Why Better Security Requires More Than Better Tech

Good cybersecurity requires more than just good security solutions. To deal with the increasing velocity of attacks, agencies must look beyond individual products and think in more holistic terms: looking at policies, processes and even communication strategies.

That was the focus of a recent GovLoop digital event, Zero Trust at the State and Local Level, which brought together thought leaders from government and industry to discuss how to develop a cyber strategy that builds public trust.

Here are some insights from their discussion.

Step Up Zero-Trust Efforts

***John Godfrey**, Chief Information Security Officer (CISO), Kansas Information Security Office*

The challenge is not only the velocity of attacks, Kansas' John Godfrey said. Successful attacks also can have a greater impact. As state and local agencies continue to digitize their operations and services, the underlying systems "become more interconnected, which creates a cascade [of problems] when an event does occur," he said.

As these threats mount, more states are likely to follow the federal government's lead and embrace zero trust. Godfrey said three components of zero trust are especially important:

Micro-segmentation: Breaking an enterprise network into multiple zones, each with its own security, makes it harder for a hacker who accesses one part of the network to jump quickly to other parts.

Least privilege: Give employees access only to the specific data, applications and network resources they need to do their jobs — which is to say, the least number of resources possible. Again, it's about limiting the damage a bad actor can do.

Audits and monitoring: As their network and security architectures evolve, agencies need to monitor performance and address any problems by making changes to the underlying technology stack.

Beyond specific technology issues, the current threat environment also requires agencies to adopt a new mindset, Godfrey said, recognizing that the best security is not foolproof. "We used to spend a lot of effort on [preventing attacks]," he said. "I think we have to shift a little bit and put more effort into [how we] respond and recover."

Plan for the Worst — and Test Your Plan

***Michael Carroll**, Area Vice President of Sales, U.S. State, Local and Education, Commvault*

When agencies turn their attention to cyber response and recovery, they might find themselves unsure how to proceed, said Commvault's Michael Carroll. Many try to adapt their disaster recovery plans, but that generally doesn't work, he said.

For example, if a data center goes down during a storm, you just shift your data and applications to a backup center. But that's not necessarily a good strategy in the event of a cyberattack. "That [would] assume the data's not corrupt, or that the bad actors aren't in the environment with their hands on the steering wheel," Carroll said.

To build an effective cyber response and recovery plan, you need to assemble a team representing all the stakeholders who would be involved following an incident: executives, departmental leaders, legislators, IT service providers, and IT and security teams, he said. Together, they can work out the appropriate response step-by-step.

The next stage of the process is more challenging, Carroll said: Test the plan. Because this is something organizations often struggle with, Commvault, whose data management and protection software supports disaster recovery operations, has a program called Minutes to Meltdown that helps customers stage simulated cyber events.

"Being able to test a cyber plan is an absolutely critical piece of the puzzle, and there are very few ways to do that, and very few partners that you can work with [that] are both technically viable and cost-effective," Carroll said.

Be Proactive in Building Trust

***Jim Richberg**, Head of Cyber Policy and Global Field CISO, Fortinet*

Across the federal space today, there's a risk of mis-, dis- and mal-information: false data used innocently, incorrect data shared maliciously or accurate data used inaccurately on purpose, respectively.

Fortinet's Jim Richberg calls this "MDM information" for short. While he describes it as a significant risk to election processes, it's something any federal agency might encounter.

Bad actors have a host of incentives, from financial gain to political advantage, to undermine trust in federal government. As agencies innovate, they must work with trusted vendors and technology providers that ensure the highest security levels, Richberg said.

Then, agencies must reassure the public that the modernized systems are, in fact, safe and secure. In the face of MDM information, it's not enough to implement all necessary cybersecurity measures, he said. Agencies also must craft clear messaging around them.

"Sunshine is the best antidote to counter these things," Richberg said. "It's being able to say, 'We have a route of trust. We can validate that something did or did not happen.'"

This is especially important when faith in government is historically low and social polarization is intensifying. "You've got to do this," he said. "You really have to build this narrative."

To learn more, watch the full session on demand.

Commvault FORTINET