FEDInsider

DATASHEET

Securing Federal Networks in a Heightened Threat Environment

Agencies are turning to a zero trust architecture and strong identity management protocols to protect networks, especially with a remote workforce.

The cyber threat landscape has vastly evolved during the pandemic, sending entire agencies to work remotely. This has resulted in an increase of high-profile cyber attacks. Agencies must act fast in their defense and responses, move to a zero trust architecture and follow the recent White House executive order on improving the nation's cybersecurity for the sake of national security.

Eight cybersecurity experts from government and industry gathered at FedInsider's recent Cyber Threats 2021 webinar to discuss the new technologies and tactics they've adopted to thwart cyber threats.

The following are some of the most important aspects of those efforts.

Setting the Cyber Threat Stage

The volume and sophistication of today's cyber threats are ever changing, said Gerald Caron III, chief information officer and assistant inspector general for IT for the Department of Health and Human Services' Office of Inspector General.

Organized, financed nation-state actors pose an urgent threat to federal systems. "I like to say there is a war going on that people don't understand every day. That secret war is one that we don't see on the battlefield, but it is ongoing within IT," Caron said.

Threat actors can change their tactics on a dime, and it's difficult to address ever changing threats with a proper defense. So, the government has taken to compliance to improve security, but Caron said agencies should really be measuring effectiveness.

"How can we make things be more effective?" he asked. "I think the greatest weakness we have is people. We still do a lot of things manually." People can unknowingly allow phishing attacks into the system, for instance, increasing the risk of insider threats depending on their administrative privileges. More user training and cyber hygiene education can help, as well as ensuring the right access is granted to the right people – and devices – at the right time.

A Pandemic-Fueled Federal Cybersecurity Landscape

Matt Swenson, chief of the Cyber Crimes Unit for the Department of Homeland Security's Homeland Security Investigations Cyber Crimes Center, said the agency has seen an uptick in the amount and volume of cyber crimes.

As society becomes more dependent on technology to accomplish day-to-day activities, attackers are using those same opportunities to exploit user activity online to steal data and monetize it. "It has become easier for [bad actors] to accomplish some fairly sophisticated attacks without necessarily having to be an expert," Swenson said.

It is important to note, however, that while the attacks can be sophisticated, they don't necessarily have to be in order to cause damage. "You also see some very

Featured Experts

- **Gerald Caron**
  CIO & Assistant Inspector General for IT, HHS, OIG

- **Matt Swenson**
  Chief, Cyber Crimes Unit, DHS HSI Cyber Crimes Ctr.

- **Patrick Sullivan**
  CTO, Security Strategy, Akamai

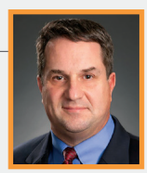
- **Jeffrey Lush**
  Chief Information Officer, USAF Air University

- **Kathleen Moriarty**
  Chief Technology Officer, Center for Internet Security

- **Dr. Robert Blumofe**
  EVP & CTO, Akamai

- **Jennifer Franks**
  Director, IT & Cybersecurity Team, GAO

- **Steve Winterfeld**
  Advisory CISO, Akamai



Akamai

effective attacks even from the world's pure nation-state attackers which are very much in line with what we see day-to-day, just automated credential attacks," said Patrick Sullivan, Chief Technology Officer of Security Strategy for Akamai.

Agencies should focus on patching vulnerabilities that can result in unauthorized access into a network. These come through exposed remote desktop service terminals, hardware remote access points or VPNs. "A lot of times, they are at the most common avenues for attackers to get that initial foothold into a network before they start moving laterally across," Swenson said.

These types of attacks were also exacerbated during the pandemic, largely due to the increased dependence on remote access points. Swenson saw an uptick of malicious web domains created for phishing attacks, cyber fraud schemes, spoof sites of pandemic-related sources or organizations, and credential harvesting.

Shifting to a zero trust architecture can vastly reduce the risk of bad actors accessing the network or server through a vulnerable point. When end users are given access to only what they need to do their job, attackers must go through various checks to get indirect access to the server, giving defenders more time to respond.

Improving Federal Security with Zero Trust Networking

"You should never have route-ability to the applications," said Dr. Robert Blumofe, Executive Vice President and CTO at Akamai. "All access to applications should go through a mediator like a proxy of some kind, and only if you are authorized can you get access to the application."

This is the theory behind a zero trust architecture, the protection approach agencies and organizations are implementing to better secure their networks and servers. Adopting zero trust, however, is a journey – and one the U.S. Air Force Air University has been constantly improving upon.

"It doesn't happen overnight. This is a multiyear project," said Jeffrey Lush, CIO of the U.S. Air Force Air University. The first step was getting stakeholders on board and agreeing to implement change, then identifying legacy systems that are not properly secured.

Kathleen Moriarty, CTO for the Center for Internet Security, added that implementing zero trust also requires making your network more encrypted. This starts by building controls at the endpoints, and by integrating hardened systems with CIS benchmarks and controls already in place.

"Requiring that of your vendors would be a big step," Moriarty said, as well as making sure that their networks are encrypted. She added that identity management is another critical place to start a zero trust journey, like focusing on access controls, privileges and implementing multi-factor authentication.

Securing Data with Identity Proofing in a Heightened Threat Environment

Implementing zero trust frameworks and identifying proofing tools helps thwart bad actors from accessing an entire organization's resources and putting mission-critical data at risk. As agencies work to improve identity management procedures, federal guidelines are in place to make the process easier.

The National Institute of Standards and Technology **published** Digital Identity Guidelines to provide agencies with a technical guide on identity proofing, and later updated the document to include resolving, validating and verifying an identity based on evidence obtained from a remote applicant.

"Having these frameworks to really center how you manage your programs and how you establish, design, implement and continue the management of your programs is really very important," said Jennifer Franks, Director of the IT and Cybersecurity Team for the Government Accountability Office.

This guidance also helps federal agencies as they form authentication systems and procedures for both employees and government contractors. That's why moving beyond username and password is critical. If there's one thing Steve Winterfeld, Advisory Chief Information Security Officer for Akamai, recommends agencies do to switch to identity management, it's to first change their mindset from simply securing an office or a data center, to being location-agnostic.

"Your identity should not care about where you are or what device you are on," he said. "Eventually, get the friction of identity out of the way for your users, and where possible, your customers too."

FEDInsider

Hosky Communications Inc.
3811 Massachusetts Avenue, NW
Washington, DC 20016

(202) 237-0300
Info@FedInsider.com
www.FedInsider.com
@FedInsiderNews
@FedInsider
Linkedin.com/company/FedInsider

Akamai

Akamai Technologies
11111 Sunset Hills Road, Suite 250
Reston, VA 20190

(617) 444-3000
Info@Akamai.com
www.Akamai.com
@AkamaiTechnologies
@Akamai
Linkedin.com/company/Akamai-Technologies