The never-ending evolution of cybersecurity

Following best practices for cyber hygiene is still a foundation for success, but agencies also need modern approaches to modern threats

Securing government systems was a complex undertaking even before the pandemic. In response to that crisis, agencies rapidly deployed cloud technology, mobile devices and collaboration tools for remote employees — and added new vulnerabilities and IT management challenges to an already long list of cybersecurity priorities.

Malicious actors have taken note of the new opportunities and continue to mount increasingly sophisticated attacks on government systems and critical infrastructure. The SolarWinds and Colonial Pipeline breaches highlighted the ever-evolving risks to the IT systems that have become integral to our daily lives.

To keep pace with those risks, government teams need multifaceted yet holistic strategies that address a wide range of threats to network endpoints, identity and access management, and data. In addition, agencies must strike the right balance of productivity and security for a mix of on-site and remote employees — a key concern of 75% of the respondents to a recent FCW reader survey.

At the state level, members of the National Association of State CIOs put cybersecurity and risk management at the top of their list of priorities for 2022. Furthermore, in "Driving Acceleration: The 2021 State CIO Survey," NASCIO researchers wrote that "while cybersecurity has long been a priority for all state CIOs, several indicated that there is now an elevated focus on and appreciation of the importance of the topic due to the pandemic."

The ongoing push for zero trust

In FCW's recent survey, respondents said their agencies were particularly interested in protecting against ransomware and other breaches (75%) and improving the security of network endpoints (71%).

Verizon's 2022 Data Breach Investigations Report states that in 2021, "ransomware has continued its upward trend with an almost 13% rise — an increase as big as the last five years combined." The report adds that organizations can block the

Cybersecurity by the numbers

Sources: FCW, Statista, Verizon

$158.9B

Projected revenue of the global cybersecurity market this year, with $64.9 billion generated in the U.S.

76%

FCW survey respondents who said the executive order was having a positive impact on their agencies' security practices

67%

FCW survey respondents who said clear guidance on standards and strategies would improve their agencies' cybersecurity

13%

Increase in ransomware breaches in 2021, which was as big as the combined increases for the previous five years

common routes to ransomware by having a plan for handling credentials, phishing, the exploitation of vulnerabilities and botnets.

In its top cybersecurity trends for 2022, Gartner acknowledges the growing complexity of IT environments by putting "attack surface expansion" in the first slot, followed by "identity system defense." Researchers wrote that "identity systems are coming under sustained attack. Misuse of credentials is now a primary method that attackers use to access systems and achieve their goals."

Fortunately, zero trust has been gaining traction because of its ability to address key challenges related to identity management, endpoint security and data protection. Interest in zero trust has skyrocketed thanks to a mandate in the Biden administration's 2021 Executive Order on Improving the Nation's Cybersecurity. A series of subsequent memos have offered further guidance and reinforced the order's central role in pushing agencies to modernize their approach to cybersecurity.

Seventy-six percent of the respondents to FCW's survey said the executive order was having a positive impact on their agencies' security practices, and 56% said a stronger commitment to zero trust would help their agencies improve cybersecurity.

The Cybersecurity and Infrastructure Security Agency has also stressed the importance of zero trust. CISA released a joint Cybersecurity Advisory in May — in concert with authorities in Canada, New Zealand, the Netherlands and the United Kingdom — to call attention to the weak security controls and practices that bad actors routinely exploit to gain access to systems. Poor cyber hygiene practices include lack of enforcement of multifactor authentication, software that is not up-to-date, unprotected cloud services, and poor endpoint detection and response.

Among the advisory's key recommendations for mitigating those risks: "Adopt a zero-trust security model that eliminates implicit trust in any one element, node or service, and instead requires continuous verification of the operational picture via real-time information from multiple sources to determine access and other system responses."

The need for more effective teamwork

Although zero trust can play a key role in ensuring that only authorized users have access to IT systems and data, it doesn't always protect against human mistakes. "Whether it is the use of stolen credentials, phishing or simply an error, people continue to play a large part in incidents and breaches alike," Verizon's report states.

Gartner researchers wrote that "progressive organizations are moving beyond outdated compliance-based awareness campaigns and investing in holistic behavior and culture change programs designed to provoke more secure ways of working."

In addition, security responsibilities have crossed traditional internal boundaries, and agencies are finding that they need to unify the priorities of security teams and mission owners. "The pandemic created an imperative within state leadership to highlight that cybersecurity is a team sport," NASCIO's report states.

In terms of more effective teamwork, many experts say the government could benefit from rethinking the role of chief information security officers (CISOs). "These disruptions don't exist in isolation; they have a compound effect," said Peter Firstbrook, a research vice president at Gartner. "To address the risks, CISOs need to transition their roles from technologists who prevent breaches to corporate strategists who manage cyber risk."

In its list of top security priorities, Gartner cites the dual need to expand the CISO's office and facilitate distributed decision-making for faster response to risks. "The CISO and the centralized function will continue to set policy, while cybersecurity leaders are placed in different parts of the organization to decentralize security decisions," the firm's researchers predict.

Making cybersecurity a budget priority

In July, Office of Management and Budget Director Shalanda Young and National Cyber Director Chris Inglis issued OMB M-22-16, which outlines the cross-agency cyber investment priorities that officials should keep in mind when formulating their fiscal 2024 budget submissions. Among the priorities:

- Improving the defense and resilience of government networks, which includes zero trust implementation and cybersecurity-centric IT modernization.
- Deepening cross-sector collaboration in defense of critical infrastructure.
- Strengthening the foundations of our digitally enabled future, which includes improving training and pay incentives for cybersecurity professionals in government.

Young and Inglis wrote that their two offices will work together to "provide feedback to agencies on whether the priorities are adequately addressed and consistent with the overall cybersecurity strategy and policy — aiding agencies' multiyear planning through the regular budget process."

The Biden administration has been widely praised for its efforts to lead the way on aggressive, modern approaches to security for the government and the country as a whole. In a recent blog post, Forrester Senior Analyst Heath Mullins wrote: "The U.S. federal government is going to great lengths to establish itself as a security leader instead of a laggard." He goes on to say that "highly regulated industries would be wise to keep a sharp eye on what the U.S. government is doing and follow a similar path to success." ■