THE
NATIONAL LAW REVIEW

Closing The Door Behind Your Multi-Factor Authentication Implementation

Thursday, March 21, 2019

I came across an article last week that indicated there was a successful attack on Microsoft's Office 365 and Google's G Suite environments that was able to bypass multi-factor authentication (MFA). However, after reading the article it was immediately clear the attack leveraged an old protocol, IMAP (Internet Message Access Protocol), which does not support MFA. So, yes, technically the hackers bypassed MFA, but I personally wouldn't say they beat MFA. This got me thinking about several reports I have seen lately that seemingly imply that hackers have found ways to successfully beat MFA. While each case that I read was unique and maybe technically accurate, it seemed to me that in each instance what the hackers actually beat was a deficiency in the implementation of MFA.

Robinson+Cole

Article By Robinson & Cole LLP
Sean Lawless
Data Privacy + Security Insider

Communications, Media & Internet
All Federal

There are number of legacy protocols that do not support MFA. Microsoft Outlook prior to the 2013 version does not support modern authentication. Therefore, if your organization is still running Outlook 2010 you have RPC (Remote Procedure Call) over HTTP-enabled. As with IMAP, it doesn't support MFA. While a user may be required to use MFA to access their webmail (Outlook Web Access), any hacker with a copy of Outlook 2010 can access that user's email account with a phished user name and password, thus bypassing MFA.

Another article claimed hackers had bypassed MFA, but the details indicated the attack was launched from the victim's internal network. It is extremely common for organizations to systematically bypass MFA when the authentication request originates from the organization's internal network. Another article seemed to indicate that the hacker used account credentials for an account with which MFA was not required, like a service account. It is very common for organizations to use membership to a directory group as the basis for requiring MFA. This is done in order to control the implementation of MFA to the organization.

All of these instances indicate that many organizations are not closing the door(s) after implementing MFA. Every organization should consider reviewing enabled legacy protocols, making risk-based decisions on requiring MFA on network, and updating MFA configuration to be required by default unless specifically excluded as opposed to specifically included. Has your organization closed the door?

Source URL: https://www.natlawreview.com/article/closing-door-behind-your-multi-factor-authentication-implementation