FEDERAL NEWS NETWORK

EXECUTIVE BRIEFING SERIES:

Mitigating Cyber Risk

Sponsored by LOOKINGGLASS

Cybersecurity in time of pandemic: How to mitigate the risks

BY TOM TEMIN

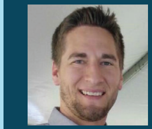
Best practices in cybersecurity aren't what they used to be. At least not since the pandemic transformed the extent of telework and virtual private network usage. Federal agencies IT and cybersecurity staffs are looking more and more at how to build in zero trust capabilities, a methodology of ensuring even known credentials – which can be hacked or misused – have carefully controlled access even once the user is authenticated.

And, they're moving to the concept known as network detection and response (NDR) – a way of getting more comprehensive visibility into networks, clouds, endpoints and applications.

For the latest into how agencies are approaching cybersecurity in the new climate, Federal News Network and LookingGlass brought together a panel of expert practitioners.

"The most important considerations now," said Nick Marinos, the director of IT and cybersecurity issues at the Government Accountability Office, "are risk assessment and inventory." Without an adequate inventory of IT assets, it simply becomes more difficult to manage the risks, he said. Across the government, Marinos said, auditors find a "nagging issue" of incomplete inventories of hardware and software. "What you can't see will take you down," he added.

PANEL OF EXPERTS



Chris Dahlheimer, Vice President of CloudShield, NextGen Cyber, LookingGlass Cyber Solutions

Jonathan Feibus, Chief Information Security Officer, Nuclear Regulatory Commission

Alper Kerman, Cybersecurity Engineer and Project Manager, National Cybersecurity Center of Excellence, National Institute of Standards and Technology

Nick Marinos, Director, IT and Cybersecurity Issues, Government Accountability Office

Mike Witt, Associate Chief Information Officer for Cybersecurity & Privacy and Senior Agency Information Security Officer, NASA

With regard to establishing a zero trust environment, agencies now have detailed guidance from the National Institute of Standards and Technology's National Cybersecurity Center of Excellence (NCCOE).

Zero trust = high trust

Alper Kerman is the lead for zero trust at the NCCOE. Kerman noted that NIST has a draft publication describing in detail the whole topic of visibility and zero trust architectures, Special Publication 800-207. He described zero trust as a "cybersecurity strategy that focuses on policy-based resource protection." Zero trust takes a comprehensive view of resources, which may be on local devices, in federal data centers, or in commercial clouds. And it encompasses an approach governed by a risk management framework, such that time and effort is concentrated on assets or resources according to their value or sensitivity.

Within that framework, Kerman said, "trust is never granted implicitly, but must be continually evaluated." The guidance, he added, "includes programs, technology and systems that provide continuous diagnostics and mitigation, industry compliance, threat intelligence, network activity logging, logging certificates" and information thrown off by security information and event management (SEIM) systems.

Kerman and others said effective products and technologies for improving security through zero trust all provide for continuous diagnostics and mitigation (CDM), identity and access management, configuration and vulnerability management, and SEIM.

"With these kinds of components we can detect privilege escalations, use of administrative privileges, unauthorized access to sensitive data, malicious access attempts, and suspicious logins and authentications," Kerman said. The tools can also help maintain up-to-date inventories of assets through device discovery and assessment. And greater visibility in network generally, which in turn aids faster response to adverse incidents.

To protect it, see it

Improving cybersecurity, then, involves many moving parts. Working practitioners know this. Jonathan Feibus, the chief information security officer at the Federal Deposit Insurance Company, described a typical situation.

Before the advent of cloud, Feibus said, it was easier to see and analyze what he called hosts connected to the network. Now, "virtual hosts are being spun up and spun down. It's more difficult to keep track of your inventory in real time. I know the types of hosts I might have on my network at any time, but not the exact number." His shop uses cloud access security brokers and tools from CDM and other sources to maintain visibility "when I bring up a new service, when I bring up a new tenant."

Feibus added, "It's not a set and forget. It's a 'keep evaluating.'" Sometimes, he said, a virtual machine might shut down. When it reappears, it needs rescanning to ensure it has whatever patches may have been required in the meantime.

NASA also had a visibility challenge when it started its CDM program three years ago, said Mike Witt, associate CIO for cybersecurity and privacy at NASA.

"We started getting visibility not just into who was on our network, but also what was on our network – devices, and what was installed on those devices. It's eye opening when you start to see the breadth of what you actually have on your enterprise."

The move cloud architectures and, more recently, by the seemingly permanent growth in telework and its need for remote access, have transformed that federal enterprise and therefore the cybersecurity strategies most suitable for protecting it. Witt described the telework situation as going from 12 NASA centers where everyone worked, to having in effect 60,000 centers, with everyone home.

"The days of castle-and-moat cybersecurity defenses are definitely over," said Chris Dahlheimer, vice president at LookingGlass Cyber Solutions. Visibility into today's hybrid network topologies, he said, requires data gathered from both the network and the endpoints.

Beyond that, be sure to see and understand the internal connections, the way micro network segments communicate and interact. "Even in the network," Dahlheimer said, "it's not just the perimeter but also enclaves. We need to look at internal communications as well as everything communicating externally. Within the zero trust paradigm, every communication needs to be authenticated, analyzed, and processed. Every asset communicating on the network needs to be critically inspected and analyzed for proper behavior."

That model leads to the need for what Dahlheimer called policy based points of enforcement and detection, for all of the communications within the mesh that comprises the contemporary IT enterprise. This is where extended detection and response, and its emerging successor NDR, come in, he said. The emerging Gartner quadrant seeks to capture the integration of endpoint and network data gathering and subsequent application of cybersecurity measures.

Detection – then what?

Detection leading to visibility, and vice versa: Those are the foundational step in the mitigation of the volumes of threats and attack attempts the average federal network faces each day. But visibility must lead to actionable information within a risk management framework – the mitigation in CDM, if you will.

Panelists agreed that processing requirements grow as you add and aggregate network log and endpoint data. They also agreed that the greater levels of data permit more fine-grained analysis.

And, Dahlheimer said, "The more you can correlate and aggregate, the more informed your decision is going to be."

Practitioners should realize the importance of understanding that you can't take the human operator out of the chain of events.

"The response shouldn't just be blocking or dropping," Dahlheimer said. Better to "quarantine the host, slow down the communications with that host, until an operator can review and make a decision."

Aggregation of multiple data sources is also important, Feibus said, because different subsystems – for instance a security orchestration tool versus an event monitor – produce

different outputs. He said network response and orchestration tools will need to work in concert to guide security operators to an answer, whether a patch or some zero-day response. And it must happen in a manner that doesn't "not take over all [users'] bandwidth and killing their video conference or their analysis session." The new levels of remote working exaggerate that potential.

A given network will have a range of resources from brand new application and devices to obsolete servers and software that might lie beyond patching. NIST's Kerman advised having a holistic approach to risk mitigation, driven by what he called a policy engine that takes into account the value of the asset in question when allowing or denying an access request. Use data from your SIEM to continuously refine the policy engine and improve the overall security posture and the zero trust quality of the network.

NASA collects the security-related data in a repository. Witt said a new vulnerability alert run against the repository showed that some NASA systems were using the software. Witt's shop could notify the users the same day of a patch requirement.

For agencies seeking to improve their cybersecurity game, the takeaway is that they must render the big data challenge from a network collection standpoint into a good data challenge through analytics.

Dahlheimer said that beyond detection and patching, a technique called vulnerability camouflaging has emerged. The technique results in the response from a server to, say, an exfiltration attack appears as if it is patched, giving the organization extra time to actually apply the requisite patches or replace the system. "There's always going to be a Windows XP server somewhere," he quipped, perhaps driving a traffic sign. You can't block its port if it's doing work, but you can at least hide the vulnerability with camouflage.

Ultimately mitigating risk in a continuously improving way requires more than the right data collection, analysis and response. CISOs must gain traction "not just in the corporate environments but specifically in the mission environments," Witt said. "That's the tough part to get into for the trust. It's really building relationships and trust, so that they see value and not just compliance." Witt added, "This is about getting together to protect our assets, our intellectual property."