Gone are the days of simply having passwords

By Lipsky Raseasala

6 Dec 2017

While some are already graduating to multi-factor authentication, an alarming number of companies rely on single-factor authentication, such as passwords, exclusively.

© Leo Wolfert via www.123RF.com

Cybercriminals are always cultivating new methods for accessing bank accounts, company information systems, and other online services. Motivated by financial gain, hackers are and will continue to find ways to get their hands on peoples' credentials to gain access to user accounts and company systems. *It's how they make their money.*

> *Companies need to move away from relying on passwords only for authorising user access to their IT systems.*

Two-factor authentication for verifying user credentials has been around for more than ten years. It's that extra layer of authentication or verification to prove who users say they are in order to access accounts and other resources. Single factor authentication can be a password, where most cases you need to enter the identity (username) and then the password to gain access.
Second-factor authentication involves an extra, identifying a link to the person that belongs to that person alone, such as a body part, like an eye or fingerprint, or a device like a smartphone, laptop or hard tokens. According to Raseasala, larger companies have added two-factor authentication to verify users accessing IT resources, especially for employees working remotely who require access to the servers via SSL (secure socket layer) VPN (virtual private network). Adding a second factor of authentication or verification adds an extra layer of security that makes it more difficult to gain unauthorised access. However, small and medium-sized businesses are lagging behind, leaving their IT systems vulnerable.

The unauthorised access of systems using usernames and passwords is now commonplace. Major breaches have occurred in organisations that use only single-factor authentication, where the credentials of a single user have been utilized to access company systems.

As hackers hone their methods of attack, breaches are also happening within organizations that have implemented two-factor authentication. Hackers, for instance, are creating malware that is designed specifically to target tokens such as soft tokens popular on smartphones.

Hackers could get even nastier in 2018

1 Dec 2017

Where unauthorised exposure of company resources would place a business at risk, such as for organizations that process and store sensitive information such as personal information, additional controls need to be incorporated to monitor and continuously authenticate users while they are accessing those resources, adding that layers such as device recognition, IP reputation, PKI certificates, geo-location, geo-fencing, group entitlements, access histories and behavioural biometrics can be added to check credentials and authenticate users. This is referred to as multi-factor authentication, something you have, something you know and something you are.

> *Multi-factor authentication is certainly the way forward.*

However, any additional layers or controls that are added need to be integrated mindfully so as not to hamper productivity. It is also important to note that no two companies have the same access and security requirements. One size certainly does not fit all when it comes allowing users' access to information resources.
If you are in doubt, consult with qualified, outsourced IT security providers who will be able to assess your security requirements and advise on a two-factor or multi-factor authentication process that will allow you to effectively manage risk and user productivity at the same time.

ABOUT THE AUTHOR

Lipsky Raseasala is an IT security consultant at Securicom, a leader in managed IT security solutions.