MULTI-FACTOR AUTHENTICATION

MFA - Why it is Critical for Businesses

ACP
AUSTBROKERS CYBER PRO

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 a cyber incident. With the cyber insurance market *hardening*, insurers are now also placing minimum security standard requirements on businesses, both in the SME and Corporate space prior to underwriting or renewing cyber insurance programs. Just like the evolution of cyber risk, the change in the cyber insurance landscape is happening at a frightening pace.

One security control that is now becoming a mandatory requirement for businesses is the use of **Multi-Factor Authentication ('MFA')** on their IT networks. This paper will explore 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 be discussing this paper with their IT providers and ensuring MFA is set up correctly on their IT networks.

What is MFA & How Does it Work?

Multi-Factor Authentication ('MFA') is defined as a method of authentication that uses two or more authentication 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 the use of a user ID and password, the 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?

Multi-Factor Authentication ('MFA') is important, because when 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 of just the user ID and password they may already have access to. 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 ('MITM') attacks
- The 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 we see, there is one common theme, which is the email account that has been compromised by hackers **never had MFA enabled.** Post breach, IT security experts tend to not only change the password of the compromised account, but also deploy MFA across a business's Office 365 email network. This begs the question, why wasn't this deployed in the first place?

Austbrokers Cyber Pro ('ACP') have launched an **Office 365 Cyber Health Check** to ensure businesses have a cost effective and efficient way in understanding and reviewing their security controls around their Office 365 email accounts. This Health Check will assist all businesses in identifying whether MFA is enabled on their Office 365 network, and if not, allow them to take steps to enable MFA with the assistance of their IT provider. We encourage all businesses to take this Health Check and enable MFA. Information on the Office 365 Cyber Health Check can be found within our Cyber Risk Management Library **here.**

MFA for Remote Desktop Protocols ('RDP')

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 COVID19 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 the ransomware incidents that it had investigated. Businesses should have active discussions with their IT providers around RDP and should consider whether RDP is completely necessary in relation to the operation of your business. If RDP is assessed to be necessary, the following ***best practices*** should be implemented:

1. Ensure that the RDP is not internet-facing but **is protected behind a Virtual Private Network ('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 a *patch management* policy is in place within your business.
4. **Enable MFA.** Whenever possible, MFA should be enabled to ensure an additional layer of protection exist for your business.

Microsoft now makes it easy for you to add MFA to your Windows Remote Desktop. Along with this, many RDP environments still use third party solutions for MFA, especially if their Windows edition does not support MFA for RDP.

It is critical that businesses engage with their IT providers and discuss the above ***best practices*** and the implementation of MFA on their RDP environment immediately.