+ + + Pressemitteilung + + +

ArchiCrypt zeigt, wie leicht ein Passwort gehackt werden kann

Ottobrunn, 17. Juni 2016 – In den vergangenen Tagen waren Hacker, die sich auf den Diebstahl von Kundendaten spezialisiert haben, wieder besonders aktiv. Das in Ottobrunn bei München ansässige Software-Unternehmen ArchiCrypt zeigt, wie leicht es für Cyberkrimielle ist, an vertrauliche Kundeninformationen zu kommen. Zumindest dann, wenn Firmen mit den Daten ihrer Kunden allzu sorglos umgehen...

Im Darknet werden permanent Millionen gestohlener Zugangsdaten angeboten. Aktuell kann man zum Beispiel Zugangsdaten von LinkedIn-, Badoo- und Twitter-Nutzern erwerben. Obwohl diese und auch andere Dienste die Passwörter mitsamt dem Anmeldenamen im Regelfall nur als Hashwert in einer Datenbank speichern, ist es für Cyberkriminelle ein Leichtes, aus diesen Werten das Passwort zu rekonstruieren.

Um zu verdeutlichen, wie leicht das in der Praxis wirklich ist, hat ArchiCrypt das kleine Tool **ArchiCrypt Passwort Cracker** entwickelt. Das Programm demonstriert, wie Hacker mit Hilfe von sogenannten Wörterbüchern, also Sammlungen von potenziellen Passwörtern, die im Internet frei verfügbar sind und einfach heruntergeladen werden können, an Passwörter kommen.

Das Tool zeigt, wie für jeden im Wörterbuch vorhandenen Eintrag der zugehörige Hashwert berechnet werden kann. Danach wird überprüft, ob der Hashwert in der Liste der gestohlenen Nutzerdaten vorhanden ist. Ist ein identischer Hashwert vorhanden, ist das Passwort gecrackt. Das Passwort wird nun als Klartext angezeigt. Mit dem Tool Passwort Cracker kann man natürlich keine echten Passwörter cracken. Es dient nur als Demonstrationsprogramm, um die grundsätzliche Arbeitsmethode von Hackern zu zeigen. Ausführliche Informationen und Tipps, wie man sich gegen Datendiebstahl wehren kann, bekommen Anwender außerdem in dem ArchiCrypt-Video "**Wie wird ein Passwort gecrackt**".

Da Hacker diese Art der Anfragen parallelisieren, können sie eine riesige Anzahl von Hashwerten in kürzester Zeit berechnen. Mit einem leistungsfähigen Mehrkernprozessor oder einem Rechnerverbund lassen sich viele Millionen von Berechnungen zeitgleich durchführen. Da die Hashwerte sich nicht ändern, lassen sich diese Berechnungen speichern und jederzeit wiederverwenden. Das spart beim nächsten Angriff jede Menge Zeit.

Im Prinzip sind Dienste-Anbieter gegen Hacker-Angriffe nicht wirklich geschützt. Die eingesetzte Software ist so komplex, dass sie niemals fehlerfrei sein kann. Diese Fehler nutzen Hacker aus, um Zugriff auf die Nutzerdaten zu bekommen.

Trotzdem kann die Rekonstruktion von Passwörtern aus den entwendeten Daten wirksam verhindert werden. Dafür muss der Dienste-Anbieter dafür sorgen, dass die Berechnung eines Hashwerts so zeitintensiv wird, dass sich der Aufwand für den Angreifer nicht mehr lohnt. Lange bekannt ist das so genannte SALT-Verfahren. Bei diesem Verfahren wird für jeden Account ein zusätzlicher, zufälliger Wert erzeugt, der dem Passwort beigefügt wird. Erst danach wird der Hashwert berechnet. Theoretisch lassen sich auch daraus Passwörter berechnen, der Zeitaufwand ist jedoch astronomisch hoch.

Nutzer können ebenfalls ihren Beitrag dazu leisten, dass Hacker gar nicht erst an ihre Daten kommen bzw. der Schaden begrenzt wird. Dazu gehört:

1) Niemals dasselbe Passwort für unterschiedliche Accounts nutzen

Anwender haben keinen Einfluss darauf, was der Dienste-Anbieter mit dem Passwort macht. Theoretisch könnte er es auch im Klartext abspeichern. Damit im Falle eines Diebstahls nicht alle Konten betroffen sind, sollte man für jeden Account ein anderes Passwort nutzen.

2) Niemals Passwörter verwenden, die lexikalische Begriffe enthalten

Durch die Zuhilfenahme von Wörterbüchern lassen sich Passwörter, die lexikalische Begriffe enthalten, leicht rekonstruieren. Das gilt auch dann, wenn dem Begriff Zahlen und Sonderzeichen hinzugefügt werden. Das Passwort 8a110n ist also ähnlich leicht zu knacken wie das Passwort Ballon.

3) Passwörter mindestens alle 3 Monate ändern

Ein Diebstahl von Passwörtern bleibt nicht selten unentdeckt oder wird erst sehr spät entdeckt. Mit einer regelmäßigen Änderung seiner Passwörter kommt man Hackern mit etwas Glück zuvor.

Einen Großteil der Arbeit kann Anwendern dabei ein Passwort-Manager wie ArchiCrypt Passwort Safe abnehmen. Mit dem Programm lassen sich Passwörter übrigens nicht nur verwalten und sicher verschlüsselt auf der Festplatte abspeichern. Das Programm informiert auch beim Bekanntwerden eines Datendiebstahls über gefährdete Einträge und zeigt, welche Passwörter schleunigst geändert werden sollten. Passwort Safe lädt dafür bei jedem Start eine kleine Datenbank vom ArchiCrypt-Server, die Informationen über gehackte Internet-Dienste enthält. Die Datenbank wird von ArchiCrypt ständig aktualisiert. Beim Öffnen des Passwort Safes werden nun alle Einträge überprüft. Sobald das Programm einen potenziell gefährdeten Eintrag findet, erscheint in der Programmoberfläche eine entsprechende Warnmeldung.

Die Freeware ArchiCrypt Passwort Cracker (lauffähig ohne Installation) können Sie hier herunterladen:
https://download.archicrypt.de/ACPasswortCracker.exe

Informationen zum ArchiCrypt Passwort Safe bekommen Sie hier:
https://www.archicrypt.de/archicrypt_passwort_safe/

Ein ausführliches Video zum Thema "Wie wird ein Passwort gecrackt" gibt es hier:
https://youtu.be/1Xq9Miz17K4

Druckfähiges Bildmaterial finden Sie hier:
http://www.laubstein-media.de/News/ArchiCrypt_2016_06.zip

Pressemitteilung zum Download:
http://www.laubstein-media.de/News/PM_ArchiCrypt_2016_06.pdf

Über Software-Entwicklung Remus - ArchiCrypt

Die Firma Software-Entwicklung Remus - ArchiCrypt wurde Anfang 1999 gegründet. Eine Kernmannschaft von drei Ingenieuren und einer Bürofachangestellten plant, entwickelt und vertreibt Software-Produkte rund um das Thema Datensicherheit. Dabei reicht das eigene Spektrum von der Echtzeitverschlüsselung bis hin zur Steganografie. Projekte, die von der Software-Entwicklung Remus bearbeitet werden, stammen oft aus Fachbereichen wie der Luft- und Raumfahrttechnik, der Informatik und dem Maschinenbau.

Bei den eigenen Entwicklungen machte das dateibasierte Verschlüsselungsprogramm ArchiCrypt Pro den Start. Ein Jahr später wurde die ArchiCrypt Live Engine fertig gestellt – ein SDK mit Echtzeitverschlüsselungsfunktion. Die eigenen Erfahrungen mündeten in die Entwicklung der ArchiCrypt Live Produktserie, die mit ArchiCrypt Live NETim Jahre 2003 eine Netzwerkverschlüsselung speziell für Firmenkunden als neues Mitglied erhielt. Gerne verwenden andere Softwarehäuser ArchiCrypt-Basistechnologie, um den eigenen Kunden Verschlüsselungslösungen anzubieten. Die Produktfamilie wächst stetig weiter und hat inzwischen viele treue Fans in ganz Europa. Zahlreiche Testsiege in der Fachpresse, namhafte Firmen und Behörden unter den Kunden sowie Übersetzungen in die englische und französische Sprache zeugen vom anhaltenden Erfolg der Produktreihe. Mehr Informationen erhalten Sie unter www.archicrypt.de.

Pressekontakt:
Laubstein Media
Anja Eichelsdörfer
UntereParkstr. 42
85540 Haar

Tel.: +49-89-41 85 84 85
Fax: +49-89-41 85 84 86
Mobil: +49-151-41 20 22 32

Mail: presse@laubstein-media.de
Web: http://www.laubstein-media.de