ENTERPRISE OUTLOOK

SPONSORED REPORT FCW

Identity and Access Management

Boost Cybersecurity with Identity as a Service

Identity and access management is critical to the success of government digital initiatives.

People are always the weakest link in security, but the stakes are higher now because of the massive amounts of sensitive information accessible online and the determination of cyberattackers. The standard username/password approach is no longer enough. Passwords are easy to breach, and when people use the same one for multiple accounts, a successful hack of passwords in the commercial sector can spill over into government agencies.

In a recent IDG survey sponsored by Okta, only 30 percent of IT and security leaders said they had a good or better ability to detect when passwords have been compromised.

Verizon's 2017 Data Breach Investigations Report states, "If you are relying on username/e-mail address and password, you are rolling the dice as far as password re-usage from other breaches or malware on your customers' devices are concerned." The report also states weak or stolen passwords were involved in 81 percent of all breaches in the past year. Verizon's 2016 report found that 91 percent of attacks targeted credentials.

Hackers famously gained access to valid user credentials to breach the Office of Personnel Management's (OPM) network and steal sensitive personal information of more than 20 million Americans in 2015. The attack was aided by the fact that the agency didn't use two-factor authentication for workers who accessed the system remotely.

In a recent IDG survey sponsored by Okta, only 30 percent of IT and security leaders said they had a good or better ability to detect when passwords have been compromised. The situation is further complicated by the growing use of cloud-based applications and services because resources are no longer entirely on premises. And given the explosion in bring-your-own-device work environments, many security experts are now saying that identity is the new network "perimeter."

It's no wonder that 91 percent of those surveyed by IDG said identity management was critical or very important to the success of broader digital initiatives. Some agencies have already begun to think about securing their enterprises beyond username and password. They plan to focus on strong authentication and restricting what a user can access based on his or her role.

A key challenge is the government's traditional inability to quickly make use of new technologies. Fortunately, cloud-based identity solutions are helping agencies deploy new security tools and authentication options as soon as they become available. "The cloud-based model is prevailing because of the ease of deployment for administrators—and the ease of use for employees," says Eric Karlinsky, director of technical marketing at Okta.

A central tenet of strong IAM is multi-factor authentication (MFA), which thwarts credential-based attacks by combining two or more factors from the list of something users know (such as a password), something they have (such as smart card) and/or something they are (a biometric identifier). MFA is more secure, but it can cause friction for users, who might view it as a roadblock to productivity. Adaptive multi-factor authentication can potentially help ease that friction.

"Adaptive MFA allows administrators to avoid prompting the end user for multi-factor authentication if the context of their request is normal for them or if it looks like something that falls within your security constraints," says Karlinsky. For example, MFA might not be required if a user is logging in from a location the system recognizes, but if he or she logs in from an unusual location, the system might require the use of a second authentication factor.

An IAM system can also streamline the user experience by linking an individual's attributes across multiple identity management systems. Single sign-on is a subset of that approach. And agencies aren't just applying it to employees. They're also recognizing the value of using SSO to give external partners and citizens access to online resources.

"Single sign-on is often described as a very simple use case: Can people use it to get access without using their passwords again?" says Karlinsky. "But we think there's a lot more to some of the latest developments."

For example, an SSO dashboard that lets users seamlessly log in to all their applications could also simplify other activities by helping them securely store notes or passwords for personal applications or by giving administrators the opportunity to improve user productivity. And as SSO evolves, it both facilitates and relies on automation.

"You can't log in to an application if you don't have an account, so what's really important for single sign-on is automating the creation of those accounts and the provisioning of those accounts with the right entitlements to the right applications," says Karlinsky. And those entitlements should be automatically updated when employees' roles change or they leave the organization.

Mobile access is another piece of the puzzle. Andrew Whelchel, senior sales engineer at Okta, advises agencies to look for IAM platforms that can support both the traditional web-based protocols and mobile SSO technology. The search for solutions that are easy to use, flexible, and comprehensive is bringing many agencies to cloud-based IAM, or Identity-as-a-Service. This approach is also well-suited to citizen-focused activities because it can expand and contract depending on sporadic demands or spikes tied to a particular time of the year, such as tax season.

Customer satisfaction with the sign-on process should be a key concern. "If you think about employees as having a short attention span or a low level of tolerance for user friction, multiply that by 10 for citizens," says Karlinsky. "They can walk away and choose not to use the service. So a high-quality end-user experience and a very fast on-boarding capability are really important."

IAM gives agencies the freedom to focus on building the service they want to provide to citizens, while benefiting from the vendor's security and identity expertise. The best solutions let agencies aggregate authorization accounts into a central repository where they can be more easily managed. Integration with other applications is also essential for striking a balance between security and ease of use. That means having connectors from the IAM system to on-premises and cloud-based applications as well as VPN infrastructures.

As IAM continues to evolve to meet the challenges of identity in an increasingly digital world, Whelchel believes individuals will eventually have more ownership over their credentials. "There are standards coming now, such as the FIDO Alliance's U2F, where you can take your identity with you," he says. "You could bring your own multi-factor authentication to whatever services you need, whether they were issued through your employer or a digital government service."

And Karlinsky predicts a strong future for biometric multi-factor identity management. "Biometric investments—combined with remote, low-friction identity proofing—are going to open the doors to more secure employee and citizen services."

> **"You can't log in to an application if you don't have an account, so what's really important for single sign-on is automating the creation of those accounts and the provisioning of those accounts with the right entitlements to the right applications."**
>
> **—Eric Karlinsky,** director of technical marketing at Okta

Okta is the leading independent provider of identity for the enterprise. The Okta Identity Cloud connects and protects employees of many of the world's largest enterprises. It also securely connects enterprises to their partners, suppliers and customers. Okta helps customers fulfill their missions faster by making it safe and easy to use the technologies they need to do their most significant work.

For more information, please visit: okta.com

okta