NEXT GEN IDENTITY MANAGEMENT

Maintaining Good Cyber Hygiene Starts with Identification, Access Management

CENTRIFY'S GREG CRANLEY AND DAVID MCNEELEY IDENTIFY STEPS AGENCIES CAN TAKE TO ENSURE THE RIGHT PEOPLE HAVE ACCESS TO THE RIGHT INFORMATION

With countless daily attempts to hack federal networks a reality for cybersecurity managers, access to reliable detection and mitigation techniques are essential. Federal managers must balance providing critical services to taxpayers with protecting network systems and information from malicious actors whose attack methods grow more complex by the day.

The Department of Homeland Security's (DHS) says it designed its Continuous Diagnostics and Mitigation (CDM) program to provide "federal departments and agencies with capabilities and tools that identify cybersecurity risks on an ongoing basis, prioritize these risks based upon potential impacts, and enable cybersecurity personnel to mitigate the most significant problems first."

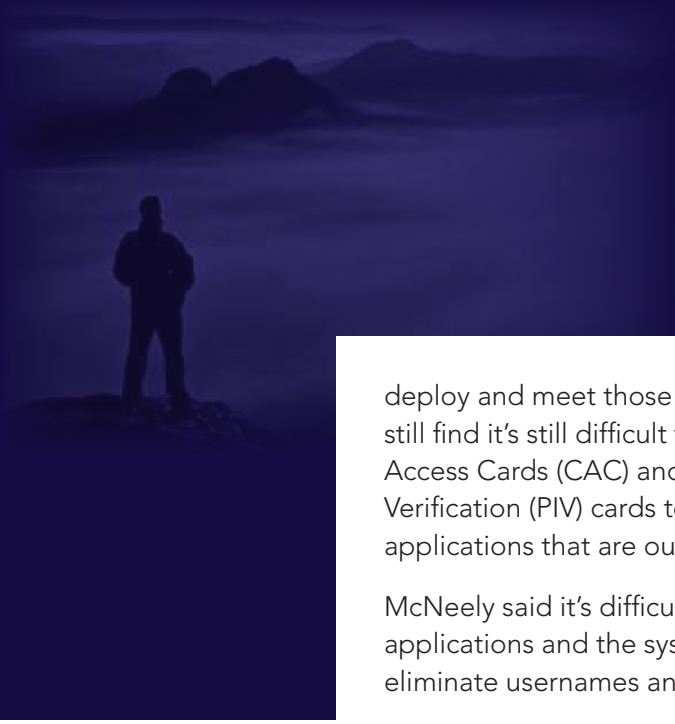
David McNeely, Centrify's vice president of product strategy, said the CDM program aims to accomplish several goals, "the biggest one being to make sure that organizations have the correct people gaining access to resources and infrastructure. Also, to prevent breaches that we've seen in the news and to make sure that organizations have secured their systems and know exactly who's on the network and who's gaining access to those resources."

Greg Cranley, Centrify's vice president of federal and public sector sales, agreed and added the issue comes down to identities and access.

"I think the goal is to ensure every agency has a level playing ground of security and how they're defending their environments," he said. "Because they've seen in the past, as David referenced earlier on the cybersecurity attacks, compromised identities have been the number one thing. The idea is to create various phases that will look at different areas to ensure that everybody at least has this level of capability."

McNeely also touched on managing identities and access for each user on the network.

"I think if you look at the fundamental goals of the program, one of the things that was created was Homeland Security Presidential Directive 12 (HSPD-12)," he said. "The goal of that was to make sure you had a strong credential for every person that needed to gain access to a resource. But the actual implementation is fairly difficult for most organizations if they don't have a strong information technology staff. The goal was to put together best practices and standards and preselect solutions in order to help those agencies



deploy and meet those requirements. We still find it's still difficult to use Common Access Cards (CAC) and Personal Identity Verification (PIV) cards to output to all of the applications that are out there."

McNeely said it's difficult to integrate the applications and the systems, and also to eliminate usernames and passwords.

"When we look at the industry as a whole, the software developers make an assumption about the authentication mechanism – I can put up a form and ask you for a user ID and a password," he said. "That's pretty simple. But most software developers don't really understand how to set up applications and computer systems. Especially the client server in the way that people are starting to move to cloud-based systems and actually use smart cards and strong credentials as a way to authenticate to those systems.

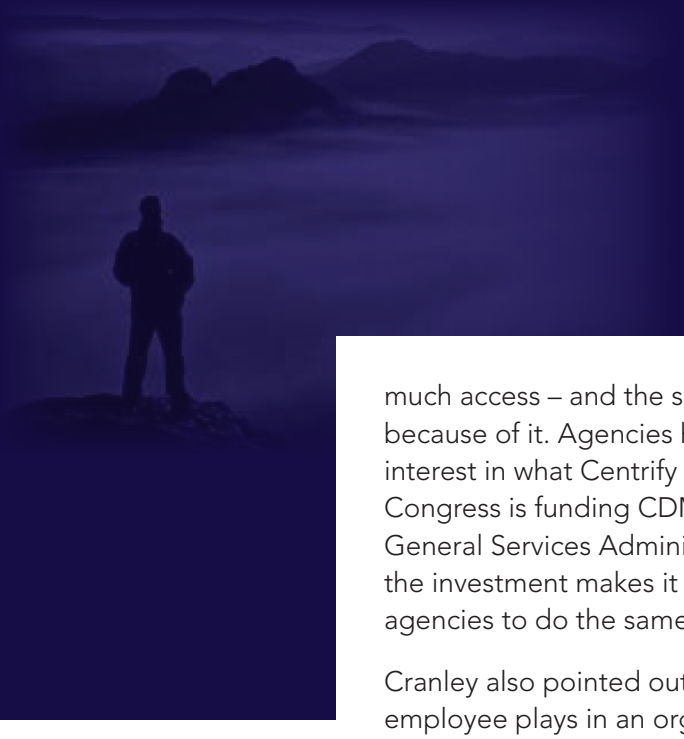
"The challenge is really enabling people to use that stronger credential for multifactor authentication and then use it across everything they need to gain access to."

Despite DHS' efforts to assist agencies with their cybersecurity, Cranley said agencies are slow to implement the CDM program and are missing out on the opportunities of how it can help them secure their networks and data.

"Sometimes it's a lack of participation," he said. "I don't think they understand that Congress has funded this and they can get these tools, which are the best tools, that not only accomplish what CDM wants to accomplish, but it also accomplishes many other goals that the National Institute of Standards and Technology (NIST) and the Office of Management and Budget (OMB) put forth on securing the environment. Despite Congress funding it and providing agencies the opportunity to access these great tools, the agencies don't always take advantage of it quickly. And it's kind of perplexing."

Within CDM's Phase 2 (Least Privilege and Infrastructure Integrity), Centrify has a particular interest in the Credentials and Authentication Management (CRED) portion.

"We've had great success in the federal government and our capabilities to address what David referred to as the heterogeneity of every environment," Cranley said. "Think about how many user IDs and passwords you have in your own life. Data centers and organizations suffer that, so all the users in the workplace have the same issue. Too many passwords and too



much access – and the security suffers because of it. Agencies have a great interest in what Centrify does and since Congress is funding CDM through the General Services Administration to support the investment makes it easy for the agencies to do the same."

Cranley also pointed out the role each employee plays in an organization's overall security effort. Whether rank-and-file employee, middle manager, or top executive, everyone has an access point into the network.

"I don't think they consider themselves as being targets," he said. "They think that's for other people and consider cybersecurity to be an issue for someone higher on the organizational chart. But because we rely so much on technology to do our jobs, no matter what your job is, you're going to have access to the network and a lot of data. And if malicious actors can get your credentials, then they are in the network. Not only that, we also give employees mobile devices they can take out the door."

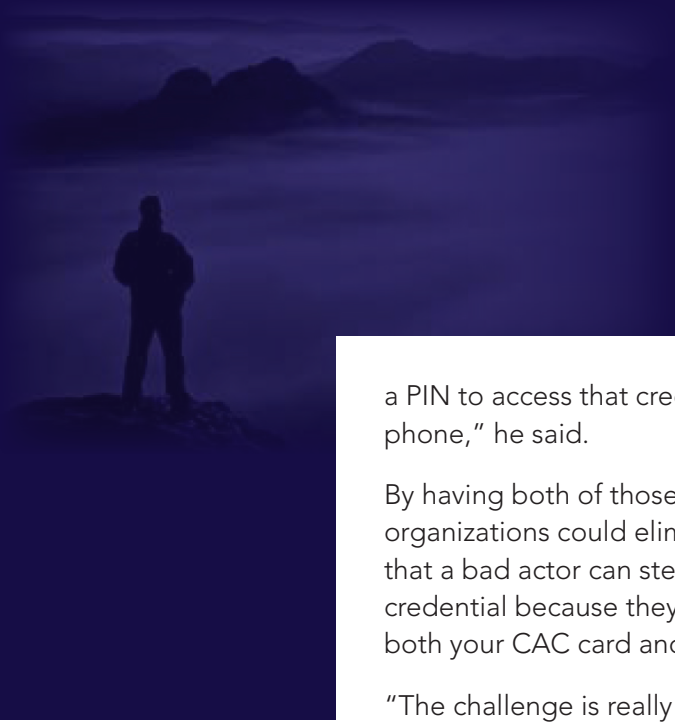
"From a security perspective, everyone needs to do a better job of protecting access to the information and assets they have available to them. Making it easier for people to adopt multifactor authentication and single sign-on makes it easier for IT and the securitystaff to be able to enforce policies they have been trying to put in place for many, many years."

To help agencies stay in front of the situation, Centrify has created a technical solution to meet the CRED task order requirements.

"The first thing most organizations need to do is consolidate the number of accounts that a single person has," McNeely said. "We view that as going around to all the computer systems and the applications and consolidating identities into one single repository. Or as the CDM calls it, a Master User Record. Once you have that single Master User Record for the person, then you can go back and more intelligently grant that person access to various computer systems. One of the things that we help to do is establish strong authentication. In other words, leverage the CAC or PIV card authentication at the desktop and enable the usage of that credential to gain access to these systems and applications so we can then eliminate passwords that are used throughout the environment."

McNeely said the goal is to enable people to get multifactor authentication.

"Something you have in your hand – the CAC or PIV card, or mobile device if it has a derived credential on it – and something you know – a PIN to unlock that CAC or PIV card, or a fingerprint on your phone or



a PIN to access that credential on the phone," he said.

By having both of those, McNeely said organizations could eliminate the possibility that a bad actor can steal an employee's credential because they would have to steal both your CAC card and the PIN.

"The challenge is really enabling people to use that stronger credential for multifactor authentication and then use it across everything they need to gain access to," McNeely said.

Cranley added that the user experience is critical to widespread adoption and implementation of any technology.

"If you make security hard, people work will work very diligently to circumvent that," he said. "We talk a lot about single sign-on, which makes it easy for the user to access the applications he's authorized to use. If I can insert my CAC or PIV card into the computer and log in, I expect to be able to use that same mechanism to gain access to the other applications. And not necessarily be challenged to type in another password or enter another credential every single time I go to a different application. So part of this is establishing a stronger way for the user to authentication, initially, but then reusing that as a way to gain access to other things. Single sign-on it makes it a lot easier for the user."

Both Cranley and McNeely are excited about the CDM program and how it can help agencies in the future.

"I think it's a great initiative," Cranley said. "I'm grateful the new administration has not changed it. I'm hopeful people understand it better and utilize the technologies that are offered to them."

McNeely added, "From a security perspective, everyone needs to do a better job of protecting access to the information and assets they have available to them. Making it easier for people to adopt multifactor authentication and single sign-on makes it easier for IT and the security staff to be able to enforce policies they have been trying to put in place for many, many years." ●