Secure user access whilst working from home!

Due to the global pandemic Covid-19, governments have imposed strict Stay at Home guidelines. This has forced many organisations to enable most of their staff to work from home. This upsurge in remote working has also driven a rise in cyberattacks.

Threatpost.com comments, “The concern is more than theoretical. Already, attackers have been leveraging coronavirus-themed cyberattacks as panic around the global pandemic continues – including various malware attacks involving Emotet and other threats.”

As cyber threats increase, all organisations need to ensure they are protecting their systems against unauthorised access.

Remote working offers great business benefits but can expose new risks that need to be managed:

The NCSC suggests that “...with mobile working or remote access to systems you should establish risk-based policies and procedures that support mobile working and/or remote access to systems that are applicable to users, as well as service providers.”

They go on to say that “…organisations that do not establish sound mobile working and remote access practices may be vulnerable to the following risks:”

The risks:

Loss or theft of device:

“Mobile devices are highly vulnerable to being lost or stolen, potentially offering access to sensitive information or systems. They are often used in open view in locations that cannot offer the same level of physical security as your own premises.”

Loss of credentials:

“If user credentials (such as username, password, or token) are stored with a device used for remote working or remote access and it is lost or stolen, the attacker could use those credentials to compromise services or information stored on (or accessible from) that device.”

Being overlooked:

“Some users will have to work in public open spaces, such as on public transport, where they are vulnerable to being observed when working. This can potentially compromise sensitive information or credentials.”

Tampering:

“An attacker may attempt to subvert the security controls on the device through the insertion of malicious software or hardware if the device is left unattended. This may allow them to monitor all user activity on the device, including authentication credentials.”

Protect your users’ authentication, wherever they may be based!

“As organisations rush to shift their business and classes online, cybercriminals are ramping up their tactics to take advantage of those who may have inadequate or naive security postures as a result. Given the challenges in securing work and learn from-home environments, the attack surface represents an attractive opportunity for threat actors.” Threatpost.com suggests.

With widespread adoption of remote working and a lack of policies and procedures that support remote access could increase the chance of falling victim to a cyber-attack.

An easy way to secure user access, whilst maintaining user efficiency, would be to implement an extra layer of security, such as a Multi-Factor Authentication (MFA) solution. Ensure your organisation deploys a solution which can help to minimise the risk of compromising your network, and ensure your users are secured when they are onsite and at home.

MFA

Can be used to protect applications such as SAP ERP systems, CRM platforms, O365 and many more.

Architecture

Whether your architecture is on-premise or cloud based, ensure you deploy an MFA solution that can adapt to your architectural needs.

SSO & RBA

Dynamic features as standard to provide users with a single point of access for all applications, that is protected by a risk based policy.

With PINsafe® technology at the core for ultimate security and risk-based authentication policy providing dynamic control, the award winning AuthControl Sentry® delivers an intelligent multi-factor authentication (MFA) solution, which can protect your organisation from unauthorised access.

Contact Swivel Secure to learn more about their award-winning MFA solution and how it can ensure secure and efficient authentication access for all your users, no matter where they are based.

Sources:

NCSC - 10 steps to cyber security. Available at: https://www.ncsc.gov.uk/collection/10-steps-to-cyber-security/the-10-steps/home-and-mobile-working

Threatpost.com - Working from Home: COVID-19’s Constellation of Security Challenges. Avaliablle at: https://threatpost.com/working-from-home-covid-19s-constellation-of-security-challenges/153720/

Abbreviation Glossary:

MFA: Multi-factor authentication - a security system that requires more than one method of authentication from independent categories of credentials to verify the user’s identity for a login.

RBA: Risk-based authentication - designed to deliver intelligent authentication by optimising security based on the user, the device and the application.

SSO: Single sign-on - A feature providing users with the ability to access all of their applications, with a single authentication process.

ERP: Enterprise resource planning