Shutterstock/FCW Staff

Taking aim at a moving CYBER TARGET

Agencies are in search of ways to secure networks that are as fluid as the cyber world in which they operate

GOVERNMENT AGENCIES were already under pressure to modernize their cybersecurity strategies before the pandemic hit. The trends toward remote work and cloud-based systems were pushing network perimeters further out from the data center, and the move to digital services had been creating new challenges for securing information and protecting privacy.

The pandemic only heightened the sense of urgency. As workplaces closed and government employees struggled to access data and systems from makeshift home offices, the cybersecurity risks grew. The use of virtual private networks in the U.S. increased to match the early spike in COVID-19 cases, rising 124% in the two weeks from March 8 to March 22, 2020, according to Statista. Around the same time, the Cybersecurity and Infrastructure Security Agency (CISA) issued an alert titled "Enterprise VPN Security," which offered both warnings and guidance on how to handle the surge in usage.

That was far from the only security alert released by government agencies as hackers sought to take advantage of the pandemic. In March 2020, the FBI warned about a rise in fraud schemes related to the health crisis, including fake email messages claiming to be from the Centers for Disease Control and Prevention. In October, CISA, the FBI and the Department of Health and Human Services called attention to ransomware attacks targeting the health care and public health sectors.

Defending against such attacks became more difficult with employees spread far and wide. Some employees connected to networks via less-than-secure personal devices, while others fell victim to clicking malicious links due to relaxed cyber hygiene concerns. In response, agencies began looking for new ways to secure government systems.

Adopting a zero trust mentality

With so many employees logging in remotely, agencies found that they had to shift their focus from securing a well-defined perimeter to securing the data that fuels government operations. In a recent survey of FCW readers, protecting data topped the list of cybersecurity priorities, with 75% of respondents citing it.

In response to such concerns, CISA released its Ransomware Guide in September 2020. The guide features a wide range of best practices, including identifying assets that are searchable via online tools and taking steps to reduce that exposure, performing frequent backups, and storing backups separately. CISA also offers services to help agencies guard against ransomware attacks, training in how to identify and mitigate vulnerabilities, and advice on how to respond to an incident.

Another way to protect critical assets is by emphasizing endpoint security and ensuring that all users and devices are safe before they are allowed to access government networks. That is a core tenet of zero trust architecture, a mindset that "assumes there is no implicit trust granted to assets or user accounts based solely on their physical or network location… or based on asset ownership," according to the National Institute of Standards and Technology (NIST).

CYBERSECURITY by the numbers

89%
FCW survey respondents who said IT modernization is having a positive impact on their agencies' cybersecurity

55%
FCW survey respondents who said enabling secure collaboration for on-site and remote employees was a priority

14,587 to 30,874
Increase in teleworkers at the Transportation Department from February to March 2020

77%
Federal employees who would like to continue teleworking after the pandemic

Sources: American Federation of Government Employees, FCW and Transportation Department

In May, President Joe Biden mandated that agencies adopt zero trust in his Executive Order on Improving the Nation's Cybersecurity, and the National Security Agency released a paper a few months ahead of that mandate titled "Embracing a Zero Trust Security Model." It recommends that critical networks such as national security systems, Defense Department networks and defense industrial base systems use the architecture.

"Even the most skilled cybersecurity professionals are challenged when defending dispersed enterprise networks from ever more sophisticated cyberthreats," the NSA document states. "Organizations need a better way to secure their infrastructure and provide unified-yet-granular access control to data, services, applications and infrastructure."

Experts also recommend that agencies extend the zero trust approach to the files employees interact with and exchange on a daily basis, which can be embedded with malicious code. A technique called content disarm and reconstruction can be used to disassemble files, remove harmful elements and rebuild the files so that they no longer pose a risk.

Jump-starting efforts to modernize security

In the FCW survey, 70% of respondents said they were particularly interested in improving their ability to anticipate and respond to evolving cyberthreats. One key strategy is to shift from relying on signature-based security, which compares threats to a database of known malicious code, to behavior-based threat detection. With the help of artificial intelligence, the latter approach identifies anomalies in user or device behavior and blocks access in real time.

In addition, many IT administrators are turning their attention to the way software and other services are developed and adopting a DevSecOps approach. The General Services Administration's DevSecOps Guide defines the methodology as "a cultural and engineering practice that breaks down barriers and opens collaboration between development, security and operations organizations using automation to focus on rapid, frequent delivery of secure infrastructure and software to production."

NIST is considering developing a DevSecOps framework and lists a number of ways the approach brings value, such as reducing vulnerabilities and malicious code in software and addressing the root cause of vulnerabilities to prevent recurrences. The methodology could help minimize threats in mobile apps, whose use has skyrocketed during the pandemic.

To address evolving cyberthreats more broadly, the White House and some lawmakers have proposed reforming the Federal Information Security Modernization Act (FISMA) to ensure agencies are following the latest cybersecurity best practices. FISMA was passed in 2002 and updated in 2014, and Federal Chief Information Security Officer Chris DeRusha said in July that the law could get a makeover again. He specified two main areas for reform: testing and validating security arrangements and increasing security automation.

Although federal offices began reopening in June, many experts believe remote work will continue now that employees and agencies have experienced the benefits and are working to minimize the risks. In FCW's survey, 68% of respondents rated the pandemic's impact on their agencies' cybersecurity strategies as a 3 or higher on a scale of 1 to 5.

When agencies pivoted quickly to address the challenges that arose during the pandemic, they jump-started the evolution to a more flexible, modern approach to cybersecurity while also empowering employees to be productive from any location. Agencies' ongoing efforts to future-proof cybersecurity strategies will continue to drive mission success across government. ■