The Cybersecurity Challenges in Government-Wide Move to Telework

Forward-thinking agencies face fewer vulnerabilities as attacks ramp up in intensity.

James Mersol

Wed, 03/25/2020 - 09:46

Photo Credit: Unitone Vector/iStock.com

Despite the hurdles that COVID-19 has presented federal agencies, the threat from adversaries in cyberspace has not diminished. Malicious actors are taking advantage of the situation to exploit insecure virtual private network (VPN) connections and other poorly configured remote security controls as well as federal employees who are distracted by these challenging times. Developing proactive, forward-thinking policies and controls as well as continuing employee training on cyber hygiene and vigilance around phishing attacks is all the more critical.

“Adversaries have exploited VPN servers for years, and today more federal employees are teleworking than ever before,” said Stephen Kovac, vice president of global government and compliance at Zscaler. “Security concerns should be at DefCon 2. Agencies will need to monitor their security controls even more closely in the coming days, weeks and maybe longer.”

To reinforce the importance of strong cybersecurity, NIST issued guidelines for telework security, especially in the context of remote access and bring your own device (BYOD) as agencies adjust to the technical requirements of telework. The bulletin draws heavily on special publication 800-46, originally issued in 2016, but still the guiding technical document for baseline remote security for many organizations.

“An organization should assume that external facilities, networks and devices contain hostile threats that will attempt to gain access to the organization’s data and resources,” the bulletin said. “Organizations should assume that malicious parties will gain control of telework client devices and attempt to recover sensitive data from them or leverage the devices to gain access to the enterprise network.”

Given these assumptions, NIST encouraged agencies to make “risk-based decisions about what levels of remote access should be permitted from which types of telework client devices.” As an example, NIST recommended developing “tiered levels of remote access” for BYOD computers and mobile devices, such as limiting BYOD phones to webmail access only.

Zero trust and its component technologies could ensure remote security, especially for organizations struggling with VPNs.

“Many agencies have or are implementing zero trust capabilities, such as SASE, endpoint management, cloud-based CDM, software-defined networking, micro-segmentation and cloud monitoring, or have solutions already in place,” Kovac said. “They will need to assess current security capabilities and existing technology, and provide a plan to secure access for a larger than normal remote user base during these times, while keeping employees safe and productive.”

Kovac also advised implementing trusted internet connection (TIC) 3.0 guidelines and reviewing existing use cases to determine the best applications for TIC 3.0 in each agency. Updated in September last year, OMB's TIC 3.0 guidance was designed to assist federal agencies that have increasingly moved to a mobile architecture where the traditional concept of an on-prem perimeter no longer applies.

One early use case agencies may want to examine is how the Department of State has used TIC 3.0 to provide secure connections to U.S. embassies and consulates worldwide, especially in areas where online infrastructure is unreliable. As organizations both public and private grow concerned about the security of their employees' home networks relative to federal networks, this use case can help them shape their remote network access policies, determining what level of security is needed for different parts of the mission. The use case also applies to agencies with employees in rural areas who may not have ubiquitous high-speed internet access.

Irrespective of the remote security solution agencies implement, keeping employees up to date on phishing and other scams is also critical during this uncertain time.

"Spearphishing is ultimately a social engineering tactic," said Tim Callan, senior fellow at Sectigo.

Callan explained that one reason there has been an uptick in spearphishing is that attackers are able to use the disruptions caused by COVID-19 to their advantage, both in terms of content and circumstances. In terms of content, Callan explained that this is a worrying time for many, who are likely to fall prey to spearphishing targeted at promises of financial assistance as well as coronavirus treatment or prevention. Even for those who are vigilant about detecting potential scams, disruption to their normal working environment and day-to-day practices can leave them open to making mistakes.

Following on from CISA's alert last week warning users of phishing attacks meant to compromise VPNs, the FBI's Internet Crime Complaint Center (IC3) released a public service announcement regarding fraudulent activity, including emails claiming to be from the Centers for Disease Control (CDC), fake offers regarding treatment or prevention and phishing attacks related to charity, government checks and business refunds.

"The FBI is reminding you to always use good cyber hygiene and security measures," the announcement states. These measures include verifying web addresses — preferably by typing them into your browser rather than clicking on a link — and never providing personal information in response to an email or robocall.

IC3 encourages everyone to report scams, attacks and other suspicious activity on the center's website.

View printer friendly version
coronavirus
cybersecurity
NIST
FBI
Zero Trust
phishing
Standard