Passwörter

1000-mal gehört, aber entweder nicht verstanden, oder zu bequem bei der Umsetzung. Bekannt ist jedoch, dass sehr viele schwere Angriffe dadurch eingeleitet wurden, indem ein einzelner Account geknackt wurde. Bildlich: Es bringt nichts die Haustüre nach dem Standard von Fort Knox zu sichern und abzuschließen, wenn die Terrassentüre daneben unbeobachtet offen steht.

Inhalt

Dokinfo

Autor: Christian Schiele
Stand: 19.12.2013
Dateiname: passwörterhow2.docx

Grundregeln für ein Gutes Passwort

Diese sollten bekannt sein:

- Länge min. 8 Zeichen
- Kein Wort aus Wörterbüchern oder Lexika
- keine Tastenfolgen (123456, asdfgh, ...)
- keine Namen
- Eine Mischung aus Großbuchstaben, Kleinbuchstaben und Zahlen (besser auch noch Sonderzeichen)

Zuviel des Guten

Man kann es auch übertreiben, und sich wegen des perfekten Passwortes aussperren (leider wird dieser Fehlertyp beim Setzen des Passwortes nicht abgefangen).

- Passwortlänge: bis 14 Zeichen ist in der Regel kein Problem, ab da kann es hin und wieder problematisch werden, häufig sind Passworte mit mehr als 24 Zeichen kritisch.
- Sonderzeichen, die in der IT mit festen Funktionen belegt sind, bereiten gerne ein Problem, und auf diese solle man verzichten (Aus eigener Erfahrung: Sonderzeichen, die häufig für Probleme sorgen: "*", "%","&","$"," ","?")

Tipps für das Bilden eines Passwortes

Klassifizieren!

- Das Passwort für ein Forum oder eine Supportseite darf etwas einfacher sein (hier darf man auch mal ein Passwort wiederverwerten).
- Passworte für Onlineshops, Onlinebanking müssen sehr sicher sein
- Das Passwort für die Korrespondenz Mailbox muss mind. So gut sein wie das der Accounts (Schwächstes Glied in der Kette…)

Vorschlag zum Bilden eines Guten Passwortbaukastens:

- Einen Komplexen Teil mit 6-8 Stellen, der alle Merkmale beinhaltet (z.B. aus einem Passwortgenerator)
- Einem Teil den man sich einfach pro Account herleiten kann, der aber nicht direkt dem Account in Verbindung steht

Beispiel:

Komplexe Basis: **Ex8wC=**
Account-Teil: für Amazon **aBu** (von: á Buch); für eBay **1Me** (von: 321 meins)
Passwort für Amazon **Ex8wC=aBu**
Passwort für Ebay **Ex8wC=1Me**
Die Passworte sind wirrer Zeichen-Salat selbst wenn das Amazon Passwort errechnet wurde kommt man nicht ohne weiteres auf das Ebay Passwort

Passwortkeeper:

Feine Tools, aber nicht alles sind gut (z.B. Die Passwortkeeper der Browser haben einen zweifelhaften Ruf).

- Das gewählte Masterpasswort muss besser sein als der zu schützende Inhalt
- Wo lagert man die Kopie der Passwortdatenbank sicher
- Wie wird das Backup aktuell gehalten
- Wehe wen der Keeper geknackt wird.

Jeder muss für sich selber abmachen ob er solch ein Tool verwenden will.

Hintergrund, wie wird eine Passwortsicherung überwunden

Passworte sichern den Zugang zu einem Dienst, das kann ein Webalbum, ein Forum, ein Einkaufsportal und auch der Zugang zum Onlinebanking sein. In den Letzten Jahren ist die Bedrohungslage dafür dass ein Account geknackt wird massiv kritischer geworden. Hier gibt es zwei Varianten die man unterscheiden muss:

- es wird versucht gezielt den Account einer Person zu knacken. In der Regel wird über Sozial Engineering versucht das Passwort direkt zu erraten oder wenn es den Mechanismus der Passwortrückstellung über eine Sicherheitsfragen gibt, dann wird versucht diese Fragen korrekt zu beantworten. Alternativ wird versucht das Passwort vor Ort auszuspähen.
- der Provider wird geknackt, und dem Angreifer fallen alle Accounts in die Hände. Hier kann man selber nichts dagegen tun, dass liegt in der Verantwortung des Dienstleisters. Diese Art der Angriffe haben in den Letzten Jahren massiv zugenommen prominente Opfer sind z.B. Sony, Adobe, O2-Telefonica (Spanien). Häufig hat sich herausgestellt, dass die gestohlenen und verschlüsselten Passworte doch errechnet werden konnten. Die Angreifer hatten damit tausende von gültigen Usernamen und Passwort Kombinationen!

Leider auch bekannt: meist geht ein gezielter Angriff auf einzelne einem schweren Provider Hack voraus!

Was tun wenn es brennt:

sollte man merkwürdige Mail oder SMS erhalten, oder Briefe/Mails kommen, die einem Vorwerfen man hätte da was gekauft aber nicht bezahlt, dann muss man reagieren:

1. Klären welcher Account steht mit den Problemen in Verbindung
2. Prüfen des Accounts auf Auffälligkeiten (dabei nie über den Link in einem Mail einloggen, sondern immer über die direkte Eingabe beim Browser).

Sofern der Einbruch bestätigt ist:

3. Sofort ein neues Passwort setzen (kann man auch prophylaktisch machen) – Aber nicht mit dem eigenen Rechner (der könnte ja die Quelle des Übels sein!)
4. Den Servicebetreiber davon in Kenntnis setzen (wenn man sich nicht anders zu helfen Weiß: admin@<Domainname> ist sehr häufig ein Mailaccount beim Provider
5. Anzeige bei der Polizei erstatten (wenn es um Geld geht dann ein Muss, ansonsten Kann)

Diese Vorgehen ist auch dann zu empfehlen, wenn in der Presse bekannt wird, dass ein Dienstleister bei dem man einen Account hat erfolgreich geknackt wurde.

Allgemeine Vorsichtsmaßnahmen?

Manchmal braucht ein Angreifer einen Account um sich übergeordnete Rechte zu verschaffen und um dann Schaden anzurichten (und der Account, den für den Angriff verwendet wird gehört in der Regel nicht dem Angreifer. Solche Angriffe werden gerne über präparierte Mails vorbereitet, die den eigenen Rechner "verseuchen" und ein Angreifer damit in der Lage ist die Login Informationen direkt bei der Eingabe mitzulesen. Da heutzutage sehr viele vertrauliche Daten elektronisch verfügbar sind, kann man auch dann zum Ziel eines Angriffs werden, wenn man "nur" ein kleiner Mitarbeiter ist, aber als Sprungbrett zu anderen Mitarbeitern dienen kann, die in sensiblen Bereichen sitzen (solche Angriffe können sehr lange laufen!).

- Ein gesundes Mistrauen, auch bei Mails von bekannten schadet nicht (Die berühmten Witz des Tages Mails sind auch Angreifern sehr willkommen....)
- Den eigenen Rechner "sauber" halten (Virenschutz und Firewall), gilt auch außerhalb der Windows Domäne!
- Verfügbare Sicherheitsupdates zeitnah einspielen (für ALLES was auf einem Rechner läuft, z.B. der Adobe Flashplayer und PDF-Reader sind mittlerweile in der Angriff-Hitliste ganz weit oben).