Codify
BY AAPC

Health Information Compliance Alert

Toolkit: Get the Scoop on Brute Force Attacks

Tip: Use MFA and password controls to combat issues.

There's no denying that COVID-19 isn't going away anytime soon. What's more, cyber criminals are using the pandemic to target remote workers, spread misinformation, and disrupt a myriad of industries, including healthcare.

Background: In addition to a plethora of releases from **Department of Health and Human Services'** (HHS) auxiliary agencies, the **Federal Bureau of Investigation** (FBI) and the **Cybersecurity and Infrastructure Security Agency** (CISA), **Interpol** has also announced signs that cyberattacks are spreading across the globe, particularly to circumvent COVID-19 relief and care efforts.

"An Interpol assessment of the impact of COVID-19 on cybercrime has shown a significant target shift from individuals and small businesses to major corporations, governments and critical infrastructure," cautions an August 4 release. "With organizations and businesses rapidly deploying remote systems and networks to support staff working from home, criminals are also taking advantage of increased security vulnerabilities to steal data, generate profits and cause disruption," Interpol says.

Plus: Reports suggest an increase in brute force attacks, too, which is worrisome. This kind of infiltration is best defined as a cyber-hijack that involves "brute force," breaking systems by repeatedly trying different passwords until finding one that finally works. Once the encryption is compromised, the hackers can take down the system.

"Brute force attacks are a concern for any system that uses passwords as the sole authenticator. This is true for remote desktop, VPN [virtual private network], cloud-based systems, or anything else connected to the Internet," warns **Adam Kehler, CISSP,** principal consultant and healthcare practice lead with **Online Business Systems**.

Pocket This Expert Insight to Thwart Attacks

Cyber criminals often use the same tactics over and over to force their way in an organization's system and cause digital mayhem. Fortunately, "many systems these days have protections in place to protect against brute force attacks," Kehler says. Read on for tips to circumvent cyberattacks with better password management and ensure your remote work is safe and secure.

Institute rate limits: A great way to monitor for brute force attacks is by setting reasonable rate limits that restrict the number of times a remote user can attempt to log into your practice's system, suggests Kehler. "For this reason, the most popular attacks against passwords these days involve password re-use and common passwords," he explains.

Watch for credential stuffing: Another thing to avoid is using a password that's already been compromised in a breach, which makes it easier for hackers to invade your system. "Password re-use attacks, or credential stuffing, involve taking a user's credentials from a data breach and trying that same password on another system," Kehler instructs. Additionally, this is a serious issue for remote work when the lines between work and home become blurred. Credential stuffing "takes advantage of the fact that many people use the same password for multiple systems, both personal and business," he cautions.

Beware password spraying: "Common password attacks - password spraying -take a few popular passwords and 'spray' them across many user-IDs," Kehler admits. Using multifactor authentication (MFA), requiring complex

passwords, and training staff on best security practices are critical to sidestep password spraying.

Be on the lookout for phishing: Social engineering is on the rise and remains an ongoing COVID-19 issue for many healthcare organizations (see Health Information Compliance Alert, Vol. 20, No. 6). Unfortunately, "phishing attacks are [also] extremely effective at harvesting users' passwords," Kehler acknowledges.

However, Kehler advises that training is a top tool to stop phishing from becoming a problem for remote staff. "Organization[s] should be conducting regular phishing exercises and training to help users recognize phishing attacks. As much as possible, the organizations should be providing tools and systems that keep ePHI [electronic protected health information] off of the end-user's systems and within the confines of the server environment," he counsels.

Reminder: As the pandemic evolves, you may need to revisit your VPN controls and remote work policies often. A comprehensive risk analysis is essential to see understand your firm's weaknesses and to address them with risk management and staff training. Your end game should always be to not only secure your organization's data but to also protect your patients' welfare and safeguard their ePHI.

Resource: Read the Interpol report at www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19.