MULTI-FACTOR AUTHENTICATION IS NOT THE ULTIMATE ANSWER

The news is full of articles about Multi-Factor Authentication, MFA, and how it will protect against the majority of cyberattacks. Some even claim it will protect against 99% of cyberattacks.

Unfortunately, it won't. The reason MFA won't reach that level of protection is the majority of attacks fall into two categories, social engineering and exploiting bugs and vulnerabilities in operating systems and applications. Both are used to deliver malware and ransomware. MFA will not protect against either one of those.

I hear you ask, if MFA won't protect against these attacks, what do I do? Please understand, MFA is effective against specific types of attacks, and you should implement it as soon as possible.

To protect against one of the two major categories of attack, cyber bugs and vulnerabilities, keep current on software updates and implement them quickly. Test first if necessary but do not delay in implementing the updates and bug fixes. Failing to do this is just asking for trouble.

That leaves social engineering. Social engineering is an attack type that uses a message to convince someone to send confidential or non-public information. The methods include BEC, Business Email Compromise, or phishing, and other forms of social engineering such as smishing, and vishing.

Phishing is an attack technique using emails that appear to come from a company executive, regulator, attorney, government agency or other authorized party. The emails request non-public information such as user ids, passwords, social security numbers, etc. and often say that time is critical, the information needs to be sent immediately.

Vishing is a variant of phishing that uses phone calls or voice mails to deliver the same message and gives a phone number to call or a link to send to.

Smishing is a variant of phishing that uses text or SMS messages to deliver the same message. The new variants of smishing use a message saying you were inadvertently overcharged, or are entitled to a refund, or a special offer. The message says to click on the enclosed link to reply.

The messages may vary but the intent is the same, to get you to send non-public information.

If MFA will not do anything to protect against these cyberattack methods, what will help?

The answer is educating your users and providing frequent updates and desktop exercises. The more they know about social engineering the less likely they are to fall for it. If users are the target of many of the successful attacks, then educating users is the way to protect against those attacks.

Do not put it off, do not delay, and certainly do not think that education is a one-time event. Attack methods evolve quickly. Keeping software and users up to date is essential to protect your data and your company.

Want to learn more about cyber security and education, contact AIM Cyber at info@AIMglb.com or call (888) 773-1920.