, ein fiktiver Name oder auch die E-Mailadresse), kann jedoch meist schnell von Dritten erraten oder herausgefunden werden. Doch alle Dienste haben eines gemeinsam. Zum Nachweis der Identität reicht nicht die Angabe des Benutzernamens aus. Nur wenn dieser mit dem richtigen Passwort angegeben wird, ist die Person authentifiziert. Wer ein zu simples Passwort wählt oder es leichtfertig weitergibt, öffnet Kriminellen Tür und Tor. Das Netzwerk elektronischer Geschäftsverkehr zeigt Ihnen hier einige Grundregeln, mit denen sie mit wenig Aufwand Ihre Daten wesentlich besser schützen können.



► Wie werden Passwörter geknackt?

Angreifer führen zum Aufspüren von Passwörtern häufig eine sogenannte „Wörterbuch Attacke“ durch. Dazu verwenden Sie digitale Wörterbücher und probieren völlig automatisiert enthaltene Einträge als Passwort aus. Dabei finden Sie ebenfalls vermeintlich sichere Passwörter wie „Schraubendreher“ oder „Taschenrechner“ als auch Vornamen wie „Ingrid“ oder „Peter“. Ebenfalls weit verbreitet: die „Brute-Force-Attacke“. Dabei werden mithilfe eines Computers einfach alle möglichen Buchstaben- und Zahlenkombinationen ausprobiert (z.B. aa, bb, ab, ba).



► **Verwenden Sie nur sichere Passwörter!**

Ein sicheres und damit starkes Passwort ist auf den ersten Blick sinnfrei zusammengesetzt, unterliegt also keiner erkennbaren Systematik. Verwenden Sie mindestens 10 Zeichen, darunter eine Mischung aus Groß- und Kleinbuchstaben, sowie Ziffern und Sonderzeichen. Mit jedem zusätzlichen Zeichen steigt der Aufwand zum Aufspüren des Passwortes enorm an. Es gibt viele Möglichkeiten sich komplizierte Passwörter mit einer einfachen Eselsbrücke zu merken. Überlegen Sie sich einen Satz, zum Beispiel: „An jedem 1. und 3. Samstag im Monat gehe ich Fußballspielen!“. Wenn Sie nur die Anfangszeichen verwenden, ergibt sich daraus folgendes Passwort: „Aj1.u3.SiMgiF!“.

► **Ändern Sie Ihr Passwort regelmäßig**

Wie häufig das Passwort gewechselt werden sollte, hängt davon ab, wie häufig Sie ihr Passwort verwenden und wie sensibel Ihre zu schützenden Daten sind (z.B. Passwort fürs Online-Banking vs. Passwort für eine Newsletter-Anmeldung). Idealerweise sollten Sie Passwörter für sensible Anwendungen (z.B. Online-Banking) etwa alle drei Monate wechseln.

► **Verwenden Sie Passwörter nur einmalig und niemals mehrfach!**

Verwenden Sie keinesfalls ein bereits in der Vergangenheit benutztes Passwort erneut. Ist der Angreifer beispielsweise vor Jahren in den Besitz eines von Ihnen passwortgesicherten Word-Dokumentes gekommen, hat er in der Zwischenzeit genug Zeit, sehr viele Passwortvariationen zu testen. Hat er das Passwort gefunden, probiert er dieses unter Umständen immer wieder bei Ihren aktuellen Dokumenten und Diensten auf Gültigkeit. Gelangt Ihr Passwort an die Öffentlichkeit, probieren Angreifer dies auch bei anderen Diensten (z.B. bei Ihrem Online-Banking) aus. Verwenden Sie daher für jeden Zweck und jeden Zugang ein anderes Passwort.

► **Verwahren Sie Ihre Passwörter an einem sicheren Ort!**

Jeder Computernutzer verwaltet heute eine Vielzahl von Passwörtern. Selbst Gedächtnisweltmeister stoßen da irgendwann an ihre Grenzen. Verwenden Sie am besten einen digitalen Passwort-Manager anstatt ein ungeschütztes Dokument, das alle Ihre Passwörter enthält.

Einige Produkte wie z.B. „Keepass“ [<http://keepass.info>] oder „Password Safe“ [<http://passwordsafe.sourceforge.net>] können Sie im Internet kostenfrei herunterladen.

► **Geben Sie Ihre Zugangsdaten nur an vertrauenswürdigen Rechnern ein!**

Vermeiden Sie es, Ihre Zugangsdaten an einem nicht vertrauenswürdigen Computer, z.B. im Internetcafé, einzugeben. Mittels eines sogenannten Keyloggers (deutsch: Tastenrekorder) können Hacker sämtliche Eingaben, die Sie über die Tastatur vornehmen, protokollieren; damit auch Ihre Passwörter.

► **Geben Sie Ihre Passwörter niemals preis!**

Häufig nutzen Angreifer die Leichtgläubigkeit der Nutzer aus. Phishing-Betrüger versenden im Namen eines vertrauenswürdigen Absenders (z.B. im Namen der Volksbank Berlin) eine E-Mail und fordern sie dazu auf, einem Link zu folgen und ihr Passwort auf einer präparierten Seite einzugeben. Keine Bank und kein seriöser Betreiber einer Online-Anwendung wird Sie via E-Mail dazu auffordern, Ihre Zugangsdaten preiszugeben.

Autoren:

Dipl.-Inform.(FH) Sebastian Spooren

Dustin Pawlitzek

Prof. Dr. (TU NN) Norbert Pohlmann

Fachhochschule Gelsenkirchen / Institut für Internet-Sicherheit – if(is)

Weiterführende Informationen:

<http://www.ec-net.de/>

<https://www.it-sicherheit.de/>

<https://www.it-sicherheit.de/topthema/passwoerter/>

<http://www.internet-sicherheit.de/institut/buch-sicher-im-internet/workshops-und-themen/topthema/>

<http://www.internet-sicherheit.de/>

<https://www.bsi.bund.de>

Bildquelle: Adam Tomasik / FOTOLIA.com

Das Netzwerk Elektronischer Geschäftsverkehr

Seit 1998 berät und begleitet das Netzwerk Elektronischer Geschäftsverkehr, in 29 über das Bundesgebiet verteilten regionalen Kompetenzzentren und einem Branchenkompetenzzentrum für den Handel, Mittelstand und Handwerk bei der Einführung von E-Business Lösungen. In dieser Zeit hat sich das Netzwerk als unabhängiger und unparteilicher Lotse für das Themengebiet „E-Business in Mittelstand und Handwerk“ etabliert. Das Netzwerk ist das einzige bundesweite Angebot seiner Art und verzeichnet jährlich rund 30.000 Besucher in Beratungen und Veranstaltungen. Es stellt Informationen in Form von Handlungsanleitungen, Studien und Leitfäden zur Verfügung, die auf dem zentralen Auftritt www.ec-net.de heruntergeladen werden können. Die Arbeit des Netzwerks wird durch das Bundesministerium für Wirtschaft und Technologie gefördert.

Fachhochschule Gelsenkirchen / Institut für Internet-Sicherheit – if(is)

Das Institut für Internet-Sicherheit ist eine fachbereichsübergreifende wissenschaftliche Einrichtung der Fachhochschule Gelsenkirchen. Es forscht und entwickelt auf Basis innovativer Konzepte im Bereich der Internet-Sicherheit. 2005 gegründet, hat es sich unter der Leitung von Prof. Dr. (TU NN) Norbert Pohlmann und in enger Zusammenarbeit mit der Wirtschaft innerhalb kurzer Zeit einen Ruf als eine der führenden deutschen Forschungsinstitutionen der IT-Sicherheit gemacht. Weitere Informationen finden Sie unter: <http://www.internet-sicherheit.de>

Sichere E-Geschäftsprozesse in KMU und Handwerk

Der IT-Sicherheitstipp wurde im Rahmen des Verbundprojekts „Sichere E-Geschäftsprozesse in KMU und Handwerk“ des Netzwerks Elektronischer Geschäftsverkehr (NEG) erstellt. Das Verbundprojekt wird vom Bundesministerium für Wirtschaft und Technologie (BMWi) unterstützt und soll helfen, in kleinen und mittleren Unternehmen mit verträglichem Aufwand die Sicherheitskultur zu verbessern. Hier werden insbesondere kleine und mittelständische Unternehmen sowie das Handwerk zu wichtigen Aspekten der Informationssicherheit sensibilisiert und praxisnah informiert. Alle Details finden Sie unter: <http://www.ec-net.de>