MULTI-FACTOR AUTHENTICATION

APRIL 2021

Multi-factor authentication (MFA) is a layered approach to securing data and applications where a system requires a user to present a combination of two or more credentials to verify a user's identity for login. MFA increases security because even if one credential becomes compromised, unauthorized users will be unable to meet the second authentication requirement and will not be able to access the targeted physical space, computing device, network, or database.

WHY SHOULD HEALTHCARE ORGANIZATIONS BE INTERESTED IN MFA?

Implementing MFA makes it more difficult for an adversary to gain access to business and clinical systems, such as remote access technology, email, and billing systems, even if passwords are compromised through phishing attacks or other means.

Adversaries are increasingly capable of guessing or harvesting passwords to gain illicit access. Password cracking techniques are becoming more sophisticated and high-powered computing is increasingly affordable. In addition, adversaries harvest credentials through phishing emails or by identifying passwords reused from other systems. MFA adds a strong protection against account takeover by greatly increasing the level of difficulty for adversaries.

HOW DOES MFA WORK?

MFA requires system or network users to present two or more credentials at login to verify their identity before they are granted access. Each additional authentication factor added to the login process increases security. A typical MFA login would require the user to present some combination of the following:

- **Something you know:** like a password, Personal Identification Number (PIN), or answers to security questions;
- **Something you have:** like a smart card, mobile token, or hardware token; and,
- **Some form of biometric factor** (e.g., fingerprint, voice recognition).

For example, MFA could require users to insert a smart card ID into a card reader (first factor) and then enter a password (second factor). An unauthorized user in possession of the card would not be able to log in without also knowing the password; likewise, the password is useless without physical access to the card.

The added security offered by MFA can simplify the user login process by using single-sign on where practicable. A single sign-on system enables authenticated users access to an environment from which they can use multiple covered applications without needing to log in separately each time.

Consider deploying MFA capabilities to Internet-facing systems, such as email, remote desktop, and Virtual Private Network (VPNs). Implementation schedules, costs, adoption willingness, and the degree of protection provided vary depending on the solutions selected and the platforms to be protected, so match the capability to the need.

If you have questions or suggestions regarding this product, please feel free to contact CISA Central at central@cisa.dhs.gov and reference the Multi-factor Authentication document in the subject line.