AGILE.

Multi-factor authentication

Why it is critical for businesses

Agile Underwriting Services Pty Ltd
ABN 48 607 908 243 — AFSL 483374

Cyber

Coverholder at LLOYD'S

Contents

Multi-factor authentication – why it is critical for businesses

As cyber risks continue to evolve and become more challenging for businesses, it is important that businesses are aware of ways they can reduce their risk of cyber incidents.

With the cyber insurance market hardening, insurers are now putting minimum security standard requirements on businesses, in both the SME and corporate sectors, before underwriting or renewing cyber insurance programs. Just as cyber risk evolves quickly, change in the cyber insurance landscape is happening at a frightening pace.

A security control that is now becoming mandatory for businesses is the use of multi-factor authentication (MFA) on their IT networks. This paper explores what MFA is, why it is important, and how it should be deployed and used to secure Office 365 and Remote Desktop Protocol (RDP) environments.

Businesses should discuss this paper with their IT providers and ensure MFA is set up correctly on their IT networks.

What is MFA and how does it work?

Multi-factor authentication (MFA) is a method of authentication that uses two or more factors to authenticate an individual when gaining access to a resource such as an application, online account or virtual private network (VPN). For example, in addition to using a user ID and password, use of at least one additional authentication method is required. This could be a hardware or software security token, third-party authentication applications providing time-bound, one-time codes and text messaging authentication.

Why is MFA important?

When MFA is implemented correctly it is significantly more difficult for a hacker to steal a complete set of credentials as the hacker has to provide the additional authentication methods, which are in addition to just the user ID and password to which they may already have access. MFA can help prevent some of the most common and successful types of cyber attacks, including, but not limited to:

- Business email compromise (BEC)
- Phishing
- Spear phishing
- Key loggers
- Credential stuffing
- Brute force attacks
- Man-in-the-middle attacks
- Deployment of ransomware on networks.

MFA for Office 365

Many cloud-based systems provide their own MFA offerings, including Microsoft's Office 365. Business Email Compromise (BEC) continues to be one of the most common cyber incidents for SME businesses. In almost all incidents, there is a common theme – the email account compromised by hackers has never had MFA enabled. Post breach, IT security experts tend to change the password of the compromised account and deploy MFA across a business's Office 365 email network. This begs the question, why wasn't this deployed in the first place?

Agile has launched an Office 365 Cyber Health Check to ensure businesses have a cost-effective, efficient way to understand and review their security controls for Office 365 email accounts. The Cyber Health Check helps businesses identify whether MFA is enabled on their Office 365 network and, if not, enable them to take steps to install MFA with the assistance of their IT provider. We encourage all businesses to take the Cyber Health Check and enable MFA.

Cost: $275 normally $495 inclusive of GST (Discount code: AGILEINSURANCE)

MFA for Remote Desktop Protocol

Remote Desktop Protocol (RDP) is a built-in part of the Windows toolkit popular for facilitating remote work access. With a shift to remote working during the Covid-19 pandemic, cyber criminals have taken great interest in compromising RDP endpoints as they provide direct access into a victim's environment via a graphic interface.

Statistics from Coveware, a company that provides ransomware incident response and negotiation services, firmly ranked RDP as the most popular entry point for ransomware incidents it has investigated.

Businesses should have active discussions with their IT providers about RDP and consider whether it is completely necessary for the operation of the business. If it is, implement these best practices:

1. Ensure the RDP is not internet-facing but is protected behind a VPN service.
2. Use strong passwords: Do not use default credentials, passwords that are the same as the username, or other passwords that are simple to guess. Brute force attacks due to weak passwords have resulted in numerous breaches of RDP environments.
3. Patch your systems: Ensure the latest security patches are deployed and your business has a patch management policy in place.
4. Enable MFA: Whenever possible, MFA should be enabled to ensure an additional layer of protection exists for your business.

Microsoft now makes it easy for you to add MFA to your Windows Remote Desktop. Many RDP environments also use third-party MFA solutions, particularly if their Windows edition does not support MFA for RDP.

It is critical that businesses engage with their IT providers to discuss the best practices and implement MFA on their RDP environment immediately.