PROVIDING STRONG TOOLS TO BOLSTER PASSWORD SECURITY AND RELATED CONTROLS

A human-centric password security and management platform protects state and local governments by closing some of the biggest holes in their cybersecurity armor.

Introduction

People often speak of cybersecurity as a technology challenge. But protecting data and IT infrastructure is also very much a matter of human behavior. Eighty-five percent of data breaches involve a human element, according to the Verizon Business 2021 Data Breach Investigations Report.[1] When state and local governments fall victim to ransomware, data theft or other attacks, bad actors often gain access through weak spots created by unsafe cybersecurity practices.

Often, those weak spots involve passwords. At least 65 percent of people use duplicate passwords on multiple sites, and 48 percent of employees use the same passwords for personal and work-related functions.[2] Even when employees understand how to deploy strong passwords, if the organization does not enforce careful habits, those rules can get lost in the shuffle of day-to-day work.

To turn good intentions into safe behavior, agencies need to give users tools that support consistent password practices. A human-centric, easy-to-use Enterprise Password Management (EPM) platform bolsters security by reducing the chance of human error.

Holes in the security net

State and local governments deploy a wide range of cybersecurity technologies on their networks. Those safeguards are important, but they don't provide complete protection. Often, common human behavior creates serious vulnerabilities.

"Almost everyone has too many online accounts and too many passwords to keep track of and secure," says Deborah Snyder, a Center for Digital Government senior fellow and former chief information security officer (CISO) for New York State. "Having to remember multiple passwords usually results in writing them down, using the same password across different accounts, or linking accounts — things that you definitely do not want people to do."

Also, users may choose weak passwords, or share passwords with coworkers or family members. All those practices increase the risk of unauthorized access to a government network.

The cyberattacks and data breaches that result may interfere with operations and trigger regulatory compliance issues, financial penalties, legal liability, reputational harm and damaging media coverage.

Hybrid work environments, with employees working remotely some or all of the time, increase the risk that human error will cause a breach. Users working from outside the office may employ personal devices or use poorly secured home networks to access government infrastructure.

Of course, many government organizations train employees on the principles of password management. "Clear policy and training set expectations, let people know what they should or shouldn't do, and what their responsibilities are," Snyder says. Good training also encourages users to contact the security team without fear of getting in trouble, if they think they have accidentally allowed a breach, she says.

But no matter how thorough the training, all too often, busy employees are apt to fall back into expedient, unsafe habits.

When it comes to cybersecurity, the best defense against human error is a strong, well-integrated, highly automated password management system.

Features to look for in an enterprise password management solution

To reduce the risks posed by human nature, a password management system should promote safe practices without creating extra work for end users or administrators. Specifically, the solution should:

Provide a secure place to store passwords on a device or in the cloud. When a system stores all passwords in a secure vault, there's no chance that any of those passwords will be compromised. "An encrypted password vault creates and stores varied, strong passwords for all the sites and applications you use, so you don't have to remember a long list of passwords," says Snyder. "The password management and security platform may also store and encrypt metadata and files, which are targeted assets by cybercriminals."

Supply passwords when needed without requiring any action by the user. Since the user doesn't need to remember a password in order to use it, there is never a temptation to create weak passwords.

Take a Zero-Trust and Zero-Knowledge approach. Zero Trust means that the system takes nothing for granted. Every time a user tries to access an area or application, the system verifies the person's identity and confirms they have permission for the action they are trying to take. Zero Knowledge means that the only person with knowledge about a password is the person who created it — the software vendor doesn't have knowledge of or access to your passwords or encryption keys. Person A can still lend a password to Person B to log into an application or site, but the password will be masked: Person B won't know what it is.

Provide randomly generated passwords for users who prefer them. When a system includes a simple tool to generate a password on request, and then save it in its secure vault, the chance of creating a weak password or inadvertently giving it to a cybercriminal drops to zero.

Detect duplicate passwords and bar their use. When users create passwords manually, a strong password management system will alert a system administrator any time someone tries to use the same password more than once. The administrator doesn't see what the password is; they simply get notified about the duplication so they can tell the user to choose a different password.

Let administrators monitor and control the use of multi-factor authentication. With fine-grained access controls, administrators can set employees' permissions to require two-factor or multi-factor authentication for every password used, or every website accessed, depending on the rules they have established. They can also monitor every aspect of each user's activity — what sites they go to, how often they go there, and from what locations or devices they access those sites.

To avoid the disruption of a ransomware attack or other breach, governments need to make password management and security easy, automatic and foolproof.

Integrate with single sign-on solutions to make them more effective. One effective approach is to implement an encryption key management application that runs on premises, on a physical or virtual server. This application enhances the security and functional capabilities of a single sign-on identity system by adding a powerful password management solution at the back end. This allows the SSO solution to integrate with native and cloud-based applications (whether or not SAML 2.0 compliant) and provides full end-to-end encryption, in addition to authentication.

Provide customizable reporting and alerting and/or integrate with popular security information management (SIM) solutions. This allows you to know whether any user — be it an employee or a contractor — has been compromised.

Allow sharing of records, securely, for collaboration in hybrid and distributed work environments. Since passwords are masked, users can allow colleagues to use them without revealing what they are.

Be compliant with important security standards such as NIST 800-63, FedRAMP, SOC 1/2/3, FIPS 140-2, ISO 27001.

Include unlimited training and support as part of the subscription. Once employees are trained to use a new password management system, some of them might need a refresher course a few weeks later. And as new employees join the enterprise, it's important to get them up to speed on the system as well. A subscription that includes unlimited training and support, with one customer service representative assigned to your account, ensures the enterprise can get maximum benefit from the solution.

Conclusion

Cybercriminals who attacked the Colonial Pipeline with ransomware in spring 2021 reportedly accessed that company's network through a single compromised password.[3] To avoid that kind of disruption, governments need to make password management and security easy, automatic and foolproof. A human-centric enterprise password management solution and security platform is essential in mitigating the risk of ransomware attack or data breach. A Zero-Trust security framework and Zero-Knowledge security architecture takes human error and insider-threat risk out of the cybersecurity equation, which is critical to protect state and local government networks.

Endnotes

1. *'Cybercrime thrives during pandemic: Verizon 2021 Data Breach Investigations Report," press release, May 13, 2021, https://www.verizon.com/about/news/verizon-2021-data-breach-investigations-report*
2. *Dan Lohrmann, "Email Security, Working from Home and World Password Day," Government Technology, May 2, 2021, https://www.govtech.com/blogs/lohrmann-on-cybersecurity/email-security-working-from-home-and-world-password-day*
3. *William Turton and Kartikay Mehrotra "Hackers Breached Colonial Pipeline Using Compromised Password," Bloomberg News, June 4, 2021, https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password*

This piece was written and produced by the Center for Digital Government Content Studio, with information and input from Keeper Security.

Produced by: CENTER FOR DIGITAL GOVERNMENT

For: KEEPER Cybersecurity Starts Here®

The Center for Digital Government, a division of e.Republic, is a national research and advisory institute on information technology policies and best practices in state and local government. Through its diverse and dynamic programs and services, the Center provides public and private sector leaders with decision support, knowledge and opportunities to help them effectively incorporate new technologies in the 21st century. **www.centerdigitalgov.com.**

Keeper Security, Inc. ("Keeper") is transforming the way organizations and individuals protect their passwords and sensitive digital assets to significantly reduce cybertheft and data breaches. Keeper is the leading provider of zero-knowledge security and encryption software covering password management, dark web monitoring, digital file storage and messaging. Named PC Magazine's Best Password Manager (2019, 2020) & Editors' Choice (2019, 2020) and awarded the Publisher's Choice Cybersecurity Password Management InfoSec Award (2020), Keeper is trusted by millions of people and thousands of organizations to protect their digital assets and help mitigate the risk of a data breach. Keeper is SOC-2, FIPS 140-2 and ISO 27001 Certified and is also listed for use by the Federal government through the System for Award Management (SAM). Keeper protects organizations of all sizes across every major industry sector.