FEDInsider

CyberSmart 2024: Cybersecurity Faces A Rapidly Changing Landscape

Cybersecurity has always contended with evolving threats. As the internet has become more embedded into social and economic life and smart phones, tablets and other handheld devices have become ubiquitous, and bad actors have devised new methods of attacks to capitalize on emerging vulnerabilities.

Just as agencies are implementing zero trust architecture to help with this wave, other IT developments are threatening to upend cybersecurity even more. For instance, artificial intelligence is being incorporated into software, even as elected officials and regulatory agencies are trying to develop new rules of the road for its use. At the same time, historically offline operations technology is beginning to be integrated with IT systems, opening up the OT to attacks that previously weren't feasible.

At the Federal CyberSmart 2024 event, thought leaders from agencies and industry discussed the evolution of cyber threats and how the government is responding.

AI and Cybersecurity

The intelligence community is looking forward to developments in AI applications, according to the CIA's CIO and Director, ITE La'Naia Jones. "At the CIA, we don't look at artificial intelligence as one thing," she said. "We look at it as an area that will continue to grow and mature – we're looking at protecting our environments, our infrastructure, to deploy solutions, to augment our existing analysts, our officers. [It's] the ability for us to do things and to do it even more in an automated fashion to get things done quicker."

Deputy CTO of the Veterans Health Administration Joseph Ronzio said AI already is making it easier for his agency to see "patterns of life" for its clients, whether individuals are actually accessing data, using tools to access data or if they are being impersonated. "These detection algorithms VHA is using have been very good to establish that. In fact, we've detected several people that have utilized generative AI technologies within our enterprise against policy. So it increases the level of security overall for the organization."

In addition, Ronzio suggested that AI has the potential to develop cybersecurity tools that are more advanced than the attackers' weapons.

At the U.S. Treasury Department, the CISO and ACIO for Cybersecurity Sarah Nur said AI can help find the needle in the haystack. "That is something that really does plague us, honestly, in most organizations … The only way to detect it is if you have some kind of behavioral analysis or traffic analysis where you contextualize certain behaviors and time frames, things like that."

For Director of Solutions Engineering at Oracle Jim Donlon, it's about getting educated right now about what AI is capable of. Second, he said, "Get started now. You do not have to wait. You don't have to wait for policy to settle, you don't have to implement your enterprise strategy tomorrow. What you can do is say, 'I want to learn how this stuff works.' And you can do it in a low-cost, low-risk way."

When It Comes to ICAM, Think Like a User

The first pillar of a zero trust architecture is establishing identity for humans and devices alike. Humans, unlike devices, often have strong opinions about what works and what doesn't, what is easy and what is more difficult than IT professionals realize.

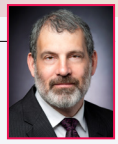
Featured Experts:

- **La'Naia Jones**
  CIO & Director, ITE, Central Intelligence Agency

- **Sarah Nur**
  ACIO-CS & CISO, U.S. Treasury Department

- **West Coile**
  Assistant Director, Center for Enhanced CS, U.S. GAO

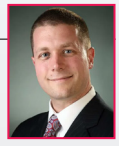
- **Russell Marsh**
  Director, CS Operations, National Nuclear Security Administration



- **Rahul Mittal**
  Cybersecurity Advisor for Region 3, CISA

- **Brian Dennis**
  Principal Technologist, Public Sector, Akamai

- **Joseph "Lucky" Ronzio**
  Deputy CTO, Veterans Health Administration



- **Anuj Mehta**
  Senior Solutions Engineer, U.S. Federal Team, Okta

- **Jim Donlon**
  Director of Solutions Engineering, Oracle

- **Marty Edwards**
  Deputy CTO, OT/IoT, Tenable

- **Blase Janov**
  Director, Business Dev. NA, Waterfall Security Solutions

Assistant Director of the Center for Enhanced CS at the Government Accountability Office West Coile said that while PIV and CAC are the "gold standard" for identity control and access management, they don't work in all situations.

"As agencies move more into the cloud, zero trust comes into play – not just for your own resources but also for controlling those in the cloud," Coile said. "Guidance is saying that you should be looking at cloud-based solutions to handle access control and the identity part of access control. If you have a hybrid environment... It's just uniquely positioned to do that."

One aspect of cybersecurity that frustrates users immensely is the password requirement. "The average American has about 80 to 100 different programs they are using that require passwords, but how many passwords do they actually have? The average American has five," said Technologist for the Public Sector at Akamai Brian Dennis. That is why educating users about why passwords are so important whether they are at work, at home or on the go for protecting their own and their employers' critical information is crucial.

Establishing a zero trust environment will go a long way to alleviating that burden, said Solutions Engineer for the U.S. Federal Team at Okta Anuj Mehta.

"We know CISA's pillars of zero trust," he said. "One is identity – know who the people are – but we need to know the context, as well. What device they are coming in on, is it a managed or unmanaged device? Where are they coming from, what location – from the office, logging in from home, logging in from the United States? Or a beach in Cancun? And then, what are they trying to access, data or applications, and what mechanism are they using? Do they have the right MFA access? Are they using their PIV card or something else?"

Mehta pointed out that in zero trust there is centralized data management to make those access decisions. "We need to have all that risk-based contextual information and bring it together to make the access decision," he said.

"Two weeks ago, the head of the cybersecurity group in the U.K. put out a report saying that the rise of AI is only going to make things worse for cybersecurity," Dennis noted.

Mehta responded, "ICAM requirements will change, increase and evolve, but in the world of AI our threats will be using those tools as well, so you have to be able to figure out what is happening immediately. So automation comes into play, to detect those events in real-time and react appropriately."

Pay Attention to IT/OT Convergence Resiliency

Historically, operations technology (OT) has not been connected to the internet, but as smartphones, tablets and other handheld devices continue to spread, organizations have begun to break down that barrier. The use of OT is spreading rapidly across government agencies at all levels as they use remotely controlled sensors and devices for many applications.

Bringing IT into an OT environment offers productivity gains, but it also opens up the OT to new cyber threats. The risks of this convergence can be seen in the Colonial Pipeline shutdown – the cyberattack was on the company's IT, but the company's pipeline OT was within reach, leading to the decision to shut the pipeline down until the attack was mitigated.

Historically, IT and OT were fairly separate systems, said the GAO's Coile. "The OT folks were dealing with things that affect the physical world, taking measurements from or making changes to. Historically, they were seen more as engineering projects, totally separate from the IT folks. That has changed, but there's a really long cycle time on changing those devices," he said.

The integration of IT and OT security practices and systems is critical, said Cybersecurity Advisor for Region 3 at CISA Rahul Mittal. In conversations between OT and IT people, "they are realizing there's a lot of benefits to working together," Mittal said. "They can share resources and they can make sure they are protecting each other. And if they see threats on their side, they can let the other side know."

The silos of IT and OT are still in place in many agencies, said Director of Cybersecurity Operations for the National Nuclear Security Administration Russell Marsh. "Just recently, we were deploying capabilities on the IT cybersecurity side of the house, and we finally found the OT engineer. He'd been working there for years, I didn't know who he was, yet their stuff is connected to the [IT] network. Once they got together and started to talk, the OT side was getting excited about what the cybersecurity staff was doing because it made some of their jobs easier."

There are commonalities between the two sides, Marsh added, but you need expertise from both sides to leverage and take full advantage of how to secure the overall system.

"I believe it's the organizational structure and the human element that probably pose the biggest challenge now," said Deputy CTO for OT and IoT at Tenable Marty Edwards, agreeing with Marsh. "There used to be a lot of animosity between the IT and the OT groups. Once you get past that, we all work for the government mission that we are supporting. So even though we work for two different departments, we are pulling the train in the same direction."

The biggest difference between the two environments is that while IT gets refreshed relatively frequently, whether with software updates or new hardware, OT systems tend to stay in place for quite a long time. "These OT environments are so sensitive," said Director of Business Development North America for Waterfall Security Solutions Blase Janov. "In a perfect world we would get the legacy systems out of there, but the reality is, across all the accounts we work with, that is not the case, and it probably won't be for some time. You have to worry about that level of sensitivity in terms of managing all your threat vectors into these environments, which becomes burdensome."

Janov said AI cybersecurity solutions aren't currently well suited to OT environments. "Where AI is not really going to deploy so much from a cybersecurity standpoint into OT is automated responses, having AI do something that humans would normally do," he said. "OT is not quite ready for that. But it is driving a lot of the requirement for the connectivity into the networks, because things like cloud analytics and predictive analytics maintenance, they're utilizing a lot of AI to crunch the data that's giving all these benefits to OT environments."

FEDInsider

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

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

carahsoft.

Carahsoft
11493 Sunset Hills Road, Suite 100
Reston, VA 20190

(703) 871-8548
Info@Carahsoft.com
Carahsoft.com
Facebook.com/Carahsoft
Linkedin.com/company/Carahsoft
@Carahsoft

© 2024 Hosky Communications, Inc. All rights reserved. FedInsider and the FedInsider logo, are trademarks or registered trademarks of Hosky Communications or its subsidiaries or affiliated companies in the United States and other countries. All other marks are the property of their respective owners.