okta | proofpoint

4 Top Considerations for State and Local Agencies Looking to Protect Against Credential-Based Attacks

It's more crucial than ever that government security systems and policies are prepared to take on threats. Here's what types of attacks are on the rise — and what governments can do about it.

A simple click on a malicious link can have devastating effects on an organization — stolen credentials, compromised security or, worse yet, a complete standstill of computer systems held hostage by hackers.

In a time when agencies across the country are working facilitating more remote work than ever, state and local governments must take action to protect against credential-based threats, which can infiltrate networks via employee inboxes, unsafe WiFi networks and a variety of other vulnerable points.

Here are the top four things public sector IT leaders should know about these attacks and how to protect against them.

1. Governments Are Increasingly Targeted by Cyberthreats

Credential theft continues to be a major headache for organizations – and phishing is the most common technique to pilfer information. The 2019 Verizon Data Breach Investigations Report highlighted how 32% of over 41,685 security incidents in 2018 involved phishing and 29% entailed use of stolen credentials. Among government entities, phishing was the top method for attackers to gain access to information and data. Overall, 16% of all reported incidents were breaches of public sector entities.

With financial transactions and critical infrastructure information housed by state and local governments, it's no wonder attackers are aiming their crosshairs there, said Stephen Gaul, solutions engineer at Okta, Inc., which has teamed with Proofpoint to deliver security solutions that protect against ransomware, email and credential-based attacks

"You're really starting to see cybercriminals doing more complex attacks to try to acquire that data or the individual credentials," he said.

If phishing attacks weren't enough of a headache, governments also have to worry about other stealthier threats.

Dual-purpose attacks, for example, are on the rise, Gaul said. In these attacks, hackers leverage tools in already existing Windows or Linux systems utilities and make use of pre-installed or fake tools on these systems. These methods are hard to detect because dual-purpose attacks —also known as so-called living-off-the-land tactic — look like legitimate processes. And they can be dangerously effective: The 2017 outbreak of ransomware NotPetya used the living-off-the-land approach to infect computers all across the globe.

2. Yesteryear's Approach to Security Isn't Enough

These increasingly sophisticated attacks have forced public sector IT leaders to look at security in a new light. Leveraging private industry, governments today have access to threat intelligence research they can integrate into their security infrastructures so they can detect, block and respond to threats.

"They're really starting to … have access to threat intelligence research — things coming out of the commercial sector, aside from what they have access at the state and local level — that gives them the details about the existence of these types of attack," Gaul said.

Also, instead of conventional information security practices, Okta and Proofpoint are promoting people-centric security aimed at striking a balance between reducing risk and still keeping employees agile.

For a remote and distributed workforce, this approach is especially important because IT teams can implement controls that provide a baseline type of protection for employees. This allows the organization to know, for example, who's in one's organization, where they are, how they're being targeted, who the adversaries are and whether there are emerging patterns of attacks against these individuals regardless of where they are located.

"It's creating that whole awareness as well as a model in the controls for the type of protection against those people Proofpoint calls VAP, a Very Attacked Person," Gaul said, referencing at-risk users often targeted by hackers. VAPs are typically an organization's CEO or other high-ranking positions, such as chief financial officer or vice president of engineering. But it's not just the C-suite, administrative assistants, financial analysts, HR professionals or buyers can also be frequently targeted.

3. People-Focused, Tech-Powered Tools Work to Keep Attacks at Bay

To help prevent credential-based attacks, Okta and Proofpoint are working to boost people-centric security and combine best-of-breed identity management with world-class email security.

Okta provides the identity and access management and policy and step-up authentication while Proofpoint drills deeper down into the information protection, gaining visibility into sensitive data.

Together, they work to lock down files in the cloud, prevent data loss, archive email and other types of communications. That way, state and local customers can stay in compliance and address the challenges of the security awareness training, get to the archives and take forensics and remediation actions.

"While Proofpoint can help them manage that bulk email and stop the threats before they reach the user's inboxes, and they can avoid that spam and that malware, Okta then allows them to safeguard their software-as-a service apps and that broader IT environment," Gaul explained.

It all starts with the TAP solution — Targeted Attack Protect — which detects, analyzes and blocks threats before even reaching an inbox. These include ransomware, zero-day threats, polymorphic malware, malicious documents and phishing attacks.

TAP then gives users visibility into an organization's email communications and the files in its SaaS service file stores, allowing users to see everything from Trojans to ransomware to the targeted attacks that could have resulted in a credentials theft.

"Now, they now have a footprint, so to speak, of that or a grasp of where that exists in someone's organization," Gaul said.

Once they have this targeted attack protection, this is where the other part of Okta's solution comes into play.

By creating a VAP group within an Okta tenant, Okta's adaptive multifactor authentication policies can be used to automatically enforce step-up authentication on those potentially compromised users. That means Proofpoint will send the list of VAPs to Okta where the VAP group is created in the Okta tenant and then Proofpoint will automatically block and quarantine messages with malicious attachments or URLs for those VAPs, so those emails stay out of inboxes.

"They automatically get policies created for them from Okta and then Proofpoint is helping to manage and stop those advanced threats before they get into the user's inbox so they can't actually click on them," Gaul explained.

4. The 4 Ingredients to a Successful Security Recipe

When considering a comprehensive security strategy, Gaul outlines a quartet of key pillars.

- Adopt a people-centric approach to protect against credential theft and phishing.
- Identify and gain visibility into the organization's most targeted users — and then apply granular security policies to them.
- Orchestrate remediation actions on these potentially compromised users, whether that entails quarantining emails, prompting for MFA or adding other adaptive controls.
- Finally, think about restricting access to sensitive resources.

"You see a lot of people in a lot of state and local governments moving to the cloud and moving their DevOps into the cloud," Gaul said. "Do they have the proper controls on that? Are they using MFA for that secure remote access? And if they're not, then are they just using password policies, and what are those password policies? Do they have the proper minimum length, complexity requirements, expiration reuse, lockout, that whole bit?"

Gaining that visibility into those users and applying those granular security policies without the proper tools can be challenging — and orchestrating those actions manually and sifting through audit logs isn't the best approach, either, Gaul said.

"Okta and Proofpoint automate that as well as a lot of those pieces," he said. "It's really going from a very, very manual type of process to putting the tools in place in order to automate these and eliminate human error, as well as be able to gain faster response to remediation."

Learn more about how Okta and Proofpoint can help your state and local government protect against credential-based attacks.
