Multi-Factor Authentication - An Update

cyber security risk management MFA

Summary: The FBI recently warned of attacks that bypass multi-factor authentication (MFA). Is MFA still a good solution?

Pew Research finds about 27% of people have not read a book (in print, in part, in whole, audibly, or electronically) in the past year. It seems though that the more money you make, the more you read, as the percentages go up for that group.

No matter what you have or have not read recently, it makes sense to do so, when it comes to cyber security. There are so many threats now, and hackers continue to evolve. Some protections still work well, like multi-factor authentication (MFA), but they are not infallible. Today we want to share a heads up from the FBI to help community financial institutions (CFIs) and your business customers better prepare.

Recently, the FBI warned of a rise in attacks that bypass MFA solutions. Specifically they highlighted sim-swapping and vulnerabilities in web pages that process MFA operations. Because these methods can have devastating consequences, we review how they work and detail some strategies to limit impact.

SIM swapping is when an attacker gets control of a victim's phone number by switching it to another device via a SIM card. The attacker employs social engineering by calling the phone company to complete the SIM swap. Then, when the attacker contacts the bank, their system recognizes the phone number allowing the attacker to authenticate via SMS. Given full control of the account, you can imagine the consequences.

So what can be done? In the cases the FBI described, bank employees did not ask unique security questions, so reviewing procedures and monitoring is important. You may also want to explore more robust technical solutions that identify a customer's phone number and device. Speak with your IT department or other providers about these developments, and recheck the provisions and reporting mechanisms you have in place.

Yet another bypass method involved an attack which took advantage of a flaw in a bank's website. The attacker first signed in with stolen credentials. Then, when a second page came up requiring a PIN, the attacker manipulated the Web URL. This action allowed the hacker's computer to become the one recognized on the account and bypassed the pages asking for the PIN and security questions. Make sure to pass on this use case to your IT team to ensure your site isn't vulnerable.

Is there any good news? Yes. The FBI says MFA is still important and effective. Microsoft and Google agree and they see hundreds of millions of attacks a day. They say MFA is highly effective, as high as 99% in automated account hacks.

Financial institutions should keep exploring stronger MFA solutions that do not use SMS authentication. Likewise, you can nudge customers to change their passwords more frequently. Some of these strategies may cause friction for customers, so educating them on these risks and how you keep their accounts safe is always a good practice. As the FBI points out, these attacks are still somewhat rare, but they demand you keep your eyes wide open.

INTERNATIONAL SERVICES TO GROW WITH YOUR CUSTOMERS

Our international services are designed to help you capture more customers and increase fee income. Contact us today for more information.