New multi-factor authentication threat highlights SA's security negligence

Issued by Entersekt

7 Jul 2022

Despite the growing levels of cyber threats, adoption of even basic multi-factor authentication (MFA) remains depressingly low amongst organisations. And, with new techniques such as prompt bombing being used to beat older versions of MFA, the need to beef up how institutions protect their customer data has become critical.

According to the 2021 Cyberthreat Defence Report, more than 43% of the more than 1,200 surveyed global IT decision makers said they had not yet deployed even basic MFA. What's more, while there had been a healthy 7% increase in MFA uptake in the previous year, a further 11.4% said they had no intention of deploying the security technology in the next 12 months.

"The same lack of urgency can be found in South Africa. Logging into a website or service using a username and password remains the favoured method of the majority of local organisations. I believe this is due to a combination of complacency, misunderstanding regarding the perceived complexities of introducing MFA and an attempt to avoid any inconvenience," says Mathew Love, senior product marketing manager at Entersekt.

Prompt bombing – the new threat on the block

Love explains that while the rapid increase in remote working has accelerated MFA adoption from some companies, the numbers are still far too low when viewed in relation to the actual threat level. And, in the wake of new threats such as prompt bombing, companies must take action or they could face more than just the reputational damage of a data breach.

"MFA prompt bombing first surfaced around 24 months ago, largely in response to the rise in well-known MFA techniques such as mobile push notifications being employed. We know that hackers continuously evolve the way they intercept data and gain access to our accounts and, as more of us moved away from traditional username and password and towards basic MFA, they also had to adapt. While we haven't seen prompt bombing attacks at scale in South Africa as yet, it is simply a matter of time," he warns.

The now infamous SolarWinds breach in 2020 as well as the Microsoft source code leak in March were both achieved through bypassing older forms of MFA security by prompt bombing methods.

These methods include: sending a flurry of MFA requests in the hope that the user will grant access to make them stop; sending one or two requests each day in a more subtle attempt to gain access; calling users and pretending to be from a service provider and duping them into granting access via a similar MFA process.

FIDO2 could hold the key

Love says one way to avoid these prompt bombing attacks is to adopt the FIDO2 passwordless authentication framework which requires that the device in the user's possession is authenticated through an embedded key which can be unlocked, usually through biometrics.

"FIDO2 comes with a number of benefits over and above its significantly better security levels. The framework is platform-agnostic, offering a more efficient authentication process without the need for passwords for account access or online payments. It is also impervious to man-in-the-middle and other related attacks while still allowing users to authenticate themselves across channels and devices at a moment's notice. A big challenge facing companies relying on in-app or push-authentication is that there is always a small portion of customers who don't have, or want, their apps. FIDO2 offers a workaround for this, while also offering advanced protection for companies choosing not to make use of apps. Moreover, it offers a better user experience at a lower operating cost," Love explains.

So many ways to steal our data

While prompt bombing is not yet a major part of our mainstream threat playbook, Love says local organisations still have their hands full when it comes to protecting their data.

According to Love, account takeover fraud such as SIM-swap fraud is a real concern at the moment. In this instance fraudsters use a combination of social engineering tactics to gather relevant personal information. They then use this to get the victim's phone number ported to one of their SIM cards, enabling them to intercept important authentication messages and OTPs.

Man-in-the-middle attacks are another big risk, occurring when fraudsters create dummy web pages which look like legitimate websites. Users are tricked into visiting these through emails and text messages posing as a service provider. When the user inputs their normal login details, the fraudsters gain access to their details and quickly empty accounts or steal sensitive information.

"There is an onus on the user to inform themselves about new threats and to remain vigilant in protecting themselves against them, but we really should be demanding better protection of our data from the institutions we support. Organisations can no longer rely on outdated or weak MFA mechanisms for protection – especially if it's just a password and SMS OTP option. It's essential that authentication is implemented that embraces the full context of the user and their connection. This includes the channel the user is on and even context about the customer themselves, their devices and their unique characteristics. It's clear that not all MFA is created equal and opting for the most basic version is simply no longer good enough," Love warns.

About Entersekt

Entersekt is a leading provider of strong device identity and customer authentication software. Financial institutions and other large enterprises in countries across the globe rely on its multi-patented technology to communicate with their clients securely, protect them from fraud, and serve them convenient new experiences irrespective of the channel or device in use. They have repeatedly credited the Entersekt Secure Platform with helping to drive adoption, deepen engagement, and open opportunities for growth, all while meeting their compliance obligations with confidence.