6 Ways to Close Your Organization's Cyber Gaps

The stakes just keep getting higher when it comes to cybersecurity. A government agency is hit with a ransomware attack every 14 seconds, according to a recent report from the Cybersecurity and Infrastructure Security Agency.

That's a scary statistic for any organization, and more so in the public sector, where there's a high bar set for accountability.

How can agencies close the cyber gap? Here are some ideas discussed during a recent GovLoop virtual event titled How Zero Trust Is Transforming the Way You Work.

1 Develop New Guidance for New Technologies

At the U.S. Government Accountability Office (GAO), "systems are complex, they're dynamic, they're geographically disbursed," said Jennifer Franks, GAO's Director of Information Technology and Cybersecurity. And at GAO, as in other government agencies, those systems are constantly evolving.

The rapid pace of technological advance is widening the attack surface and complicating the cyber threat environment. To address emerging vulnerabilities, government needs to develop cyber policies that look beyond the existing IT infrastructure, to anticipate the unknown.

"Because it is a moving target … we're going to have to really look at what types of rules and procedures and guidance we can establish at more of a technology-agnostic level," Franks said.

2 Shift From Perimeter to Holistic Protection

Amid this rapidly changing IT landscape, there's been a shift in where data and applications reside. Defense today goes beyond "protecting the physical assets, protecting the networks, protecting the physical areas where data and applications were housed," said David Rubal, Head of U.S. Federal Business Development at AWS Storage Services, AWS Worldwide Public Sector.

To meet the present challenge, IT needs to look beyond the traditional perimeter-line of cyber defense. The notion of perimeter control "is now giving way to a more holistic level of protection," he said.

Supported by zero trust, the emerging vision is of "an inside/outside protection" that encompasses the entire technology infrastructure, both on premises and in the cloud, he said.

3 Focus on Recovery

Given the pace of cyberattacks and the perseverance of the attackers, government agencies need to assume they will be breached at some point. "With that many attacks occurring, something is most likely going to get through," said Timothy Pedro, Field Chief Technology Officer of Cloud Architecture at Veritas.

With that in mind, agencies need to invest not just in defenses, but in recovery mechanisms. "You can't just try to prevent these attacks from succeeding. You also have to build entire systems within the organization in order to be able to recover from those," he said. "You don't want to be on the news saying, 'We had to pay out a ransom because we had no way to recover from this.'"

4 Educate the Users

Given the prevalence of phishing attacks and other threat vectors that target human fallibility, robust zero-trust cybersecurity demands a high level of end-user awareness. Going forward, "we're going to have to enhance everyone's situational awareness," Franks said.

Contractors and federal employees alike need to understand their roles in supporting good cyber hygiene. Training needs to focus on "being more cyber smart and aware," she said. "It's going to take an educational shift for all of our employees."

5 Leverage AI in Support of Risk Management

Agencies are shifting toward a centralized risk-management approach to cyber. They're managing risk at the enterprise level in order to address emerging threats more proactively, Rubal said. He added that systems and tools that leverage artificial intelligence (AI) and machine learning (ML) can be brought to bear in support of this effort.

AI and ML are adept at detecting patterns, "whether it's over the last second, over the last year, over the last five years or 10 years," he said. Agencies can leverage that capability to help calculate risk in order to better align their resources in defense of the assets and systems that are most valuable and most vulnerable.

"We're at a very interesting time right now in industry, and in innovation, where these things are possible. There's an opportunity for agencies [to] leverage this innovation [at the] intersection of cybersecurity and AI and machine learning," he said.

6 Focus on Continuous Evolution

There's no sitting still here. "Just as you think you have hit your goal, there is a new goal that has been planted 300 yards away," Pedro said. "The threat landscape is continually evolving."

With this in mind, agency leaders need to invest in new solutions and approaches in order to keep ahead of the bad actors. As new defensive technologies emerge, "within government agencies, we need to test this stuff out," he said. "Don't be afraid of machine learning. Don't be afraid of AI."

These cutting-edge tools may seem somewhat far afield for people used to more conventional cyber solutions. But the innovative nature of these tools is exactly what will help keep federal cyber efforts one step ahead, Pedro said.

Watch the full event here

govloop aws VERITAS