Protecting the Vote:

How One Northeastern State Secured Elections Using Strong Multi-Factor Authentication

Safe, fair and secure elections are the bedrock of America's political system, but states throughout the country face increasing challenges protecting their elections. From aging voting infrastructure to cybercriminals attempting to hack into voting systems, it's never been more crucial for states to strengthen their security posture.

One Northeastern U.S. state has taken significant steps in recent years to achieve this, including investing in ongoing cybersecurity training for election officials, conducting security audits and modernizing its election infrastructure. Along with these efforts, one of the most meaningful steps the state took was adopting a hardware security key-based multi-factor authentication (MFA) solution to protect its voter registration system. This MFA solution is an essential part of the state's holistic approach to improving election security and giving voters more faith in the election process — potentially serving as a model for other states.

Confronting Challenges with Election Security

Election security has become a pressing concern for both election officials and voters. One 2018 Pew Research survey found just 45 percent of Americans were somewhat confident the country's election systems were secure.[1]

Current cybersecurity challenges undermine the public's trust in fairness of elections, which is why the Northeastern state has enacted several changes to bolster election security. (Given the sensitive nature of election security, many state leaders prefer to remain anonymous when discussing specific measures they have put in place.)

"After 2016 and reports that nation-state actors were trying to interfere with U.S. elections, we wanted to do everything to ensure we took advantage of all the tools and opportunities available to make sure our systems were as secure as possible," the state's election director says.

Despite budget and resource constraints — and although it hadn't yet faced a security breach itself — the state has taken a proactive approach to reduce its security vulnerabilities. Cybersecurity training is integrated into its election management, voter registration, candidate management and nomination paper trainings. Using resources from the Department of Homeland Security, the IT team conducts regular phishing and external penetration tests, as well as risk and vulnerability assessments. The state also performs post-election security audits, reviewing ballots to ensure vote tallies are correct.

"After 2016 and reports that nation-state actors were trying to interfere with U.S. elections, we wanted to do everything to ensure we took advantage of all the tools and opportunities available to make sure our systems were as secure as possible," the state's election director says.

"We're trying to change the mindset of everybody, so that they're always thinking about cybersecurity, not just at work and not just at home, but really all the time," the election director says.

One of the biggest steps was replacing the 15-year-old voter registration system with a new system. The state worked with an external vendor to build the system from scratch with the latest security standards in mind. But even with that built-in security, state leaders realized they needed to take additional measures to properly secure the system. They turned to the YubiKey, a hardware-based MFA solution, to provide the highest assurance authentication possible.

"If someone gets into our voter registration system and even does something minor, it could sow doubt in the minds of voters when they go to the ballot box — and we just can't have that," the election director says.

Securing Elections by Harnessing an MFA Solution

Passwords can be easily compromised, especially if cybercriminals can hack into a government agency's wireless network. In one recent report, the National Association of Secretaries of State said "the strongest password protocols are not even safe from intrusion" and that the only effective way to combat security threats is to adopt a new security approach. "Creating an additional authentication protocol that requires a physical element virtually blocks the bad actor's access to the application," the organization said.[2]

The Northeastern state transformed its security approach by adopting an MFA solution that relies on the YubiKey. The state has distributed individual security keys to election officials, poll workers and other authorized users who require access to its voter registration system. Each user has a unique registered key. After a user enters her username and password, she must insert the key into the USB port on her computer and then touch the capacitive button on the key to log in and access the system. The user's touch serves as verification that a human — and not a remote hacker — is trying to access the system. In addition to improved security, this approach also delivers a better user experience than other forms of MFA, such as mobile-based authenticators. Since the security key is portable, it allows election officials, registrars and poll workers to use different devices and systems simply entering their credentials and using this one-touch solution.

The YubiKey, which supports open industry security standards like FIDO U2F and FIDO2, also works on NFC-enabled Android phones. A user simply taps the key against the phone to complete the authentication process. The solution also provides email confidentiality by acting as a strong second-factor authenticator for Office 365, Gmail and other email platforms used by election officials and poll workers.

The state's previous voter registration system required a username and password to log on. The new system, which incorporates the YubiKey, includes an added step, the state's election director says. "Now, I need to not only have my username and password, but also that physical piece that has to be inserted into my computer and pushed in, in order for me to gain access."

Relying on hardware-based security has enabled the state to strengthen its security posture. Research has shown that many MFA solutions available today, including SMS codes, one-time passcodes and mobile MFAs, can be vulnerable to phishing attacks, malware and other security threats. A hardware-based security key is more effective at stopping account takeovers. A security key stops 100 percent of account takeovers, compared to a 90 percent prevention rate for on-device prompts, a 79 percent prevention rate for secondary email and a 76 percent prevention rate for SMS codes.[3] It's also four times faster than typing in an SMS code,[4] which is one of the most common approaches for multi-factor authentication in the public sector, according to Cody Hussey, a solutions engineer for Yubico, which manufactures the YubiKey.

Hussey adds that a security key is better than mobile-based multi-factor authentication tools because it reduces reliance on a phone or network connectivity as part of the authentication process, which ultimately makes systems more secure.

"It also doesn't have a battery and it's not dependent on a cell signal, which is a big differentiator when you're talking about phone applications and push notifications on phone apps. It's pretty indestructible," Hussey says. "There's also a lot of regulation around users using personal devices for authentication in work scenarios, so using a hardware-based security key is really effective when compliance or regulation mandates that a user can't use their own phone or if they're logging into a phone and can't use that phone within the authentication process."

The state's previous system required a username and password, the election director says. "Now, I need not only my username and password, but also that physical piece that has to be inserted into my computer and pushed in, in order to gain access."

The Northeastern state's election director says relying on hardware security keys was especially beneficial during primary elections when temporary workers had to be hired to manage an influx of mail-in ballots. Every temporary employee received their own security key, which they could use to access the state's voter registration system. Rather than relying on a software-or password-based solution, the keys gave election leaders more control over who could access voter records and reduced the risk that a hacked password could lead to unauthorized access of this sensitive information.

The state also has been able to simplify its hardware management, because the security key can be easily numbered, tracked and managed. If an employee leaves or their temporary employment ends, the state can securely reassign the key to another user.

Relying on hardware keys strengthened the state's security posture during recent primary elections, when temporary workers had to be hired to manage an influx of mail-in ballots.

"Jurisdictions are moving toward implementing multifactor authentication on their voter registration databases. It's a very cost-effective and easy process and it didn't cost us a lot of money," the state's election director says. "It's such a huge part of making sure systems are secure. I don't see how you can't do it."

This piece was developed and written by the Government Technology *Content Studio, with information and input from Yubico.*

Endnotes:

1. https://www.pewresearch.org/politics/2018/10/29/election-security/
2. https://www.nass.org/sites/default/files/2018-07/pcc-gcr-white-paper-nass-summer18_0.pdf
3. https://security.googleblog.com/2019/05/new-research-how-effective-is-basic.html
4. https://resources.yubico.com/53ZDUYE6/as/qbdf10-duv63c-4cajzy/Modernizing_election_security_with_the_YubiKey.pdf

Produced by:

government technology

Government Technology is about solving problems in state and local government through the smart use of technology. Government Technology is a division of e.Republic, the nation's only media and research company focused exclusively on state and local government and education.
www.govtech.com

For:

yubico

Yubico puts an end to account takeovers for businesses and individuals. The YubiKey — the world's #1 hardware-based security key — is the most secure, easy-to-use, and affordable multi-factor authentication. The world's largest governments, technology companies, and financial institutions trust Yubico to secure their most important information, accounts, and applications. **Learn more at www.yubico.com**