sourceSecurity.com
making the world a safer place

How organisations can secure user credentials from data breaches and password hacks

Published on 14 Jan 2019

In the age of massive data breaches, phishing attacks and password hacks, user credentials are increasingly unsafe. So how can organisations secure accounts without making life more difficult for users? Marc Vanmaele, CEO of TrustBuilder, explains.

User credentials give us a sense of security. Users select their password, it's personal and memorable to them, and it's likely that it includes special characters and numbers for added security. Sadly, this sense is most likely false. If it's anything like the 5.4 billion user IDs on haveibeenpwned.com, their login has already been compromised. If it's not listed, it could be soon. Recent estimates state that 8 million more credentials are compromised every day.

Ensuring safe access

Data breaches, ransomware and phishing campaigns are increasingly easy to pull off. Cyber criminals can easily find the tools they need on Google with little to no technical knowledge. Breached passwords are readily available to cyber criminals on the internet. Those that haven't been breached can also be guessed, phished or cracked using one of the many "brute-force" tools available on the internet.

It's becoming clear that login credentials are no longer enough to secure your users' accounts. Meanwhile, organisations have a responsibility and an ever-stricter legal obligation to protect their users' sensitive data. This makes ensuring safe access to the services they need challenging, particularly when trying to provide a user experience that won't cause frustration – or worse, lose your customers' interest.

Importance of data protection

So how can businesses ensure their users can safely and simply access the services they need while keeping intruders out, and why is it so important to strike that balance?

After GDPR was implemented across the European Union, organisations could face a fine of up to €20 million, or 4% annual global turnover – whichever is higher, should they seriously fail to comply with their data protection obligations. This alone was enough to prompt many organisations to get serious about their user's security. Still, not every business followed suit.

Cloud security risks

> Breaches were most commonly identified in organisations using cloud computing or where staff use personal devices

According to a recent survey conducted at Infosecurity Europe, more than a quarter of

organisations did not feel ready to comply with GDPR in August 2018 – three months after the compliance deadline. Meanwhile, according to the UK Government's 2018 Cyber Security Breaches survey, 45% of businesses reported breaches or attacks in the last 12 months.

According to the report, logins are less secure when accessing services in the cloud where they aren't protected by enterprise firewalls and security systems. Moreover, breaches were most commonly identified in organisations using cloud computing or where staff use personal devices (known as BYOD).

According to the survey, 61% of UK organisations use cloud-based services. The figure is higher in banking and finance (74%), IT and communications (81%) and education (75%). Additionally, 45% of businesses have BYOD. This indicates a precarious situation. The majority of businesses hold personal data on users electronically and may be placing users at risk if their IT environments are not adequately protected.

Hackers have developed a wide range of tools to crack passwords, and these are readily available within a couple of clicks on a search engine

Hacking methodology

In a recent exposé on LifeHacker, Internet standards expert John Pozadzides revealed multiple methods hackers use to bypass even the most secure passwords. According to John's revelations, 20% of passwords are simple enough to guess using easily accessible information. But that doesn't leave the remaining 80% safe.

Hackers have developed a wide range of tools to crack passwords, and these are readily available within a couple of clicks on a search engine. Brute force attacks are one of the easiest methods, but criminals also use increasingly sophisticated phishing campaigns to fool users into handing over their passwords.

> Users expect organisations to protect their passwords and keep intruders out of their accounts

Once a threat actor has access to one password, they can easily gain access to multiple accounts. This is because, according to Mashable, 87% of users aged 18-30 and 81% of users aged 31+ reuse the same passwords across multiple accounts. It's becoming clear that passwords are no longer enough to keep online accounts secure.

Securing data with simplicity

Users expect organisations to protect their passwords and keep intruders out of their accounts. As a result of a data breach, companies will of course suffer financial losses through fines and remediation costs. Beyond the immediate financial repercussions, however, the reputational damage can be seriously costly. A recent Gemalto study showed that 44% of consumers would leave their bank in the event of a security breach, and 38% would switch to a competitor offering a better service.

Simplicity is equally important, however. For example, if it's not delivered in ecommerce, one in

three customers will abandon their purchase – as a recent report by Magnetic North revealed. If a login process is confusing, staff may be tempted to help themselves access the information they need by slipping out of secure habits. They may write their passwords down, share them with other members of staff, and may be more susceptible to social engineering attacks.

So how do organisations strike the right balance? For many, Identity and Access Management solutions help to deliver secure access across the entire estate. It's important though that these enable simplicity for the organisation, as well as users.

Organisations need an IAM solution that will adapt to both of these factors, providing them with the ability to apply tough access policies when and where they are needed and prioritising swift access where it's safe to do so

Flexible IAM

While IAM is highly recommended, organisations should seek solutions that offer the flexibility to define their own balance between a seamless end-user journey and the need for a high level of identity assurance.

Organisations' identity management requirements will change over time. So too will their IT environments. Organisations need an IAM solution that will adapt to both of these factors, providing them with the ability to apply tough access policies when and where they are needed and prioritising swift access where it's safe to do so.

Importantly, the best solutions will be those that enable this flexibility without spending significant time and resource each time adaptations need to be made. Those that do will provide the best return on investment for organisations looking to keep intruders at bay, while enabling users to log in safely and simply.

Author Profile

Marc Vanmaele

You may also be interested in...

The ongoing challenge of IT and data risk management

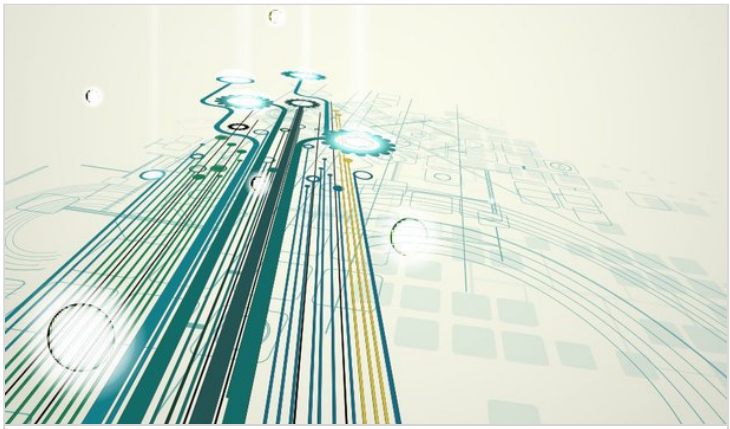
Managing IT and data risk is a challenging job. When we outsource our IT, applications and data processing to third-parties more and more ev...

Data security experts at Bosch and Genetec discuss impact of GDPR on v...

Today, more and more video security cameras are increasingly connected to the internet and transitioning into intelligent sensors that colle...

Beyond cyber security: Why physical security must be a key element of...

Edward Snowden’s name entered the cultural lexicon in 2013, after he leaked thousands of classified National Security Agency documents...



Trends of 2019 to watch out for: The connected system and commercial s...

Users of security systems have long been willing to sacrifice certain aspects of security in favour of convenience and ease of use. The tide...

A glance at the winners and losers of the security industry in 2018

In my coverage of China Tariffs impacting the security industry over four recent articles, products on the tariff schedules routinely integr...