Four Key Ways Governments Can Prepare for the Growing Ransomware Threat

Ransomware has quickly emerged as one of the biggest cybersecurity threats facing state and local government agencies. Numerous government entities have been victims of attacks over the past few years, and these assaults are costly. The FBI's National Cyber Investigative Joint Task Force reported that between 2013 and 2019, an estimated $144 million in Bitcoin cryptocurrency was paid out as ransom as a result of these attacks. In addition, ransomware attacks increased 150 percent in 2020 over 2019.[1]

While ransomware can affect any industry or organization, the task force said it's particularly concerned about attacks against the networks of state, local, tribal and territorial governments; police and fire departments; municipalities; and other critical infrastructure.

The COVID-19 pandemic and resulting work-from-home models have exacerbated the problem, with some of the newest ransomware threats aimed at remote employees. And ransomware continues to pose a considerable threat in 2021, with sophisticated attacks targeting all levels of government.

This brief, which draws from a *Government Technology* webinar sponsored by BeyondTrust, explores the ransomware mitigation strategies government entities can take to find and stop these attacks before they can do costly damage.

Conduct Training Programs

Training employees at all levels of the organization — including the most senior officials — about the ransomware threat is vital to building a strong defense.

Agencies need to provide education about what these attacks typically look like, how they work, what users need to do, and the damage the attacks can inflict on the organization if not addressed in the right ways.

It's especially important that employees recognize activities such as phishing — where hackers send digital communications seemingly from reputable sources and request sensitive information — so they can take the proper steps to avoid infecting their organization with ransomware.

Remote workers, in particular, need to be extremely mindful of the dangers of phishing and social engineering, given they are often prime targets of attackers. One study found the number of active phishing websites has grown 350 percent during the pandemic.[2]

Still, training should go well beyond focusing on one or two forms of an attack. Ransomware uses multiple techniques to infiltrate an environment, and can cause quite a bit of damage, says Morey Haber, CTO and CISO at BeyondTrust. "The attack vectors are now wider than just phishing, wider than just email, wider than just unpatched systems," Haber says.

It's important to remember that training can't be a one-and-done proposition. Security programs must provide periodic training sessions to keep their people apprised of the latest threats.

Implement an Extensive Toolbox

Traditional anti-malware software alone is not sufficient to deal with today's increasingly sophisticated attacks. Single, standalone solutions simply will not protect agencies from ransomware.

"Organizations are relying on anti-malware [software] to protect them, and we all know that's not quite going to cut it in this day and age," says Deborah Snyder, senior fellow at the Center for Digital Government. "Some may have advanced to dedicated tools, but even there, I think there's room for improvement."

Agencies need to deploy multiple tools and services, and these components must be able to work together as part of a cohesive strategy.

Beyond anti-malware, agencies should be looking to deploy a defense-in-depth strategy that includes data encryption, network segregation, endpoint privilege management, secure remote access, credential management, multi-factor authentication to protect mobile devices and apps, and access controls/permissions.

Prior to selecting and deploying any of these security tools, it's important to assess the current technology

environment and identify any potential weak points within the organization, including remote access setups.

Adopt Zero-Trust Design and Policies

Agencies should consider building a zero-trust architecture and policies. In a zero-trust environment, networked devices are not trusted by default, even if they're connected to a managed corporate network and were previously verified.

A zero-trust approach continuously establishes trust every time a user or device requests access to a network or resource, helping prevent attackers from exploiting weaknesses in the perimeter to gain entry and achieve lateral movement.

With this method, agencies can reduce the time it takes to detect breaches and gain visibility into network traffic. They gain protection against internal and external threats and limit the likelihood of data exfiltration or lateral movement.

"Consider dissolving everything you know about network security and apply authentication and authorization access to any resources that you have. That's where zero trust comes in and becomes quite powerful," Haber says.

Ensure Data Backup and Recovery

Government entities need to have up-to-date, effective data backup and recovery mechanisms in place to protect their information assets. Some ransomware attacks target data backup systems, so agencies need to ensure those systems are sufficiently protected. They should regularly back up systems and data and have tight controls over access to backups.

Data backup systems should include security capabilities to guard against known ransomware threats, and be able to restore quickly to avoid a major impact in the event of an attack.

The Time to Act Is Now

Creating an effective strategy to combat ransomware needs to be a high priority for government agencies. The sense of urgency is heightened by the fact that these attacks are becoming more sophisticated, more people are working remotely, and data and systems are becoming more decentralized.

"This subject can be as complicated and overwhelming as any other highly technical subject," says Adam Ford, CISO and acting chief data officer for the Illinois Department of Innovation & Technology. "But in each and every case, wherever you are, start to look for tools and make incremental progress. The goal here is just to reduce your risk."

View the full webinar, "Ransomware in 2021: How to Strengthen and Fund Your Cyber Protection Measures," here.

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

Endnotes:

1. Ransomware Uncovered 2020/2021.
2. Group-IB. March 2021.https://www.pcmag.com/news/phishing-attacks-increase-350-percent-amid-covid-19-quarantine

FUNDING SUPPORT FOR RANSOMWARE DEFENSES

State and local government agencies looking to defend against ransomware attacks might be able to get cybersecurity funding from several resources.

For example, the Coronavirus Aid, Relief, and Economic Security Act, also known as the CARES Act, a $2.2 trillion economic stimulus bill signed into law in March 2020, provides funding for education, training and advising in areas including the risks of and mitigation of cyber threats in remote customer service or telework practices.

The State and Local Cybersecurity Improvement Act, currently in the U.S. Senate, would authorize a new Department of Homeland Security (DHS) grant program to address cybersecurity vulnerabilities on state and local government networks. The act aims to improve the ability of state and local governments to detect and defend against cyberattacks by authorizing dedicated resources and support. Among other provisions, it establishes a $400 million DHS grant program with a graduating cost-share that incentivizes states to increase funding for cybersecurity in their budgets; and requires the Cybersecurity and Infrastructure Security Agency (CISA) to develop a strategy to improve the cybersecurity of state, local, tribal, and territorial governments.

In addition, the American Rescue Plan Act of 2021, signed into law by President Biden in March 2021, makes $650 million available to CISA for cybersecurity risk mitigation until Sept. 30, 2023. The agency works with partners to defend against threats and collaborates to build more secure and resilient infrastructure for the future.

Produced by: CENTER FOR DIGITAL GOVERNMENT

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.**

For: BeyondTrust

BeyondTrust is the worldwide leader in Privileged Access Management (PAM), empowering agencies to secure and manage their entire universe of privileges. The BeyondTrust Universal Privilege Management approach secures and protects privileges across passwords, endpoints, and access, giving agencies the visibility and control they need to reduce risk, achieve compliance, and boost operational performance.

To learn more about how BeyondTrust can help protect against ransomware, visit: **www.beyondtrust.com/solutions/ransomware**

IMAGE PROVIDED BY SHUTTERSTOCK.COM