BIZCOMMUNITY

Why your *P@s$word* is a fail

By Jonas Thulin

21 May 2015

Passwords have become practically useless as the sole security measure protecting your personal information, says Fortinet.

The IT security industry has been warning about the fallibility of passwords for years, yet the situation hasn't changed. Millions of people still depend on the most common password - 'password', simple number sequences like '12345' or the name of their dog to secure their important personal details and authenticate themselves for online transactions. Millions use the same password for all their authentications, because remembering multiple complicated passwords can be difficult.

Many others diligently use different passwords for each site they access, substituting symbols for letters in a bid to make their passwords more secure. Unfortunately, this is not enough. Because truly complex and hard-to-hack passwords would be too difficult for most people to remember, the average person's password is relatively simple to crack. In fact, researchers presented with stolen databases have been able to crack 90% of the passwords within days.

The threats

Salvatore Vuono via
www.freedigitalphotos.net

In an online environment, a hacker can make a limited number of attempts to guess a user's password before being locked out of the account. But because data theft can put user databases into the hands of hackers in an offline environment, thousands of attempts can be made to crack the password, and it can all be done automatically, running user names against extensive password 'dictionaries' of all possible word combinations. In a targeted attack, where cyber criminals focus on a high value individual or senior company employee, their public social media accounts provide a great deal of personal information that can help hackers guess at their passwords.

This points to passwords being virtually useless as the sole means of securing data. It also points to the fault being not just the weakness of the passwords in use, but the failure of websites and service providers to properly secure and encrypt the user names and passwords of their clients. Too many websites focus most of their energies on securing the actual transactions, and on the design and functionality of the site, and neglect to adequately secure their databases. All of the hacks we have seen have involved weakness in companies' defences and the way in which data was stored. In fact, we have even seen cases where passwords were kept in clear text or not encrypted at all.

The solutions

One way to improve password strength and still remember the complex combinations is to use a password manager application, which saves logon and password information securely, and is accessed by a single, master password. Backing up your passwords has its appeal, but a web-based password manager could still be vulnerable to attack. The most secure password manager would be one hosted on your personal device and secured by a combination of authentication measures, such as a master password and biometric authentication. Ironically, writing down your user names and passwords on a piece of paper might be equally secure, particularly if the paper is stored where nobody is likely to find it.

In an environment with a fast growing threat of cyber crime and increasing security complexity for users, it may well prove more effective not to have passwords at all. Instead, service providers could move to using strong multi-factor authentication, such as devices that generate single-use passwords and one-time PINs sent to mobile devices, combined with biometrics.

At the same time, enterprises, websites and service providers need to ensure that all transactions, data, systems and networks are effectively secured using best of breed, next generation security.

ABOUT JONAS THULIN

Jonas Thulin, security consultant at Fortinet
- Betting the farm on untested tech - 25 May 2015
- Why your *P@s$word* is a fail - 21 May 2015

View my profile and articles...