#ForensicPerspectives

Top 10 ways to enhance MFA

Got MFA? Great! But it doesn't mean that the risk of a cyber breach has been eliminated. Here are 10 ways to reduce such risks further…

While the deployment of multi-factor authentication ("MFA") can reduce the risk of a cyber breach by requiring at least two forms of identification to access corporate systems, the mere act of deploying MFA does not eliminate such risk: threat actors have identified ways to bypass less sophisticated implementations of MFA, and/or have successfully exploited other vulnerabilities to gain access.

Based on our experience responding to thousands of cyber incidents, we have summarized practical, tactical steps to enhance the efficacy of a company's MFA deployment and further strengthen its overall information security environment:

01 **Determine which applications can be MFA-enabled.** By risk-ranking applications in use, organizations can make decisions on how to reduce opportunities to gain access to the network.

02 **Find the right MFA tool for your organization.** Employing a formal software selection methodology and confirming the fit can be critical to achieving the business case objectives.

03 **Reduce the risk of accounts being exploited.** Replace text message or email-based MFA with a secure authenticator app to reduce the risk of accounts being exploited.

04 **Make MFA a standard job responsibility.** Reward those who follow the process, and identify, educate, and hold accountable those who try to bypass the process.

05 **Control and monitor MFA disablement.** The ability to turn off MFA should be carefully controlled, and notifications should be generated and monitored whenever such activity occurs.

06 **Implement a zero-trust security model.** Zero trust requires verification from all devices and users trying to access any corporate systems. In parallel, access is further restricted so that even verified users can access only those systems, websites, and files necessary to perform their job functions.

07 **Transaction due diligence.** When performing preacquisition due diligence, understanding their layered defenses and whether and how they use MFA is critical. Validating that a common MFA platform has been deployed across the organization will assist the information security team with proper monitoring and protection.

08 **Remove legacy systems.** By eliminating legacy systems which have inherently poor security, companies can further reduce the attack surface of their software environment, making it more difficult for crime syndicates to discover and exploit vulnerabilities, and reducing the burden on existing information technology and security teams.

09 **Patch internal and internet-facing applications and operating systems in a timely manner.** Software bugs are often discovered in the days, weeks, or months after deployment. Any delays in deploying patches to remediate bugs could compromise security and put the organization at significant, incremental risk.

10 **Monitor information security risk from vendors and trusted business partners.** Consider designing and deploying a risk-based approach to monitoring the ongoing – and ever-changing – risks associated with the underlying business relationships, including requiring them to use MFA, where appropriate.

Kristofer Swanson, CPA/CFF, CFE, CAMS | Vice President and Practice Leader, Forensic Services
+1-312-619-3313 | kswanson@crai.com

Aniket Bhardwaj, GREM, GCIA, GNFA, GCFA | Vice President, Forensic Services
+1-416-323-5574 | abhardwaj@crai.com