NEXT GEN IDENTITY MANAGEMENT

Multi-Factor Authentication

CENTRIFY'S GREG CRANLEY AND DAVID MCNEELEY ON MULTI-FACTOR AUTHENTICATION AND ITS ROLE IN CYBER BREACH PROTECTION

The idea behind multi-factor authentication is to have something different than a username and password, ideally something you have in addition to something you know.

"What has been proven in the last several years to be the root cause of all breaches – every data breach that we've had in the last several years, including the Office of Personnel Management breach – was caused by someone stealing a user ID and password," said Greg Cranley, vice president of federal and public sector sales for Centrify. "So multi-factor authentication provides an opportunity to use a physical digital credential along with something only the user knows and or has in their possession, employing the concept of something you have and something you know."

"Multi-factor authentication provides an opportunity to use a physical digital credential along with something only the user knows and or has in their possession, employing the concept of something you have and something you know."

Cranley said it is very difficult for a thief or hacker to gain access to two or three representations of a user. It would be difficult to separate the two or three representations with this approach because you are talking about people and physical items.

"It can be very diverse in the way you accomplish that, but it can be done and it proves to be very successful in securing one's identity and therefore their access to their resources," he said.

From a technical perspective, David McNeely, vice president of product strategy for Centrify, said there are many different ways to provide authentication for a user.

"When a user types a password, it's just something that he knows, but the challenge being that he's typing it in on a keyboard that other people might be able to observe," McNeely said. "For example, if you unlock your phone and type in a four-digit passcode, it's pretty easy for an attacker to watch you type in the four-digit PIN, then later swipe your phone, type the discovered passcode and gain access. That's why we moved to biometrics with a much longer passcode on modern phones because it's harder to bypass the biometric.

Centrify®
THE BREACH STOPS HERE™

"Similarly, for access to computers, we want to make that harder for bad guys to be able to break into your account. And if we can introduce another form factor, whether it's something that you have like a smart card, Common Access Card (CAC) or Personal Identity Verification (PIV) card, or a token that has a number that will change periodically on it – a one-time password – that makes it much more difficult for a bad guy to break into your account."

But how much more secure will that make users? The impact is significant, McNeely said.

"We look at different authentication factors as various levels of assurance," he said. "The National Institute of Standards and Technology (NIST) has a document, SP 800-63 that's currently going through a revision. The document describes the various Levels of Assurance for authentication and there is a difference between just a password that's at Level of Assurance 1. If I have a one-time password, a device that has a number that changes periodically, that's Level of Assurance 2. If I have a smart card, it actually contains a public and private key pair and certificate that's been signed by an authoritative system. It is typically issued by a badging officer and that gets you to Level of Assurance 3 or 4, depending on how strong the cryptography is inside the device."

Cranley concluded the opportunity with multi-factor authentication is to connect it with user access.

"The ability to have multi-factor authentication and to be able to devise exactly what access people have is extremely important, so that you can maintain exactly who has access to what and how much access they have. That is an imperative for all federal agencies," he said. "Given the value of information stored by an organization and the enormous risk surface organizations have today, there is a scary threat environment that bad operators want to exploit for many reasons. Whether it is foreign nationals, other countries or individuals, it does not really matter. There are people that want ill-gotten goods and we have created a large landscape of opportunity for them. Multi-factor authentication will slow them down quite a bit." ●