Weak passwords threaten the enterprise

By Simon Campbell-Young

12 Oct 2014

Research reveals time and time again that weak login credentials, including passwords, remain among the top causes of data breaches around the world. Despite this, individuals continue to choose weak and insecure passwords to protect their most sensitive data.

Choosing a strong password is even more important as more businesses leverage the cloud, and BYOD practices.

A strong password is the first line of defence against attackers. Less vulnerable authentication information can be an extremely valuable weapon in the cyber crime prevention battle, whereas using a password that can be easily guessed makes it child's play for attackers to access your most sensitive information.

Authenticating passwords

Unfortunately, due to the myriad passwords that each individual is obliged to remember, choosing a highly secure password can be a daunting task. Social media sites, loyalty programmes, bank accounts... the list is endless. Too many people simply cannot remember the sometimes hundreds of passwords used in the average day to access sites or conduct business.

Too many users are unaware of the possibly disastrous potential consequences should their passwords be discovered by an attacker. Over and above the obvious factors of being able to read your private communications, attackers could use your machine to breach the corporate network and steal intellectual property or proprietary information. Password theft can open the floodgates to abuse, and should never be underestimated.

One of the greatest challenges faced by the connected world is making sure someone is who he claims to be - in a nutshell, authentication. The use of passwords for authentication has been common practice for many years now, but the use of weak passwords completely negates what it is trying to achieve. Not only passwords that can be easily guessed, but weak passwords that make brute force attacks so successful.

The method behind a strong password

Too many passwords make use of personal information, such as names of loved ones, birthdays or similar. In addition, passwords that are easy to remember, such as 12345, or 'password' are worse than useless.

A strong password will make use of a combination of uppercase and lowercase letters, special characters and numbers, and will be a very minimum of eight characters long. The longer, the better.

In addition, never divulge passwords to anyone, nor write them down. Moreover, do not let your applications or frequently visited websites remember your passwords, as they cannot guarantee that they are saved in a secure and encrypted format.

ABOUT SIMON CAMPBELL-YOUNG

Having started his career as a startup partner for FSA Distribution in 1990, Simon Campbell-Young went on to start his own company called Memtek Distribution in 1995. This was sold to a public company called Siltek Holdings between 1998 to 2000. Shortly thereafter, he took his experience in the technology sector, garnered over more than 23 years, to form specialist distribution company Phoenix Distribution in 2000.

- Do's and don'ts of digital marketing - 20 Jul 2016
- Weak passwords threaten the enterprise - 12 Oct 2014
- Big data, big advantages - 22 Jul 2014
- U.S. shutdown proves how global the supply chain has become - 5 Mar 2014

View my profile and articles...