BIZCOMMUNITY

Business security: is simpler better?

By Carey van Vlaanderen

13 Oct 2015

While some companies can be pretty strict about their cyber security policies, and risk that at the end of the day this might be counterproductive, others apply a more flexible approach. The problem with being too rigid is that it could be like trying to control the tide. You might succeed in keeping a part of the shore dry, but you have to be careful with the rising water that might find its way, says Carey van Vlaanderen, CEO at ESET.

©Wavebreak Media Ltd via 123RF

Over the years, passwords have evolved quite a bit. They grew in length and complexity, but most significantly in numbers. And employees are often the ones who have suffered under this trend. They are asked to remember numerous security codes for work accounts, work-related and personal apps, online services, emails, smartphones and other devices. Moreover, usually they should be at least 10 characters long, contain caps, numbers and symbols.

However, what some of the employees do is to create one strong password for all the services and devices or go for many easy-to-remember ones. Yet both of these strategies present a risk possibly leading to a security breach that could prove damaging to your firm and clients.

So what can businesses do to break the vicious password cycle?

There are different things to keep in mind. Firstly, companies can start by cutting the number of passwords. If an app, a service or device isn't essential for the business, a good rule of thumb is to only require a simple passcode or use other less demanding security measures. The other way to address the password overflow is by pre-installing a password manager from a respected vendor to employee devices.

It should also be noted that if you push people to modify the security codes too often, they end up sometimes making minor changes or even worse, they could use post-its for "storing" the codes on their table. Finding the right balance when setting the period for password renewal might be tricky. Extending it might be a more effective approach, but companies should also keep in mind, that the longer the passcode is used, the less secure it becomes.

Support the usage of strong passwords by using strength meters and blacklists of the most common choices. That way your people know in an instant if their pick is secure enough or not.

But no matter how strong the passwords are, your company might still be vulnerable to brute-force attacks (automated guessing of large amounts of passwords). By applying account throttling (prolonging the time to make another login attempt) and account lockouts (locking the account after approximately 10 unsuccessful logins) you reduce the risk without overloading your people.

Banning personal devices? Simple rules to give you more control

It isn't all about the passwords, you may say. And you are right, as the risks may come also from private devices used by employees for work purposes. But if you are thinking of banning this practice, you might have to think twice. As surveys have shown that a great number of people will smuggle their devices to the workplace anyway.

Rather, you can advise your people to use screen locks on their smartphones and tablets, passwords being the strongest option, but even PIN or pattern logins are better than no security at all. Using encryption for all the data is also a good idea. Instruct all your employees who use private laptops, tablets or smartphones to apply at least the pre-installed built-in solutions or recommend reputable software of your choice.

Is work from home one of the perks your company offers? If so, apply two-factor authentication (2FA) for remote connections. Generating unique one-time password for every login provides an extra layer of security for the sensitive data and makes it much harder to crack. What's more, installing such a solution onto the smartphone makes it simple to use and easy to carry around.

ABOUT CAREY VAN VLAANDEREN

Carey van Vlaanderen is CEO of ESET Southern Africa. ESET is a global provider of security software for enterprises and consumers and is dedicated to delivering instant, comprehensive protection against evolving computer security threats.

- 4 ways to manage the human threat to cybersecurity - 18 Jul 2023
- A cybercriminal's tricks and trades to get into your phone - 23 Mar 2018
- What is encryption, how does it work and why is it important? - 6 Mar 2017
- Five common security threats that demand attention - 9 Mar 2016
- Face 2016 with a proactive attitude of security awareness - 22 Jan 2016

View my profile and articles...